ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEBINTELLIGENCE

Ασφάλεια σε Φορετές Ιατρικές Συσκευές

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΜΑΓΔΑΛΗΝΗΣ ΜΠΑΛΑΤΑΖΗΣ

Επιβλέπων : Χρήστος Ηλιούδης

Καθηγητής ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Φεβρουάριος 2026

Η σελίδα αυτή είναι σκόπιμα λευκή.

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEB INTELLIGENCE

Ασφάλεια σε Φορετές Ιατρικές Συσκευές

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΜΑΓΔΑΛΗΝΗΣ ΜΠΑΛΑΤΑΖΗΣ

Επιβλέπων : Χρήστος Ηλιούδης
Καθηγητής ΔΙ.ΠΑ.Ε.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις ……..

(Υπογραφή)	(Υπογραφή)	(Υπογραφή)
……..	……..	……..
Όνομα Επώνυμο ΔΙ.ΠΑ.Ε.	Όνομα Επώνυμο ΔΙ.ΠΑ.Ε.	Όνομα Επώνυμο ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Φεβρουάριος 2026

(Υπογραφή)

.....

Τίτλος Δ.Ε. Ασφάλεια σε Φορετές Ιατρικές Συσκευές
Κωδικός Δ.Ε. 25291
Ονοματεπώνυμο φοιτητή/τών Μαγδαληνή Μπαλτατζή
Ονοματεπώνυμο εισηγητή Χρήστος Ηλιούδης
Ημερομηνία ανάληψης Δ.Ε. 4/8/2025
Ημερομηνία περάτωσης Δ.Ε. 6/2/2026

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Η ραγδαία εξέλιξη της τεχνολογίας έχει οδηγήσει στην εμφάνιση και τη μαζική υιοθέτηση των φορετών ιατρικών συσκευών, οι οποίες υπόσχονται να φέρουν επανάσταση στον τομέα της υγείας, παρέχοντας συνεχή παρακολούθηση και εξατομικευμένη φροντίδα. Ωστόσο, η συλλογή, αποθήκευση και μετάδοση ευαίσθητων προσωπικών και ιατρικών δεδομένων καθιστά την ασφάλεια αυτών των συσκευών ένα ζήτημα υψίστης σημασίας, τόσο για τους χρήστες όσο και για τους επαγγελματίες υγείας. Η επιλογή του θέματος, ασφάλεια φορετών ιατρικών συσκευών, αποτέλεσε φυσική απόρροια του ιδιαίτερου ενδιαφέροντός μου για την διασφάλιση της κυβερνοασφάλειας σε αυτό το εξαιρετικά ευαίσθητο και κρίσιμο περιβάλλον της ψηφιακής υγείας. Η σπουδαιότητα των δεδομένων υγείας, σε συνδυασμό με την ταχύτατη εξάπλωση της τεχνολογίας IoT στον ιατρικό τομέα, κατέστησε το θέμα αυτό την ιδανική και επίκαιρη επιλογή για την ολοκλήρωση των σπουδών μου.

Η εκπόνηση της εργασίας αυτής υπήρξε εξαιρετικά ωφέλιμη. Απέκτησα εξειδικευμένη γνώση στην εφαρμογή πρωτοκόλλων ασφάλειας και κρυπτογράφησης για ιατρικές φορετές συσκευές. Επίσης, με βοήθησε, μέσω της κριτικής σκέψης, να εντοπίσω και να ιεραρχήσω τους πραγματικούς κινδύνους που αντιμετωπίζουν οι συσκευές, λαμβάνοντας υπόψη τόσο την τεχνολογία όσο και τη νομοθεσία για τα δεδομένα.

Περίληψη

Η παρούσα διπλωματική εργασία, ασχολείται με τη διττή πρόκληση της τεχνολογικής εξέλιξης και της κυβερνοασφάλειας στο πεδίο των φορετών ιατρικών συσκευών. Ενώ οι συγκεκριμένες συσκευές υπόσχονται μια επανάσταση στην προληπτική ιατρική, η μαζική συλλογή και διαχείριση ευαίσθητων προσωπικών δεδομένων τις καθιστά στόχο, αναδεικνύοντας την επιτακτική ανάγκη για ισχυρά μέτρα προστασίας. Βασικός σκοπός της εργασίας είναι η συστηματική τεχνολογική επισκόπηση των συσκευών, η ανάλυση των πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται και η αξιολόγηση των ευπαθειών ασφάλειας που προκύπτουν σε αυτό το ευαίσθητο περιβάλλον.

Η ανάλυση ξεκινά με την αρχιτεκτονική του συστήματος, εξετάζοντας τη λειτουργική δομή των συσκευών και τη διαστρωμάτωση του δικτύου, από το επίπεδο συλλογής δεδομένων έως την τελική εφαρμογή, δίνοντας έμφαση στις κρίσιμες τεχνικές ενεργειακής βελτιστοποίησης που διασφαλίζουν τη βιωσιμότητα του συστήματος. Ακολούθως, εξετάζονται οι ευπάθειες που εντοπίζονται σε επίπεδο επικοινωνίας, υλικού και λογισμικού. Παράλληλα, γίνεται αναφορά στο νομικό πλαίσιο και στα προσωπικά δεδομένα εστιάζοντας στις επιπτώσεις της κακόβουλης χρήσης και στις απαιτήσεις για αξιοπιστία των δεδομένων υγείας. Ο πυρήνας της έρευνας επικεντρώνεται στην ανάλυση των διαύλων επικοινωνίας, όπου διερευνώνται διεξοδικά τα σχετικά πρωτόκολλα, ενώ παράλληλα αξιολογούνται προηγμένοι μηχανισμοί ασφάλειας για τη θωράκιση των δεδομένων. Τέλος, παρουσιάζεται το πειραματικό μέρος της εργασίας, το οποίο αφορά την ανάπτυξη και αξιολόγηση ενός Συστήματος Ανίχνευσης Εισβολών (IDS).

Τα συμπεράσματα της εργασίας αναδεικνύουν τις κρίσιμες ευπάθειες σε κάθε επίπεδο και σε κάθε πρωτόκολλο επικοινωνίας. Η έρευνα προτείνει την εφαρμογή συνδυασμού ισχυρών κρυπτογραφικών μεθόδων και την πλήρη υιοθέτηση των σχετικών προτύπων, ως απαραίτητη προϋπόθεση για την επίτευξη αξιόπιστης και ασφαλούς ενσωμάτωσης των φορετών ιατρικών συσκευών στον κόσμο της ψηφιακής υγείας. Η συμβολή της εργασίας έγκειται στην παροχή μιας λεπτομερούς ανάλυσης των τεχνικών και ρυθμιστικών προκλήσεων, συμβάλλοντας στην ασφάλεια των ιατρικών δεδομένων.

Λέξεις Κλειδιά: Ασφάλεια δεδομένων, Φορετές Ιατρικές Συσκευές, IoMT, Κρυπτογράφηση, Πρότυπα Ασφάλειας, Πρωτόκολλα Επικοινωνίας.

Η σελίδα αυτή είναι σκόπιμα λευκή.

«Security in Wearable Medical Devices»

«Magdalini Baltatzi»

Abstract

This thesis addresses the dual challenge of technological evolution and cybersecurity in the field of wearable medical devices. While these devices promise a revolution in preventive medicine, the massive collection and management of sensitive personal data makes them a prime target, highlighting the imperative need for robust protection measures. The primary objective of this work is a systematic technological overview of these devices, an analysis of the communication protocols used, and an evaluation of the security vulnerabilities arising in this sensitive environment.

The analysis begins with the system architecture, examining the functional structure of the devices and the network layering, from the data collection level to the end-user application, with an emphasis on critical energy optimization techniques that ensure system sustainability. Subsequently, vulnerabilities identified at the communication, hardware, and software levels are examined. Concurrently, reference is made to the legal framework and personal data, focusing on the implications of unauthorized use and the requirements for the integrity of health data. The core of the research focuses on the analysis of communication channels, where relevant protocols are thoroughly investigated, alongside the evaluation of advanced security mechanisms for data fortification. Finally, the experimental part of the thesis is presented, involving the development and evaluation of an Intrusion Detection System (IDS).

The conclusions of this work highlight critical vulnerabilities at every layer and within each communication protocol. The research proposes the implementation of a combination of strong cryptographic methods and the full adoption of relevant standards as a necessary prerequisite for achieving the reliable and secure integration of wearable medical devices into the world of digital health. The contribution of this thesis consists in providing a detailed analysis of technical and regulatory challenges, thereby enhancing medical data security.

Keywords: Data Security, Wearable Medical Devices, Internet of Medical Things, Encryption, Security Standards, Communication Protocols.

Η σελίδα αυτή είναι σκόπιμα λευκή

Ευχαριστίες

Θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες σε όλους όσοι συνέβαλαν, άμεσα ή έμμεσα, στην ολοκλήρωση της παρούσας διπλωματικής εργασίας. Ιδιαίτερες ευχαριστίες απευθύνω στον επιβλέποντα καθηγητή κ. Ηλιούδη, για την επιστημονική καθοδήγηση και τη στήριξη καθ' όλη τη διάρκεια της εκπόνησής της.

Θερμές ευχαριστίες στην οικογένειά μου, η οποία στάθηκε δίπλα μου σε κάθε δυσκολία και απογοήτευση, προσφέροντας αδιάκοπη ηθική υποστήριξη και ενθάρρυνση.

Περιεχόμενα

Κατάλογος Σχημάτων

Συντομογραφίες

BLE	Bluetooth Low Energy
CSMA	Carrier Sense Multiple Access
CCD	Continuity of Care Document
DP	Differential Privacy
e-PHI	Electronic Protected Health Information
EDA	Energy Depletion Attack
GDPR	General Data Protection Regulation
HDP	Health Device Profile
HIPAA	Health Insurance Portability and Accountability Act
ISMS	Information Security Management System
ISO	International Organization for Standardization
IoMT	Internet of Medical Things
IDS	Intrusion Detection System
KNN	K-Nearest Neighbors
LDP	Label Distribution Protocol
MitM	Man in the Middle
MBAN	Medical Body Area Network
MDSW	Medical Device Software
MANET	Mobile Ad hoc NETwork
NIST	National Institute of Standards and Technology
OEP	Optimized Exchange Protocol
PAN	Personal Area Network
PHD	Personal Health Devices

SMOTE	Synthetic Minority Over-sampling Technique
TPC	Transmission Power Control
WUSTL-EHMS	Washington University in St. Louis - Enhanced Healthcare Monitoring System
WMDs	Wearable Medical Devices
WBAN	Wireless Body Area Network
ΗΚΓ	Ηλεκτροκαρδιογράφημα

Κεφάλαιο 1ο: Εισαγωγή

1.1 Ερευνητικό πλαίσιο

Η συνεχής πρόοδος της τεχνολογίας στον τομέα του Internet of Medical Things (IoMT) έχει καταστήσει τις φορετές ιατρικές συσκευές βασικά εργαλεία παρακολούθησης της υγείας των ασθενών, τόσο εντός όσο και εκτός νοσοκομείων. Συσκευές όπως έξυπνα ρολόγια, αισθητήρες καρδιακού ρυθμού και γλυκόζης, χρησιμοποιούνται ευρέως για τη συνεχή συλλογή και αποστολή βιομετρικών δεδομένων. Ωστόσο, συνοδεύονται από σημαντικές προκλήσεις ασφάλειας και ιδιωτικότητας, εξαιτίας της φύσης των δεδομένων και του τρόπου λειτουργίας τους. Συγκεκριμένα:

- Λειτουργούν με περιορισμένους υπολογιστικούς και ενεργειακούς πόρους.
- Χρησιμοποιούν συχνά μη ασφαλή πρωτόκολλα επικοινωνίας.
- Αποστέλλουν ευαίσθητα ιατρικά δεδομένα σε απομακρυσμένα δίκτυα και cloud servers.

Η παραβίαση της ασφάλειας μπορεί να οδηγήσει σε διαρροή προσωπικών δεδομένων, παραποίηση ιατρικών ενδείξεων ή ακόμα και παρεμπόδιση της λειτουργίας της συσκευής, γεγονός που ενδέχεται να θέσει τη ζωή του ασθενούς σε κίνδυνο. Επομένως, η διατήρηση της ασφάλειας, της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας των δεδομένων, καθώς και η διασφάλιση της ορθής λειτουργίας των συσκευών, αποτελεί κρίσιμη πρόκληση.

1.2 Σκοπός και στόχοι της εργασίας

Σκοπός της παρούσας εργασίας είναι η συστηματική διερεύνηση και αξιολόγηση των κινδύνων ασφάλειας που αντιμετωπίζουν οι σύγχρονες φορετές ιατρικές συσκευές. Η παρούσα μελέτη διερευνά την αρχιτεκτονική που διέπει τις φορετές ιατρικές συσκευές, εστιάζοντας στη διαχείριση δεδομένων και την ενεργειακή απόδοση, την ανάλυση του νομοθετικού πλαισίου, τις επιπτώσεις της μη εξουσιοδοτημένης χρήσης και την αξιοπιστία των δεδομένων υγείας. Επικεντρώνεται επίσης, στα πρωτόκολλα επικοινωνίας και τα πρότυπα που χρησιμοποιούνται, με έμφαση στις ευπάθειες ασφάλειας καθώς και τους βασικούς κρυπτογραφικούς αλγορίθμους ως μέτρα προστασίας των δεδομένων κατά τη μετάδοση και την αποθήκευση.

1.3 Ερευνητικά ερωτήματα

Η εργασία, καλείται να απαντήσει σε ερευνητικά ερωτήματα που σχετίζονται με:

- Την πολυεπίπεδη αρχιτεκτονική δικτύου των φορετών ιατρικών συσκευών, η οποίο δημιουργεί ευάλωτα σημεία που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι.
- Τις κύριες ευπάθειες ασφάλειας που χαρακτηρίζουν τα βασικά πρωτόκολλα ασύρματης επικοινωνίας και πώς μπορούν να οδηγήσουν σε παραβίαση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.
- Την αποτελεσματικότητα των προτεινόμενων μηχανισμών κρυπτογράφησης και ασφάλειας, στη διασφάλιση της συμμόρφωσης με τις απαιτήσεις του GDPR, HIPAA και των προτύπων ISO, NIST SP και IEEE για την προστασία των προσωπικών δεδομένων.
- Την επίτευξη μιας ολοκληρωμένη στρατηγικής ασφάλειας που να λαμβάνει υπόψη τόσο τις τεχνικές προκλήσεις όσο και τις κανονιστικές υποχρεώσεις στην ανάπτυξη και λειτουργία των φορετών ιατρικών συσκευών

1.4 Δομή εργασίας

Η εργασία αποτελείται από επτά κεφάλαια, τα οποία εστιάζουν στις φορετές ιατρικές συσκευές, την αρχιτεκτονική και τα πρωτόκολλα επικοινωνίας που χρησιμοποιούν. Πιο συγκεκριμένα, στο πρώτο κεφάλαιο παρουσιάζεται το ερευνητικό πλαίσιο, οι στόχοι και τα ερευνητικά ερωτήματα. Στο δεύτερο κεφάλαιο αναλύεται η αρχιτεκτονική των φορετών ιατρικών συσκευών, τα προηγμένα υλικά και οι τεχνικές ενεργειακής απόδοσης δίνοντας ιδιαίτερη έμφαση στις προκλήσεις της διαχείρισης δεδομένων σε περιβάλλοντα περιορισμένων πόρων. Στο τρίτο κεφάλαιο περιγράφονται οι ευπάθειες των φορετών ιατρικών συσκευών καθώς και θέματα που σχετίζονται με την ασφάλεια των συσκευών. Στο τέταρτο κεφάλαιο γίνεται αναφορά στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR), στο Health Insurance Portability and Accountability Act (HIPAA), στα πρότυπα ISO, NIST και IEEE για την προστασία των προσωπικών δεδομένων υγείας καθώς και πως εφαρμόζονται σε συσκευές IoMT. Εξετάζονται οι συνέπειες της μη εξουσιοδοτημένης χρήσης και οι απαιτήσεις για την κυβερνοασφάλεια και την αξιοπιστία των δεδομένων. Στο πέμπτο κεφάλαιο αναλύονται τα βασικά πρωτόκολλα επικοινωνίας, τονίζοντας τις σχετικές ευπάθειες ασφάλειας. Στο έκτο κεφάλαιο παρουσιάζεται η πειραματική υλοποίηση και η αξιολόγηση του προτεινόμενου συστήματος ανίχνευσης εισβολών (IDS) και τέλος στο έβδομο κεφάλαιο καταγράφονται τα συμπεράσματα καθώς και μελλοντικές επεκτάσεις.

Κεφάλαιο 2ο: Τεχνολογική Επισκόπηση

2.1 Εισαγωγή

Τα τελευταία χρόνια, η ψηφιοποίηση της υγειονομικής περίθαλψης έχει επιταχυνθεί ραγδαία, με τις φορετές ιατρικές συσκευές να βρίσκονται στο επίκεντρο αυτής της επανάστασης. Οι φορετές ιατρικές συσκευές έχουν εξελιχθεί σε πολυλειτουργικά εργαλεία ικανά να συλλέγουν, να αναλύουν και να μεταδίδουν ζωτικής σημασίας κλινικά δεδομένα σε πραγματικό χρόνο. Η ικανότητά τους να παρέχουν συνεχή, μη επεμβατική παρακολούθηση έχει ανοίξει νέους δρόμους για την εξατομικευμένη ιατρική, την πρόληψη ασθενειών, τη διαχείριση χρόνιων παθήσεων και τη μείωση του κόστους περίθαλψης. Πριν εμβαθύνουμε στις κρίσιμες πτυχές της ασφάλειας και της ιδιωτικότητας που σχετίζονται με αυτόν τον τομέα, το παρόν κεφάλαιο έχει ως στόχο να παρουσιάσει μία συστηματική τεχνολογική επισκόπηση του συστήματος των φορετών ιατρικών συσκευών.

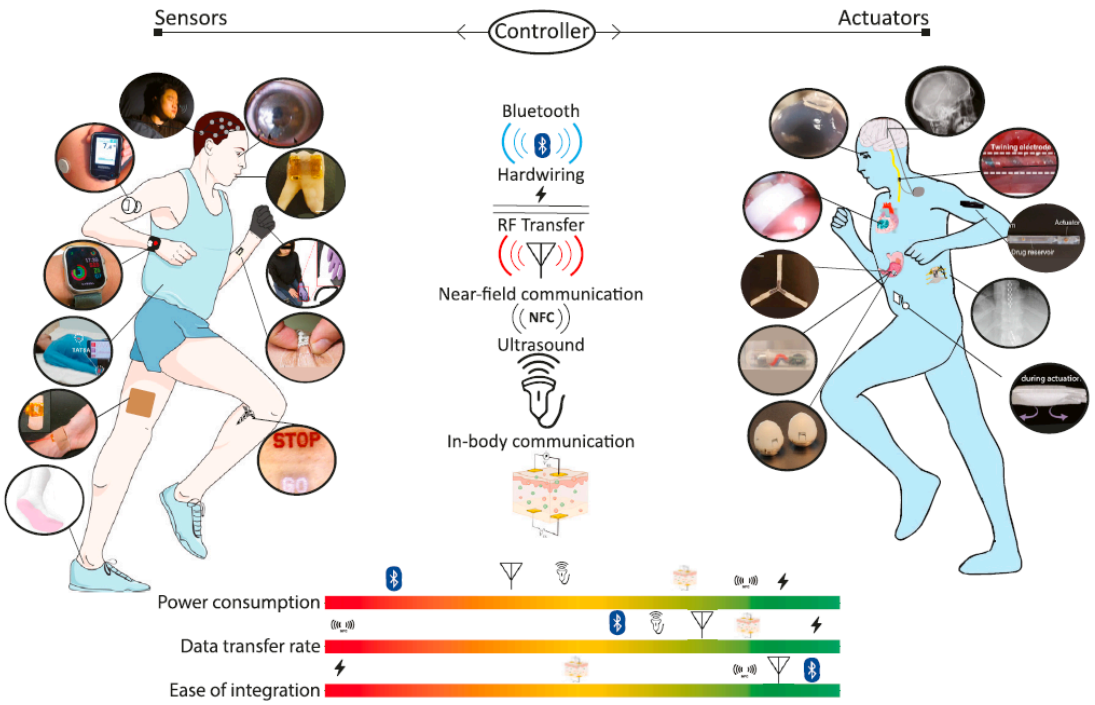
Θα γίνει λόγος για τους βασικούς τύπους και τις εφαρμογές των σύγχρονων φορετών ιατρικών συσκευών, τα δομικά στοιχεία των συσκευών, με έμφαση στους αισθητήρες και τους μικροεπεξεργαστές, τους μηχανισμούς επικοινωνίας και την αρχιτεκτονική δικτύωσης που καθιστούν δυνατή τη μεταφορά ευαίσθητων δεδομένων. Επιπλέον, θα παρουσιάσουμε τις προκλήσεις που σχετίζονται με τη διαχείριση ενέργειας και την αξιοπιστία των δεδομένων.

Η κατανόηση αυτού του τεχνολογικού πλαισίου είναι απαραίτητη για την ακριβή αξιολόγηση των ευπαθειών και των κινδύνων που ελλοχεύουν σε αυτό το διασυνδεδεμένο περιβάλλον, θέτοντας έτσι τη βάση για την ανάλυση της ασφάλειας.

2.2 Φορετές ιατρικές συσκευές

Η σύγχρονη υγειονομική περίθαλψη μετασχηματίζεται ριζικά, απομακρυνόμενη από το παραδοσιακό μοντέλο όπου το νοσοκομείο ήταν το κέντρο σε μια προσωποκεντρική προσέγγιση [1]. Σε αυτό το πλαίσιο, οι φορετές ιατρικές συσκευές (Wearable Medical Devices) αποτελούν καινοτόμες λύσεις, επιδεικνύοντας τεράστιο δυναμικό για ένα ευρύ φάσμα εξατομικευμένων εφαρμογών και θεραπευτικών λύσεων [2].

Οι φορετές ιατρικές συσκευές στοχεύουν στην ανάπτυξη ασφαλών και αξιόπιστων λύσεων για τη συνεχή παρακολούθηση της υγείας, την έγκαιρη ανίχνευση ασθενειών και την προληπτική ιατρική. [3]. Σύμφωνα με την βιβλιογραφία [4-5], οι συγκεκριμένες συσκευές χαρακτηρίζονται από αυτονομία και δυνατότητα εκτέλεσης μιας συγκεκριμένης ιατρικής λειτουργίας όπως παρακολούθηση ή υποστήριξη για παρατεταμένο χρονικό διάστημα. Στο Σχήμα 1 παρουσιάζεται η δομή και οι τεχνολογικές πτυχές των φορετών ιατρικών συσκευών, που περιλαμβάνει τους αισθητήρες, τις τεχνολογίες επικοινωνίας και τους ενεργοποιητές.



Σχήμα 1: Φορετές συσκευές και τεχνολογίες επικοινωνίας σε ένα δίκτυο αισθητήρων [6]

Ο όρος φορετή είναι το κεντρικό χαρακτηριστικό που διακρίνει τις συγκεκριμένες ιατρικές συσκευές από τις παραδοσιακές. Υποδηλώνει τη φυσική θέση και τον τρόπο εφαρμογής της συσκευής, ο οποίος πρέπει να είναι συνεχής, άνετος και μη επεμβατικός για τον χρήστη. Επίσης, είναι άρρηκτα συνδεδεμένος με τη δυνατότητα της συσκευής να υποστηρίζεται με δύο κύριους τρόπους, επιτρέποντας τη μακροχρόνια και συνεχή παρακολούθηση της υγείας [4]:

1. Συστήματα υποστηριζόμενα από το ανθρώπινο σώμα

Τα συγκεκριμένα συστήματα έρχονται σε άμεση επαφή με το δέρμα του χρήστη, επιτυγχάνοντας μια ακριβή και οικεία διεπαφή [2]. Η τοποθέτηση αυτή είναι κρίσιμη για τη συλλογή υψηλής ποιότητας βιομετρικών δεδομένων, όπως τα ηλεκτρικά σήματα της καρδιάς ή η θερμοκρασία. Παραδείγματα αποτελούν, τα δερματικά επιθέματα όπως, εύκαμπτοι αισθητήρες που εφάπτου στο δέρμα και συχνά χρησιμοποιούνται για την συνεχή παρακολούθηση της γλυκόζης, οι εύκαμπτες οθόνες, συσκευές που φοριούνται ως βραχιόλια ή δαχτυλίδια, σχεδιασμένες με μαλακά, ελαστικά υλικά για να προσαρμόζονται ανατομικά, μιμούμενες την ηλεκτρονική επιδερμίδα [4] και οι οπτικοί αισθητήρες, όπως οι φακοί επαφής που παρακολουθούν βιοχημικούς δείκτες από τα δάκρυα, ή τα ακουστικά βαρηκοΐας [7-8].

2. Συστήματα υποστηριζόμενα από την ένδυση

Σε αυτή την κατηγορία, οι ιατρικοί αισθητήρες και τα ηλεκτρονικά συστήματα ενσωματώνονται απρόσκοπτα μέσα στα ρούχα ή τα υφάσματα. Τα έξυπνα ρούχα όπως, μπλούζες που ενσωματώνουν αισθητήρες για συνεχή καταγραφή της αναπνοής, χωρίς να απαιτείται η απευθείας τοποθέτηση ηλεκτροδίων στο στήθος και τα έξυπνα παπούτσια που παρακολουθούν τον βηματισμό, την ισορροπία ή την πίεση που ασκείται στα πόδια, κρίσιμα για την αποκατάσταση ή τη διαχείριση νευρολογικών παθήσεων [4], αποτελούν εφαρμογές των συγκεκριμένων συστημάτων.

Για να διατηρηθεί η ιδιότητα της φορετότητας και να είναι η συσκευή λειτουργική στην καθημερινή ζωή, απαιτείται η ενσωμάτωση υψηλής μηχανικής ευελιξίας δηλαδή, η συσκευή πρέπει να μπορεί να κάμπτεται και να τεντώνεται μαζί με το δέρμα και τους μυς, ώστε να ελαχιστοποιούνται τα σφάλματα κίνησης κατά τη διάρκεια της σωματικής δραστηριότητας [3]. Καθώς επίσης και εισαγωγή βιο-συμβατότητας ώστε να είναι άμεση η επαφή με το σώμα καθιστώντας υποχρεωτική τη χρήση υλικών που δεν προκαλούν τοξικές ή ανοσολογικές αντιδράσεις [7].

Οι φορετές ιατρικές συσκευές έχουν σχεδιαστεί για να πραγματοποιούν συνεχή παρακολούθηση της υγείας και να συλλέγουν πληθώρα δεδομένων σε πραγματικό χρόνο, με στόχο την έγκαιρη ανίχνευση μη φυσιολογικών σημείων και την ενίσχυση της προληπτικής ιατρικής [3]. Οι βασικοί τύποι πληροφοριών που παρακολουθούν σχετίζονται με ζωτικά σημεία όπως καρδιακός ρυθμός, αρτηριακή πίεση, θερμοκρασία, επίπεδα γλυκόζης στο αίμα καθώς και δεδομένα που αφορούν τη μέτρηση των βασικών λειτουργιών του ανθρώπινου σώματος [4].

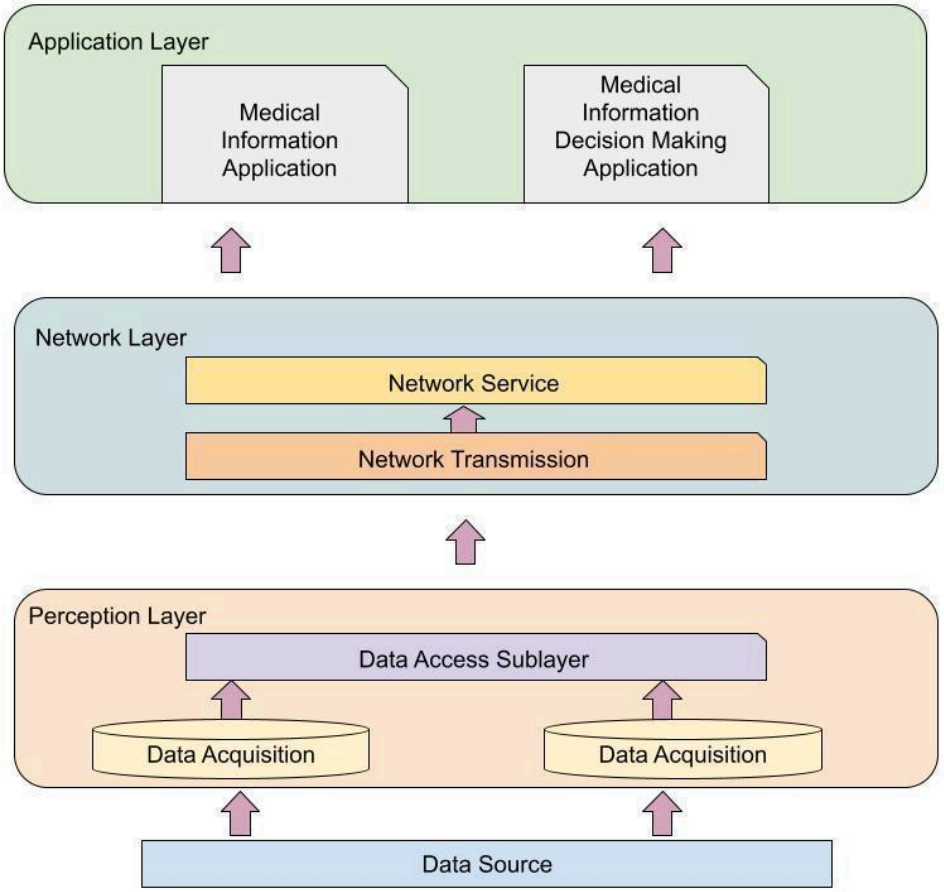
Η πιο προηγμένη μορφή είναι οι έξυπνες φορετές ιατρικές συσκευές, οι οποίες στοχεύουν στη δημιουργία συστημάτων κλειστού βρόχου, ενσωματώνοντας βιο-ανίχνευση σε πραγματικό χρόνο καθώς και χορήγηση φαρμάκων κατ' απαίτηση, μόλις ανιχνευθεί ανάγκη [5]. Αυτό επιτρέπει την εξατομικευμένη θεραπεία, αντικαθιστώντας τις ξεχωριστές διαδικασίες των παραδοσιακών συστημάτων.

Οι φορετές ιατρικές συσκευές είναι αυτόνομα, μη-επεμβατικά συστήματα σχεδιασμένα για να λειτουργούν διαρκώς στο βιολογικό περιβάλλον του χρήστη. Ο θεμελιώδης σκοπός τους είναι η συνεχής παρακολούθηση της υγείας, επιτυγχάνοντας άνεση και απρόσκοπτη ενσωμάτωση.

2.3 Αρχιτεκτονική φορετών ιατρικών συσκευών

Η αρχιτεκτονική των φορετών ιατρικών συσκευών συνιστά ένα σύνθετο, πολυεπίπεδο σύστημα που συνδυάζει λογική δικτύωση, ευέλικτη υλική δομή, ενεργειακή αυτονομία και ισχυρούς μηχανισμούς ασφάλειας για τη συνεχή και αξιόπιστη παρακολούθηση της υγείας.

Η αρχιτεκτονική, περιγράφει τη ροή δεδομένων από τον αισθητήρα στον τελικό ιατρικό φάκελο, ακολουθώντας μοντέλα δικτύου πολλαπλών βαθμίδων. Όπως φαίνεται και στο Σχήμα 2, διακρίνεται σε τρία βασικά επίπεδα, τα οποία περιγράφουν την ροή των δεδομένων.



Σχήμα 2: Αρχιτεκτονική συστήματος φορετών ιατρικών συσκευών [9]

2.3.1 Επίπεδο συλλογής δεδομένων (Perception Layer)

Το Perceptual Layer λειτουργεί ως η διεπαφή μεταξύ του φυσικού και του ψηφιακού κόσμου και αποτελεί την αρχική πηγή των βιολογικών δεδομένων [9]. Περιλαμβάνει φορητούς αισθητήρες (Wearable sensors), εξωτερικά συνδεδεμένους και αισθητήρες στο σώμα (On-body sensors) για τη συλλογή φυσιολογικών παραμέτρων, όπως ΗΚΓ, θερμοκρασία και επίπεδα γλυκόζης [10]. Οι αισθητήρες ανιχνεύουν φυσικά, χημικά ή βιοχημικά σήματα και τα μετατρέπουν σε ψηφιακά δεδομένα [11]. Λόγω της άμεσης επαφής με το σώμα, η υλική αρχιτεκτονική είναι αναπόσπαστο μέρος του λειτουργικού σχεδιασμού.

Χωρίζεται σε δύο υποεπίπεδα: το data acquisition, το οποίο χρησιμοποιεί αισθητήρες και τα βιομετρικά σήματα για να καταγράφει πληροφορίες από το περιβάλλον και το υποεπίπεδο data access, το οποίο αναλαμβάνει τη μεταφορά αυτών των δεδομένων [9]. Μέσω τεχνολογιών μικρής εμβέλειας, όπως το Bluetooth, το Wi-Fi και το ZigBee, το επίπεδο αυτό διασφαλίζει ότι η πληροφορία θα διοχετευθεί με ασφάλεια και ταχύτητα προς το δίκτυο, επιτρέποντας την περαιτέρω επεξεργασία και ανάλυσή της [9]. Σκοπός είναι η ακριβής και συνεχής ανίχνευση σημάτων για την παροχή πολύτιμων πληροφοριών στην ιατρική κοινότητα.

2.3.2 Επίπεδο δικτύου (Network Layer)

Το επίπεδο δικτύου λειτουργεί ως το κρίσιμο ενδιάμεσο σημείο μεταξύ του σώματος και του cloud [9]. Ο Coordinator Node, ο οποίος συχνά είναι ένα smartphone ή μια μονάδα ελέγχου σώματος, διαχειρίζεται το δίκτυο, δίνει άδεια σε νέους κόμβους να συνδεθούν και λαμβάνει τα δεδομένα από τους κόμβους. [12]. Αυτή η αρχιτεκτονική διευκολύνει τη διαχείριση της ισχύος, καθώς οι συσκευές του συγκεκριμένου επιπέδου χρησιμοποιούν πρωτόκολλα εξαιρετικά χαμηλής κατανάλωσης, όπως BLE και ZigBee, για να επικοινωνήσουν με την πύλη, η οποία αναλαμβάνει την μετάδοση μεγάλων αποστάσεων προς το cloud.

Η πύλη δρα ως δυναμικό σημείο επαφής για τη διαχείριση και την ασφάλεια [13]. Το network transmission χρησιμοποιεί δίκτυα επικοινωνίας για την μετάδοση δεδομένων που λαμβάνονται από το perception layer σε πραγματικό χρόνο [9]. Για την επικοινωνία χρησιμοποιούνται τεχνολογίες μικρής εμβέλειας (Short-Range Wireless Technologies), όπως: Bluetooth Low Energy (BLE) και ZigBee (IEEE 802.15.4) [10], [13], [14]. Η πύλη, συνήθως μια εφαρμογή smartphone, αποτελεί σημείο επίθεσης, καθώς οι εφαρμογές προσωπικού υπολογιστή ή smartphone είναι επιρρεπείς σε επιθέσεις λόγω υπερβολικά προνομιούχας φύσης και μη συμμόρφωσης με τους κανονισμούς. Στην επικοινωνία real-time, η διαδρομή πρέπει να είναι βελτιστοποιημένη για υψηλή αξιοπιστία και χαμηλή καθυστέρηση, ειδικά σε κρίσιμες εφαρμογές υγείας που απαιτούν έγκαιρη διάγνωση όπως καρδιαγγειακή παρακολούθηση.

2.3.3 Επίπεδο εφαρμογής (Application Layer)

Αυτή η βαθμίδα αξιοποιεί την υπολογιστική ισχύ του cloud για την ανάλυση και την τελική διάθεση των πληροφοριών. Χρησιμοποιεί τις πληροφορίες που συλλέγονται από το επίπεδο δικτύου ώστε να μπορέσει να διαχειριστεί μέσο εφαρμογών το ιατρικό αρχείο [9]. Το συγκεκριμένο επίπεδο, περιλαμβάνει όλες τις πληροφορίες του ασθενή και λαμβάνει αποφάσεις με βάση τις πληροφορίες που έχουν συλλεχθεί [9].

Εφαρμόζονται προηγμένοι αλγόριθμοι μηχανικής μάθησης και deep learning, όπως μοντέλα συνελικτικού νευρωνικού δικτύου, για την αυτόματη διάγνωση και την εξαγωγή χρήσιμων πληροφοριών [10], [15]. Η ενσωμάτωση deep learning και μηχανικής μάθησης στο επίπεδο επεξεργασίας μετατρέπει τα ακατέργαστα δεδομένα σε αυτόματη διάγνωση και πρόβλεψη. Αυτό είναι ζωτικής σημασίας για την αποφόρτιση του ανθρώπινου δυναμικού και την ταχεία κλινική υποστήριξη.

Για την μετάδοση σε αυτό το επίπεδο χρησιμοποιείται 5G καθώς προσφέρει υψηλό εύρος ζώνης και χαμηλή καθυστέρηση για την υποστήριξη κρίσιμων ιατρικών αποφάσεων σε πραγματικό χρόνο [15]. Οι τελικοί χρήστες όπως ιατροί και ασθενείς χρησιμοποιούν εφαρμογές κινητών ή διεπαφές παρόχων υγείας για την απομακρυσμένη παρακολούθηση [13].

Το επίπεδο εφαρμογής είναι ο κύριος στόχος των κυβερνοεπιθέσεων, καθώς εδώ αποθηκεύονται τα ευαίσθητα προσωπικά δεδομένα υγείας. Η αποθήκευση δεδομένων στο cloud και η σύνδεση της πύλης στο cloud αποτελούν κρίσιμα σημεία επίθεσης λόγω της ανάγκης για ισχυρή κρυπτογράφηση.

2.4 Προηγμένα υλικά

Η αρχιτεκτονική του φυσικού σχεδιασμού καθορίζει τη βιοσυμβατότητα, τη μηχανική ευελιξία και την ενεργειακή αυτονομία της φορετής συσκευής. Οι συσκευές πρέπει να είναι εύκαμπτες και ελαστικές για να προσαρμόζονται στη μηχανική κίνηση του ανθρώπινου δέρματος. Οι αισθητήρες, η

επεξεργασία και η ενέργεια πρέπει να ενσωματώνονται χρησιμοποιώντας εύκαμπτους ημιαγωγούς και νανοσύρματα [3].

Η ενσωμάτωση των λειτουργιών στο εύκαμπτο υπόστρωμα επιτυγχάνεται μέσω προηγμένων υλικών όπως, ευέλικτοι ημιαγωγοί, νανοϋλικά όπως τα νανοσύρματα, τα οποία αποτελούν κρίσιμο κομμάτι για τη διατήρηση της ευελιξίας, επιτρέποντας στους αισθητήρες και τις μονάδες επεξεργασίας να είναι μέρος της ενιαίας δομής [3]. Καθώς επίσης και microfluidic technologies που ενσωματώνονται στην αρχιτεκτονική του δέρματος, επιτρέποντας την ακριβή και σε πραγματικό χρόνο ανάλυση δεδομένων στο μικροεπίπεδο [16].

Η μηχανική συμμόρφωση δεν είναι απλώς ένα χαρακτηριστικό άνεσης. Είναι ένα κρίσιμο λειτουργικό ζήτημα διότι όταν μια άκαμπτη συσκευή κινείται σε σχέση με το δέρμα, δημιουργείται θόρυβος κίνησης [3]. Οι εύκαμπτες e-skins ελαχιστοποιούν αυτό το σφάλμα, βελτιώνοντας την ακρίβεια και την αξιοπιστία των βιολογικών μετρήσεων. Η άνεση που παρέχουν τα μαλακά υλικά είναι απαραίτητη για τη διασφάλιση της συμμόρφωσης του χρήστη και της μακροχρόνιας, συνεχούς παρακολούθησης.

Η αρχιτεκτονική του μέλλοντος για τις ιατρικές συσκευές, όχι μόνο φορετές, αλλά και εμφυτεύσιμες, εισάγει τα βιοδιασπώμενα υλικά [11]. Τα συγκεκριμένα υλικά έχουν σχεδιαστεί για να διαλύονται βιολογικά ή να απορροφώνται από το σώμα μετά την ολοκλήρωση της αποστολής τους [11]. Αυτή η προσέγγιση εξαλείφει την ανάγκη για δεύτερη χειρουργική επέμβαση ανάκτησης στην περίπτωση των εμφυτεύσιμων καθώς και την ασφαλή απόρριψη, απλοποιώντας τον κύκλο ζωής της ιατρικής συσκευής [11].

2.5 Τεχνικές ενεργειακής απόδοσης

Η συνεχής και αξιόπιστη λειτουργία των φορετών ιατρικών συσκευών καθορίζεται κεντρικά από την ικανότητά τους για ενεργειακή αυτονομία. Η ενεργειακή απόδοση αποτελεί το κεντρικό και κρίσιμο ζήτημα των συγκεκριμένων συσκευών, καθώς οι αισθητήρες απαιτείται να λειτουργούν για μήνες ή και χρόνια, ιδίως στις εμφυτεύσιμες εφαρμογές, όπου η αντικατάσταση της μπαταρίας συνεπάγεται επεμβατική διαδικασία [14]. Η επίτευξη αυτής της μακροζωίας απαιτεί μία σύνθετη στρατηγική που συνδυάζει την αρχιτεκτονική του υλικού τμήματος, με τη βελτιστοποίηση των λειτουργιών του δικτύου. Για τη βελτιστοποίηση της διάρκειας ζωής του δικτύου και των επιμέρους κόμβων, εφαρμόζονται διάφορες τεχνικές που στοχεύουν στη μείωση της κατανάλωσης ενέργειας τόσο σε επίπεδο λογισμικού όσο και σε επίπεδο πρωτοκόλλων επικοινωνίας [14].

Η πρώτη κρίσιμη στρατηγική αφορά τη μείωση δεδομένων. Αυτός ο μηχανισμός είναι ζωτικής σημασίας για τη μείωση του όγκου των δεδομένων που απαιτείται να αποθηκευτούν και κυρίως, να μεταδοθούν, επιτυγχάνοντας έτσι σημαντική εξοικονόμηση ενεργειακού κόστους. Η βασική στρατηγική σε αυτόν τον τομέα είναι η απαλοιφή διπλοτύπων δεδομένων, η οποία εξαλείφει τα πλεονάζοντα δεδομένα από τα συστήματα αποθήκευσης και μετάδοσης [14]. Η μετάδοση δεδομένων είναι παραδοσιακά μία από τις πιο ενεργοβόρες λειτουργίες του δικτύου. Συνεπώς, η μείωση του όγκου τους αποτελεί μία απλή, αλλά εξαιρετικά αποτελεσματική μέθοδο για την εξοικονόμηση ενέργειας σε επίπεδο δικτύου. Παράλληλα, στρατηγικές όπως Protocol Overhead Reduction χρησιμοποιούνται για τον έλεγχο της ροής και τη μείωση του κόστους του πρωτοκόλλου, αυξάνοντας έτσι τη συνολική αποδοτικότητα της μεταφοράς δεδομένων στα δίκτυα επικοινωνίας [14].

Σε επίπεδο πρωτοκόλλου, εφαρμόζεται power green routing. Τα πρωτόκολλα αυτά σχεδιάζονται με κύριο στόχο τη μεγιστοποίηση της διάρκειας ζωής του δικτύου των φορετών ιατρικών συσκευών. Αυτό επιτυγχάνεται μέσω της μείωσης της κατανάλωσης ενέργειας κατά τη μετάδοση από άκρο σε άκρο και κυρίως, μέσω της αποφυγής δρομολόγησης δεδομένων μέσω κόμβων που έχουν χαμηλή

πλεονάζουσα ενέργεια [14]. Προτείνετε η χρήση πρωτοκόλλων multi-hop, καθώς αυξάνουν την ορθή μετάδοση πακέτων και επεκτείνουν τη διάρκεια ζωής του δικτύου. Με αυτόν τον τρόπο, η έξυπνη δρομολόγηση μετατρέπει την ενεργειακή διαχείριση από παθητική σε ενεργητική, λαμβάνοντας υπόψη την κατάσταση της μπαταρίας κάθε κόμβου για την καλύτερη και πιο ισορροπημένη κατανομή του φόρτου.

Δύο άμεσα συνδεδεμένες τεχνικές για την εξοικονόμηση ενέργειας στο υλικό είναι ο duty cycle και ο transmission power control (TPC). Ο duty cycle ορίζει το ποσοστό του χρόνου κατά τον οποίο οι αισθητήρες παραμένουν ενεργοί για αποστολή και λήψη δεδομένων έναντι του χρόνου που βρίσκονται σε κατάσταση αδράνειας [14]. Η βελτιστοποίησή του είναι κρίσιμη για τη μακροζωία του συστήματος. Ο TPC ρυθμίζει δυναμικά την ισχύ μετάδοσης, εξασφαλίζοντας ότι χρησιμοποιείται μόνο η ελάχιστη απαραίτητη ισχύς για την επίτευξη της επικοινωνίας [14]. Ο συνδυασμός του χρονισμού και της ισχύος αποτελεί την πιο άμεση και αποτελεσματική παρέμβαση στην κατανάλωση ενέργειας του υλικού διότι όσο λιγότερο χρόνο και όσο πιο αδύναμα εκπέμπουν οι κόμβοι, τόσο μεγαλύτερη είναι η διάρκεια ζωής τους.

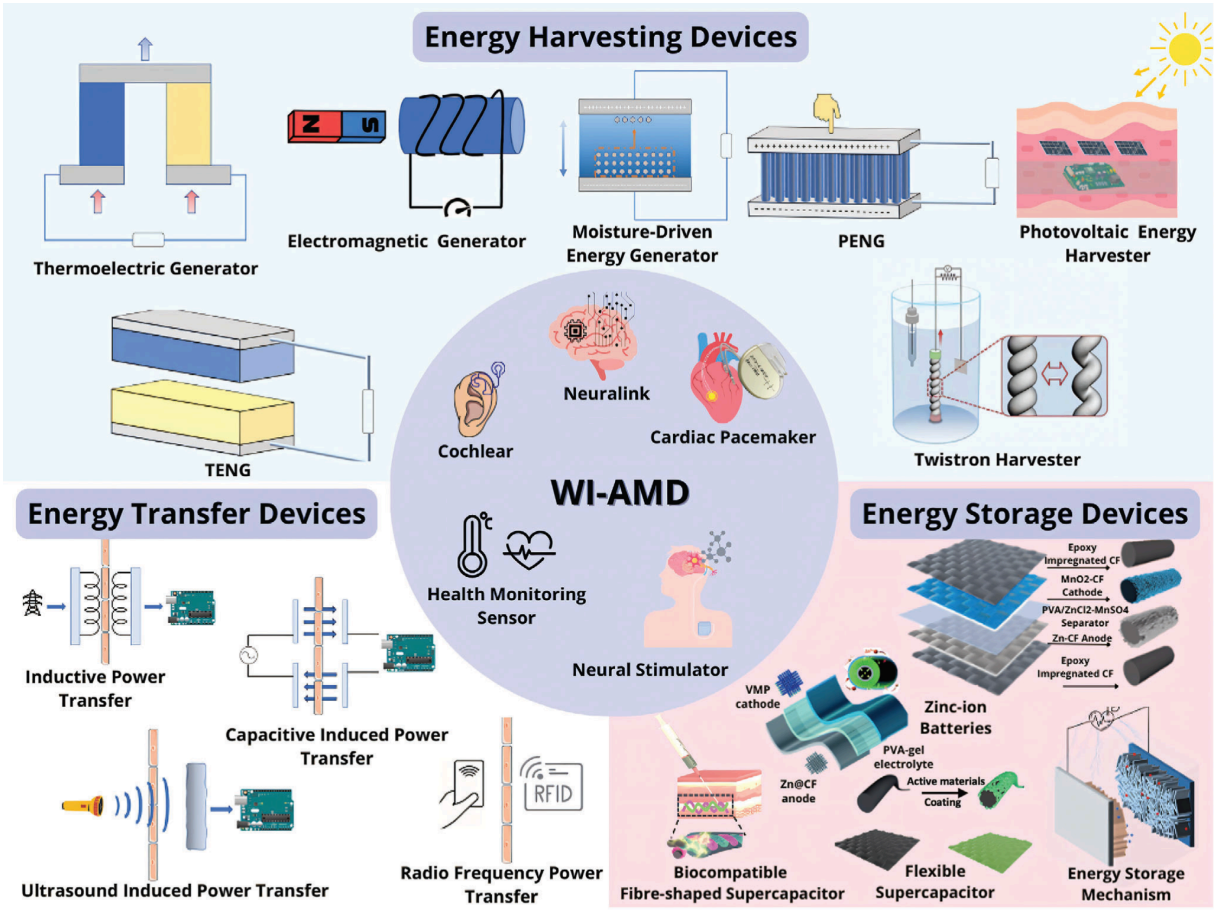
Η υιοθέτηση καθιερωμένων προτύπων και ο σχεδιασμός του υλικού παίζουν καθοριστικό ρόλο. Η εφαρμογή του προτύπου IEEE 802.15.4/ZigBee στα WBANs θεωρείται μία από τις πιο αποδοτικές μεθόδους διαχείρισης ενέργειας, ιδιαίτερα μέσω της λειτουργίας Beacon-Enabled Mode, όπου ένας συντονιστής στέλνει beacons για συγχρονισμό των συνδεδεμένων κόμβων [14]. Η υιοθέτηση προτύπων χαμηλής κατανάλωσης, όπως το ZigBee, παρέχει μια σταθερή και δοκιμασμένη βάση για την ενεργειακή απόδοση. Ένας μικρός κόμβος, όχι μόνο εξασφαλίζει μέγιστη ευελιξία, αλλά ο βελτιστοποιημένος σχεδιασμός του υλικού του εξυπηρετεί ταυτόχρονα τη βιοσυμβατότητα και την ενεργειακή οικονομία [14].

Παράλληλα με τη βελτιστοποίηση του δικτύου, η ενεργειακή αρχιτεκτονική των φορετών ιατρικών συσκευών έχει σχεδιαστεί για να λειτουργεί ως αυτοτροφοδοτούμενο σύστημα, αντιμετωπίζοντας την πρόκληση της αντικατάστασης μπαταριών μέσω προηγμένων υλικών [17]. Οι φορετές ιατρικές συσκευές απαιτούν συνεχή τροφοδοσία για τις βασικές λειτουργίες τους: ανίχνευση, ενεργοποίηση, διέγερση και επικοινωνία [17]. Ο ρόλος των προηγμένων υλικών όπως νανοσύρματα, είναι κεντρικός στην αρχιτεκτονική αυτή, καθώς αυξάνουν την απόδοση μετατροπής και εξασφαλίζουν την ευελιξία και τη βιοσυμβατότητα του συστήματος [17].

Συσκευές συλλογής, μεταφοράς και αποθήκευσης ενέργεια, όπως απεικονίζονται και στο Σχήμα 3 είναι [1], [17]:

- Triboelectric Nanogenerators - TENGs: Οι TENGs συλλέγουν μηχανική ενέργεια μέσω μιας αρχιτεκτονικής στρατηγικής που εκμεταλλεύεται την πρόσφυση, την τριβή και τη δόνηση του σώματος. Συλλογή ενέργειας μπορεί να πραγματοποιηθεί από την αναπνοή, τους καρδιακούς παλμούς, ή την κίνηση των άκρων.
- Piezoelectric Nanogenerators - PENGs: Οι PENGs αξιοποιούν τη μηχανική ενέργεια, παράγοντας ηλεκτρικό φορτίο ως άμεση απόκριση σε μηχανική πίεση ή τάση. Αυτή η τεχνική εφαρμόζεται αποτελεσματικά σε βιολογικές κινήσεις, όπως οι παλμοί του αίματος ή η αναπνοή.
- Thermoelectric Generators - TEGs: Οι TEGs μετατρέπουν τη θερμική ενέργεια, διαφορά θερμοκρασίας, σε ηλεκτρισμό. Η αρχιτεκτονική τους εκμεταλλεύεται τη διαφορά θερμοκρασίας μεταξύ του δέρματος και του περιβάλλοντος, χρησιμοποιώντας το φαινόμενο Seebeck.

- Φωτοβολταϊκή και RF συλλογή: Τέλος, χρησιμοποιούνται τεχνικές που βασίζονται σε εξωτερικές πηγές, όπως η ηλιακή ενέργεια, μέσω εύκαμπτων solar cells, καθώς και οι ραδιοσυχνότητες (RF), οι οποίες επιτρέπουν την ασύρματη μεταφορά ενέργειας μέσω εξωτερικών πομπών.



Σχήμα 3: Τεχνολογίες συλλογής, μεταφοράς και αποθήκευσης ενέργειας για την τροφοδοσία φορετών ιατρικών συσκευών [17]

Στα πλαίσια της ανάπτυξης συστημάτων ασύρματων αισθητήρων σώματος, η ενεργειακή αυτονομία αποτελεί κρίσιμο παράγοντα, καθιστώντας τις τεχνολογίες συλλογής ενέργειας απαραίτητες για την τροφοδοσία φορετών συσκευών. Οι πηγές ενέργειας από το ανθρώπινο σώμα ταξινομούνται σε βιοχημικές, όπως η γλυκόζη, βιομηχανικές, όπως ο καρδιακός παλμός και η πίεση του αίματος, καθώς και σε ενέργεια περιβάλλοντος, όπως η θερμότητα. Με βάση τα δεδομένα, η βιοχημική συλλογή ενέργειας από τη γλυκόζη εμφανίζει την υψηλότερη απόδοση, παράγοντας 1.8 mJ/s, ακολουθούμενη από τον θερμοηλεκτρισμό (1.35 mJ/s) που αξιοποιεί τη θερμότητα του σώματος [12]. Αντίθετα, οι βιομηχανικές πηγές από τον καρδιακό παλμό ή την πίεση του αίματος παρουσιάζουν σημαντικά χαμηλότερη απόδοση, με μόλις 0.012 mJ/s και 0.03 mJ/s αντίστοιχα [12]. Αυτή η ποσοτικοποίηση αναδεικνύει την βιοχημική και θερμική ενέργεια ως τις πιο αποδοτικές και υποσχόμενες πηγές για τη συνεχή, αυτόνομη τροφοδοσία των συσκευών από τα συστήματα ασύρματων αισθητήρων σώματος.

Η λεπτομερής ταξινόμηση των τεχνικών συλλογής ενέργειας δείχνει την εξειδίκευση της ενεργειακής αρχιτεκτονικής, η οποία προσαρμόζει τον μετατροπέα στην εκάστοτε πηγή ενέργειας του ανθρώπινου σώματος. Δεδομένης της ασυνέχειας των πηγών ενέργειας, η συσκευή απαιτεί αξιόπιστη

αρχιτεκτονική αποθήκευσης. Οι παραδοσιακές επαναφορτιζόμενες μπαταρίες προσφέρουν υψηλή ενεργειακή πυκνότητα, ενώ οι υπερπυκνωτές προσφέρουν υψηλή πυκνότητα ισχύος, κατάλληλη για στιγμιαίες απαιτήσεις όπως η μετάδοση δεδομένων [17]. Η μονάδα διαχείρισης ισχύος είναι ένα κρίσιμο αρχιτεκτονικό στοιχείο που ρυθμίζει και ελέγχει τη ροή της ενέργειας, διασφαλίζοντας σταθερή τάση και ρεύμα για όλα τα ηλεκτρονικά του συστήματα [1].

Το πιο ρεαλιστικό μοντέλο είναι το υβριδικό σύστημα, το οποίο εξασφαλίζει μέγιστη αξιοπιστία και αυτονομία [17]. Η δομή ενσωματώνει τη μονάδα συλλογής ενέργειας, διαχείρισης ισχύος, αποθήκευσης ενέργειας και το φορτίο [17]. Η υβριδική στρατηγική συνδυάζει πολλαπλές τεχνικές συλλογής ενέργειας για αύξηση της συνολικής παραγόμενης ισχύος, μπαταρίες και υπερπυκνωτές [1]. Η υβριδική αρχιτεκτονική είναι η απάντηση στην αστάθεια των βιολογικών πηγών ενέργειας. Δημιουργεί έναν ρυθμιστή ενέργειας, επιτρέποντας στη συσκευή να είναι αυτόνομη και να εξασφαλίζει σταθερή λειτουργία, απομακρύνοντας την αρχιτεκτονική από τις απλές εξωτερικές πηγές σε έξυπνες, ενσωματωμένες δομές.

Συνολικά, η ενεργειακή αρχιτεκτονική στις φορετές ιατρικές συσκευές αποτελεί ένα ολιστικό ζήτημα που αντιμετωπίζεται σε όλα τα επίπεδα, από τον σχεδιασμό των νανοϋλικών για τη συλλογή ενέργειας, έως τα πρωτόκολλα δρομολόγησης για την εξοικονόμηση δεδομένων, με απώτερο στόχο την παροχή διαρκούς και αξιόπιστης παρακολούθησης στην ψηφιακή υγειονομική περίθαλψη.

2.6 Διαχείριση δεδομένων

Η αποτελεσματική και ασφαλής διαχείριση των δεδομένων αποτελεί το κεντρικό ζήτημα για την αξιοπιστία των φορετών ιατρικών συσκευών. Δεδομένης της ευαίσθητης φύσης των δεδομένων υγείας, η ιδιωτικότητα και η ασφάλεια είναι οι κύριες τεχνικές προκλήσεις. Η διαχείριση αυτή καλύπτει ολόκληρο τον κύκλο ζωής των δεδομένων, από τη στιγμή της συλλογής τους από τους αισθητήρες μέχρι την αποθήκευση, τη μετάδοση και την τελική ανάλυση. Η διασφάλιση της ακρίβειας και της ιδιωτικότητας σε κάθε στάδιο είναι υψίστης σημασίας.

Οι φορετές συσκευές συλλέγουν δεδομένα μέσω αισθητήρων, παράγοντας πραγματικού χρόνου δεδομένα [18]. Αυτά τα δεδομένα είναι συχνά προσωπικά αναγνωρίσιμα και περιλαμβάνουν ζωτικούς δείκτες όπως καρδιακό ρυθμό και αρτηριακή πίεση. Η φυσική ακεραιότητα της συσκευής είναι η βάση για την ακεραιότητα των δεδομένων. Συστήματα όπως οι microfluidics επιτρέπουν την ακριβή και αξιόπιστη συλλογή δεδομένων στα συγκεκριμένα περιβάλλοντα [16]. Η χρήση βιοσυμβατών υλικών διασφαλίζει τη μακροπρόθεσμη σταθερότητα της συσκευής πάνω ή μέσα στο σώμα. Μία συσκευή που υποβαθμίζεται ή αποτυγχάνει δεν μπορεί να παρέχει αξιόπιστα δεδομένα, οδηγώντας σε αποτυχία της ακεραιότητας. Κρίσιμα ζητήματα, πρέπει να εξασφαλίζουν την αξιόπιστη ροή του βιολογικού δείγματος προς τον αισθητήρα, καθώς ένα αποτυχημένο σύστημα μπορεί να οδηγήσει σε λανθασμένα δεδομένα [16]. Στο σημείο συλλογής, η τοπική διαφορική ιδιωτικότητα (LDP) παρέχει ιδιωτικότητα σε τοπικό επίπεδο, προστατεύοντας τη διαδικασία συλλογής δεδομένων. Ο χρήστης προσθέτει θόρυβο στα ατομικά του δεδομένα πριν τα στείλει στον aggregator, διασφαλίζοντας την ατομική ιδιωτικότητα [18].

Τα δεδομένα που συλλέγονται μεταδίδονται ασύρματα σε ένα ενδιάμεσο τερματικό, όπως smartphone και στη συνέχεια σε έναν απομακρυσμένο διακομιστή [18]. Η φορετή συσκευή μεταφέρει τα δεδομένα στο smartphone μέσω Bluetooth ή BLE [14], [18]. Το smartphone λειτουργεί ως manager, το οποίο μεταφέρει τα δεδομένα μέσω κινητού δικτύου ή WiFi στον Server/Cloud Server [8].

Ο ασφαλής χειρισμός δεδομένων είναι επιτακτικός. Απαιτείται κρυπτογράφηση από άκρο σε άκρο και ισχυρά πρωτόκολλα ελέγχου ταυτότητας για τη διασφάλιση της ακεραιότητας κατά τη μεταφορά [15]. Η RF communication ενέχει κινδύνους διότι τα σήματα RF διασκορπίζονται σε μεγάλο βαθμό και αφομοιώνονται στο ανθρώπινο σώμα, με αποτέλεσμα οι συσκευές να απαιτούν υψηλότερη ισχύ για μεγαλύτερη εμβέλεια [11]. Αυτή η υψηλή ισχύς δημιουργεί κίνδυνο θερμικής βλάβης και αυξημένης τιμής στο ρυθμό ειδικής απορρόφησης. Η ποιότητα της ασύρματης σύνδεσης πρέπει να αξιολογείται ακόμα και σε συνθήκες χαμηλής συνδεσιμότητας για την αποτροπή απώλειας κατά τη μεταφορά και αποθήκευση δεδομένων [8].

Με την ολοκλήρωση της μετάδοσης τα δεδομένα του server διαμοιράζονται με επαγγελματίες υγείας, ερευνητές ή μέλη της οικογένειας, με την σύμφωνη γνώμη του χρήστη. Η διαφορική ιδιωτικότητα (DP) είναι μια μέθοδος που χρησιμοποιείται για την κοινή χρήση συγκεντρωτικών πληροφοριών από ευαίσθητα δεδομένα, χωρίς να αποκαλύπτεται η ταυτότητα κανενός [18]. Η DP επιτυγχάνεται με την προσθήκη θορύβου, μιας βαθμονομημένης τιμής που χρησιμοποιείται για την ανωνυμοποίηση των δεδομένων [18]. Οι πιο δημοφιλείς μηχανισμοί για αριθμητικά δεδομένα είναι ο Laplace Mechanism και ο Gaussian Mechanism [18]. Η βασική πρόκληση της DP είναι η ισορροπία μεταξύ της απώλειας ιδιωτικότητας και της μεγιστοποίησης της χρησιμότητας [18].

Τα δεδομένα των φορετών συσκευών είναι υψηλά συσχετισμένα. Αυτή η συσχέτιση αποτελεί μεγάλη πρόκληση, καθώς μπορεί να επιτρέψει σε έναν επιτιθέμενο να αποκαλύψει ευαίσθητες πληροφορίες, συνδυάζοντας τα αποκρυπτογραφημένα δεδομένα με υπάρχουσες συσχετίσεις [18].

Οι προσεγγίσεις Big Data, μπορεί να είναι παραπλανητικές για μεμονωμένα άτομα, καθώς οι ροές μπορούν να επισκιάσουν τις ακραίες τιμές, δημιουργώντας καταστροφικά στατιστικά συμβάντα για ορισμένους ασθενείς [8]. Οι φορετές τεχνολογίες πρέπει να είναι ικανές να αναγνωρίζουν τα δεδομένα του ατόμου για να παρέχουν προσαρμοσμένη παρακολούθηση.

2.7 Επίλογος

Το παρόν κεφάλαιο ανέλυσε τη σύνθετη και πολυεπίπεδη αρχιτεκτονική των φορετών ιατρικών συσκευών και των δικτύων WBANs, αναδεικνύοντας πώς η αποτελεσματική λειτουργία τους εξαρτάται από τη συνεργασία του υλικού, της ενέργειας, του δικτύου και της ασφάλειας των δεδομένων.

Αρχικά, εξετάστηκε η αρχιτεκτονική των φορετών ιατρικών συσκευών ως ένα τριμερές μοντέλο. Το επίπεδο συλλογής δεδομένων αποτελεί τη βάση, όπου οι αισθητήρες, συλλέγουν σε πραγματικό χρόνο βιολογικά δεδομένα. Αυτή η φυσική ακεραιότητα της συσκευής, είναι η προϋπόθεση για την ακεραιότητα των δεδομένων. Στη συνέχεια, τα δεδομένα διέρχονται από το επίπεδο δικτύου και καταλήγουν στο επίπεδο εφαρμογής, όπου μετατρέπονται σε πληροφορίες χρήσιμες για ιατρικούς σκοπούς.

Η λειτουργική αξιοπιστία των φορετών ιατρικών συσκευών είναι άμεσα συνδεδεμένη με την τεχνολογία υλικών. Η απαίτηση για μακροχρόνια λειτουργία επέβαλε την ανάπτυξη τεχνικών ενεργειακής απόδοσης που υπερβαίνουν τους περιορισμούς των συμβατικών μπαταριών. Η αρχιτεκτονική συλλογής ενέργειας αξιοποιεί την TENGs, PENGs και τη θερμική ενέργεια του σώματος, ενώ το υβριδικό σύστημα όπως μπαταρίες και υπερπυκνωτές, εξασφαλίζει αυτόνομη λειτουργία. Σε επίπεδο δικτύου, η ενεργειακή απόδοση επιτυγχάνεται μέσω τεχνικών όπως ο duty cycle και η power green routing, μειώνοντας το κόστος μετάδοσης.

Το πιο κρίσιμο σημείο του κύκλου ζωής των δεδομένων παραμένει η διαχείριση. Δεδομένου ότι τα ιατρικά δεδομένα είναι προσωπικά δεδομένα, η ιδιωτικότητα και η ασφάλεια αποτελούν τη βασική τεχνική πρόκληση. Χρησιμοποιούνται τεχνικές όπως η διαφορική ιδιωτικότητα (DP) και η τοπική διαφορική ιδιωτικότητα (LDP) για την ανωνυμοποίηση των δεδομένων, εξασφαλίζοντας ότι η παρουσία ενός ατόμου στο σύνολο δεδομένων δεν μπορεί να εντοπιστεί. Η ασύρματη μετάδοση απαιτεί κρυπτογράφηση από άκρο σε άκρο και ισχυρά πρωτόκολλα ελέγχου ταυτότητας. Επίσης, οι σχεδιαστές πρέπει να λαμβάνουν υπόψη τους κινδύνους θερμικής βλάβης και SAR που προκύπτουν από την υψηλή ισχύ εκπομπής, ειδικά για τις φορετές συσκευές.

Συνοψίζοντας, η επιτυχία των φορετών ιατρικών συσκευών εξαρτάται από την ικανότητα να συνθέτουν υψηλή ακρίβεια ανίχνευσης και μακροπρόθεσμη ενεργειακή αυτονομία με μια ισχυρή και πολυεπίπεδη αρχιτεκτονική ασφάλειας, διασφαλίζοντας έτσι την προστασία του χρήστη και την ακεραιότητα των ιατρικών δεδομένων.

Κεφάλαιο 3ο: Θέματα Ασφάλειας στις Φορετές Ιατρικές Συσκευές

3.1 Εισαγωγή

Η ενσωμάτωση των φορετών ιατρικών συσκευών στο σύγχρονο οικοσύστημα υγείας προσφέρει ανεκτίμητα οφέλη, όπως η συνεχής παρακολούθηση ζωτικών σημείων και η αυτοματοποιημένη χορήγηση θεραπειών. Ωστόσο, η μετάβαση από τις αυτόνομες συσκευές στις δικτυωμένες ιατρικές συσκευές άνοιξε έναν νέο κύκλο απειλών στην κυβερνοασφάλεια.

Οι ευπάθειες των συστημάτων αυτών δεν αποτελούν απλώς τεχνικά σφάλματα, αλλά δυνητικούς κινδύνους που απειλούν άμεσα την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των ιατρικών δεδομένων και υπηρεσιών. Λόγω της φύσης τους, οι συσκευές αυτές παρουσιάζουν ένα πλαίσιο απειλών για τους εξής λόγους [19-24]:

- Περιορισμοί πόρων: Η ανάγκη για μικρό μέγεθος και μεγάλη διάρκεια μπαταρίας συχνά οδηγεί στη χρήση ασθενών πρωτοκόλλων κρυπτογράφησης.
- Attack Surface: Η χρήση ασύρματων τεχνολογιών (Bluetooth, Wi-Fi) καθιστά τις συσκευές προσβάσιμες από απόσταση σε κακόβουλους χρήστες.
- Κρισιμότητα λειτουργίας: Σε αντίθεση με τις συμβατικές συσκευές, μια δυσλειτουργία ή μια κυβερνοεπίθεση σε μια ιατρική συσκευή μπορεί να έχει μοιραία αποτελέσματα για τον ασθενή.

Στην παρούσα ενότητα, εξετάζονται οι κυριότερες κατηγορίες ευπαθειών που εντοπίζονται σε επίπεδο επικοινωνίας, στο υλικό (hardware) και το λογισμικό (software) αναλύοντας τον τρόπο με τον οποίο αυτές οι αδυναμίες μπορούν να γίνουν αντικείμενο εκμετάλλευσης.

Τέλος, η ενότητα θα διερευνήσει τις απειλές που προκύπτουν από την κακόβουλη χρήση των δεδομένων, όπως η εκβίαση, η κλοπή ταυτότητας και η αλλοίωση ιατρικών πληροφοριών. Ολοκληρώνοντας, θα παρουσιαστούν οι τεχνικές και οργανωτικές απαιτήσεις για τη διασφάλιση της ασφάλειας και αξιοπιστίας των δεδομένων, καλύπτοντας την κρυπτογράφηση, την ανωνυμοποίηση και την ακεραιότητα των πληροφοριών, στοιχεία απαραίτητα για την εδραίωση της εμπιστοσύνης του κοινού στην ψηφιακή υγειονομική περίθαλψη.

3.2 Ευπάθειες σε Επίπεδο Επικοινωνίας

Η ραγδαία εξέλιξη του IoMT έχει καταστήσει την ασύρματη επικοινωνία τον κεντρικό άξονα της σύγχρονης υγειονομικής περίθαλψης. Οι φορετές ιατρικές συσκευές βασίζονται σε μια ποικιλία πρωτοκόλλων, όπως το Bluetooth Low Energy (BLE), το Wi-Fi και το ZigBee, προκειμένου να μεταδίδουν ζωτικά δεδομένα σε πραγματικό χρόνο [19]. Ωστόσο, αυτή η ανάγκη για συνεχή συνδεσιμότητα δημιουργεί ένα διευρυμένο πεδίο έκθεσης σε κινδύνους. Οι ασύρματες τεχνολογίες συχνά στερούνται ισχυρών κρυπτογραφικών πρωτοκόλλων λόγω των περιορισμένων πόρων των συσκευών, καθιστώντας το επίπεδο επικοινωνίας το πιο ευάλωτο σημείο στην αρχιτεκτονική της ψηφιακής υγείας [20].

Μια από τις σημαντικότερες αδυναμίες εντοπίζεται στη διαδικασία της σύζευξης (pairing). Κατά την εφαρμογή του Unauthenticated Pairing, η απουσία πρωτοκόλλων αυθεντικοποίησης δημιουργεί σημαντικά κενά στην ασφάλεια, αφήνοντας την επικοινωνία εκτεθειμένη σε επιθέσεις τύπου Man-in-the-Middle [19]. Ένα από τα κρισιμότερα ζητήματα ασφάλειας παρατηρείται στη χρήση της παλαιότερης μεθόδου σύνδεσης Legacy Pairing, η οποία θεωρείται πλέον παρωχημένη και εξαιρετικά επικίνδυνη για την προστασία των ασθενών [19]. Κρίνεται επικίνδυνη καθώς πηγάζει κυρίως από το γεγονός ότι η μέθοδος επιτρέπει την παθητική υποκλοπή, δίνοντας τη δυνατότητα σε έναν επιτιθέμενο να "ακούει" την ασύρματη επικοινωνία κατά τη στιγμή της σύνδεσης της ιατρικής συσκευής με το κινητό τηλέφωνο, χωρίς να γίνει αντιληπτός από τον χρήστη [19], [21]. Εάν ο επιτιθέμενος καταγράψει αυτή την αρχική επικοινωνία, μπορεί στη συνέχεια να επεξεργαστεί τα δεδομένα στον δικό του υπολογιστή, δοκιμάζοντας εκατομμύρια συνδυασμούς το δευτερόλεπτο μέχρι να βρει τον σωστό κωδικό. Μόλις επιτευχθεί η παραβίαση, ο εισβολέας αποκτά πλήρη πρόσβαση στα ευαίσθητα δεδομένα του ασθενούς, έχοντας πλέον τη δυνατότητα να αποκρυπτογραφήσει το σύνολο των μηνυμάτων που ανταλλάσσονται, με τον χρήστη να παραμένει σε πλήρη άγνοια για την παραβίαση της ιδιωτικότητάς του [19].

Η ασύρματη φύση του BLE επιτρέπει σε κακόβουλους χρήστες την επιβολή μη εξουσιοδοτημένων συνδέσεων με ελάχιστη προσπάθεια [23]. Αυτή η αυθαίρετη δημιουργία επικοινωνίας οφείλεται στην ασθενή κρυπτογράφηση και την έλλειψη αμοιβαίας αυθεντικοποίησης, επιτρέποντας στον εισβολέα να στείλει ψευδείς εντολές, όπως να ζητήσει από μια αντλία ινσουλίνης να χορηγήσει δόση, ή να υποκλέψει όλα τα ιστορικά δεδομένα υγείας που είναι αποθηκευμένα στη μνήμη της, χωρίς ο ασθενής να αντιληφθεί ποτέ ότι η συσκευή του δεν επικοινωνεί με το κινητό του, αλλά με έναν ξένο.

Η έλλειψη ελέγχου και ισχυρής κρυπτογράφησης κατά τη μετάδοση καθιστά τα δεδομένα των ασθενών προσβάσιμα σε τρίτους μέσω επιθέσεων υποκλοπής (eavesdropping) [19]. Χρησιμοποιώντας εργαλεία όπως το Wireshark, οι επιτιθέμενοι μπορούν να πραγματοποιήσουν sniffing στο Bluetooth και να υποκλέψουν μια μη ασφαλή κίνηση δικτύου, αποκτώντας πρόσβαση σε κωδικούς και προσωπικά ιατρικά αρχεία [23]. Πέρα από την υποκλοπή, υπάρχει ο κίνδυνος αλλοίωσης των δεδομένων κατά τη μεταφορά, γεγονός που μπορεί να οδηγήσει σε λανθασμένες διαγνώσεις ή επικίνδυνες ιατρικές εντολές [25]. Οι επιθέσεις αναπαραγωγής (replay attacks), όπου ο εισβολέας καταγράφει και επαναλαμβάνει νόμιμα μηνύματα, αποτελούν διαρκή απειλή για την ακεραιότητα των συστημάτων IoMT [26]. Παράλληλα, η χρήση στατικών διευθύνσεων MAC δημιουργεί ευπάθειες στην ιδιωτικότητα, επιτρέποντας στον επιτιθέμενο να παρακολουθεί και να εντοπίζει γεωγραφικά τον χρήστη [22].

Είναι ιδιαίτερα ανησυχητικό το γεγονός ότι οι επιθέσεις EDA και οι επιθέσεις DoS μετατρέπουν ένα ψηφιακό πρόβλημα σε άμεση φυσική απειλή. Σε αντίθεση με ένα smartphone, μια επίθεση σε μια αντλία ινσουλίνης ή έναν βηματοδότη δεν αφορά μόνο την κλοπή δεδομένων, αλλά τον έλεγχο μιας συσκευής που υποστηρίζει τη ζωή. Σύμφωνα με την βιβλιογραφία [26] η λύση πρέπει να αναζητηθεί σε lightweight cryptography και σε αλγόριθμους που μπορούν να ανιχνεύουν ενεργειακή απόκλιση, λειτουργώντας ως συστήματα ανίχνευσης εισβολών στο επίπεδο της επικοινωνίας. Συνοψίζοντας, η αντιμετώπιση αυτών των κινδύνων απαιτεί μια ολιστική προσέγγιση που να περιλαμβάνει ισχυρή αυθεντικοποίηση, μέσω PUF ή Hash συναρτήσεων, κρυπτογράφηση και δυναμική διαχείριση των διευθύνσεων δικτύου για την προστασία της ιδιωτικότητας του ασθενούς.

Η πολυπλοκότητα των επικοινωνιακών ευπαθειών επιτείνεται από την έλλειψη τυποποίησης. Παρά την ύπαρξη πλαισίων όπως το NIST SP 800-53, παρατηρείται συχνά κενό στη συμμόρφωση όσον αφορά την ασφαλή μετάδοση δεδομένων.

3.3 Ευπάθειες Υλικού

Η θεμελιώδης ευπάθεια των φορετών ιατρικών συσκευών (WMDs) και των συσκευών IoMT πηγάζει από τον σχεδιασμό τους ως συστήματα περιορισμένων πόρων. Η ανάγκη για μικρό μέγεθος, εργονομία και χαμηλή κατανάλωση ενέργειας οδηγεί σε συσκευές με χαμηλή επεξεργαστική ισχύ και περιορισμένη μνήμη [19]. Αυτοί οι σημαντικοί περιορισμοί καθιστούν τεχνικά αδύνατη την υιοθέτηση συμβατικών αρχιτεκτονικών ασφάλειας ή πολύπλοκων αλγορίθμων κρυπτογράφησης [20]. Ως εκ τούτου, οι κατασκευαστές καταφεύγουν σε λύσεις lightweight cryptography, οι οποίες όμως, λόγω της απλουστευμένης φύσης τους, αποδεικνύονται συχνά ανασφαλείς, επιτρέποντας σε επιτιθέμενους να παραβιάσουν την εμπιστευτικότητα των δεδομένων ή ακόμα και να αποκτήσουν τον έλεγχο της συσκευής [21].

Οι ευπάθειες στο επίπεδο του υλικού συνδέονται άρρηκτα με τους περιορισμούς των ενσωματωμένων χημικών πηγών ενέργειας, όπως οι μπαταρίες ιόντων λιθίου [24]. Η περιορισμένη χωρητικότητα των μπαταριών δημιουργεί ένα αναπόφευκτο συμβιβασμό μεταξύ της ακρίβειας των μετρήσεων και της κατανάλωσης ενέργειας. Σε περίπτωση που μια συσκευή μειώσει τον ρυθμό δειγματοληψίας για να εξοικονομήσει ενέργεια, ενδέχεται να αποτύχει να καταγράψει κρίσιμες ιατρικές μετρήσεις, όπως οι καρδιακές αρρυθμίες [24].

Επιπλέον, το υλικό είναι ευάλωτο σε επιθέσεις resource depletion. Οι επιθέσεις Denial of Service (DoS) στοχεύουν ακριβώς στη διαχείριση ισχύος, αναγκάζοντας τους αισθητήρες να παραμένουν σε πλήρη λειτουργία αντί να εισέρχονται σε κατάσταση αδράνειας, μέχρι την πλήρη εξάντληση των ενεργειακών αποθεμάτων [23]. Σε κρίσιμες συσκευές, όπως οι εμφυτεύσιμοι απινιδωτές (ICDs), η πρόωρη εξάντληση της μπαταρίας αποτελεί άμεση απειλή για τη ζωή, καθώς η αντικατάστασή τους απαιτεί νέα χειρουργική επέμβαση [27].

Η φορητότητα των WMDs αυξάνει δραματικά τον κίνδυνο φυσικής παραβίασης. Οι συσκευές συχνά διαθέτουν ανοιχτές διεπαφές ελέγχου και προγραμματισμού, οι οποίες, αν παραμείνουν προσβάσιμες μετά την παραγωγή δεδομένων, επιτρέπουν σε κάποιον με φυσική πρόσβαση να εξάγει το υλικολογισμικό [22]. Στην περίπτωση των ICDs, έχει παρατηρηθεί ότι οι διεπαφές προγραμματισμού στερούνται ισχυρής αυθεντικοποίησης, επιτρέποντας σε έναν εισβολέα με τον κατάλληλο εξοπλισμό να παρέμβει απευθείας στις ρυθμίσεις της συσκευής [27]. Επιπλέον, η ύπαρξη memory leaks στο υλικό μπορεί να αξιοποιηθεί για την κλοπή προσωπικών πληροφοριών ή την παρακολούθηση του χρήστη [23].

Στο φυσικό επίπεδο επικοινωνίας του υλικού, οι επιθέσεις jamming αποδεικνύονται εξαιρετικά αποτελεσματικές. Αυτές οι επιθέσεις αναγκάζουν τους αισθητήρες να σαρώνουν συνεχώς για ανοιχτά κανάλια επικοινωνίας, αυξάνοντας την κατανάλωση ενέργειας κατά 30-50% [24]. Η έλλειψη θωράκισης στο φυσικό επίπεδο επιτρέπει σε κακόβουλους χρήστες να παρεμβαίνουν στα σήματα ραδιοσυχνοτήτων, ενώ οι modeling attacks επιτρέπουν σε εισβολείς να προβλέψουν την έξοδο των κυκλωμάτων ασφαλείας [26].

Για την ενίσχυση της ασφάλειας, προτείνεται η χρήση physical unclonable function (PUF). Οι PUFs εκμεταλλεύονται τα μοναδικά φυσικά χαρακτηριστικά του υλικού κάθε συσκευής για να παράγουν μοναδικές αποκρίσεις σε συγκεκριμένες προκλήσεις, λειτουργώντας ως ψηφιακό αποτύπωμα του υλικού [26]. Η χρήση ελεγχόμενων κυκλωμάτων (MC-PUF) κρίνεται απαραίτητη για την προστασία αυτών των διεπαφών από απόπειρες μοντελοποίησης.

Γίνεται σαφές ότι η ασφάλεια των φορετών ιατρικών συσκευών υπονομεύεται από τους φυσικούς περιορισμούς του υλικού τους. Επίσης, αξιοσημείωτα είναι τα θέματα που σχετίζονται με την ενεργειακή ασφάλεια. Η ενέργεια στις συγκεκριμένες συσκευές δεν αποτελεί έναν απλό αναλώσιμο πόρο, αλλά είναι ζωτικής σημασίας για τη διασφάλιση της ανθρώπινης ζωής. Καθώς η λειτουργία των αισθητήρων εξαρτάται άμεσα από τη διαθεσιμότητα ισχύος, οποιαδήποτε κακόβουλη παρέμβαση στην μπαταρία μετατρέπεται αυτόματα από τεχνικό σφάλμα σε απειλή κατά της φυσικής ακεραιότητας του ασθενούς. Οι ευπάθειες υλικού στις φορετές συσκευές είναι δομικές και απορρέουν από τον συνεργασία μεταξύ εργονομίας, ενέργειας και ασφάλειας. Η αντιμετώπιση επιθέσεων όπως η εξάντληση πόρων, η φυσική παραβίαση διεπαφών και η παρεμβολή σημάτων απαιτεί επανασχεδιασμό των συσκευών δίνοντας προτεραιότητα στην ενίσχυση της ανθεκτικότητας του φυσικού επιπέδου και τη χρήση εξειδικευμένων κυκλωμάτων ασφαλείας.

3.4 Ευπάθειες Λογισμικού

Το υλικολογισμικό (firmware) αποτελεί το ενδιάμεσο στρώμα που επιτρέπει στο λογισμικό να ελέγχει το υλικό της ιατρικής συσκευής. Οι ευπάθειες σε αυτό το επίπεδο εντοπίζονται κυρίως στη διαχείριση και την αλλοίωσή του firmware [24]. Οι επιτιθέμενοι στοχεύουν στην τροποποίηση του κώδικα με σκοπό την υπονόμευση της ενεργειακής αυτονομίας, μια τακτική που μπορεί να καταστήσει τη συσκευή ανενεργή σε κρίσιμες στιγμές.

Μια από τις πιο επικίνδυνες αδυναμίες είναι η απουσία ισχυρών πρωτοκόλλων αυθεντικοποίησης κατά τη διαδικασία των ενημερώσεων. Η έλλειψη ψηφιακών υπογραφών επιτρέπει την εισαγωγή κακόβουλου λογισμικού, μετατρέποντας μια ψηφιακή ευπάθεια σε άμεση απειλή για τη ζωή [27].

Το λογισμικό δεν αποτελεί μόνο στόχο υποκλοπής, αλλά και μέσο για την εκτέλεση επιθέσεων κατανάλωσης κρίσιμων πόρων του συστήματος. Οι επιθέσεις sleep deprivation attacks είναι ιδιαίτερα διαδεδομένες, καθώς εμποδίζουν το λογισμικό να εισέλθει σε καταστάσεις χαμηλής ισχύος, διπλασιάζοντας την κατανάλωση ενέργειας [24]. Η παραλλαγή, sleep deprivation torture, αυτών των επιθέσεων εκμεταλλεύεται τις ρυθμίσεις των πρωτοκόλλων δρομολόγησης για να εξαντλήσει συστηματικά την ενέργεια των κόμβων επικοινωνίας [24].

Επιπλέον, οι επιθέσεις "Ghost" προσομοιώνουν ψευδή γεγονότα στο δίκτυο, αναγκάζοντας το λογισμικό να επεξεργάζεται ανύπαρκτα δεδομένα, γεγονός που μειώνει τη διάρκεια ζωής της συσκευής κατά 20-40% [245]. Χαρακτηριστική είναι η περίπτωση ανάκλησης βηματοδοτών, όπου το λογισμικό δέχθηκε συνεχή ερωτήματα εντολών, οδηγώντας σε υπερβολική χρήση ενέργειας και πρόωρη αποφόρτιση [24].

Η ανεπάρκεια στους μηχανισμούς επαλήθευσης ταυτότητας αποτελεί δομικό πρόβλημα. Πολλά ιατρικά συστήματα λογισμικού επιτρέπουν την πρόσβαση χωρίς τη χρήση ισχυρών κωδικών ή άλλων μεθόδων επαλήθευσης. Μια από τις πιο κοινές και επικίνδυνες πρακτικές είναι η χρήση

προκαθορισμένων κωδικών πρόσβασης μέσα στον κώδικα, οι οποίοι δεν μπορούν να αλλαχθούν από τον ασθενή ή τον γιατρό, προσφέροντας μόνιμη πρόσβαση σε όποιον τους γνωρίζει [27].

Η έλλειψη αυθεντικοποίησης σημαίνει ότι η ιατρική συσκευή δεν μπορεί να βεβαιωθεί ότι το κινητό τηλέφωνο ή ο διακομιστής με τον οποίο επικοινωνεί είναι έμπιστος, επιτρέποντας σε μη εξουσιοδοτημένες συσκευές να αντλούν Προσωπικά Δεδομένα Υγείας (PHI) ή να αλλάζουν κρίσιμες ρυθμίσεις [19].

Οι φορετές συσκευές σπάνια λειτουργούν αυτόνομα, βασίζονται σε εφαρμογές Android/iOS και Software Development Kits. Η έρευνα μέσω reverse engineering σε εφαρμογές δημοφιλών συσκευών αποκάλυψε ότι οι εφαρμογές αυτές συχνά αποθηκεύουν κλειδιά κρυπτογράφησης και ευαίσθητα δεδομένα με μη ασφαλή τρόπο στη μνήμη του κινητού [22].

Μια αναδυόμενη και εξαιρετικά σοβαρή απειλή είναι το Ransomware, το οποίο δύναται να προκαλέσει λειτουργικό αποκλεισμό της συσκευής. Μέσω του περιορισμού της πρόσβασης στις ρυθμίσεις ή της πλήρους διακοπής της λειτουργίας της, ο επιτιθέμενος εκβιάζει τον ασθενή, καθιστώντας την ασφάλεια του λογισμικού άρρηκτα συνδεδεμένη με την επιβίωση του χρήστη [27]. Παράλληλα, η απουσία αυθεντικοποίησης στις πύλες που συνδέονται με τους διακομιστές επιτρέπει την αλλοίωση των ιατρικών δεδομένων. Αυτό επηρεάζει άμεσα την ακρίβεια των διαγνώσεων, καθώς ο γιατρός μπορεί να λαμβάνει παραποιημένες μετρήσεις και να προβαίνει σε λανθασμένες θεραπευτικές ενέργειες [20].

Η ανάλυση των ευπαθειών λογισμικού αναδεικνύει μια ανησυχητική πραγματικότητα όπου οι φορετές ιατρικές συσκευές συχνά αντιμετωπίζονται από τους κατασκευαστές περισσότερο ως απλές συσκευές και λιγότερο ως κρίσιμα ιατρικά εργαλεία. Οι επιθέσεις Ghost και Sleep Deprivation [24] δεν προϋποθέτουν την αποκρυπτογράφηση των δεδομένων για να βλάψουν έναν ασθενή, αρκεί να εξαντλήσει την μπαταρία της συσκευής μέσω του λογισμικού. Επιπλέον, η εξάρτηση από τις εφαρμογές κινητών τηλεφώνων [23] διευρύνει το εύρος της επίθεσης.

Η λύση που προτείνεται στη βιβλιογραφία, είναι η χρήση hash συναρτήσεων για ανώνυμη ταυτότητα και μηχανισμοί forward secrecy [26], όπου είναι τεχνικά εφικτή. Επίσης, είναι επιτακτική ανάγκη οι κατασκευαστές να επενδύσουν σε ασφαλείς κύκλους ανάπτυξης λογισμικού (SDLC). Η ασφάλεια των ιατρικών δεδομένων και η φυσική ακεραιότητα του ασθενούς δεν μπορούν να βασίζονται σε ανασφαλή συστήματα.

Οι ευπάθειες λογισμικού στις φορετές ιατρικές συσκευές είναι πολυεπίπεδες και στοχεύουν τόσο στην εμπιστευτικότητα των δεδομένων όσο και στη λειτουργική διαθεσιμότητα της συσκευής. Η ενίσχυση της ασφάλειας απαιτεί την υιοθέτηση ψηφιακών υπογραφών για τις ενημερώσεις καθώς και την κατάργηση των προκαθορισμένων κωδικών.

3.5 Μη εξουσιοδοτημένη χρήση και εκμετάλλευση των δεδομένων

Η ραγδαία επέκταση του IoMT, το οποίο περιλαμβάνει φορετές ιατρικές συσκευές, έχει κλιμακώσει το επίπεδο διακινδύνευσης του υγειονομικού κλάδου, αυξάνοντας την έκθεσή του σε κυβερνοαπειλές και την πιθανότητα μη εξουσιοδοτημένης εκμετάλλευσης δεδομένων [28]. Η ευαίσθητη και διαχρονική φύση των πληροφοριών υγείας τις καθιστά πρωταρχικό στόχο εκμετάλλευσης. Ως εκ τούτου, η συγκεκριμένη ενότητα αναλύει τις κυριότερες μορφές μη εξουσιοδοτημένης χρήσης και

εκμετάλλευσης των δεδομένων, από την άμεση κυβερνοεπίθεση έως τις κοινωνικές και οικονομικές συνέπειες.

Η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα υγείας αποτελεί την πρώτη και πιο κρίσιμη μορφή εκμετάλλευσης. Οι επιτιθέμενοι στοχεύουν στην απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πολύτιμα δεδομένα ασθενών, ιατρικούς φακέλους ή άλλες ευαίσθητες πληροφορίες [28]. Η πρωταρχική πρόθεση των επιτιθέμενων είναι να παραβιάσουν τα ιδιωτικά δεδομένα των ασθενών. Οι διαδικασίες συλλογής και αποθήκευσης δεδομένων εκθέτουν τις προσωπικές πληροφορίες υγείας σε κινδύνους, συμπεριλαμβανομένων της μη εξουσιοδοτημένης πρόσβασης, των παραβιάσεων δεδομένων, τη δημιουργία ψεύτικων προφίλ, της παρακολούθησης και της κακής χρήσης από τρίτα άτομα [29]. Τα δεδομένα φορετών συσκευών πωλούνται ή κοινοποιούνται σε ασφαλιστές, διαφημιστές και Data Brokers για τη δημιουργία προφίλ καταναλωτών και προωθητικών ενεργειών [29]. Η απειλή δεν προέρχεται μόνο από εξωτερικούς παράγοντες. Εργαζόμενοι ή συνεργάτες οι οποίοι έχουν πρόσβαση στα δεδομένα ενδέχεται να κάνουν σκόπιμα κακή χρήση δεδομένων για οικονομικό όφελος, ανταγωνιστικό πλεονέκτημα ή προσωπικά κίνητρα [29].

Η μη εξουσιοδοτημένη χρήση και εκμετάλλευση μπορεί να επιφέρει άμεση φυσική ή λειτουργική βλάβη:

- Ransomware: Λογισμικό που κρυπτογραφεί σημαντικά ιατρικά δεδομένα και στη συνέχεια απαιτεί μεγάλα χρηματικά ποσά για την ανάκτησή τους, παραβιάζοντας την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών [28]. Οι απειλές έχουν κλιμακωθεί, συμπεριλαμβάνοντας επιθέσεις ransomware μεγάλης εμβέλειας που στοχεύουν τις πλατφόρμες υγείας που φιλοξενούνται στο cloud [30].
- Επιθέσεις τροποποίησης: Ένας active attacker μπορεί να προκαλέσει αλλοίωση, τροποποίηση και διαγραφή των διαβιβαζόμενων πληροφοριών [28].
- Κίνδυνος ζωής ή σωματική βλάβη: Οι επιθέσεις εναντίον συσκευών IoMT έχουν τη δυνατότητα να προκαλέσουν σωματική βλάβη στους ασθενείς, καθώς η θεραπεία τους εξαρτάται από την ακρίβεια των ιατρικών δεδομένων [28].

Η εκμετάλλευση των δεδομένων, καθίσταται δυνατή μέσω της αξιοποίησης των τεχνικών ευπαθειών της αρχιτεκτονικής των φορετών συσκευών και των εφαρμογών τους. Οι επιτιθέμενοι μπορούν να εισάγουν κακόβουλους ή πλαστούς κόμβους στο δίκτυο IoMT, αποκτώντας έτσι πλήρη πρόσβαση και έλεγχο σε ολόκληρο το δίκτυο [28]. Επιπλέον, μη εξουσιοδοτημένες οντότητες μπορούν να προσποιούνται παράνομα ότι είναι εξουσιοδοτημένες για να αποκτήσουν μεγαλύτερα προνόμια στο σύστημα [31]. Ο επιτιθέμενος μπορεί να κλέψει τα διαπιστευτήρια σύνδεσης του χρήστη και να αποκτήσει μη εξουσιοδοτημένα προνόμια για πρόσβαση στα αποθηκευμένα ευαίσθητα δεδομένα υγείας, προσποιούμενος τον νόμιμο χρήστη [31]. Παράλληλα, η έλλειψη κρυπτογράφησης στη διαβίβαση δεδομένων αφήνει ευαίσθητα δεδομένα εκτεθειμένα σε υποκλοπή κατά τη μεταφορά, καθιστώντας τα ευάλωτα σε επιθέσεις MitM [29], [30], όπου ένα τρίτο μέρος μπορεί να υποκλέψει κακόβουλα και να αποκτήσει τις ιδιωτικές πληροφορίες του χρήστη κατά τη διαδικασία επικοινωνίας [31]. Οι κίνδυνοι προέρχονται επίσης από ευπάθειες όπως αδυναμίες συσκευής ή cloud, που είναι εγγενείς στην ασύρματη επικοινωνία, την ανεπαρκή κρυπτογράφηση, την μη ασφαλή αποθήκευση στο cloud και τις πρακτικές κοινής χρήσης δεδομένων από τρίτους [30]. Ιδιαίτερα, συσκευές με προεπιλεγμένα διαπιστευτήρια ή μη ενημερωμένο υλικολογισμικό παρουσιάζουν εύκολα σημεία εισόδου για τους επιτιθέμενους [30]. Τέλος, η επέκταση των συσκευών IoMT αυξάνει γενικά τη συνολική δυνατότητα hacking του συστήματος [28].

3.6 Κυβερνοασφάλεια και αξιοπιστία των δεδομένων

Η διασφάλιση της κυβερνοασφάλειας και της ακεραιότητας των δεδομένων είναι θεμελιώδης για την επιτυχή ενσωμάτωση των φορετών ιατρικών συσκευών και του IoMT στην περίθαλψη. Η χρήση δικτυωμένων συσκευών έχει αυξήσει δραματικά την ευαισθησία του τομέα της υγείας σε επιθέσεις και κακόβουλη εκμετάλλευση. Η ευαίσθητη και διαχρονική φύση των πληροφοριών υγείας τις καθιστά πρωταρχικό στόχο εκμετάλλευσης.

Η διασφάλιση της κυβερνοασφάλειας στις φορετές ιατρικές συσκευές απαιτεί την τήρηση των τριών θεμελιωδών αρχών ασφάλειας [32], [33]:

- Εμπιστευτικότητα: Διασφαλίζει ότι οι ευαίσθητες πληροφορίες δεν είναι προσβάσιμες από μη εξουσιοδοτημένα άτομα. Η κρυπτογράφηση κωδικοποιεί ιατρικές πληροφορίες, ώστε μόνο οι κάτοχοι του κλειδιού αποκρυπτογράφησης να μπορούν να τις διαβάσουν.
- Ακεραιότητα: Εγγυάται ότι τα δεδομένα παραμένουν ακριβή καθ' όλη τη διάρκεια του κύκλου ζωής τους. Αυτό είναι ζωτικής σημασίας για την αξιοπιστία των ιατρικών αποτελεσμάτων, αποτρέποντας την αλλοίωση της διάγνωσης ή της ομάδας αίματος.
- Διαθεσιμότητα: Διασφαλίζει ότι τα συστήματα, όπως βηματοδότες, λειτουργούν και είναι προσβάσιμα, όταν είναι απαραίτητο, για τους εξουσιοδοτημένους χρήστες. Οι επιθέσεις άρνησης υπηρεσίας (DoS) είναι μια συνήθης απειλή που στοχεύει τη διαθεσιμότητα.

Οι κυβερνοεπιθέσεις έχουν σαφή στόχευση, με κεντρικό κίνητρο την κλοπή και την εκμετάλλευση των δεδομένων. Η πρωταρχική πρόθεση των επιτιθέμενων είναι να παραβιάσουν τα ιδιωτικά δεδομένα των ασθενών [28]. Οι διαδικασίες συλλογής και αποθήκευσης δεδομένων εκθέτουν τις προσωπικές πληροφορίες υγείας σε κινδύνους, συμπεριλαμβανομένων της μη εξουσιοδοτημένης πρόσβασης, της παραβίασης των δεδομένων και της κακής χρήσης από μη εξουσιοδοτημένους χρήστες [29].

Η εκμετάλλευση καθίσταται δυνατή αξιοποιώντας τα τεχνικά κενά της αρχιτεκτονικής των φορετών ιατρικών συσκευών και των εφαρμογών. Λόγω των περιορισμένων πόρων των φορετών ιατρικών συσκευών, δεν είναι δυνατή η ενσωμάτωση παραδοσιακών μηχανισμών ασφάλειας [34]. Η έλλειψη, σε ορισμένες περιπτώσεις, κρυπτογράφησης στη μεταφορά δεδομένων αφήνει ευαίσθητα δεδομένα εκτεθειμένα σε υποκλοπή κατά τη μεταφορά, καθιστώντας τα ευάλωτα σε επιθέσεις [29]. Οι επιτιθέμενοι μπορούν να εισάγουν κακόβουλους ή πλαστούς κόμβους στο δίκτυο IoMT, αποκτώντας έτσι πλήρη πρόσβαση και έλεγχο σε ολόκληρο το δίκτυο [28]. Επίσης, μη εξουσιοδοτημένες οντότητες προσποιούνται παράνομα ότι είναι εξουσιοδοτημένες οντότητες για να αποκτήσουν μεγαλύτερα προνόμια στο σύστημα [31]. Επιπλέον, οι επιτιθέμενοι μπορούν να πραγματοποιούν Side Channel Attacks για να αποκτήσουν ευαίσθητες πληροφορίες υγείας, αναλύοντας την κατανάλωση ενέργειας ή την ηλεκτρομαγνητική ακτινοβολία για την εξαγωγή μυστικών κλειδιών [33].

Για την αντιμετώπιση των απειλών και τη διασφάλιση της ακεραιότητας, απαιτούνται εξειδικευμένοι μηχανισμοί κυβερνοασφάλειας και ρυθμιστικής δράσης. Η χρήση λύσεων που βασίζονται σε blockchain για τα WBANs ενισχύει την ακεραιότητα των δεδομένων υγείας [35] καθώς λειτουργεί ως αποκεντρωμένη οντότητα για την αποφυγή του single point of failure [36]. Επιπλέον, απαιτούνται ασφαλή κρυπτογραφικά πρωτόκολλα και μηχανισμοί ταυτοποίησης για την εξασφάλιση των φορετών ιατρικών συσκευών [33], [34]. Ο εκτεταμένος αλγόριθμος PRESENT είναι ένας αλγόριθμος χαμηλού υπολογιστικού κόστους κρυπτογράφησης που καταναλώνει λιγότερη ενέργεια και παρέχει υψηλότερη ασφάλεια και αξιοπιστία στους αισθητήρες [36]. Για την αποτροπή επιθέσεων που θέτουν σε κίνδυνο την ακεραιότητα, οι μηχανισμοί ακεραιότητας ροής δεδομένων και η χρήση συστημάτων

ταυτοποίησης, χρησιμοποιούν τη μέθοδο του κατακερματισμού προκειμένου να επαληθεύσουν την ακριβή εκτέλεση του προγράμματος μιας ιατρικής συσκευής [33]. Η διασφάλιση της αξιοπιστίας των ιατρικών δεδομένων εξαρτάται άμεσα από την εφαρμογή ισχυρής κυβερνοασφάλειας και την επαρκή εκπαίδευση των ανθρώπων που διαχειρίζονται τις συγκεκριμένες τεχνολογίες [37].

3.7 Επίλογος

Η ανάλυση των ευπαθειών στις φορετές ιατρικές συσκευές αποκαλύπτει μια πολυεπίπεδο και αλληλένδετο περιβάλλον. Οι φυσικοί περιορισμοί του υλικού, όπως η περιορισμένη επεξεργαστική ισχύς και η πεπερασμένη ενέργεια της μπαταρίας, αποτελούν την αρχή του προβλήματος, καθώς επιβάλλουν τη χρήση ανασφαλούς λογισμικού. Αυτός ο συμβιβασμός αφήνει εκτεθειμένα τα πρωτόκολλα επικοινωνίας, επιτρέποντας σε επιτιθέμενους να πραγματοποιούν υποκλοπές δεδομένων, packet sniffer ή ακόμα και φυσικό εντοπισμό του χρήστη. Μια ευπάθεια στο πρωτόκολλο επικοινωνίας μπορεί να δώσει πρόσβαση στο λογισμικό, το οποίο με τη σειρά του μπορεί να εκτελέσει επιθέσεις Denial of Service, οδηγώντας σε επιταχυνόμενη αποφόρτιση της μπαταρίας και καθιστώντας αναγκαία σε πολλές περιπτώσεις τη χειρουργική αντικατάσταση της συσκευής.

Η ασφάλεια των WMDs δεν μπορεί να επιτευχθεί μεμονωμένα σε ένα επίπεδο. Απαιτείται μια ολιστική προσέγγιση, η οποία θα ενσωματώνει τη θωράκιση του φυσικού επιπέδου, την αυθεντικοποίηση των ενημερώσεων λογισμικού και την κρυπτογράφηση των επικοινωνιών, διασφαλίζοντας ότι η τεχνολογική πρόοδος στην ιατρική παρακολούθηση δεν θα αποβεί εις βάρος της ασφάλειας και της ίδιας της ζωής του ασθενούς.

Η απουσία ενιαίας ρύθμισης και οι τεχνικές αδυναμίες διευκολύνουν την κακόβουλη εκμετάλλευση. Οι επιθέσεις δεν περιορίζονται πλέον στην απλή κλοπή, αλλά επεκτείνονται στην εμπορευματοποίηση και την άμεση βλάβη του ασθενούς. Οι επιθέσεις ransomware και τροποποίησης δεδομένων απειλούν την ακεραιότητα των συστημάτων, με κίνδυνο την εσφαλμένη χορήγηση φαρμάκου ή ακόμα και τη σωματική βλάβη.

Για την αντιμετώπιση αυτών των απειλών, η έμφαση δίνεται στην ενίσχυση της ακεραιότητας των δεδομένων. Οι τεχνικές λύσεις πρέπει να ξεπεράσουν τους περιορισμένους πόρους των συσκευών μέσω της ανάπτυξης κρυπτογραφικών πρωτοκόλλων και μηχανισμών πιστοποίησης, οι οποίοι χρησιμοποιούν κατακερματισμό για να επαληθεύσουν την ακρίβεια της ροής εκτέλεσης του λογισμικού. Η υιοθέτηση τεχνολογιών όπως το blockchain προτείνεται ως λύση για την εγγύηση της αμετάβλητης καταγραφής των ιατρικών δεδομένων, ενώ η ανάγκη για εξειδικευμένη εκπαίδευση σε θέματα κυβερνοασφάλειας καθίσταται επιτακτική για τους επαγγελματίες υγείας.

Η ολοκληρωμένη προσέγγιση που συνδυάζει ισχυρή νομική συμμόρφωση, ενεργητική άμυνα έναντι της εκμετάλλευσης και τεχνολογίες διασφάλισης ακεραιότητας, είναι ο μόνος δρόμος για να αξιοποιηθούν με ασφάλεια τα επαναστατικά οφέλη των φορετών ιατρικών συστημάτων.

Κεφάλαιο 4ο: Πρότυπα Ασφάλειας και Αξιολόγηση της Εφαρμογής τους σε Περιβάλλοντα

4.1 Εισαγωγή

Η σύγχρονη ιατρική υιοθετεί όλο και περισσότερο τις φορετές ιατρικές συσκευές, οι οποίες συλλέγουν, αποθηκεύουν και μεταδίδουν τεράστιες ποσότητες δεδομένων υγείας σε πραγματικό χρόνο. Αυτή η συνεχής ροή πληροφοριών προσφέρει ανεκτίμητα οφέλη, όπως η εξατομικευμένη φροντίδα και η έγκαιρη διάγνωση, αλλά φέρει παράλληλα τεράστιες ευθύνες όσον αφορά την ασφάλεια και την ιδιωτικότητα. Δεδομένου ότι τα δεδομένα υγείας θεωρούνται ειδικές κατηγορίες προσωπικών δεδομένων, η προστασία τους καθίσταται ύψιστη προτεραιότητα.

Η παρούσα ενότητα εστιάζει στην κρίσιμη διασταύρωση της τεχνολογίας, της ιατρικής και της νομοθεσίας, αναλύοντας το περιβάλλον στο οποίο κινούνται αυτά τα ευαίσθητα δεδομένα. Αρχικά, θα εξεταστεί λεπτομερώς η φύση των προσωπικών δεδομένων που συλλέγονται από τις φορετές συσκευές αναδεικνύοντας τον ευαίσθητο χαρακτήρα τους.

Στη συνέχεια, θα αναλυθεί το νομοθετικό πλαίσιο που επιχειρεί να ρυθμίσει αυτήν την τεχνολογική εξέλιξη, με έμφαση στον GDPR (Γενικός Κανονισμός για την Προστασία των Δεδομένων), ο οποίος επιβάλλει σαφείς κανόνες για τη συγκατάθεση, τη διαφάνεια και την ασφάλεια της επεξεργασίας, καθώς και στον κανονισμό HIPAA. Παράλληλα, εξετάζεται η συμβολή διεθνών προτύπων όπως το ISO 27001, το οποίο προσφέρει το ολιστικό πλαίσιο διαχείρισης της ασφάλειας και το ISO 27799, που εξειδικεύει τους συγκεκριμένους ελέγχους για τις πληροφορίες υγείας. Επιπλέον, θα γίνει αναφορά στο πλαίσιο NIST SP 800-53, το οποίο παρέχει έναν αναλυτικό κατάλογο τεχνικών ελέγχων για τη ενίσχυση των πληροφοριακών συστημάτων.

Η διασφάλιση της διαλειτουργικότητας και της αξιόπιστης μετάδοσης δεδομένων σε συστήματα προσωπικής υγείας επιτυγχάνεται μέσω του συνδυασμού του προτύπου IEEE 802.15.6 για ασύρματα δίκτυα σώματος (BAN) με την οικογένεια προτύπων IEEE 11073, η οποία περιλαμβάνει το πλαίσιο ανταλλαγής δεδομένων IEEE 11073-20601 και τις εξειδικευμένες προδιαγραφές όπως 11073-10404, IEEE 11073-10406, IEEE 11073-10407 και IEEE 11073-10417. Επίσης, είναι ζωτικής σημασίας να κατανοηθούν οι νομικές υποχρεώσεις των κατασκευαστών και των παρόχων υπηρεσιών, καθώς και ο βαθμός στον οποίο τα παραπάνω πρότυπα εφαρμόζονται αποτελεσματικά σε IoMT περιβάλλοντα.

4.2 Προσωπικά δεδομένα

Οι φορετές ιατρικές συσκευές συλλέγουν συνεχώς ευαίσθητα δεδομένα σχετικά με την υγεία, τα οποία εμπίπτουν στις ειδικές κατηγορίες προσωπικών δεδομένων [38]. Στην συγκεκριμένη κατηγορία απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν γενετικά δεδομένα, βιομετρικά δεδομένα και δεδομένα που αφορούν την υγεία, καθώς θεωρούνται ειδικές κατηγορίες προσωπικών δεδομένων και χρήζουν προστασίας.

Η συλλογή ιατρικών δεδομένων είναι εκτεταμένη και μπορεί να περιλαμβάνει: δεδομένα ζωτικής σημασίας, καρδιακό ρυθμό, ΗΚΓ, επίπεδα γλυκόζης στο αίμα, αρτηριακή πίεση, κορεσμό οξυγόνου, θερμοκρασία σώματος, αναπνευστικό ρυθμό όπως και ένα ευρύ φάσμα πρόσθετων μετρήσεων [29].

4.3 Νομοθετικό πλαίσιο

Η ανάπτυξη των φορετών ιατρικών συσκευών και η συνεχής συλλογή ευαίσθητων δεδομένων υγείας δημιούργησαν μια σύνθετη νομική και ρυθμιστική πρόκληση. Το κύριο ζήτημα έγκειται στο γεγονός ότι η τεχνολογική πρόοδος έχει σε μεγάλο βαθμό ξεπεράσει την εξέλιξη των νομικών πλαισίων, δημιουργώντας ρυθμιστικά κενά σχετικά με το ποιες συσκευές και ποια δεδομένα καλύπτονται από τους υφιστάμενους νόμους. Δεδομένου ότι τα δεδομένα υγείας θεωρούνται ειδικές κατηγορίες προσωπικών δεδομένων που απαιτούν το υψηλότερο επίπεδο προστασίας, η διαχείριση, η αποθήκευση και η επεξεργασία τους πρέπει να διέπονται από αυστηρούς κανόνες για την αποφυγή κακόβουλης χρήσης. Σε διεθνές επίπεδο, δύο νομικά πλαίσια αποτελούν τους βασικούς άξονες γύρω από τους οποίους περιστρέφεται η συζήτηση για την προστασία δεδομένων υγείας σε ψηφιακά περιβάλλοντα: ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση (ΕΕ) και ο Health Insurance Portability and Accountability Act (HIPAA) στις Ηνωμένες Πολιτείες της Αμερικής.

4.3.1 Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR - Κανονισμός [ΕΚ] 2016/679) αποτελεί το νομικό πλαίσιο της Ευρωπαϊκής Ένωσης και αναφέρεται στην προστασία των δεδομένων υγείας που συλλέγονται από φορετές ιατρικές συσκευές [38]. Ο GDPR είναι μία από τις πιο ολοκληρωμένες κανονιστικές ρυθμίσεις ιδιωτικότητας και έχει εφαρμοστεί για τη βελτίωση της διακυβέρνησης των δεδομένων υγείας. Ο κανονισμός επιδιώκει να εναρμονίσει τους νόμους για την ιδιωτικότητα στην Ευρώπη [13].

Ο GDPR εφαρμόζεται σε όλες τις επιχειρήσεις και οργανισμούς που επεξεργάζονται τα προσωπικά δεδομένα κατοίκων της ΕΕ, ανεξάρτητα από τη γεωγραφική τους θέση [13]. Δίνει ιδιαίτερη προσοχή σε δεδομένα που θεωρούνται ευαίσθητα, συμπεριλαμβανομένων των δεδομένων υγείας. Ευαίσθητες πληροφορίες στον τομέα της υγειονομικής περίθαλψης περιλαμβάνουν βιομετρικά δεδομένα, γενετικά δεδομένα και δεδομένα που σχετίζονται με την υγεία και υπόκεινται στους αυστηρότερους κανόνες του Άρθρου 9 [39]. Σύμφωνα με το Άρθρο 4 του GDPR οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών που είναι διαθέσιμοι στο κοινό είναι υποχρεωμένοι να εφαρμόζουν τα απαραίτητα τεχνικά και οργανωτικά μέτρα για να διασφαλίζουν την ασφάλεια των υπηρεσιών τους [40]. Αυτά τα μέτρα πρέπει να λαμβάνονται, όπου χρειάζεται, σε συνεργασία με τον πάροχο του δημόσιου δικτύου επικοινωνιών, όσον αφορά την ασφάλεια του δικτύου. Είναι κρίσιμο τα συγκεκριμένα μέτρα να είναι ανάλογα με τον υφιστάμενο κίνδυνο, λαμβάνοντας πάντα υπόψη τις πιο σύγχρονες τεχνικές δυνατότητες και το κόστος εφαρμογής τους. Εάν προκύψει ιδιαίτερα σοβαρός κίνδυνος παραβίασης της ασφάλειας του δικτύου, ο πάροχος της υπηρεσίας ηλεκτρονικών επικοινωνιών οφείλει να ενημερώσει άμεσα τους συνδρομητές του [40]. Επιπλέον, αν ο κίνδυνος υπερβαίνει τα μέτρα που απαιτείται να λάβει ο ίδιος ο πάροχος, υποχρεούται να γνωστοποιήσει στους συνδρομητές όλες τις διαθέσιμες μεθόδους για την αποτροπή του κινδύνου, καθώς και το εκτιμώμενο κόστος αυτών των μέτρων [40].

Ως κανονισμός, ο GDPR απαγορεύει την επεξεργασία αυτών των δεδομένων έως ότου ληφθεί συγκατάθεση [28]. Επίσης, επιβάλλει την αρχή προστασίας δεδομένων εξ ορισμού, απαιτώντας από τους κατασκευαστές να ενσωματώνουν μέτρα προστασίας από το αρχικό στάδιο του σχεδιασμού [39].

4.3.2 Health Insurance Portability and Accountability Act (HIPAA)

Οι κανονισμοί του HIPAA αποτελούν το θεμελιώδες νομικό πλαίσιο στις ΗΠΑ, θεσπίζοντας πρότυπα για τη χρήση και την προστασία των πληροφοριών υγείας των ατόμων (PHI) [41]. Το πλαίσιο αυτό διακρίνεται σε δύο βασικούς κανόνες: τον κανόνα ιδιωτικότητας και τον κανόνα ασφάλειας. Ο κανόνας ιδιωτικότητας ρυθμίζει τη χρήση και την αποκάλυψη των προστατευόμενων πληροφοριών υγείας (PHI) από τις υπόχρεες οντότητες [41]. Υπόχρεες οντότητες αποτελούν οι πάροχοι υγείας, οι φορείς ασφάλισης, οι υγειονομικοί οργανισμοί καθώς και όλοι όσοι εμπλέκονται νομικά και είναι υποχρεωμένοι να προστατεύουν τα δεδομένα υγείας. Έχει ως στόχο την προστασία των ατομικών πληροφοριών υγείας, συμβάλλοντας παράλληλα στην παροχή ποιοτικών υπηρεσιών υγείας και στην αποτελεσματική προστασία του κοινωνικού συνόλου [41]. Οι υπόχρεες οντότητες επιτρέπεται να χρησιμοποιούν και να αποκαλύπτουν δεδομένα προσωπικού χαρακτήρα, για την υγεία εφόσον πληρούνται συγκεκριμένες προϋποθέσεις: για σκοπούς θεραπείας, για δημόσιο συμφέρον μεταξύ των οποίων περιλαμβάνονται περιπτώσεις που απαιτούνται από το νόμο, έρευνα υπό προϋποθέσεις, καθώς και για την αποτροπή σοβαρής απειλής για την δημόσια υγεία ή την ασφάλεια.

Ενώ ο κανόνας ιδιωτικότητας προστατεύει τις πληροφορίες για την υγεία, ο κανόνας ασφάλειας προστατεύει ένα υποσύνολο τις electronic protected health information (e-PHI), δηλαδή κάθε αναγνωρίσιμη πληροφορία υγείας που δημιουργείται, λαμβάνεται, διατηρείται ή διαβιβάζεται σε ηλεκτρονική μορφή [41]. Όλες οι υπόχρεες οντότητες πρέπει να συμμορφώνονται με τις ακόλουθες απαιτήσεις: να διασφαλίζουν το απόρρητο, την ακεραιότητα και τη διαθεσιμότητα όλων των e-PHI, να εντοπίζουν και να προστατεύουν από αναμενόμενες απειλές κατά της ασφάλειας των πληροφοριών και από αναμενόμενες μη επιτρεπόμενες χρήσεις ή γνωστοποιήσεις καθώς και να πιστοποιούν τη συμμόρφωση του προσωπικού τους δυναμικού [41].

Ο HIPAA αντιμετωπίζει σημαντικές προκλήσεις και εμφανίζει κενά στην προστασία των δεδομένων. Νέες συσκευές υγείας που πωλούνται στους καταναλωτές συλλέγουν πληροφορίες υγείας που ενδέχεται να μην εμπίπτουν στην παραδοσιακή κατηγορία των προστατευόμενων πληροφοριών για την υγεία [42]. Λόγω της απουσίας ρυθμιστικού πλαισίου, ένας σημαντικός όγκος των συλλεγόμενων μετρήσεων μπορεί να γίνει αντικείμενο εμπορικής εκμετάλλευσης [42].

Όπως και με τον GDPR, πολλές φορετές συσκευές δεν συμμορφώνονται με τους κανονισμούς ιδιωτικότητας του HIPAA. Η αντιμετώπιση αυτών των κινδύνων απαιτεί πολυμερή προσέγγιση για τη διασφάλιση της εμπιστοσύνης και της ηθικής χρήσης των δεδομένων.

4.4 ISO 27001

Το ISO/IEC 27001 αναγνωρίζεται παγκοσμίως ως το κορυφαίο πρότυπο για τη δημιουργία και συνεχή βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS) [43]. Αποτελεί έναν κεντρικό πυλώνα για την ασφάλεια των ιατρικών συσκευών, καθώς ενσωματώνει την τεχνολογία, τις διαδικασίες και τον ανθρώπινο παράγοντα σε ένα ενιαίο πλαίσιο [25]. Στο περιβάλλον του IoMT, το πρότυπο προσφέρει τη συστηματική προσέγγιση που απαιτείται για τον εντοπισμό και την αντιμετώπιση των απειλών [44]. Η εφαρμογή του είναι καθοριστική για τη διασφάλιση της ακεραιότητας των δεδομένων υγείας και τη συμμόρφωση με αυστηρές νομικές απαιτήσεις [45]. Η εισαγωγή του προτύπου δεν είναι μια απλή τεχνική επιλογή, αλλά μια στρατηγική απόφαση που θέτει τις βάσεις για την εμπιστοσύνη. Το ISO 27001 λειτουργεί ως κοινό σημείο αναφοράς μεταξύ των κατασκευαστών, των ιατρών και των ασθενών, διασφαλίζοντας ότι η καινοτομία των φορετών

συσκευών εξελίσσεται χωρίς να υπονομεύεται η ασφάλεια των δεδομένων. Για τις εταιρείες που αναπτύσσουν φορετές ιατρικές συσκευές και λογισμικό (MDSW), το πρότυπο αυτό δεν είναι απλώς μια τεχνική προδιαγραφή, αλλά ένα στρατηγικό εργαλείο που διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των ευαίσθητων δεδομένων υγείας [43].

Η κεντρική λογική του προτύπου βασίζεται στην εκτίμηση του risk assessment [45]. Το πρότυπο απαιτεί από τον οργανισμό να αναγνωρίσει όλους τους πιθανούς κινδύνους για τα δεδομένα των ασθενών και να εφαρμόσει ελέγχους που μειώνουν την πιθανότητα εμφάνισης περιστατικών ασφάλειας [45]. Εστιάζει στη δημιουργία ελέγχων που διασφαλίζουν ότι τα ιατρικά δεδομένα παραμένουν προστατευμένα καθ' όλη τη διάρκεια, από τη φορετή συσκευή προς τα κεντρικά συστήματα [44]. Μέσω των ελέγχων του, το πρότυπο καθοδηγεί τους οργανισμούς στο να εντοπίζουν έγκαιρα τις ευπάθειες πριν αυτές μετατραπούν σε ενεργές απειλές [25].

Η εφαρμογή του προτύπου στα wearables περιλαμβάνει τη διαχείριση κινδύνου κατά τη μετάδοση δεδομένων, όπως μέσω Bluetooth [43]. Το ISO 27001 βοηθά στην τυποποίηση των διαδικασιών ασφάλειας, επιβάλλοντας κοινούς ελέγχους πρόσβασης και κρυπτογράφησης, ανεξάρτητα από τη συσκευή [44]. Η ασφάλεια των παρόχων cloud που φιλοξενούν δεδομένα wearables αποτελεί κρίσιμο παράγοντα αξιοπιστίας. Για το λόγο αυτό, το πρότυπο επιβάλλει αυστηρά πρωτόκολλα ελέγχου, προκειμένου να θωρακιστεί η ακρίβεια των ευαίσθητων πληροφοριών και να διασφαλιστεί ότι η πρόσβαση παραχωρείται αποκλειστικά βάσει εξουσιοδότησης [45].

Η υιοθέτηση του ISO 27001 είναι συχνά προαπαιτούμενο για τη συμμόρφωση με τον ευρωπαϊκό κανονισμό. Το πρότυπο λειτουργεί ως η βάση που συμπληρώνεται από το ISO 27799, το οποίο προσαρμόζει τους ελέγχους ασφάλειας ειδικά για τις πληροφορίες υγείας [43]. Η χρήση του ISO 27001 προσφέρει τη δομή πάνω στην οποία μπορούν να εφαρμοστούν οι πιο λεπτομερείς τεχνικοί έλεγχοι άλλων πλαισίων, όπως το NIST [44]. Επιπλέον, βοηθά τους εμπλεκόμενους να αποδείξουν τη συμμόρφωσή τους με τον GDPR.

Συμπερασματικά, το ISO/IEC 27001 διασφαλίζει την ακεραιότητα των φορετών συσκευών καθιστώντας την ασφάλεια αναπόσπαστο κομμάτι του σχεδιασμού τους. Επίσης, επιτρέπει στις συσκευές να παραμένουν ασφαλείς απέναντι σε διαρκώς εξελισσόμενες απειλές. Τέλος, η συμμόρφωση με το πρότυπο δεν είναι μόνο νομική υποχρέωση, αλλά και εγγύηση για την εμπορική επιτυχία και την προστασία της ανθρώπινης ζωής.

4.5 ISO 27799

Το πρότυπο ISO/IEC 27799 λειτουργεί ως εξειδικευμένο πλαίσιο αναφοράς, το οποίο προσαρμόζει τους ελέγχους ασφάλειας του ISO 27002 στις ιδιαίτερες απαιτήσεις και τις κρίσιμες ανάγκες του υγειονομικού κλάδου [43]. Το συγκεκριμένο πρότυπο είναι ζωτικής σημασίας για τη διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των ιατρικών δεδομένων, λαμβάνοντας υπόψη το ευαίσθητο περιβάλλον της υγειονομικής περίθαλψης. Η ανάγκη για εξειδίκευση οδηγεί στην έκδοση του 2025 του ISO 27799, η οποία αποτελεί μια σημαντική αναθεώρηση εστιασμένη στην ασφάλεια πληροφοριών, την κυβερνοασφάλεια και την προστασία της ιδιωτικότητας [46]. Το νέο αυτό πλαίσιο παρέχει καθοδήγηση για την προστασία των PHI, λαμβάνοντας υπόψη τις σύγχρονες απειλές σε περιβάλλοντα όπου τα δεδομένα διακινούνται μέσω δικτύων και έξυπνων συσκευών. όπως οι φορετές ιατρικές συσκευές [46]. Το ISO 27799:2025 αναγνωρίζει πως μια φορετή συσκευή δεν είναι απλώς ένα αρχείο δεδομένων, αλλά ένας ενεργός στόχος κυβερνοεπίθεσης που απαιτεί δυναμική προστασία.

Ιδιαίτερη έμφαση δίνεται στην προστασία των PHI σε όλες τις μορφές τους, διασφαλίζοντας ότι η επεξεργασία τους από λογισμικό ιατρικών συσκευών (MDSW) γίνεται με ασφάλεια [43]. Το νέο

έγγραφο του 2025 συνδέεται άρρηκτα με το πρότυπο ISO 81001-1 για θέματα ασφάλειας και αποτελεσματικότητας των λογισμικών που σχετίζονται με την υγεία, κάτι που είναι κρίσιμο για τα wearables, καθώς η ασφάλειά τους εξαρτάται από τις εφαρμογές που τα συνοδεύουν [46]. Το πρότυπο απαιτεί αυστηρούς ελέγχους για τη διαχείριση της πρόσβασης και την προστασία της ιδιωτικότητας κατά τη μετάδοση των βιομετρικών δεδομένων [46], παρέχοντας κατευθυντήριες γραμμές για τη διατήρηση της εμπιστοσύνης του ασθενούς [43]. Το πρότυπο δεν εξετάζει μόνο τη συσκευή, αλλά και το λογισμικού με την ίδια αυστηρότητα για θέματα ασφάλειας.

Παράλληλα, το ISO 27799 ενισχύει την προστασία δεδομένων σε πραγματικό χρόνο και στο πλαίσιο του IoMT, δίνοντας έμφαση σε διεθνή πρότυπα ανταλλαγής δεδομένων [46]. Αυτό διασφαλίζει ότι η ανταλλαγή πληροφοριών εγγυάται την ακεραιότητα της μέτρησης από τον αισθητήρα μέχρι την αποθήκευση των δεδομένων [46]. Επίσης, η εφαρμογή του προτύπου βοηθά στην ικανοποίηση υψηλών απαιτήσεων προστασίας εθνικών πλαισίων υγείας και χρησιμοποιείται συχνά ως αναφορά σε πλαίσια αξιολόγησης [43].

Τέλος, το πρότυπο επιβάλλει μια συνεχή διαδικασία διαχείρισης κινδύνου που περιλαμβάνει τον εντοπισμό απειλών και την ψηφιακή ανθεκτικότητα των συστημάτων [46]. Η ψηφιακή ανθεκτικότητα μετατοπίζει την εστίαση από το πώς θα εμποδίσουμε την επίθεση στο πώς θα επιβιώσουμε από αυτήν. Στις φορετές ιατρικές συσκευές, είναι κρίσιμο διότι μια παραβίαση δεν πρέπει να οδηγήσει σε παύση της λειτουργίας της συσκευής, καθώς αυτό θα έθετε σε άμεσο κίνδυνο την υγεία του χρήστη. Η τήρηση του ISO 27799 αποτελεί απόδειξη ότι ο κατασκευαστής έχει λάβει υπόψη τις εξειδικευμένες απειλές που προέρχονται από τον τομέα της υγείας.

4.6 NIST SP 800-53

Το NIST SP 800-53 αποτελεί ένα από τα πιο ολοκληρωμένα πλαίσια παγκοσμίως, παρέχοντας έναν λεπτομερή κατάλογο ελέγχων ασφάλειας και προστασίας της ιδιωτικότητας για πληροφοριακά συστήματα και οργανισμούς [44]. Στον τομέα της υγείας, λειτουργεί ως το ρυθμιστικό πλαίσιο πάνω στο οποίο βασίζεται η στρατηγική κυβερνοασφάλειας, διασφαλίζοντας τη συμμόρφωση με αυστηρά πλαίσια όπως ο HIPAA [47]. Ειδικά για τις φορετές ιατρικές συσκευές, το πρότυπο αυτό προσφέρει τη δομή για την εφαρμογή τεχνικών μέτρων που θωρακίζουν τη συσκευή έναντι κυβερνοαπειλών [44]. Η διαφορά του NIST SP 800-53 από άλλα πρότυπα, όπως το ISO 27001, είναι η τεχνική του λεπτομέρεια. Ενώ το ISO θέτει τους στρατηγικούς στόχους, το NIST προσφέρει τις συγκεκριμένες οδηγίες υλοποίησης. Στα wearables, αυτή η λεπτομέρεια μετατρέπει τις γενικές οδηγίες σε πρακτικά τεχνικά βήματα για την προστασία των αισθητήρων και του λογισμικού.

Οι συσκευές IoMT χαρακτηρίζονται από υψηλή ετερογένεια, γεγονός που καθιστά δύσκολη την εφαρμογή ενιαίων μέτρων ασφάλειας [44]. Το NIST SP 800-53 επιτρέπει στους κατασκευαστές να προσαρμόζουν τους ελέγχους ανάλογα με το επίπεδο έκθεσης και τις τεχνικές δυνατότητες κάθε φορετής συσκευής [25]. Η δυνατότητα προσαρμογής επιτρέπει στον μηχανικό να επιλέξει ακριβώς τους ελέγχους που απαιτούνται, χωρίς να εξαντλεί τους περιορισμένους πόρους της συσκευής, όπως η μπαταρία και η επεξεργαστική ισχύς. Αυτή η προσέγγιση είναι κρίσιμη για τη διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων υγείας [44].

Η τελευταία (πέμπτη) αναθεώρηση του προτύπου ενσωματώνει πλήρως τους ελέγχους ιδιωτικότητας παράλληλα με τους ελέγχους ασφάλειας, κάτι που είναι ζωτικής σημασίας για συσκευές που επεξεργάζονται συνεχή ροή βιομετρικών δεδομένων [48]. Συγκεκριμένοι έλεγχοι που αναδεικνύονται ως απαραίτητοι για τα wearables περιλαμβάνουν [49]:

- SI-7 (Software and Firmware Integrity): Χρήση κρυπτογραφικών υπογραφών για την προστασία των ενημερώσεων.
- SC-8 & SC-13 (Transmission Security): Προστασία των καναλιών επικοινωνίας μεταξύ wearable και cloud.
- IA-3 (Identification and Authentication): Αυστηρή ταυτοποίηση συσκευής και χρήστη.
- SR (Supply Chain Risk Management): Έλεγχος της προέλευσης του υλικολογισμικού.

Οι παραπάνω έλεγχοι αποτελούν κρίσιμο σημείο επαφής μεταξύ της κυβερνοασφάλειας και της κλινικής ασφάλειας, διασφαλίζοντας ότι η ακεραιότητα των δεδομένων συνεπάγεται την προστασία της υγείας του χρήστη. Η ασφάλειας και η ιδιωτικότητα που προσφέρει το NIST 800-53 διασφαλίζει ότι η προστασία των δεδομένων είναι ένα θεμελιώδες χαρακτηριστικό της ψηφιακής ανθεκτικότητας της συσκευής.

Μελέτες δείχνουν ότι η πλειονότητα των ιατρικών συσκευών παραμένει εκτεθειμένη σε κρίσιμες ευπάθειες για μεγάλα χρονικά διαστήματα [50]. Το NIST SP 800-53 παρέχει τη βάση για τους ελέγχους ασφάλειας, οι οποίοι είναι απαραίτητοι για να αποτραπεί η μετατροπή ενός ψηφιακού κινδύνου σε κίνδυνο για την ανθρώπινη ζωή [51]. Επιβάλλει τη συνεχή παρακολούθηση και την ασφαλή διαχείριση διορθώσεων, αποτρέποντας downgrade attacks [47], [49]. Το NIST 800-53 προάγει τη φιλοσοφία του Security by Design, αποτελώντας τον συνδετικό κρίκο που επιτρέπει την ενσωμάτωση καθιερωμένων πρακτικών κυβερνοασφάλειας στις ιδιαίτερες απαιτήσεις ενός ιατρικού οικοσυστήματος.

Το NIST SP 800-53 αποτελεί το τεχνικό υπόβαθρο και τον κεντρικό πυλώνα προστασίας των wearables. Μετατρέπει τις αφηρημένες νομικές απαιτήσεις σε συγκεκριμένες τεχνικές λειτουργίες, διασφαλίζοντας ότι η καινοτομία των φορετών συσκευών εξελίσσεται χωρίς να υπονομεύεται η ασφάλεια των δεδομένων και η υγεία του ασθενούς. Η υιοθέτηση του συγκεκριμένου πλαισίου μειώνει δραστικά την πιθανότητα σφαλμάτων κατά την υλοποίηση. Στην ψηφιακή εποχή, η προστασία των δεδομένων υγείας μέσω προτύπων όπως το NIST 800-53 είναι εξίσου σημαντική με την ίδια την ιατρική θεραπεία.

4.7 IEEE 11073

Το ISO/IEEE 11073 είναι μια οικογένεια προτύπων, η οποία δημιουργήθηκε για τη διασφάλιση της διαλειτουργικότητας μεταξύ ιατρικών συσκευών και συσκευών υγειονομικής περίθαλψης με εξωτερικές εφαρμογές τηλεπαρακολούθησης [52], [53]. Η πρωτοβουλία IEEE 11073 Personal Health Devices (PHD) σχεδιάστηκε ειδικά για να υποστηρίξει τις απαιτήσεις των ενσωματωμένων συσκευών χαμηλής κατανάλωσης και των ασύρματων τεχνολογιών πολύ χαμηλής κατανάλωσης, όπως αυτές που χρησιμοποιούνται στις φορετές συσκευές [54]. Η τυποποίηση αυτή είναι θεμελιώδης για τη συλλογή βιοϊατρικών μετρήσεων σε κινητά περιβάλλοντα, καλύπτοντας ζωτικούς τομείς, όπως η παρακολούθηση υγείας και φυσικής κατάστασης, η υποστήριξη ανεξάρτητης διαβίωσης και η διαχείριση χρόνιων ασθενειών [54]. Η εστίαση του X73PHD στις συσκευές χαμηλής κατανάλωσης αποδεικνύει την προσαρμοστικότητά του στην εξέλιξη του mHealth. Αυτή η έμφαση είναι κρίσιμη για τη μακροζωία των wearables αισθητήρων, καθώς επιτρέπει τη συνεχή παρακολούθηση για μεγάλες χρονικές περιόδους χωρίς συχνή φόρτιση, καθιστώντας τις συσκευές πρακτικές για την καθημερινή ζωή των ασθενών.

Το πλαίσιο του X73PHD βασίζεται στο ενιαίο πρωτόκολλο ISO/IEEE 11073-20601 (Optimized Exchange Protocol), το οποίο, σε συνδυασμό με εξειδικευμένες συσκευές, διασφαλίζει τη διαλειτουργικότητα σε επίπεδο εφαρμογής [53]. Ο οργανισμός Continua Health Alliance ενισχύει την

υιοθέτηση του προτύπου, καθορίζοντας οδηγίες σχεδιασμού που περιορίζουν το ISO/IEEE 11073 για συγκεκριμένα προφίλ μεταφοράς (όπως Bluetooth HDP, USB) [52]. Η παρέμβαση του Continua Health Alliance είναι στρατηγικά σημαντική, παρόλο που το ISO/IEEE 11073 είναι ένα ολοκληρωμένο πρότυπο, η Continua το περιορίζει σε συγκεκριμένα προφίλ μεταφοράς δεδομένων. Αυτή η πρακτική είναι απαραίτητη για να διασφαλιστεί η πραγματική, απρόσκοπτη διαλειτουργικότητα στην αγορά, καθώς μειώνει τις επιλογές υλοποίησης των κατασκευαστών, αναγκάζοντάς τους να χρησιμοποιούν κοινούς, αξιόπιστους τεχνολογικούς διαύλους.

4.7.1 Αρχιτεκτονική επικοινωνίας, μοντέλα και λειτουργίες

Η επικοινωνία στο πλαίσιο του IEEE 11073 βασίζεται σε σαφώς καθορισμένους ρόλους υλικού και λογισμικού. Ο IEEE Agent (PHD / HDP Source) αποτελεί τη μονάδα υλικού στις φορετές ιατρικές συσκευές, η οποία είναι υπεύθυνη για την απόκτηση και την επεξεργασία των δεδομένων [52]. Ο Agent χρησιμοποιεί επεξεργαστές ψηφιακού σήματος (DSPs) για την επεξεργασία δεδομένων σε πραγματικό χρόνο, συμπεριλαμβανομένης της αφαίρεσης θορύβου [52]. Αντίστοιχα, ο IEEE Manager (HDP Sink) αντιστοιχεί στο λειτουργικό σύστημα της εφαρμογής smartphone, το οποίο λαμβάνει και διαχειρίζεται τα επεξεργασμένα δεδομένα [52]. Η διαλειτουργικότητα διασφαλίζεται μέσω των εξειδικευμένων συσκευών (ISO/IEEE 11073-104xx), οι οποίες λειτουργούν για να ορίσουν λεπτομερώς τον τρόπο με τον οποίο κάθε τύπος συσκευής διαμορφώνει και μεταδίδει τα χαρακτηριστικά των δεδομένων [53]. Για παράδειγμα, το παλμικό οξύμετρο είναι η πιο διαδεδομένη τυποποιημένη συσκευή σε αυτά τα συστήματα (43% των περιπτώσεων) [54]. Επιπλέον, το σύστημα ενσωματώνει λειτουργίες διαχείρισης προειδοποιήσεων όπως ανίχνευση κινδύνου, παρακολουθώντας αλλαγές στον καρδιακό ρυθμό και εκπέμποντας προειδοποιήσεις για βραδυκαρδία και ταχυκαρδία [54]. Η ύπαρξη σαφών ρόλων Agent/Manager και η χρήση εξειδικεύσεων συσκευών αποτελούν το βασικό πλεονέκτημα του προτύπου, επιλύοντας το πρόβλημα της ασυμβατότητας. Ωστόσο, η κυριαρχία συγκεκριμένων συσκευών στο υπάρχον ερευνητικό τοπίο δείχνει ότι, παρόλο που το πρότυπο είναι επεκτάσιμο, η πραγματική υιοθέτησή του σε νεότερους και πιο εξειδικευμένους τύπους wearables συσκευών χρειάζεται περαιτέρω ενίσχυση.

4.7.2 Προκλήσεις ασφάλειας, Wearables και ενσωμάτωση στο IoT

Παρόλο που το X73PHD παρέχει ένα ισχυρό μοντέλο διαλειτουργικότητας, η ασφάλεια είναι περιορισμένη [53]. Το πρότυπο δεν ορίζει μηχανισμό κρυπτογράφησης δεδομένων, με αποτέλεσμα η κρυπτογράφηση να εξαρτάται αποκλειστικά από το υποκείμενο πρωτόκολλο μεταφοράς [53]. Επιπλέον, η πιστοποίηση της συσκευής (Agent-Manager) είναι περιορισμένη, καθώς δεν υπάρχει μηχανισμός για αμοιβαία πιστοποίηση, αλλά χρησιμοποιείται μόνο το System-ID (IEEE EUI-64) για αναγνώριση [53]. Αυτή η προσέγγιση είναι κατανοητή λόγω των περιορισμών σε υπολογιστική ισχύ και ενέργεια των παλαιότερων PHDs, ωστόσο αποτελεί μια σημαντική παράλειψη για σύγχρονα συστήματα, ειδικά σε κρίσιμα περιβάλλοντα όπου η ακεραιότητα των δεδομένων είναι ζωτικής σημασίας. Αυτές οι αδυναμίες καθιστούν τις PHDs ευάλωτες σε κινδύνους όπως η πλαστοπροσωπία, οι επιθέσεις επανεκπομπής και η άρνηση ευθύνης για τις μετρήσεις [53]. Ως εκ τούτου, οι εφαρμογές mHealth πρέπει να βασίζονται σε εξωτερικά πρωτόκολλα τα οποία θα προσθέσουν απαραίτητα επίπεδα προστασίας, όπως η κρυπτογράφηση και η ψηφιακή υπογραφή των δεδομένων [53]. Η ανάγκη για εξωτερική επέκταση της ασφάλειας, υπογραμμίζει τη φύση του X73PHD ως πρωτοκόλλου διαλειτουργικότητας και όχι ως ολοκληρωμένης λύσης ασφάλειας (end-to-end security solution). Ωστόσο, αυτό προσθέτει πολυπλοκότητα και επιπλέον κόστος στην ανάπτυξη συστημάτων, το οποίο θα μπορούσε να αποφευχθεί με μια πιο ισχυρή αρχιτεκτονική ασφάλειας.

Στο πλαίσιο της ενσωμάτωσης IoT και Wearables, το πρότυπο αντιμετωπίζει προκλήσεις από τους περιορισμούς των συσκευών, όπως η περιορισμένη παροχή ενέργειας και η χωρητικότητα CPU [54]. Για την ενσωμάτωση του 40% των μη συμβατών συσκευών, προτείνεται η χρήση ειδικών μονάδων X73 wrapper ή adaptor, οι οποίες λειτουργούν ως μεταφραστές [55]. Τέλος, το X73PHD είναι η γέφυρα τυποποίησης που καθιστά τεχνικά εφικτή την αποτελεσματική και μεγάλης κλίμακας ανάπτυξη εφαρμογών Digital Twin στην υγειονομική περίθαλψη και πιο συγκεκριμένα στις φορετές ιατρικές συσκευές [56].

4.8 IEEE 11073-20601

Το IEEE 11073-20601 (Optimized Exchange Protocol - OEP) αποτελεί το θεμελιώδες πρωτόκολλο στη μηχανική των πολύπλοκων ιατρικών συστημάτων [57]. Ο ρόλος του είναι να εγγυάται τη διαλειτουργικότητα των συσκευών προσωπικής υγείας που κατασκευάζονται από διαφορετικούς προμηθευτές, επιτρέποντας στους χρήστες να επιλέγουν ελεύθερα οποιαδήποτε ιατρική συσκευή [65]. Το πρωτόκολλο σχεδιάστηκε ειδικά για ανταλλαγή δεδομένων προσωπικής υγείας σε αυστηρά πλαίσια, όπου οι συσκευές είναι περιορισμένες σε πόρους σε σύγκριση με τον επαγγελματικό κλινικό εξοπλισμό [57].

Το 20601 OEP θεσπίζει τις λογικές συνδέσεις και παρέχει τις υπηρεσίες επικοινωνίας [58]. Η συνολική αρχιτεκτονική του 11073 βασίζεται σε ένα αντικειμενοστραφές σύστημα διαχείρισης [59] και αποτελείται από τρεις βασικές συνιστώσες:

- Domain Information Model (DIM): Χαρακτηρίζει τις πληροφορίες της συσκευής ως ένα σύνολο αντικειμένων [58]. Το αντικείμενο Medical Device System (MDS) βρίσκεται στην κορυφή και περιγράφει τη συσκευή και τις ιδιότητές της [59]. Αυτό το μοντέλο είναι κρίσιμο, καθώς διασφαλίζει τη σημασιολογική διαλειτουργικότητα, επιτρέποντας σε ένα Manager να κατανοήσει τη φύση και τη μονάδα μέτρησης των δεδομένων ανεξάρτητα από τον κατασκευαστή της συσκευής.
- Service Model: Καθορίζει τον εννοιολογικό μηχανισμό αλληλεπίδρασης και παρέχει τις αρχικές ενέργειες για την πρόσβαση στα δεδομένα [58]. Τα δεδομένα μετρήσεων αποστέλλονται μέσω του event report [57].
- Communication Model: Ορίζει τη λογική τοπολογία, μία ή περισσότερες συσκευές Agent επικοινωνούν με έναν Manager και περιγράφει τη δυναμική συμπεριφορά του συστήματος μέσω του αλγορίθμου [65]. Το πρωτόκολλο έχει σχεδιαστεί ώστε να είναι φορητό σε διαφορετικά μέσα μεταφοράς, όπως USB και Bluetooth [57].

Το πρωτόκολλο 20601 λειτουργεί ως ο κορμός πάνω στον οποίο βασίζεται η οικογένεια προτύπων ISO/IEEE 11073-104xx (Device Specializations) [59]. Κάθε εξειδίκευση χρησιμοποιεί την ορολογία και τα μοντέλα του 20601 για να ορίσει τον τρόπο μοντελοποίησης των συγκεκριμένων δεδομένων. Το πρωτόκολλο είναι βελτιστοποιημένο για τις απαιτήσεις χρήσης προσωπικών συσκευών και σχεδιασμένο ώστε να φιλοξενήσει τις δυνατότητες των συσκευών χαμηλής ισχύος [59].

Το 20601 OEP εισήγαγε το concept Persistent Metric Store (PM-store) ως μηχανισμό για την αρχειοθέτηση και μεταφορά μεγάλων ποσοτήτων δεδομένων που είναι αποθηκευμένα στη συσκευή Agent [58]. Ο PM-store χρησιμοποιείται για μετρήσεις που υπερβαίνουν το όριο των εικοσιπέντε προσωρινά αποθηκευμένων μετρήσεων που επιτρέπεται σε μία αναφορά συμβάντος, και είναι ιδανικός για συνεχείς μεγάλες κυματομορφές, όπως το ΗΚΓ [58]. Όλες οι αλληλεπιδράσεις για την ανάκτηση και τον καθαρισμό των δεδομένων του PM-store ξεκινούν από τον Manager [58].

Παρά την πολυπλοκότητα του OEP, το πρωτόκολλο αντιμετωπίζει ένα κρίσιμο πρόβλημα στα σενάρια παρακολούθησης σε πραγματικό χρόνο: το 20601 OEP δεν υποστηρίζει κανένα είδος συμπιεσμένων δεδομένων, παρά μόνο τα αρχικά δεδομένα [58]. Δεδομένης της περιορισμένης ασύρματης χωρητικότητας και των ασταθών συνθηκών καναλιού, η εφαρμογή τεχνικών συμπίεσης είναι απαραίτητη. Λόγω του ορισμού του PM-store, ο οποίος επιτρέπει την αποθήκευση μόνο του ίδιου αντικειμένου δεδομένων, ένα PM-store σχεδιασμένο για την κυματομορφή (RT-SA object) δεν μπορεί να χρησιμοποιηθεί για την αποθήκευση συμπιεσμένων δεδομένων [58].

Για να αντιμετωπιστεί το πρόβλημα της συμπίεσης, προτείνετε μια νέα εκτεταμένη αρχιτεκτονική Agent/Manager [58]:

- Δύο PM-Stores: Οι εκτεταμένες συσκευές διαθέτουν δύο PM-stores σε διαφορετικά επίπεδα. Ένα άνω επίπεδο (Upper Layer) για την αρχική κυματομορφή, εξασφαλίζοντας τη συμβατότητα και ένα κάτω επίπεδο (Lower Layer) για τα συμπιεσμένα δεδομένα.
- Διαφάνεια μετάδοσης: Ο εκτεταμένος Manager ανακτά τα συμπιεσμένα δεδομένα από το κάτω επίπεδο, τα αποσυμπιέζει και αποθηκεύει την αποκαταστημένη κυματομορφή στο PM-store του άνω επιπέδου, καθιστώντας τη διαδικασία διαφανή για το τελικό σύστημα. Το νέο σχήμα μετάδοσης επιδεικνύει καλύτερη απόδοση στην αποστολή δεδομένων ΗΚΓ μέσω θορυβώδους ασύρματου καναλιού.

Τέλος, η πολυπλοκότητα του πρωτοκόλλου καθιστά αναγκαία τη χρήση τυπικών μεθόδων. Η μοντελοποίηση του ISO/IEEE 11073-20601:2016 με τη γλώσσα Promela και ο έλεγχος με το εργαλείο Spin αποκάλυψαν προβλήματα σε ροές εργασίας που θα μπορούσαν να προκαλέσουν προβλήματα [57].

4.9 IEEE 11073-10404

Η τυποποίηση των ιατρικών μετρήσεων εξαρτάται σε μεγάλο βαθμό από τις προδιαγραφές των συσκευών ISO/IEEE 11073-104xx [52]. Κάθε εξειδίκευση ορίζει λεπτομερώς το μοντέλο πληροφοριών (objects, attributes, term codes) και τον τρόπο με τον οποίο πρέπει να κωδικοποιούνται και να αποστέλλονται τα δεδομένα για τον αντίστοιχο τύπο ιατρικής συσκευής [52]. Συγκεκριμένα, το πρότυπο IEEE 11073-10404 παρέχει την τυπική αναπαράσταση για την επικοινωνία δεδομένων από παλμικό οξύμετρο [52].

Αυτό το πρότυπο θεσπίζει έναν νομοθετικό ορισμό της επικοινωνίας μεταξύ προσωπικών συσκευών τηλεϊατρικής παλμικού οξύμετρου και compute engines [60]. Ο κύριος στόχος του είναι να επιτρέψει τη διαλειτουργικότητα "plug-and-play" [60]. Το πρότυπο καθορίζει την κωδικοποίηση των μετρήσεων του κορεσμού οξυγόνου στο αίμα και του καρδιακού ρυθμού.

Η εφαρμογή του προτύπου επιτρέπει την αποτελεσματική παρακολούθηση ζωτικών σημείων και τη χρήση ειδικών μηχανισμών προειδοποίησης για την ανίχνευση καταστάσεων κινδύνου, όπως η υποξαιμία [52]. Επιπλέον, το πρότυπο περιορίζει τις προαιρετικές δυνατότητες στα βασικά πλαίσια υπέρ της διαλειτουργικότητας, ορίζοντας έναν κοινό πυρήνα λειτουργικότητας επικοινωνίας για τα παλμικά οξύμετρα τηλεϊατρικής [60].

Η απλότητα και η τυποποίηση του 10404 μέσω έτοιμων λύσεων firmware και της καθοδήγησης του οργανισμού Continua αποτελεί το κύριο πλεονέκτημα για τη γρήγορη ανάπτυξη συστημάτων τηλεϊατρικής [52]. Η υποχρέωση περιορισμού των επιλογών που θέτει το πρότυπο εξηγεί γιατί η υλοποίησή του είναι απλή: εστιάζει στην αποτελεσματική μετάδοση τυποποιημένων, διακριτών τιμών, καθιστώντας το ιδανικό για εφαρμογές βασικής παρακολούθησης [60]. Η εστίαση στην απλότητα και

στις διακριτές τιμές σηματοδοτεί μια συνειδητή διάκριση του X73PHD από τα πρότυπα που αφορούν τον διαγνωστικό εξοπλισμό. Ενώ για τη διάγνωση απαιτείται η ανάλυση της αρχικής κυματομορφής, για την τηλεπαρακολούθηση και την ανίχνευση κινδύνου αρκούν οι τιμές που έχουν επεξεργαστεί. Συνεπώς, το 10404 επιτυγχάνει βέλτιστη ισορροπία μεταξύ της απαιτούμενης κλινικής αξίας, της ανάγκης για χαμηλό bandwidth καθώς και της περιορισμένης επεξεργαστικής ισχύος στις φορετές συσκευές.

4.10 IEEE 11073-10406

Το πρότυπο IEEE 11073-10406 αφορά την τυποποίηση της μετάδοσης δεδομένων από ηλεκτροκαρδιογράφο, συμπεριλαμβανομένης της κυματοφόρμας [52]. Αυτό το πρότυπο θεσπίζει έναν νομοθετικό ορισμό της επικοινωνίας μεταξύ προσωπικών συσκευών ηλεκτροκαρδιογράφου και εφαρμογών διαχείρισης, με απώτερο στόχο την επίτευξη αυτόματης διαλειτουργικότητας [61]. Ορίζει έναν κοινό πυρήνα λειτουργικότητας για προσωπικές συσκευές τηλειατρικής, υποστηρίζοντας ΗΚΓ με έναν έως τρεις αγωγούς (leads) [61].

Η αρχιτεκτονική δεδομένων ορίζει ένα σύνθετο μοντέλο αντικειμένων, απαραίτητο για τη μεταφορά τόσο αριθμητικών δεδομένων όσο και δεδομένων συνεχούς ροής [52]. Συνεπώς, η υλοποίηση ροής απαιτεί τη χρήση ενός καναλιού ροής μέσω του Bluetooth HDP για τη συνεχή κυματομορφή, παράλληλα με ένα αξιόπιστο κανάλι για τις κρίσιμες αριθμητικές πληροφορίες [52].

Λόγω της πολυπλοκότητας των απαιτήσεων που σχετίζονται ιδίως με τη μετάδοση της κυματομορφής, οι εφαρμογές συχνά καθιστούν απαραίτητη την προσαρμοσμένη ανάπτυξη υλικολογισμικού, ώστε να υλοποιηθεί με ακρίβεια το πρωτόκολλο διαχείρισης κατάστασης του προτύπου IEEE 11073-20601 [52]. Η απαίτηση για προσαρμοσμένο λογισμικό στην υλοποίηση του 10406, σε αντίθεση με την απλότητα του 10404, υποδεικνύει ότι αυτό το πρότυπο ωθεί τα όρια των περιορισμένων Personal Health Devices, καθώς η μετάδοση κυματομορφής απαιτεί σημαντικά μεγαλύτερη επεξεργαστική ισχύ.

Παρ' όλα αυτά, η κλινική αξία του προτύπου δικαιολογεί αυτή την πολυπλοκότητα. Η εξειδίκευση υποστηρίζει την έγκαιρη ανίχνευση καρδιακών αρρυθμιών. Μάλιστα, η λειτουργία προειδοποίησης περιλαμβάνει την αποθήκευση και μετάδοση δεδομένων ηλεκτροκαρδιογράφου πριν και μετά το συμβάν, μια κρίσιμη λειτουργία για τη λεπτομερή κλινική αξιολόγηση [52].

Είναι σημαντικό ότι το πρότυπο διαχωρίζει τις συσκευές παρακολούθησης από τον διαγνωστικό εξοπλισμό, καθώς δεν απαιτεί τη δυνατότητα ανάλυσης ή σχολιασμού της ανιχνευόμενης ηλεκτρικής δραστηριότητας. Η υποχρέωση αυτής της διάκρισης και ο περιορισμός στους τρεις αγωγούς [61] δικαιολογεί την πολυπλοκότητα. Το 10406 επιτυγχάνει μια βέλτιστη ισορροπία επιτρέποντας την αποστολή κρίσιμης κυματομορφής για την ανίχνευση συμβάντων χωρίς να επιβαρύνει τη φορετή συσκευή με τις σύνθετες απαιτήσεις πλήρους διαγνωστικής ανάλυσης.

4.11 IEEE 11073-10407

Το 10407 πρόκειται για το πρότυπο της σειράς IEEE 11073 που καθορίζει ρητά τις τεχνικές προδιαγραφές για την επικοινωνία των δεδομένων από τις συσκευές παρακολούθησης αρτηριακής πίεσης προς τις κεντρικές μονάδες επεξεργασίας [62]. Στις μονάδες λήψης και επεξεργασίας των δεδομένων συγκαταλέγονται συσκευές όπως κινητά τηλέφωνα, προσωπικοί υπολογιστές, συσκευές προσωπικής υγείας και αποκωδικοποιητές [62], [63].

Ο πρωταρχικός στόχος του προτύπου είναι να επιτρέψει τη διαλειτουργικότητα plug-and-play [62]. Το πρότυπο αξιοποιεί κατάλληλα μέρη υφιστάμενων προτύπων της οικογένειας IEEE 11073, συμπεριλαμβανομένων, των μοντέλων πληροφοριών, των προτύπων εφαρμογών και των προτύπων μεταφοράς [63].

Συγκεκριμένα, καθορίζει λεπτομερώς την υποχρεωτική χρήση ειδικών μορφών, δομές δεδομένων και κανόνων επικοινωνίας στα συστήματα τηλεϊατρικής [63]. Αυτός ο καθορισμός γίνεται μέσω του περιορισμού των προαιρετικών δυνατοτήτων στα βασικά πλαίσια, υπέρ της διαλειτουργικότητας. Ουσιαστικά, το πρότυπο ορίζει έναν κοινό πυρήνα λειτουργικότητας επικοινωνίας για τις συσκευές παρακολούθησης αρτηριακής πίεσης.

Η κεντρική φιλοσοφία του 10407 έγκειται στην προτεραιότητα της συμβατότητας έναντι της ευελιξίας, κάτι που είναι ζωτικής σημασίας για την επιτυχία των συστημάτων τηλεϊατρικής. Ένα σύστημα λήψης δεδομένων πρέπει να είναι σε θέση να λαμβάνει και να ερμηνεύει αμέσως και χωρίς σφάλματα τα δεδομένα πίεσης από οποιοδήποτε συσκευή παρακολούθησης αρτηριακής πίεσης που φέρει το σήμα 11073-10407, ανεξάρτητα από τον κατασκευαστή του. Μέσω του αυστηρού περιορισμού των προαιρετικών στοιχείων, διασφαλίζεται ότι τα δεδομένα πίεσης που συλλέγονται από διαφορετικά μοντέλα συσκευών παρακολούθησης αρτηριακής πίεσης θα γίνονται απολύτως κατανοητά από τα συστήματα διαχείρισης ηλεκτρονικών αρχείων υγείας, ενισχύοντας την αξιοπιστία και την αυτοματοποίηση της απομακρυσμένης παρακολούθησης ασθενών.

4.12 IEEE 11073-10417

Το πρότυπο IEEE 11073-10417 αποτελεί την κρίσιμη εξειδίκευση για την συσκευή μέτρησης της γλυκόζης [64]. Η συγκεκριμένη τυποποίηση είναι απαραίτητη για τη διαχείριση του διαβήτη, καθώς επιτρέπει την ανταλλαγή δεδομένων, μετρήσεων γλυκόζης με το συστήματα υγείας [59].

Στο πλαίσιο της ανάπτυξης εφαρμογών για την αυτοπαρακολούθηση της γλυκόζης αίματος σε ασθενείς με διαβήτη, το πρότυπο 11073-10417 λειτουργεί ως κεντρική συνιστώσα [64]. Ένας από τους βασικούς τεχνολογικούς πυλώνες του συστήματος είναι η επικοινωνία. Η επικοινωνία με τον μετρητή γλυκόζης επιτυγχάνεται μέσω της υλοποίησης του IEEE 11073 Manager και του Bluetooth HDP Connector [64], ένα από τα πιο κοινά κανάλια επικοινωνίας για προσωπικές ιατρικές συσκευές.

Η δομή του πρωτοκόλλου IEEE 11073 περιλαμβάνει τρεις βασικούς άξονες: το Optimized Exchange Protocol, τις Device Specializations (όπως το 10417) και τα Communication Protocols (Bluetooth HDP) [64]. Το μοντέλο πληροφοριών του 10417 υλοποιείται χρησιμοποιώντας τις κλάσεις του Domain Information Model (DIM) του X73PHD, όπως οι κλάσεις Numeric και Enumeration, καθώς και την κορυφαία κλάση Medical Device System (MDS) [64]. Επιπλέον, το πρότυπο 10417 βασίζεται σε μια συγκεκριμένη φιλοσοφία διαχείρισης δεδομένων που διασφαλίζει την ακεραιότητα και τη διαθεσιμότητα των μετρήσεων [59]. Συγκεκριμένα, το 11073-10417 προβλέπει δύο αμοιβαία αποκλειόμενους τρόπους μετάδοσης δεδομένων στον Manager μέσω event reports [59].

Η έννοια του Transcoding είναι θεμελιώδης για τη γεφύρωση του τεχνολογικού κενού μεταξύ των απλών πρωτοκόλλων, όπως το Bluetooth, και του μοντέλου του IEEE 11073 [59]. Αυτή η διαδικασία περιλαμβάνει τη χαρτογράφηση των τιμών των χαρακτηριστικών Bluetooth στα αντίστοιχα αντικείμενα και τα χαρακτηριστικά του 11073-10417 [59]. Οι τιμές γλυκόζης από το Bluetooth μετατρέπονται σε Basic-Nu-Observed-Value στο 11073-10417, χρησιμοποιώντας τον τύπο δεδομένων SFLOAT [59]. Αυτή η μετατροπή είναι ζωτικής σημασίας για να διαβάζεται η μέτρηση με τον ίδιο τρόπο από οποιοδήποτε συμβατό σύστημα.

Πέρα από τις βασικές μετρήσεις, η λεπτομερής ανάλυση του 10417 αποδεικνύει ότι η οικογένεια προτύπων ISO/IEEE 11073 παρέχει ένα ολοκληρωμένο μοντέλο για τη συλλογή και την ερμηνεία όχι μόνο των βασικών μετρήσεων αλλά και των κρίσιμων κλινικών πλαισίων [59]. Το πρότυπο επιτρέπει την προαιρετική μετακωδικοποίηση πληροφοριών που είναι κρίσιμες για την αποτελεσματική διαχείριση του διαβήτη, όπως τα δεδομένα άσκησης, που περιλαμβάνουν τη διάρκεια και την ένταση, η φαρμακευτική αγωγή, που καταγράφει τον τύπο και την ποσότητα ινσουλίνης και οι υδατάνθρακες, που καταγράφουν την ποσότητα που καταναλώθηκε.

Η υλοποίηση του 11073-10417 έχει άμεση κλινική αξία. Η αυτόματη λειτουργία που καταγράφει το επίπεδο γλυκόζης αίματος μέσω Bluetooth κρίθηκε ιδιαίτερα χρήσιμη, καθώς επιτρέπει στους επαγγελματίες να παρατηρούν τις τάσεις στις αλλαγές της γλυκόζης [64]. Η εφαρμογή μπορεί επίσης να χρησιμοποιηθεί για την παροχή ακριβούς ανατροφοδότησης σε επαγγελματίες κατά τη διαχείριση των ασθενών [64]. Αυτή η αυτοματοποίηση μειώνει το ανθρώπινο λάθος και βελτιώνει την ποιότητα της φροντίδας. Τα δεδομένα γλυκόζης που αποθηκεύονται τοπικά μετατρέπονται σε έγγραφο Continuity of Care Document (CCD) και μεταδίδονται στον διακομιστή web μέσω HTTP [64].

4.13 IEEE 802.15.6

Το WBAN, που τυποποιείται από το IEEE 802.15.6, αντιπροσωπεύει μια κομβική τεχνολογία στα σύγχρονα συστήματα υγείας, η οποία αποτελεί καινοτομία στην ιατρική περίθαλψη αντικαθιστώντας τις παραδοσιακές ενσύρματες μεθόδους [65]. Ο πρωταρχικός ρόλος του είναι η συνεχής παρακολούθηση της υγείας, συλλέγοντας κρίσιμα στατιστικά στοιχεία για τους ασθενείς μέσω ασύρματων αισθητήρων που τοποθετούνται μέσα ή πάνω στο ανθρώπινο σώμα [65]. Τα δεδομένα αποστέλλονται σε πραγματικό χρόνο, επιταχύνοντας τη διάγνωση και την έγκαιρη θεραπεία. Το πρότυπο, του οποίου η πρώτη έκδοση ανακοινώθηκε το 2012, είναι θεμελιώδες για τα MBANs [66], τα οποία αποτελούν υποομάδα των WBANs.

Το πρότυπο IEEE 802.15.6 προτάθηκε από την Task Group 6 (TG6) ως απάντηση στην αδυναμία των προηγούμενων προτύπων, όπως το 802.15.4, να καλύψουν πλήρως τις ανάγκες των ιατρικών εφαρμογών, ιδίως όσον αφορά την αξιοπιστία, την εξαιρετικά χαμηλή κατανάλωση ενέργειας και τα ζητήματα μετάδοσης δεδομένων [65]. Ο σχεδιασμός επιβάλλει αυστηρές απαιτήσεις για τις ιατρικές συσκευές WBAN. Η αξιοπιστία είναι πρωταρχικής σημασίας, με τη χρονική καθυστέρηση για τις ιατρικές εφαρμογές να πρέπει να είναι μικρότερη από 125 ms [65]. Οι συνδέσεις MBAN πρέπει να υποστηρίζουν ρυθμούς bit από 10 Kbps έως 10 Mbps [67].

Το πρότυπο ορίζει τρία φυσικά επίπεδα για την μετάδοση των δεδομένων [67]:

- Narrowband (NB): Στοχεύει στην επικοινωνία με εμφυτεύσιμους και φορητούς κόμβους.
- Ultra-wideband (UWB): Αυξάνει τη στιβαρότητα, επιτυγχάνει χαμηλή κατανάλωση ενέργειας και υποστηρίζει υψηλούς ρυθμούς δεδομένων (έως 20 Mbps) που είναι απαραίτητοι για σήματα υψηλής συχνότητας.
- Human Body Communication Layer (HBC): Έχει πολύ χαμηλή κατανάλωση ενέργειας και λιγότερες παρεμβολές, αν και απαιτεί οι κόμβοι να είναι σε άμεση επαφή με το σώμα .

Το επίπεδο Media Access Control (MAC) του 802.15.6 είναι ζωτικής σημασίας για τη διαχείριση της πρόσβασης και της ενέργειας. Το πρότυπο πρέπει να υποστηρίζει κυκλοφορία έκτακτης ανάγκης, η οποία λαμβάνει προτεραιότητα έναντι άλλων μηνυμάτων [65]. Το MAC χρησιμοποιεί φάσεις όπως η Exclusive Access Phase (EAP) για την κυκλοφορία έκτακτης ανάγκης [66]. Το Contention Window

(CW) του CSMA/CA χρησιμοποιείται για την διαχείριση της ροής, όπου οι κόμβοι με υψηλότερη προτεραιότητα έχουν μικρότερο CW, επιτρέποντάς τους να αποκτούν πρόσβαση στο κανάλι γρηγορότερα [12].

Η χαμηλή κατανάλωση ενέργειας και η μακρά διάρκεια ζωής της μπαταρίας είναι κρίσιμες απαιτήσεις [82]. Το πρότυπο επιτρέπει τη διαδικασία κύκλου λειτουργίας [12] και τη χρήση τεχνικών όπως η προσέγγιση Event-Driven (ED-802.15.6) όπου εφαρμόζεται φιλτράρισμα δεδομένων, επιτρέποντας τη μετάδοση προς τον κεντρικό κόμβο (HUB) μόνο των ενδείξεων που παρουσιάζουν στατιστικά σημαντική απόκλιση από τις προκαθορισμένες παραμέτρους, μειώνοντας την κατανάλωση ενέργειας κατά 67% και την καθυστέρηση κατά 21% σε σχέση με την παραδοσιακή συνεχή αποστολή [12]. Επίσης, εξετάζεται η χρήση ενέργειας που παράγεται από το ίδιο το ανθρώπινο σώμα ή το περιβάλλον του και έπειτα η μετατροπή αυτής σε ηλεκτρικής μορφής την ενέργεια, προκειμένου να τροφοδοτήσουν τους αισθητήρες και τους κόμβους [12].

Παρόλο που το πρότυπο προβλέπει τρία επίπεδα ασφάλειας, εμπιστευτικότητα ώστε τα δεδομένα να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, ακεραιότητα για να μην αλλοιώνονται τα δεδομένα κατά τη μεταφορά και διαθεσιμότητα ώστε το δίκτυο να είναι διαθέσιμο όλο το εικοσιτετράωρο, οι προδιαγραφές του θεωρούνται ανεπαρκείς για ρεαλιστικά σενάρια MBAN [68]. Πιο συγκεκριμένα:

- Single Point of Failure (SPOF): Ο hub μπορεί να αποτελέσει ενιαίο σημείο αστοχίας [67], [68]. Επίθεση Jamming μπορεί να προκαλέσει προβλήματα σε ολόκληρο το δίκτυο ή να προκαλέσει γρήγορη αποφόρτιση της μπαταρίας [65]. Αυτό είναι ιδιαίτερα επικίνδυνο για τους εμφυτεύσιμους αισθητήρες.
- Επιθέσεις τροποποίησης δεδομένων: Η τροποποίηση δεδομένων είναι μια ενεργητική επίθεση όπου ο εισβολέας αλλοιώνει εν μέρει ή πλήρως τα δεδομένα του ασθενούς προτού τα στείλει πίσω στον πάροχο υγειονομικής περίθαλψης ή στον γιατρό. Παράδειγμα αποτελεί ο χρόνος μεταξύ των μεταδόσεων όπου τα δεδομένα μπορούν να τροποποιηθούν έπειτα από πρόσβαση στην πλατφόρμα. Αυτό επιτρέπει στον εισβολέα να παραποιήσει τα αρχικά δεδομένα και να παρεμποδίσει τη διαγνωστική διαδικασία λήψης αποφάσεων [67], [68].
- Επιθέσεις υποκλοπής δεδομένων: Η υποκλοπή είναι μια παθητική επίθεση όπου ο εισβολέας ακούει το δίκτυο και διαβάζει τις εμπιστευτικές πληροφορίες που μεταδίδονται. Παράδειγμα αποτελεί η περίπτωση όπου ένας εισβολέας μπορεί να υποκλέψει την κίνηση και να καταγράψει πακέτα που περιέχουν δεδομένα όπως η γλυκόζης αίματος και η δοσολογίας ινσουλίνης [68].
- Προβλήματα αυθεντικοποίησης: Έχουν βρεθεί σοβαρά τρωτά σημεία στα πρωτόκολλα σύνδεσης/αυθεντικοποίησης του 802.15.6. Η μη αυθεντικοποιημένη σύνδεση αφήνει το σύστημα ευάλωτο σε επιθέσεις πλαστοπροσωπίας. Πρωτόκολλα όπως το password authenticated association και το display authenticated association δεν είναι κατάλληλα ή είναι ευάλωτα σε επιθέσεις [68].

Για την αντιμετώπιση αυτών των αδυναμιών, η έρευνα έχει προτείνει διάφορους μηχανισμούς [65], [66]:

- Κρυπτογράφηση βασισμένη σε λογισμικό στο επίπεδο σύνδεσης και κρυπτογράφηση υλικού (Hardware Encryption) με χρήση AES 128-bit.
- Έλεγχος πρόσβασης χρησιμοποιώντας Fuzzy Attribute-Based Signcryption (FABSC) για κρυπτογράφηση, ψηφιακή υπογραφή και έλεγχο πρόσβασης. Καθώς επίσης και χρήση των βιομετρικών χαρακτηριστικών του σώματος για έλεγχο ταυτότητας και καθιέρωση κλειδιών.

- Διαχείριση αποτυχίας λαμβάνοντας υπόψη τους μηχανισμούς CSMA/Back-off και Contention Windows για τη διαχείριση συγκρούσεων. Καθώς και διασφάλιση ότι η κυκλοφορία έκτακτης ανάγκης λαμβάνει άμεση προτεραιότητα. Η χρήση 2-hop αναμεταδοτών βελτιώνει το Packet Delivery Ratio (PDR) για την κυκλοφορία έκτακτης ανάγκης (στο 99% σε σύγκριση με 61% χωρίς αναμετάδοση).

Το πρότυπο IEEE 802.15.6 έθεσε τις βάσεις για τα WBAN/MBAN, εστιάζοντας ορθώς στην ενέργεια και την αξιοπιστία. Ωστόσο, η έμφαση στην ασφάλεια ως πρωταρχική πρόκληση υποδηλώνει ότι το ίδιο το πρότυπο, όπως σχεδιάστηκε, δεν κατάφερε να καλύψει επαρκώς τις ανάγκες ρεαλιστικών ιατρικών εφαρμογών. Η βασική αρχιτεκτονική του, με τον hub ως SPOF [68] και τα τρωτά σημεία στα πρωτόκολλα σύνδεσης, δημιουργούν ένα υψηλό ρίσκο το οποίο καθιστά απαραίτητη την εφαρμογή πρόσθετων μηχανισμών όπως FABSC και συστήματα ελέγχου ταυτότητας βασισμένα σε βιομετρικά στοιχεία, για την αντιμετώπιση των απειλών DoS, πλαστοπροσωπίας και εξάντλησης μπαταρίας [65]. Η επιλογή του κατάλληλου πρωτοκόλλου και η χρήση τεχνικών εξοικονόμησης ενέργειας, παραμένουν κρίσιμες αποφάσεις σχεδιασμού [12].

4.14 Επίλογος

Το παρόν κεφάλαιο ανέλυσε διεξοδικά το κρίσιμο πεδίο των προσωπικών δεδομένων υγείας των φορετών ιατρικών συσκευών, επιβεβαιώνοντας τη θεμελιώδη σημασία της ασφάλειας και της ακεραιότητας των πληροφοριών. Η ραγδαία ψηφιοποίηση των υπηρεσιών υγείας, αν και προσφέρει πρωτοποριακές δυνατότητες για την απομακρυσμένη παρακολούθηση, έχει μετατρέψει τα δεδομένα υγείας σε πρωταρχικό στόχο.

Η ανάγκη για προστασία των ευαίσθητων δεδομένων οδήγησε στην εξέταση των δύο κεντρικών νομικών πλαισίων. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης θέτει αυστηρούς κανόνες, θεωρώντας τα δεδομένα υγείας ειδικές κατηγορίες που απαιτούν ρητή συγκατάθεση για την επεξεργασία τους. Αντίστοιχα, στις ΗΠΑ, ο HIPAA αποτελεί τον ομοσπονδιακό νόμο για την προστασία των πληροφοριών υγείας (PHI). Η πρακτική συμμόρφωση με τα νομοθετικά πλαίσια επιτυγχάνεται μέσω της υιοθέτησης διεθνών προτύπων, όπως το ISO 27001, το οποίο διασφαλίζει ένα ολιστικό σύστημα διαχείρισης της ασφάλειας των πληροφοριών. Το πλαίσιο αυτό εξειδικεύεται περαιτέρω από το ISO 27799, το οποίο προσαρμόζει τους ελέγχους ασφάλειας στις ιδιαίτερες απαιτήσεις των δεδομένων υγείας, ενώ το NIST SP 800-53 παρέχει ένα αυστηρό πλαίσιο τεχνικών ελέγχων για τη μεγιστοποίηση της ανθεκτικότητας των πληροφοριακών υποδομών του IoMT. Συνολικά, η συνέργεια αυτών των προτύπων και κανονισμών κρίνεται απαραίτητη για τη δημιουργία ενός ασφαλούς και αξιόπιστου ψηφιακού οικοσυστήματος υγείας.

Η διασφάλιση της κλινικής χρησιμότητας των δεδομένων επιτυγχάνεται μέσω της σημασιολογικής τυποποίησης που καθορίζεται από τη σειρά προτύπων IEEE 11073, το οποίο ορίζει το γενικό πλαίσιο επικοινωνίας. Τα εξειδικευμένα πρότυπα όπως τα IEEE 11073-10404, -10406, -10407 και -10417 διασφαλίζουν ότι τα δεδομένα που λαμβάνονται από οποιαδήποτε συμβατή συσκευή είναι ομοιογενή και μπορούν να ενσωματωθούν απρόσκοπτα στα ηλεκτρονικά αρχεία υγείας.

Ο σχεδιασμός πρωτοκόλλων για ιατρικές φορετές συσκευές αποτελεί ένα σύνθετο πρόβλημα βελτιστοποίησης. Η βασική αρχιτεκτονική του IEEE 802.15.6 με τον κεντρικό συντονιστή και τα τρωτά σημεία στα πρωτόκολλα αυθεντικοποίησης καθιστούν επιτακτική την υιοθέτηση υβριδικών σχημάτων και τεχνικών όπως η κρυπτογράφηση Signcryption ή η χρήση βιομετρικών στοιχείων για την επίτευξη πλήρους ασφάλειας, αξιοπιστίας και λειτουργικής διάρκειας. Εξάλλου, η ασφάλεια

θεωρείται η πρωταρχική πρόκληση στο WBAN, απαιτώντας ισχυρούς κρυπτογραφικούς μηχανισμούς για την προστασία της εμπιστευτικότητας, ακεραιότητας και της διαθεσιμότητας.

Κεφάλαιο 5ο: Πρωτόκολλα Επικοινωνίας Φορετών Ιατρικών Συσκευών

5.1 Εισαγωγή

Οι φορετές ιατρικές συσκευές αποτελούν πλέον ένα βασικό εργαλείο στη σύγχρονη υγειονομική περίθαλψη, καθώς επιτρέπουν τη συνεχή παρακολούθηση βιοσημάτων, την έγκαιρη διάγνωση παθήσεων και τη βελτίωση της ποιότητας ζωής των ασθενών. Η δυνατότητα τους να συνδέονται ασύρματα με απομακρυσμένους διακομιστές και να μεταδίδουν σε πραγματικό χρόνο κρίσιμα δεδομένα υγείας τις καθιστά ιδιαίτερα σημαντικές για την ανάπτυξη εξατομικευμένων ιατρικών υπηρεσιών.

Ωστόσο, η ασύρματη επικοινωνία, τις καθιστά ευάλωτες σε κακόβουλες επιθέσεις, όπως υποκλοπές, αλλοίωση δεδομένων και μη εξουσιοδοτημένη πρόσβαση. Τα ζητήματα αυτά θέτουν σε κίνδυνο τόσο την ασφάλεια των ασθενών όσο και την προστασία της ιδιωτικότητάς τους. Για τον λόγο αυτό, η ανάπτυξη αξιόπιστων και αποδοτικών πρωτοκόλλων ασφάλειας είναι απαραίτητη, προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η διαθεσιμότητα και η ακεραιότητα στις επικοινωνίες.

Το βασικό εμπόδιο σε αυτήν την κατεύθυνση είναι οι περιορισμένοι υπολογιστικοί πόροι των φορετών συσκευών, οι οποίοι δεν επιτρέπουν την απευθείας εφαρμογή πολύπλοκων αλγορίθμων ασφάλειας, όπως συμβαίνει σε ισχυρότερα συστήματα. Επομένως, απαιτούνται lightweight αλλά ισχυρά πρωτόκολλα που να είναι συμβατά με τις δυνατότητες των μικροελεγκτών και ταυτόχρονα να προσφέρουν υψηλό επίπεδο προστασίας έναντι ποικίλων απειλών.

Το παρόν κεφάλαιο έχει ως στόχο να διερευνήσει και να αναλύσει τα βασικά πρωτόκολλα επικοινωνίας που υιοθετούνται στις ιατρικές φορετές συσκευές. Θα δοθεί έμφαση στα πρωτόκολλα Bluetooth Low Energy και ZigBee, στις τεχνολογίες που χρησιμοποιούνται τόσο για την επικοινωνία σε κοντινή απόσταση, όσο και για τη μεταφορά δεδομένων σε μεγάλες αποστάσεις προς τα συστήματα αποθήκευσης και ανάλυσης, καθώς και στις προκλήσεις ασφάλειας που προκύπτουν κατά την εφαρμογή τους.

5.2 Πρωτόκολλα επικοινωνίας IoMT

Η χρησιμότητα των πρωτοκόλλων επικοινωνίας στο χώρο των ιατρικών φορετών συσκευών δεν έγκειται απλώς στη μεταφορά δεδομένων, αλλά στην εγγύηση της ασφαλούς και αποδοτικής λειτουργίας συστημάτων που συχνά είναι ζωτικής σημασίας. Ένα πρωτόκολλο επικοινωνίας ορίζεται ως το σύνολο των κανόνων και των προτύπων που καθορίζουν τον τρόπο με τον οποίο οι συσκευές μεταδίδουν δεδομένα [69]. Στον χώρο της ιατρικής, τα πρωτόκολλα αυτά πρέπει να ικανοποιούν ένα ιδιαίτερα αυστηρό σύνολο απαιτήσεων που υπερβαίνουν την απλή μεταφορά δεδομένων.

Λόγω των περιορισμών στην κατανάλωση ενέργειας, οι φορετές ιατρικές συσκευές διαθέτουν μειωμένη υπολογιστική ικανότητα. Τα πρωτόκολλα πρέπει να είναι ενεργειακά αποδοτικά για να παρατείνουν τη διάρκεια ζωής της συσκευής, δεδομένου ότι η τροφοδοσία τους με μπαταρία είναι περιορισμένη. Απαιτείται η χρήση υπολογιστικά χαμηλών σε κατανάλωση ενέργειας πρωτοκόλλων, καθώς σε αντίθετη περίπτωση δεν είναι κατάλληλοι για συσκευές χαμηλής ισχύος [69]. Τα ενεργειακά αποδοτικά πρωτόκολλα επιτρέπουν την αύξηση της διάρκειας ζωής από ώρες σε μήνες, εξασφαλίζοντας ότι η συσκευή μπορεί να λειτουργεί συνεχώς στο σώμα χωρίς συχνή παρέμβαση [6].

Η ασύρματη σύνδεση μεταξύ φορετών συσκευών και απομακρυσμένων διακομιστών είναι εξαιρετικά ευάλωτη σε κακόβουλες επιθέσεις. Τα πρωτόκολλα πρέπει να παρέχουν αξιόπιστα μέτρα για την ασφάλεια της ασύρματης επικοινωνίας. Για τον έλεγχο ταυτότητας, τα πρωτόκολλα παρέχουν αμφίδρομη ταυτοποίηση μεταξύ της φορετής συσκευής και του διακομιστή [69]. Ο έλεγχος ταυτότητας συσκευής αποτρέπει τη διαρροή πληροφοριών του ασθενούς σε μη εξουσιοδοτημένα πρόσωπα. Παρέχεται επίσης, κρυπτογράφηση δεδομένων για τη διασφάλιση της ιδιωτικής επικοινωνίας μεταξύ της συσκευής και του διακομιστή. Η κρυπτογράφηση προστατεύει το απόρρητο του ασθενούς από διάφορες απειλές δικτύου.

Τα πρωτόκολλα επικοινωνίας είναι ο ακρογωνιαίος λίθος που καθιστά δυνατή τη μετάβαση από την απλή παρακολούθηση στη συνεχή, ασφαλή και θεραπευτικά αποτελεσματική διαχείριση της υγείας.

5.3 Bluetooth Low Energy (BLE)

Η τεχνολογία Bluetooth αποτελεί μία από τις πλέον διαδεδομένες λύσεις ασύρματης επικοινωνίας, καθώς βασίζεται στο πρότυπο IEEE 802.15.1 και είναι κατάλληλη για συσκευές χαμηλού κόστους και περιορισμένης ενεργειακής κατανάλωσης [70], λειτουργώντας στη ζώνη των 2.4 GHz [10]. Η εκδοχή Bluetooth Low Energy (BLE) έχει εξελιχθεί σε βασικό πρωτόκολλο για φορετές και μικρο-ιατρικές συσκευές, καθώς συνδυάζει μικρού μεγέθους ολοκληρωμένα κυκλώματα με μπαταρίες περιορισμένης χωρητικότητας, επιτρέποντας λειτουργίες όπως ενεργοποίηση γεγονότων, αποθήκευση και μετάδοση δεδομένων προς έξυπνες συσκευές, όπως smartphones [71].

Το Bluetooth υποστηρίζει Personal Area Networks (PANs) σε τοπολογία αστέρα, με χαμηλή κατανάλωση ενέργειας, ελάχιστο χρόνο αρχικοποίησης και δυνατότητα υποστήριξης μεγάλου αριθμού κόμβων [10]. Για την επικοινωνία μεταξύ αισθητήρων και ενεργοποιητών απαιτείται και οι δύο πλευρές να διαθέτουν ενσωματωμένα κυκλώματα με κεραία [6]. Το εύρος λειτουργίας εξαρτάται από την έκδοση, ενδεικτικά, η έκδοση 2.1 φτάνει έως τα 100 μέτρα, ενώ η έκδοση 5 (BLE) μπορεί να επεκταθεί έως τα 400 μέτρα [10].

Η έκδοση BLE 5.0 προσφέρει θεωρητικό ρυθμό μετάδοσης έως 2 Mbps, με πραγματικές επιδόσεις που συνήθως κυμαίνονται κάτω από 1 Mbps, εξαιτίας παραμέτρων όπως το επιπλέον φορτίο του πρωτοκόλλου, οι ηλεκτρομαγνητικές παρεμβολές και τα χαρακτηριστικά κάθε chipset. Παρά τον περιορισμό αυτό, ο μικρός χρόνος σύζευξης, μόλις λίγα ms και η χαμηλή καθυστέρηση καθιστούν το BLE ιδανικό για εφαρμογές πραγματικού χρόνου σε ιατρικούς αισθητήρες και φορετές συσκευές [6], [10].

Σε σύγκριση με άλλα πρωτόκολλα χαμηλής ισχύος, όπως ZigBee και Z-Wave, το BLE προσφέρει ανώτερο ρυθμό μετάδοσης, ενώ η χρήση τεχνικών όπως το frequency hopping επιτρέπει την παράλληλη λειτουργία με άλλα ασύρματα δίκτυα. Ωστόσο, παρουσιάζει υψηλότερη κατανάλωση σε σχέση με το NFC και απαιτεί διαδικασία σύζευξης συσκευών [72]. Πέρα από ζητήματα ενεργειακής κατανάλωσης, οι υπάρχουσες BLE μονάδες παρουσιάζουν περιορισμούς βιοσυμβατότητας. Επιπλέον, η μακροχρόνια τροφοδοσία από μήνες μέχρι έτη, παραμένει τεχνικά δύσκολη και κοστοβόρα, παρά τις εξελίξεις σε system-on-chip λύσεις [6].

Συνολικά, το BLE είναι ιδιαίτερα αποδοτικό σε δίκτυα IoT με συσκευές χαμηλού κόστους που τροφοδοτούνται με μπαταρία, επιτρέποντας γρήγορη ένταξη στο δίκτυο και δημιουργία απλών συνδέσμων συσκευής προς συσκευή ή τοπολογιών αστέρα. Λόγω των περιορισμών μεγέθους, κατανάλωσης και βιοσυμβατότητας, η κλινική του χρήση επικεντρώνεται κυρίως σε επιφανειακές φορετές συσκευές, όπου αποδεικνύεται ιδιαίτερα αποτελεσματικό για τη συνεχή παρακολούθηση

βιοσημάτων και άλλων κλινικών παραμέτρων μέσω εξωτερικών συσκευών, όπως smartphones ή προσωπικοί υπολογιστές [6], [4].

5.3.1 Προκλήσεις Ασφάλειας BLE

Το BLE, εισήγαγε προηγμένες δικλείδες ασφαλείας, προσφέροντας πλέον τέσσερα διαφορετικά επίπεδα λειτουργίας (security modes). Στις σύγχρονες ιατρικές εφαρμογές, προτείνεται η χρήση της Κατάστασης 4 (Mode 4), η οποία θεωρείται η πλέον ισχυρή [10]. Το κύριο χαρακτηριστικό της είναι η εφαρμογή του μηχανισμού Secure Simple Pairing (SSP) [10]. Η αυθεντικοποίηση της συσκευής ολοκληρώνεται υποχρεωτικά πριν από την οριστική αποκατάσταση της σύνδεσης, διασφαλίζοντας ότι μόνο εξουσιοδοτημένες συσκευές ανταλλάσσουν δεδομένα. Για τη θωράκιση της επικοινωνίας, το Mode 4 χρησιμοποιεί κρυπτογράφηση ροής (stream cipher encryption) [10], [73]. Η μέθοδος αυτή είναι ιδιαίτερα αποτελεσματική για την αποτροπή επιθέσεων τύπου MitM, όπου ένας μη εξουσιοδοτημένος χρήστης προσπαθεί να παρεμβληθεί και να υποκλέψει ή να αλλοιώσει τις μετρήσεις του ασθενούς.

Ο αλγόριθμος κρυπτογράφησης λειτουργεί με τη χρήση συμμετρικών κλειδιών, τα οποία παράγονται δυναμικά συνδυάζοντας τρία κρίσιμα μεταδεδομένα [10]:

- Τη μοναδική διεύθυνση (address) της κύριας συσκευής.
- Τον χρόνο ρολογιού (clock time) της συσκευής.
- Ένα εξειδικευμένο κρυπτογραφικό κλειδί.

Πέρα από το λογισμικό, η ασφάλεια ενισχύεται και σε επίπεδο υλικού. Σε κάθε Bluetooth chip που είναι ενσωματωμένο σε μια ιατρική συσκευή ανατίθενται μοναδικά αναγνωριστικά [10]. Αυτό επιτρέπει στο σύστημα να αναγνωρίζει με απόλυτη ακρίβεια τη συγκεκριμένη συσκευή του ασθενούς, αποκλείοντας την περίπτωση σύνδεσης με παραποιημένο (cloned) ή μη εξουσιοδοτημένο εξοπλισμό.

Η υιοθέτηση του Mode 4 και του μηχανισμού SSP καθιστά το BLE ένα αξιόπιστο πρωτόκολλο για τη μεταφορά ευαίσθητων ιατρικών πληροφοριών, καθώς εξισορροπεί την ανάγκη για χαμηλή κατανάλωση ενέργειας με υψηλά επίπεδα κρυπτογράφησης και αυθεντικοποίησης.

Παρά τους μηχανισμούς προστασίας, η εφαρμογή του BLE στις ιατρικές συσκευές παρουσιάζει σημαντικές προκλήσεις ασφάλειας που πηγάζουν τόσο από τη φύση του πρωτοκόλλου όσο και από τον τρόπο υλοποίησής του.

Μια βασική αδυναμία του BLE είναι ότι η κρυπτογράφηση περιορίζεται εξ ορισμού στο payload και δεν καλύπτει ολόκληρο το πακέτο δεδομένων [10]. Πολλές ιατρικές συσκευές χρησιμοποιούν παρόμοιους τύπους διεπαφής και συγκεκριμένα κανάλια για υπηρεσίες όπως η επαλήθευση μοντέλου, γεγονός που επιτρέπει σε επιτιθέμενους να αναγνωρίσουν ευάλωτα σημεία εισόδου.

Οι επιτιθέμενοι μπορούν να συγχρονιστούν με τις εναλλαγές συχνοτήτων (frequency hops) της σύνδεσης Bluetooth, επιτρέποντάς τους να υποκλέπτουν πακέτα δεδομένων. Η λειτουργία Just Works έχει αποδειχθεί ευάλωτη σε επιθέσεις MitM, οι οποίες αναγκάζουν τους νόμιμους χρήστες να κάνουν επανεκκίνηση των συζεύξεων [10].

Επιθέσεις που στοχεύουν το πρωτόκολλο Bluetooth είναι [73]:

- Man-in-the-Middle (MitM): Ο επιτιθέμενος τοποθετείται ανάμεσα σε δύο συσκευές, ελέγχοντας και παραποιώντας τη ροή των πληροφοριών. Στις ιατρικές συσκευές, αυτό θα μπορούσε να σημαίνει την αλλαγή μιας κρίσιμης μέτρησης ή εντολής.

- Eavesdropping (Υποκλοπή): Κατά τη διάρκεια της σύζευξης, εάν χρησιμοποιούνται παλαιότερες εκδόσεις του πρωτοκόλλου, ένας εισβολέας μπορεί να υποκλέψει το Temporary Key και στη συνέχεια να αποκρυπτογραφήσει όλη την επικοινωνία.
- Denial of Service (DoS): Επιθέσεις που στοχεύουν στην εξάντληση της μπαταρίας ή στη διακοπή της σύνδεσης, καθιστώντας την ιατρική συσκευή μη λειτουργική.

Έχουν καταγραφεί μέθοδοι για την παραβίαση των PINs μέσω brute-force κατά τη διαδικασία σύζευξης, καθώς και η αποστολή ανεπιθύμητων μηνυμάτων [73]. Αξίζει να σημειωθεί ότι οι πιο αποτελεσματικές επιθέσεις συνήθως εκμεταλλεύονται κενά σε συγκεκριμένες υλοποιήσεις συσκευών και όχι απαραίτητα εγγενείς αδυναμίες του ίδιου του πρωτοκόλλου Bluetooth.

Για την πλήρη προστασία των συσκευών, προτείνονται οι εξής πρακτικές και τεχνικές λύσεις [10], [73]:

- Συντήρηση και ενημέρωση συσκευών: Είναι κρίσιμο να διατηρείται το λογισμικό και οι ρυθμίσεις των συσκευών στην τελευταία διαθέσιμη έκδοση. Παράλληλα, η συχνή αλλαγή των κωδικών και των διαπιστευτηρίων εισόδου ενισχύει την άμυνα έναντι μη εξουσιοδοτημένης πρόσβασης.
- Έλεγχος ασύρματης ορατότητας: Το Bluetooth θα πρέπει να ενεργοποιείται αποκλειστικά κατά τη διάρκεια της χρήσης, ενώ η συσκευή επιβάλλεται να παραμένει σε κατάσταση «μη ανιχνεύσιμη» (undiscoverable mode) για την αποφυγή εντοπισμού από τρίτους.
- Αυστηρά πρωτόκολλα σύνδεσης: Η σύζευξη πρέπει να περιορίζεται αυστηρά σε πιστοποιημένες και έμπιστες συσκευές, καταργώντας κάθε λειτουργία αυτόματης σύνδεσης που θα μπορούσε να εκθέσει τα δεδομένα του ασθενούς.
- Προηγμένη διαχείριση κλειδιών: Για την αποτελεσματική εξουδετέρωση επιθέσεων MitM, προτείνεται η χρήση combination keys έναντι των απλών κλειδιών.
- Κρυπτογράφηση σύνδεσης: Η εφαρμογή κρυπτογράφησης στον δίαυλο επικοινωνίας (link encryption) είναι απαραίτητη για την αποτροπή υποκλοπών (eavesdropping).

5.4 ZigBee

Στα WBANs η κατανάλωση ενέργειας είναι ιδιαίτερα κρίσιμη, καθώς οι αισθητήρες που χρησιμοποιούνται βασίζονται σε μπαταρίες οι οποίες πρέπει να λειτουργούν για μεγάλο χρονικό διάστημα χωρίς συχνές αντικαταστάσεις [74]. Το ζήτημα αυτό είναι ιδιαίτερα κρίσιμο για τους εμφυτεύσιμους και φορετούς αισθητήρες, καθώς η αλλαγή της μπαταρίας, ακόμα και για μικρές συσκευές, δεν είναι πάντα εφικτή ή πρακτική [10]. Για τον λόγο αυτό, η σχεδίαση πρωτοκόλλων MAC με στόχο την εξοικονόμηση ενέργειας στις φορετές ιατρικές συσκευές έχει αποτελέσει βασικό πεδίο έρευνας τα τελευταία χρόνια [14].

Η χρήση του προτύπου IEEE 802.15.4/ZigBee στα WBANs αποτελεί μια από τις πιο οικονομικές και ενεργειακά αποδοτικές επιλογές [10], [13], [14]. Το ZigBee είναι ένα ασύρματο πρωτόκολλο επικοινωνίας που στηρίζεται στο πρότυπο IEEE 802.15.4 και έχει σχεδιαστεί με έμφαση στη χαμηλή κατανάλωση ενέργειας, το μικρό κόστος και τις μέτριες ταχύτητες μετάδοσης δεδομένων [13]. Το εύρος λειτουργίας του μπορεί να φτάσει έως τα 100 μέτρα, ενώ οι ρυθμοί μετάδοσης κυμαίνονται από 40 Kbps έως 250 Kbps, χαρακτηριστικά που το καθιστούν ιδιαίτερα αποδοτικό για εφαρμογές όπου δεν απαιτούνται υψηλές ταχύτητες αλλά είναι κρίσιμη η εξοικονόμηση ενέργειας [10]. Το ZigBee προορίζεται κυρίως για δίκτυα προσωπικής επικοινωνίας (PANs) και λειτουργεί στις συχνότητες 868 MHz, 915 MHz και 2.4 GHz [10]. Επιπλέον, είναι ιδιαίτερα ευέλικτο καθώς υποστηρίζει διαφορετικές

τοπολογίες δικτύου, προσφέροντας τη δυνατότητα ανάπτυξης τόσο απλών όσο και πολύπλοκων δικτυακών δομών [13].

Στα βασικά στοιχεία ενός ZigBee δικτύου περιλαμβάνονται οι τερματικές συσκευές, οι δρομολογητές και ο συντονιστής [75]. Ο συντονιστής είναι η κύρια συσκευή πλήρους λειτουργίας, υπεύθυνος για τη δημιουργία, διαχείριση και συντονισμό του δικτύου [75]. Οι δρομολογητές επεκτείνουν την εμβέλεια του δικτύου μέσω λειτουργίας δρομολόγησης, αλλά δεν μπορούν να δημιουργήσουν δίκτυο από μόνοι τους [75]. Οι τερματικές συσκευές έχουν περιορισμένες δυνατότητες και κύριος ρόλος τους αποτελεί η ανίχνευση και μετάδοση δεδομένων, αξιοποιώντας τον δρομολογητή και τον συντονιστή για τη μεταφορά πληροφοριών [75].

Η ευελιξία του ZigBee έχει οδηγήσει στη χρήση του σε ένα ευρύ φάσμα εφαρμογών που σχετίζονται με το IoT. Στον τομέα της υγείας στις φορετές συσκευές, αξιοποιείται εκτεταμένα για την ασύρματη διασύνδεση αισθητήρων με τον συντονιστή του δικτύου, επιτρέποντας τη συλλογή κρίσιμων βιολογικών δεδομένων από τους ασθενείς [10]. Παράλληλα, δίνει τη δυνατότητα επικοινωνίας και συνεργασίας μεταξύ διαφορετικών συντονιστών, διευκολύνοντας την ανάπτυξη πιο σύνθετων συστημάτων παρακολούθησης και υγειονομικής φροντίδας [13].

Το 2009, η ZigBee Alliance παρουσίασε το ZigBee Health Care application profile, ένα προφίλ εφαρμογής ειδικά σχεδιασμένο για φορετές και βοηθητικές συσκευές μη επεμβατικής ιατρικής παρακολούθησης [10]. Η πρωτοβουλία αυτή είχε ως στόχο να καθιερώσει ένα κοινό, βιομηχανικό πρότυπο για την αξιόπιστη ανταλλαγή δεδομένων μεταξύ διαφορετικών συσκευών, τόσο ιατρικών όσο και μη ιατρικών, διασφαλίζοντας τη διαλειτουργικότητα και τη συμβατότητα σε ετερογενή περιβάλλοντα υγείας [10]. Το το συγκεκριμένο προφίλ στηρίζεται στο ZigBee Pro και εισάγει ένα πλήρες και λειτουργικό πρωτόκολλο στο επίπεδο εφαρμογής, το οποίο ανταποκρίνεται στις ιδιαίτερες απαιτήσεις των συστημάτων παρακολούθησης και υγειονομικής περίθαλψης [10]. Επιπλέον, υποστηρίζει το διεθνές πρότυπο IEEE 11073, που χρησιμοποιείται για την τυποποιημένη επικοινωνία και τη διαχείριση ιατρικών συσκευών, καθιστώντας το ιδανικό για εφαρμογές που απαιτούν ασφαλή και αξιόπιστη μετάδοση δεδομένων υγείας, όπως τα συστήματα φορετών συσκευών για ασθενείς και οι πλατφόρμες τηλεϊατρικής [10].

Η διαχείριση της ενέργειας παραμένει το σημαντικότερο ζήτημα στα WBANs, με αρκετές μελέτες να εστιάζουν στις διαφορετικές του πτυχές [14]. Σε ένα σύστημα παρακολούθησης υγείας, οι επικοινωνίες χωρίζονται σε δύο βασικές κατηγορίες: (i) ανταλλαγή δεδομένων μεταξύ των αισθητήρων και των ιατρικών σταθμών βάσης και (ii) αποστολή δεδομένων προς τους εξυπηρετητές ιατρικού ελέγχου [76]. Η συνεχής ροή δεδομένων καταναλώνει σημαντική ενέργεια, περιορίζοντας τη διάρκεια ζωής των αισθητήρων [14]. Δεδομένου ότι οι αισθητήρες είναι μικροί, με ελαφρύ προφίλ και εξαρτώνται από μπαταρίες περιορισμένης χωρητικότητας, η δημιουργία ενός αποδοτικού και μακροχρόνιου συστήματος παρακολούθησης πολλαπλών ασθενών απαιτεί βελτιστοποιημένα WBANs [14]. Συνήθως, τέτοια δίκτυα έχουν απλή τοπολογία λόγω περιορισμών, αλλά χρησιμοποιούν εξελιγμένα πρωτόκολλα και αλγορίθμους για αποτελεσματική οργάνωση σημάτων και για να ανταποκριθούν στις υψηλές απαιτήσεις ποιότητας υπηρεσιών [14]. Σε αυτό το πλαίσιο, ο έλεγχος ισχύος εκπομπής (TPC) [14], προσφέρει έναν πρακτικό και αποδοτικό τρόπο εξοικονόμησης ενέργειας χωρίς να μειώνεται η αξιοπιστία της επικοινωνίας.

Η εμβέλεια μετάδοσης του ZigBee φτάνει μερικές εκατοντάδες μέτρα, ωστόσο η κατανάλωση ενέργειας είναι υψηλότερη σε σχέση με το Bluetooth Low Energy (BLE) [77]. Αυτό καθιστά το ZigBee κατάλληλο για εφαρμογές όπου οι συσκευές πρέπει να λειτουργούν πολλά χρόνια με χαμηλή συντήρηση, ενώ η συνολική ιεράρχηση κατανάλωσης ενέργειας είναι: ANT > ZigBee > BLE, δηλαδή

το ZigBee καταναλώνει λιγότερη ενέργεια από το ANT αλλά περισσότερη από το BLE [77]. Το BLE, αν και πιο αποδοτικό ενεργειακά, παρουσιάζει περιορισμούς λόγω πολύ χαμηλού ρυθμού μετάδοσης και πιθανών παρεμβολών στις ζώνες 868 MHz, 915 MHz και 2.4 GHz, γεγονός που το καθιστά λιγότερο κατάλληλο για μεγάλης κλίμακας, πραγματικού χρόνου WBAN εφαρμογές [77].

Από την άλλη, το ZigBee αντιμετωπίζει προβλήματα σε κρίσιμες ιατρικές εφαρμογές, λόγω υψηλής πιθανότητας εξασθένισης καναλιού και καθυστερήσεων στη μετάδοση δεδομένων, γεγονός ιδιαίτερα κρίσιμο για άμεση και αξιόπιστη ανταπόκριση σε δεδομένα υγείας [77]. Για τον λόγο αυτό, δεν θεωρείται κατάλληλο για επείγουσες ή κρίσιμες WBAN εφαρμογές, όπου η αμεσότητα στη μεταφορά των δεδομένων είναι ζωτικής σημασίας.

5.4.1 Προκλήσεις Ασφάλειας ZigBee

Η ασφάλεια των δικτύων ZigBee βασίζεται στον AES (Advanced Encryption Standard) 128-bit, με τρία διαφορετικά είδη κλειδιών: το master key, προρυθμισμένο πριν από την ανάπτυξη, το link key, μοναδικό για κάθε ζεύγος κόμβων και το network key, που παράγεται από το trust center [13]. Παρά την ασφάλεια που προσφέρει ο AES, το ZigBee παραμένει ευάλωτο σε επιθέσεις όπως γρήγορη κατανάλωση ενέργειας, DoS attacks, replay attacks και sniffing [13]. Επιπλέον, η χρήση του AES είναι απαιτητική σε επίπεδο υπολογιστικής ισχύος και ενέργειας, κάτι που μπορεί να αποτελέσει πρόβλημα για αισθητήρες με περιορισμένους πόρους [13].

Πολλές από τις καταγεγραμμένες ευπάθειες δεν αφορούν το σχεδιασμό του ZigBee, αλλά τον τρόπο με τον οποίο οι εταιρείες παραμετροποιούν τις συσκευές τους. Συγκεκριμένα [10]:

- Διαχείριση κρυπτογραφικών κλειδιών: Παρατηρείται συχνά η χρήση ανασφαλών μεθόδων μεταφοράς για τα preshared keys.
- Πρακτικές κατασκευαστών: Πολλοί προμηθευτές εγκαθιστούν κοινά, προκαθορισμένα (default) κλειδιά σύνδεσης σε όλες τις συσκευές τους.
- Επαναχρησιμοποίηση δεδομένων: Η επαναχρησιμοποίηση των Initialization Vectors (IVs) κατά την κρυπτογράφηση αποτελεί συχνό λάθος που υπονομεύει την ασφάλεια.

Το ZigBee κληρονομεί αρκετά τρωτά σημεία από το πρότυπο 802.15.4 στο οποίο βασίζεται [10]:

- Πλαστογράφηση επιβεβαιώσεων (ACKs): Τα πακέτα επιβεβαίωσης στερούνται ελέγχων ακεραιότητας, βασιζόμενα μόνο σε αριθμούς ακολουθίας που υποκλέπτονται εύκολα. Αυτό επιτρέπει σε εισβολείς να πλαστογραφούν ACKs στο επίπεδο MAC, προκαλώντας αποσύνδεση νόμιμων συσκευών από τις υπηρεσίες τους.
- Παραβίαση κλειδιών: Κατά την ενημέρωση των κλειδιών δικτύου, τα νέα κλειδιά κρυπτογραφούνται με τα προϋπάρχοντα πριν μεταδοθούν. Αυτή η πρακτική δεν διασφαλίζει την αυτονομία και ανεξαρτησία των κρυπτογραφικών κλειδιών.
- Εκμετάλλευση PAN IDs: Η απουσία επαλήθευσης των ταυτοτήτων δικτύου (PAN IDs) επιτρέπει σε επιτιθέμενους να επαναφέρουν τις συνδέσεις στις εργοστασιακές ρυθμίσεις και μέσω παραποιημένων μηνυμάτων Beacon, να κατευθύνουν τις συσκευές σε κακόβουλα δίκτυα.

Λαμβάνοντας υπόψη την ιδιαίτερη φύση των φορετών συσκευών, η διασφάλιση της διαθεσιμότητας των υπηρεσιών και η διατήρηση της διάρκειας ζωής της μπαταρίας αναδεικνύονται σε παράγοντες ζωτικής σημασίας για την ασφάλεια του ασθενούς. Στο πλαίσιο αυτό, το επίπεδο MAC του πρωτοκόλλου ZigBee παρουσιάζει ευπάθεια σε επιθέσεις τύπου flooding, οι οποίες έχουν ως στόχο να κατακλύσουν το δίκτυο με περιττή κίνηση, προκαλώντας έτσι άρνηση υπηρεσίας (DoS) και πλήρη

διακοπή της λειτουργίας του συστήματος [10]. Παράλληλα, οι φορητές ιατρικές συσκευές απειλούνται από επιθέσεις εξάντλησης πόρων, όπου οι εισβολείς στοχεύουν σκόπιμα σε ενεργοβόρες λειτουργίες με απώτερο σκοπό την ταχεία εξάντληση της μπαταρίας, γεγονός που μπορεί να θέσει σε άμεσο κίνδυνο την αδιάλειπτη παρακολούθηση της υγείας του χρήστη [13].

Το ZigBee επιτρέπει την επαναχρησιμοποίηση κλειδιών μεταξύ διαφορετικών επιπέδων της ίδιας συσκευής και εφαρμόζει το ίδιο επίπεδο ασφάλειας για όλα τα σημεία του δικτύου [10], [13]. Αυτή η ομοιομορφία, αν και απλοποιεί τη διαχείριση, μπορεί να διευκολύνει την κλιμάκωση μιας επίθεσης αν παραβιαστεί ένα μόνο σημείο.

5.5 Επίλογος

Το παρόν κεφάλαιο ανέλυσε το πλαίσιο των πρωτοκόλλων επικοινωνίας που διέπουν τη λειτουργία των ιατρικών φορετών συσκευών. Όπως κατέδειξε η έρευνα, η επιλογή του πρωτοκόλλου είναι μια πολυπαραμετρική απόφαση που εξισορροπεί τις απαιτήσεις της ενεργειακής αποδοτικότητας, της ασφάλειας και της διαλειτουργικότητας των δεδομένων, καθώς οι συσκευές αυτές λειτουργούν σε ένα περιβάλλον περιορισμένων πόρων.

Η ανάγκη για συνεχή, αξιόπιστη ροή δεδομένων από το Wireless Body Area Network (WBAN) προς τα κεντρικά συστήματα οδήγησε στην υιοθέτηση διαφοροποιημένων λύσεων, ανάλογα με την εμβέλεια και την κατανάλωση. Η ενσωμάτωση των πρωτοκόλλων BLE και ZigBee στις φορετές ιατρικές συσκευές αποτελεί μια τεχνολογική πρόκληση όπου η ενεργειακή αυτονομία συναντά την επιτακτική ανάγκη για απόλυτη ασφάλεια δεδομένων. Καθώς οι συσκευές αυτές μεταφέρουν ζωτικής σημασίας πληροφορίες η επιλογή του πρωτοκόλλου επικοινωνίας δεν είναι απλώς ζήτημα συνδεσιμότητας, αλλά μια απόφαση που επηρεάζει άμεσα την ιδιωτικότητα και τη σωματική ακεραιότητα του ασθενούς.

Το πρωτόκολλο BLE εδραιώνεται ως μια ιδανική επιλογή για την προσωπική παρακολούθηση της υγείας μέσω φορετών συσκευών, καθώς καταφέρνει να συνδυάσει την υψηλή ενεργειακή αυτονομία με εξελιγμένους μηχανισμούς κρυπτογράφησης και αυθεντικοποίησης, διασφαλίζοντας την εμπιστευτικότητα των δεδομένων του ασθενούς στο επίπεδο του σωματικού δικτύου. Όμως, παρά την ισχυρή κρυπτογράφηση, το BLE παραμένει εκτεθειμένο σε επιθέσεις Man-in-the-Middle και υποκλοπές κατά τη διαδικασία της απλής σύζευξης, καθιστώντας απαραίτητη την αυστηρή διαχείριση της ορατότητας και των δικαιωμάτων πρόσβασης των ιατρικών αισθητήρων.

Το ZigBee παραμένει ο πυλώνας επικοινωνίας των δικτύων πλέγματος (mesh), προσφέροντας μια ισχυρή αρχιτεκτονική βασισμένη στο πρότυπο IEEE 802.15.4 που επιτρέπει τη διασύνδεση πολλαπλών ιατρικών αισθητήρων με κεντρικό έλεγχο, παρά τις προκλήσεις που αντιμετωπίζει στη διαχείριση της ενεργειακής κατανάλωσης και στην αποφυγή επιθέσεων άρνησης υπηρεσίας. Παρόλο που το ZigBee χρησιμοποιεί ισχυρή κρυπτογράφηση, παρουσιάζει κενά ασφάλειας στα κλειδιά κρυπτογράφησης. Επιπλέον, είναι ευάλωτο σε επιθέσεις που υπερφορτώνουν το δίκτυο, προκαλώντας διακοπή στη λειτουργία της συσκευής, γεγονός που μπορεί να αποβεί επικίνδυνο για την παρακολούθηση του ασθενούς.

Στο σύστημα του IoMT, η ασφάλεια των πρωτοκόλλων αυτών πρέπει να προσεγγίζεται μέσω της αρχής Security by Design. Αυτό σημαίνει ότι η κρυπτογράφηση σε επίπεδο ζεύξης (Link Layer) δεν επαρκεί. Απαιτείται η εφαρμογή επιπλέον επιπέδων ασφάλειας στο επίπεδο της εφαρμογής (Application Layer), καθώς και η χρήση τεχνικών για την αποφυγή παρεμβολών.

Η αξιοπιστία των BLE και ZigBee στις ιατρικές εφαρμογές κρίνεται από την ικανότητά τους να θωρακίζουν την υγεία του ασθενούς. Η ασφάλεια δεν πρέπει να αντιμετωπίζεται ως στατικό χαρακτηριστικό, αλλά ως μια δυναμική διαδικασία συνεχών ενημερώσεων και ελέγχων. Μόνο μέσα από μια ολιστική στρατηγική προστασίας, που εξαλείφει τα κενά κατά την αρχική σύζευξη και διασφαλίζει την αυθεντικότητα κάθε πακέτου δεδομένων, μπορούν οι συγκεκριμένες τεχνολογίες να θέσουν τις βάσεις για ένα αξιόπιστο ψηφιακό σύστημα υγείας με τρόπο ασφαλή, ηθικό και βιώσιμο.

Κεφάλαιο 6ο: Ανάπτυξη Συστήματος Ανίχνευσης Εισβολών (IDS) για την Αντιμετώπιση Επιθέσεων σε Περιβάλλοντα IoMT

6.1 Εισαγωγή

Η ραγδαία ενσωμάτωση των τεχνολογιών του IoMT στην υγειονομική περίθαλψη έχει επιφέρει σημαντικά οφέλη, παράλληλα όμως έχει δημιουργήσει νέα τρωτά σημεία, εκθέτοντας τα δίκτυα IoMT σε κακόβουλες ενέργειες και στοχευμένες κυβερνοεπιθέσεις. Οι φορετές ιατρικές συσκευές, λόγω των περιορισμένων υπολογιστικών τους πόρων και της φύσης των πρωτοκόλλων επικοινωνίας που χρησιμοποιούν, είναι ιδιαίτερα ευάλωτες σε επιθέσεις παρεμβολής, με κυριότερη την επίθεση MitM.

Στην παρούσα ενότητα, αναπτύσσεται μια πειραματική προσέγγιση για την ενίσχυση της ασφάλειας των συστημάτων IoMT. Μετά από αξιολόγηση των διαθέσιμων εργαλείων, επιλέχθηκε η χρήση της γλώσσας προγραμματισμού Python και τεχνικών Μηχανικής Μάθησης, καθώς προσφέρουν την απαραίτητη ευελιξία για την ανάλυση πραγματικών δεδομένων δικτύου και βιομετρικών μετρήσεων.

Ο αντικειμενικός σκοπός αυτής της προσέγγισης είναι ο σχεδιασμός ενός συστήματος ανίχνευσης εισβολών (IDS), το οποίο θα είναι σε θέση:

1. Να αναγνωρίζει πρότυπα επιθέσεων σε πραγματικό χρόνο.
2. Να λειτουργεί με υψηλή ακρίβεια, ελαχιστοποιώντας τους ψευδείς συναγερμούς.
3. Να διατηρεί χαμηλή υπολογιστική πολυπλοκότητα, καθιστώντας το συμβατό με τους περιορισμούς ενέργειας και επεξεργαστικής ισχύος των φορετών συσκευών.

Για την εκπαίδευση και αξιολόγηση του συστήματος χρησιμοποιήθηκε το εξειδικευμένο σύνολο δεδομένων WUSTL-EHMS 2020, το οποίο παρέχει έναν συνδυασμό δεδομένων δικτύου και βιομετρικών ροών, επιτρέποντας μια ολιστική θεώρηση της ασφάλειας στο συστήματος του IoMT. Στο πλαίσιο της αξιολόγησης, πραγματοποιείται μια συγκριτική ανάλυση μεταξύ του αλγορίθμου Random Forest και του μοντέλου KNN (K-Nearest Neighbors). Στόχος της διαδικασίας είναι η ανάδειξη της βέλτιστης αρχιτεκτονικής μηχανικής μάθησης, με γνώμονα την ακρίβεια εντοπισμού στις ιδιαίτερες απαιτήσεις του δικτύου IoMT.

6.2 Περιγραφή του Συνόλου Δεδομένων WUSTL-EHMS 2020

Για την υλοποίηση και την αξιολόγηση του συστήματος ανίχνευσης εισβολών, χρησιμοποιήθηκε το σύνολο δεδομένων WUSTL-EHMS 2020 (Washington University in St. Louis - Enhanced Healthcare Monitoring System) [78]. Το συγκεκριμένο dataset αποτελεί μια από τις πλέον σύγχρονες πηγές δεδομένων στον τομέα του IoMT, καθώς συνδυάζει δύο κρίσιμες ροές πληροφορίας:

1. Network traffic: Περιλαμβάνει χαρακτηριστικά ροής (flow features).
2. Βιομετρικά δεδομένα: Περιλαμβάνει πραγματικές μετρήσεις από αισθητήρες ιατρικών συσκευών.

Το dataset περιέχει συνολικά 44 χαρακτηριστικά (features) που περιγράφουν κάθε επικοινωνία μεταξύ του αισθητήρα της ιατρικής συσκευής και της πύλης (gateway). Οι εγγραφές ταξινομούνται σε δύο κύριες κατηγορίες:

- Normal (Κανονική λειτουργία): Δεδομένα που αντιστοιχούν σε ασφαλή και απρόσκοπτη μετάδοση πληροφοριών.
- Attack (Επίθεση): Δεδομένα που αφορούν επιθέσεις MitM, όπου ένας εισβολέας παρεμβάλλεται στη ροή, με στόχο την υποκλοπή ή την παραποίηση των ιατρικών μετρήσεων.

Τα χαρακτηριστικά του συνόλου δεδομένων WUSTL-EHMS 2020 μπορούν να οργανωθούν σε διακριτές κατηγορίες, επιτρέποντας στο σύστημα ανίχνευσης να αξιολογήσει την ασφάλεια του δικτύου IoMT μέσα από διαφορετικά επίπεδα πληροφορίας:

- Στοιχεία ταυτοποίησης και πρωτοκόλλου: Περιλαμβάνουν πληροφορίες για τις συσκευές και τον τρόπο σύνδεσης, όπως οι διευθύνσεις IP (SrcAddr, DstAddr), οι φυσικές διευθύνσεις (SrcMac, DstMac), οι θύρες επικοινωνίας (Sport, Dport), καθώς και ενδείξεις κατάστασης της σύνδεσης (Flgs, Dir).
- Στατιστικά στοιχεία ροής (Traffic Flow): Αναφέρονται στην ανταλλαγή δεδομένων. Περιλαμβάνουν τη διάρκεια της σύνδεσης (Dur), τον αριθμό των πακέτων (TotPkts, Packet_num), το μέγεθος των δεδομένων σε bytes (TotBytes, SrcBytes, DstBytes), καθώς και τον φόρτο και τον ρυθμό μετάδοσης (Load, Rate, SrcLoad, DstLoad).
- Χαρακτηριστικά χρονισμού: Αποτελούν τα πιο κρίσιμα στοιχεία για τον εντοπισμό επιθέσεων MitM. Περιλαμβάνουν τη διακύμανση του χρόνου άφιξης των πακέτων (SrcJitter, DstJitter), τα χρονικά μεσοδιαστήματα μεταξύ των πακέτων (SIntPkt, DIntPkt, SIntPktAct, DIntPktAct), καθώς και τις περιπτώσεις απώλειας δεδομένων (Loss, pLoss).
- Βιομετρικές μετρήσεις: Δεδομένα που σχετίζονται με την υγεία του χρήστη και περιλαμβάνουν τη θερμοκρασία (Temp), τον καρδιακό ρυθμό (Pulse_Rate, Heart_rate, Pulse), τον κορεσμό οξυγόνου (SpO2), την αρτηριακή πίεση (SYS, DIA), τον ρυθμό αναπνοής (Resp_Rate) και δείκτες ηλεκτροκαρδιογραφήματος (ST).
- Τεχνικά χαρακτηριστικά πακέτων: Καταγράφουν λεπτομέρειες για τη δομή των πακέτων, όπως τα μέγιστα και ελάχιστα μεγέθη τους (sMaxPktSz, dMaxPktSz, sMinPktSz, dMinPktSz), καθώς και τα κενά διαστήματα στη ροή (SrcGap, DstGap, Trans).

6.3 Προ-επεξεργασία και Εξισορρόπηση Δεδομένων (SMOTE)

Η υλοποίηση του συστήματος ανίχνευσης εισβολών πραγματοποιήθηκε στο περιβάλλον Google Colab, μια διαδραστική πλατφόρμα βασισμένη στο Cloud Computing που υποστηρίζει την εκτέλεση κώδικα Python. Το συγκεκριμένο περιβάλλον παρέχει την απαραίτητη υπολογιστική ισχύ και προ-εγκατεστημένες βιβλιοθήκες, εξασφαλίζοντας την ταχύτητα και την δυνατότητα επανάληψης των πειραμάτων. Όπως φαίνεται και στο Σχήμα 4 για την ολοκλήρωση της πειραματικής διαδικασίας χρησιμοποιήθηκαν οι εξής εξειδικευμένες βιβλιοθήκες:

- Pandas & NumPy: Για τη φόρτωση, τον καθαρισμό και την αριθμητική επεξεργασία του συνόλου δεδομένων.
- Scikit-learn: Για την εφαρμογή του αλγορίθμου Random Forest, το διαχωρισμό των δεδομένων σε σύνολα εκπαίδευσης και δοκιμής (Train/ Test), καθώς και για τον υπολογισμό Accuracy, Confusion Matrix, ROC AUC.
- Imbalanced-learn (SMOTE): Για την ενίσχυση της μειονοτικής κλάσης, η οποία επέτρεψε την εξισορρόπηση των κλάσεων και την αμερόληπτη εκπαίδευση του μοντέλου.
- Matplotlib & Seaborn: Για την οπτικοποίηση των αποτελεσμάτων και τη δημιουργία των γραφημάτων ανάλυσης.

- Time: Αξιολόγηση υπολογιστικής ταχύτητας και latency.

```
import pandas as pd
import numpy as np
import time
import matplotlib.pyplot as plt
import seaborn as sns
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.neighbors import KNeighborsClassifier
from sklearn.preprocessing import StandardScaler, LabelEncoder
from sklearn.metrics import (classification_report, confusion_matrix,
                             ConfusionMatrixDisplay, roc_curve, auc)
from imblearn.over_sampling import SMOTE
```

Σήμα 4: Περιβάλλον Ανάπτυξης Colab και Βιβλιοθήκες

Μέσω αυτού του υπολογιστικού πλαισίου, τα δεδομένα υποβλήθηκαν σε προ-επεξεργασία, κωδικοποίηση και εξισορρόπηση, θέτοντας τις βάσεις για την υψηλή απόδοση του ταξινομητή που ακολουθεί.

Η ποιότητα των δεδομένων εισόδου αποτελεί καθοριστικό παράγοντα για την αξιοπιστία ενός μοντέλου Μηχανικής Μάθησης. Στο στάδιο αυτό, τα αρχικά δεδομένα του συνόλου WUSTL-EHMS 2020 υποβλήθηκαν σε μια σειρά μετασχηματισμών, ώστε να καταστούν κατάλληλα για την εκπαίδευση του αλγορίθμου Random Forest

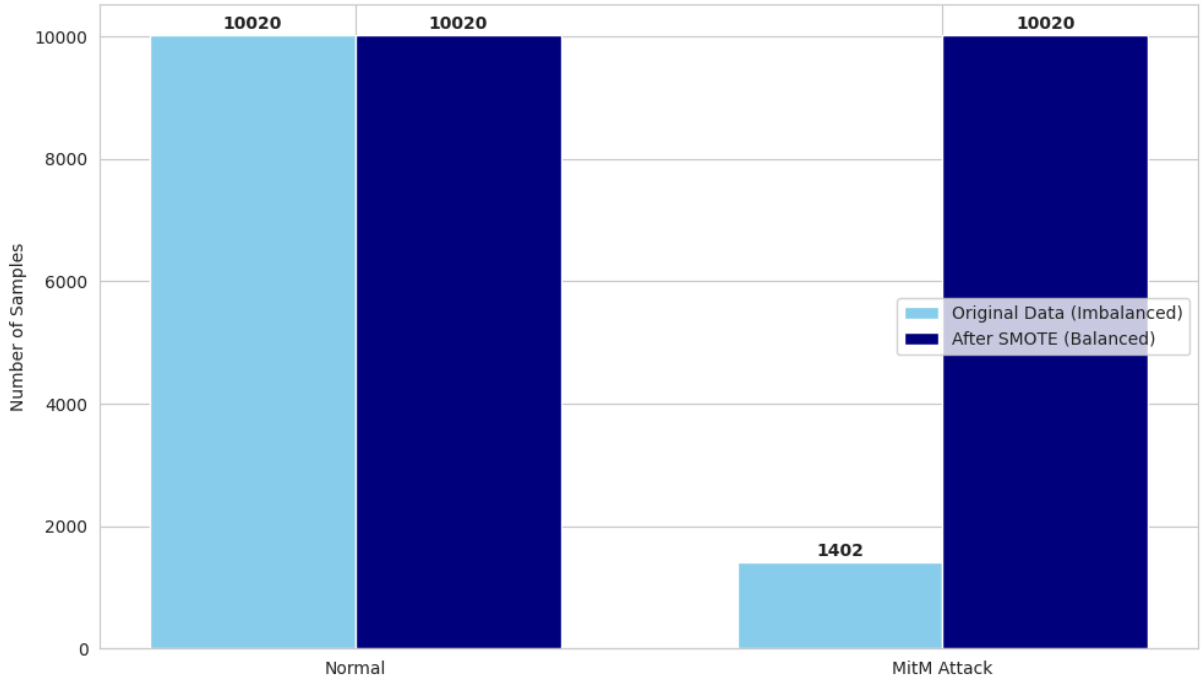
Το αρχικό σύνολο δεδομένων περιλαμβάνει χαρακτηριστικά σε μορφή κειμένου (object types), όπως οι διευθύνσεις IP (SrcAddr, DstAddr) και οι φυσικές διευθύνσεις MAC (SrcMac, DstMac). Δεδομένου ότι οι μαθηματικοί αλγόριθμοι απαιτούν αποκλειστικά αριθμητικές τιμές, εφαρμόστηκε η τεχνική Label Encoding. Η συγκεκριμένη μέθοδος μετασχηματίζει κάθε διακριτή αλφαριθμητική τιμή σε μια αντίστοιχη αριθμητική αναπαράσταση υπό τη μορφή ακεραίου, διασφαλίζοντας τη μαθηματική συνοχή του συνόλου δεδομένων, χωρίς να αλλοιώνεται η δομή του συνόλου δεδομένων.

Με στόχο την ανάπτυξη ενός συστήματος ανίχνευσης που βασίζεται στη συμπεριφορά (behavioral analysis), πραγματοποιήθηκε επιλεκτική αφαίρεση χαρακτηριστικών. Συγκεκριμένα, αφαιρέθηκε η στήλη Attack Category (Σχήμα 5), η οποία αναφέρετε στην επίθεση, καθώς η παραμονή της θα οδηγούσε σε υπερ-εκπαίδευση (overfitting) του μοντέλου. Όπως επίσης και οι διευθύνσεις (SrcAddr, DstAddr, SrcMac, DstMac) και θύρες (Sport, Dport), ώστε να μην αναγνωρίζει συγκεκριμένες συσκευές. Διατηρήθηκαν όλα τα χαρακτηριστικά που αφορούν τον χρονισμό των πακέτων (Jitter, Inter-packet time) και τις βιομετρικές μετρήσεις, καθώς αυτά φέρουν το χαρακτηριστικό της κακόβουλης παρέμβασης.

```
cols_to_drop = ['Label', 'Attack Category', 'SrcAddr', 'DstAddr', 'Sport', 'Dport', 'SrcMac', 'DstMac']
X = df.drop(columns=[col for col in cols_to_drop if col in df.columns])
y = df['Label']
```

Σχήμα 5: Διαδικασία αφαίρεσης στηλών ταυτοποίησης

Ένα από τα σημαντικότερα προβλήματα στα δεδομένα κυβερνοασφάλειας είναι η ανισορροπία μεταξύ των κλάσεων (class imbalance), όπου οι κανονικές ροές δεδομένων υπερτερούν αριθμητικά των δειγμάτων επίθεσης. Όπως φαίνεται στο Σχήμα 6 στο συγκεκριμένο dataset, η κλάση Normal ήταν σημαντικά μεγαλύτερη από την κλάση Attack. Για την επίλυση αυτού του προβλήματος, χρησιμοποιήθηκε ο αλγόριθμος SMOTE. Η μέθοδος αυτή δεν περιορίζεται στην απλή αντιγραφή των υπαρχόντων δειγμάτων της μειονότητας, αλλά δημιουργεί σύνθετα δείγματα αναλύοντας τον χώρο των χαρακτηριστικών και εφαρμόζοντας τον αλγόριθμο των KNN [79].



Σχήμα 6: Σύγκριση της κατανομής των κλάσεων του συνόλου δεδομένων πριν και μετά την εφαρμογή του αλγορίθμου SMOTE

Όπως φαίνεται στο Σχήμα 7, η εξισορρόπηση των δεδομένων πραγματοποιήθηκε με την εφαρμογή της μεθόδου SMOTE στο σύνολο εκπαίδευσης. Η επιτυχής εκτέλεση του αλγορίθμου οδήγησε σε ένα ισορροπημένο σύνολο 20.040 δειγμάτων. Εξασφαλίστηκε ότι ο ταξινομητής Random Forest θα εκπαιδευτεί αποδοτικά, αποφεύγοντας τη μεροληψία προς την επικρατέστερη κλάση.

```
sm = SMOTE(random_state=42)
X_train_res, y_train_res = sm.fit_resample(X_train, y_train)

print(f"Dataset size after SMOTE: {len(X_train_res)} samples")

...   Dataset size after SMOTE: 20040 samples
```

Σχήμα 7: Επιβεβαίωση της επιτυχούς εξισορρόπησης του συνόλου δεδομένων

6.4 Αρχιτεκτονική του Ταξινομητή Random Forest

Μετά το στάδιο της προ-επεξεργασίας και της εξισορρόπησης των δεδομένων, επιλέχθηκε ο αλγόριθμος Random Forest [80] για την υλοποίηση του Συστήματος Ανίχνευσης Εισβολών (IDS). Η επιλογή αυτή βασίστηκε στην αποδεδειγμένη ικανότητα του αλγορίθμου να διαχειρίζεται πολύπλοκα σύνολα δεδομένων με υψηλή ακρίβεια και χαμηλή υπολογιστική επιβάρυνση.

Ο Random Forest ανήκει στην κατηγορία της ensemble learning [80]. Αντί να βασίζεται σε ένα μεμονωμένο Decision Tree, ο αλγόριθμος κατασκευάζει ένα μεγάλο πλήθος ανεξάρτητων μοντέλων κατά τη διάρκεια της εκπαίδευσης. Η τελική πρόβλεψη προκύπτει μέσω της διαδικασίας της majority voting, όπου το μοντέλο κατατάσσει μια ροή δεδομένων ως «Επίθεση» ή «Κανονική» με βάση την κατηγορία που επέλεξε η πλειοψηφία των μοντέλων.

Η αρχιτεκτονική αυτή προσφέρει κρίσιμα πλεονεκτήματα όπως:

- Αποφυγή υπερ-εκπαίδευσης (Overfitting): Λόγω της τυχαίας επιλογής υποσυνόλων χαρακτηριστικών (feature bagging) σε κάθε μοντέλο, ο αλγόριθμος δεν μαθαίνει το dataset εκπαίδευσης, αλλά μαθαίνει να αναγνωρίζει γενικά πρότυπα συμπεριφοράς.
- Επεξεργασία πολυπαραμετρικών δεδομένων: Το μοντέλο επεξεργάστηκε αποτελεσματικά και τα 44 χαρακτηριστικά του WUSTL-EHMS 2020, αξιολογώντας τη σημασία κάθε μεταβλητής.
- Υπεροχή έναντι διαφορετικών αρχιτεκτονικών: Ο Random Forest επέδειξε ανώτερη και σταθερότερη απόδοση σε σύγκριση με τον αλγόριθμο KNN (93,32% έναντι 90,07%), επιβεβαιώνοντας ότι η συνδυαστική προσέγγιση Ensemble Learning είναι πιο αποτελεσματική στον εντοπισμό σύνθετων επιθέσεων MitM από τις μεθόδους που βασίζονται αποκλειστικά σε distance-based metrics.

6.5 Ανάλυση Αποτελεσμάτων

Η επιλογή του test set σε ποσοστό 30% εξασφάλισε την αντικειμενική αξιολόγηση του μοντέλου σε πραγματικές συνθήκες. Με αυτόν τον τρόπο, αποφεύχθηκε το φαινόμενο της υπερεκπαίδευσης (overfitting) και επιβεβαιώθηκε ότι η υψηλή ακρίβεια του Random Forest οφείλεται στην επιτυχή εξαγωγή προτύπων και όχι στην απλή απομνημόνευση των δεδομένων εκπαίδευσης. Το σύστημα πέτυχε συνολική ακρίβεια (Accuracy) της τάξης του 93,32%. Η ανάλυση των επιμέρους δεικτών ανά κλάση φανερώνει την υψηλή αξιοπιστία του συστήματος:

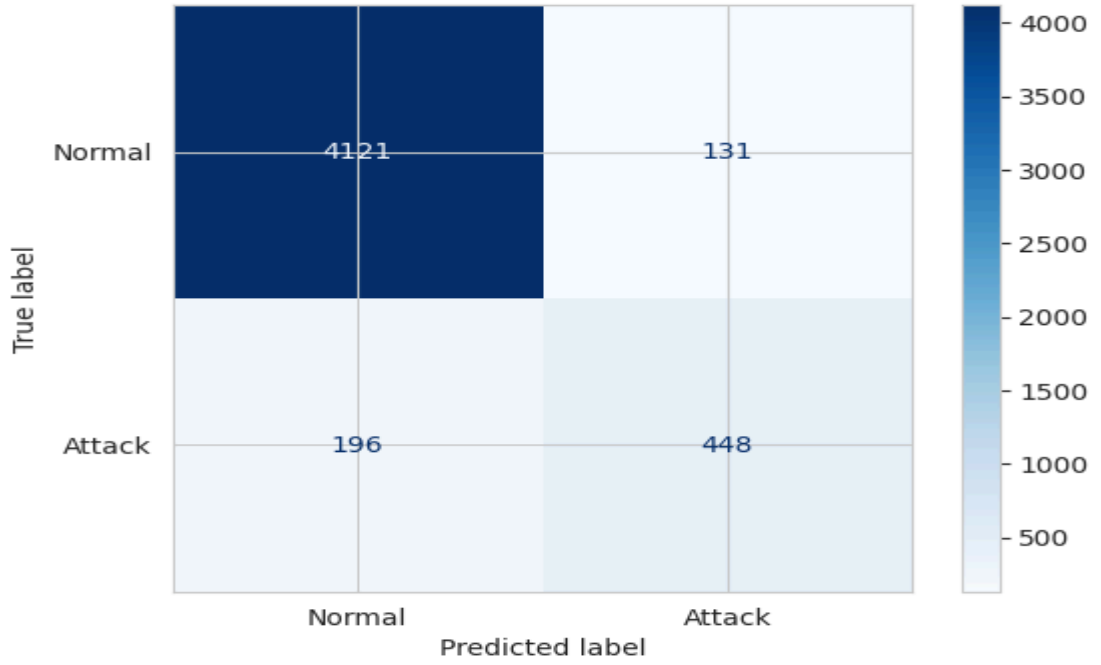
- Κλάση Normal: Το μοντέλο εμφάνισε Precision 0,95 και Recall 0,97 (Σχήμα 8). Αυτό σημαίνει ότι το σύστημα αναγνωρίζει την ροή δεδομένων, διασφαλίζοντας ότι η ιατρική παρακολούθηση δεν θα διακόπτεται από άσκοπους συναγερμούς.
- Κλάση Attack: Στην ανίχνευση κακόβουλων ενεργειών, το σύστημα σημείωσε Precision 0,77 και Recall 0,70 (Σχήμα 8). Οι τιμές αυτές θεωρούνται ικανοποιητικές για επιθέσεις MitM , δεδομένου ότι η ανίχνευση βασίστηκε αποκλειστικά σε δυναμικά χαρακτηριστικά (όπως ο χρονισμός) και όχι σε στατικές πληροφορίες ταυτότητας.

	precision	recall	f1-score	support
0	0.95	0.97	0.96	4252
1	0.77	0.70	0.73	644

Σχήμα 8: Αναφορά ταξινόμησης μοντέλου Random Forest

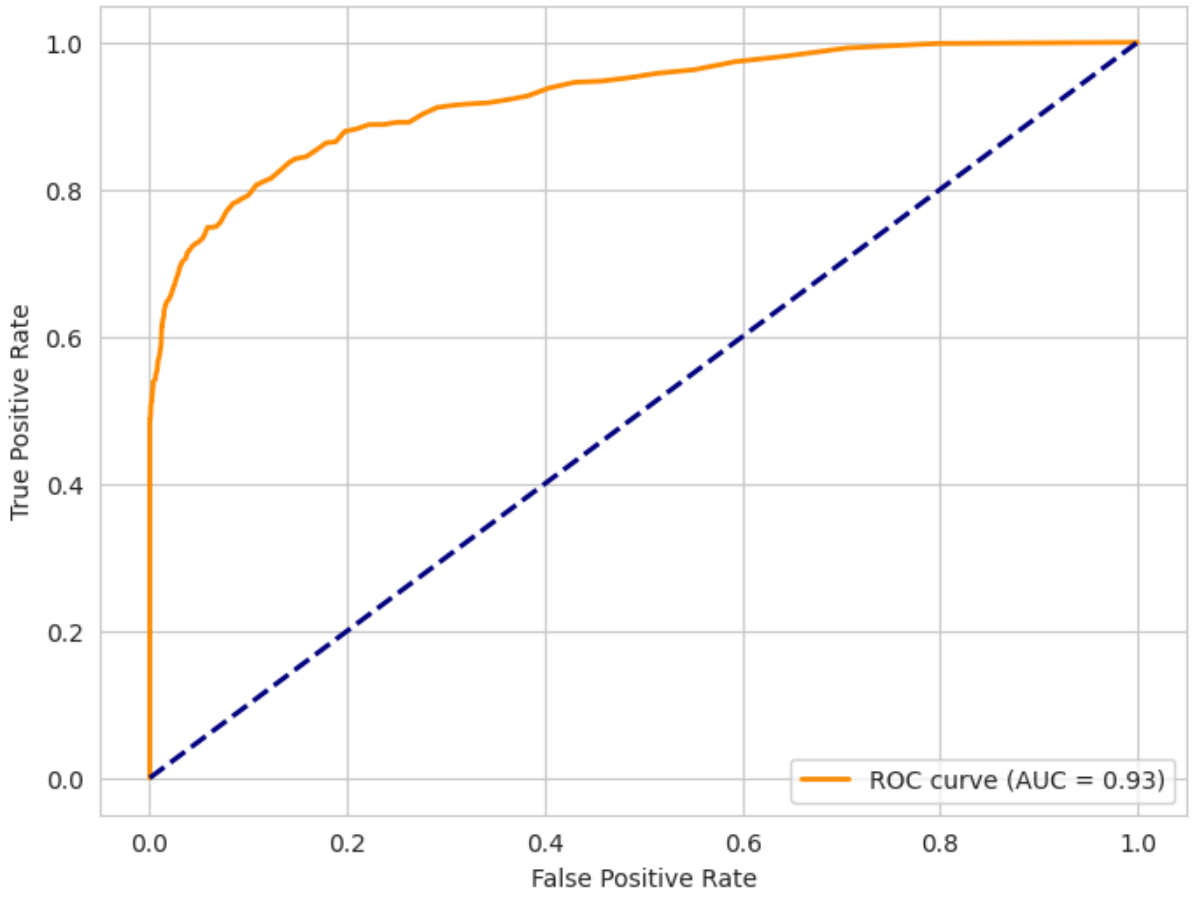
Ο Confusion Matrix (Σχήμα 9) προσφέρει μια λεπτομερή καταγραφή των προβλέψεων του μοντέλου:

- True Negatives (4.121): Σωστός εντοπισμός κανονικής κίνησης.
- True Positives (448): Επιτυχημένη ανίχνευση επιθέσεων.
- False Positives (131): Εσφαλμένοι συναγερμοί. Το εξαιρετικά χαμηλό αυτό νούμερο (approx 3%) είναι κρίσιμο για το IoMT, καθώς οι πολλοί ψευδείς συναγερμοί θα μπορούσαν να οδηγήσουν σε alarm fatigue από το ιατρικό προσωπικό και τον ασθενή.
- False Negatives (196): Επιθέσεις που διέφυγαν της προσοχής του συστήματος. Αντανακλά τη δυσκολία εντοπισμού εξελιγμένων επιθέσεων MitM , οι οποίες συχνά παρουσιάζουν παρόμοιο αποτύπωμα με την κανονική ροή δεδομένων.



Σχήμα 9: Confusion Matrix για την αξιολόγηση των προβλέψεων του μοντέλου

Η ικανότητα του μοντέλου να διαχωρίζει τις δύο κλάσεις αποτυπώνεται στον δείκτη AUC (Area Under the Curve), ο οποίος ανήλθε στο 0,93 (Σχήμα 10). Η ταχεία άνοδος της καμπύλης στο αριστερό τμήμα του διαγράμματος (Σχήμα 10) και η υψηλή τιμή του AUC (0.93) υποδηλώνουν ότι ο αλγόριθμος επιτυγχάνει μέγιστη ευαισθησία διατηρώντας παράλληλα εξαιρετικά χαμηλά ποσοστά ψευδών συναγερμών, γεγονός κρίσιμο για την αξιοπιστία ενός συστήματος IDS σε περιβάλλοντα IoMT. Η διακεκομμένη γραμμή αντιπροσωπεύει την απόδοση ενός τυχαίου ταξινομητή (AUC = 0.5). Η σημαντική απόκλιση της καμπύλης ROC του προτεινόμενου μοντέλου από τη διαγώνιο αυτή, αποδεικνύει την υψηλή προγνωστική ικανότητα του αλγορίθμου. Η περιοχή κάτω από την καμπύλη (AUC = 0.93) επιβεβαιώνει ότι ο Random Forest διαθέτει την ικανότητα να διακρίνει τις κακόβουλες δραστηριότητες MitM από τη φυσιολογική ροή δεδομένων του IoMT δικτύου, εκμηδενίζοντας την πιθανότητα τυχαίας ταξινόμησης.



Σχήμα 10: Καμπύλη ROC (Receiver Operating Characteristic) του μοντέλου Random Forest

6.6 Συγκριτική Αξιολόγηση Μοντέλων

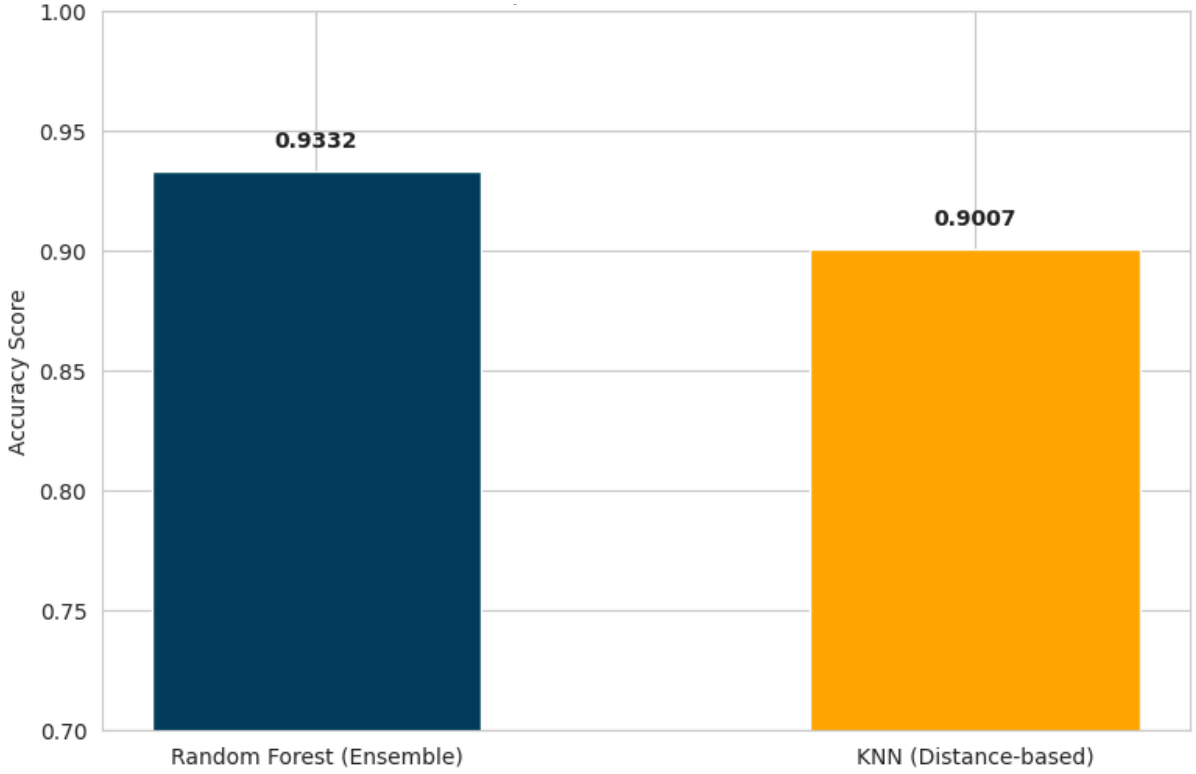
Για την επικύρωση της αποτελεσματικότητας του προτεινόμενου συστήματος, πραγματοποιήθηκε συγκριτική δοκιμή μεταξύ δύο διαφορετικών προσεγγίσεων Μηχανικής Μάθησης του αλγορίθμου Random Forest (Ensemble Learning) και του αλγορίθμου KNN (Distance-based Learning). Η σύγκριση αυτή κρίθηκε απαραίτητη προκειμένου να διαπιστωθεί ποια αρχιτεκτονική ανταποκρίνεται καλύτερα στις ιδιαιτερότητες των δεδομένων του δικτύου IoMT.

Όπως καταγράφεται στο Σχήμα 11, ο Random Forest παρουσιάζει ακρίβεια 93,32%, υπερτερώντας του KNN ο οποίος σημείωσε 90,07%. Η υπεροχή του Random Forest αποδίδεται στους εξής παράγοντες:

1. Ανθεκτικότητα στον θόρυβο: Τα δεδομένα από ιατρικούς αισθητήρες (IoMT) συχνά περιέχουν θόρυβο ή ακραίες τιμές (outliers). Ο KNN επηρεάζεται σημαντικά από αυτές καθώς βασίζεται στην απόσταση μεταξύ μεμονωμένων σημείων, ο Random Forest, μέσω της χρήσης πολλαπλών δέντρων απόφασης, εξομαλύνει τέτοιες διακυμάνσεις, προσφέροντας πιο σταθερές προβλέψεις.
2. Πολυπλοκότητα χαρακτηριστικών: Οι επιθέσεις MitM δεν είναι πάντα γεωμετρικά διακριτές. Ο Random Forest μπορεί να δημιουργήσει σύνθετους λογικούς κανόνες συνδυάζοντας

διαφορετικά χαρακτηριστικά όπως ο χρόνος πακέτου και μια βιομετρική τιμή, κάτι που ο KNN δυσκολεύεται να επιτύχει.

3. Γενίκευση (Generalization): Η τεχνική του bagging που χρησιμοποιεί ο Random Forest τον καθιστά λιγότερο επιρρεπή σε υπερεκπαίδευση (overfitting) σε σύγκριση με τον KNN, ειδικά σε σύνολα δεδομένων όπως το WUSTL-EHMS 2020.



Σχήμα 11: Συγκριτική απεικόνιση της ακρίβειας (Accuracy) μεταξύ του προτεινόμενου μοντέλου Random Forest και του μοντέλου αναφοράς KNN

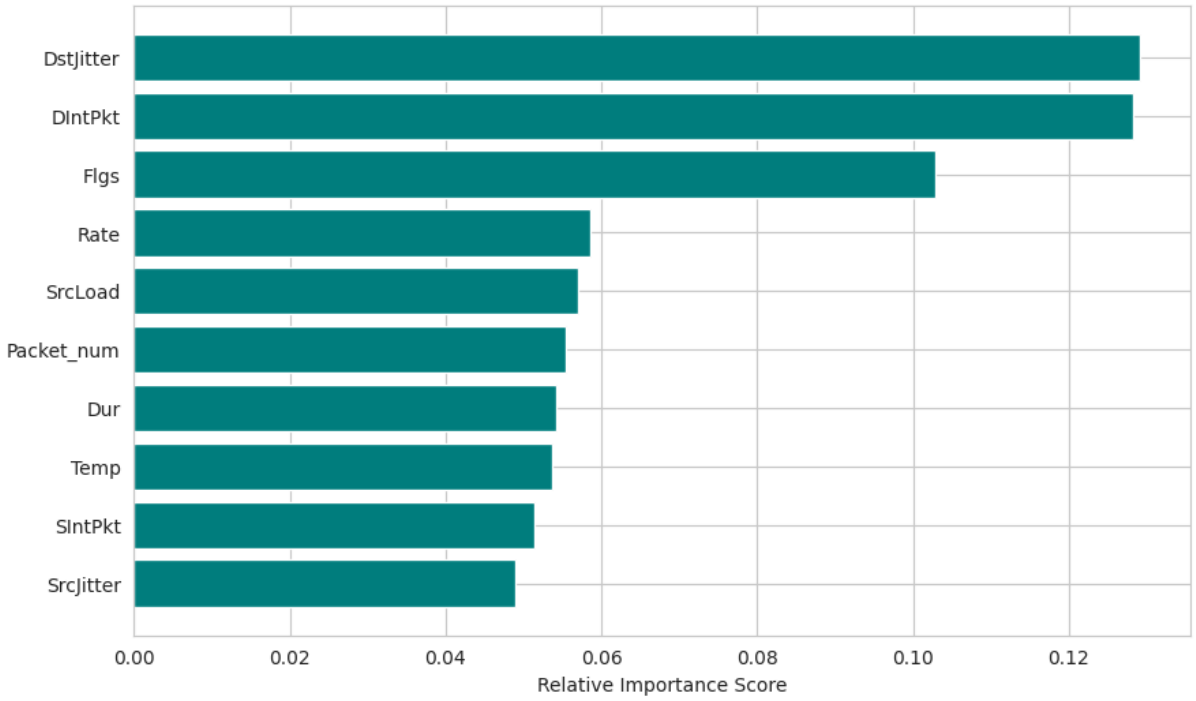
6.7 Αξιολόγηση Σπουδαιότητας Χαρακτηριστικών και Χρόνου Απόκρισης του Random Forest

Η επιτυχία ενός συστήματος ανίχνευσης εισβολών δεν κρίνεται μόνο από τη συνολική του ακρίβεια, αλλά και από την ικανότητά του να ερμηνεύει ποια στοιχεία της δικτυακής κίνησης υποδηλώνουν κίνδυνο, καθώς και από την ταχύτητα με την οποία αντιδρά.

Ένα από τα σημαντικότερα πλεονεκτήματα του Random Forest είναι η δυνατότητα εξαγωγής της σπουδαιότητας (importance) κάθε χαρακτηριστικού. Στο Σχήμα 12, παρατηρούμε ότι το μοντέλο βασίστηκε κυρίως σε παραμέτρους χρονισμού για τον εντοπισμό των επιθέσεων MitM:

- DstJitter και SrcJitter: Αναδείχθηκαν ως οι πλέον κρίσιμοι δείκτες. Η διακύμανση στον χρόνο άφιξης των πακέτων (jitter) αποτελεί το αποτύπωμα μιας παρέμβασης MitM, καθώς η μεσολάβηση ενός επιτιθέμενου στη ροή των δεδομένων προκαλεί αναπόφευκτες χρονικές καθυστερήσεις.

- DIntPkt (Destination Inter-packet Time): Ο χρόνος μεταξύ των πακέτων στον προορισμό έπαιξε επίσης σημαντικό ρόλο, επιβεβαιώνοντας ότι οι επιθέσεις αλλοιώνουν τον σταθερό ρυθμό μετάδοσης των βιομετρικών δεδομένων.
- Βιομετρικές τιμές: Αν και τα δικτυακά χαρακτηριστικά ήταν τα πιο καθοριστικά για την ανίχνευση της εισβολής, οι βιομετρικές μετρήσεις (όπως το Heart_rate και η Temp) παρείχαν το απαραίτητο πλαίσιο για την αξιολόγηση της σοβαρότητας της κατάστασης.



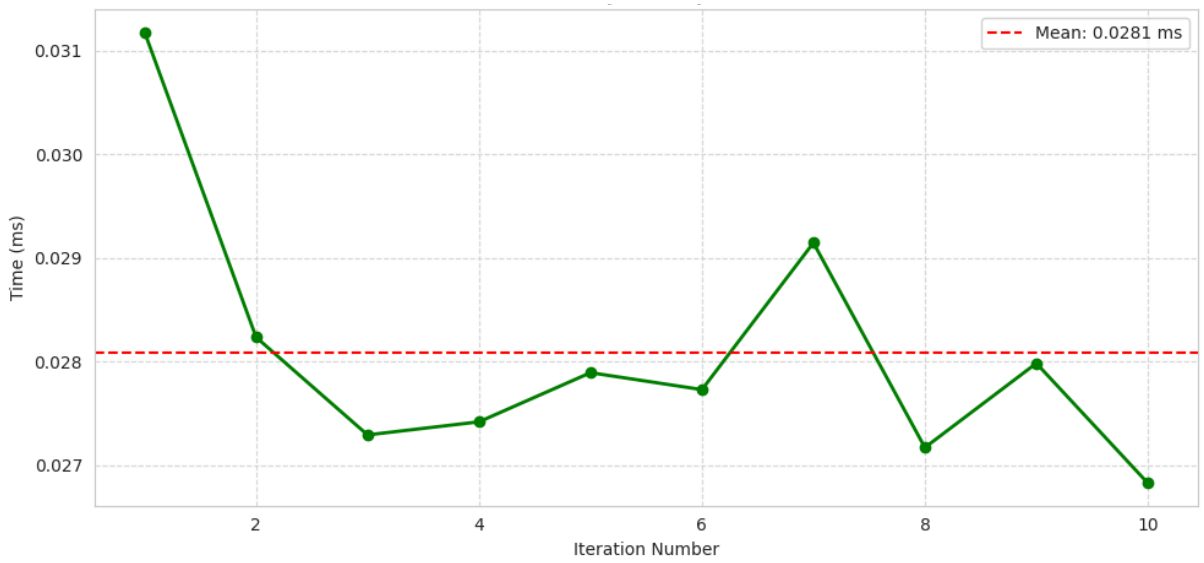
Σχήμα 12: Κατάταξη των δέκα Feature Importance του δικτύου και των βιομετρικών δεδομένων για την ανίχνευση εισβολών

Για τα συστήματα IoMT, η καθυστέρηση (latency) στην ανίχνευση μπορεί να αποβεί μοιραία. Κατά τη διάρκεια της πειραματικής διαδικασίας, μετρήθηκε ο μέσος χρόνος που απαιτείται (Σχήμα 13) για την επεξεργασία μιας ροής δεδομένων και την έκδοση απόφασης από το μοντέλο (Σχήμα 14):

- Μέσος χρόνος ανίχνευσης ανά δείγμα: 0,0281 ms (χιλιοστά του δευτερολέπτου) ή 28,1 μs (microseconds).
- Τυπική απόκλιση (Standard Deviation): 0,0011 ms, γεγονός που υποδηλώνει εξαιρετική σταθερότητα και αξιοπιστία στην απόδοση του αλγορίθμου Random Forest υπό συνεχή ροή δεδομένων.

```
[Final Results Summary]
Mean Latency: 0.028087 ms
Standard Deviation: 0.001199 ms
```

Σχήμα 13: Μέση καθυστέρηση και τυπική απόκλιση



Σχήμα 14: Διακύμανση του χρόνου ανίχνευσης (latency) σε 10 διαδοχικές επαναλήψεις

Ο χρόνος αυτός κρίνεται ως αμελητέος, επιτρέποντας στο IDS να λειτουργεί σε πραγματικό χρόνο (real-time) με δυνατότητα επεξεργασίας χιλιάδων πακέτων ανά δευτερόλεπτο. Η απόκριση σε επίπεδο microseconds διασφαλίζει ότι οποιαδήποτε κακόβουλη ενέργεια ανιχνεύεται ακαριαία, προτού ο επιτιθέμενος καταφέρει να αλλοιώσει κρίσιμες ιατρικές πληροφορίες ή να προκαλέσει δυσλειτουργία στις φορετές συσκευές.

6.8 Επίλογος

Η ανάπτυξη και αξιολόγηση του Συστήματος Ανίχνευσης Εισβολών (IDS) μέσω της γλώσσας προγραμματισμού Python και του αλγορίθμου Random Forest επικυρώνει τη μετάβαση από τη θεωρητική μοντελοποίηση στην ουσιαστική ενίσχυση της ασφάλειας σε περιβάλλον IoMT. Λαμβάνοντας υπόψη τη διαφορά του 3,25% στην ακρίβεια, αλλά και την ανώτερη ικανότητα διαχείρισης σύνθετων μοτίβων, ο Random Forest επιλέχθηκε ως ο κεντρικός ταξινομητής της παρούσας μελέτης σε σχέση με τον KNN. Η πειραματική διαδικασία απέδειξε ότι η ασφάλεια των ευαίσθητων ιατρικών δεδομένων δεν αποτελεί πλέον ένα στατικό πρόβλημα, αλλά μια δυναμική πρόκληση που απαιτεί προηγμένες λύσεις Μηχανικής Μάθησης.

Η αξιολόγηση των αποτελεσμάτων αναδεικνύει ορισμένα κρίσιμα συμπεράσματα, τα οποία συνοψίζονται ως εξής:

- Αποτελεσματικότητα στην ανίχνευση: Το μοντέλο πέτυχε υψηλή ακρίβεια (93,32%) στον εντοπισμό επιθέσεων Man-in-the-Middle, αποδεικνύοντας ότι ο συνδυασμός δεδομένων δικτύου και βιομετρικών χαρακτηριστικών παρέχει μια αξιόπιστη βάση για την αναγνώριση κακόβουλων προτύπων συμπεριφοράς.
- Εξισορρόπηση: Η χρήση της τεχνικής SMOTE υπήρξε καθοριστική, καθώς επέτρεψε στο σύστημα να εκπαιδευτεί ομοιόμορφα πάνω σε 20.040 δείγματα, επιλύοντας το πρόβλημα της ανισορροπίας των δεδομένων και ενισχύοντας την ικανότητα του μοντέλου να ανιχνεύει σπάνιες αλλά κρίσιμες απειλές.
- Λειτουργία σε πραγματικό χρόνο: Ο εξαιρετικά χαμηλός χρόνος απόκρισης των 0,0281 ms (28,1 μs) επιβεβαιώνει ότι η προτεινόμενη λύση είναι εφαρμόσιμη σε πραγματικές συνθήκες

κλινικής παρακολούθησης, όπου η ταχύτητα ανίχνευσης είναι άρρηκτα συνδεδεμένη με την ασφάλεια του ασθενούς.

- Ανάλυση συμπεριφοράς: Η ανάλυση της σπουδαιότητας των χαρακτηριστικών ανέδειξε το Jitter ως τον κυριότερο δείκτη επίθεσης. Το εύρημα αυτό υπογραμμίζει ότι η θωράκιση των wearables πρέπει να επικεντρώνεται στην ανάλυση της ροής των δεδομένων, η οποία παραμένει διακριτή ακόμα και όταν ο επιτιθέμενος προσπαθεί να μιμηθεί την κανονική λειτουργία.

Η παρούσα μελέτη καταδεικνύει ότι η ενσωμάτωση έξυπνων μηχανισμών παρακολούθησης στις gateways μπορεί να περιορίσει δραστικά το εύρος της επίθεσης, διασφαλίζοντας την ακεραιότητα των ιατρικών υπηρεσιών και την εμπιστοσύνη των ασθενών στις σύγχρονες τεχνολογίες υγείας.

Κεφάλαιο 7ο: Συμπεράσματα και Μελλοντικές Επεκτάσεις

7.1 Συμπεράσματα

Η ολοκλήρωση της παρούσας εργασίας επιβεβαιώνει ότι η ασφάλεια στα περιβάλλοντα IoMT δεν αποτελεί μια μονοδιάστατη διαδικασία, αλλά μια συνεχή δυναμική πρόκληση. Ξεκινώντας από την τεχνολογική επισκόπηση, έγινε σαφές ότι η πολυπλοκότητα των φορετών ιατρικών συσκευών, από τα υλικά κατασκευής έως την αρχιτεκτονική τριών επιπέδων, δημιουργεί πολλαπλά σημεία δυνητικής παραβίασης, καθιστώντας το σύστημα εκτεθειμένο σε κάθε επίπεδο της αρχιτεκτονικής του.

Παρά την ευρεία χρήση προτύπων, η ανάγκη για χαμηλή ενεργειακή κατανάλωση συχνά περιορίζει τη δυνατότητα ενσωμάτωσης ισχυρών κρυπτογραφικών μεθόδων, αφήνοντας το σύστημα εκτεθειμένο σε εξελιγμένες κυβερνοαπειλές. Η ανάλυση έδειξε ότι οι ευπάθειες σε επίπεδο υλικού και λογισμικού καθιστούν τις συσκευές ευάλωτες σε υποκλοπές και παραποίηση δεδομένων, γεγονός που καθιστά επιτακτική την αυστηρή τήρηση προτύπων όπως το ISO 27001 και ο GDPR. Αναδείχθηκε ότι η πλήρης ενσωμάτωση των προτύπων IEEE 11073-20601 και των ειδικών εφαρμογών τους (10404, 10406, 10407, 10417) στο επίπεδο επικοινωνίας του IEEE 802.15.6, διασφαλίζει τη βιωσιμότητα και την ακρίβεια στη μεταφορά δεδομένων εντός των σύγχρονων δικτύων αισθητήρων σώματος.

Τα πρωτόκολλα επικοινωνίας αποτελούν τον πιο κρίσιμο κρίκο στην αλυσίδα του IoMT. Παρά την ενσωμάτωση προηγμένων αλγορίθμων, η ανάγκη για lightweight υλοποίηση περιορίζει τη δυνατότητα εφαρμογής σύνθετων κρυπτογραφικών ελέγχων, αφήνοντας τις συσκευές εκτεθειμένες σε επιθέσεις υποκλοπής και παραποίησης σε πραγματικό χρόνο. Συμπερασματικά, η υιοθέτηση των πρωτοκόλλων BLE και ZigBee αποτελεί τον ακρογωνιαίο λίθο για την εξέλιξη των ιατρικών wearables, υπό την προϋπόθεση ότι η ενεργειακή τους αποδοτικότητα θα πλαισιώνεται πάντα από μια δυναμική στρατηγική ασφάλειας που διασφαλίζει την αδιαπραγμάτευτη ιδιωτικότητα των ασθενών.

Η πειραματική προσέγγιση με τη χρήση του αλγορίθμου Random Forest απέδειξε ότι η μηχανική μάθηση μπορεί να λειτουργήσει ως ένα αξιόπιστο εργαλείο προστασίας. Η επίτευξη ακρίβειας 93% στο σύνολο δεδομένων WUSTL-EHMS 2020 υπογραμμίζει ότι η ανάλυση της κίνησης του δικτύου μπορεί να εντοπίσει κακόβουλες εισβολές τις οποίες ένα απλό σύστημα ελέγχου θα αδυνατούσε να κατηγοριοποιήσει ως απειλές λόγω της πολυπλοκότητάς τους. Η χρήση της μεθοδολογίας SMOTE ανέδειξε ότι η σωστή προ-επεξεργασία των δεδομένων είναι εξίσου σημαντική με τον ίδιο τον αλγόριθμο. Η εξισορρόπηση των κλάσεων επέτρεψε στο σύστημα να αναγνωρίζει τις επιθέσεις με την ίδια ευκολία που αναγνωρίζει τη φυσιολογική λειτουργία, διασφαλίζοντας ότι το σύστημα παραμένει σε διαρκή ετοιμότητα. Ο χαμηλός χρόνος απόκρισης (0,0281 ms) που καταγράφηκε, αποτελεί την πλέον καθοριστική παράμετρο για την ενσωμάτωση τέτοιων συστημάτων σε πραγματικά ιατρικά περιβάλλοντα, όπου ο χρόνος αποτελεί κρίσιμο παράγοντα.

7.2 Μελλοντικές Επεκτάσεις

Η παρούσα εργασία ανέδειξε τις θεμελιώδεις προκλήσεις ασφάλειας στα περιβάλλοντα IoMT, ωστόσο η ραγδαία εξέλιξη της τεχνολογίας καθιστά αναγκαία τη συνεχή επέκταση της έρευνας. Οι μελλοντικές κατευθύνσεις προτείνεται να εστιάσουν στους ακόλουθους άξονες:

- Ανάπτυξη αποδοτικών μηχανισμών προστασίας: Η κυρίαρχη πρόκληση που αναδείχθηκε από την παρούσα μελέτη είναι η ισορροπία ανάμεσα στην πολυπλοκότητα των αλγορίθμων και την αυτονομία της συσκευής. Οι φορετές συσκευές, λόγω του περιορισμένου μεγέθους τους,

ενσωματώνουν μικροελεγκτές με περιορισμένη μνήμη RAM και επεξεργαστική ισχύ. Η μελλοντική έρευνα οφείλει να εστιάσει στη δημιουργία Lightweight Cryptography πρωτοκόλλων, τα οποία θα προσφέρουν ασφάλεια με το ελάχιστο δυνατό υπολογιστικό κόστος. Επιπλέον, η έρευνα πρέπει να στραφεί προς την ενεργειακά αποδοτική ασφάλεια. Αυτό σημαίνει την ανάπτυξη αλγορίθμων που προσαρμόζουν το επίπεδο κρυπτογράφησης ανάλογα με την κρισιμότητα των δεδομένων ή τη στάθμη της μπαταρίας. Κατά τη μετάδοση δεδομένων ρουτίνας θα μπορούσε να χρησιμοποιείται Lightweight Cryptography, ενώ σε κατάσταση έκτακτης ανάγκης το σύστημα θα υιοθετεί αυστηρότερα κρυπτογραφικά πρότυπα, διασφαλίζοντας την ακεραιότητα των κρίσιμων δεδομένων. Η τεκμηρίωση αυτής της ανάγκης βασίζεται στο γεγονός ότι η εξάντληση της μπαταρίας σε μια ιατρική συσκευή δεν αποτελεί απλώς τεχνικό σφάλμα, αλλά άμεση απειλή για τη ζωή του ασθενούς. Συνεπώς, η βελτιστοποίηση των πόρων μέσω αλγορίθμων χαμηλού ενεργειακού αποτυπώματος αποτελεί μονόδρομο για τη βιώσιμη ενσωμάτωση των wearables στο πεδίο της υγειονομικής φροντίδας.

- Προηγμένες τεχνικές αναγνώρισης προτύπων: Η αποτελεσματικότητα του αλγορίθμου Random Forest που εξετάστηκε στην παρούσα εργασία αποτελεί το θεμέλιο για την ανάπτυξη πιο σύνθετων μοντέλων. Μια κρίσιμη μελλοντική κατεύθυνση είναι η υλοποίηση συστημάτων Explainable AI. Στα ιατρικά περιβάλλοντα, η απλή ανίχνευση δυσλειτουργιών δεν επαρκεί, το ιατρικό προσωπικό πρέπει να κατανοεί τους λόγους για τους οποίους στο σύστημα εμφανίστηκε κάποια ένδειξη συναγερμού. Η έρευνα θα πρέπει να εστιάσει σε μοντέλα που παρέχουν ερμηνεύσιμα αποτελέσματα, διαχωρίζοντας με σαφήνεια τις κυβερνοεπιθέσεις από τις παθολογικές μεταβολές του ασθενούς. Μια κρίσιμη ερευνητική κατεύθυνση αποτελεί η βελτιστοποίηση της ταχύτητας απόκρισης αυτών των σύνθετων μοντέλων. Στα ιατρικά περιβάλλοντα, η καθυστέρηση μερικών δευτερολέπτων στην ανίχνευση μιας παραβίασης μπορεί να αποβεί μοιραία. Η ανάπτυξη τεχνικών μείωσης της πολυπλοκότητας των μοντέλων είναι απαραίτητη ώστε ορισμένες από τις προηγμένες τεχνικές αναγνώρισης προτύπων να μπορούν να εκτελούνται απευθείας πάνω στις φορετές συσκευές χαμηλής κατανάλωσης, χωρίς να εξαρτώνται αποκλειστικά από τη συνδεσιμότητα με το Cloud.
- Προστασία ιδιωτικότητας: Η προστασία της ιδιωτικότητας στα IoMT περιβάλλοντα απαιτεί πλέον μια προληπτική προσέγγιση. Σε θεσμικό πλαίσιο, η πολυπλοκότητα αυξάνεται λόγω της διεθνούς φύσης των δεδομένων. Η έρευνα οφείλει να προτείνει αυτοματοποιημένα εργαλεία συμμόρφωσης που θα παρακολουθούν τη ροή της πληροφορίας σε πραγματικό χρόνο, διασφαλίζοντας ότι τηρούνται οι κανονισμοί του GDPR και του HIPAA. Η ηθική διάσταση της διαχείρισης των δεδομένων πρέπει να ενσωματωθεί στα ίδια τα πρωτόκολλα επικοινωνίας. Η χρήση τεχνολογιών Blockchain θα μπορούσε να αυτοματοποιήσει τη συγκατάθεση του ασθενούς για τη χρήση των δεδομένων του, επιτρέποντας την πρόσβαση μόνο σε εξουσιοδοτημένο προσωπικό και καταγράφοντας αμετάβλητα κάθε ενέργεια, ενισχύοντας έτσι τη διαφάνεια και τη λογοδοσία του συστήματος.
- Αντιμετώπιση αναδυόμενων απειλών: Η ταχύτατη εξέλιξη της κβαντικής υπολογιστικής αποτελεί μια από τις μεγαλύτερες μελλοντικές προκλήσεις για την κυβερνοασφάλεια. Οι παραδοσιακοί αλγόριθμοι ασύμμετρης κρυπτογράφησης, που χρησιμοποιούνται σήμερα στα wearables, θεωρούνται μαθηματικά ευάλωτοι σε μελλοντικές κβαντικές επιθέσεις. Η έρευνα πρέπει, συνεπώς, να προσανατολιστεί άμεσα προς την Post-Quantum Cryptography. Η πρόκληση εδώ είναι διπλή, οι νέοι αλγόριθμοι πρέπει να είναι ανθεκτικοί σε κβαντικούς υπολογιστές, αλλά ταυτόχρονα lightweight ώστε να τρέχουν στις περιορισμένες πηγές των ιατρικών wearables. Καθώς μια φορετή συσκευή αποτελείται από υλικό και λογισμικό πολλών

διαφορετικών κατασκευαστών, η μελλοντική έρευνα πρέπει να αναπτύξει μεθοδολογίες για την επαλήθευση της ακεραιότητας κάθε στοιχείου της αλυσίδας. Προτείνεται η διερεύνηση στον τομέα της ανάπτυξης μηχανισμών συνεχούς ταυτοποίησης, οι οποίοι αναλύουν μοναδικά βιομετρικά χαρακτηριστικά του χρήστη σε πραγματικό χρόνο. Αυτό διασφαλίζει ότι η συσκευή παραμένει λειτουργική μόνο όσο βρίσκεται σε χρήση από τον εξουσιοδοτημένο ασθενή, ακυρώνοντας την πρόσβαση σε περίπτωση κλοπής ή μη εξουσιοδοτημένης χρήσης.

Συμπερασματικά, η μελλοντική έρευνα οφείλει να διασφαλίσει ότι οι φορετές ιατρικές συσκευές θα παραμείνουν αξιόπιστες και ασφαλείς, διασφαλίζοντας την απαραίτητη εμπιστοσύνη για την καθολική υιοθέτηση των συγκεκριμένων τεχνολογιών στα σύγχρονα συστήματα υγειονομικής περίθαλψης.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] M. M. H. Shuvo et al., “Energy Harvesting in Implantable and Wearable Medical Devices for Enduring Precision Healthcare,” *Energies*, vol. 15, p. 7495, Oct. 2022, doi: 10.3390/en15207495.

[2] W. Gao and C. Yu, “Wearable and Implantable Devices for Healthcare,” *Adv. Healthcare Mater.*, vol. 10, p. 2101548, 2021, doi: 10.1002/adhm.202101548.

[3] L. Wang, K. Jiang, and G. Shen, “Wearable, Implantable, and Interventional Medical Devices Based on Smart Electronic Skins,” *Adv. Mater. Technol.*, vol. 6, p. 2100107, May 2021, doi: 10.1002/admt.202100107.

[4] D. Hemapriya, P. Viswanath, V. M. Mithra, S. Nagalakshmi and G. Umarani, "Wearable medical devices — Design challenges and issues," *2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT)*, Coimbatore, India, 2017, pp. 1-6, doi: 10.1109/IGEHT.2017.8094096.

[5] M. Tan et al., “Recent Advances in Intelligent Wearable Medical Devices Integrating Biosensing and Drug Delivery,” *Adv. Mater.*, vol. 34, p. 2108491, Apr. 2022, doi: 10.1002/adma.202108491.

[6] R. Ghanim, A. Kaushik, J. Park, and A. Abramson, "Communication protocols integrating wearables, ingestibles, and implantables for closed-loop therapies," *Device*, vol. 1, no. 1, p. 100092, Sep. 2023, doi: 10.1016/j.device.2023.100092.

[7] L. Wang et al., “Bio‐Multifunctional Smart Wearable Sensors for Medical Devices,” *Adv. Intell. Syst.*, vol. 1, p. 1900040, Oct. 2019, doi: 10.1002/aisy.201900040.

[8] H. C. Koydemir and A. Ozcan, “Wearable and Implantable Sensors for Biomedical Applications,” *Annu. Rev. Anal. Chem.*, vol. 11, pp. 127–146, 2018, doi: 10.1146/annurev-anchem-061417-125956.

[9] Retracted: Internet of Medical Things (IoMT)-Based Smart Healthcare System: Trends and Progress," *Comput. Intell. Neurosci.*, vol. 2023, p. 7218113, Nov. 2023. doi: 10.1155/2022/7218113.

[10] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, “Security in IoMT Communications: A Survey,” *Sensors*, vol. 20, no. 17, p. 4828, Aug. 2020, doi: 10.3390/s20174828.

[11] Z. Chu, Y. Zhou, S. Li, Q. Xu, and L. Pan, “Implantable Medical Electronic Devices: Sensing Mechanisms, Communication Methods, and the Biodegradable Future,” *Appl. Sci.*, vol. 15, no. 13, p. 7599, Jul. 2025, doi: 10.3390/app15137599.

[12] M. Cicioğlu and A. Çalhan, "Energy Efficiency Solutions for IEEE 802.15.6 Based Wireless Body Sensor Networks," *Wirel. Pers. Commun.*, vol. 119, no. 3, pp. 1499–1513, Feb. 2021, doi: 10.1007/s11277-021-08292-8.

[13] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723–3766, Fourth Quarter 2019, doi: 10.1109/COMST.2019.2914094.

[14] M. T. T. Bajwa, A. Yousaf, A. Quyyum, F. Tehreem, H. M. F. Tahir, and A. Mehmood, “Optimizing energy efficiency in wireless body area networks for smart health monitoring,” *Spectrum of Engineering Sciences*, vol. 1, no. 7, pp. 1213–1218, Jul. 2025, doi: 10.5281/zenodo.16595651.

[15] L. Tan, K. Yu, A. K. Bashir, *et al.*, “Toward real-time and efficient cardiovascular monitoring for COVID-19 patients by 5G-enabled wearable medical devices: a deep learning approach,” *Neural Comput & Applic*, vol. 35, pp. 13921–13934, Jul. 2023, doi: 10.1007/s00521-021-06219-9.

[16] Z. Wang, A. Shah, H. Lee, and C. H. Lee, “Microfluidic technologies for wearable and implantable biomedical devices,” *Lab Chip*, vol. 25, no. 25, pp. 4542–4576, 2025, doi: 10.1039/d5lc00499c.

[17] Z. Gao, Y. Zhou, J. Zhang, J. Foroughi, S. Peng, R. H. Baughman, Z. L. Wang, and C. H. Wang, “Advanced Energy Harvesters and Energy Storage for Powering Wearable and Implantable Medical Devices,” *Adv. Mater.*, vol. 36, no. 37, p. 2404492, 2024, doi: 10.1002/adma.202404492.

[18] M. Saifuzzaman, T. N. Ananna, M. J. M. Chowdhury, M. S. Ferdous, and F. Chowdhury, “A Systematic Literature Review on Wearable Health Data Publishing under Differential Privacy,” arXiv e-print, arXiv:2109.07334v1, Sep. 2021, doi: 10.48550/arXiv.2109.07334.

[19] G. A. Zendehdel, R. Kaur, I. Chopra, N. Stakhanova, and E. J. Scheme, "Automated Security Assessment Framework for Wearable BLE-enabled Health Monitoring Devices," *ACM Trans. Internet Technol.*, vol. 22, no. 1, pp. 1–27, Feb. 2022, doi: 10.1145/3448649.

[20] L. Hernández-Álvarez, J. J. Bullón Pérez, F. K. Batista, and A. Queiruga-Dios, "Security Threats and Cryptographic Protocols for Medical Wearables," *Mathematics*, vol. 10, no. 6, p. 886, Mar. 2022, doi: 10.3390/math10060886.

[21] A. Barua, M. A. A. Alamin, M. S. Hossain, and E. Hossain, "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 251–281, 2022, doi: 10.1109/OJCOMS.2022.3149732.

[22] M. Terzidis *et al.*, "Challenges in Medical Device Communication: A Review of Security and Privacy Concerns in Bluetooth Low Energy (BLE)," in *Proc. 8th Int. Conf. Cyber-Technol. Cyber-Syst. (CYBER)*, 2023, pp. 69–74. [Online]. Available: https://www.thinkmind.org/library/CYBER/CYBER_2023/cyber_2023_1_110_80054.html. [Accessed: Jan. 2, 2026].

[23] S. A. Khan, H. R. Bajwa, J. Sundaram, Pritika, and B. Shanmugam, "Vulnerability Analysis and Exploitation Attacks on Smart Wearable Devices," in *Proc. 2nd Int. Conf. Adv. Comput. Comput. Technol. (InCACCT)*, 2024, pp. 911–916, doi: 10.1109/InCACCT61598.2024.10550999.

[24] S. Mehdiyev, "Adaptive Protection Against Energy Depletion Attacks in Wearable Medical Devices," in *Proc. 2nd Republican Sci.-Pract. Conf. "Digital Medicine 4.0: Problems, Opportunities and Perspectives"*, Baku, Azerbaijan, May 23, 2025, p. 14, doi: 10.25045/SPCDH4.0.2025.14.

[25] M. Ulloa-Zamora, C. Barría-Huidobro, M. Sánchez-Rubio, and L. Galeazzi, "Integral Security Pillars for Medical Devices: A Comprehensive Analysis," *Appl. Sci.*, vol. 15, no. 12, p. 6634, Jun. 2025, doi: 10.3390/app15126634.

[26] P. K. Sadhu, A. Baul, V. P. Yanambaka, and A. Abdelgawad, "Machine Learning and PUF based Authentication Framework for Internet of Medical Things," in *Proc. Int. Conf. Microelectron. (ICM)*, 2022, pp. 190–193, doi: 10.1109/ICM56065.2022.10005380.

[27] A. Alsuwaidi *et al.*, "Security Vulnerabilities Detected in Medical Devices," in *Proc. 12th Annu. Undergraduate Res. Conf. Appl. Comput. (URC)*, 2020, pp. 1–6, doi: 10.1109/URC49141.2020.9133303.

[28] R. U. Z. Wani, F. Thabit, and O. Can, "Security and privacy challenges, issues, and enhancing techniques for Internet of Medical Things: A systematic review," *Security Privacy*, vol. 7, pp. e409, Apr. 2024, doi: 10.1002/spy2.409.

[29] A. Rajuroy, J. Ngahemelwa, J. Oluwasogo, and O. Isreal, "Data Privacy Risks in Medical Wearable Ecosystems," ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/393361649_Data_Privacy_Risks_in_Medical_Wearable_Ecosystems. [Accessed: Nov. 14, 2025]

[30] O. Isreal, A. Rajuroy, B. Penzenstadler, S. Abrahão, K. Aya, A. Mandal, and B. Matthew, "Medical Data Breaches: Risks from Connected Wearables," *ResearchGate*, 2024. [Online]. Available: https://www.researchgate.net/publication/393362145_Medical_Data_Breaches_Risks_from_Connected_Wearables. [Accessed: Nov. 14, 2025]

[31] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, vol. 33, Art. no. e4049, 2022, doi: 10.1002/ett.4049.

[32] S. K. Shandilya, N. Wagner, and A. K. Nagar, Eds., *Advances in Cyber Security Analytics and Decision Systems*. Cham, Switzerland: Springer Nature Switzerland AG, 2020, doi: 10.1007/978-3-030-19353-9.

[33] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3723–3768, 2019, doi: 10.1109/COMST.2019.2914094.

[34] A. S. George and A. S. H. George, "The Emergence of Cybersecurity Medicine: Protecting Implanted Devices from Cyber Threats," *Partners Universal Innovative Res. Publ. (PUIRP)*, vol. 1, no. 2, pp. 93–111, Nov./Dec. 2023, doi: 10.5281/zenodo.10206563

[35] A. K. Singh and S. Kumar, Eds., *Security, Privacy, and Trust in WBANs and E-Healthcare*. Boca Raton, FL: CRC Press, 2025, doi: 10.1201/9781032635101.

[36] H. S. Anbarasan and J. Natarajan, "Blockchain Based Delay and Energy Harvest Aware Healthcare Monitoring System in WBAN Environment," *Sensors*, vol. 22, no. 15, Art. no. 5763, Aug. 2022, doi: 10.3390/s22155763.

[37] M. M. Ramim, "Security and Privacy of Wearable and Implantable Medical Devices: A Course-Based Approach to Medical Device Cybersecurity Education," *J. Cybersecurity Educ. Res. Pract.*, Manuscript 1275, doi: 10.62915/2472-2707.1275

[38] Ευρωπαϊκή Επιτροπή, “Προστασία δεδομένων στο πλαίσιο του ΓΚΠΔ,” [Online]. Διαθέσιμο: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm.

[39] R. Rak and P. Quinn, *Enhancing digital health innovation in the EU with effective industrial strategy policies – A focus on wearable medical devices*. European Commission: Joint Research Centre, Publications Office of the European Union, 2025, doi: 10.2760/88816.

[40] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (Οδηγία για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες),

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης (EE L), [Online]. Διαθέσιμο: https://eur-lex.europa.eu/eli/dir/2002/58/oj. [Πρόσβαση: Οκτ. 15, 2025]

[41] U.S. Congress, “Health Insurance Portability and Accountability Act of 1996 (HIPAA),” Centers for Disease Control and Prevention (CDC), [Online]. Διαθέσιμο: https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html. [Πρόσβαση: Οκτ. 15, 2025]

[42] A. Sifaoui and M. S. Eastin, "“Whispers from the Wrist”: Wearable Health Monitoring Devices and Privacy Regulations in the U.S.: The Loopholes, the Challenges, and the Opportunities," *Cryptography*, vol. 8, pp. 26, 2024, doi: 10.3390/cryptography8020026.

[43] M. Montell, "Roadmap of cybersecurity regulatory framework for a medical device software," Master's thesis, Faculty of Medicine and Health Technology, Tampere University, Mar. 2025. [Online]. Available: https://urn.fi/URN:NBN:fi:tuni-202503172841. [Accessed: Jan. 2, 2026].

[44] Pritika, B. Shanmugam, and S. Azam, "Risk Assessment of Heterogeneous IoMT Devices: A Review," *Technologies*, vol. 11, no. 1, p. 31, Feb. 2023, doi: 10.3390/technologies11010031.

[45] P. Dobski, "Information security management in the operations of healthcare entities," *Sci. Papers Silesian Univ. Technol. Org. Manage. Ser.*, no. 192, pp. 179–198, 2024, doi: 10.29119/1641-3466.2024.192.11.

[46] *Health informatics — Information security management in health using ISO/IEC 27002*, ISO/DIS Standard 27799, 2025. [Online]. Available: https://www.sls.se/media/ulvkaohc/standardforslag_sistk334-00015.pdf. [Accessed: Jan. 3, 2026].

[47] H. Borges, "HealthSecure’s Comprehensive Cybersecurity Architecture," Course Project, Dept. Sci. Cybersecurity, ECPI Univ., Virginia Beach, VA, USA, May 2025. Available: https://www.researchgate.net/publication/395759398_HealthSecure's_Comprehensive_Cybersecurity_Architecture. [Accessed: Jan. 8, 2026].

[48] *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53, Revision 5, Sep. 2020, doi: 10.6028/NIST.SP.800-53r5.

[49] M. Mannila, "Generalized Patch Delivery Framework for Medical Devices: A Comprehensive Approach to Cybersecurity Compliance and Patch Management," Master's thesis, School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden, Jul. 2025. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1988002&dswid=5946. [Accessed: Jan. 3, 2026].

[50] L. Bracciale, P. Loreti, and G. Bianchi, "Cybersecurity vulnerability analysis of medical devices purchased by national health services," *Sci. Rep.*, vol. 13, p. 19509, Nov. 2023, doi: https://doi.org/10.1038/s41598-023-45927-1.

[51] S. Deb *et al.*, "Securing the Internet of Medical Things (IoMT): Real-World Attack Taxonomy and Practical Security Measures," *Imperial Global Singapore*, Singapore, Jul. 2025, doi: 10.48550/arXiv.2507.19609.

[52] A. Cristobal-Huerta, A. Torrado-Carvajal, C. Rodriguez-Sanchez, J. A. Hernandez-Tamames, M. Luaces, and S. Borromeo, "Implementation of ISO/IEEE 11073 PHD SpO2 and ECG Device

Specializations over Bluetooth HDP following Health Care Profile for Smart Living," *Sensors*, vol. 22, no. 15, p. 5648, 2022, doi: 10.3390/s22155648.

[53] Ó. J. Rubio, J. D. Trigo, Á. Alesanco, L. Serrano, and J. García, "Analysis of ISO/IEEE 11073 built-in security and its potential IHE-based extensibility," *J. Biomed. Inform.*, vol. 60, pp. 270–285, Apr. 2016. doi: 10.1016/j.jbi.2016.02.006.

[54] H. F. Badawi, F. Laamarti, and A. El Saddik, "ISO/IEEE 11073 Personal Health Device (X73-PHD) Standards Compliant Systems: A Systematic Literature Review," *IEEE Access*, vol. 7, pp. 3062–3073, 2019, doi: 10.1109/ACCESS.2018.2886818.

[55] M. Kasparick, S. Schlichting, F. Golatowski, and D. Timmermann, "Medical DPWS: New IEEE 11073 Standard for safe and interoperable Medical Device Communication," *in 2015 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 212–217, 2015, doi: 10.1109/CSCN.2015.7390446.

[56] F. Laamarti, H. F. Badawi, Y. Ding, F. Arafsha, B. Hafidh, and A. El Saddik, "An ISO/IEEE 11073 Standardized Digital Twin Framework for Health and Well-Being in Smart Cities," *IEEE Access*, vol. 8, pp. 105950–105961, 2020, doi: 10.1109/ACCESS.2020.2999871.

[57] N. Goga, A. Vasilateanu, D. Zhong and X. Duan, "Model checking the properties of ISO/IEEE 11073-20601:2016 standard-based communication protocol for personal health device," *2017 IEEE International Systems Engineering Symposium (ISSE)*, Vienna, Austria, 2017, pp. 1-4, doi: 10.1109/SysEng.2017.8088268.

[58] S. K. Kim, T. K. Kim, and H. Lee, "A Novel Transmission Scheme for Compressed Health Data Using ISO/IEEE11073-20601," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 12, pp. 5855–5877, 2017, doi: 10.3837/tiis.2017.12.010

[59] Bluetooth SIG Medical Devices Working Group, "Personal Health Devices Transcoding," Bluetooth SIG White Paper v16, 2015. [Online]. Available: https://www.bluetooth.com/wp-content/uploads/2019/03/PHD_Transcoding_WP_v16.pdf. [Accessed: Oct. 23, 2025].

[60] IEEE Standards Association. Health Informatics—Personal Health Device Communication—Part 10404: Device Specialization—Pulse Oximeter. IEEE Std 11073-10404-2020. [Online]. Available: https://standards.ieee.org/ieee/11073-10404/11099/. [Accessed: Oct. 25, 2025].

[61] IEEE Standards Association. Health Informatics—Device Interoperability—Part 10406: Personal Health Device Communication—Device Specialization—Basic Electrocardiograph (ECG) (1- to 3-lead ECG). IEEE Std 11073-10406-2023. [Online]. Available: https://standards.ieee.org/ieee/11073-10406/6848/. [Accessed: Oct. 29, 2025].

[62] *Health informatics—Device interoperability—Part 10407: Personal health device communication—Device specialization—Blood pressure monitor*, ISO/IEEE 11073-10407:2022(E), Dec. 2022, pp. 1–72. doi: 10.1109/IEEESTD.2022.9984145.

[63] IEEE Standards Association. *Health Informatics—Device Interoperability—Part 10407: Personal Health Device Communication—Device Specialization—Blood Pressure Monitor*, IEEE Std 11073-10407-2022. [Online]. Available: https://standards.ieee.org/ieee/11073-10407/6222/. [Accessed: Oct. 24, 2025].

[64] H. S. Park, H. Cho, and H. S. Kim, "Development of Cell Phone Application for Blood Glucose Self-Monitoring Based on ISO/IEEE 11073 and HL7 CCD," *Healthcare Informatics Research*, vol. 21, no. 2, pp. 83–94, 2015, doi: 10.4258/hir.2015.21.2.83.

[65] S. A. Noman, H. A. Noman, Q. Al-Maatouk, and T. Atkison, "A Survey of IEEE 802.15.6: Body Area Networks," *International Journal of Computing and Digital Systems*, vol. 14, no. 1, pp. 691-705, Sep. 2023. [Online]. Available: http://dx.doi.org/10.12785/ijcds/140153. [Accessed: Oct. 30, 2025].

[66] T. Waheed, A. Rehman, F. K. Shaikh, "IEEE 802.15.6 Relaying Protocol for MBANs," in *Proc. 2021 Mohammad Ali Jinnah Univ. Int. Conf. on Comput. (MAJICC)*, Karachi, Pakistan, 2021, pp. 1-6. doi: 10.1109/MAJICC53071.2021.9526263.

[67] G. Hahn, "Assessing the state of security of Medical BANs and the IEEE 802.15.6 standard," *Master Thesis*, Delft University of Technology and Erasmus Medical Center, Delft, The Netherlands, 2021. [Online]. Available: https://resolver.tudelft.nl/uuid:e570b86d-1e7e-424c-ad36-2692cc74d292. [Accessed: Oct. 31, 2025].

[68] M. A. Siddiqi, G. Hahn, S. Hamdioui, W. A. Serdijn, and C. Strydis, "Improving the Security of the IEEE 802.15.6 Standard for Medical BANs," *IEEE Access*, vol. 10, pp. 62953-62975, June 2022, doi: 10.1109/ACCESS.2022.3181630.

[69] W. J. Long and W. Lin, "An authentication protocol for wearable medical devices," *2017 13th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT)*, Stony Brook, NY, USA, 2017, pp. 1-5, doi: 10.1109/CEWIT.2017.8263140.

[70] S. Al-Sarawi, M. Anbar, K. Alieyan and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," *2017 8th International Conference on Information Technology (ICIT)*, Amman, Jordan, 2017, pp. 685-690, doi: 10.1109/ICITECH.2017.8079928.

[71] Y. S. Choi *et al.*, "A transient, closed-loop network of wireless, body-integrated devices for autonomous electrotherapy," *Science*, vol. 376, no. 6596, pp. 1006–1012, May 2022, doi: 10.1126/science.abm1703.

[72] N. Fatema and R. Brad, “Security requirements, counterattacks and projects in healthcare applications using WSNs—A review,” *Int. J. Comput. Netw. Commun.*, vol. 2, no. 2, pp. 1–9, 2014, doi: 10.48550/arXiv.1406.1795.

[73] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, "Security Vulnerabilities in Bluetooth Technology as Used in IoT," *J. Sens. Actuator Netw.*, vol. 7, no. 3, p. 28, Aug. 2018, doi: 10.3390/jsan7030028.

[74] Liang Zhou. 2017. QoE-Driven Delay Announcement for Cloud Mobile Media. IEEE Trans. Cir. and Sys. for Video Technol. 27, 1 (January 2017), 84–94. [Online]. Available: https://doi.org/10.1109/TCSVT.2016.2539698.

[75] D. S. Bhatti *et al.*, "A Survey on Wireless Wearable Body Area Networks: A Perspective of Technology and Economy," *Sensors*, vol. 22, no. 20, p. 7722, Oct. 2022, doi: 10.3390/s22207722.

[76] M. N. Vadlamudi and A. Hussain, "Design and implementation of energy-aware cross-layer routing protocol for wearable body area network," *Int. J. Pervasive Comput. Commun.*, vol. 18, no. 5, pp. 645–663, 2022. doi: 10.1108/IJPCC-02-2021-0055.

[77] F. Wu, T. Wu, and M. R. Yuce, "An Internet-of-Things (IoT) Network System for Connected Safety and Health Monitoring Applications," *Sensors*, vol. 19, no. 1, p. 21, Jan. 2019. doi: 10.3390/s19010021.

[78] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "WUSTL-EHMS 2020 Dataset for Internet of Medical Things (IoMT) Cybersecurity," Washington University in St. Louis, 2020. [Online]. Available: https://www.cse.wustl.edu/~jain/ehms/index.html. [Accessed: Jan. 15, 2026].

[79] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," *J. Artif. Intell. Res.*, vol. 16, pp. 321–357, Jun. 2002. doi: 10.1613/jair.953.

[80] L. Breiman, "Random Forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, Oct. 2001. doi: 10.1023/A:1010933404324.

ΠΑΡΑΡΤΗΜΑ Α : Κώδικας Υλοποίησης σε Python

Στο παρόν παράρτημα παρατίθεται ο πλήρης κώδικας που αναπτύχθηκε για τις ανάγκες της πειραματικής διαδικασίας της διπλωματικής εργασίας. Η υλοποίηση πραγματοποιήθηκε στη γλώσσα προγραμματισμού Python, κάνοντας χρήση του περιβάλλοντος Google Colab.

```
import pandas as pd
import numpy as np
import time
import matplotlib.pyplot as plt
import seaborn as sns
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.neighbors import KNeighborsClassifier
from sklearn.preprocessing import StandardScaler, LabelEncoder
from sklearn.metrics import (classification_report, confusion_matrix,
                             ConfusionMatrixDisplay, roc_curve, auc)
from imblearn.over_sampling import SMOTE

df = pd.read_csv('WUSTL_EHMS_2020.csv')

le = LabelEncoder()
object_cols = df.select_dtypes(include=['object']).columns
for col in object_cols:
    df[col] = le.fit_transform(df[col].astype(str))

cols_to_drop = ['Label', 'Attack Category', 'SrcAddr', 'DstAddr',
'Sport', 'Dport', 'SrcMac', 'DstMac']
X = df.drop(columns=[col for col in cols_to_drop if col in df.columns])
y = df['Label']

X_train, X_test, y_train, y_test = train_test_split(X, y,
test_size=0.3, random_state=42)
```

```
original_counts = [sum(y_train == 0), sum(y_train == 1)]

sm = SMOTE(random_state=42)
X_train_res, y_train_res = sm.fit_resample(X_train, y_train)

print(f"Dataset size after SMOTE: {len(X_train_res)} samples")

resampled_counts = [sum(y_train_res == 0), sum(y_train_res == 1)]

labels = ['Normal', 'MitM Attack']
x = np.arange(len(labels))
width = 0.35
sns.set_style("whitegrid")
plt.figure(figsize=(10, 6))
plt.bar(x - width/2, original_counts, width, label='Original Data (Imbalanced)', color='#87CEEB')
plt.bar(x + width/2, resampled_counts, width, label='After SMOTE (Balanced)', color='#000080')
plt.ylabel('Number of Samples')
plt.title('Class Distribution Before and After SMOTE')
plt.xticks(x, labels)
plt.legend()
for i, v in enumerate(original_counts):
        plt.text(i - width/2, v + 100, str(v), ha='center', fontweight='bold')
for i, v in enumerate(resampled_counts):
        plt.text(i + width/2, v + 100, str(v), ha='center', fontweight='bold')
plt.tight_layout()
plt.show()

scaler = StandardScaler()
X_train_scaled = scaler.fit_transform(X_train_res)
```

```
X_test_scaled = scaler.transform(X_test)


models = {
                                    "Random        Forest        (Ensemble)":
RandomForestClassifier(n_estimators=100, random_state=42),
    "KNN (Distance-based)": KNeighborsClassifier(n_neighbors=5)
}


results = {}
print("\n--- Algorithm Benchmarking ---")
for name, model in models.items():
    model.fit(X_train_scaled, y_train_res)
    acc = model.score(X_test_scaled, y_test)
    results[name] = acc
    print(f"{name} Accuracy: {acc:.4f}")


plt.figure(figsize=(9, 6))
colors = ['#003f5c', '#ffa600']
bars    =    plt.bar(results.keys(),    results.values(),    color=colors,
width=0.5)
plt.ylim(0.70, 1.0)
plt.ylabel('Accuracy Score')
plt.title('Performance Comparison: Tree-based vs Distance-based')
for bar in bars:
    yval = bar.get_height()
          plt.text(bar.get_x()   +   bar.get_width()/2,   yval   +   0.01,
f'{yval:.4f}', ha='center', fontweight='bold')
plt.show()



final_model = models["Random Forest (Ensemble)"]
y_pred = final_model.predict(X_test_scaled)
```

```
y_probs = final_model.predict_proba(X_test_scaled)[:, 1]

print(classification_report(y_test, y_pred))

cm = confusion_matrix(y_test, y_pred)
tn, fp, fn, tp = cm.ravel()

print("--- Confusion Matrix Values ---")
print(f"True Negatives (TN): {tn}")
print(f"False Positives (FP): {fp}")
print(f"False Negatives (FN): {fn}")
print(f"True Positives (TP): {tp}")


total = tn + fp + fn + tp
accuracy = (tn + tp) / total
print(f"\nCalculated Accuracy: {accuracy:.4f}")

cm = confusion_matrix(y_test, y_pred)
plt.figure(figsize=(8, 6))
disp = ConfusionMatrixDisplay(confusion_matrix=cm,
display_labels=['Normal', 'Attack'])
disp.plot(cmap=plt.cm.Blues)
plt.title('Confusion Matrix (Random Forest)')
plt.show()

fpr, tpr, _ = roc_curve(y_test, y_probs)
roc_auc = auc(fpr, tpr)
plt.figure(figsize=(8, 6))
plt.plot(fpr, tpr, color='darkorange', lw=2, label=f'ROC curve (AUC =
{roc_auc:.2f})')
plt.plot([0, 1], [0, 1], color='navy', lw=2, linestyle='--')
```

```
plt.xlabel('False Positive Rate')
plt.ylabel('True Positive Rate')
plt.title('Receiver Operating Characteristic (ROC) Curve')
plt.legend(loc="lower right")
plt.show()

importances = final_model.feature_importances_
indices = np.argsort(importances)[-10:]
plt.figure(figsize=(10, 6))
plt.title('Top 10 Feature Importance (Network & Biometric)')
plt.barh(range(len(indices)), importances[indices], color='teal',
align='center')
plt.yticks(range(len(indices)), [X.columns[i] for i in indices])
plt.xlabel('Relative Importance Score')
plt.show()

num_samples = 1000
test_samples = X_test_scaled[:num_samples]
latencies = []

for i in range(10):
    start_time = time.time()
    final_model.predict(test_samples)
    end_time = time.time()

    # Latency per sample in milliseconds (ms)
    iter_latency = ((end_time - start_time) * 1000) / num_samples
    latencies.append(iter_latency)

plt.figure(figsize=(10, 5))
plt.plot(range(1, 11), latencies, marker='o', linestyle='-',
color='green', lw=2)
```

```
plt.axhline(y=np.mean(latencies),      color='red',      linestyle='--',
label=f'Mean: {np.mean(latencies):.4f} ms')
plt.xlabel('Iteration Number')
plt.ylabel('Time (ms)')
plt.title('Detection Latency Stability (10 Iterations)')
plt.legend()
plt.grid(True, linestyle='--', alpha=0.7)
plt.tight_layout()
plt.show()

print(f"\n[Final Results Summary]")
print(f"Mean Latency: {np.mean(latencies):.6f} ms")
print(f"Standard Deviation: {np.std(latencies):.6f} ms")
```