



Ιόνιο Πανεπιστήμιο
Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής
Τμήμα Πληροφορικής
Ανθρωπιστικές και Κοινωνικές Επιστήμες

Επισκόπηση των Μεθοδολογιών Ανίχνευσης και
Αποφυγής των Αδυναμιών Ασφαλείας σε
Συστήματα IoMT

Πτυχιακή Εργασία
του
Αριστοτέλη Συμεωνίδη

Τριμελής Επιτροπή:

Εμμανουήλ Μάγκος

Αγγελική Τσώχου

Βασίλειος Χρυσικόπουλος

Αναπληρωτής Καθηγητής,
Επιβλέπων

Επίκουρη Καθηγήτρια

Καθηγητής - Πρύτανης Ι.Π

Κέρκυρα, 2019

Επισκόπηση των Μεθοδολογιών Ανίχνευσης και
Αποφυγής των Αδυναμιών Ασφαλείας σε
Συστήματα IoMT

Αριστοτέλης Συμεωνίδης
p15syme@ionio.gr

24 Σεπτεμβρίου 2019

Περίληψη

Η αγορά της τεχνολογίας Internet-of-Things (IoT) αναπτύσσεται ταχύρρυθμα τα τελευταία χρόνια, με αποτέλεσμα την χρήση της σε πληθώρα τομέων όπως στα στρατιωτικά συστήματα (Internet of Battlefield Things (IoBT)), το τομέα των μετακινήσεων (Internet of Vehicle Things (IoVT)) και τον ιατρικό τομέα (Internet of Medical Things (IoMT)). Η περίπτωση των IoMT παρουσιάζει εξαιρετικό ενδιαφέρον, καθώς ο σκοπός τους είναι η βελτίωση των προσφερόμενων ιατροφαρμακευτικών υπηρεσιών σε επίπεδο χρηστών (ασθενών και επαγγελματιών υγείας) και σε επίπεδο συστήματος (με τον αυτοματισμό λειτουργιών και την ενημέρωση του συστήματος).

Σκοπός της παρούσας Πτυχιακής Εργασίας είναι η καταγραφή και μελέτη των συστημάτων ασφάλειας στις τεχνολογίες IoMT, αναδεικνύοντας τα πλεονεκτήματα τους και αναζητώντας τα πιθανά κενά ασφάλειας. Ταυτόχρονα, εξετάζεται η εγκυρότητα της χρήσης αποκεντρωμένων τεχνικών ασφάλειας για την ενίσχυση των συστημάτων IoMT.

Αρχικά, έγινε η σκιαγράφηση των IoMT καταγράφοντας την αρχιτεκτονική των συστημάτων και τους διαφορετικούς τύπους συσκευών. Έπειτα, αναλύθηκαν τα προβλήματα που φέρουν τα IoMT όσον αφορά τη πληθώρα ευπαθειών που μπορεί να υπάρχουν, τις αδυναμίες και τις συνέπειες που επιφέρουν στους χρήστες και το σύστημα. Γίνεται ξεχωριστή ανάλυση για τις διαφορετικές τεχνολογίες και τα πρωτόκολλα που χρησιμοποιούνται στα IoMT συστήματα. Στη συνέχεια, καταγράφονται οι γενικότερες απαιτήσεις σε επίπεδο ασφάλειας και ιδιωτικότητας ξεχωριστά, που είναι θεμιτό να ικανοποιηθούν στα IoMT συστήματα, δίνοντας έμφαση σε αυτές που προκύπτουν από τα καταγεγραμμένα προβλήματα. Επισημειώνονται τα μέτρα και αντίμετρα της προτεινόμενης βιβλιογραφίας ανακαλύπτοντας τυχόν κενά που μπορεί υπάρχουν. Τέλος, ως εναλλακτική προσέγγιση αναφέρονται τα μέτρα ασφάλειας με αποκεντρωμένο χαρακτήρα, τα οποία έχουν ως βάση την τεχνολογία Blockchain διακρίνοντας τα πλεονεκτήματα και μειονεκτήματα της.

Η συνεισφορά της Πτυχιακής Εργασίας έγκειται στην συγκεντρωτική μελέτη των αποκεντρωμένων προσεγγίσεων στα συστήματα IoMT που είναι διαθέσιμα στη προτεινόμενη βιβλιογραφία, εξετάζοντας αν είναι κατάλληλες για αυτά. Ένα μεγάλο ζήτημα για τα συστήματα IoMT είναι η αντιμετώπιση των trade-offs μεταξύ της υπολογιστικής απόδοσης και της ορθής εκμετάλλευσης των ενεργειακών πόρων. Οι αποκεντρωμένες προσεγγίσεις, ενώ αντιμετωπίζουν σημαντικά ζητήματα στα συστήματα IoMT, αφήνουν κενά όσον αφορά την ιδιωτικότητα του χρήστη και την συνολική απόδοση του συστήματος. Έτσι, οι συγγραφείς προτείνουν ένα νέο μέτρο με βάση την τεχνολογία Blockchain, το οποίο εκμεταλλεύεται τα πλεονεκτήματα της για την διασφάλιση των συστημάτων IoMT και ταυτόχρονα προτείνει λύσεις οι οποίες μετριάζουν τα ζητήματα ασφάλεια που προκύπτουν στα συστήματα IoMT που χρησιμοποιούν αποκεντρωμένες λύσεις.

Ευχαριστίες

Θα ήθελα καταρχήν να ευχαριστήσω τον καθηγητή κ. Εμμανουήλ Μάγκο για την επίβλεψη αυτής της Πτυχιακής Εργασίας και για την ευκαιρία που μου έδωσε να την εκπονήσω στο Εργαστήριο Δικτύων, Πολυμέσων και Ασφάλειας Συστημάτων (NMSLab). Επίσης, ευχαριστώ ιδιαίτερα τον υποψήφιο διδάκτορα Στυλιανό Καραγιάννη για την καθοδήγησή του και την εξαιρετική συνεργασία που είχαμε. Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου για την καθοδήγηση και την ηθική συμπαράσταση που μου προσέφεραν όλα αυτά τα χρόνια.

Στην οικογένειά μου...

Κεφάλαιο 1

Εισαγωγή

Η αγορά των Internet-of-Things (IoT) τα τελευταία χρόνια αναπτύσσεται ταχύρρυθμα εκτιμώντας ότι το 2020 θα υπάρχουν πάνω από 25 εκατομμύρια συσκευές παγκοσμίως (Yu et al., 2015), μετατρέποντας έτσι την έννοιά σε Internet-of-Everything (IoE), με τη προσθήκη του ανθρώπινου παράγοντα (Chen et al., 2014). Τα συστήματα IoT αποτελούν το πυλώνα της επόμενης γενιάς τεχνολογιών, οι οποίες θα διαμορφώσουν το επαγγελματικό φάσμα και θα θεωρηθούν ως η σύνδεση των μοναδικά αναγνωρίσιμων συσκευών με το διαδίκτυο και τα ευρύτερα οφέλη του (Islam et al., 2015). Γενικότερα, τα IoT είναι η σύνδεση ετερογενών δικτύων και των πληροφοριών πλαισίου τους, με σκοπό να αλληλοσυμπληρώνονται οι συσκευές, και να δημιουργήσουν ένα δίκτυο πληροφοριών, παρέχοντας εξειδικευμένες και 'έξυπνες' υπηρεσίες στον τελικό χρήστη (Alaba et al., 2017).

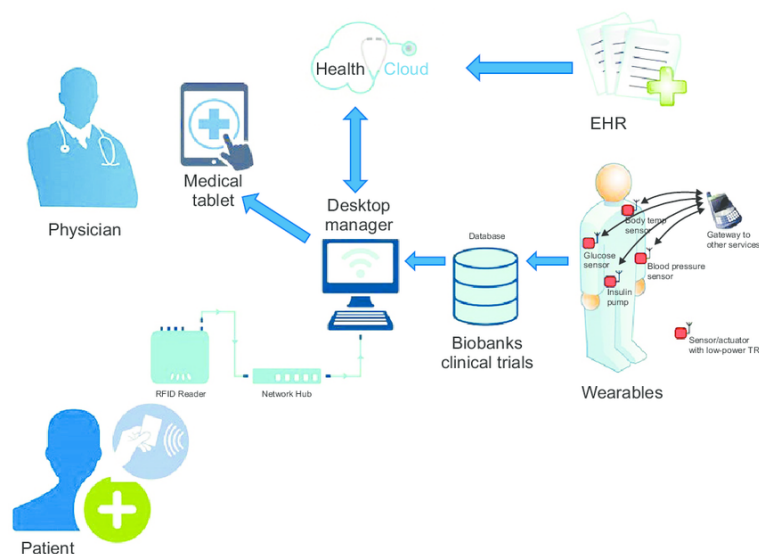
Τα συστήματα IoT έχουν δείξει ότι μπορούν να παίξουν καθοριστικό ρόλο, με τη χρήση τους σε βιομηχανικά συστήματα υψηλού κινδύνου όσον αφορά το Περιβάλλον, την Υγεία και την Ασφάλεια (high-risk Environment, Health, and Safety (EHS)), δηλαδή σε αυτών, που η ανθρώπινη ζωή κατέχει κρίσιμο ρόλο στις προσφερόμενες υπηρεσίες (Thibaud et al., 2018). Καταλήγοντας, έρχονται να ενισχύσουν τον τομέα της ιατρικής, δημιουργώντας μία νέα υπό κατηγορία συστημάτων, τα Internet-of-Medical-Things (IoMT).

Το δίκτυο που διασυνδέει τα συστατικά των συστημάτων IoMT, περιλαμβάνει συχνά ένα μεγάλο αριθμός συσκευών και αισθητήρων, όπου λαμβάνουν μετρήσεις ζωτικών δεδομένων σε πραγματικό χρόνο. Τα δίκτυα IoMT αποτελούνται από τον συνδυασμό δικτύων όπως Δίκτυα Προσωπικού Χώρου (Personal Area Networks - PAN) και Τοπικά Δίκτυα (Local Area Networks - LAN), όπου συσκευές βρίσκονται μέσα ή πάνω στο σώμα του ασθενούς, ενώ υπάρχουν και συσκευές που παίρνουν μετρήσεις από το περιβάλλοντα χώρο τους -όπως στη περίπτωση των πασχόντων ασθενών με άνοια, όπου χρησιμοποιούνται οι εν λόγω συσκευές δημιουργώντας μοτίβα των κινήσεων τους, με σκοπό την ενεργοποίηση συναγερμών, σε περιπτώσεις ύποπτων κινήσεων-.

Επειδή γίνεται λόγος για ασύρματα δίκτυα, οι όροι αναβαθμίζονται σε Ασύρματα Προσωπικά και Τοπικά Δίκτυα αντίστοιχα (Wireless PAN - WPAN, Wireless LAN - WLAN). Για την απομακρυσμένη επικοινωνία των συσκευών του ασθενούς, χρησιμοποιούνται δίκτυα μεγαλύτερης εμβέλειας, όπως Δίκτυα Ευρείας Περιοχής (Wide Area Networks (WAN)) και Μητροπολιτικά Δίκτυα (Metropolitan Area Networks (MAN)), συνδυαστικά με το ιδιωτικό δίκτυο του ασθενούς, δημιουργώντας ένα υβριδικό μοντέλο, με σκοπό τον διαμοιρασμό των μετρήσεων των δεδομένων που προέρχονται από τον ασθενή

(Dey et al., 2017).

Η αποδοχή της τεχνολογία IoMT, ακολουθεί τα πρότυπα των συστημάτων IoT. Στον χώρο της ιατρικής έρχονται για να αναβαθμίσουν την ποιότητα και την φροντίδα των ασθενών, προσφέροντας επικοινωνία σε πραγματικό χρόνο (real-time) των ασθενών με τους επαγγελματίες υγείας ή με τους φροντιστές τους, περιορίζοντας τα κόστη, και χρησιμοποιώντας νέες τεχνολογίες για την περισυλλογή, ανάλυση και το διαμοιρασμό πληροφοριών. Με τον πολλαπλασιασμό των συσκευών IoT που διατίθενται στην αγορά, σε συνδυασμό με την υπολογιστική ισχύ των συσκευών, δίνουν λύσεις στις ανάγκες του γηράσκοντος πληθυσμού και των χρόνιων παθήσεων (Gatoullat et al., 2018). Οι εφαρμογές των IoMT, φέρνουν αλλαγές και στην περίθαλψη των ασθενών που πάσχουν από νευροεκφυλιστικές ασθένειες, αναλύοντας τα εγκεφαλικά κύματα και τις εναλλαγές των συναισθημάτων τους, αλλά και για άτομα που πάσχουν από προβλήματα παχυσαρκίας και καρδιαγγειακά προβλήματα (Banerjee et al., 2018). Χαρακτηριστικό παράδειγμα αποτελούν οι πάσχοντες της νόσου Alzheimer, όπου δίνεται η δυνατότητα μέσω της τεχνολογίας RFID να γνωρίζουν την τοποθεσία του ανά πάσα στιγμή (Chen et al., 2017). Στο Σχ. 1.1 διακρίνεται το γενικότερο πεδίο εφαρμογών των IoMT. Η διάδραση του ασθενούς (Patient) με τον επαγγελματία υγείας (Physician) γίνεται εξ αποστάσεως, για τον διαμοιρασμό των προσωπικών δεδομένων του (Biobanks clinical trials), τη διαχείριση του ιατρικού φακέλου του ασθενούς (EHR), όπως επίσης και τη παρακολούθηση ασθενούς με τη χρήση αισθητήρων (Wearables), που παρακολουθούν τα ζωτικά δεδομένα του ασθενούς.



Σχήμα 1.1: Τυπική απεικόνιση των εφαρμογών των Internet of Things (IoT) στις ιατρικές υπηρεσίες. Medical Internet of Things and Big Data in Healthcare - Scientific Figure on ResearchGate. Available from: www.researchgate.net/figure/An-illustration-of-how-this-revolution-in-medicine-will-look-in-a-typical-Internet-of_fig1_306022306

Ωστόσο, στις προσφερόμενες υπηρεσίες, το πλήθος των ιατρικών πληροφοριών που ανταπεξέρχονται σε αυτού του είδους την επεξεργασία ενδέχεται να αγγίζει κατά προσέγγιση, το 2025 τα 180 zettabytes (Akmandor et al., 2018). Λαμβάνοντας υπόψη ότι τα δεδομένα που ανταλλάσσονται μεταξύ των συσκευών και του δικτύου είναι ευαίσθητα, έγκειται η ανάγκη της υλοποίηση ασφαλών καναλιών επικοινωνίας, διότι η έκθεση και η αθέμιτη χρήση τους από τρίτες οντότητες, μπορεί να φέρει σε κίνδυνο

τόσο τη ζωή των ασθενών - δημιουργώντας κοινωνικά προβλήματα, τα οποία μπορεί να οδηγήσουν και στην απώλεια της δουλείας του - όσο και την λειτουργικότητα του συστήματος (Al-Janabi et al., 2017).

Τα δίκτυα επικοινωνίας των συσκευών IoMT γίνονται στόχος κακόβουλων επιθέσεων, λόγω των τεράστιων μεγεθών ευαίσθητων δεδομένων, τα οποία διακινούνται. Έτσι, για τους παραπάνω λόγους δημιουργήθηκαν πρωτόκολλα και αρχιτεκτονικές, με τα οποία διασφαλίζεται η επικοινωνία των συστημάτων IoT σε Φυσικό επίπεδο και επίπεδο Δικτύου. Οι τεχνολογίες πρέπει να προσφέρουν την απαιτούμενη ασφάλεια όσον αφορά την *Εμπιστευτικότητα*, *Ακεραιότητα*, *Διαθεσιμότητα* και *Αυθεντικότητα* των δεδομένων. Επιπλέον, πρέπει να λαμβάνουν υπόψη την *Ιδιωτικότητα* των ευαίσθητων δεδομένων, τα οποία θα συμμορφώνονται με τις οδηγίες του νέου Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR). Ωστόσο, οι πρόσφατες προτεινόμενες τεχνολογίες, δεν καλύπτουν όλες τις απαιτούμενες ανάγκες, οδηγώντας στη δημιουργία κενών ασφαλείας στα συστήματα αυτά.

Η *Πτυχιακή Εργασία* εντάσσεται στο τεχνολογικό πλαίσιο. Στη Πτυχιακή Εργασία γίνεται ανάλυση των μέτρων ασφάλειας στα συστήματα IoMT, διακρίνοντας τις ελλείψεις που υπάρχουν σε επίπεδο Ασφάλειας και Ιδιωτικότητας με σκοπό την διερεύνηση νέων προσεγγίσεων με τη χρήση της τεχνολογίας Blockchain. Έπειτα, οι συγγραφείς προτείνουν το δικό τους μοντέλο βασισμένο στην τεχνολογία Blockchain. Το αντικείμενο των συστημάτων IoMT βρίσκεται στις ανερχόμενες τεχνολογίες που θα απασχολήσουν την αγορά τα επόμενα χρόνια, έτσι χρήζουν σημαντική προσοχή, καθώς επεξεργάζονται ευαίσθητα προσωπικά δεδομένα.

1.1 Τελευταίες Έρευνες

Οι Gatouillat et al., 2015 εκτελούν αναλυτική περιγραφική ανασκόπηση της βιβλιογραφίας, η οποία επικεντρώνεται στην βελτίωση των ιατρικών υπηρεσιών με τη χρήση των συστημάτων IoMT και πιο συγκεκριμένα των Φυσικών Συστημάτων του Κυβερνοχώρου (Cyber Physical Systems - CPS). Αναφέρονται στη ταξινόμηση και τις εφαρμογές των συστημάτων, στις απαιτήσεις ασφάλειας και στις προκλήσεις που θα κληθούν να αντιμετωπίσουν οι συσκευές IoMT. Αναφέρονται σε ένα σύνολο μέτρων ασφάλειας, όπου ο σχεδιασμός του συστήματος είναι έχει ως επίκεντρο τις προσφερόμενες υπηρεσίες (Service-Oriented Architecture - SOA). Ωστόσο δεν περιγράφουν καθόλου τεχνολογίες όπως αυτές του Blockchain. Επιπλέον, η συγκεκριμένη εργασία αναφέρεται σε ένα σύνολο γενικών μέτρων ασφάλειας και δεν επικεντρώνονται σε συγκεκριμένες αρχιτεκτονικές ή μοντέλα.

Οι Khan et al., 2018, μέσω της αφηγηματικής ανασκόπησης στη βιβλιογραφία, εντοπίζουν το σύνολο των βασικών προκλήσεων, που αφορούν τα συστήματα IoT. Αναφέρονται οι πιθανές απειλές αντιστοιχώντας τα μέτρα ασφαλείας, που προτείνονται από τη βιβλιογραφία με τα οποία προσπαθούν να τις αντιμετωπίσουν. Τέλος, προτείνουν από τη βιβλιογραφία μεθόδους που αφομοιώνουν την τεχνολογία Blockchain ως τρόπο αντιμετώπισης των άμεσων απειλών για τα συστήματα IoT. Η συγκεκριμένη εργασία έχει πανομοιότυπη δομή με την εν λόγω εργασία, ωστόσο η *Πτυχιακή Εργασία* επικεντρώνεται αποκλειστικά στα συστήματα IoMT. Επεκτείνεται στην περιγραφή της αρχιτεκτονικής και τοπολογίας των συστημάτων IoMT, στα προβλήματα που αντιμετωπίζουν, τις επιπτώσεις που επιφέρουν και τις απαιτήσεις που προκύπτουν σε αυτά.

Δίνεται έμφαση στα προτεινόμενα μέτρα ασφάλειας και στις state-of-the-art προσεγγίσεις με αντικείμενο τη τεχνολογία Blockchain.

Οι Gulraiz et al., 2017, κάνοντας αφηγηματική ανασκόπηση της βιβλιογραφίας, παρουσιάζουν το σύνολο των εργασιών, που χρησιμοποιούν την τεχνολογία των IoT για τη βελτίωση των προσφερόμενων υπηρεσιών στα ιατρικά συστήματα. Επισημαίνουν τα πλεονεκτήματα της εφαρμογής τους, τομείς στους οποίους δραστηριοποιούνται οι συσκευές IoT στις ιατρικές υπηρεσίες και ένα πλήθος προκλήσεων που προκύπτουν. Σε αντίθεση με την Πτυχιακή Εργασία, η εν λόγω εργασία δεν αναφέρεται εκτενώς στις απειλές που αντιμετωπίζουν τα συστήματα IoMT, ενώ δεν αναφέρεται καθόλου στις απαιτήσεις των συστημάτων και στα μέτρα ασφάλειας που εφαρμόζονται. Τέλος, η Πτυχιακή Εργασία εξετάζει τα μέτρα ασφάλειας που χρησιμοποιούν τη Blockchain τεχνολογία, αντικείμενο με το οποίο δεν ασχολείται η παραπάνω εργασία.

1.2 Μεθοδολογία

Η Πτυχιακή Εργασία αποτελεί βιβλιογραφική επισκόπηση συλλέγοντας πληθώρα ερευνητικών εργασιών, οι οποίες αναφέρονται στα συστήματα IoMT στο τρόπο επικοινωνίας, στην αλληλεπίδραση των συσκευών και στη δομή των δικτύων. Επιπλέον, μελετήθηκαν επιστημονικά συγγράμματα, που επικεντρώνονται στη δομή των δικτύων και της ασφάλειά τους με απώτερο σκοπό την καλύτερη κατανόηση τους.

Η μελέτη της σχετικής βιβλιογραφίας έγινε με σκοπό την ανάδειξη των προβλημάτων, που αντιμετωπίζουν οι τεχνολογίες των συστημάτων IoMT, τις απαιτήσεις που απορρέουν από αυτό, και την αξιολόγηση των προτεινόμενων λύσεων. Εντοπίζονται τα πλεονεκτήματα και τα κενά ασφάλειας στις προτεινόμενες λύσεις, με σκοπό την μελέτη των προσεγγίσεων που βασίζονται στην τεχνολογία Blockchain:

- Δημοσιεύσεις και άρθρα:
 - που αναφέρονται στον τρόπο λειτουργίας των συσκευών IoT, στην αρχιτεκτονική τους, στη ταξινόμηση των πρωτοκόλλων που χρησιμοποιούνται για την επικοινωνία των συσκευών,
 - που αναφέρονται στα συστήματα IoMT, τις υποκατηγορίες τους, πώς και πού χρησιμοποιούνται, το αντίκτυπο που έχουν στη κοινωνία,
 - που κάνουν λόγο για τα δίκτυα και τις τεχνολογίες που χρησιμοποιούνται για την επικοινωνία των συσκευών IoMT,
 - που παρέχουν χαρακτηριστικά παραδείγματα εφαρμογών των συστημάτων IoMT σε ιατρικές εφαρμογές,
 - που μελετάνε τις απειλές στις οποίες είναι επιρρεπή τα συστήματα IoMT
 - που μελετάνε το τρόπο διασφάλισης των δικτύων και συσκευών IoMT, αναδεικνύοντας τα προβλήματα των υπάρχοντων συστημάτων ασφάλειας,
 - που αναφέρουν το σύνολο των απαιτήσεων που πρέπει να πληρούν τα συστήματα IoMT για να διασφαλίζονται τα ευαίσθητα προσωπικά δεδομένα των χρηστών,
 - άρθρα που επικεντρώνονται στην εφαρμογή της τεχνολογίας Blockchain στα συστήματα IoT, δίνοντας έμφαση στις μελέτες που επικεντρώνονται στις ιατρικές εφαρμογές.

- Συγγράμματα και άρθρα, με τα οποία γίνεται καλύτερη η κατανόηση των προτύπων και των πρωτοκόλλων που χρησιμοποιούνται στα συστήματα IoMT. Άρθρα, που περιγραφούν αναλυτικά τις πτυχές και τα χαρακτηριστικά των τεχνολογιών αυτών,
- Έρευνες και άρθρα, οι οποίες προέκυψαν από πειραματικές δοκιμές Penetration Testing (PT) σε συστήματα και συσκευές IoT και IoMT.
 - Στόχος των PT, είναι η ανακάλυψη των αδυναμιών στις μεθόδους ασφαλείας για τα συστήματα IoMT και του τρόπου με τον οποίο τα κακόβουλα λογισμικά επιτίθενται και παρεμβαίνουν.

1.3 Στόχοι

Η συγγραφή της παρούσας Πτυχιακής Εργασίας (ΠΕ), στοχεύει στην καταγραφή και μελέτη των μεθόδων ανίχνευσης και αποφυγής αδυναμιών στα συστήματα IoMT. Αυτό περιλαμβάνει:

- Την ανάλυση και ταξινόμηση των συστημάτων IoMT, τα χαρακτηριστικά της δομής των δικτύων που χρησιμοποιούνται, των πρωτοκόλλων και της διαδικασίας με τα οποία εκτελείται η επικοινωνία,
- Την καταγραφή των απειλών, αδυναμιών και συνεπειών, που αντιμετωπίζουν οι τεχνολογίες που χρησιμοποιούνται στα συστήματα IoMT, τα πρωτόκολλα επικοινωνίας και οι συσκευές IoMT. Αναφέρονται τα κενά και οι προκλήσεις που προκύπτουν στην ασφάλεια των συστημάτων,
- Καταγραφή των απαιτήσεων που υπάρχουν στα συστήματα IoMT, όσον αφορά την ασφάλεια και την ιδιωτικότητα τους με γνώμονα και τα προβλήματα που αναγνωρίστηκαν,
- Την ανάλυση των προτεινόμενων μεθοδολογιών πρόληψης, αποφυγής, ανίχνευσης και αντιμετώπισης των προκλήσεων, που είναι διαθέσιμες στην βιβλιογραφία, εξετάζοντας το σύνολο των απαιτήσεων που ικανοποιούνται και την εύρεση πιθανών κενών ασφάλειας,
- Μελέτη νέων προσεγγίσεων για την διασφάλιση των συστημάτων IoMT, με επίκεντρο την αποκεντρωμένη τεχνολογία Blockchain. Αναλύονται πλήρως τα συστατικά των συστημάτων αυτών, εξετάζοντας τα πλεονεκτήματα και τα μειονεκτήματά τους, και ο βαθμός χρηστικότητάς τους στα συστήματα IoMT σε σύγκριση με τις προηγούμενες μεθόδους,
- Την πρόταση μιας καινούργιας προσέγγισης με αποκεντρωμένο χαρακτήρα, στα πρότυπα της τεχνολογίας Blockchain, η οποία βρίσκεται σε πρωταρχικό στάδιο.

Εφόσον η Πτυχιακή Εργασία, έχει αναφορικό ρόλο, το *ερευνητικό ερώτημα* που τίθεται, επικεντρώνεται στην αξιολόγηση των συγκεκριμένων μεθοδολογιών.

1.4 Συνεισφορά

Η Πτυχιακή Εργασία αποτελεί βιβλιογραφική ανασκόπηση (Critical Review), με σκοπό την παροχή κριτικής αξιολόγησης και ερμηνευτικής ανάλυσης της υπάρχουσας βιβλιογραφίας για τα συστήματα των IoMT και την αποκάλυψη των ισχυρών

και αδύναμων σημείων και κενών σε σχέση με τις θεωρίες, τις υποθέσεις, τις ερευνητικές μεθόδους ή τα αποτελέσματα. Εξετάζεται το ευρύ φάσμα υφιστάμενων ερευνών, με στόχο η εργασία να αποτελέσει σημείο παραπομπής για τα υπάρχοντα μοντέλα, στην ανάλυσή τους, στην καταγραφή των απειλών που αντιμετωπίζουν και στη μελέτη νέων προσεγγίσεων. Επόμενα, η συνεισφορά της εργασίας στοχεύει:

- Στην αναλυτική καταγραφή των μέτρων ασφάλειας που λαμβάνονται στα IoMT συστήματα, στην ανακάλυψη κενών ασφαλείας και παραληήψεων,
- Στην εξέταση και ανάλυση της τεχνολογίας Blockchain ως εναλλακτική προσέγγιση για την διασφάλιση των συστημάτων IoMT,
- Στην πρόταση ενός νέου μέτρου ασφάλειας με αποκεντρωμένο χαρακτήρα, που θα ικανοποιεί το σύνολο των απαιτήσεων, τις οποίες αδυνατούν να καλύψουν οι προτεινόμενες λύσεις.

Για να επιτευχθεί αυτό, μελετήθηκε λεπτομερώς η βιβλιογραφία, που αναφέρεται στη δομή των συστημάτων IoMT, στις προτεινόμενες τεχνολογίες για τις συσκευές, στα μέσα που χρησιμοποιούνται για την διασφάλισή τους και σε έρευνες που εκτέλεσαν Δοκιμές Διείσδυσης (PT) στα υπάρχοντα μοντέλα.

1.5 Ενδεικτική Δομή

Η πτυχιακή εργασία δομείται ως εξής: στο *Κεφάλαιο 2* αναφέρονται λεπτομερώς οι τύποι των συσκευών και η δομή της αρχιτεκτονικής των συστημάτων IoMT, στο *Κεφάλαιο 3* καταγράφονται οι απειλές, οι αδυναμίες και τα οι συνέπειες που επιφέρονται στα δίκτυα IoMT, στο *Κεφάλαιο 4* αναγράφονται οι απαιτήσεις που πρέπει να πληρούν τα συστήματα IoMT, για την διευθέτηση των προβλημάτων που αντιμετωπίζουν.

Στο *Κεφάλαιο 5* παραθέτονται οι υπάρχουσες λύσεις και τεχνολογίες ασφαλείας οι οποίες είναι θεμιτό να ικανοποιούν τις απαιτήσεις του προηγούμενου κεφαλαίου, στο *Κεφάλαιο 6* μελετάται η χρήση αποκεντρωμένων συστημάτων ασφαλείας με βάση τη τεχνολογία Blockchain παρουσιάζοντας ένα καινούργιο μέτρο ασφαλείας στα ίδια πρότυπα, και στο *Κεφάλαιο 7* γίνεται η σύνοψη της Πτυχιακής Εργασίας και αναφέρεται ένα σύνολο ανοιχτών ζητημάτων. Τέλος, παρατίθεται η *Βιβλιογραφία* της Πτυχιακής Εργασίας, ο κατάλογος των Πινάκων (Παράρτημα Α) και των Σχημάτων (Παράρτημα Β).

Κεφάλαιο 2

Η Τύποι Συσκευών και η Αρχιτεκτονική των Συστημάτων IoMT

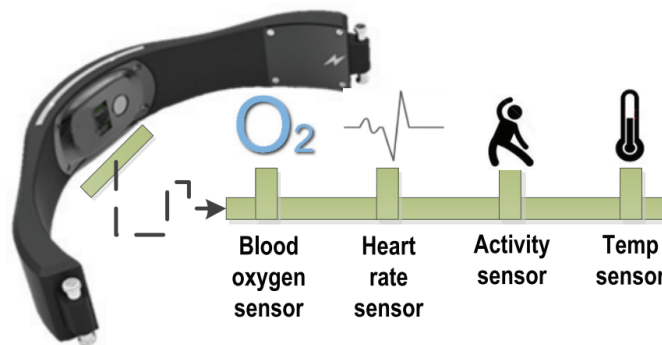
Η κατηγορία των συστημάτων IoT αποτελείται από ένα ευρύ φάσμα συσκευών, συμπεριλαμβάνοντας εμπορικές wristbands, smartwatches και έξυπνες οικιακές συσκευές, μέχρι και πιο εξειδικευμένες, οι οποίες βρίσκονται είτε σε πειραματικό ή παραγωγικό στάδιο, και παίρνουν μετρήσεις, αξιοποιώντας τους αισθητήρες που διαθέτουν. Οι συσκευές αυτές επικοινωνούν άμεσα με τη χρήση πρωτοκόλλων επικοινωνίας, χωρίς την παρέμβαση τρίτου παράγοντα, όπως ο ανθρώπινος παράγοντας ή μία υπολογιστική οντότητα. Με τη χρήση του διαδικτύου, τα δίκτυα IoT δεν καλύπτουν μία ενιαία λειτουργικότητα, αλλά αλληλεπιδρούν με το σύστημα χρησιμοποιώντας τεχνικές τεχνητής νοημοσύνης (AI), προσφέροντας περισσότερες και πιο εξειδικευμένες υπηρεσίες (Akmandor et al., 2018). Έτσι, εκμεταλλευόμενοι τις καινοτόμες τεχνολογίες των IoT, εμφανίζονται τα συστήματα IoMT στο τομέα της ιατρικής, για να προσφέρουν καλύτερες και πιο οικονομικές υπηρεσίες υγείας στον ασθενή. Στο κεφάλαιο που ακολουθεί, καταγράφονται οι διαφορετικοί τύποι συσκευών, που χρησιμοποιούνται στα συστήματα IoMT και αναλύεται η αρχιτεκτονική των δικτύων, στα οποία τα συστήματα λειτουργούν.

2.1 Τύποι Συσκευών στα Συστήματα IoMT

Τα συστήματα IoMT διαμορφώνουν ένα δικτυακό σύνολο, το οποίο αποτελείται από μικροσυσκευές και αισθητήρες με σκοπό την παροχή ιατρικών υπηρεσιών σε έναν ασθενή, αυτοματοποιώντας διαδικασίες ή λειτουργώντας ως βοηθήματα στους επαγγελματίες υγείας. Οι συσκευές IoMT χρησιμοποιούνται είτε στις οικίες των ασθενών, είτε εντός των νοσοκομειακών μονάδων. Σύμφωνα με τους Monassaghi et al. 2014, οι συσκευές ανάλογα με το σκοπό και τη χρήση τους χωρίζονται σε τρεις τύπους. Οι Wearables, ή διαφορετικά συσκευές που φοριούνται, οι Εμφυτευμένες (IMD) και τέλος οι συσκευές που χρησιμοποιούνται για την παρακολούθηση του χώρου των ασθενών.

1. **Φορετές Συσκευές (Wearables):** Λειτουργεί για κάθε άνθρωπο ως εποπτικό μέσο για την παρακολούθηση των αποδόσεων του σε καθημερινή βάση. Κάποιες από τις εφαρμογές των Wearables συσκευών είναι σχετικά απλές και τις συναντάμε

καθημερινά (Σχ. 2.1). Για παράδειγμα, συσκευές Wristband, έχουν την δυνατότητα ανά τακτά χρονικά διαστήματα να μετράνε την πίεση(Heart Rate sensor) του χρήστη, τον κορεσμό του οξυγόνου(Blood oxygen sensor), το ιστορικό των δραστηριοτήτων του(Activity Sensor) και τη θερμοκρασία του σώματός του(Temp sensor). Η μικρή υπολογιστική ισχύς δεν επιτρέπει στις συσκευές να προδούν σε πιο σύνθετους υπολογισμούς. Δίνεται η δυνατότητα στον επιβλέποντα γιατρό του να παρακολουθεί τον ασθενή του εξ αποστάσεως σε πραγματικό χρόνο, έτσι ώστε εάν παρατηρηθεί κάποια ασυνήθιστη μέτρηση να τον ενημερώσει ή να προβεί στις ενέργειες που αυτός θεωρεί κρίσιμες για την υγεία του ασθενούς. Μια τυπική εφαρμογή των φορετών συσκευών, αποτελεί η μελέτη ύπνου με τη χρήση αισθητήρων στο σπίτι.



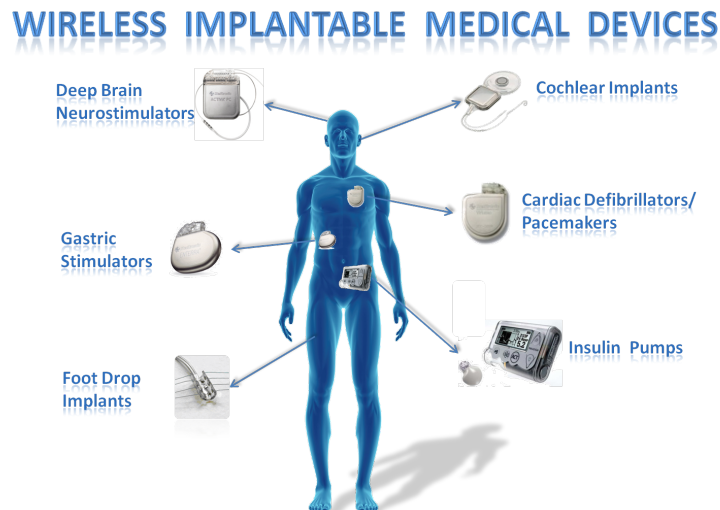
Σχήμα 2.1: Φορητή IoMT συσκευή. Adapted from 'The Internet of Things for Health Care - A Comprehensive Survey', by S. M. R. Islam et al., 2015.

Οι νέες τεχνολογίες και εφαρμογές που έχουν αναπτυχθεί (Mathias et al., 2018; Suratha et al., 2016) επιτρέπουν την διεκπεραίωση της εξέτασης του πολυσομνογραφήματος (PSG), προσομοιώνοντας εν και οίκον μελέτες ύπνου, εξάγοντας με μεγάλη ακρίβεια αποτελέσματα, παρόμοια με το πολυσομνογράφημα. Στην εξέταση PSG, οι Φορετές συσκευές καταγράφουν τις απαραίτητες μετρήσεις όπως ο κορεσμός του οξυγόνου, θωρακική κίνηση, ρινική ροή αέρα και μέσω αλγορίθμων, παίρνουν το απαιτούμενο πόρισμα, για το οποίο μπορεί να ενημερωθεί άμεσα και ο επιβλέπων γιατρός. Όπως φαίνεται και από το παράδειγμα οι φορητές συσκευές αποκτούν πρόσβαση σε μεγάλο πλήθος ευαίσθητων προσωπικών δεδομένων, γεγονός που εγείρει την ανάγκη διασφάλισης των συσκευών με σκοπό την προστασία των χρηστών του συστήματος.

2. **Εμφυτευμένες Συσκευές (IMDs):** Ήταν αρκετά διαδεδομένες από τα προγενέστερα χρόνια με τη χρήση των βηματοδοτών. Τοποθετούνται χειρουργικά κάτω από το δέρμα ή στο εσωτερικό του ανθρώπινου οργανισμού. Εξίσου σημαντικές με τις Φορετές συσκευές, οι συσκευές IMDs αποτελούν βασικό κομμάτι των δικτύων MCPs, παραχωρώντας την θεμιτή πληροφορία, ωστόσο λόγω της φύσης τους είναι ακόμα πιο σημαντική η διασφάλισή τους και οι προκλήσεις με τις οποίες έρχονται αντιμέτωπες απαιτούν μεγαλύτερη προσοχή.

Χαρακτηριστικό παράδειγμα αποτελούν οι αντλίες ινσουλίνης(Insulin Pumps), οι οποίες καθ'όλη τη διάρκεια της ημέρας εγχύουν μικρές ποσότητες ινσουλίνης στον οργανισμό, το οποίο είναι προγραμματισμένο από τον θεράπων γιατρό, και όταν είναι αναγκαίο αυξομειώνεται η χορηγούμενη ποσότητα. Με την ίδια λογική, το δίκτυο MCPs που παρακολουθεί και ρυθμίζει τα επίπεδα

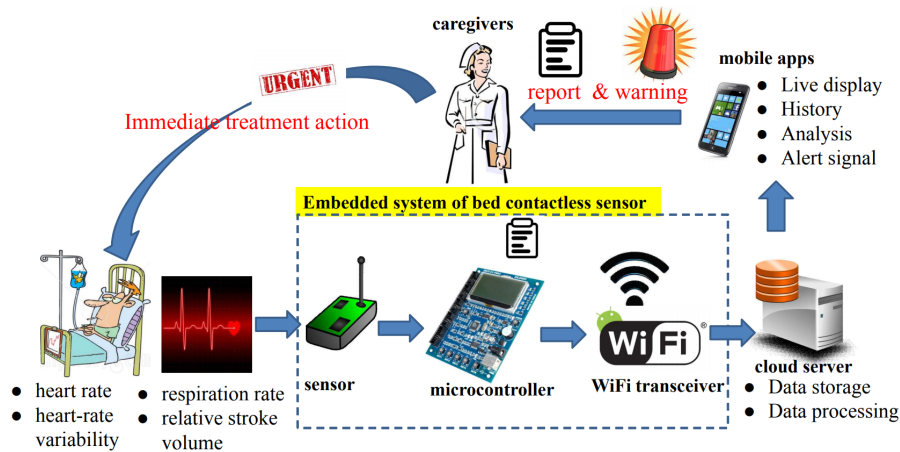
γλυκόζης στον οργανισμό ενός ασθενή, μπορεί να έχει σαν τελικό σημείο επικοινωνίας μια συσκευή Smartphone με την οποία γίνεται η αλληλεπίδραση του ασθενή. Άλλα παραδείγματα είναι ο βηματοδότης (Pacemaker), το κοχλιακό εμφύτευμα (Cochlear Implant), ο γαστρικός διεγέρτης (Gastric Stimulator) κ.ο.κ. Στο Σχ. 2.2, διακρίνονται ορισμένες από τις εμφυτευμένες συσκευές που χρησιμοποιούνται.



Σχήμα 2.2: Χαρακτηριστικά παραδείγματα εμφυτευόμενων συσκευών. Adapted from ‘Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications’, by S. Al-Janabi et al., 2017.

3. **Συσκευές Απομακρυσμένης Παρακολούθησης (ΣΑΠ):** Συμμετέχουν στην απομακρυσμένη παρακολούθηση των ασθενών (ΣΑΠ). Σκοπός των προσωπικών δικτύων είναι η αρμονική συνεργασία των ΣΑΠ με τις παραπάνω αναφερθέντες συσκευές, έτσι ώστε να προσφέρονται οι θεμιτές υπηρεσίες στον θεράποντα γιατρό και τον ασθενή. Επιπλέον, με τη συνεχή παρακολούθηση, δίνεται η δυνατότητα στον θεράπων γιατρό να ενεργεί, όταν θεωρηθεί απαραίτητο, όπως επισημαίνεται παρακάτω. Στην εν λόγω κατηγορία συγκαταλέγονται οι συσκευές Smart Home Appliances και οι εφαρμογές της τηλεϊατρικής. Για τη περίπτωση των πρώτων μπορεί να μην είναι συσκευές που εκτελούν εξειδικευμένες λειτουργίες, ωστόσο είναι σημαντικές για τη συνολική εικόνα του ασθενούς. Στο συγκεκριμένο κομμάτι, ως IoMT θεωρούνται και οι συσκευές, που βρίσκονται εντός των νοσοκομειακών μονάδων και επιτρέπουν στον θεράπων γιατρό να εκτελέσει τις υπηρεσίες του. Χαρακτηριστικό παράδειγμα, αποτελούν οι εφαρμογές της τηλεϊατρικής στον χειρουργικό τομέα, όπου ο χειρουργός έχει την δυνατότητα να εκτελέσει την επέμβαση σε απομακρυσμένη περιοχή.

Στο Σχ. 2.3 περιγράφεται το παράδειγμα της μελέτης ύπνου των ασθενών από την άνεση του σπιτιού τους. Μέχρι πρότινος, οι μελέτες ύπνου συνέβαιναν στις κλινικές ύπνου. Πλέον, με τη βοήθεια των συσκευών IoMT η εξέταση αλλά και η παρακολούθηση των απνοιακών ασθενών μπορεί να γίνει εξ αποστάσεως. Πληθώρα μετρήσεων λαμβάνονται από τους αισθητήρες (sensor), μέσω συσκευών (microcontroller) και δικτυακών υποδομών (WiFi transceiver) μεταφέρονται στο σύστημα (cloud server) και από εκεί στις εφαρμογές με τις οποίες γίνεται η διεπαφή (mobile apps) για τη λήψη αποφάσεων.



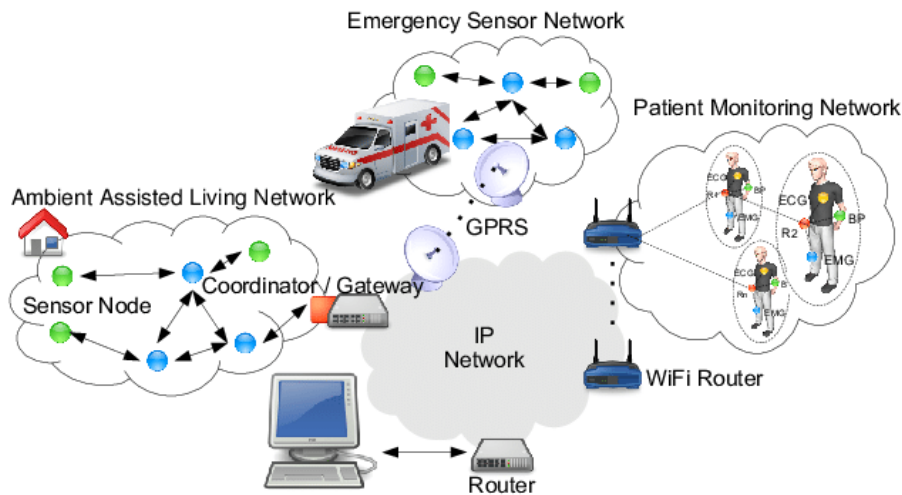
Σχήμα 2.3: Χαρακτηριστικό παράδειγμα απομακρυσμένης παρακολούθησης ασθενούς με υπνικά θέματα υγείας. Adapted from 'Internet of Things for Sleep Quality Monitoring System A Survey', N. Suratha et al., 2017.

Ως συμπέρασμα παρατηρούμε ότι είναι απαραίτητη η διασφάλιση των δικτυακών υποδομών στις οποίες διαμοιράζεται η ευαίσθητη πληροφορία των χρηστών, καθώς η πιθανή παραβίαση τους θα εκθέσει ένα σύνολο χρηστών.

2.1.1 Συστήματα Υποβοηθούμενης Διαβίωσης - Ambient Assisted Living (AAL)

Οι παραπάνω συσκευές συνοψίζονται γύρω από τον όρο του Ambient Assisted Living (AAL). Με τα δίκτυα AAL, καθίσταται δυνατή η απομακρυσμένη παροχή των ιατρικών υπηρεσιών, με τη παρακολούθηση των ασθενών και την εκτέλεση των προσφερόμενων ιατρικών υπηρεσιών. Φυσικά, κάτω από την ομπρέλα του όρου IoMT ανήκουν και τα AAL δίκτυα. Παράδειγμα των δικτύων φαίνεται στο Σχ. 2.4 όπου η επικοινωνία των αισθητήρων του ασθενούς (Sensor Node, Patient Monitoring Network) και των έξυπνων οικιακών συσκευών (Coordinator/Gateway), γίνεται με τη χρήση σημείων πρόσβασης (AP), που είναι διαμοιρασμένα στο δίκτυο (GPRS). Μέσω του υπολογιστικού νέφους (IP Network) τα αιτήματα και οι πληροφορίες προωθούνται στο δίκτυο (WiFi Router, Router) φτάνοντας στους απαραίτητους υπολογιστικούς πόρους, εκτελώντας τα αιτήματα.

Προχωρώντας ένα βήμα παραπέρα, εμπλέκονται οι συσκευές που βρίσκονται κατανομημένες στα πλαίσια των Μητροπολιτικών Δικτύων, καλύπτοντας σημεία μιας πόλης, και τα οποία επικοινωνούν με το προσωπικό δίκτυο του ασθενούς σε περίπτωση επείγοντος περιστατικού (Emergency Sensor Network). Ένας ανοϊκός ασθενής ή ασθενής της νόσου Alzheimer που είναι πιθανό να χαθεί, μπορεί να εντοπιστεί με τη χρήση των συσκευών IoMT, οι οποίες γνωστοποιούν την τοποθεσία του και την ζωτική κατάσταση του. Σε κάθε περίπτωση, όπως αναλύονται παρακάτω, τα προσωπικά δίκτυα των χρηστών κατέχουν συντονιστικό ρόλο στην ομαλή λειτουργία των συσκευών IoMT με τους ασθενείς, καθώς έχουν ως σκοπό την αναβάθμιση της ποιότητας των ιατρικών υπηρεσιών (Quality-of-Service (QoS)) ως προς όφελος των ασθενών και κατ'επέκταση των γιατρών. Οι ευκαιρίες, που προκύπτουν από τη χρήση των εν λόγω τεχνολογιών είναι πολλές και αποσκοπούν στην διευκόλυνση της καθημερινότητας των ασθενών, που βρίσκονται και σε απρόσιτα μέρη.

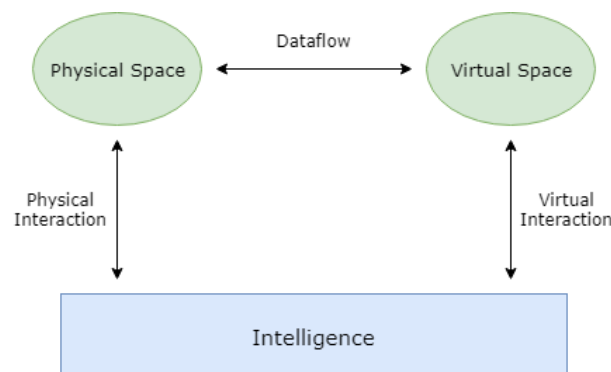


Σχήμα 2.4: Αναπαράσταση AAL λειτουργιών. Framework for QoS Performance Assessment on Biomedical Wireless Sensor Networks - Scientific Figure on ResearchGate. Available from: www.researchgate.net/figure/BWSN-applied-to-different-healthcare-scenarios-ambient-assisted-living-AAL-emergence_fig1_230580519

Ωστόσο, η διασφάλιση των υπηρεσιών και η ταυτόχρονη διατήρηση της ποιότητας της ασφάλειας Quality of Protection (QoP) στα δίκτυα επικοινωνίας των συσκευών, αποτελεί κρίσιμο κομμάτι, καθώς διατρέχουν πολλοί κίνδυνοι από τη παραβίαση τους.

2.2 Αρχιτεκτονική των Συστημάτων IoMT

Η αρχιτεκτονική των δικτύων, στα οποία αλληλεπιδρούν οι συσκευές IoMT είναι όμοια αυτής των δικτύων IoT. Με τον όρο αρχιτεκτονική, γίνεται αναφορά στα συστατικά του συστήματος, η δομή τους και η αλληλεπίδρασή τους. Στα συστήματα IoMT, δεν υπάρχει κοινή θεωρία για την αρχιτεκτονική τους, ωστόσο τα προτεινόμενα μοντέλα έχουν πολλά κοινά στοιχεία. Υπάρχουν βασικοί παράγοντες, όπως τα ευαίσθητα προσωπικά δεδομένα και ο μεγάλος όγκος τους, όπου οι τεχνολογίες και τα πρωτόκολλα που χρησιμοποιούνται στα συστήματα IoT αδυνατούν να αντεπεξέλθουν στις απαιτήσεις τους και χρειάζονται ριζικές τροποποιήσεις. Μια απλοποιημένη προσέγγιση για την ροή της πληροφορίας στα συστήματα IoMT αναπαριστάται από τους Dey et al., 2017 στο Σχ. 2.5.

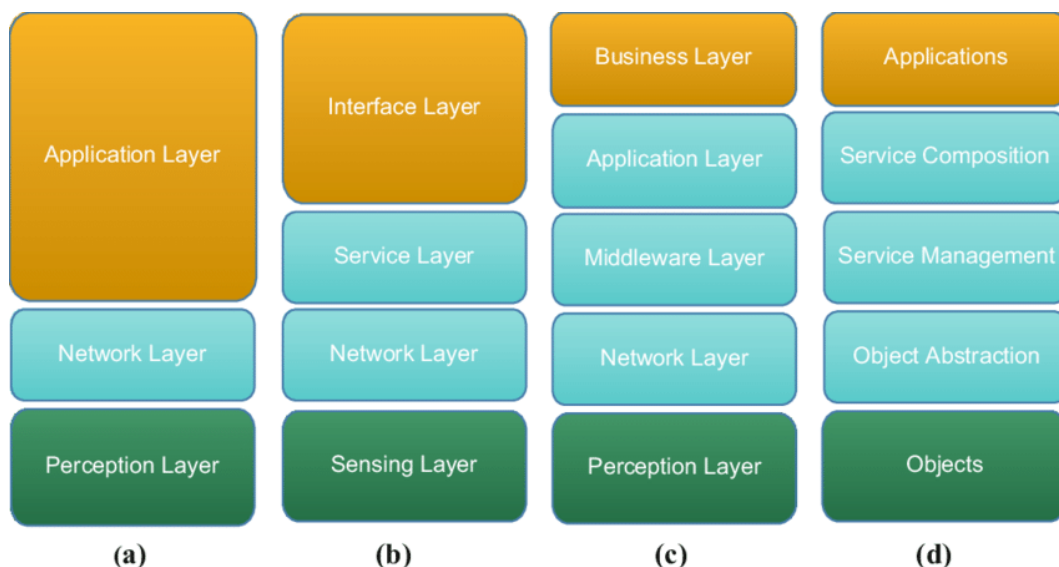


Σχήμα 2.5: Η τυπική ροή των δεδομένων σε ένα σύστημα IoMT με τις αλληλεπιδράσεις των συστατικών του.

Δεδομένα ρέουν από τους αισθητήρες και τις συσκευές του φυσικού χώρου (Physical Space) στις οποίες γίνονται όλες οι βιομετρικές μετρήσεις, προς τον κοινόχρηστο εικονικό χώρο του συστήματος (Virtual Space), στον οποίο πιθανόν να βρίσκονται υπολογιστική πόροι του συστήματος ή αποθηκευτικοί χώροι, όπως κάποια βάση δεδομένων ή το υπολογιστικό νέφος. Τα δεδομένα ακολουθούν διαφορετική πορεία και από τους δύο χώρους προς τα συστήματα αποφάσεων του δικτύου (Intelligence) για την επεξεργασία των δεδομένων, τη δημιουργία της επιθυμητής πληροφορίας και τη λήψη αποφάσεων. Όσον αφορά τη πορεία των δεδομένων από και προς το φυσικό χώρο (Physical Interaction), γίνεται λόγος για τοπικές υπηρεσίες, όπως η μέτρηση της αρτηριακής. Η πορεία από και προς τον εικονικό χώρο (Virtual Interaction) μπορεί να αναφέρεται σε οποιαδήποτε λειτουργία που έχει υψηλότερες υπολογιστικές απαιτήσεις.

2.2.1 Η Δομή των Στρωμάτων Επικοινωνίας στα Συστήματα IoMT

Τα συστήματα IoMT διαθέτουν υπηρεσίες επικοινωνίας και δικτύων και ως παράδειγμα στο Σχ.2.6 διακρίνονται οι διαφορετικές προσεγγίσεις της ταξινόμησης των στρωμάτων στις συσκευές των IoT. Στην Πτυχιακή Εργασία, υιοθετείται η δεύτερη προσέγγιση **-(b)-** των τεσσάρων στρωμάτων. Η κοινώς αποδεκτή αρχιτεκτονική είναι η **-(a)-**, ωστόσο, με τη δεύτερη προσέγγιση διαχωρίζονται οι λειτουργίες περισυλλογής, μεταφοράς, επεξεργασίας και απεικόνισης των δεδομένων από τους αισθητήρες. Επιπλέον, τα πρωτόκολλα επικοινωνίας που περιγράφονται παρακάτω τοποθετούνται σε τέσσερα στρώματα και είναι επιθυμητό να γίνει η αντιστοιχία των στρωμάτων με αυτά.



Σχήμα 2.6: Αρχιτεκτονική στρωμάτων επικοινωνίας στις συσκευές IoMT. Biometric Security and Internet of Things(IoT) - Scientific Figure on ResearchGate. Available from: www.researchgate.net/figure/IoT-architecture-a-3-layer-b-4-layer-c-5-layer-and-d-SOA-based-5_fig1_328516514 [accessed 23 Jun, 2019]

Ενδεικτικά, το κατώτατο στρώμα ή *Sensing Layer* είναι υπεύθυνο για τη περισυλλογή των δεδομένων, από τους αισθητήρες που διαθέτει η συσκευή. Το στρώμα δικτύου ή *Network Layer* είναι υπεύθυνο για τη μεταφορά των δεδομένων από το προηγούμενο στρώμα.

γούμενο στρώμα στο στρώμα υπηρεσιών ή *Service Layer*. Στο τρίτο στρώμα διεκπεραιώνονται οι επιθυμητές ιατρικές υπηρεσίες. Από εδώ, εξάγεται η επιθυμητή πληροφορία και γίνεται η λήψη των αποφάσεων. Τέλος, στο ανώτερο στρώμα ή *Interface Layer* ή *Application Layer* γίνεται η οπτικοποίηση των δεδομένων και η αλληλεπίδραση των χρηστών με το σύστημα.

2.2.2 Τύποι Δικτύων

Με βάση τα μοντέλα αυτά, τα δίκτυα IoMT απαρτίζονται από πληθώρα τεχνολογιών. Με επίκεντρο τον ασθενή, οι αισθητήρες που χρησιμοποιούνται για τη παροχή των προσφερόμενων υπηρεσιών λαμβάνουν τις σωματικές μετρήσεις των χρηστών, δημιουργώντας ένα Δίκτυο από Σωματικούς Αισθητήρες -Medical Cyber Physical System (MCPS)-, δηλαδή συστήματα, τα οποία χαρακτηρίζονται ως φυσικά. Οι διαδικασίες παρακολουθούνται, επεξεργάζονται και ενσωματώνονται με ασφάλεια σε έναν πυρήνα επικοινωνίας και υπολογιστικής ισχύος σε όλα τα επίπεδα. Όπως φαίνεται στο Σχ. 2.8 στη ζώνη (α) τα δίκτυα MCPS απαρτίζονται από ένα σύνολο αισθητήρων, τις εμφυτευμένες ιατρικές συσκευές -συσκευές που βρίσκονται στο σώμα του ασθενούς ή υπό το δέρμα του- και από τις φορεμένες συσκευές- οι οποίες μπορεί να βρίσκονται μέχρι και 2 εκατοστά μακριά από το σώμα του ασθενούς- (End Devices), λαμβάνοντας τα βιομετρικά δεδομένα του ασθενούς.

Με τον όρο του Ασύρματου Δικτύου Αισθητήρων (WSN), ομαδοποιείται το σύνολο των αισθητήρων και συσκευών, που χρησιμοποιούνται για την παροχή των ιατρικών υπηρεσιών στον χρήστη και την συλλογή των ευαίσθητων δεδομένων του. Σε αυτά, ανήκουν οι έξυπνες οικιακές συσκευές (Smart Home Appliances), με τις οποίες συγκεντρώνονται περισσότερα δεδομένα για τον χρήστη. Η ενσωμάτωση των δικτύων MCPS στα WSN εμπλουτίζεται η επικοινωνία μεταξύ των συσκευών -Machine-to-Machine (M2M)- και πληθύνοντας τον συνολικό αριθμό των αισθητήρων που επικεντρώνονται σε έναν χρήστη, επιτρέπουν την συλλογή περισσότερης και ακριβέστερης πληροφορίας, η οποία αφορά έναν χρήστη. Η χρησιμότητα της πληροφορίας πλουτίζει με το σύνολο των διαφορετικών δεδομένων που ομαδοποιούνται και αναλύονται. Εφόσον ανακτάται περισσότερη πληροφορία, τότε βελτιώνεται η προσφερόμενη υπηρεσία. Ωστόσο, η ασφάλιση της πληροφορίας αποτελεί μεγάλη πρόκληση για τους σχεδιαστές των συστημάτων.

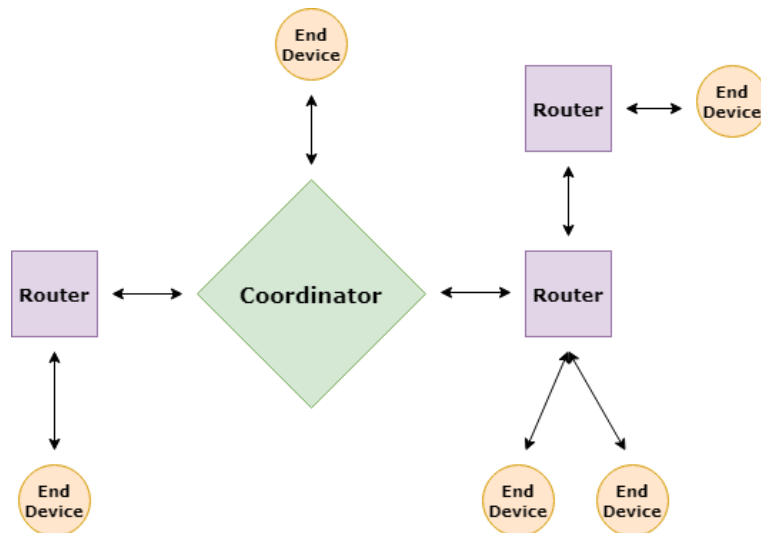
Ο όρος των Wireless Body Area Network (WBAN) περιγράφει το σύνολο των αισθητήρων που αναφέρονται παραπάνω με τη χρήση τεχνολογιών επικοινωνίας. Στο Σχ. 2.8 τα δίκτυα WBAN αποτελούν μια ευρύτερη έννοια των WSN. Σύμφωνα με το πρότυπο επικοινωνίας IEEE 802.15.6, που χρησιμοποιείται για την επικοινωνία των συσκευών, οι Al-Janabi et al., 2017 αναφέρουν τη δομή της ταξινόμησης των δικτύων WBAN. Όπως παρουσιάζεται στο Σχ. 2.7, τα δίκτυα WBAN, αποτελούνται από τις συσκευές Router και End Devices. Οι συσκευές Coordinator συνδέουν τα υποδίκτυα μεταξύ τους και με το συνολικό δίκτυο. Έτσι, περιγράφονται οι εξής αλληλεπιδράσεις:

- **Συντονιστής (Coordinator Node):** Λειτουργεί σαν gateway και συνδέει το δίκτυο WBAN με το υπόλοιπο διαδίκτυο ή με άλλο WBAN. Βρίσκονται στο συνολικό δίκτυο, ωστόσο υπάρχουν και συσκευές στα δίκτυα WSN των ασθενών, που μεταξύ άλλων λειτουργιών αναλαμβάνουν και το ρόλο του συντονιστή, ως προς το τρόπο διανομής των δεδομένων και διαχείρισης των ενεργειακών πόρων. Σε ένα δίκτυο IoMT, το ρόλο του συντονιστή κατέχουν κεντρικές συσκευές όπως Switches ή

Gateways, που ελέγχουν το υποδίκτυο και επικοινωνούν με το συνολικό δίκτυο,

- **Τελικοί Κόμβοι (End Devices):** Περιορίζονται στις λειτουργίες που τους έχουν οριστεί. Ένας τελικός κόμβος είναι αυτός που αναμεταδίδει ο,τι δεδομένο έχει αποκτήσει από τις μετρήσεις του. Στη περίπτωση των συστημάτων IoMT θεωρούνται οι συσκευές και οι αισθητήρες που βρίσκονται στο δίκτυο WSN. Οι μετρήσεις των αισθητήρων στέλνονται στους Αναμεταδότες, οι οποίοι έπειτα προωθούν τα δεδομένα στους Συντονιστές.
- **Αναμεταδότες (Router):** Λειτουργούν ως διαμεσολαβητές, έχοντας από έναν κόμβο-γονέα και έναν κόμβο-παιδί και μηνυμάτων. Οι αναμεταδότες έχουν την ικανότητα να διαισθάνονται δεδομένα από άλλους κόμβους. Οι συσκευές Gateways και Access Points που αναφέρονται παρακάτω έχουν τον χαρακτήρα του αναμεταδότη. Αναμεταδότες υπάρχουν στο συνολικό δίκτυο. Κλασικό παράδειγμα αναμεταδότη αποτελούν οι συσκευές Router, οι οποίες λαμβάνουν από τους κόμβους-συντονιστές δεδομένα με οδηγίες, για να αποσταλούν στον σωστό κόμβο-παραλήπτη. Για λόγους διαλεύκανσης, η έννοια των συσκευών Router χρησιμοποιείται στο σχήμα, καθώς Αναμεταδότες με Συντονιστές διαθέτουν κοινές συσκευές, ωστόσο με διαφορετικές λειτουργίες.

Συνεχίζοντας, στο Σχ. 2.8 διακρίνεται το Wireless Personal Area Network (WPAN)), που δημιουργείται μεταξύ των δικτύων WBAN του χρήστη και των λοιπών συσκευών που χρησιμοποιούνται στα δίκτυα IoMT. Smartphones, προσωπικοί υπολογιστές (Personal Appliances), και συσκευές που χρησιμοποιούνται σαν διαμεσολαβητές (Personal Server) του προσωπικού δικτύου του ασθενούς με το υπόλοιπο δίκτυο, για να φτάσει η πληροφορία στον επιθυμητό παραλήπτη, ο οποίος μπορεί να είναι ένας γιατρός, ένας επαγγελματίας υγείας, μια νοσοκομειακή μονάδα ή μια ασφαλιστική εταιρεία, περνάει από συσκευές Access Points (AP), που βρίσκονται καταναμημένες σε μια ευρύτερη περιοχή.

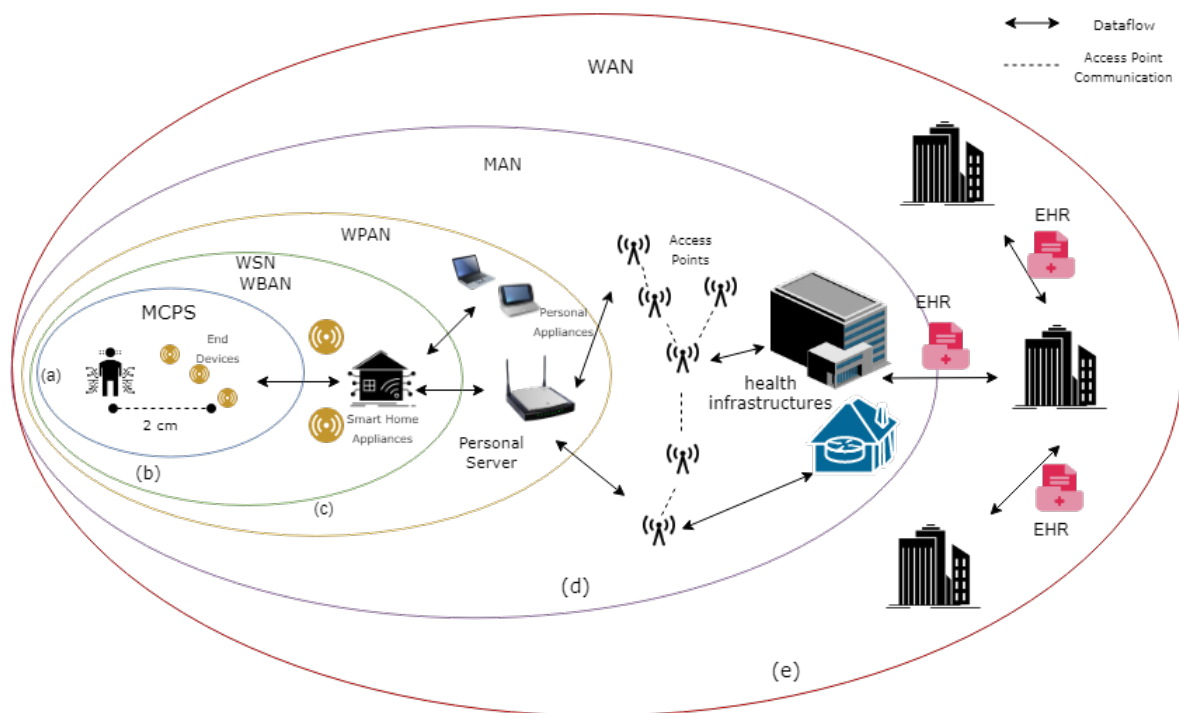


Σχήμα 2.7: Τύποι κόμβων και η μεταξύ τους συσχέτιση.

Οι Φορετές και Εμφυτευμένες συσκευές (βλ. Κεφάλαιο 2.1) χρησιμοποιούνται στα προσωπικά δίκτυα των χρηστών για την περισυλλογή και επεξεργασία των απαραίτητων μετρήσεων. Οι συσκευές που ανήκουν στη κατηγορία των ΣΑΠ (βλ. 2.1), μαζί με τα δομικά συστατικά των δικτύων, χρησιμοποιούνται στους υπόλοιπους τύπους δικτύων. Η πληροφορία, αφού αποσταλεί από το δίκτυο WBAN του χρήστη, μεταπηδάει μεταξύ

των συσκευών AP, με σκοπό να φτάσει στον κόμβο-παραλήπτη. Η πληροφορία, που μεταβιβάζεται έχει τις απαραίτητες οδηγίες, έτσι ώστε οι συσκευές AP να τη μεταφέρουν στον κατάλληλο κόμβο.

Οι συσκευές AP μπορεί να είναι είτε τα Router των τηλεπικοινωνιακών παρόχων μιας χώρας, είτε συσκευές αφιερωμένες για την εκτέλεση των παραπάνω ενεργειών, όπως οι συσκευές Raspberry Pi και ZigBee. Οι συσκευές AP σε συνδυασμό με τα δίκτυα WPAN του κάθε χρήστη δημιουργούν ένα δίκτυο Metropolitan Area Network (MAN), τα οποία επικοινωνούν με μεγαλύτερες μονάδες όπως νοσοκομεία, ιατρεία, κέντρα υγείας (health infrastructure) όπως παρουσιάζονται στο Σχ. 2.8. Το δίκτυο αυτό, μπορεί να αφορά μια πόλη, ένα χωριό ή μια περιοχή περιορισμένης ακτίνας.



Σχήμα 2.8: Κατανομή των διαφορετικών τύπων δικτύων που συμμετέχουν στα IoMT συστήματα.

Τέλος, όπως φαίνεται στο Σχ. 2.8 τα δίκτυα Wide Area Networks (WAN), δημιουργούνται μεταξύ πόλεων και χωρών, σε μια ευρεία γεωγραφική περιοχή. Αν για παράδειγμα, ανήκει στο δίκτυο IoMT ο Ηλεκτρονικός Ιατρικός Φάκελος (EHR) ενός χρήστη, τότε σε περίπτωση επείγοντος περιστατικού, ενώ βρίσκεται σε άλλη χώρα, μέσω του συστήματος είναι δυνατή η αποστολή του EHR στον επείγοντα γιατρό. Η παραπάνω περιγραφή συνοψίζεται στο Σχ. 2.8, από τα μικρότερης εμβέλειας τοπικά δίκτυα, που αφορούν έναν χρήστη ή ένα σύνολο χρηστών, μέχρι και την διασύνδεση μεγάλων δικτύων που αφορούν ολόκληρες κοινωνίες.

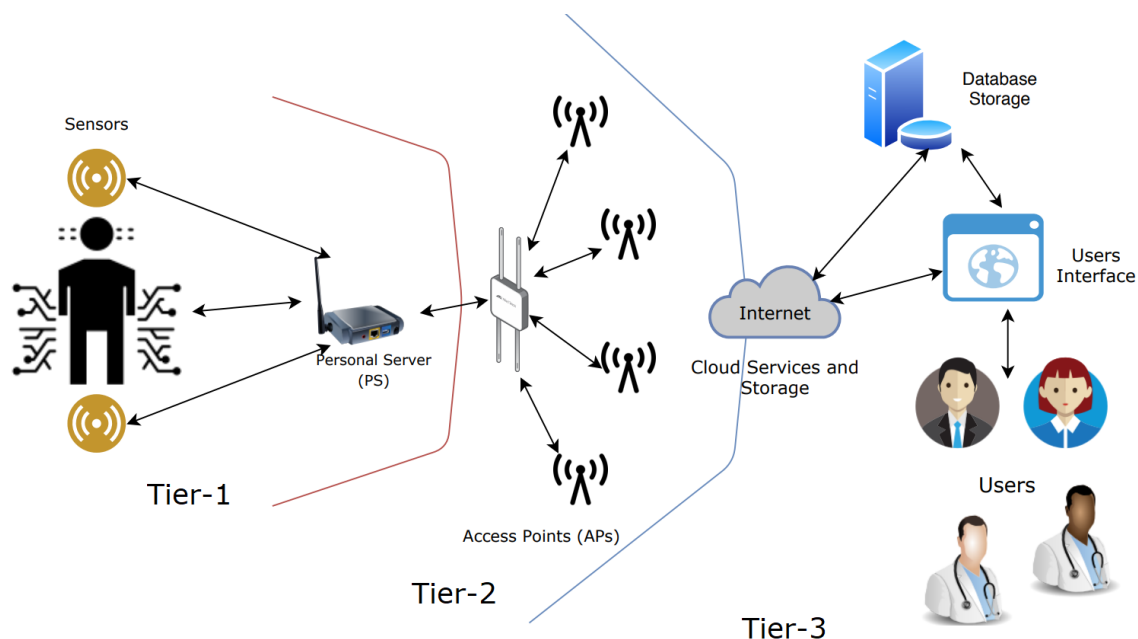
2.2.3 Τα Επίπεδα της Αρχιτεκτονικής των Δικτύων IoMT

Σύμφωνα με την βιβλιογραφία (Mosenia and Jha, 2017, Roman et al., 2013), δεν υπάρχει ένα πρότυπο, το οποίο να περιγράφει τη δομή των συστημάτων IoMT. Ωστόσο, ένα κοινά αποδεκτό μοντέλο για την αρχιτεκτονική των συστημάτων αποτελείται από τρία επίπεδα, όπως φαίνεται στο Σχ. 2.9.

Το πρώτο επίπεδο είναι το Φυσικό επίπεδο ή επίπεδο Περισυλλογής (Σχ. 2.9 - Tier-1) και Προεπεξεργασίας. Γίνεται η περισυλλογή όλων των θεμιτών ακατέργαστων δεδομένων από τους αισθητήρες και τις συσκευές, στατικές ή κινητές (βλ. 2.1, τύποι 1 και 2).

1. **Στατικές Συσκευές:** Αναφέρονται σε έξυπνες οικιακές συσκευές, οι οποίες παρακολουθούν τις κινήσεις, συνήθειες και γενικά τα μοτίβα του ασθενούς. Επιπλέον, στατικές μπορούν να χαρακτηριστούν και οι εμφυτευμένες συσκευές, καθώς βρίσκονται είτε εντός του ανθρώπινου οργανισμού είτε πάνω σε αυτόν,
2. **Κινητές Συσκευές:** Wristbands, Earbuds, Smartphones ή γενικά οποιαδήποτε συσκευή υποστηρίζει αισθητήρες, που λαμβάνουν τα βιομετρικά δεδομένα των ασθενών κυρίως με την επαφή τους με το ανθρώπινο σώμα.

Η μετάδοση των δεδομένων του φυσικού στρώματος, γίνεται με τη χρήση διαφόρων πρωτοκόλλων, τα οποία εδραιώνουν οδούς επικοινωνίας με το δεύτερο στρώμα, αλλά σε ορισμένες περιπτώσεις και την επικοινωνία μεταξύ των συσκευών. Τεχνολογίες όπως τα Bluetooth, ZigBee, NFC και QR Stamps, χρησιμοποιούνται για τον σκοπό αυτό. Στο πρώτο επίπεδο ανήκουν και οι συσκευές, με τις οποίες ο χρήστης αλληλεπιδρά με τους αισθητήρες που του αντιστοιχούν, όπως για παράδειγμα μια συσκευή Smartphone.



Σχήμα 2.9: Τυπική αναπαράσταση ενός IoMT συστήματος τριών επιπέδων.

Το επόμενο στάδιο στο Φυσικό επίπεδο είναι η προετοιμασία των ακατέργαστων δεδομένων. Στην ουσία ένα σύστημα IoMT αποτελεί ένα Low-power and Lossy Networks (LLN), δηλαδή ένα δίκτυο του οποίου τα στοιχεία διαθέτουν χαμηλούς πόρους και χαλαρές συνδέσεις. Έτσι, οι συσκευές Gateways παρουσιάζονται ως ενδιάμεσες οντότητες, οι οποίες συνήθως είναι συσκευές Raspberry Pi, Zigbee, Router, ή γενικά συσκευές, στις οποίες συγκεντρώνονται όλα τα θεμιτά δεδομένα.

Οι παραπάνω συσκευές επικοινωνούν με τις συσκευές Access Points (AP) του επόμενου επιπέδου, προκειμένου να προωθήσουν την επιθυμητή πληροφορία στο δίκτυο. Οι συσκευές AP, λειτουργούν ως συνδετική κρίκοι μεταξύ των υποδικτύων, του

συνολικού δικτύου και του υπολογιστικού νέφους του τρίτου επιπέδου. Έχουν συνήθως προγραμματισμένες τις χρονικές περιόδους που οι συσκευές IoMT στέλνουν τα δεδομένα τους, ωστόσο εκτελούν εντολές, κατά την αίτηση αποστολής ή λήψης πληροφοριών από έναν κόμβο.

Σε αυτό το επίπεδο οι συσκευές που παραλαμβάνουν τα ακατέργαστα δεδομένα, τα προετοιμάζουν για την προώθηση τους στο επίπεδο του δικτύου, από το οποίο φτάνουν στον κόμβο-παραλήπτη, αλλά και στο επίπεδο εφαρμογών. Τα συγκεντρώνουν, τα επεξεργάζονται και τα ασφαλίζουν με κρυπτογραφικές μεθόδους, για την διασφάλιση της πληροφορίας και της ιδιωτικότητας του χρήστη.

Οι Alaba et al., 2017 αναφέρουν δύο τύπους αισθητήρων (Sensors), που χρησιμοποιούνται στο πρώτο επίπεδο, τους (I) Αισθητήρες, οι οποίοι συλλέγουν και επεξεργάζονται τα δεδομένα, ενώ αλληλεπιδρούν και με τους υπόλοιπους αισθητήρες του δικτύου και τις συσκευές (II) Gateways, στις οποίες γίνεται η περισυλλογή των δεδομένων, που είτε εισέρχονται στο δίκτυο είτε αποστέλλονται σε έναν κόμβο-παραλήπτη:

1. **Αισθητήρας (Sensors):** Οι αισθητήρες διαθέτουν μικρή υπολογιστική δύναμη, οπότε λειτουργίες όπως η μέτρηση της αρτηριακής πίεσης και των παλμών ενός χρήστη, ο κορεσμός του οξυγόνου, τα επίπεδα άγχους ή η θερμοκρασία του δωματίου, είναι κάποιες από τις λειτουργίες που επιτελούν. Οι αισθητήρες εφαρμόζουν στα δίκτυα MCPS και WBAN, όπου λαμβάνουν τα βιομετρικά δεδομένα του ασθενούς (Φορετές και Εμφυτευμένες), αλλά και τα περιβαλλοντικά δεδομένα με τις ΣΑΠ.
2. **Gateways (Personal Servers):** Όσον αφορά τις συσκευές Gateways που ανήκουν και στο επόμενο επίπεδο, συλλέγουν διαρκώς δεδομένα για τη κατάσταση και λειτουργία των κόμβων του δικτύου τους. Επίσης, ανιχνεύουν οποιαδήποτε διαταραχή προκύψει στον ασθενή και όταν χρειαστεί δρουν χρησιμοποιώντας τους ενεργοποιητές των συσκευών IoMT, είτε αυτόματα είτε με την εντολή του επιβλέποντα γιατρού.

Στη περίπτωση του πρώτου επιπέδου χρησιμοποιούνται Gateways ως Personal Servers (PS), όπου λειτουργούν ως σημεία περισυλλογής όλων των δεδομένων, που προβλέπεται να μεταδοθούν σε έναν κόμβο, ο οποίος βρίσκεται έξω από το δίκτυο που ανήκει. Επικοινωνούν με τις συσκευές AP του επόμενου επιπέδου. Έχουν τον χαρακτήρα ενός διακομιστή και είναι υπεύθυνοι για τα δεδομένα που εισέρχονται στο δίκτυο τους.

Εν συνεχεία, ακολουθεί το δεύτερο επίπεδο (Σχ. 2.9 - Tier-2) ή επίπεδο Δικτύου. Εδώ, ανήκουν τα δίκτυα MAN και WAN. Δύο είναι τα βασικά μέρη του, οι συσκευές AP και το υπολογιστικό νέφος (Cloud Server). Το υπολογιστικό νέφος συνυπάρχει μεταξύ του δεύτερου και του τρίτου στρώματος. Οι συσκευές του δεύτερου στρώματος ανήκουν στις ΣΑΠ (βλ. 2.1 τύπος 3). Τα δεδομένα ταξιδεύουν μεταξύ των συσκευών AP με στόχο είτε να προσεγγίσουν ένα κοντινό δίκτυο, είτε στο υπολογιστικό νέφος, μέσω του διαδικτύου με τη χρήση των πρωτοκόλλων επικοινωνίας, που αναλύονται παρακάτω όπως τα 6LoWPAN, MQTT, CoAP. Οι συσκευές AP, ωστόσο λόγω της κοινής θέσης τους, μπορεί να αποτελέσουν αντικείμενο παραβίασης.

Συνήθως, τα υπολογιστικά νέφη χρησιμοποιούν τη τεχνολογία του Software Defined Networks (SDN). Με τη χρήση τους, γίνεται ο έλεγχος και η εκμετάλλευση των συσκευών από μια κεντρική οντότητα (Channegowda, et al., 2013). Χαρακτηριστικές επιθέσεις, όπως επιθέσεις Παρεμβολής, Παθητικής Ακρόασης και Υποκλοπής Δεδομένων

μπορούν να γίνουν, εάν δεν υπάρχουν τα κατάλληλα μέτρα ασφαλείας. Στο επίπεδο δικτύου βρίσκονται και οι υπηρεσίες αποθήκευσης των δεδομένων στα υπολογιστικά νέφη.

Το επίπεδο διαθέτει ισχυρή υπολογιστική ισχύ, με χαμηλά κόστη και αντίκτυπο στο συνολικό δίκτυο, όπου δεδομένα επεξεργάζονται για τη δημιουργία της επιθυμητής πληροφορίας. Έτσι, τα δεδομένα του κάθε χρήστη αποθηκεύονται στο επίπεδο, με σκοπό την οπτικοποίηση τους στο επόμενο. Ισχυρά μέτρα ασφαλείας απαιτούνται στο εν λόγω επίπεδο, καθώς η παραβίαση του θα εκθέσει τους χρήστες του συστήματος.

Τέλος, στο ανώτερο επίπεδο βρίσκεται το επίπεδο Εφαρμογής (Σχ. 2.9 - Tier-3). Τυπικά, το επίπεδο εφαρμογής αποτελείται από ένα Middleware, το Πρωτόκολλο Επικοινωνίας μεταξύ δύο συσκευών, ενός Cloud Server και μιας πλατφόρμας αντιμετώπισης προβλημάτων στο σύστημα (Yaqoob et al., 2017). Στο εν λόγω επίπεδο γίνεται η οπτικοποίηση των δεδομένων από το επίπεδο δικτύου και των αναλύσεων τους, και η διάδραση των χρηστών με το σύστημα. Εδώ, ανήκουν τα δίκτυα WPAN, MAN και WAN, σε αυτά δηλαδή που υπάρχουν οι τεχνολογίες όπως συσκευές Smartphone και προσωπικοί υπολογιστές από τις οποίες οι εξουσιοδοτημένοι χρήστες όπως οι ασθενείς και οι θεράποντες γιατροί έχουν πρόσβαση στα δεδομένα.

Η οπτικοποίηση των δεδομένων και η διάδραση των χρηστών συμβαίνει μέσω της διεπαφής χρήστη (Users Interface), το οποίο προβάλλεται σε οθόνες, κινητά, υπολογιστές κ.ο.κ. Σε κάθε χρήστη αντιστοιχούν συγκεκριμένα δικαιώματα, όπως για παράδειγμα αν είναι απλός χρήστης-ασθενής παρακολουθεί τα δεδομένα που του αντιστοιχούν, ενώ ένας γιατρός παρακολουθεί τα δεδομένα των ασθενών του. Τυπικά, από το συγκεκριμένο επίπεδο, γίνεται η διάδραση των χρηστών με το σύστημα. Οι επαγγελματίες υγείας μπορούν και επιβλέπουν την εξέλιξη του ασθενή, κυρίως μέσα από την οπτικοποίηση των πληροφοριών που προκύπτει από την ανάλυση των δεδομένων. Επίσης, οι ασθενείς είναι σε θέση να ελέγχουν την πρόοδο τους. Το τελευταίο επίπεδο διαθέτει τις βάσεις δεδομένων, που συγκρατούν μαζικά όλα τα δεδομένα, τις πληροφορίες και τα μεταδεδομένα που αντιστοιχούν στους χρήστες του συστήματος, αφού φιλοξενούνται στις κτηριακές μονάδες των συστημάτων IoMT.

Για παράδειγμα, έστω ένας ασθενής με εμφυτευμένη μια συσκευή βηματοδότη, όπου ανιχνεύει ολιγόλεπτα επεισόδια αρρυθμιών. Ο θεράπων γιατρός βλέποντας την διατάραξη του ασθενούς, και συμβουλευοντας τις αναλύσεις που του προσφέρει το σύστημα, μπορεί να πάρει τις κατάλληλες αποφάσεις και να ρυθμίσει την συσκευή του ασθενούς εξ αποστάσεως. Δίνοντας εντολή μέσω του συστήματος να αλλάξουν οι απαραίτητες ρυθμίσεις, μέσω του συστήματος η εντολή μεταφέρεται στην συσκευή IoMT και εκτελείται η εντολή του γιατρού. Φυσικά, στο εν λόγω επίπεδο είναι σημαντικά τα μέτρα ασφαλείας για λόγους ιδιωτικότητας και ασφάλειας των χρηστών.

2.2.4 Συμπεράσματα

Καταλήγοντας, το μοντέλο που περιγράφηκε (Σχ. 2.9) δεν αποτελεί ένα πρότυπο, αλλά μία γενίκευση των τεχνολογιών και των αντίστοιχων Framework, που υπάρχουν αυτή τη στιγμή. Ωστόσο, αποτελεί μια ενδεικτική προσέγγιση, κατά την οποία ένα σύστημα IoMT, θα μπορούσε να βασιστεί για την διεκπεραίωση των υπηρεσιών υγείας. Στον Πίνακα 2.1 γίνεται η αντιστοίχιση των περιγραφόμενων τεχνολογιών με τα επίπεδα(Tier) του Σχ. 2.9. Στο πρώτο επίπεδο συμμετέχουν οι αισθητήρες, φορητοί και εμφυτευμένοι (IMD, Wearable) και οι συσκευές εν κατοίκo παρακολούθησης (Smart

Home Appliances), που βρίσκονται στο προσωπικό δίκτυο του χρήστη(WBAN) λαμβάνοντας το σύνολο των σωματικών και χωρικών μετρήσεων που αφορούν τον χρήστη.

Tier	Layer	Network Type	IoMT Device
1	Sensing	MCPS WSN WBAN	Εμφυτευμένες Φορητές
2	Network	MAN	ΣΑΠ
3	Service	WAN	
	Interface	WPAN	

Tiers: Επίπεδα Αρχιτεκτονικής, Layer: Στρώματα Επικοινωνίας, Network Type: Τύποι Δικτύων, IoMT Device: Τύποι Συσκευών

Πίνακας 2.1: Αντιστοίχιση των επιπέδων αρχιτεκτονικής με τα στρώματα επικοινωνίας τους τύπους δικτύων και τις IoMT συσκευές.

Στο δεύτερο επίπεδο συμμετέχουν οι δικτυακές (Network) υποδομές, όπως συσκευές Gateway, Router και Access Points που ανήκουν στις ΣΑΠ και δραστηριοποιούνται στα δίκτυα MAN και WAN. Τέλος, στο τρίτο επίπεδο συμμετέχουν οι υπηρεσίες οπτικοποίησης(Interface) και επεξεργασίας(Service) προσωπικών δεδομένων, που γίνονται στις υποδομές των δικτύων WAN και των προσωπικών δικτύων των ασθενών WPAN, όπως σε μια συσκευή Smartphone. Οι διαφορετικές προσεγγίσεις αναλογικά με τον αριθμό των επιπέδων δράσης αναγράφονται στον Πίνακα 2.2.

Tiers: Αριθμός Επιπέδων Αρχιτεκτονικής , AP: Access Points, GWs: Gateways, CSe: Cloud Υπηρεσίες, CSt: Cloud Αποθηκευτικές Υπηρεσίες, Analytics: Υπηρεσίες Αναλυτικής, PS: Personal Server, DB: Βάση Δεδομένων

	Alaba et al., 2017	Al-Janabi et al., 2017	Almohri et al., 2017	Chen et al., 2017	Dey et al., 2017	He et al., 2018	Islam et al., 2015	Kartsakli et al., 2014	Kocabas et al., 2016	Movassaghi et al., 2014
Tiers	3	3	3	4	3	3	4	3	4	3
AP	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes
GWs	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes
CSe	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes
CSt	Yes	No	No	Yes	No	No	Yes	No	Yes	No
Analytics	No	No	No	No	Yes	No	No	No	Yes	No
PS	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DB	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Πίνακας 2.2: Βιβλιογραφική ανασκόπηση των τελευταίων ερευνητικών εργασιών, που αναλύουν την αρχιτεκτονική των IoMT συστημάτων.

Συγκεκριμένα παρατίθενται συνοπτικά οι τελευταίες ερευνητικές εργασίες που αναλύουν την αρχιτεκτονική των συστημάτων IoMT. Στην αριστερή στήλη παρατίθενται

τα χαρακτηριστικά των IoMT συστημάτων με τα οποία δομούνται από τους συγγραφείς των ερευνητικών εργασιών της πρώτης σειράς. Οι αρχιτεκτονικές της βιβλιογραφίας, διαφέρουν μερικώς. Όπως και στην Πτυχιακή Εργασία, έτσι και η πλειονότητα των προσεγγίσεων αναφέρονται σε τρία επίπεδα δράσης. Οι προσεγγίσεις με τέσσερα επίπεδα θέτουν τις υπηρεσίες περισυλλογής και προεπεξεργασίας σε ένα ξεχωριστό επίπεδο. Η πλειονότητα των αρχιτεκτονικών χρησιμοποιεί την υπολογιστική ισχύ και τα αποθηκευτικά μέσα ενός υπολογιστικού νέφους. Επιπλέον, χρησιμοποιούν συσκευές Gateways, ξεχωριστές Βάσεις Δεδομένων και συσκευές που έχουν τον χαρακτήρα του προσωπικού Διακομιστή.

Συμπερασματικά, η φύση των δεδομένων που διαμοιράζονται στα συστήματα IoMT απαιτούν την διασφάλιση τους. Η αρχιτεκτονική των συστημάτων IoMT δεν προσφέρει την απαιτούμενη ασφάλεια που χρειάζεται στα δεδομένα. Έτσι, στο επόμενο κεφάλαιο περιγράφονται τα προβλήματα στην ασφάλεια και την ιδιωτικότητα των συστημάτων IoMT, τα οποία είναι αποτέλεσμα της ανεπάρκειας που χαρακτηρίζει τα υπάρχοντα μέτρα.

Κεφάλαιο 3

Απειλές Ασφάλειας και Ιδιωτικότητας στα Συστήματα IoMT

Η άνοδος των συστημάτων IoT, είχε ως αποτέλεσμα την διακίνηση τεράστιου όγκου ευαίσθητων δεδομένων. Για την ανερχόμενη τεχνολογία των IoMT, οι συσκευές που χρησιμοποιούνται στις προσφερόμενες ιατρικές υπηρεσίες, φαίνεται να μη διαθέτουν τις κατάλληλες υποδομές για τη διασφάλιση ευαίσθητων προσωπικών δεδομένων. Αυτό συμβαίνει, διότι οι προτεραιότητες των κατασκευαστών των συστημάτων IoT επικεντρώνονται στην πολυλειτουργικότητα και ευχρηστία τους. Επιπλέον, τα κανάλια επικοινωνίας είναι αναξιόπιστα και το περιβάλλον στο οποίο υπάρχουν εχθρικό. Προβλήματα τόσο στην ασφάλεια των συστημάτων όσο και στην ιδιωτικότητα προκύπτουν από τα ανθρώπινα λάθη και τις σκόπιμες δράσεις, που εκθέτουν τα στοιχεία του συστήματος IoMT και κατ'έκταση το ίδιο σε κινδύνους.

Γενικότερα, τα ιατρικά συστήματα γίνονται θύματα παραβιάσεων, καθώς τα ευαίσθητα προσωπικά δεδομένα είναι θελκτικό αντικείμενο των επιτιθέμενων για οικονομικούς παράγοντες. Η πλειονότητα των εφαρμογών και προγραμμάτων που χρησιμοποιούνται είναι ξεπερασμένων τεχνολογιών (outdated), χαρακτηριστικό που τα εκθέτει απέναντι σε επιθέσεις (Noimanee et al., 2016).

Μεγάλα ζητήματα από τις παραβιάσεις των ευαίσθητων δεδομένων στα συστήματα IoMT προκύπτουν και στο τομέα της ιδιωτικότητας. Η ενσωμάτωση των συστημάτων IoT στα δίκτυα, αποτελεί βασικό παράγοντα για τους παραβάτες, καθώς οι συσκευές αποτελούν το αδύναμο σημείο από το οποίο εισέρχονται στα πληροφοριακά συστήματα ενός οργανισμού, αποκτώντας πρόσβαση στις ευαίσθητες πληροφορίες των παρελκόμενων ατόμων (Yu et al., 2015).

Στη συνέχεια του κεφαλαίου γίνεται εκτενής αναφορά στα προβλήματα της ασφάλειας και της ιδιωτικότητας των συστημάτων IoMT, δίνοντας βάση στις τεχνολογίες και τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται καταγράφοντας τις απειλές, τις αδυναμίες που προκύπτουν και τις επιπτώσεις που αυτά έχουν στα συστήματα IoMT εξετάζοντας τις περιπτώσεις παραβιάσής τους.

3.1 Απειλές Ασφάλειας στα Συστήματα IoMT

Όπως αναφέρθηκε, τα συστήματα IoMT δεν διαθέτουν ισχυρά μέτρα, που να ασφαλίζουν το σύστημα και τη πληροφορία. Αναπόφευκτα, οι επιτιθέμενοι επιχειρούν

να παραβιάσουν το σύστημα, έτσι ώστε να αποκτήσουν πρόσβαση στα ιατρικά δεδομένα των χρηστών. Παρακάτω, αναλύονται οι παθητικές και ενεργητικές επιθέσεις που διεκπεραιώνονται στα συστήματα IoMT, με βάση το επίπεδο της αρχιτεκτονικής (βλ. 2.9) και τη τεχνολογία που χρησιμοποιείται.

Στις παθητικές επιθέσεις, ο επιτιθέμενος (hacker) στη πλειονότητα των περιπτώσεων δεν γίνεται αντιληπτός. Μπορεί απλά να 'κρυφτεί' στο σύστημα πραγματοποιώντας λόγω χάριν επίθεση Eavesdropping, σε ένα κανάλι επικοινωνίας μεταξύ του δικτύου WBAN ενός χρήστη και του συνολικού δικτύου, αποκτώντας γνώση τόσο για το σύστημα όσο και για τα δεδομένα των χρηστών. Οι παθητικές επιθέσεις επηρεάζουν και τη περίπτωση της ιδιωτικότητας που θα αναλυθεί παρακάτω. Στις περιπτώσεις των συστημάτων IoMT, ίσως μία παθητική επίθεση να θεωρηθεί πιο κερδοφόρα σε σχέση με μία ενεργητική. Οι hackers πλέον, έχουν στραφεί στα οικονομικά πλεονεκτήματα που μπορούν να αποκτήσουν, πουλώντας τα αποκτηθέντα δεδομένα σε ενδιαφερόμενες οντότητες (Wirth A., 2016). Ο επιτιθέμενος μπορεί να ανακτήσει ένα μεγάλο αριθμό ευαίσθητων δεδομένων και έπειτα να τα εκμεταλλευτεί οικονομικά.

Οι ενεργητικές επιθέσεις, είναι πιο επικίνδυνες από τις παθητικές. Μπορούν να προκαλέσουν προβλήματα λειτουργικότητας και διαθεσιμότητας στο σύστημα, τα οποία ως επακόλουθο έχουν και τη πρόκληση προβλημάτων υγείας σε ασθενείς. Για παράδειγμα, εάν ο επιτιθέμενος παραβιάσει την αντλία ινσουλίνης ενός ασθενούς, καταστέλλοντας την λειτουργία του, μπορεί να οδηγήσει μέχρι και στο θάνατο του χρήστη. Στη περίπτωση των ενεργητικών επιθέσεων, είναι πιθανόν να συμβούν είτε από λάθος, είτε από έναν ιό που εξαπλώνεται σε διάφορα συστήματα μέσω του διαδικτύου. Όσον αφορά τα συστήματα IoMT, είναι λιγότερο πιθανό να συμβεί μια ενεργητική παράβαση, καθώς οι hackers δεν στοχεύουν τόσο στην φήμη και στην δημιουργία προβλημάτων στους χρήστες των ιατρικών συστημάτων, όσο στο κέρδος από οικονομική άποψη (Noimanee et al., 2016).

Στα δίκτυα IoMT, οι συσκευές για να επικοινωνήσουν μεταξύ τους, χρησιμοποιούν πρωτόκολλα και τεχνολογίες, με τα οποία εδραιώνονται τα κανάλια επικοινωνίας. Οι συσκευές έτσι δημιουργούν μικρά τοπικά δίκτυα, στα οποία βρίσκονται σε συνεχή αλληλεπίδραση για την διεκπεραίωση των απαιτούμενων ιατρικών διεργασιών. Τα πρωτόκολλα αυτά ποικίλουν. Χρησιμοποιούνται στα τοπικά δίκτυα που δημιουργούνται με επίκεντρο τον ασθενή, έτσι ώστε να προσφέρονται με βέλτιστο και ασφαλή τρόπο οι ιατρικές υπηρεσίες. Επιπλέον, πρωτόκολλα χρησιμοποιούνται και για την εδραίωση καναλιών επικοινωνίας των υποδικτύων με το συνολικό δίκτυο. Η ανάλυση των προκλήσεων στα συστήματα IoMT γίνονται με γνώμονα τα τρία επίπεδα της προτεινόμενης αρχιτεκτονικής στο Σχ. 2.9.

Φυσικό Επίπεδο (Tier-1)

Το πρώτο επίπεδο αποτελεί και το επίπεδο περισυλλογής, στο οποίο ανήκουν όλες οι συσκευές και οι αισθητήρες, που έρχονται σε έμμεση ή άμεση επαφή με τον χρήστη και λαμβάνουν τα βιομετρικά δεδομένα του ασθενούς, προωθώντας από τις δικτυακές δομές στο κόμβο παραλήπτη. Εδώ, εφαρμόζουν οι Φορετές και Εμφυτευμένες συσκευές, αλλά και οι συσκευές που χρησιμοποιούνται για την παρακολούθηση του ασθενούς, όπως οι συσκευές Smart Home Appliances. Επιπλέον, με τις συσκευές Smartphone οι χρήστες έχουν τη δυνατότητα να αλληλεπιδρούν με το προσωπικό δίκτυο τους (WPAN). Αποτελεί το πιθανό σημείο εισόδου των επιτιθέμενων, καθώς οι συσκευές IoMT διαθέτουν χαμηλά επίπεδα υπολογιστικών πόρων και ισχύος. Η διασφάλιση της τριάδας CIA στις συσκευές IoMT αποτελεί σημαντική πρόκληση για τους σχεδιαστές

των συστημάτων, καθώς κινδυνεύει άμεσα η ψυχοσωματική υγεία του χρήστη.

Τα προβλήματα στο πρώτο επίπεδο προκύπτουν τόσο από τις ενέργειες των χρηστών, όσο και από τις αδυναμίες που υπάρχουν στις τεχνολογίες που χρησιμοποιούνται. Στις συσκευές IoT χρησιμοποιούνται κατά κόρον οι τεχνολογίες Bluetooth, RFID, NFC, ZigBee. Αντίστοιχα, και στις συσκευές IoMT, χρησιμοποιούνται οι ίδιες τεχνολογίες. Ωστόσο, οι συγκεκριμένες τεχνολογίες είναι ευάλωτες σε πληθώρα επιθέσεων (Alzahrani et al., 2013; Chahid et al., 2017; Chen et al., 2017; Hassan et al., 2018; Jain et al., 2018; Lonsetta et al., 2018; Ronen et al., 2017), γεγονός που δημιουργεί κώλυμα στην εφαρμογή τους στα συστήματα IoMT, λόγω της φύσης των ευαίσθητων δεδομένων.

Επίπεδο Δικτύου (Tier-2)

Όσον αφορά το επίπεδο δικτύου βρίσκονται οι δικτυακές και υπολογιστικές υποδομές, οι οποίες γίνονται θελκτικό αντικείμενο παραβίασης των επιτιθέμενων. Οι κόμβοι επικοινωνίας του δικτύου που βρίσκονται διασκορπισμένοι στα δίκτυα WAN και MAN, είναι εύκολα προσβάσιμα για τους επιτιθέμενους, καθώς είναι εκτεθειμένα και συνήθως δεν διαθέτουν μέτρα ασφάλειας. Η παραβίαση του υπολογιστικού νέφους είναι εφικτή, ωστόσο δεν είναι εξίσου εύκολη (Ali et al., 2015). Όπως τονίστηκε στο Σχ. 2.7 σημαντικό ρόλο παίζουν οι συντονιστές (Coordinator) και οι δρομολογητές (Router). Από αυτές προωθούν τα βιομετρικά δεδομένα των αισθητήρων που αντιστοιχούν στους χρήστες του δικτύου. Ως αποτέλεσμα, ένας παραβάτης μπορεί να επιτεθεί στις συγκεκριμένες συσκευές για να κερδίσει μεγαλύτερο αριθμό δεδομένων. Οι τεχνολογίες που χρησιμοποιούνται σε αυτό το επίπεδο για την διαβίβαση των αιτημάτων και των πακέτων δεδομένων είναι οι MQTT, CoAP, AMQP, XMPP και 6LoWPAN. Ενώ, εφαρμόζουν στα συστήματα IoT, στις ιατρικές υπηρεσίες υστερούν ως προς την διαλειτουργικότητα, απόδοση, διαχείριση πόρων και ασφάλεια (Burange et al., 2018; Nitin Naik, 2017; Pongle et al, 2015; Yokotani. T and Sasaki Y., 2016).

Τα προβλήματα στο δεύτερο επίπεδο προκύπτουν από ελαττώματα των τεχνολογιών που χρησιμοποιούνται και την εκμετάλλευση των ευάλωτων σημείων από τους επιτιθέμενους. Σε ένα σύστημα IoMT οι επιτιθέμενοι προσπαθούν να προσπελάσουν το πιο αδύναμο σημείο, το οποίο θα τους προσφέρει τη μέγιστη δυνατή πληροφορία. Οι συντονιστές αποτελούν ένα κομβικό σημείο, καθώς μεγάλες ποσότητες από διαφορετικούς χρήστες φτάνουν σε αυτούς. Δεύτεροι έρχονται οι δρομολογητές, οι οποίοι αφορούν ένα μικρότερο υποσύνολο υποδικτύων. Και στις δύο περιπτώσεις οι παραβιάσεις των δύο τύπων συσκευών σημαίνει την έκθεση των χρηστών του συστήματος.

Επίπεδο Εφαρμογής (Tier-3)

Στο επίπεδο εφαρμογής ανήκουν οι αποθηκευτικές δομές του συστήματος, δηλαδή οι βάσεις δεδομένων. Επιπλέον, στο τρίτο επίπεδο γίνεται η αλληλεπίδραση των χρηστών με το σύστημα μέσω της διεπαφής του χρήστη. Η διασφάλιση των υποδομών αποτελεί τη μεγαλύτερη πρόκληση. Η πιθανή παραβίαση του καταστέλλει την λειτουργία του συστήματος και εκθέτει τα ευαίσθητα προσωπικά δεδομένα των χρηστών.

Με τη παραβίαση των υποδομών ενός συστήματος IoMT, παραβιάζεται το ιατρικό απόρρητο δημιουργώντας νομικά προβλήματα. Επιπλέον, η καταστολή του συστήματος IoMT θέτει σε κίνδυνο και την ακεραιότητα των χρηστών, αφού θα σταματήσουν να λειτουργούν οι προσφερόμενες ιατρικές υπηρεσίες για ένα χρονικό διάστημα. Σε κάθε περίπτωση η διασφάλιση τους είναι απαραίτητη για την συνολική λειτουργία του συστήματος. Η σχετική βιβλιογραφία για τα στοιχεία των επιπέδων βρίσκεται στα άρθρα Yao et al., 2017; Jain et al., 2018; Singh M. and Hassan R., 2015; Jokar P. and

Leung V., 2016; Ronen et al., 2017.

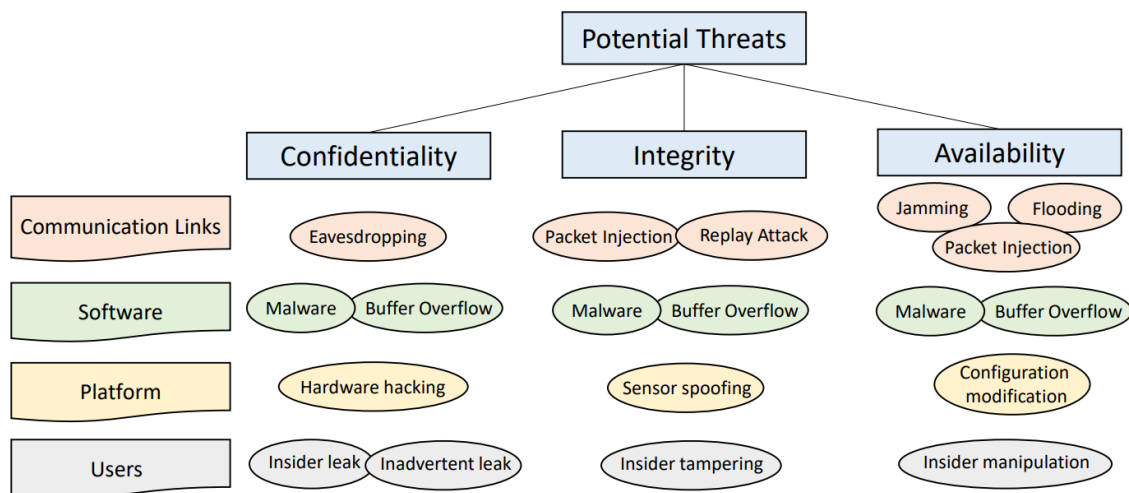
Τα προβλήματα με τα οποία έρχονται αντιμέτωπα τα συστήματα IoMT κυμαίνονται μεταξύ της λειτουργικότητας του συστήματος και της ασφάλειας. Οι δύο περιπτώσεις αλληλοεξαρτώνται. Στα συστήματα IoMT οι βασικοί παράγοντες, που ευθύνονται για τα κενά στην ασφάλεια των συστημάτων είναι:

- **Χαμηλοί Ενεργειακοί Πόροι:** Οι συσκευές IoT δεν διαθέτουν ισχυρή Επεξεργαστική ισχύ. Έτσι, είναι δύσκολη η εφαρμογή ισχυρών κρυπτογραφικών τεχνικών, που θα διασφαλίσουν τα βιομετρικά δεδομένα του ασθενούς. Επιπλέον, δεν μπορούν να εφαρμόσουν τεχνικές ανίχνευσης ή αντιμετώπισης απειλών, καθώς ένα μεγάλο μέρος των ενεργειακών πόρων χρησιμοποιείται για την εκτέλεση των ιατρικών υπηρεσιών. Από την άλλη, οι χαμηλοί Αποθηκευτικοί πόροι δημιουργούν κενά στην ασφάλεια, καθώς μια επίθεση που θα υπερφορτώσει τη μνήμη των αισθητήρων όπως οι Buffer overflow και SQL Injection μπορεί να έχουν ως αποτέλεσμα την καταστολή της λειτουργίας τους και κατ'επέκταση των ιατρικών υπηρεσιών.

Επιπλέον, οι Thibaud et al., 2018 προσθέτουν τρεις παράγοντες για τα high-risk Environment, Health and Safety (EHS) περιβάλλοντα, οι οποίοι ευθύνονται για την εμφάνιση αδυναμιών που απειλούν τα συστήματα IoMT:

- **Ασφάλεια και Ιδιωτικότητα:** Το ζήτημα της Ασφάλειας, αναμενόμενα είναι αρκετά κρίσιμο, καθώς τα συστήματα IoMT λειτουργούν πάνω σε ευαίσθητα προσωπικά δεδομένα, και η διαρροή τους μπορεί να δημιουργήσουν ζωτικά προβλήματα στους χρήστες του συστήματος. Έτσι, η Ασφάλεια εκ του Σχεδιασμού (Secure by Design) αποτελεί μια από τις μεγαλύτερες προκλήσεις, που έχουν να αντιμετωπίσουν οι σχεδιαστές των συστημάτων. Όπως αναφέρουν οι Al-Janabi et al., 2017 μεταξύ άλλων, το σύστημα στο σύνολο του πρέπει να είναι ασφαλές μαζί με τα αρχεία των ασθενών, τα οποία θα είναι καταλλήλως μορφοποιημένα. Εξίσου σημαντική είναι η διατήρηση της Ιδιωτικότητας, η οποία αποτελεί μείζον ζήτημα για τους σχεδιαστές των συστημάτων IoMT, αφού σε κάθε άλλη περίπτωση κινδυνεύει η σωματική και ψυχική ακεραιότητα των χρηστών.
- **Ανάπτυξη Standard προτύπων:** Εξαιτίας της μεγάλης πληθώρας τεχνολογιών που χρησιμοποιούνται στα συστήματα IoMT, κρίνεται απαραίτητη η ύπαρξη ενός προτύπου επικοινωνίας, το οποίο οι τεχνολογίες θα ακολουθούν για την ομαλή επικοινωνία των συσκευών μέσα στο δίκτυο. Η δημιουργία ενός προτύπου είναι απαραίτητη για περιβάλλοντα με ετερογενείς πηγές δεδομένων, ενισχύοντας την διαλειτουργικότητα μεταξύ των ετερογενών συσκευών. Η έλλειψη του προκαλεί ζητήματα απόδοσης και λειτουργικότητας στο σύστημα.
- **Επεκτατική Διάθεση των Δικτύων IoMT:** Εφόσον αυξάνεται ο πιθανός αριθμός των χρηστών στα συστήματα και των συσκευών που του αντιστοιχούν με άγνωστο ρυθμό, είναι απαραίτητο τα συστήματα να έχουν επεκτατική ικανότητα, δηλαδή κρατώντας την ομοιογένεια του δικτύου και ρυθμίζοντας κατάλληλα την ενεργειακή απόδοση του, να προσθέτουν τα καινούργια στοιχεία στο σύστημα. Επιπλέον, η Επεκτασιμότητα αναφέρεται στην ικανότητα του δικτύου να μπορέσει να ανταπεξέλθει σε περιπτώσεις αυξανόμενης ποσότητας διεργασιών στο δίκτυο. Η έλλειψη της Επεκτατικής διάθεσης μπορεί να οδηγήσει στη καταστολή του συστήματος. Για παράδειγμα μια επίθεση DDoS, η οποία γίνεται με την αποστολή αφύσικα μεγάλης ποσότητας δεδομένων από τις συσκευές IoMT που αντιστοιχούν σε έναν χρήστη.

Παρακάτω αναλύονται τα προβλήματα, που προκύπτουν στα επίπεδα της προτεινόμενης αρχιτεκτονικής (βλ. Σχ. 2.9). Η ανάλυση γίνεται με γνώμονα την τριάδα CIA, εξετάζοντας ξεχωριστά για κάθε επίπεδο τα προβλήματα που προκύπτουν σε θέματα Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητα, ανακαλύπτοντας τα αδύναμα σημεία του συστήματος και τις συνέπειες που οι παραβιάσεις μπορεί να επιφέρουν. Οι Almohri et al., 2017, όπως στη Πτυχιακή Εργασία παραθέτουν τις απειλές που βρίσκονται στο Σχ. 3.1 και τις χωρίζουν με βάση τα στρώματα επικοινωνίας και την τριάδα CIA, ωστόσο χρησιμοποιούν μοντέλο επικοινωνίας τεσσάρων στρωμάτων.



Σχήμα 3.1: Παραδείγματα επιθέσεων στα μοντέλο επικοινωνίας 4 στρωμάτων σε σχέση με τη τριάδα CIA. Adapted from ‘On threat modeling and mitigation of medical cyber-physical systems’, by H. Almohri et al., 2017.

3.1.1 Απειλές Εμπιστευτικότητας στα Συστήματα IoMT

Η έννοια της Εμπιστευτικότητας (C) εγγυάται ότι τα ιατρικά δεδομένα των χρηστών δεν θα φτάσουν σε άλλους χρήστες ή σε ξένες οντότητες, παρά μόνον στον κόμβο παραλήπτη που αυτοί επιθυμούν, όπως ο θεράπωντα γιατρός τους, μια νοσοκομειακή μονάδα ή στις αποθηκευτικές δομές του συστήματος όπως τα υπολογιστικά νέφη και οι βάσεις δεδομένων. Επιπλέον, εξασφαλίζει ότι τα αιτήματα που διαμοιράζονται φτάνουν στους επιθυμητούς χρήστες, όπως για παράδειγμα η απομακρυσμένη ρύθμιση ενός βηματοδότη από τον θεράπωντα γιατρό.

Με την Εμπιστευτικότητα συνδέεται άρτια η έννοια της Ιδιωτικότητας που αναλύεται παρακάτω, καθώς η μη εξουσιοδοτημένη πρόσβαση στα ευαίσθητα δεδομένα των χρηστών, αυτόματα σημαίνει απειλή προς την ιδιωτικότητα. Για παράδειγμα δεδομένου ενός χρήστη του συστήματος, ο οποίος πάσχει από καρδιακά προβλήματα και χρησιμοποιεί μια συσκευή Wristband για να κρατάει ιστορικό του καρδιογραφήματος του. Εφόσον ο χρήστης από αμέλεια αφήσει τη συσκευή του ανιχνεύσιμη, ο επιτιθέμενος εκτελώντας μια επίθεση Bluesnarfing μπορεί να αποκτήσει πρόσβαση στο ιστορικό του καρδιογραφήματος του χρήστη. Οι παθητικές επιθέσεις είναι πιθανότερο να προσβάλλουν την Εμπιστευτικότητα του συστήματος. Έτσι, η βλάβη που θα υποστεί το σύστημα και οι χρήστες είναι ανεπανόρθωτη, διότι και στα τρία επίπεδα διαμοιράζονται τα ευαίσθητα προσωπικά δεδομένα των χρηστών.

3.1.1.1 Απειλές στο Φυσικό Επίπεδο (Tier-1)

Οι επιθέσεις τύπου Man-in-the-Middle (MitM) μεταξύ συσκευών και κόμβων στα τοπικά δίκτυα των χρηστών συνήθως δημιουργούν θέματα εμπιστευτικότητας, καθώς οι επιτιθέμενοι υποκλέπουν τα δεδομένα που ταξιδεύουν μεταξύ των κόμβων. Οι επιθέσεις στην τεχνολογία Bluetooth Bluesnarfing και Bluebugging, προκύπτουν από την αφέλεια των χρηστών, όπου μη εξουσιοδοτημένοι χρήστες αποκτούν πρόσβαση σε ανιχνεύσιμες συσκευές αποκαλύπτοντας τα ευαίσθητα προσωπικά δεδομένα των χρηστών. Η εμπιστευτικότητα των συστημάτων IoMT παραβιάζεται όταν με την επίθεση Sensor Tracking γνωστοποιείται στον επιτιθέμενο η τοποθεσία ενός αισθητήρα και ταυτόχρονα προσωπικά στοιχεία για τον χρήστη του, εμφανίζοντας στοιχεία που τον αναγνωρίζουν μοναδικά όπως η τοποθεσία του.

Η επίθεση Replay επιτρέπει σε μη εξουσιοδοτημένες οντότητες να αποκτήσουν πρόσβαση σε πολλαπλές συνόδους μεταξύ συσκευών. Ένας επιτιθέμενος κάνοντας μια επίθεση Spoofing κατά των συσκευών και αισθητήρων του δικτύου μπορεί να αποκτήσει πρόσβαση σε ένα μεγάλο σύνολο ευαίσθητων προσωπικών δεδομένων. Για παράδειγμα, ένας επιτιθέμενος προσποιούμενος έναν χρήστη του δικτύου μπορεί να αποκτήσει πρόσβαση στον Ηλεκτρονικό Φάκελο Υγείας του. Οι συνέπειες στο πρώτο επίπεδο μπορεί να είναι μικρότερης κλίμακας, αλλά έχουν την ίδια αξία.

3.1.1.2 Απειλές στο Επίπεδο Δικτύου (Tier-2)

Όπως αναφέρθηκε, οι συσκευές που εφαρμόζουν στο επίπεδο δικτύου είναι οι συντονιστές και οι δρομολογητές. Επιπλέον, χρησιμοποιούνται συσκευές Raspberry Pi και ZigBee. Γίνονται αντικείμενο παραβίασης, καθώς είναι εύκολο να αποκτήσουν πρόσβαση σε έναν μεγάλο αριθμό δεδομένων. Προβλήματα δημιουργούνται όταν δεν υπάρχουν μηχανισμοί ανίχνευσης ύποπτης συμπεριφοράς. Επίσης, προβλήματα δημιουργούνται όταν στις συσκευές φτάνουν πακέτα δεδομένων που δεν έχουν διασφαλιστεί με μεθόδους κρυπτογράφησης.

Χαρακτηριστική επίθεση στο δεύτερο επίπεδο αποτελεί η Eavesdropping, όπου οι παραβάτες μπορούν να συλλέξουν μεγάλες ποσότητες ιατρικών δεδομένων από πληθώρα χρηστών. Επιθέσεις όπως Buffer overflow οδηγούν στην παραβίαση του συστήματος και στην διαρροή των βιομετρικών δεδομένων των χρηστών. Σε συνέχεια με τη παραπάνω, επιθέσεις DDoS στα υπολογιστικά νέφη έχουν ως αποτέλεσμα την διαρροή προσωπικών δεδομένων. Οι συνέπειες του δεύτερου επιπέδου είναι μεγαλύτερης κλίμακας, αφού παραβιάζονται και ανακτούνται τα βιομετρικά δεδομένα μεγάλου αριθμού χρηστών.

3.1.1.3 Απειλές στο Επίπεδο Εφαρμογής (Tier-3)

Προβλήματα στην Εμπιστευτικότητα του τρίτου επιπέδου δημιουργούνται όταν μη εξουσιοδοτημένες οντότητες καταφέρουν να κερδίσουν σε γνώση εντός των δικτυακών υποδομών. Αυτό συμβαίνει συνήθως όταν δεν υπάρχουν κατάλληλοι μηχανισμοί ανίχνευσης και αντιμετώπισης παραβατικών συμπεριφορών. Εάν τα συστήματα δεν ασφαλιστούν σωστά και ταυτόχρονα δεν εκπαιδευτεί το ανθρώπινο δυναμικό που το διαχειρίζεται κατάλληλα, τότε είναι πιθανή η διαρροή δεδομένων εκ των έσω (Insider leak) ή ακούσια (Inadvertent leak). Επιθέσεις MitM, Spoofing, Counterfeiting και Replay είναι πιθανό να συμβούν επιπλέον. Και οι δύο περιπτώσεις προβλημάτων εκθέτουν έναν

αριθμό χρηστών του δικτύου, καθώς είναι άγνωστο το μέγεθος των επιθέσεων σε αυτές τις δομές. Στο τρίτο επίπεδο μεγιστοποιούνται οι συνέπειες στην Εμπιστευτικότητα, καθώς παραβιάζεται το σύστημα και αποκαλύπτεται ένας μεγάλος αριθμός προσωπικών δεδομένων άγνωστης αξίας.

3.1.2 Απειλές Ακεραιότητας στα Συστήματα IoMT

Η έννοια της Ακεραιότητας (I) εξασφαλίζει την αξιοπιστία και τη συνέπεια των δεδομένων ενός χρήστη. Είναι χρήσιμη για τα συστήματα IoMT, καθώς είναι θεμιτό τα δεδομένα του χρήστη να παραμένουν άθικτα, ενώ μόνο οι εξουσιοδοτημένοι χρήστες έχουν δικαίωμα να τα επεξεργάζονται, διασφαλίζοντας έτσι και το ιατρικό απόρρητο. Επιπλέον, διασφαλίζεται και η ακρίβεια των δεδομένων, στοιχείο σημαντικό για τα συστήματα IoMT, καθώς η αλλοίωση της πληροφορίας θέτει σε κίνδυνο τους χρήστες του συστήματος. Για παράδειγμα, η αλλοίωση των μετρήσεων μιας αντλίας ινσουλίνης, μπορεί να οδηγήσει στην λανθασμένη ποσότητα έγχυσης ινσουλίνης στον οργανισμό του χρήστη.

Η Ακεραιότητα των βιομετρικών δεδομένων στα συστήματα IoMT πρέπει να εξασφαλίζεται εκ του σχεδιασμού, αφού οι λειτουργίες του εξαρτώνται από την ακρίβεια και την εγκυρότητα των δεδομένων. Η ανάλυση και επεξεργασία των δεδομένων απαιτεί την ορθότητα τους. Για παράδειγμα, είναι θεμιτό οι μετρήσεις από το σύνολο των αισθητήρων που αντιστοιχούν σε έναν ασθενή να αντικατοπτρίζουν τη πραγματική εικόνα του ασθενούς, έτσι ώστε να γνωστοποιείται στον θεράποντα γιατρό και να χορηγεί τις κατάλληλες οδηγίες στον χρήστη.

3.1.2.1 Απειλές στο Φυσικό Επίπεδο (Tier-1)

Η Ακεραιότητα στο πρώτο επίπεδο κατέχει σημαντικό ρόλο, αφού η διατήρηση της ακρίβειας και ορθότητας των δεδομένων είναι σημαντική για τα ιατρικά συστήματα. Συνήθως, το πρόβλημα της έλλειψης ελέγχου για την εγκυρότητα των δεδομένων, των κόμβων αποστολών και της ταυτότητας των χρηστών οδηγεί στην μείωση της Ακεραιότητας του δικτύου. Επιπλέον, ένα σύνηθες πρόβλημα για την Ακεραιότητα είναι η κίνηση του σώματος, μειώνοντας την ακρίβεια των μετρήσεων. Οι δύο επιθέσεις (Bluebugging, Bluesnarfing) της τεχνολογίας Bluetooth επιτρέπουν την τροποποίησή των δεδομένων.

Οι παραπάνω επιθέσεις μπορούν να συνδυαστούν με επίθεση Replay, όπου ο χρήστης αποκτώντας μη εξουσιοδοτημένη πρόσβαση από τις προηγούμενες συνόδους μπορεί να στείλει δεδομένα διαφορετικά από αυτά που αντιστοιχούν στον χρήστη. Η φύση της τεχνολογίας RFID επιτρέπει επιθέσεις τύπου Counterfeiting και Masquerade. Τα αδύναμα σημεία της τεχνολογίας NFC μπορεί να οδηγήσουν σε επιθέσεις Phishing και Relay (Singh et al., 2018). Έτσι, προκύπτει η αλλοίωση των ιατρικών δεδομένων, η οποία μπορεί να οδηγήσει στη λανθασμένη διάγνωση παθήσεων ή ακόμα και στην χορήγηση μη ορθής θεραπευτικής αγωγής, προσβάλλοντας έτσι τον χρήστη του δικτύου.

3.1.2.2 Απειλές Επίπεδο Δικτύου (Tier-2)

Φυσικά, η Ακεραιότητα των δεδομένων στο δεύτερο επίπεδο μπορεί να αλλοιωθεί από την επίθεση Buffer overflow, καθώς μπορεί να οδηγήσει στην παραβίαση του συστήματος, όπου οι επιτιθέμενοι να είναι σε θέση να επεξεργαστούν το περιεχόμενο. Στα συστήματα IoMT, επιθέσεις Replay επιχειρούν να προσθέσουν περιεχόμενο, το οποίο θα διαφοροποιήσει τα δεδομένα ενός χρήστη. Εφικτές είναι και οι επιθέσεις Packet Injection, οι οποίες προσομοιώνουν μια επίθεση Spoofing εκ των έσω, στέλνοντας πακέτα δεδομένων στο σύστημα IoMT ως εξουσιοδοτημένη οντότητα. Για παράδειγμα, μια συσκευή, η οποία εκτελεί κατ' οίκον μελέτη ύπνου και αυτόματα στέλνει στον θεράποντα γιατρό τα αποτελέσματα. Μια επίθεση Replay μπορεί να αλλοιώσει τα αποτελέσματα και να δοθεί στον ασθενή θεραπεία που δεν του αντιστοιχεί.

3.1.2.3 Απειλές στο Επίπεδο Εφαρμογής (Tier-3)

Στο τρίτο επίπεδο, τα προβλήματα δημιουργούν απειλές που επικεντρώνονται στην απόκτηση όσο το δυνατόν περισσότερης γνώσης. Επιθέσεις Masquerade και MitM ως προς την Ακεραιότητα μπορεί να επιφέρουν σημαντικά προβλήματα στα συστήματα IoMT και κατ' επέκταση στους χρήστες, καθώς τα ιατρικά δεδομένα των χρηστών αλλοιώνονται. Επιπλέον, είτε ακούσια είτε οικειοθελώς μπορεί να γίνει αλλοίωση των δεδομένων εκ των έσω (Data Tampering). Για παράδειγμα, το προσωπικό που διαχειρίζεται το σύστημα IoMT, λόγω χάριν η γραμματειακή υποστήριξη μιας νοσοκομειακής μονάδας να αλλοιώσει τα στοιχεία των ασθενών.

3.1.3 Απειλές Διαθεσιμότητας στα συστήματα IoMT

Η έννοια της Διαθεσιμότητας (A) είναι κρίσιμη για τα δίκτυα IoMT. Εξαιτίας της φύσης των δεδομένων τα συστήματα IoMT πρέπει να είναι μονίμως διαθέσιμα. Πιο συγκεκριμένα με την διαθεσιμότητα εξασφαλίζεται η λειτουργικότητα και η ακεραιότητα του υλικολογισμικού(hardware) των συστημάτων. Η Διαθεσιμότητα των συστημάτων IoMT είναι κρίσιμη. Το προσωπικό δίκτυο του χρήστη πρέπει πάντα να είναι διαθέσιμο για να επικοινωνήσει με το υπόλοιπο δίκτυο, όπως επίσης και οι συσκευές του χρήστη. Τόσο τα δεδομένα όσο και το σύστημα πρέπει να είναι πάντα διαθέσιμα στους χρήστες.

Η χαμηλή διαθεσιμότητα σε υπολογιστικούς και ενεργειακούς πόρους αντικρο-ύει την απόδοση του συστήματος με την ασφάλεια του, δημιουργώντας τα ζητήματα trade-offs. Στα συστήματα IoMT απόδοση και ασφάλεια είναι απαραίτητη για την εκτέλεση των ιατρικών υπηρεσιών και διασφάλιση τους. Το παραπάνω πρόβλημα οδηγεί στην δημιουργία κενών στην ασφάλεια. Παραδείγματος χάριν, ένας χρήστης του συστήματος, στον οποίο συμβαίνει ένα επείγον περιστατικό. Το σύστημα πρέπει να έχει την δυνατότητα ανά πάσα στιγμή να διαθέσει τα προσωπικά δεδομένα του όπως τον Ηλεκτρονικό Φάκελο Υγείας στον χρήστη ή τον επείγοντα γιατρό και την επικοινωνία με τον θεράποντα γιατρό του. Η καταστολή της διαθεσιμότητας του συστήματος, επιφέρει σοβαρές συνέπειες στην ψυχοσωματική υγεία των χρηστών, αφού σταματάνε οι παρεχόμενες ιατρικές υπηρεσίες.

Οι Alsubaei F. and Abuhussein A., 2017 στην ερευνητική τους εργασία κατέγραψαν τις απειλές προς τη τριάδα CIA με βάση το μοντέλο πέντε στρωμάτων επι-

κοινωνίας των IoMT συσκευών, διαφορετικό από αυτό της Πτυχιακής Εργασίας (βλ. Κεφάλαιο 2.2.1). Από τη μελέτη οι συγγραφείς ανέλυσαν τις επιθέσεις σε κάθε στρώμα επικοινωνίας με βάση τους τύπους συσκευών που όρισαν, σε Εμφυτευμένες, Φορητές, Στατικές και ΣΑΠ. Διέκριναν ότι επιθέσεις στις έννοιες της Εμπιστευτικότητας και Διαθεσιμότητας είναι πιθανότερο να συμβούν όπως οι Eavesdropping και Tag cloning και λιγότερο στην έννοια της Διαθεσιμότητας όπως επιθέσεις DoS και Replay. Γεγονός το οποίο δεν προκαλεί έκπληξη αφού όπως αναφέρθηκε παραπάνω (βλ. Κεφάλαιο 3.1) οι επιτιθέμενοι επιθυμούν στα συστήματα IoMT να κερδίσουν σε γνώση παρά να το καταστείλουν. Έτσι, υφίσταται μεγαλύτερη προσοχή στη διασφάλιση των εννοιών της Εμπιστευτικότητας και Ακεραιότητας. Στον Πίνακα 3.1 παραθέτονται οι απειλές κατά της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας με βάση τα τρία επίπεδα της προτεινόμενης αρχιτεκτονικής.

CIA	Επίπεδο	Απειλές
Εμπιστευτικότητα	Επίπεδο 1	MitM, Bluesnarfing, Bluebugging, Sensor Tracking, Replay, Spoofing
	Επίπεδο 2	Eavesdropping, Buffer overflow, DDoS
	Επίπεδο 3	Insider Leak, Inadvertent Leak, MitM, Spoofing, Counterfeiting, Relay
Ακεραιότητα	Επίπεδο 1	Bluebugging, Bluesnarfing, Replay, Counterfeiting, Masquerade, Phishing, Relay
	Επίπεδο 2	Buffer overflow, Replay, Packet Injection, Spoofing
	Επίπεδο 3	Masquerade, MitM, Data Tampering
Διαθεσιμότητα	Επίπεδο 1	DoS, DDoS, RoS, Brute-force, Jamming
	Επίπεδο 2	DoS, DDoS, RoS, Brute-force, Jamming, Flooding, Packet Injection
	Επίπεδο 3	DoS, DDoS, RoS, Brute-force, Buffer overflow, Insider manipulation

Πίνακας 3.1: Συνοπτική παράθεση των απειλών στα συστήματα IoMT με βάση την Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα

Τα συστήματα IoMT αντιμετωπίζουν προβλήματα, εξαιτίας της φύσεως των δεδομένων, των ελλειπών μέτρων ασφάλειας στα συστήματα και τις τεχνολογίες που χρησιμοποιούνται, όπως επίσης και στους υπολογιστικούς και ενεργειακούς περιορισμούς που υπάρχουν. Επιπρόσθετα, υπάρχει και ο ανθρώπινος παράγοντας, όπου είτε από αμέλεια είτε οικειοθελώς παραβιάζεται το σύστημα. Μάλιστα, η επίθεση διαρροής εκ των έσω είναι πιθανή για καταστολή της Διαθεσιμότητας. Από τα προβλήματα γεννιέται μια σειρά απαιτήσεων, που τα προτεινόμενα μέτρα ασφάλειας στην βιβλιογραφία πρέπει να καλύψουν. Στο κεφάλαιο που ακολουθεί παρατίθενται το σύνολο των απαιτήσεων που

χρειάζονται για την αντιμετώπιση των προβλημάτων στα συστήματα IoMT.

3.1.3.1 Απειλές στο Φυσικό Επίπεδο (Tier-1)

Οι επιτιθέμενοι, όταν διατελούν επιθέσεις κατά της Διαθεσιμότητας, στοχεύουν κυρίως στην εξάντληση των πόρων. Οι Επιθέσεις DoS, DDoS, RoS και Brute-force χρησιμοποιούνται για το σκοπό αυτό. Στέλνοντας τεράστιες ποσότητες δεδομένων στις συσκευές, στη προσπάθεια τους να επεξεργαστούν όλα τα αιτήματα, εξαντλούν τα ενεργειακά τους αποθέματα ή υπερφορτώνοντας τα επεξεργαστικά αποθέματα, καταστέλλοντας την λειτουργία τους.

Επιπρόσθετα, προσπαθούν να κλείσουν τις διόδους επικοινωνίας μεταξύ συσκευών και κόμβων. Χαρακτηριστική επίθεση αποτελεί η Jamming, όπου είναι υποσύνολο της επίθεσης DoS, παρεμβάλλοντας με σήματα μεταξύ δύο κόμβων αγνοώντας την επικοινωνία μεταξύ τους. Για παράδειγμα, ένας ασθενής, ο οποίος είναι χρήστης αντλίας ινσουλίνης. Δεδομένου ότι εντοπίζονται αφύσικες ποσότητες ινσουλίνης στον οργανισμό του, εάν ο χρήστης δεν μπορεί να επικοινωνήσει με το κεντρικό σύστημα εξαιτίας μιας επίθεσης Jamming, τότε αυτό μπορεί να επιφέρει σοβαρές συνέπειες στην υγεία του.

3.1.3.2 Απειλές στο Επίπεδο Δικτύου (Tier-2)

Οι τεχνολογίες επικοινωνίας που χρησιμοποιούνται στα συστήματα IoMT δεν λαμβάνουν υπόψη την ευαισθησία των βιομετρικών δεδομένων. Έτσι, δημιουργούνται κενά εκ του σχεδιασμού ως προς την ιδιωτικότητα και την εμπιστευτικότητα.

Στις τεχνολογίες MQTT, XMPP, CoAP και AMQP προκύπτουν ζητήματα διαλειτουργικότητας και απόδοσης εκθέτοντας τα συστήματα IoMT. Έτσι όπως και στο πρώτο, έτσι και στο δεύτερο επίπεδο επιθέσεις DoS, DDoS, RoS και Brute-force μπορούν να γίνουν με σκοπό την καταστολή της επικοινωνίας των υποδικτύων με το συνολικό δίκτυο και των ιατρικών υπηρεσιών του υπολογιστικού νέφους. Επίσης, η Διαθεσιμότητα στο δεύτερο επίπεδο προσβάλλεται από επιθέσεις Flooding, Jamming και Packet Injection.

3.1.3.3 Απειλές στο Επίπεδο Εφαρμογής (Tier-3)

Οι δικτυακές δομές των συστημάτων IoMT πρέπει να διαφυλάσσονται με ισχυρά μέτρα. Ωστόσο, λόγω της φύσης τους γίνονται στόχοι των επιτιθέμενων, παράγοντας ο οποίος δημιουργεί κενά στην ασφάλεια. Έτσι, πληθώρα επιθέσεων όπως DoS, DDoS, RoS, Brute-force και Buffer Overflow μπορεί να αναστείλουν τη λειτουργία ολόκληρου του συστήματος.

Συνοπτικά, ένας χρήστης που έχει εξουσιοδότηση στις δικτυακές υποδομές του συστήματος μπορεί να κάνει επίθεση Insider manipulation χειραγωγώντας τις λειτουργίες του. Φυσικά, ο αντίκτυπος για τα συστήματα IoMT είναι καταστροφικός, αφού οι επιθυμητές ιατρικές υπηρεσίες δεν θα είναι διαθέσιμες σε όλους τους χρήστες του δικτύου.

3.2 Απειλές Ιδιωτικότητας στα Συστήματα IoMT

Το ζήτημα της ιδιωτικότητας στα συστήματα IoMT ίσως να αποτελεί την πιο απαιτητική πρόκληση. Μεγάλος όγκος ευαίσθητων προσωπικών δεδομένων ανταλλάσσονται στα δίκτυα IoMT. Τα δεδομένα αυτά έχουν ζωτικό χαρακτήρα, αναγνωρίζοντας τον κάθε χρήστη μοναδικά. Από αυτά, μπορεί ένας παραβάτης να διακρίνει τις συνήθειες ενός χρήστη, αλλά και να αναγνωρίσει τα θέματα υγείας που αντιμετωπίζει. Το συγκεκριμένο ζήτημα μπορεί να λάβει μεγάλες διαστάσεις, χάνοντας την αφάνεια των δεδομένων και του ιατρικού απορρήτου, δημιουργώντας κοινωνικά και νομικά ζητήματα. Ακολούθως, όπως και στα κοινά ιατρικά συστήματα, το απόρρητο του ασθενούς του κάθε γιατρού αποτελεί μεγάλη υπόθεση, και δεν πρέπει να χάνεται ο έλεγχος τους το σύστημα.

Τα συστήματα IoMT μπορεί να αντιμετωπίσουν τεχνικές δυσκολίες. Είτε γίνεται λόγος για εμπορικές συσκευές είτε για εξειδικευμένες συσκευές που ανήκουν στη συγκεκριμένη κατηγορία έξυπνων συσκευών, τα ιατρικά δεδομένα που περιέχονται και μοιράζονται πρέπει να παραμείνουν αφανή σε μη εξουσιοδοτημένες οντότητες. Μεγάλη σημασία στην λειτουργία των συστημάτων είναι και η έννοιά της εμπιστοσύνης.

3.2.1 Διαρροή της Ιδιωτικότητας (Privacy Leakage - PL)

Οι Zhang et al., 2015 αναλύουν τη περίπτωση Διαρροής (Privacy Leakage - PL) η οποία αποτελεί σημαντικό πρόβλημα για την ιδιωτικότητα. Τα προσωπικά δεδομένα των χρηστών επεξεργάζονται σε καθημερινή βάση. Κατάλληλα μέτρα ασφαλείας, πρέπει να διασφαλίζουν την ταυτότητα των δεδομένων και τα στοιχεία, που τα χαρακτηρίζουν μοναδικά, όπως επίσης και τις συναλλαγές των δεδομένων αυτών μέσα στο δίκτυο. Σε κάθε άλλη περίπτωση μπορεί να οδηγήσει σε PL. Αυξάνοντας τις απαιτήσεις σε υπολογιστική ισχύ, ισχυροποιούνται οι μέθοδοι διασφάλισης τους και κατ'επέκταση αποφυγής διαρροών. Αυτό, όμως μπορεί να οδηγήσει σε μείωση της απόδοσης των συσκευών. Έτσι, δημιουργείται το ζήτημα των trade-offs, το οποίο αναλύεται στο παρακάτω κεφάλαιο.

Όπως αναφέρθηκε παραπάνω (βλ. 3.1.1), οι έννοιες της Εμπιστευτικότητας και Ιδιωτικότητας έχουν κοινά σημεία. Εφόσον, χαθεί η Εμπιστευτικότητα στο σύστημα, τότε δημιουργούνται απειλές κατά της Ιδιωτικότητας. Επιπλέον, ζητήματα διαρροή της ιδιωτικότητας προκύπτουν και από τις ενέργειες των χρηστών. Η αφέλεια των χρηστών, όπως οι συσκευές που παραμένουν ανιχνεύσιμες ή οι χαμηλής δυναμικότητας κωδικοί ασφαλείας, μπορεί να οδηγήσουν στην παραβίαση του συστήματος, αλλά και στην διαρροή των ευαίσθητων προσωπικών δεδομένων του χρήστη. Βέβαια, η παραβίαση του συστήματος από τη μεριά ενός χρήστη, μπορεί να οδηγήσει στη αλυσιδωτή παραβίαση όλου του συστήματος, με αποτέλεσμα τη διαρροή των προσωπικών δεδομένων μεγάλου αριθμού χρηστών. Χαρακτηριστικές επιθέσεις προς την ιδιωτικότητα είναι οι Eavesdropping και MitM.

Στη περίπτωση των πρώτων ο επιτιθέμενος προσπαθεί ακούγοντας τα κανάλια επικοινωνίας να κερδίσει σε γνώση. Για τη περίπτωση των δεύτερων επιθέσεων, ο χρήστης προσπαθεί να μιμηθεί μια εξουσιοδοτημένη οντότητα του συστήματος με σκοπό να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα. Τέτοιες επιθέσεις είναι οι Spoofing, Counterfeiting, Relay. Έτσι, προκύπτουν ηθελημένες ή ακούσιες απειλές διαρροής εκ των έσω (Insider leak, Inadvertent leak). Αποτέλεσμα αυτού, είναι η παραβίαση του ιατρικού απορρήτου το οποίο επιφέρει νομικά ζητήματα και κοινωνικά προβλήματα στους

χρήστες. Για παράδειγμα, αν γίνει γνωστό για έναν χρήστη ότι πάσχει από το σύνδρομο επίκτητης ανοσολογικής ανεπάρκειας (AIDS), μπορεί να οδηγήσει στην κοινωνική απομόνωση του.

Οι προκλήσεις που υπάρχουν στα συστήματα IoMT, είναι αρκετά κρίσιμες, καθώς γίνεται λόγος για ευαίσθητα δεδομένα, στα οποία καταγράφεται η καθημερινότητα των χρηστών, οι βιομετρικές τους μετρήσεις ή ακόμα μπορεί να εξαρτάται και η ζωή τους από αντίστοιχες συσκευές. Έτσι, δημιουργείται η ανάγκη εφαρμογής ενός συνόλου μέτρων, τα οποία θα αντιμετωπίσουν τα προβλήματα σε επίπεδο ασφάλειας και ιδιωτικότητας, λαμβάνοντας υπόψη την ιδιαιτερότητα των συστημάτων. Σε βιομηχανικό και ερευνητικό επίπεδο έχουν προταθεί λύσεις, κάποιες από τις οποίες εφαρμόζονται και κάποιες βρίσκονται σε πειραματικό επίπεδο. Όπως φαίνεται στον Πίνακα 3.2 και στα τρία επίπεδα η έννοια της Ιδιωτικότητας παραβιάζεται κυρίως από παθητικές επιθέσεις. Οι επιτιθέμενοι προσπαθούν να αποκτήσουν σε γνώση, εξαπατώντας το σύστημα (MitM, Replay) ή απλά ακούγοντας τα κανάλια επικοινωνίας (Eavesdropping).

CIA	Επίπεδο	Απειλές
Ιδιωτικότητα	Επίπεδο 1	Inadvertent Leak, Spoofing, Counterfeiting, Relay
	Επίπεδο 2	Eavesdropping, Buffer overflow
	Επίπεδο 3	Counterfeiting, Spoofing, Replay, MitM, Insider Leak

Πίνακας 3.2: Συνοπτική παράθεση των απειλών στα συστήματα IoMT με βάση την Ιδιωτικότητα

3.2.1.1 Απειλές στο Φυσικό Επίπεδο (Tier-1)

Στο πρώτο επίπεδο η Διαρροή στην Ιδιωτικότητα προκύπτει κυρίως από λάθη των χρηστών. Αφήνοντας συσκευές ανιχνεύσιμες ή χρησιμοποιώντας χαμηλά μέτρα ασφάλειας (λ.χ αδύναμους κωδικούς) επιτρέπουν τους επιτιθέμενους να παραβιάσουν το τοπικό τους δίκτυο δημιουργώντας ακούσια διαρροή(Inadvertent leak). Επιπλέον, το δίκτυο WBAN ενός χρήστη μπορεί να αποτελέσει το κενό στο σύστημα. Πραγματοποιώντας επιθέσεις Spoofing, Counterfeiting, Relay μπορεί ο επιτιθέμενος να προσποιηθεί έναν έμπιστο κόμβο και να ανακτήσει τα δεδομένα που αφορούν τον χρήστη.

3.2.1.2 Απειλές στο Επίπεδο Δικτύου (Tier-2)

Στο δεύτερο επίπεδο πιθανές είναι οι επιθέσεις Eavesdropping όπου ο επιτιθέμενος προσπαθεί να κερδίσει όσο το δυνατόν περισσότερη γνώση γίνεται, καθώς από τις συσκευές του δεύτερου επιπέδου περνάνε βιομετρικά δεδομένα πολλαπλών χρηστών. Επιπλέον, με την επίθεση Buffer overflow ο επιτιθέμενος επιχειρεί να καταστείλει τη λειτουργία των κόμβων του δικτύου και ταυτόχρονα να προκαλέσει διαρροή των δεδομένων που είχαν φτάσει σε αυτόν για να προωθηθούν στο υπόλοιπο δίκτυο.

3.2.1.3 Απειλές στο Επίπεδο Εφαρμογής (Tier-3)

Στο τρίτο επίπεδο είναι πιθανές οι απειλές εκ των έσω που προκαλούν διαρροή ή των ευαίσθητων δεδομένων. Επιθέσεις Spoofing, Counterfeiting, Replay και MitM

αποσκοπούν στην ανάκτηση μεγάλων ποσοτήτων ευαίσθητων δεδομένων που αφορούν πολλούς χρήστες. Με τις παραπάνω επιθέσεις ο επιτιθέμενος μιμείται μια εξουσιοδοτημένη οντότητα που έχει δικαιοδοσία σε έναν μεγάλο αριθμό δεδομένων (πχ. ένας γιατρός, ο διαχειριστής του συστήματος) και επιχειρεί να αποκτήσει πρόσβαση στα δεδομένα του. Φυσικά, η περίπτωση της διαρροής εκ των έσω (Insider Leak) ισχύει και εδώ, εφόσον οι χρήστες δεν διαχειρίζονται με ασφάλεια το σύστημα, αφήνοντας εκτεθειμένα δεδομένα, με τα οποία ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση, όπως κλειδιά συνόδου.

Τέλος, μια ακόμα πρόκληση αποτελούν οι εμπορικές συσκευές που δεν προορίζονται για εξειδικευμένη χρήση. Πιο συγκεκριμένα, χρησιμοποιώντας αισθητήρες και συσκευές του εμπορίου, που δεν προορίζονται αποκλειστικά για ιατρικές εφαρμογές, μπορεί να μη διαθέτουν κατάλληλους μηχανισμούς για τη προστασία τους και έτσι να οδηγήσουν στην διαρροή των ευαίσθητων ιατρικών δεδομένων του χρήστη ή ακόμα και την είσοδο του επιτιθέμενου στο σύστημα συνολικά, όπου μπορεί να προκαλέσει μεγαλύτερη ζημιά στο σύνολο του.

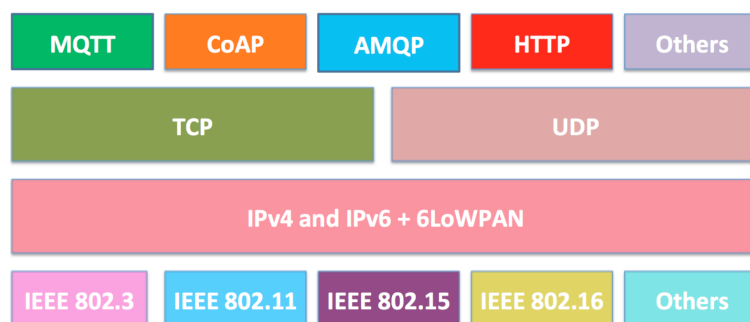
Κεφάλαιο 4

Απαιτήσεις Ασφάλειας και Ιδιωτικότητας στα Συστήματα IoMT

Φτάνοντας στο τέταρτο κεφάλαιο, και έχοντας αναλύσει τις προκλήσεις που προκύπτουν στα συστήματα IoMT, είναι αναγκαία η καταγραφή των απαιτήσεων ασφάλειας που γεννιούνται. Οι απαιτήσεις αφορούν γενικά το σύστημα, δηλαδή τον τρόπο με τον οποίο θωρακίζεται το δίκτυο, η επικοινωνία των κόμβων, οι χρήστες και τα δεδομένα που διαμοιράζονται στο δίκτυο. Επιπλέον, η διατήρηση και διασφάλιση της Ιδιωτικότητας των χρηστών στα συστήματα IoMT εγείρει απαιτήσεις, καθώς αποτελεί κρίσιμο παράγοντα για την ομαλή λειτουργία του. Μεγάλη έμφαση δίνεται στο κομμάτι της ιδιωτικότητας, αποτελώντας μια από τις σημαντικότερες ιδιότητες των IoMT, καθώς έτσι διατηρείται η ακεραιότητα του ιατρικού απορρήτου.

Η εφαρμογή του νέου Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ), εγείρει νέες απαιτήσεις με σκοπό τη προστασία του χρήστη και των προσωπικών δεδομένων του. Επεκτείνοντας το ζήτημα των απαιτήσεων, η ικανοποίησή τους έρχεται σε σύγκρουση με τις επιδόσεις των συστημάτων. Σε περιπτώσεις όπου οι μηχανισμοί κρυπτογράφησης χρειάζονται μεγάλα αποθέματα πόρων για τον υπολογισμό και την εκτέλεση του αλγορίθμου. Παράλληλα όμως, η υπολογιστική δύναμη που χρησιμοποιείται από τους μηχανισμούς κρυπτογράφησης μπορεί να είναι απαραίτητη για την εκτέλεση κάποιας λειτουργίας του συστήματος. Έτσι, γεννάται το ζήτημα των συμβιβασμών (*trade-offs*), που αναλύεται παρακάτω. Σε σχέση με τις προκλήσεις των συστημάτων, προτιμήθηκε η ανάλυση των απαιτήσεων στα συστήματα IoMT με βάση τα στρώματα επικοινωνίας (βλ. Σχ. 2.6).

Οι μελέτες της βιβλιογραφίας χρησιμοποιούν την ίδια προσέγγιση, καθώς οι απαιτήσεις κάθε στρώματος επικοινωνίας αφορούν ομάδες τεχνολογιών. Στο Σχ. 4.1 παρουσιάζονται τα πρωτόκολλα επικοινωνίας των συστημάτων IoT. Ενδεικτικά, γίνεται αντιστοίχιση της κατανομής των στρωμάτων με αυτή του Σχ. 2.6.



Σχήμα 4.1: Πρωτόκολλα επικοινωνίας των IoT. Adapted from ‘Choice of Effective Messaging Protocols - for IoT Systems MQTT, CoAP, AMQP and HTTP’, (by Nitin Naik, 2017.)

Στον Πίνακα 4.1 διακρίνεται η σχέση των στρωμάτων επικοινωνίας με τα επίπεδα της αρχιτεκτονικής στο Σχ. 2.9 και με τις τεχνολογίες επικοινωνίας. Αυτές φυσικά είναι ενδεικτικές, καθώς υπάρχει πληθώρα τεχνολογιών που χρησιμοποιούνται στα συστήματά IoT (Krisnha et al., 2018).

Στρώμα	Επίπεδο	Πρωτόκολλα Επικοινωνίας
Interface	Tier-1 Tier-3	MQTT CoAP AMQP HTTP XMPP
Service	Tier-2	TCP UDP RPL
Network	Tier-3	6LoWPAN IPv4 IPv6
Sensing	Tier-1	IEEE 802.3 IEEE 802.11 IEEE 802.15 IEEE 802.16

Πίνακας 4.1: Αντιστοίχιση πρωτοκόλλων επικοινωνίας με το επίπεδο και στρώμα εφαρμογής τους σύμφωνα με την αρχιτεκτονική του Σχ 2.9

Τα τελευταία χρόνια, διάφορες χώρες ξεκίνησαν εκστρατείες με τις οποίες προσπαθούν να εντάξουν την έννοια της ηλεκτρονικής υγείας στα πλαίσια του συστήματος υγείας τους. Κάθε χώρα, ανάλογα με τη περιοχή στην οποία υπάγεται, πρέπει να συμμορφωθεί σε ορισμένους κανόνες. Εντός της Ευρωπαϊκής Ένωσης, πλέον βρίσκει εφαρμογή ο νέος Γενικός Κανονισμός Προστασίας των Δεδομένων (ΓΚΠΔ), ο οποίος οριοθετεί τον τρόπο με τον οποίο γίνεται η αποθήκευση και επεξεργασία των δεδομένων στα συστήματα, ενώ υπάρχουν κανόνες συγκεκριμένα για τη κατηγορία των ευαίσθητων προσωπικών δεδομένων. Οι απαιτήσεις στα συστήματα IoMT προβλέπουν την ικανοποίηση των κανόνων του ΓΚΠΔ, καθώς η μη ικανοποίηση τους μπορεί να οδηγήσει σε νομικές επιπτώσεις. Στο κεφάλαιο παρακάτω, γίνεται η ανάλυση των στρωμάτων επικοινωνίας στα συστήματα IoMT με βάση τις απαιτήσεις που έχουν σε επίπεδο Ασφάλειας (Security) και Ιδιωτικότητας (Privacy).

4.1 Απαιτήσεις Ασφάλειας στα Συστήματα IoMT

Τα μετρά ασφαλείας πρέπει να στοχεύουν στην θωράκιση των πληροφοριών του ασθενούς, στην διατήρηση και την ορθή κατανομή των πόρων του συστήματος και στην ασφάλεια του δικτύου στο σύνολο του. Για αρχή, ως καλή πρακτική θεωρείται η μοντελοποίηση των απειλών, από τις οποίες ένα σύστημα IoMT κινδυνεύει να παραβιαστεί

(Zheng et al., 2017; Kocabas et al., 2016). Η συγκεκριμένη διαδικασία αποτελεί τη τυπική ανάλυση κινδύνου. Η μοντελοποίηση των απειλών, ουσιαστικά είναι η καταγραφή των επικείμενων επιθέσεων σε ένα σύστημα, δηλαδή η διαδικασία που ακολουθήθηκε στο τρίτο κεφάλαιο για την αναγνώριση των προκλήσεων στα συστήματα IoMT. Έτσι, οι απαιτήσεις των IoMT απορρέουν από τις απειλές των προκλήσεων. Στην ουσία, οι απαιτήσεις θέτουν τις βάσεις προδιαγραφής των μέτρων ασφάλειας σε ένα σύστημα, για να αντιμετωπιστούν με επιτυχία οι πιθανές προκλήσεις.

Ξεκινώντας, υπάρχουν απαραίτητες έννοιες για το σύνολο των συστημάτων IoMT. Κάτω από τον όρο της **Ασφαλούς Πληροφορίας** (Information Security) συγκαταλέγονται όλες οι παρακάτω απαιτήσεις. Είναι θεμιτή η διασφάλιση της τριάδας CIA για τις πληροφορίες που διαμοιράζονται στο σύστημα IoMT. Η έννοια της **Επείγουσας Αυθεντικοποίησης** (Emerging Authentication) αναφέρεται στην ιδιότητα του συστήματος σε περίπτωση επείγοντος περιστατικού να επιτρέπει σε οντότητες όπως ο επείγον γιατρός να έχουν πρόσβαση στα βιομετρικά δεδομένα των ασθενών και στους αισθητήρες (Φορητοί και Εμφυτευμένοι), για τους οποίους μπορεί να μην είναι εξουσιοδοτημένοι (Challa et al., 2018). Αυτό όπως φαίνεται παρακάτω αντιβαίνει ιδιότητες απαραίτητες για την διασφάλιση της τριάδας CIA.

Η έννοια της **Επεκτασιμότητας** (Scalability) είναι ιδιαίτερα σημαντική. Με τη προσθήκη αισθητήρων στους χρήστες ή νέων χρηστών στο σύστημα και των αισθητήρων που τους αντιστοιχούν αυξάνεται η χρήση των υπολογιστικών και αποθηκευτικών πόρων. Τα συστήματα IoMT πρέπει να προσαρμόζονται στις αλλαγές, αφού σε αντίθετη περίπτωση μπορεί να προσβληθεί η Διαθεσιμότητα του συστήματος.

Στις παρακάτω ενότητες πραγματοποιείται η ανάλυση των επιπέδων και έχει ως σκοπό την ανάδειξη των απαιτήσεων στα συστήματα IoMT, οι οποίες αποσκοπούν στην ικανοποίηση και ενίσχυση της τριάδας CIA. Επιπρόσθετα, σε συστήματα που διαχειρίζονται ιατρικά δεδομένα και διαπραγματεύονται λειτουργίες που σχετίζονται με την ακεραιότητα των χρηστών, είναι απαραίτητη η Αυθεντικοποίηση των χρηστών, δηλαδή κάθε χρήστης να έχει δικαιώματα επεξεργασίας μόνο στα δεδομένα που τον αφορούν.

4.1.1 Απαιτήσεις στο Φυσικό Στρώμα (Sensing Layer)

Το κατώτερο στρώμα αποτελεί το σημείο περισυλλογής βιομετρικών δεδομένων από τους ασθενείς του δικτύου. Είναι το σημείο άμεσης επαφής των συστημάτων IoMT με τους χρήστες, γεγονός που το καθιστά το πιο απαιτητικό στρώμα. Έτσι, η φύση των συσκευών IoMT σε συνδυασμό με τα ακατέργαστα βιομετρικά δεδομένα, εγείρουν ένα σύνολο απαιτήσεων για τη προστασία της τριάδας CIA. Επιπλέον, είναι αναγκαία η διασφάλιση των διαύλων επικοινωνίας μεταξύ των αισθητήρων (Point-to-Point, Multipoint-to-Point, Multipoint-to-Multipoint), λειτουργία η οποία συντελείται στο κατώτερο επίπεδο, με τις τεχνολογίες που αναγράφονται στο Σχ.(4.1).

Με την έννοια της **Εξουσιοδότησης** (Authorization) δικαίωμα στην επεξεργασία και την πρόσβαση στα βιομετρικά δεδομένα του χρήστη μπορεί να έχουν μόνο χρήστες με τα απαιτούμενα δικαιώματα (π.χ ο ασθενής ή ο θεράπων γιατρός). Συμπληρώνοντας την έννοια της Εξουσιοδότησης, μόνο οι **Αυθεντικοποιημένες** (Authentication) οντότητες, δηλαδή χρήστες του δικτύου μπορούν να έχουν πρόσβαση στο σύστημα. Με τη χρήση τεχνικών **Ελέγχου Πρόσβασης** (Access Control), οι αυθεντικοποιημένες οντότητες επιτελούν μόνο τις λειτουργίες για τις οποίες είναι εξουσιοδοτημένες (Rathore

et al., 2017). Έτσι, αντιμετωπίζονται απειλές κατά της Εμπιστευτικότητας (βλ.3.1.1.1) που προκύπτουν από την αφέλεια των χρηστών, της Ακεραιότητας και Διαθεσιμότητας που προκύπτουν από την έλλειψη ελέγχου (βλ. 3.1.2.1, 3.1.3.1).

Ο έλεγχος πρόσβασης χρησιμοποιείται και στην αλληλεπίδραση μεταξύ συσκευών, όπου μόνο μεταξύ αυθεντικοποιημένων συσκευών ανταλλάσσονται βιομετρικά δεδομένα (π.χ μεταξύ του προσωπικού διακομιστή του χρήστη και των αισθητήρων του). Εδώ, εφαρμόζει η έννοια της **Εμπιστοσύνης** (Trust) μεταξύ των συσκευών, όπου μπορεί να μην υφίσταται σαν έννοια, ωστόσο είναι απαραίτητη σαν ιδιότητα για την άρτια λειτουργία των συστημάτων IoMT, αφού εξαρτάται η ομαλή επικοινωνία των συσκευών (Sicari et al., 2015). Φυσικά, όπως αναφέρθηκε παραπάνω σημαντική είναι και η έννοια της **Επείγουσας Αυθεντικοποίησης**, επιτρέποντας τη πρόσβαση στις επείγουσες οντότητες στους αισθητήρες των χρηστών. Η **Επεκτασιμότητα** είναι αναγκαία, καθώς είναι πιθανή η προσθήκη νέων αισθητήρων στα προσωπικά δίκτυα των χρηστών (WBAN).

4.1.2 Απαιτήσεις στο Στρώμα Δικτύου (Network Layer)

Το στρώμα δικτύου αφορά τις δικτυακές τεχνολογίες που χρησιμοποιούνται στα συστήματα, δηλαδή στον τρόπο και τα μέσα με τα οποία ταξιδεύει η πληροφορία μεταξύ των υποδικτύων και του συνολικού δικτύου. Η διασφάλιση των διόδων επικοινωνίας εγγυάται την ομαλή λειτουργικότητα του συστήματος, αυξάνοντας την εμπιστευτικότητα και ισχυροποιώντας την ακεραιότητα των δεδομένων. Ωστόσο, επειδή οι δικτυακές δομές του συστήματος (διακομιστές, Router, Gateways, Access Points) είναι εκτεθειμένες, προτιμάται η διασφάλιση της διαμοιραζόμενης πληροφορίας σε συνδυασμό με μηχανισμούς ανίχνευσης (που αναλύονται στο παρακάτω κεφάλαιο).

Με τη χρήση τεχνικών **Αυθεντικοποίησης**, θωρακίζεται η διαμοιραζόμενη πληροφορία, επιτρέποντας μόνο στον εξουσιοδοτημένο κόμβο παραλήπτη να έχει πρόσβαση, αποτρέποντας επιθέσεις Eavesdropping και ενισχύονται οι έννοιες της Ακεραιότητας και Εμπιστευτικότητας. Επιπρόσθετα με τις παραπάνω έννοιες, για την εξασφάλιση της Διαθεσιμότητας μεταξύ των κόμβων του συστήματος, η έννοια της **Εμπιστοσύνης** είναι απαραίτητη στις δικτυακές υποδομές των συστημάτων IoMT, αφού η επικοινωνία έμπιστων κόμβων συντελεί στην ομαλή και ασφαλή επικοινωνία του συστήματος. Επιπλέον σημαντικό χαρακτηριστικό, είναι η **Ευρωστία** (Robustness), δηλαδή η ιδιότητα του συστήματος να παραμένει δυνατό και υγιές (Rathore et al., 2017).

Με την Ευρωστία, το σύστημα είναι ικανό να ανέχεται διαταραχές, χωρίς να επηρεαστεί το λειτουργικό σώμα του. Έτσι, με τεχνικές που αφομοιώνουν την εν λόγω ιδιότητα εξασφαλίζεται η συνεχής λειτουργία του συστήματος. Ταυτόχρονα, όμως, πρέπει να είναι προσιτή η **Επεκτασιμότητα** του συστήματος. Η Επεκτασιμότητα μπορεί να ενισχυθεί με τη χρήση τεχνικών **Εξουσιοδότησης**, επιτρέποντας μόνο σε αναγνωρίσιμες συσκευές να επικοινωνούν στο σύστημα IoMT. Όπως και στο επόμενο στρώμα επικοινωνίας, έτσι και στο στρώμα δικτύου με τις παραπάνω ιδιότητες καθίσταται δυνατή η αντιμετώπιση απειλών κατά της Διαθεσιμότητας του δικτύου όπως επιθέσεις RoS, DDoS και Brute-force (βλ. Κεφάλαιο 3.1.3.2).

4.1.3 Απαιτήσεις στο Στρώμα Υπηρεσιών (Service Layer)

Στο στρώμα υπηρεσιών ανήκουν οι αποθηκευτικοί και επεξεργαστικοί πόροι (βάσεις δεδομένων, υπολογιστικά νέφοι). Συλλέγονται, αποθηκεύονται και επεξεργάζονται τεράστιοι όγκοι ευαίσθητων προσωπικών δεδομένων. Η διασφάλιση της τριάδας CIA είναι απαραίτητη, καθώς είναι κρίσιμη η ακρίβεια, εγκυρότητα και αξιοπιστία των δεδομένων για την επιτέλεση των ιατρικών δεδομένων, όπως επίσης και η διατήρηση της λειτουργικότητας του συστήματος. Αρχικά, το σύστημα πρέπει να είναι **Ασφαλές εκ του Σχεδιασμού** (Safe by Design), μια ιδιότητα που διασφαλίζει την ομοιογένεια του. Πρέπει να διασφαλίζονται οι υποδομές στις οποίες φιλοξενούνται οι πόροι, τόσο για εξωτερικούς όσο και για εσωτερικούς παράγοντες (βλ. Κεφάλαιο 3.1.1.3, 3.1.2.3, 3.1.3.3).

Αφού γίνεται λόγος για μεγάλες ποσότητες βιομετρικών δεδομένων, είναι απαραίτητη η ύπαρξη μηχανισμών, που θα επιτρέπουν μόνο σε **Εξουσιοδοτημένες** οντότητες να έχουν πρόσβαση στους πόρους. Επιπλέον, για τον έλεγχο των δεδομένων, είναι θεμιτό μόνον **Αυθεντικοποιημένα** δεδομένα θα γίνονται αποδεκτά από το σύστημα, αντιμετωπίζοντας έτσι επιθέσεις χειραγώγησης, όπως οι Relay και Spoofing, προστατεύοντας τις έννοιες της Εμπιστευτικότητας και Ακεραιότητας. Στο στρώμα διεργασιών με την έννοια της **Ευρωστίας** γίνεται λόγος στην ικανότητα του συστήματος όποτε είναι απαραίτητο να προσαρμόζει τους υπολογιστικούς πόρους ενισχύοντας τις ιατρικές υπηρεσίες που το χρειάζονται (π.χ κατά την εκτέλεση χειρουργικής επέμβασης μέσω τηλεϊατρικής), διατηρώντας τη λειτουργικότητα του υπόλοιπου συστήματος ως έχει και αντιμετωπίζοντας επικείμενες απειλές στο σύστημα.

Ταυτόχρονα, κυρίως για τους αποθηκευτικούς πόρους του συστήματος, η **Επεκτασιμότητα** είναι απαραίτητη για τη Διαθεσιμότητα του συστήματος, καθώς η προσθήκη καινούργιων αυθεντικοποιημένων οντοτήτων στο σύστημα σημαίνει μεγαλύτερα μεγέθη δεδομένων ως προς επεξεργασία. Εδώ, σημαντικό ρόλο για τα συστήματα IoMT καταλαμβάνει η ιδιότητα της **Ελαχιστοποίησης Δεδομένων**. Εφόσον, στα συστήματα IoMT είναι μεγάλος ο αριθμός των βιομετρικών δεδομένων, είναι θεμιτοί οι μηχανισμοί ελαχιστοποίησης του μεγέθους, καθώς ενισχύεται η ακρίβεια των δεδομένων και κατ'επέκταση η Ακεραιότητά τους, ενώ απελευθερώνεται οι πόροι του συστήματος (Roman et al., 2013). Οι παραπάνω ιδιότητες συμβάλλουν στην αντιμετώπιση απειλών όπως Buffer overflow και DDoS (βλ. Κεφάλαιο 3.1.1.2, 3.1.2.2, 3.1.3.2) προστατεύοντας την έννοια της Διαθεσιμότητας.

4.1.4 Απαιτήσεις στο Στρώμα Διεπαφής (Interface Layer)

Το τελευταίο στρώμα επικοινωνίας αποτελεί το σημείο αλληλεπίδρασης των χρηστών με το σύστημα. Οι εφαρμογές διεπαφής δίνουν τη δυνατότητα στους χρήστες να επικοινωνήσουν με τους πόρους του συστήματος και με τις συσκευές-αισθητήρες που τους αντιστοιχούν (π.χ ασθενείς) ή που έχουν πρόσβαση ως εξουσιοδοτημένες οντότητες (π.χ επαγγελματίες υγείας). Από εδώ, είναι θεμιτό οι πληροφορίες και υπηρεσίες που εκτελούνται να είναι φρέσκα, ακριβείς και μη-περιττά (Pirbhulal et al., 2019).

Η εξασφάλιση της τριάδας CIA στα συστήματα IoMT αποτελεί μεγάλη πρόκληση, καθώς ο αριθμός των ευαίσθητων δεδομένων που διακινούνται σε αυτά είναι μεγάλος και αποτελούν θελκτικό αντικείμενο των παραβατών. Λαμβάνοντας υπόψη το μεγάλο πλήθος απαιτήσεων που πρέπει να ικανοποιηθούν, είναι αναγκαία η εγκαθίδρυση ισχυ-

ρών μέτρων ασφάλειας. Στον Πίνακα 4.2 συνοψίζονται οι απαιτήσεις που είναι θεμιτό να ικανοποιούνται στην Ασφάλεια, για κάθε στρώμα επικοινωνίας ξεχωριστά.

	Sensing	Network	Service	Interface
CIA	✓	✓	✓	✓
Επείγουσα Αυθεντικοποίηση	✓	✓	—	✓
Επεκτασιμότητα	✓	✓	✓	✓
Εξουσιοδότηση	✓	—	✓	✓
Αυθεντικοποίηση	✓	✓	✓	✓
Έλεγχος Πρόσβασης	✓	—	—	✓
Εμπιστοσύνη	✓	✓	—	✓
Ευρωστία	—	✓	✓	—
Ελαχιστοποίηση Δεδομένων	—	—	✓	—
Μη-άρνηση	—	—	—	✓

Πίνακας 4.2: Σύνοψη των απαιτήσεων ασφάλειας στα τέσσερα στρώματα επικοινωνίας

Το στρώμα διεπαφής έχει ανάλογες απαιτήσεις με το φυσικό στρώμα. Αυτό συμβαίνει καθώς και τα δύο στρώματα επικοινωνίας είναι σημεία άμεσης επαφής των χρηστών με το σύστημα IoMT. Έτσι, μόνο **Αυθεντικοποιημένες** οντότητες θα έχουν πρόσβασης τις λειτουργίες του συστήματος, ενώ σύμφωνα με το επίπεδο **Εξουσιοδότησης**, έχουν ανάλογα δικαιώματα για την επεξεργασία δεδομένων και την εκτέλεση εντολών για τις ιατρικές υπηρεσίες. Οι δύο έννοιες χρησιμοποιούνται από τους μηχανισμούς **Ελέγχου Πρόσβασης** (Suo et al., 2012). Τοιουτοτρόπως, επιθέσεις χειραγώγησης όπως επιθέσεις MitM, Replay, Relay μπορούν και αντιμετωπίζονται. Επιπλέον, η έννοια της **Επείγουσας Αυθεντικοποίησης** κατέχει και στο στρώμα διεπαφής κρίσιμο ρόλο, αφού μέσω αυτού γίνεται η επικοινωνία των χρηστών με το σύστημα. Έτσι, σε περίπτωση επείγοντος περιστατικού οι χρήστες να μπορούν να επικοινωνήσουν χωρίς εμπόδια με το σύστημα. Βέβαια, για την ορθή εκτέλεση των μηχανισμών Επείγουσας Αυθεντικοποίησης είναι απαραίτητη να αναγνωρίζεται ποιο σήμα είναι κακόβουλο.

Συνεχίζοντας, για την ασφάλεια του συστήματος IoMT είναι απαραίτητες οι έννοιες της **Ευθύνης** και **Μη-άρνησης**. Όπως περιγράφηκε στο τρίτο κεφάλαιο (βλ. Κεφάλαιο 3.1.1.3, 3.1.2.3, 3.1.3.3) πιθανή είναι η παραβατική συμπεριφορά στο σύστημα IoMT από τους χρήστες του. Σκοπός των εννοιών είναι ο καταλογισμός ευθυνών στις αυθεντικοποιημένες οντότητες, από τις οποίες παρατηρήθηκε παραβατική συμπεριφορά. Συμπληρωματικά, με την έννοια της **Εμπιστοσύνης** μεταξύ του συστήματος και των χρηστών και διατηρώντας αρχεία με τις κινήσεις των χρηστών και τις λειτουργίες των συσκευών (backlogs), το σύστημα εκπαιδεύεται και βαθμολογεί τους χρήστες. Έτσι, δημιουργείται ένα σύστημα εμπιστοσύνης, το οποίο ενισχύει την τριάδα CIA.

4.2 Απαιτήσεις Ιδιωτικότητας στα συστήματα IoMT

Η διατήρηση της Ιδιωτικότητας στα συστήματα IoMT έχει ως στόχο την απόκρυψη της ταυτότητας των χρηστών, των δεδομένων που διαμοιράζονται, των συσκευών και

πόρων που χρησιμοποιούνται, όπως επίσης και την αντιστοίχιση των συσκευών IoMT με τους χρήστες. Σε περίπτωση παραβίασης του συστήματος, προσβάλλεται το ιατρικό απόρρητο των ασθενών, και σε κάθε περίπτωση, μπορεί να δημιουργήσει ανεπανόρθωτες βλάβες τόσο στο σύστημα όσο και στους χρήστες. Ο ΓΚΠΔ θέτει τα όρια επεξεργασίας των δεδομένων, έχοντας ξεχωριστούς κανόνες για τη κατηγορία των ευαίσθητων προσωπικών δεδομένων, όπως αυτά στα συστήματα IoMT. Έτσι, γίνεται ανάλυση των κανόνων του ΓΚΠΔ με σκοπό την αντιστοίχιση τους στις προβλεπόμενες απαιτήσεις της Ιδιωτικότητας.

Ως αποτέλεσμα, κατά το σχεδιασμό των συστημάτων IoMT οι τεχνικές διατήρησης της Ιδιωτικότητας παίρνουν μεγάλες διαστάσεις. Επόμενα, σε αντίθεση με τις απαιτήσεις της ασφάλειας, εδώ γίνεται πρώτα περιγραφή των απαιτήσεων της ιδιωτικότητας και μετά η αντιστοίχιση στα στρώματα επικοινωνίας, καθώς είναι θεμιτό να εκπληρώνονται όλες σε καθένα από αυτά.

Η έννοια της Ιδιωτικότητας επιπρόσθετα αντιμετωπίζει παρόμοια προβλήματα με αυτά της Εμπιστευτικότητας. Έτσι, παθητικές επιθέσεις, που αποσκοπούν στην ανάκτηση γνώσης από τα συστήματα (Eavesdropping, MitM, Masquerade) ή επιθέσεις από τις οποίες τα προσωπικά δεδομένα των ασθενών μπορεί να διαρρεύσουν (Buffer overflow) είναι θεμιτό να αντιμετωπιστούν. Επιπλέον, μεγάλη πρόκληση για την Ιδιωτικότητα στα συστήματα IoMT είναι η αντιμετώπιση εσωτερικών απειλών (βλ. Κεφάλαιο 3.2.1).

Αρχικά, σημαντική έννοια για την Ιδιωτικότητα είναι η **Ανωνυμία** (Anonymity) των χρηστών, δηλαδή η ιδιότητα μιας οντότητας να παραμένει κρυφή ως προς έναν επιτιθέμενο. Οι χρήστες του δικτύου πρέπει να παραμένουν στην αφάνεια, χωρίς να γνωστοποιείται η ταυτότητα τους όταν δραστηριοποιούνται στο σύστημα IoMT. Σε συνέχεια της Ανωνυμίας, πρέπει να μην διακρίνονται οι συσκευές που αντιστοιχούν σε κάθε χρήστη. Για παράδειγμα, ένας hacker κάνει επίθεση Eavesdropping σε ένα κανάλι επικοινωνίας ενός ασθενούς με τη φορητή συσκευή Wristband, η οποία μετράει την αρτηριακή πίεση του. Με τη **Μη-συνδεσιμότητα** (Unlinkability) ο επιτιθέμενος δεν μπορεί να αντιστοιχίσει τον χρήστη με την συσκευή. Σε περίπτωση παραβίασης της συσκευής, ο επιτιθέμενος δεν θα μπορεί να αντιστοιχίσει τα βιομετρικά δεδομένα στον χρήστη της συσκευής. Έπειτα, σε ένα σύστημα IoMT είναι θεμιτή η αφάνεια των υπηρεσιών που χρησιμοποιούν οι χρήστες. Η έννοια της **Μη-παρατηρησιμότητας** (Unobservability), δίνει την ιδιότητα στο σύστημά να αποκρύπτει τις υπηρεσίες ή τους πόρους του συστήματος, που χρησιμοποιούνται από έναν χρήστη.

Με την έννοια της **Μη-ανιχνευσιμότητας** (Undetectability) ο επιτιθέμενος δεν μπορεί να διακρίνει την ύπαρξη μιας οντότητας (Kokoliou et al., 2017). Συμπληρώνοντας την παραπάνω έννοια, η **Μυστικότητα** (Forward/Backward Secrecy) αναφέρεται στην ιδιότητα των συστημάτων να κρύβουν τα δεδομένα επικοινωνίας μίας συνεδρίας. Αν, για παράδειγμα εκτελεστεί μια απειλή κατά της Εμπιστευτικότητας ή Ιδιωτικότητας (βλ. Κεφάλαιο 3.1.1, 3.2.1) στο σύστημα IoMT όπως μια επίθεση MitM στο κανάλι επικοινωνίας ενός χρήστη με τον βηματοδότη του, ο επιτιθέμενος ενώ βλέπει το κανάλι επικοινωνίας δεν μπορεί να ξέρει την ύπαρξη των δύο οντοτήτων, ούτε τη πληροφορία που διαμοιράζονται. Τέλος, κάθε χρήστης πρέπει να επεξεργάζεται αυστηρά, μόνο τα δεδομένα που του αντιστοιχούν. Για παράδειγμα, ένας ασθενής πρέπει να έχει πρόσβαση μόνο στα δικά του δεδομένα, ενώ ο θεράπων γιατρός στα προσωπικά δεδομένα των χρηστών του. Ωστόσο, ο γιατρός πρέπει να έχει περιορισμένα δικαιώματα επεξεργασίας των δεδομένων. Το ζήτημα αυτό αντιμετωπίζεται με τις έννοιες της **Αυθεντικοποίησης**

(Authentication) και **Εξουσιοδότησης** (Authorization).

4.2.1 Απαιτήσεις στο Φυσικό Στρώμα (Sensing Layer)

Στο κατώτερο στρώμα επικοινωνίας, βρίσκεται το προσωπικό δίκτυο του χρήστη. Είναι θεμιτή η αφάνεια των συσκευών που χρησιμοποιούνται από τον χρήστη (Μη-συνδεσιμότητα, Μη-ανιχνευσιμότητα) και της ταυτότητάς του (Ανωνυμία). Επίσης, δεν πρέπει να φαίνεται ποιος πόρος του συστήματος IoMT χρησιμοποιεί ο χρήστης (Μη-παρατηρησιμότητα). Με τον τρόπο αυτό διασφαλίζεται η ταυτότητα και τα δεδομένα του χρήστη, αποτρέποντας των επιτιθέμενο να δημιουργήσει προβλήματα. Επιπλέον, επιτρέποντας τη πρόσβαση σε Εξουσιοδοτημένες οντότητες του συστήματος, αντιμετωπίζονται οι εσωτερικές επιθέσεις (βλ. Κεφάλαιο 3.1.1.1, 3.2.1.1). Λαμβάνοντας υπόψη το χειρότερο σενάριο, εάν το προσωπικό δίκτυο ενός χρήστη παραβιαστεί, τότε λαμβάνοντας υπόψη τις παραπάνω απαιτήσεις ο επιτιθέμενος δεν θα γνωρίζει σε ποιον ανήκει το υποδίκτυο, την ύπαρξη και λειτουργία των συσκευών μέσα σε αυτό, ούτε τους πόρους του συστήματος που χρησιμοποιεί.

4.2.2 Απαιτήσεις στο Στρώμα Δικτύου (Network Layer)

Οι δικτυακές δομές των συστημάτων IoMT, απαιτούν την κάλυψη της ταυτότητας των χρηστών, του περιεχομένου της διαμοιραζόμενης πληροφορίας και τη κάλυψη των διαύλων επικοινωνίας. Για την αντιμετώπιση των επικείμενων παραβιάσεων (βλ. Κεφάλαιο 3.1.1.2, 3.2.1.2), με την έννοια της Μη-συνδεσιμότητας ο επιτιθέμενος δε μπορεί να γνωρίζει σε ποιον ανήκει η πληροφορία που έχει στα χέρια του. Ακόμα και αν παραβιαστεί επιτυχημένα το σύστημα, ο επιτιθέμενος δεν μπορεί να αναγνώρισή τον κόμβο-προέλευση των δεδομένων. ενώ με τη Μυστικότητα, προστατεύονται τα στοιχεία της συνόδου επικοινωνίας. Για παράδειγμα, ο θεράπων γιατρός επιθυμεί εξ αποστάσεως να ρυθμίσει την αντλία ινσουλίνης του ασθενή που είναι χρήστης του συστήματος. Εάν υπάρχει μια παραβατική οντότητα στο δίκτυο που πράττει επίθεση Eavesdropping με τεχνικές Μυστικότητας, τα στοιχεία συνόδου παραμένουν στην αφάνεια. Επιπλέον, χρησιμοποιώντας την έννοια της Μη-ανιχνευσιμότητας, οι επιτιθέμενοι δεν μπορούν να γνωρίζουν τους πόρους του συστήματος που χρησιμοποιούνται εκείνη τη στιγμή.

4.2.3 Απαιτήσεις στο Στρώμα Διεργασιών (Service Layer)

Οι αποθηκευτικοί και επεξεργαστικοί πόροι στα συστήματα IoMT χρησιμοποιούνται διαρκώς για την επιτέλεση των ιατρικών υπηρεσιών. Ο επιτιθέμενος δεν πρέπει να γνωρίζει πώς γίνεται η εκμετάλλευση των πόρων του συστήματος (Μη-παρατηρησιμότητα). Ταυτόχρονα, δεν πρέπει να γνωρίζει ούτε την ταυτότητα των χρηστών (Μη-συνδεσιμότητα) που εκμεταλλεύονται τις ιατρικές υπηρεσίες του συστήματος. Αποτελεί κομβικό σημείο για τα συστήματα IoMT λόγω του τεράστιου όγκου ευαίσθητων προσωπικών δεδομένων. Εάν το σύστημα παραβιαστεί τότε ο επιτιθέμενος μπορεί να κερδίσει σε γνώση, ωστόσο δεν θα είναι σε θέση να αντιστοιχίσει τα βιομετρικά δεδομένα με τους αντίστοιχους χρήστες του δικτύου. Έτσι, αντιμετωπίζονται οι επιθέσεις, που ακούν' την κίνηση στο δίκτυο και προσπαθούν να κερδίσουν σε γνώση (βλ. Κεφάλαιο 3.1.1.2, 3.2.1.2).

4.2.4 Απαιτήσεις στο Στρώμα Διεπαφής (Interface Layer)

Η προστασία της Ιδιωτικότητας των χρηστών στα συστήματα IoMT, συνεπάγεται στην διασφάλιση του ιατρικού απορρήτου. Είναι απαραίτητο στα συστήματα IoMT να υιοθετηθούν τεχνικές, οι οποίες θα εξασφαλίζουν την εκπλήρωση των παραπάνω απαιτήσεων. Ωστόσο, με την προσθήκη μεγάλου αριθμού μέτρων ασφάλειας, δεσμεύεται ένα μεγάλο μέρος των πόρων του συστήματος, δημιουργώντας προβλήματα απόδοσης και λειτουργικότητας στα συστήματα. Έτσι, γεννάται το ζήτημα των συμβιβασμών (Trade-offs) στα συστήματα IoMT, μεταξύ της απόδοσης του συστήματος και της ασφάλειας. Παρακάτω στον Πίνακα 4.3 συνοψίζονται οι απαιτήσεις Ιδιωτικότητας για τα στρώματα επικοινωνίας των συστημάτων IoMT.

	Sensing	Network	Service	Interface
Ανωνυμία	✓	—	—	✓
Μη-συνδεσιμότητα	✓	✓	✓	✓
Μη-παρατηρησιμότητα	✓	—	✓	✓
Μη-ανιχνευσιμότητα	✓	✓	—	✓
Μυστικότητα	—	✓	—	✓
Αυθεντικοποίηση	✓	—	—	✓
Εξουσιοδότηση	✓	—	—	✓

Πίνακας 4.3: Σύνοψη των απαιτήσεων ιδιωτικότητας στα τέσσερα στρώματα επικοινωνίας

Στο ανώτερο στρώμα επικοινωνίας, η πλειονότητα των απαιτήσεων είναι χρεωστικές για να αντιμετωπιστούν τα προβλήματα σε επίπεδο εφαρμογής και χρηστών (βλ. Κεφάλαιο 3.1.1.3, 3.2.1.3). Έστω ένας χρήστης του δικτύου που διαθέτει κοχλιακό εμφύτευμα. Σε περίπτωση που ο θεράπων γιατρός του θέλει να δει την πρόοδο του ή να ρυθμίσει τη συσκευή εξ αποστάσεως, δημιουργεί ένα κανάλι επικοινωνίας, το οποίο χειρίζεται μέσω του στρώματος διεπαφής.

Είναι απαραίτητο οι χρήστες που χρησιμοποιούν τους πόρους του συστήματος μια χρονική στιγμή να μην αναγνωριστούν (Ανωνυμία), όπως επίσης να μην γνωστοποιηθεί στους επιτιθέμενους ποιους πόρους χρησιμοποιεί (Μη-παρατηρησιμότητα), ούτε ποιες συσκευές του αντιστοιχούν (Μη-συνδεσιμότητα). Επιπλέον, είναι θεμιτό να παραμένουν στην αφάνεια οι κινήσεις του χρήστη στο σύστημα, χρησιμοποιώντας τεχνικές της Μη-ανιχνευσιμότητας. Αφού γίνεται λόγος για τη διεπαφή του χρήστη με το σύστημα, πρέπει μόνο οι Αυθεντικοποιημένες οντότητες να έχουν πρόσβαση σε δεδομένα που είναι Εξουσιοδοτημένοι να επεξεργαστούν. Φυσικά, η διασφάλιση της Μυστικότητας των στοιχείων συνόδου, όπως για παράδειγμα το κλειδί συνόδου, πρέπει να προστατευτεί, αφού σε άλλη περίπτωση μπορεί να υπάρξει παραβίαση του συστήματος.

4.3 Συμβιβασμοί στα Συστήματα IoMT (Trade-offs)

Μεγάλη πρόκληση για τα συστήματα IoMT είναι τα trade-offs ή διαφορετικοί συμβιβασμοί που πρέπει να γίνουν μεταξύ της Ασφάλειας και της Απόδοσης του συστήματος. Τα trade-offs εγείρουν καινούργιες προκλήσεις, αφού οι σχεδιαστές των συστημάτων μπαίνουν στη διαδικασία να δημιουργήσουν λύσεις, με τις οποίες το σύστημα

θα προσφέρει ασφάλεια για τους χρήστες και τα δεδομένα τους, θωρακίζοντας το, αλλά παράλληλα εκμεταλλεύοντας με όσο το δυνατόν αποδοτικότερο τρόπο τους πόρους του συστήματος.

Γενικότερα, τα συστήματα IoMT αποτελούνται από ένα σύνολο μικροσυσκευών και αισθητήρων, τα οποία διαθέτουν χαμηλούς υπολογιστικούς και αποθηκευτικούς πόρους. Η φύση των συσκευών στα συστήματα IoMT καθιστά αναγκαία την εγκαθίδρυση ισχυρών μέτρων ασφάλειας ενώ, τα βιομετρικά δεδομένα των ασθενών που συλλέγουν απαιτούν τη διασφάλιση τους από τυχόν επιθέσεις. Ταυτόχρονα, για την ομαλή εκτέλεση των ιατρικών υπηρεσιών και έπειτα την αποθήκευση των δεδομένων, απαιτείται ένας σημαντικό μέγεθος των διαθέσιμων πόρων.

Τα trade-offs προκύπτουν ως προς την προσέγγιση, που είναι επιθυμητό να ακολουθήσουν στα συστήματα. Από τη μία, υπάρχει η έννοια της ποιότητας των ιατρικών υπηρεσιών (Quality of Service - QoS), όπου οι σχεδιαστές των συστημάτων προσπαθούν να δημιουργήσουν ένα πλήρες ανταποκρίσιμο σύστημα, το οποίο θα επιτελεί τις λειτουργίες του κατά το θεμιτό τρόπο και ιδιαίτερα σε αντίξοες συνθήκες με πλήρη Ασφάλεια, Αξιοπιστία, Ευρωστία, Διαλειτουργικότητα και κυρίως Διαθεσιμότητα. Τα συστήματα IoMT έρχονται αντιμέτωπα με τέτοιες καταστάσεις, κυρίως στις περιπτώσεις των επείγοντων περιστατικών. Οι Zhang et al., 2017 ξεχωρίζουν για τη περίπτωση των Εμφυτευμένων συσκευών περιπτώσεις, οι οποίες επικεντρώνονται στη περίπτωση των επείγοντων περιστατικών.

Αρχικά, αντικρούονται οι απαιτήσεις Ασφάλειας και Διαθεσιμότητας (Security vs. Availability) σε Επείγοντα Περιστατικά. Τα μέτρα ασφαλείας, που εφαρμόζονται πρέπει να είναι αρκετά αυστηρά, γιατί αφορούν ευαίσθητα προσωπικά δεδομένα, ενώ είναι θεμιτό τα δεδομένα να γίνονται διαθέσιμα στους χρήστες ή τους γιατρούς οποιαδήποτε στιγμή. Οι Εμφυτευμένες συσκευές διαθέτουν μηχανισμούς απλής και επείγουσας λειτουργίας. Ωστόσο, σε περίπτωση επείγοντος περιστατικού παίρνει μεγαλύτερες διαστάσεις, καθώς η πρόσβαση στα προσωπικά δεδομένα του ασθενούς πρέπει να είναι εφικτή από τον επείγοντα γιατρό.

Αναφέρονται στη περίπτωση που αντικρούεται η έννοια της Επείγουσας Αυθεντικοποίησης με τις Τακτικές Επισκέψεις στον θεράπων γιατρό για τους ασθενείς χρόνιων παθήσεων, οι οποίες μπορεί να εφιστούν την ανάγκη βοηθητικής εξωτερικής συσκευής Επείγουσας Αυθεντικοποίησης, δημιουργώντας μεγαλύτερες απαιτήσεις ενεργειακών πόρων. Ταυτόχρονα, τονίζουν την ανικανότητα των εμφυτευμένων συσκευών να στηρίζουν ισχυρά μέτρα ασφάλειας, τα οποία καταναλώνουν μεγάλες ποσότητες ενεργειακών πόρων μειώνοντας τον χρόνο ζωής των συσκευών.

Θέματα Συμβιβασμών προκύπτουν μεταξύ της Ασφάλειας του συστήματος (Security) και αυτής των χρηστών (Safety). Εφόσον εφαρμοστούν πολύ ισχυρά μέτρα ασφάλειας, υπάρχει κίνδυνος περιορισμού της ελευθερίας των χρηστών. Για παράδειγμα, ένας ασθενής ο οποίος διαθέτει ένα κοχλιακό εμφύτευμα (βλ. 2.2 και βρίσκεται σε ένα μέρος μακριά από τον θεράπων γιατρό του. Σε περίπτωση που το εμφύτευμα απορυθμιστεί, ο ασθενής πρέπει να επισκεφτεί τον κοντινότερο γιατρό. Εάν τα μέτρα ασφάλειας είναι αρκετά αυστηρά (Security), ο ασθενής δεν θα είναι σε θέση να το ρυθμίσει δημιουργώντας πιθανά προβλήματα (Safety).

Από την άλλη, με την έννοια της ποιότητας στην προστασία (Quality of Protection - QoP), οι σχεδιαστές των συστημάτων, επιθυμούν να εφαρμόσουν τις ιδανικότερες μεθοδολογίες, με τις οποίες θα προστατεύονται τα αγαθά του συστήματος ικανοποιώντας τις παραπάνω απαιτήσεις. Και οι δύο έννοιες απαιτούν πολλούς ενεργειακούς πόρους,

οπότε το ζήτημα που τίθεται, είναι η αποδοτικότερη εκμετάλλευση των πόρων, με την κάλυψη όσο το δυνατόν περισσότερων ευπαθειών και την καλύτερη λειτουργία του συστήματος, θέτοντας προτεραιότητες και κάνοντας τις κατάλληλες παραδοχές.

Καταληκτικά, παρατηρείται ότι η πλειονότητα των ερευνητικών εργασιών (AlTawy and Youssef, 2016; Challa et al., 2018; Zheng et al., 2017), που κάνουν λόγο για τα ζητήματα των trade-offs, αφορούν τις Εμφυτευμένες συσκευές ή γενικά για τις συσκευές, που χρησιμοποιούνται στα δίκτυα MCPs. Στα πλαίσια των συστημάτων IoMT, ζητήματα προκύπτουν μεταξύ της **Ισχυρής Ασφάλειας** των συστημάτων με τεχνικές **Ελέγχου Πρόσβασης**, που θα προστατεύουν το σύστημα και τα δεδομένα του χρήστη, των μηχανισμών **Έκτακτης Αυθεντικοποίησης** σε περίπτωση επείγοντος περιστατικού, και στις **Αποδοτικότερης** διαχείρισης των Ενεργειακών και Υπολογιστικών Πόρων. Στο Σχ. 4.2, τα trade-offs, που αναγράφονται αφορούν το σύνολο των συσκευών IoMT, στις οποίες αντικρούονται οι παραπάνω έννοιες. Σε κάθε περίπτωση, οι σχεδιαστές των συστημάτων IoMT, πρέπει να κάνουν σημαντικές υποχωρήσεις, που θεωρούν ότι θα ισορροπήσουν τις έννοιες των QoP και QoS, προσφέροντας την ιδανικότερη λύση.



Σχήμα 4.2: Το σύνολο των εννοιών που αντικρούονται στα συστήματα IoMT.

Στο επίκεντρο τοποθετούνται οι περιορισμένοι **Υπολογιστικοί** και **Αποθηκευτικοί** πόροι, όπου στόχος του συστήματος είναι η εκμετάλλευσή τους για την μεγιστοποίηση της **Ασφάλειας** των χρηστών και του συστήματος (QoP), προσφέροντας λειτουργικές και αποδοτικές ιατρικές **Υπηρεσίες** (QoS). Απαιτούνται τεχνικές **Ελέγχου Πρόσβασης**, καθώς είναι επιθυμητό μόνον εξουσιοδοτημένες οντότητες να έχουν πρόσβαση σε συγκεκριμένα δεδομένα. Ταυτόχρονα, πρέπει να εφαρμοστούν τεχνικές **Επείγουσας Αυθεντικοποίησης**, που θα επιτρέψουν την πρόσβαση στα βιομετρικά δεδομένα του ασθενούς σε περίπτωση επείγοντος περιστατικού. Καταληκτικά, για την καλύτερη εξυπηρέτηση των χρηστών, είναι επιθυμητή η επεκτατική διάθεση του

συστήματος(**Επεκτασιμότητα**) για την προσθήκη καινούργιων αισθητήρων ή ενός συνόλου αισθητήρων που αφορούν έναν χρήστη και ταυτόχρονα την γρήγορη προσαρμογή του συστήματος στα καινούργια δεδομένα, με σκοπό την διατήρηση της ομοιογένειας του. (**Ευρωστία**).

Οι συμβιβασμοί αποτελούν σημαντικό ζήτημα για τον σχεδιασμό των συστημάτων IoMT. Έτσι, ανάλογα με τη φύση των συσκευών που θέλουν να διασφαλίσουν (Εμφυτευμένοι, Φορητοί, ΣΑΠ) πρέπει να λαμβάνονται και αντίστοιχα μέτρα ασφάλειας, τα οποία θα εναρμονίζονται μεταξύ των εννοιών QoS και QoP. Φαίνεται ότι υφίσταται η προσοχή περισσότερο στη ποιότητα των υπηρεσιών παρά στην ασφάλεια τους. Στο επόμενο κεφάλαιο, μελετούνται οι προτεινόμενες λύσεις της βιβλιογραφίας, εξετάζοντας ποιες απαιτήσεις ικανοποιούνται και σε ποιο βαθμό, διακρίνοντας τα πιθανά κενά ασφάλειας που αφήνουν.

Κεφάλαιο 5

Μέτρα για την Ενίσχυση της Ασφάλειας και της Ιδιωτικότητας στα Συστήματα IoMT

Όπως αναφέρθηκε στα προηγούμενα κεφάλαια, η διασφάλιση της τριάδας CIA στα συστήματα IoMT αποτελεί μείζων ζήτημα, λόγω της φύσεως των δεδομένων και των συστημάτων. Οι υπάρχουσες λύσεις ασφάλειας επιχειρούν να ικανοποιήσουν τις απαιτήσεις που εγείρονται από το σύνολο των απειλών στα συστήματα IoMT. Επιπλέον, ως προτεραιότητα για τους χρήστες των δικτύων IoMT αποτελεί η διασφάλιση του ιατρικού απορρήτου. Παρακάτω στο κεφάλαιο, αναλύονται οι λύσεις της προτεινόμενης βιβλιογραφίας.

Αρχικά, γίνεται αναφορά σε ένα σύνολο μέτρων, όπου κάθε σύστημα πρέπει να λαμβάνει για την αποφυγή βασικών απειλών. Έπειτα, οι συγγραφείς μελετούν τις προτεινόμενες λύσεις της βιβλιογραφίας με γνώμονα τις απαιτήσεις που ικανοποιούν, τις απειλές που αντιμετωπίζουν και τα τυχόν κενά στην ασφάλεια που αφήνουν. Τέλος, γίνεται εκτενής αναφορά των ανοιχτών ζητημάτων στα υπάρχοντα συστήματα ασφάλειας για τη περίπτωση των δικτύων IoMT. Η ανάλυση γίνεται με γνώμονα τα στρώματα επικοινωνίας (βλ. 2.6, καθώς οι προτεινόμενες λύσεις αναφέρονται στις τεχνολογίες που χρησιμοποιούνται. Στο κείμενο γίνεται η αντιστοίχιση με τα επίπεδα της αρχιτεκτονικής όπως στον Πίνακα 4.1.

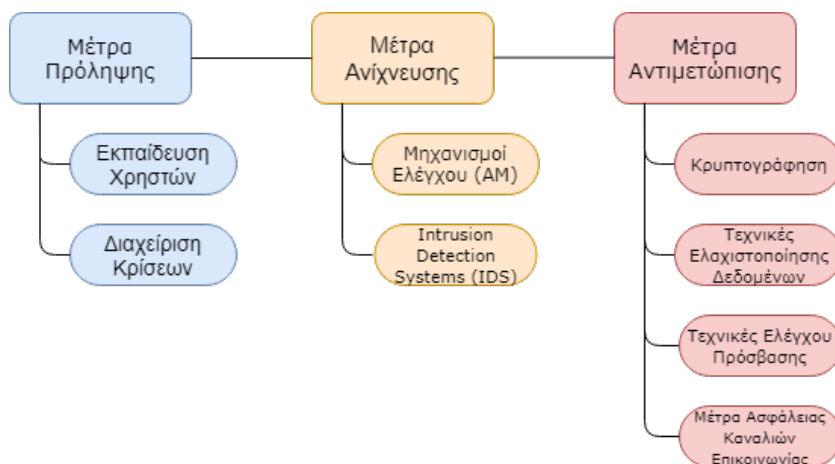
5.1 Προκαθορισμένες Λύσεις στην Ασφάλεια και Ιδιωτικότητα

Στην πρώτη ενότητα καταγράφονται οι λύσεις που κάθε οργανισμός, ο οποίος διαχειρίζεται ευαίσθητα προσωπικά δεδομένα όπως δηλαδή τα συστήματα IoMT, πρέπει να λάβει. Σκοπός των προτεινόμενων μέτρων είναι η ικανοποίηση των απαιτήσεων (βλ. Κεφάλαιο 4), καθώς τίθενται οι βάσεις για την αντιμετώπιση της πλειονότητας των απειλών (βλ. Κεφάλαιο 3) στα συστήματα IoMT.

Ωστόσο, τα μέτρα ασφάλειας που δημιουργούνται για τα συστήματα IoMT, εξαιτίας των συμβιβασμών (βλ. Κεφάλαιο 4.3) δεν μπορούν να καλύψουν όλες τις απαιτήσεις των συστημάτων. Όπως φαίνεται στο Σχ. 5.1 τα προκαθορισμένα μέτρα χωρίζονται σε

τρεις ομάδες:

1. Μέτρα Πρόληψης,
2. Μέτρα Ανίχνευσης,
3. Μέτρα Αντιμετώπισης.



Σχήμα 5.1: Διαχωρισμός των μέτρων ασφάλειας ανάλογα με το στάδιο εφαρμογής.

5.1.1 Μέτρα Πρόληψης

Απαραίτητο για ένα σύστημα είναι η προετοιμασία αυτού και των χρηστών του για την αποφυγή όσο το δυνατόν περισσότερων απειλών. Γίνονται τα πρώτα βήματα για την διασφάλιση και των τριών επιπέδων της προτεινόμενης αρχιτεκτονικής (2.9). Αρχικά, γίνεται με την Εκπαίδευση των Χρηστών, αντιμετωπίζονται προβλήματα που προκύπτουν εσωτερικά του συστήματος, ενώ με το σχεδιασμό πλάνου Διαχείρισης Κρίσεων, μπορούν να αντιμετωπιστούν κλασικές επιθέσεις όπως SQL Injection, Replay και Relay. Ωστόσο, και στις δύο περιπτώσεις εξαιτίας της αυξημένης κατανάλωσης ενεργειακών πόρων, είναι πιθανό να μειωθεί η απόδοση το συστήματος προσβάλλοντας τις προσφερόμενες ιατρικές υπηρεσίες (βλ. Κεφάλαιο 4.3).

5.1.1.1 Εκπαίδευση Χρηστών

Από τα πρωταρχικά βήματα για τη διασφάλιση των συστημάτων είναι η εκπαίδευση των χρηστών του. Όπως προαναφέρθηκε, ένα σύνολο χρηστών δεν είναι γνώριμο με τις καινούργιες τεχνολογίες, ή ακόμα δεν αντιλαμβάνεται πώς γίνεται η περισυλλογή και επεξεργασία των ευαίσθητων προσωπικών δεδομένων του. Επιπλέον, δείχνουν απάθεια ως προς το τρόπο εκμετάλλευσης των δεδομένων τους. Οι παραπάνω ενέργειες εκθέτουν το σύστημα σε εσωτερικούς κινδύνους, όπως διαρροή εκ των έσω ή ακούσια (βλ. Κεφάλαιο 3.1.1.3).

Εκπαιδύοντας τους χρήστες των συστημάτων IoMT μειώνονται οι πιθανότητες εκδήλωσης εσωτερικών συμβάντων, καθώς τους γνωστοποιείται το σύνολο των ενεργειών στις οποίες είναι απαγορευτικό να προβούν και στις επιπτώσεις αυτών. Έτσι, ενισχύονται οι έννοιες της Εμπιστευτικότητας, Ακεραιότητας, Διαθεσιμότητας, Ιδιωτικότητας και Ευθύνης. Όπως είναι λογικό, αυτό το μέτρο αφορά και τα τέσσερα στρώματα επικοινωνίας.

5.1.1.2 Διαχείριση Κρίσεων

Η Διαχείρισή Κρίσεων αναφέρεται στην ιδιότητα των συστημάτων να θέτουν στο δίκτυο τους όρια σύγκρισης με σκοπό την εύρεση πιθανών απειλών. Τα μέτρα διαχείρισης κρίσεων τοποθετούνται πριν τα μέτρα ανίχνευσης. Η δημιουργία ενός συνόλου κανόνων σε περίπτωση κρίσεως αποτελεί ένα ακόμα μέτρο πρόληψης. Χρησιμοποιείται σαν μέτρο σε περιπτώσεις κλασικών επιθέσεων όπως Replay, Brute-force, Buffer overflow και Masquerade. Όταν τα μέτρα ανίχνευσης απειλών εντοπίσουν παραβατικές συμπεριφορές, τότε το σύστημα πρέπει να δράσει βάσει των κανόνων του μοντέλου Διαχείρισης Κρίσεων. Όπως και το προηγούμενο μέτρο, αφορά και τα τέσσερα στρώματα επικοινωνίας. Η χρήση τους ενισχύει τις έννοιες της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας, αφού αντιμετωπίζονται απειλές κατά αυτών. Επιπλέον, οι έννοιες της Ευρωστίας και Εμπιστοσύνης μεταξύ των συσκευών ενισχύονται, καθώς ισχυροποιούνται οι προσπάθειες προσαρμογής του συστήματος κατά τη διάρκεια μιας επίθεσης.

5.1.2 Μεθοδολογίες Ανίχνευσης

Η συγκεκριμένη υποενότητα αποτελείται από τους προτεινόμενους μηχανισμούς που χρησιμοποιούνται για τη παρακολούθηση και ανάλυση του συστήματος και των συσκευών IoMT, με σκοπό τον εντοπισμό και τη καταγραφή παραβατικών συμβάντων. Είναι επιθυμητό, οι Μηχανισμοί Ανίχνευσης να λαμβάνουν υπόψη ότι οι πιθανές ενέργειες κατά του συστήματος, μπορεί να προέρχονται από εσωτερικούς ή εξωτερικούς παράγοντες του συστήματος, οι οποίοι δεν έχουν άμεση πρόσβαση σε αυτό. Επιπλέον, πρέπει τα μέτρα ανίχνευσης να έχουν τη δυνατότητα να αναγνωρίζουν τα σφάλματα και τα ανθρώπινα λάθη, που προκύπτουν στο σύστημα.

5.1.2.1 Μηχανισμοί Ελέγχου - Audit Mechanisms (AM)

Αποτελεί τον πιο απλό μηχανισμό ανίχνευσης. Στην ουσία, οι μηχανισμοί AM ελέγχουν τα εσωτερικά αρχεία των συσκευών και του συστήματος, τα οποία περιέχουν πληροφορίες για τις κινήσεις των χρηστών. Σε περίπτωση, που ένας χρήστης υποστεί επίθεση Masquerade και ο επιτιθέμενος, εκτελέσει μια ασυνήθιστη για τον χρήστη κίνηση, τότε οι μηχανισμοί εντοπίζουν και ενημερώνουν έγκαιρα το σύστημα.

Οι συσκευές διατηρούν αρχεία εγγραφών με λεπτομερή περιγραφές (logs) όπως ο τρόπος με τον οποίο γίνεται η διάδραση του χρήστη με τη συσκευή. Σε συνδυασμό με τις μεθόδους ανίχνευσης ανώμαλης δραστηριότητας που αναλύονται παρακάτω, μπορούν να εντοπιστούν οι παραβατικές συμπεριφορές, δηλαδή αυτές που δεν αρμόζουν στη συμπεριφορά ούτε του συστήματος ούτε των χρηστών του. Εφόσον οι μηχανισμοί AM ελέγχουν όλο το σύστημα, αφορά και τα τέσσερα επίπεδα επικοινωνίας. Εκτός από τη διασφάλιση της τριάδας CIA, ενισχύονται οι έννοιες Ελέγχου Πρόσβασης, Ευθύνης, και Μη-άρνησης των χρηστών στο σύστημα.

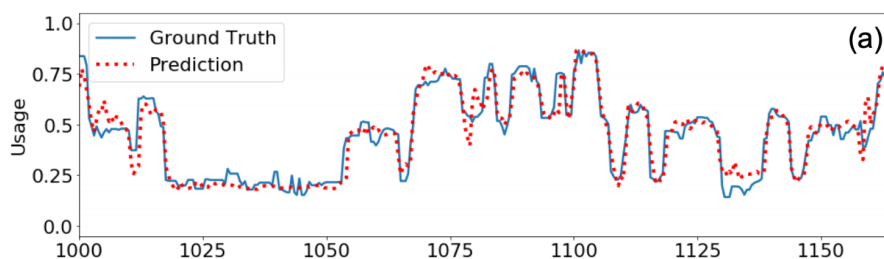
Στα αρνητικά των μηχανισμών AM συγκαταλέγεται η αυξημένη ανάγκη αποθηκευτικών πόρων στις συσκευές και το σύστημα IoMT για την αποθήκευση των αρχείων. Σε περίπτωση επίθεσης Buffer overflow, εάν δεν λειτουργήσουν σωστά οι μηχανισμοί να προκύψει διαρροή στην ιδιωτικότητα (βλ. Κεφάλαιο 3.1.1.1, 3.2.1.1).

5.1.2.2 Συστήματα Ανίχνευσης Παραβατικής Συμπεριφοράς (Intrusion Detection Systems - IDS)

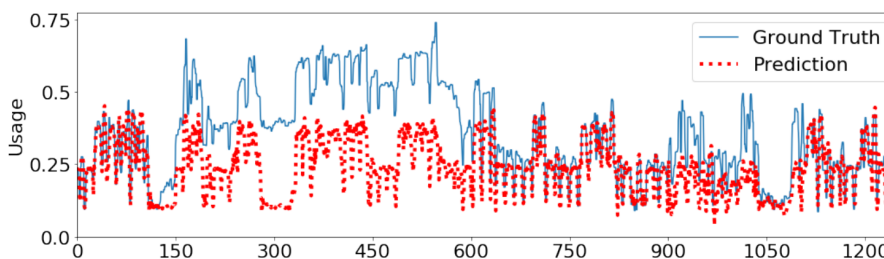
Ως ανώμαλη συμπεριφορά στο σύστημα ορίζεται το σύνολο των δεδομένων, που δεν έχουν κοινά σημεία με το σύνολο των δεδομένων ή δεν ακολουθούν την αναμενόμενη τάση ή χαρακτηριστικά (Ukil et al., 2016). Για να επιτευχθεί αυτό, συχνά χρησιμοποιούνται τεχνικές, που βασίζονται σε Μηχανικής Μάθησης (Supervised Machine Learning - SML), κατά την οποία το μοντέλο του μηχανισμού IDS, εκπαιδεύεται γύρω από τις συνήθειες του χρήστη, έτσι ώστε όταν ανιχνεύσει μια κακεντρεχή συμπεριφορά στο σύστημα - όπως η ασυνήθιστη κατανάλωση ενεργειακών πόρων από μια συσκευή - να ενημερώνει τον θεράποντα ιατρό, κάποιον επαγγελματία υγείας, τον χρήστη ή τον διαχειριστή του δικτύου (Rathore et al., 2017). Οι τεχνικές IDS εφαρμόζουν και στα τέσσερα στρώματα επικοινωνίας, ελέγχοντας τις συσκευές και τη κίνηση του δικτύου, ενισχύοντας τις έννοιες Ελέγχου Πρόσβασης, Ευθύνης, Εμπιστοσύνης, Ιδιωτικότητας και Ευρωστίας.

Η πλειονότητα των προτεινόμενων λύσεων επικεντρώνονται στις ηλεκτρονικές επιθέσεις και λιγότερο στις φυσικές. Ένα χαρακτηριστικό παράδειγμα τέτοιου μηχανισμού παρατίθενται από τους Li et al., 2019, οι οποίοι προτείνουν ένα μοντέλο το οποίο βασίζεται στον έλεγχο της κατανάλωσης των ενεργειακών πόρων των συσκευών IoMT, χρησιμοποιώντας τεχνικές Μηχανικής Μάθησης.

Πιο συγκεκριμένα, η μέθοδος τους βασίζεται σε τεχνικές ML. Όπως φαίνεται στο Σχ. 5.2, προβλέπεται ένα μοτίβο για τη κατανάλωση ενέργειας της συσκευής, το οποίο έχει δημιουργηθεί από προηγούμενες μετρήσεις. Έτσι, η κόκκινη γραμμή δείχνει την πρόβλεψη του μηχανισμού (Prediction), ενώ η μπλε γραμμή (Ground Truth) δείχνει την κατανάλωση αναλογικά με τον αναγραφόμενο χρόνο.



(α) Προβλεπτικό γράφημα ενεργειακής κατανάλωσης υπό φυσιολογικές συνθήκες.



(β) Προβλεπτικό γράφημα ενεργειακής κατανάλωσης υπό φυσική και cyber επίθεση.

Σχήμα 5.2: Ανάλυση απόδοσης μεθοδολογιών ανίχνευσης επιθέσεων με βάση των Μηχανική Μάθηση.

Στο Σχ. 5.2(α') φαίνεται ότι η κατανάλωση της ενέργειας συνάδει με την πρόβλε-

ψη της μεθόδου, αφού η πρόβλεψη του μηχανισμού σε σχέση με την πραγματική μέτρηση έχουν παρόμοια πορεία, οπότε δεν ανιχνεύεται ανώμαλη συμπεριφορά στο σύστημα. Στο Σχ. 5.2(β'), φαίνεται ξεκάθαρα ότι η κατανάλωση της ενέργειας δεν συμφωνεί με αυτή της πρόβλεψης. Χαρακτηριστικά, η επίθεση στο σύστημα συμβαίνει στα χρονικά σημεία του γραφήματος, που φαίνεται ότι η κατανάλωση είναι υψηλότερη σε σχέση με το προβλεπτικό γράφημα.

Από την άλλη, οι προκλήσεις που αντιμετωπίζουν οι μηχανισμοί IDS κυμαίνονται στον διαχωρισμό ανώμαλων συμβάντων με πραγματικά επεισόδια. Το ζήτημα λαμβάνει μεγαλύτερες διαστάσεις, όταν γίνεται λόγος για επείγοντα περιστατικά, όπου η λειτουργία του συστήματος και τα σήματα που παρέχονται από το χρήστη βγαίνουν εντελώς εκτός από τα συνηθισμένα, δημιουργώντας προβλήματα στην Ευρωστία του συστήματος. Επιπλέον, ένα κρίσιμο ζήτημα για τα συστήματα IoMT είναι η Επείγουσα Αυθεντικοποίηση, όπου αντικρούεται με τους Μηχανισμούς Ανίχνευσης ως προς το τρόπο αντιμετώπισης των εν λόγω ζητημάτων, καθώς πρέπει το σύστημα να διαχωρίζει αλάνθαστα τα επείγοντα περιστατικά από τις παραβατικές συμπεριφορές.

Οι κλασσικές τεχνικές IDS δεν μπορούν να εφαρμοστούν στα συστήματα IoT, λόγω των περιορισμένων ενεργειακών πόρων και της ετερογένειας που τα χαρακτηρίζει. Οι Zarpelao et al., 2017, κάνοντας αφηγηματική βιβλιογραφική ανασκόπηση για τα συστήματα IDS που έχουν προταθεί για τη περίπτωση των συστημάτων IoT, ταξινόμησαν τις τεχνικές με βάση τα τέσσερα χαρακτηριστικά. Η πρώτη διαφοροποίηση αναφέρεται στο σημείο του συστήματος που εφαρμόζουν οι τεχνικές IDS. Έπειτα, οι τεχνικές διαχωρίζονται ανάλογα με τη μέθοδο ανίχνευσης, τον τύπο επίθεσης και τη στρατηγική αξιολόγησης. Καταλήγουν, αναφέροντας την αδυναμία των τεχνικών να καλύψουν τις ανάγκες των συστημάτων IoT και των επικείμενων επιθέσεων, δεν διακρίνεται ποια τεχνική είναι η πιο επαρκής για τα συστήματα.

5.1.3 Μεθοδολογίες Αντιμετώπισης Προβλημάτων στα Συστήματα IoMT

Είναι σημαντικό τα μέτρα που εφαρμόζονται στα συστήματα IoMT να χαρακτηρίζονται έντονα από την έννοια της Ευρωστίας. Τα συστήματα είναι θεμιτό να ανακάμπτουν άμεσα από οποιαδήποτε επίθεση, διατηρώντας τη Λειτουργικότητα τους, καθώς γίνεται λόγος για ιατρικές υπηρεσίες και η λειτουργικότητα τους επηρεάζει τη ζωή των χρηστών. Όπως αναφέρουν οι Andrea et al., 2015 η χρήση τεχνικών Antivirus, Anti-adware ή Anti-spyware, αυξάνει την *Αξιοπιστία* του συστήματος, την γενικότερη *Ασφάλεια Πληροφοριών*, την *Εμπιστευτικότητα* και την *Ακεραιότητα* του. Επιπλέον, με τη χρήση τείχους προστασίας (Firewall), προστίθεται ένα στρώμα προστασίας. Φυσικά, τα εν λόγω μέτρα δεν μπορούν να εγγυηθούν την καθολική ασφάλεια του συστήματος, αλλά έναν βασικό έλεγχο. Όπως προαναφέρθηκε, (βλ. Κεφάλαιο 3) τα συστήματα IoMT αποτελούν βασικό στόχο για τους παραβάτες. Έτσι, είναι απαραίτητη η χρήση πιο ισχυρών και πολύπλοκων μέτρων ασφάλειας.

5.1.3.1 Κρυπτογράφηση

Η κρυπτογραφία αποτελεί έναν από τους δομικούς λίθους στις μεθόδους αντιμετώπισης των προκλήσεων σε όλα τα συστήματα. Ωστόσο, πολλές από τις τεχνικές που χρησιμοποιούνται κατά κόρον στα γενικού σκοπού συστήματα δεν μπορούν να εφαρμο-

στούν στα συστήματα IoMT, εξαιτίας της περιορισμένης υπολογιστικής ισχύος και του περιορισμένου διαθέσιμου αποθηκευτικού χώρου στις συσκευές. Στα συστήματα IoMT εφαρμόζονται κυρίως τεχνικές ασύμμετρης κρυπτογράφησης και τεχνικές Hashing. Μέσω αυτών διασφαλίζονται η Εμπιστευτικότητα του συστήματος και η Ακεραιότητα των δεδομένων. Ταυτόχρονα, η Αυθεντικοποίηση των δεδομένων ισχυροποιείται. Με τη διατήρηση της Ανωνυμίας των κρυπτογραφημένων δεδομένων διατηρείται και η Ιδιωτικότητα των χρηστών. Τεχνικές κρυπτογράφησης εφαρμόζουν σε όλα τα επίπεδα.

Στο πρώτο επίπεδο κατά την προετοιμασία των βιομετρικών δεδομένων από τους αισθητήρες του προσωπικού δικτύου με σκοπό τη προώθησή του στο επόμενο επίπεδο. Έπειτα, σημαντικό χαρακτηριστικό για το δεύτερο επίπεδο είναι η κρυπτογραφία, αφού πλέον τα δεδομένα είναι ευάλωτα στις εκτεθειμένες δικτυακές δομές του συστήματος. Επιπλέον, σε περίπτωση που παραβιαστούν οι αποθηκευτικές και επεξεργαστικές δομές του συστήματος τα δεδομένα πρέπει να είναι κωδικοποιημένα. Τέλος, στο τρίτο επίπεδο τα αιτήματα και τα δεδομένα πρέπει να παραμένουν προστατευμένα, έτσι ώστε σε περίπτωση παραβίασης τους να μην μπορούν οι επιτιθέμενοι να κερδίσουν εύκολα σε γνώση.

Όπως αναφέρθηκε, στα συστήματα IoMT εφαρμόζονται τεχνικές κρυπτογράφησης Lightweight, διότι οι πόροι που διαθέτουν είναι περιορισμένοι και χρειάζονται για την ολοκλήρωση των προσφερόμενων υπηρεσιών. Με αυτό το τρόπο, ικανοποιούνται το κατά δύναμιν οι παραπάνω απαιτήσεις, αλλά ταυτόχρονα εξοικονομείται σημαντικό μέρος των ενεργειακών πόρων των συσκευών. Έτσι, μπορεί κανείς να θεωρήσει ότι διασφαλίζεται και η Διαθεσιμότητα των συσκευών, καθώς οι ενεργειακές ανάγκες των προβλεπόμενων απαιτήσεων εκπληρώνονται και μένουν πόροι για το σύστημα.

Χαρακτηριστικό παράδειγμα, αποτελεί ο αλγόριθμος Advanced Encryption Standard (AES), όπου έχει εφαρμοστεί ένα σύνολο διαφορετικών παραλλαγών του στα συστήματα IoMT, οι οποίοι ικανοποιούν τις έννοιες της Εμπιστευτικότητα και Ιδιωτικότητας (Mosenia and Jha, 2017). Χρησιμοποιούνται οι αλγόριθμοι SHA-1 και SHA256 για την προστασία της Ακεραιότητας των μηνυμάτων. Ωστόσο, η τεχνική της κρυπτογράφησης πρέπει συνδυαστικά να λειτουργήσει με ένα σύνολο από μέτρα, καθώς από μόνη της δεν μπορεί να σταθεί. Ειδικά σε συστήματα IoMT, το οποίο δεν προσφέρει λύσεις για τις υπόλοιπες απαιτήσεις.

Ο αλγόριθμος Elliptic Curve Cryptography (ECC), αποτελεί τη πιο διαδεδομένη λύση, προσφέροντας μια ισχυρή λύση για την ασφάλεια των συστημάτων. Αν και προσφέρει συμπαγής και ισχυρές υπογραφές, με μικρό μέγεθος στα κλειδιά συνόδων, ως τεχνική δημοσίου κλειδιού, οι ενεργειακές απαιτήσεις της τεχνικής ECC είναι αρκετά υψηλές, όπου η εφαρμογή της αποτελεί σημαντική πρόκληση για τα συστήματα IoMT (Zhang et al., 2017).

5.1.3.2 Τεχνικές Ελαχιστοποίηση Δεδομένων

Οι τεχνικές εφαρμόζονται στο δεύτερο επίπεδο της προτεινόμενης αρχιτεκτονικής που αφορά τα στρώματα Δικτύου και Διεργασιών. Είναι θεμιτό η διαμοιραζόμενη πληροφορία να φτάνει το συντομότερο στον κόμβο παραλήπτη και να καταλαμβάνει το κατά δύναμιν ελάχιστο χώρο στις αποθηκευτικές δομές του συστήματος όπως οι βάσεις δεδομένων και τα υπολογιστικά νέφη. Φυσικά, ελευθερώνοντας πόρους στο σύστημα, μειώνεται η επιρρέπεια των συστημάτων IoMT σε επιθέσεις όπως Buffer overflow, ενισχύοντας τις έννοιες της Ευρωστίας, Επεκτασιμότητας.

Οι Akmandor et al., 2018, προτείνουν μια αρχιτεκτονική για τα συστήματα IoT, η οποία βασίζεται στην συμπίεση των δεδομένων και σε μηχανισμούς λήψεων αποφάσεων Μηχανικής Μάθησης. Σκοπός της συμπίεσης των δεδομένων είναι η μείωση του μεγέθους, αλλά ταυτόχρονα η διατήρηση της συνολικής πληροφορίας ανέγγιχτη. Έτσι, το σύστημα επωφελείται σε θέματα ενέργειας και χώρου, αφού ελαττώνονται οι απαιτούμενοι πόροι του συστήματος, που καταναλώνονται για θέματα επεξεργασίας, αποθήκευσης και μεταφοράς.

Έπειτα, με τις τεχνικές Ελαχιστοποίησης των Δεδομένων που παράγονται από τις συσκευές, μειώνεται το μέγεθος της συνολικής πληροφορίας, ελευθερώνοντας τους αποθηκευτικούς πόρους του συστήματος και ταυτόχρονα δεσμεύοντας όσο το δυνατόν λιγότερους ενεργειακούς πόρους για την επεξεργασία τους. Οι Xu et al., 2018, προτείνουν μια δομή Framework, βασισμένη στην έννοια Edge Computing, όπου η ιατρική πληροφορία μεταφέρεται σε κόμβους με ισχυρούς υπολογιστικούς πόρους - όπως συσκευές Router ή σημεία περισυλλογής -, στα οποία ελαχιστοποιούνται τα δεδομένα και γίνεται ανοικοδόμηση της πληροφορίας. Η νέα πληροφορία προωθείται στο υπολογιστικό νέφος, όπου με τεχνικές Data Analytics επεξεργάζεται για τη παραγωγή μεταδεδομένων. Έτσι, μεταξύ άλλων εξοικονομείται ένα μέρος των ενεργειακών αποθεμάτων του συστήματος.

Με την εφαρμογή τους γίνεται συλλογή πιο έγκυρης και ακριβής πληροφορίας από τις συσκευές IoMT, χρησιμοποιώντας λιγότερους υπολογιστικούς και ενεργειακούς πόρους, και ταυτόχρονα αντιμετωπίζοντας το ζήτημα της Συσσώρευσης Δεδομένων στο σύστημα, ενισχύοντας τις έννοιες της Εμπιστευτικότητας και Ακεραιότητας των συστημάτων IoMT. Ωστόσο, έχουν υψηλές απαιτήσεις σε πόρους κατά τη διαδικασία αποσυμπίεσης των δεδομένων για την απόκτηση της συνολικής επιθυμητής πληροφορίας.

5.1.3.3 Τεχνικές Ελέγχου Πρόσβασης

Οι μηχανισμοί Αυθεντικοποίησης παίζουν καθοριστικό ρόλο στα συστήματα IoMT, καθώς η λειτουργία των συστημάτων βασίζεται σε αυτούς. Με την Αυθεντικοποίηση, δημιουργούνται ομάδες χρηστών που έχουν συγκεκριμένα δικαιώματα. Έτσι, κάθε Εξουσιοδοτημένος χρήστης έχει πρόσβαση στα δικά του δεδομένα και κάθε επαγγελματία υγείας έχει πρόσβαση σε συγκεκριμένα δεδομένα των ασθενών του. Συνεργάζονται άμεσα και εναρμονίζονται με τους μηχανισμούς Ελέγχου Πρόσβασης, καθώς η λειτουργία του ενός εξαρτάται από την λειτουργία του άλλου, προστατεύοντας την Ιδιωτικότητα των χρηστών απορρίπτοντας την πρόσβαση σε δεδομένα που δεν έχουν πληρεξούσιο.

Οι μηχανισμοί Ελέγχου Πρόσβασης λειτουργούν σαν μέσο ασφάλειας σε όλα τα συστήματα. Στις περιπτώσεις των συστημάτων IoMT είναι απαραίτητοι, διότι διαμοιράζονται ευαίσθητα προσωπικά δεδομένα ασθενών, και η πρόσβαση τους από μη εξουσιοδοτημένους χρήστες δημιουργεί σοβαρές επιπτώσεις στο σύστημα. Στα δίκτυα IoMT η χρήση των μηχανισμών φυσικής πρόσβασης μπορεί να θεωρηθεί πιο αποτελεσματικοί, καθώς αναφέρεται σε συστήματα που η πρόσβαση τους απαιτεί την φυσική επαφή των ασθενών. Εφαρμόζουν στο πρώτο και τρίτο επίπεδο.

Στο πρώτο επίπεδο υπάγεται το φυσικό στρώμα (Sensing). Είναι απαραίτητο να αποκτήσουν πρόσβαση μόνον εξουσιοδοτημένες αυθεντικοποιημένες οντότητες στους αισθητήρες. Από το τρίτο επίπεδο γίνεται η αλληλεπίδραση των χρηστών με το

σύστημα. Αιτήματα στέλνονται από και προς τον χρήστη. Κάθε χρήστης έχει συγκεκριμένα δικαιώματα επεξεργασίας και πρόσβασης σε δεδομένα, τα οποία διασφαλίζονται μέσω τεχνικών Ελέγχου Πρόσβασης. Έτσι, με τη χρήση τους μπορεί να διασφαλιστεί η Εμπιστευτικότητα του συστήματος, η Εξουσιοδότηση, ο Έλεγχος πρόσβασης και η Ακεραιότητα των δεδομένων. Από τη μεριά της Ιδιωτικότητας είναι πιθανό η Ανωνυμία των χρηστών να διασφαλιστεί.

Στα συστήματα IoMT ο Έλεγχος Πρόσβασης μπορεί να διεκπεραιωθεί με τη χρήση των βιομετρικών στοιχείων του ασθενούς (Rathore et al., 2017). Με τη χρήση τους η Αυθεντικοποίηση του χρήστη γίνεται με τη ταύτιση των σωματικών του μετρήσεων όπως η ίριδα του ματιού, η φωνή του χρήστη και το δακτυλικό αποτύπωμα και έπειτα χορηγείται στον χρήστη η πρόσβαση στο σύστημα. Έτσι, έννοιες όπως η Εξουσιοδότηση και Αξιοπιστία του συστήματος διασφαλίζονται. Ακολούθως, αποτελεσματική μέθοδος αποτελεί η αυθεντικοποίηση με πολλούς παράγοντες (Multi-factor Authentication). Με τη χρήση των βιομετρικών στοιχείων του ασθενή, ή με εξωτερικές φορητές συσκευές, όπως αναφέρεται παρακάτω, αυξάνεται η ασφάλεια όσον αφορά την αυθεντικοποίηση του χρήστη. Ωστόσο, η χρήση των βιομετρικών στοιχείων μπορεί να εκθέσει τα ευαίσθητα δεδομένα που χρησιμοποιούνται κατά τη διάρκεια μιας πιθανής παραβίασης.

5.1.3.4 Μέτρα Ενίσχυσης της Ασφάλειας στο Κανάλι Επικοινωνίας

Τα σύστημα IoMT βασίζονται στην επικοινωνία τόσο των συσκευών και των αισθητήρων, όσο και της επικοινωνίας των κόμβων του δικτύου στο σύνολο του. Έτσι, είναι αναγκαία η εδραίωση αξιόπιστων οδών επικοινωνίας μεταξύ των κόμβων του δικτύου. Φυσικά, η εδραίωση τους βασίζεται σε τεχνικές κρυπτογράφησης και των πρωτοκόλλων επικοινωνίας, που χρησιμοποιούνται για την ανταλλαγή πληροφοριών μεταξύ των κόμβων.

Οι εφαρμογές του συστήματος, που επεξεργάζονται ζωτικής σημασίας δεδομένα, προτείνεται να απομονωθούν, ιδιαίτερα όταν χρησιμοποιούνται εμπορικές συσκευές - όπως IMDs, Smartphones, Smartwatches, Wristbands κ.ο.κ -, διότι μειώνεται ο κίνδυνος παραβιάσεις από κοινές επιθέσεις που μπορεί να φανούν μοιραίες. Μάλιστα, παρατηρήθηκε ότι με τη συγκεκριμένη πρακτική επωφελείται η εσωτερική Αυθεντικοποίηση και αυξάνεται η Ακεραιότητα του συστήματος (Almohri et al., 2017). Όσον αφορά την Ιδιωτικότητα των χρηστών, με τη διασφάλιση των καναλιών επικοινωνίας δεν επιτρέπεται σε επιτιθέμενες οντότητες να αντιστοιχίσουν τις επικοινωνούντες οντότητες ενισχύοντας τις έννοιες της Ανωνυμίας, Μη-συνδεσιμότητας, Μη-ανιχνευσιμότητας και Μη-παρατηρησιμότητας.

Η πιο διαδεδομένη λύση στα συστήματα IoT για το επίπεδο δικτύου (Network Layer), αποτελεί το πρωτόκολλο TLS/SSL, με το οποίο διασφαλίζεται η επικοινωνία των επικοινωνούντων οντοτήτων. Όμως, η πληθώρα των προτεινόμενων λύσεων εφαρμόζονται στο επίπεδο διεπαφής (Interface Layer). τα πρωτόκολλα έχουν ως στόχο την διασφάλιση του συστήματος, της επικοινωνίας του χρήστη, του χρήστη σαν άτομο και του μετριασμού των trade-offs που προκύπτουν. Ωστόσο, τα προτεινόμενα πρωτόκολλα επικοινωνίας δεν προσφέρουν μέτρα ασφάλειας, τα οποία να καλύπτουν πλήρως τις ανάγκες των συστημάτων IoMT. Έτσι, έγκειται η ανάγκη εφαρμογής μέτρων ασφάλειας, τα οποία μπορεί να επιβαρύνουν το σύστημα στο σύνολο του και να μειώσουν την απόδοσή του (βλ. Κεφάλαιο 4.3).

Η περίπτωση των Εμφυτευμένων συσκευών εγείρει αυστηρότερα μέτρα ασφάλειας,

λόγω της φύσεως των δεδομένων που υπάρχουν και της φυσικής επαφής της συσκευής με το χρήστη. Έτσι, οι Challa et al., 2018 παραθέτουν τέσσερα μοντέλα Αυθεντικοποίησης που χρησιμοποιούνται για τη διασφάλιση της επικοινωνίας τους. Η πρώτη προσέγγιση (Proximity Based) αναφέρεται στην αυθεντικοποίηση των χρηστών με την επαφή τους με τη συσκευή, όπου δημιουργούνται ζητήματα Εμπιστευτικότητας και Ακεραιότητας. Έπειτα, η χρήση εξωτερικών συσκευών (Proxy Based) μπορεί να αποτελέσει ασπίδα προστασίας για τις συσκευές IoMT, προφυλάσσοντας έννοιες όπως η Ακεραιότητα των δεδομένων, η Αυθεντικοποίηση και η Εμπιστευτικότητα, ωστόσο εάν πέσουν θύμα επιθέσεως πλαστοπροσωπίας όπως Masquerade μπορεί να προσκληθούν οι παραπάνω έννοιες, όπως επίσης και η Διαθεσιμότητα των συσκευών. Έπειτα, η χρήση βιομετρικών τεχνικών αυθεντικοποίησης χαρακτηρίζουν μοναδικά τον χρήστη προστατεύοντας τις έννοιες της τριάδας CIA, ωστόσο η υποκλοπή των δεδομένων δημιουργούν ζητήματα Ιδιωτικότητας και Εμπιστευτικότητας στο σύστημα. Τέλος, η υβριδική προσέγγιση (Hybrid Based) προσπαθεί να αφομοιώσει τα ισχυρά χαρακτηριστικά των παραπάνω μεθοδολογιών.

Οι κλασικές προσεγγίσεις για τη διασφάλιση των συστημάτων IoMT φαίνεται να ικανοποιούν ένα σύνολο απαιτήσεων (Κεφάλαιο 4). Έτσι, προσπαθώντας οι σχεδιαστές των συστημάτων ασφάλειας να μετριάσουν τις απειλές που δέχονται οι παραπάνω τεχνικές, τις αφομοιώνουν στα προτεινόμενα μέτρα ασφάλειας με σκοπό την δημιουργία λύσεων που θα είναι όσο το δυνατόν λιγότερο επιρρεπής στα θέματα συμβιβάσιμων των συστημάτων IoMT. Παρακάτω, αναφέρεται η προσπάθεια των ερευνητών να δημιουργήσουν λύσεις που θα ικανοποιούν τις απαιτήσεις των IoMT.

5.2 Προτεινόμενες Λύσεις στα Ζητήματα Ασφάλειας και Ιδιωτικότητας των Συστημάτων IoMT

Στη ενότητα παρακάτω παρατίθενται οι προτεινόμενες από τη βιβλιογραφία state-of-the-art λύσεις ασφάλειας για τα συστήματα IoMT, τα οποία αφομοιώνουν τα παραπάνω μέτρα. Όπως φαίνεται παρακάτω, οι προτάσεις βρίσκονται σε πειραματικό στάδιο έχοντας δοκιμαστεί μόνο σε εργαστηριακό επίπεδο, με αποτέλεσμα να μην είναι γνωστή η δυναμικότητα τους.

Η βιβλιογραφία παρουσιάζεται ελλιπής ως προς την ασφάλεια των συστημάτων IoMT, καθώς αποτελεί γενικά καινούργιος τομέας. Οι προτεινόμενες λύσεις ενώ παρουσιάζουν θετικά δείγματα ως προς την προστασία των συστημάτων IoMT, όπως φαίνεται στο Πίνακα 5.1 υστερούν σε θέματα ασφάλειας, απόδοσης. Η περίπτωση του πρώτου μέτρου διασφαλίζει τη διαμοιραζόμενη πληροφορία ωστόσο έχει υψηλές ενεργειακές απαιτήσεις, ένα θέμα που αντιμετωπίζουν τα συστήματα IoMT (βλ. Κεφάλαιο 3). Το δεύτερο αποτελεί μέτρο ελέγχου για τα συστήματα IoMT, το οποίο προσφέρει μερική ασφάλεια. Τα δύο τελευταία μέτρα δεν προσφέρουν προστασία, αλλά ανάλυση των συστημάτων IoMT με σκοπό την εφαρμογή των πιο ιδανικών μέτρων και των μετριασμό των επικείμενων κινδύνων. Επιπλέον, οι προτεινόμενες λύσεις παρουσιάζονται ελλιπείς, χωρίς να έχουν μια ολοκληρωμένη ανάλυση. Έτσι, έγκειται η ανάγκη δημιουργίας νέων λύσεων που θα καλύψουν τα προβλήματα στην ασφάλεια των συστημάτων IoMT, ικανοποιώντας τη πλειονότητα των απαιτήσεων τους.

Ref.	Μέθοδοι Αντιμετώπισης	Απαιτήσεις	Προκλήσεις
Mahmud et al., 2018	ECC, CGA, Εξωτερικές Συσκευές.	Ακεραιότητα, Αυθεντικότητα, Εμπιστευτικότητα, Διαθεσιμότητα, Ευρωστία	Υψηλές ενεργειακές απαιτήσεις
Celdran et al., 2018	VMD, NFV, SDN, H-IDS, NIDS	Εμπιστευτικότητα, Διαθεσιμότητα, Επείγουσα Αυθεντικοποίηση	Υψηλές ενεργειακές απαιτήσεις, Μείωση της λειτουργικότητας
Mnjama et al., 2017	—	—	—
Islam et al., 2015	IDS, IPS, Dynamic algorithms	—	—

Πίνακας 5.1: Σύνοψη των απαιτήσεων ιδιωτικότητας στα τέσσερα στρώματα επικοινωνίας

Συγκεκριμένα, οι **Mahmud et al., 2018** προτείνουν το SecuPAN, ένα ολοκληρωμένο σχήμα, το οποίο βασίζεται στο πρωτόκολλο Message Authentication Code (MAC). Αναλαμβάνει το διαμοιρασμό της πληροφορίας στο τρίτο επίπεδο παραλαμβάνοντας το από το πρώτο επίπεδο (βλ. Κεφάλαιο 2.2.3) εφαρμόζοντας στο δεύτερο επίπεδο. Στοχεύει στον περιορισμό κατακερματισμένων επιθέσεων, που διεκπεραιώνονται στα δίκτυα, με βάση το πρωτόκολλο 6LoWPAN εφαρμόζοντας στο στρώμα δικτύου (Network Layer). Χρησιμοποιεί για την διασφάλιση των δεδομένων τη τεχνική Cryptographically Generated Address (CGA), μια διεύθυνση έχοντας ένα αναγνωριστικό, που έχει προκύψει από τον υπολογισμό μιας συνάρτησης Hash. Η δημιουργία διαύλων επικοινωνίας διεκπεραιώνεται με ασφάλεια μέσω μιας εξωτερικής συσκευής Joining Device. Για να αποτραπούν επιθέσεις, χρησιμοποιούνται τεχνικές κρυπτογράφησης ECC για τον υπολογισμό της διεύθυνσης CGA-IPv6, τα οποία εγγυώνται την *Ακεραιότητα* και *Αυθεντικότητα* με τη χρήση ενός σχήματος MAC.

Ως αποτέλεσμα, οι συγγραφείς έδειξαν ότι το σχήμα τους, αντιμετωπίζει με επιτυχία πληθώρα επιθέσεων όπως Replay, Spoofing, επίθεση Πλαστοπροσωπίας, Buffer Exhaustion κ.α, ικανοποιώντας την έννοια της Εμπιστευτικότητας. Επιπρόσθετα, κατά τη διάρκεια επιθέσεων, το SecuPAN είναι ικανό να κρατήσει σε χαμηλά επίπεδα τη κατανάλωση ενέργειας, και ταυτόχρονα να συνεχίζει η λειτουργία του δικτύου με χαμηλά επίπεδα καθυστέρησης μεταξύ τελικών κόμβων, ενισχύοντας τις έννοιες της Διαθεσιμότητας και Ευρωστίας. Στα αρνητικά του σχήματος συγκαταλέγονται οι υψηλές απαιτήσεις σε ενεργειακούς πόρους, οι οποίες μπορεί να αποτελέσουν αίτιο για την άρση της Διαθεσιμότητας του δικτύου και την μείωση της λειτουργικότητάς του.

Οι **Celdran et al., 2018** προτείνουν ένα Framework βασισμένο στην τεχνολογία του υπολογιστικού νέφους, το οποίο χρησιμοποιείται ως στρώμα ελέγχου στα συστήματα IoMT. Εφαρμόζει και στα τρία επίπεδα της αρχιτεκτονικής, αναλύοντας τα στρώματα επικοινωνίας για τυχόν παραβατικές συμπεριφορές. Ως νέα προσέγγιση χρησιμοποιεί τεχνικές Virtual Medical Devices (VMD) στα προσωπικά δίκτυα MCPS. Επιπλέον, η προτεινόμενη λύση προσφέρει δυναμισμό στο δίκτυο και χαμηλό latency, ενισχύοντας

την ασφάλεια στα MCPS. Οι λειτουργίες του Framework γίνονται με τη χρήση τεχνικών Network Function Virtualization (NFV) και Software Defined Networks (SDN), όπου ανάλογα με τα ζωτικά χαρακτηριστικά των ασθενών, την τοποθεσία τους, των συσκευών που τους αντιστοιχούν και της επικοινωνίας τους, δημιουργείται ένα σετ από οδηγίες με τις οποίες διαχειρίζονται τα δεδομένα των ασθενών και τις συσκευές τους.

Η αρχιτεκτονική του συστήματος αποτελείται από τέσσερα στρώματα. Στα δύο πρώτα γίνεται η περισυλλογή και ανάλυση των βιομετρικών και δικτυακών δεδομένων, ενώ στα δύο τελευταία γίνεται η ανάλυση τους και οι λήψεις αποφάσεων. Για την ανίχνευση ανωμαλιών στο συνολικό δίκτυο και στο υπολογιστικό σύστημα χρησιμοποιούνται τεχνολογίες όπως Network Intrusion Detection System (NIDS) και Host Intrusion Detection System (HIDS). Έτσι, το σύστημα αναγνωρίζει κλασικές επιθέσεις πλαστοπροσωπίας ή χειραγώγησης MitM, Spoofing, όπως επίσης και επιθέσεις Brute-force, Buffer overflow. Απόρροια των παραπάνω είναι η ενίσχυση των εννοιών της Εμπιστευτικότητας, Διαθεσιμότητας και της Επείγουσας Αυθεντικοποίησης. Επειδή οι συγγραφείς προτείνουν ένα μέτρο ελέγχου, δεν προσφέρεται μέτρα ασφάλειας στο σύστημα IoMT. Απόρροια αυτού είναι η ανάγκη χρήσης επιπρόσθετων μέτρων, τα οποία θα διασφαλίσουν τα δεδομένα που διαμοιράζονται και τον χρήστη. Ταυτόχρονα όμως αυτό σημαίνει την δέσμευση ενεργειακών πόρων ελαττώνοντας την απόδοση και λειτουργικότητα του συστήματος.

Ένα χρήσιμο εργαλείο προτείνεται από τους **Mnjama et al., 2017**, οι οποίοι περιγράφουν την δημιουργία ενός Framework, που μοντελοποιεί και αξιολογεί τις απειλές των συστημάτων IoMT, που προκύπτουν σε θέματα ασφάλειας και ιδιωτικότητας. Η δομή βρίσκεται και στα τρία επίπεδα της προτεινόμενης αρχιτεκτονικής και μελετάει τις απειλές των τεσσάρων στρωμάτων επικοινωνίας. Για να πετύχουν το επιθυμητό αποτέλεσμα, αφομοιώνουν τα βασικά συστατικά της τριάδας CIA και του Microsoft STRIDE Framework. Οπότε, η νέα προτεινόμενη προσέγγιση, είναι απλούστερη και έχει κατεύθυνση προς τις εφαρμογές IoMT. Σκοπός του μοντέλου είναι η καλύτερη κατανόηση των απειλών που δέχονται τα συστήματα από τη μεριά των επιτιθέμενων για την δημιουργία ασφαλέστερων και πιο αποδοτικών μέτρων. Δεν επιφέρει καμία λύση για τα συστήματα IoMT. Στα αρνητικά του προτεινόμενου σχήματος είναι η ανάγκη ενός ειδικού ασφάλειας για τη χρήση και τη κατανόηση των απειλών.

Οι **Islam et al., 2015** προτείνουν ένα μοντέλο ασφαλείας, το οποίο στοχεύει στην ανάλυση των απειλών και την μείωση του ρίσκου στην ασφάλεια των συστημάτων. Επιπλέον, η μελέτη είχε ως σκοπό την πλήρη ανασκόπηση των ζητημάτων ασφαλείας, που προκύπτουν στις εφαρμογές των συστημάτων IoMT. Έτσι, αναγνωρίζοντας τα προβλήματα, το προτεινόμενο μοντέλο συνδυάζει Μηχανισμούς Ανίχνευσης, οι οποίοι στοχεύουν στην έγκαιρη εξουδετέρωση επικείμενων παραβιάσεων, Μηχανισμούς Προστασίας, με σκοπό την ανίχνευση και ελάττωση των επιθέσεων, που μπορεί να δεχθεί το σύστημα, και Μηχανισμούς Αντίδρασης, που αξιοποιούνται για την διατήρηση της Ευρωστίας του συστήματος, αφού έχει παραβιαστεί. Οι συγγραφείς σχεδίασαν τις παραπάνω λειτουργίες με τη χρήση δυναμικών αλγορίθμων, οι οποίοι εκπαιδεύονται από το σύστημα, καθώς ταξιδεύουν μεταξύ των τεσσάρων στρωμάτων επικοινωνίας (Sensing, Network, Service, Interface) με σκοπό την εκπαίδευση των αλγορίθμων για την μεγιστοποίηση της ασφάλειας του συστήματος. Ωστόσο, οι συγγραφείς περιορίζονται στον απλό σχεδιασμό του σχήματος. Δεν επεκτείνονται σε περαιτέρω ανάλυση.

5.3 Ανοιχτά Ερωτήματα και Προκλήσεις στα Συστήματα IoMT.

Είναι κατανοητό ότι οι προτεινόμενες λύσεις δεν είναι σε θέση να καλύψουν όλες τις απαιτήσεις στην ασφάλεια (Challa et al., 2018). Οι συμβιβασμοί μεταξύ των απαιτήσεων (Trade-offs) αποτελούν έναν από τους παράγοντες που ευθύνονται, καθώς οι σχεδιαστές των συστημάτων πρέπει να διακρίνουν τα μέτρα ασφαλείας, στα οποία θα επιτύχουν μεγαλύτερη προσοχή, ενώ ταυτόχρονα θα κρατήσουν σε επιθυμητά επίπεδα την απόδοσή τους. Ο δυναμισμός και η πολυπλοκότητα, που χαρακτηρίζει τα συστήματα IoMT σε συνδυασμό με την φύση τους, ευθύνεται για το σχηματισμό κενών στο σύστημα, αυξάνοντας τις απαιτήσεις σε μέτρα ασφαλείας. Αν και ο αριθμός των προτεινόμενων αρχιτεκτονικών είναι ικανοποιητικός για τα συστήματα IoT, αυτές που επικεντρώνονται στα συστήματα IoMT είναι ελάχιστες. Επιπλέον, υπάρχουν μελέτες, που επικεντρώνονται στα συστήματα EHR, τοποθετώντας τα συστήματα IoMT σε μια γενικότερη κατηγορία δικτύων με ευαίσθητα δεδομένα.

Ωστόσο, η φύση των δικτύων IoMT απαιτεί την δημιουργία εξατομικευμένων τεχνολογιών. Ακόμα και για τις προτεινόμενες λύσεις, δεν υπάρχουν μελέτες, οι οποίες να εξετάζουν σε βάθος τα θέματα ασφαλείας, με αποτέλεσμα να μην γνωστοποιούνται τα κενά τους. Οι σχεδιαστές των συστημάτων είναι πιθανό να μην λαμβάνουν υπόψη τις έννοιες που αναλύονται παρακάτω. Οι μελέτες που εκτελούν Penetration Tests στα προτεινόμενα συστήματα ασφαλείας, γίνονται σε ελεγχόμενο περιβάλλον, όπου τα αποτελέσματα δεν αντικατοπτρίζουν τους πραγματικούς κινδύνους (AlTawy and Youssef, 2016).

Έτσι, όπως φαίνεται στις πρόσφατες μελέτες (Islam et al., 2015; Granjal et al., 2015; Challa et al., 2018), παρακάτω διακρίνονται οι έννοιες που δεν λαμβάνονται υπόψη για την ασφάλεια των συστημάτων IoMT:

1. **Επεκτασιμότητα:** Από τα σημαντικότερα χαρακτηριστικά για τα συστήματα IoMT είναι η ικανότητα του δικτύου να μπορεί να προσθέτει καινούργιες οντότητες. Αυτές μπορεί να είναι το σύνολο αισθητήρων που αντιστοιχούν στο υποδίκτυο ενός υπάρχοντος ή καινούργιου χρήστη. Η έλλειψη Επεκτασιμότητας για τα συστήματα IoMT μπορεί να δημιουργήσει θέματα Διαθεσιμότητας στο σύστημα, καθώς η προσθήκη μεγάλου αριθμού οντοτήτων μπορεί να οδηγήσει στην υπερκατανάλωση ενεργειακών πόρων και τελικά στην καταστολή της λειτουργίας του. Σημαντικός για τα συστήματα IoMT είναι ο συνδυασμός της Επεκτασιμότητας με την Ευρωστία, καθώς η διατήρηση της ομοιόστασης τους κατά τη προσθήκη καινούργιων στοιχείων είναι εξαιρετικά σημαντική για τη λειτουργικότητα τους,
2. **Ασφαλή Δομή:** Η έλλειψη Ασφαλούς Δομής έγκειται και από την ανυπαρξία ενός προτύπου, το οποίο θα ακολουθούν οι σχεδιαστές των συστημάτων IoMT. Έτσι, δημιουργούνται θέματα που προσβάλλουν τις έννοιες της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των συστημάτων IoMT, καθώς υπάρχει χάσμα στην επικοινωνία των συσκευών και των υποδικτύων. Ευθύνη φέρει η ετερογένεια που χαρακτηρίζει τα συστήματα IoMT. Είναι απαραίτητο να βρεθεί τρόπος να επικοινωνούν όλες οι συσκευές με βάση ένα πρότυπο, το οποίο θα προσφέρει ασφάλεια και εγκυρότητα στα δεδομένα και ταυτόχρονα θα διασφαλίζει τους χρήστες και το σύστημα. Στην ουσία, το πρότυπο πρέπει να προσδιορίζει το τρόπο αλληλεπίδρασης των στρωμάτων επικοινωνίας, των συσκευών μεταξύ των επιπέδων της

αρχιτεκτονικής και στη διασύνδεση των κόμβων του δικτύου,

3. **Επείγουσα Αυθεντικοποίηση:** Μοναδικό χαρακτηριστικό των συστημάτων IoMT, δεν λαμβάνεται υπόψη από καμία προτεινόμενη λύση. Πρέπει να δημιουργηθούν μηχανισμοί, οι οποίοι θα είναι σε θέση να αναγνωρίζουν το επείγον περιστατικό από μια επικείμενη παραβατική συμπεριφορά, δηλαδή από μια συμπεριφορά που δεν συνάδει με αυτά του συστήματος. Το ζήτημα της Επείγουσας Αυθεντικοποίησης πρέπει να αντιμετωπιστεί, καθώς συνδέεται άμεσα με την σωματική ακεραιότητα των χρηστών,
4. **Ασφαλή Εδραίωση Επικοινωνίας:** Είναι απαραίτητη για την διασφάλιση των διαμοιραζόμενων πληροφοριών, καθώς είναι επιθυμητό να μην μπορεί μια κακόβουλη οντότητα μέσω επίθεσης Eavesdropping να κερδίσει σε γνώση κατά τη διάρκεια μιας υπηρεσίας. Όπως φαίνεται από την ανάλυση μόνο μια μελέτη λαμβάνει υπόψη το εν λόγω ζήτημα (Mahmud et al., 2018),
5. **Αφάνεια Δεδομένων:** Τα ευαίσθητα προσωπικά δεδομένα των χρηστών βρίσκονται αποθηκευμένα σε κοινόχρηστους αποθηκευτικούς χώρους (Βάσεις Δεδομένων, Υπολογιστικά Νέφη). Ωστόσο, δεν λαμβάνουν υπόψη την διαφάνεια των δεδομένων, που είναι αναγκαία όταν αυτά μεταφέρονται στον κοινόχρηστο χώρο. Στη περίπτωση των συστημάτων IoMT, εξαιτίας της διατήρησης του ιατρικού απορρήτου η Διαφάνεια των δεδομένων, ακολουθεί αντίστροφη λογική, αφού είναι απαραίτητο η ευαίσθητη προσωπική πληροφορία να μείνει κρυφή, εξασφαλίζοντας τις έννοιες της Ιδιωτικότητας (βλ. Κεφάλαιο 3.2),
6. **Μεγάλα Δεδομένα:** Είναι αντιληπτό το μεγάλο μέγεθος των δεδομένων, που παράγονται διαρκώς από τα συστήματα IoMT. Έτσι, μείζον ζήτημα δημιουργείται για τη παροχή μέτρων ασφαλείας, τη διαχείριση και μεταφορά των δεδομένων αυτών, χωρίς να επηρεαστούν τα ζητήματα ασφαλείας που αφορούν τους χρήστες. Η έννοια των Μεγάλων Δεδομένων, μέχρι στιγμής δεν έχει απασχολήσει τους ερευνητές, δημιουργώντας έτσι ένα ερευνητικό χάσμα. Φυσικά, η συσσώρευση των μεγάλων αποθεμάτων δεδομένων που δημιουργείται, μπορεί να δημιουργήσει πρόβλημα Διαλειτουργικότητας, Ευρωστίας και Ιδιωτικότητας (βλ. Κεφάλαιο 3) στο σύστημα, καθώς δεν θα υπάρχουν διαθέσιμη πόροι για να τα επεξεργαστούν,
7. **Ιδιωτικότητα:** Όπως γίνεται αντιληπτό, η έννοια της Ιδιωτικότητας δεν λαμβάνεται υπόψη από τους σχεδιαστές των συστημάτων IoMT. Οι έννοιες της Μη-συνδεσιμότητας, Μη-παρατηρησιμότητας και Μη-ανιχνευσιμότητας δεν ικανοποιούνται από κανένα προτεινόμενο μέτρο. Η διατήρηση του ιατρικού απορρήτου στα συστήματα IoMT, δηλαδή η εξασφάλιση της αφάνειας των χρηστών, της συσχέτισης τους με τα δεδομένα τους, με τις υπηρεσίες και τους πόρους που χρησιμοποιούν.

Συνοψίζοντας, είναι απαραίτητη η δημιουργία ενός καθολικά αποδεκτού προτύπου, το οποίο θα είναι σχεδιασμένο με γνώμονα τις ιδιαιτερότητες των συστημάτων IoMT, ισορροπώντας τα ζητήματα των συμβιβασμών, ικανοποιώντας τη πλειονότητα των απαιτήσεων και δημιουργώντας ένα εξατομικευμένο περιβάλλον στο οποίο η αλληλεπίδραση των συσκευών με τους χρήστες γίνεται με ασφαλή και αποτελεσματικό τρόπο. Ένα πρότυπο, που θα ενισχύει ολοκληρωτικά τα συστήματα IoMT, από τις συσκευές και τους χρήστες μέχρι τις δικτυακές και υπολογιστικές υποδομές του. Όπως αναφέρουν οι Sicari et al., 2015, τα θέματα επεκτασιμότητας που εγείρονται εξαιτίας του μεγάλου αριθμού των διασυνδεδεμένων συσκευών στα δίκτυα IoT, απαιτούν την δημιουργία υποδομών, οι οποίες θα έχουν την ικανότητα να αντιμετωπίζουν τις απειλές της ασφαλείας

σε δυναμικά περιβάλλοντα.

Παρακάτω, οι νέες προσεγγίσεις που μελετώνται, προσεγγίζουν την τεχνολογία Blockchain. Επιλέχθηκε η εν λόγω τεχνολογία, καθώς προσφέρει ένα αποκεντρωμένο και ασφαλή περιβάλλον, χαρακτηριστικά τα οποία πηγάζουν Εκ του Σχεδιασμού. Έτσι, η μελέτη της τεχνολογίας Blockchain, μπορεί να καινούργιες δυνατότητες στα συστήματα, που θα μετριάσουν εξαρχής κάποιους από τους βασικούς παράγοντες ασφάλειας και ταυτόχρονα με τις απαραίτητες προσθήκες να δημιουργήσουν ένα ιδανικό περιβάλλον για τη φιλοξενία αυτών των συστημάτων.

Κεφάλαιο 6

Αποκεντρωμένες Προσεγγίσεις στην Ασφάλεια των Συστημάτων IoMT

Η ταχεία ανάπτυξη της αγοράς IoT και η μεγάλη αύξηση του αριθμού των συσκευών έχει φέρει στο προσκήνιο το θέμα της ασφάλειάς τους, αποτελώντας τα τελευταία χρόνια αντικείμενο των ερευνητών. Ωστόσο, φαίνεται η πλειονότητα των κλασικών προσεγγίσεων πως δεν εξυπηρετεί πλήρως τις ανάγκες των συστημάτων IoT, καθώς έχουν αυξημένες ενεργειακές και αποθηκευτικές απαιτήσεις. Επόμενα, μελετώνται οι state-of-the-art λύσεις, που έχουν ως βάση τη τεχνολογία Blockchain. Η τεχνολογία Blockchain, συγκρότησε ένα καινούργιο ερευνητικό αντικείμενο για την τεχνολογία IoT, η οποία φαίνεται υποσχόμενη στην αντιμετώπιση των προκλήσεων που αντιμετωπίζουν τα συστήματα.

Όπως αναλύεται παρακάτω προτιμήθηκε η μελέτη της τεχνολογίας Blockchain και οι εφαρμογές της στα συστήματα IoMT, καθώς προσφέρει δυναμισμό στην επικοινωνία των συσκευών, αυτονομία και ασφαλή δομή. Ωστόσο, η τεχνολογία Blockchain δεν χρησιμοποιείται ως σύστημα ασφάλειας, αλλά σαν δομή δικτύου. Τα χαρακτηριστικά της επιτρέπουν την διασφάλιση των οντοτήτων της, οπότε παρακάτω εξετάζονται οι εφαρμογές της τεχνολογίας στα συστήματα IoMT. Καθώς οι μελέτες που έχουν πραγματοποιηθεί για τα ιατρικά συστήματα είναι περιορισμένες γίνεται παραπομπή στις εφαρμογές της τεχνολογίας στα συστήματα IoT για την εξαγωγή πλουσιότερων συμπερασμάτων. Έπειτα, διακρίνονται τα προβλήματα ασφάλειας που προκύπτουν στην τεχνολογία Blockchain. Τέλος, παρατίθεται το προτεινόμενο μοντέλο ασφάλειας των συγγραφέων, με αποκεντρωμένο χαρακτήρα.

6.1 Η Τεχνολογία Blockchain και τα Συστήματα IoT

Η τεχνολογία Blockchain πρωτοσυστήθηκε το 2009 με την εμφάνιση του κρυπτονομίσματος Bitcoin, αποτελώντας μια τεχνολογία άμεσης επικοινωνίας δύο οντοτήτων (Peer-to-Peer - P2P), η οποία κρατάει το ιστορικό όλων των συναλλαγών και κινήσεων, που διεκπεραιώθηκαν στο δίκτυο από τους χρήστες (Satoshi Nakamoto, 2008). Πλέον, βρίσκει εφαρμογή σε τομείς όπως οι μεταφορές (Kamath R., 2018), η ιατρική (Ying et al., 2016) και τα κυβερνητικά συστήματα. Η περίπτωση της τεχνολογίας Blockchain εφαρμόζει ιδανικά στα συστήματα IoT, καθώς προσφέρει ένα ασφαλές και αποκεντρωμένο περιβάλλον για την επικοινωνία των συσκευών.

Με τις κρυπτογραφικές τεχνικές Hashing η τεχνολογία Blockchain εγγυάται τη προστασία της τριάδας CIA (Dorri et al., 2017). Έπειτα, η ασύμμετρη κρυπτογραφία που χρησιμοποιείται στη διαδικασία της Ψηφιακής Υπογραφής, κατά την εκτέλεση μιας συναλλαγής από έναν χρήστη, ενισχύει την έννοια της Αυθεντικοποίησης και Ιδιωτικότητας, καθώς μόνον οι Εξουσιοδοτημένες οντότητες για τις οποίες προορίζεται η πληροφορία έχουν πρόσβαση σε αυτή. Έπειτα, επιτρέπει την αλληλεπίδραση P2P, χωρίς την παρέμβαση τρίτης ενδιάμεσης οντότητας, η οποία εγγυάται τη φύση και τη ταυτότητα τους, αφού για να είναι έγκυρη μια συναλλαγή στο σύστημα, πρέπει η πλειονότητα των χρηστών του δικτύου να συμφωνήσουν με τις οδηγίες του Πρωτοκόλλου Συναίνεσης και έπειτα να προστεθεί στην αλυσίδα'.

Η τεχνολογία Blockchain εφαρμόζει στο δεύτερο επίπεδο της προτεινόμενης αρχιτεκτονικής (βλ. Κεφάλαιο 2.2.3), στο οποίο βρίσκονται τα στρώματα δικτύου και διεργασιών (Network, Service) (Πίνακας 2.1). Αναλαμβάνει την ασφαλή διαβίβαση των βιομετρικών δεδομένων από το πρώτο επίπεδο στο τρίτο. Δημιουργεί ευνοϊκές συνθήκες έχοντας Εκ του Σχεδιασμού Ασφάλεια, εξασφαλίζοντας τη τριάδα CIA. Προστατεύεται η έννοια της **Εμπιστευτικότητας**, αφού όλοι οι χρήστες του δικτύου μοιράζονται αντιγράφα των συναλλαγών, ενισχύεται και η Εμπιστευτικότητα των δεδομένων. Επιπλέον, μέσω του Πρωτοκόλλου Συναίνεσης δημιουργείται μια άσπιδά' γύρω από το δίκτυο, αφού κάθε συναλλαγή είναι φανερή στο σύνολο των χρηστών. Η έννοια της **Ακεραιότητας** διασφαλίζεται, καθώς η πληροφορία ταξιδεύει εντός ενός ασφαλούς περιβάλλοντος, κρυπτογραφημένο με τεχνικές δημοσίου κλειδιού. Διατηρείται η **Διαθεσιμότητα** του δικτύου, καθώς το σύστημα δεν εξαρτάται από μια κεντρική οντότητα που τα διαχειρίζεται. Έτσι, επιθέσεις DDoS και Buffer overflow, οι οποίες καταστέλλουν το σύστημα, αντιμετωπίζονται με επιτυχία. Επιπλέον, η διαθεσιμότητα του δικτύου προφυλάσσεται, καθώς μόνον ένας αριθμός συναλλαγών γίνεται αποδεκτός στο σύστημα. Ακολουθώς, η εδραίωση ασφαλών καναλιών επικοινωνίας στα συστήματα IoT ενισχύει τις έννοιες:

- **Αυθεντικότητα:** Με τη χρήση των ψηφιακών υπογραφών κάθε οντότητα χαρακτηρίζει τα δεδομένα του και τη συναλλαγή που θέλει να επικυρώσει,
- **Ακεραιότητα:** Με τη χρήση των τεχνικών hashing. Μια από τις πιο ισχυρές μεθόδους κρυπτογράφησης, ανήκει στις μονόδρομες συναρτήσεις, από τις οποίες είναι ακατόρθωτο να ανακτηθεί πληροφορία από ένα μη-εξουσιοδοτημένο πρόσωπο,
- **Ανωνυμία:** Εντός της αλυσίδας Blockchain οι χρήστες μπορούν να αντιληφθούν την διαδικασία μιας συναλλαγής, χωρίς να ταυτοποιήσουν τις οντότητες. Αυτό συμβαίνει, καθώς στην τεχνολογία Blockchain τα δημόσια κλειδιά των χρηστών παραμένουν στην αφάνεια. Επιπρόσθετα, με τη χρήση των δημόσιων κλειδιών διασφαλίζεται και η έννοια της *Εξουσιοδότησης*, καθώς μόνον ο χρήστης με το αντίστοιχο ιδιωτικό κλειδί μπορεί να έχει πρόσβαση στα απεσταλμένα δεδομένα,
- **Μη-άρνηση και Ευθύνη:** Με την διατήρηση του ιστορικού των συναλλαγών στην αλυσίδα', ικανοποιούνται οι έννοιες της Μη-άρνησης και Ευθύνης, καθώς είναι θεμιτό οι κινήσεις των χρηστών στο σύστημα να μην φαίνονται, ταυτόχρονα όμως είναι αναγκαίο να υπάρχουν αποδεικτικά σε περίπτωση παραβατικής συμπεριφοράς ενός χρήστη.

Επόμενα, στη τεχνολογία Blockchain μπορεί να θεωρηθεί η ύπαρξη ενός άτυπου μηχανισμού Ελέγχου Πρόσβασης, καθώς δεν γίνονται αποδεκτές όλες οι συναλλαγές. Μια συναλλαγή πρέπει να εγκριθεί από τη πλειονότητα του συνόλου των χρηστών για να

περάσει στην αλυσίδα Blockchain. Χαρακτηριστικό παράδειγμα, αποτελεί η περίπτωση ενός επιτιθέμενου, ο οποίος για να μπορέσει να παραβιάσει ένα Blockchain δίκτυο πρέπει να αποκτήσει κατ'ελάχιστο το 51% της συνολικής ισχύς του (Biswas et al., 2016). Εάν γίνεται λόγος για ιδιωτικό δίκτυο Blockchain, τότε υπάρχει κίνδυνος παραβίασης του από Pool-Miners, οντότητες που ανήκουν στις δομές του Blockchain και έχουν τεράστια αποθέματα υπολογιστικής δύναμης (Ahmed et al., 2018). Συνοπτικά, στον πίνακα 6.1 αναγράφονται οι έννοιες που ικανοποιούνται από τη τεχνολογία Blockchain και οι μέθοδοι της τεχνολογίας που το διασφαλίζουν. Φαίνεται ότι ικανοποιεί τις βασικές απαιτήσεις των συστημάτων IoT χωρίς τη χρήση επιπρόσθετων μέτρων.

Έννοιες Ασφάλειας	Μέθοδοι Ενίσχυσης Ασφάλειας
<i>Εμπιστευτικότητα</i>	Πρωτόκολλα Συναίνεσης, τα χαρακτηριστικά της τεχνολογίας Blockchain.
<i>Διαθεσιμότητα, Ευθύνη, Μη-άρνηση</i>	Τα χαρακτηριστικά της τεχνολογίας Blockchain.
<i>Αυθεντικότητα</i>	Με τη χρήση των <i>Ψηφιακών Υπογραφών</i> .
<i>Ακεραιότητα</i>	Με τη χρήση μονόδρομων hashing κρυπτογραφικών τεχνικών.
<i>Ανωνυμία</i>	Με τη χρήση <i>Ασύμμετρης Κρυπτογραφίας</i> και δημόσιων κρυπτογραφικών κλειδιών.
<i>Εξουσιοδότηση</i>	Με τη χρήση Δημόσιων Κλειδιών.

Πίνακας 6.1: Απαιτήσεις Ασφάλειας τις οποίες καλύπτει Εκ του Σχεδιασμού η Τεχνολογία Blockchain.

Τα παραπάνω χαρακτηριστικά, οριοθετούν την έννοια της Ασφαλούς Δομής, η οποία αποτελεί το πρώτο βήμα για τον μετριασμό των συμβιβασμών. Έχοντας Επεκτατική διάθεση δημιουργεί ένα εύφορο περιβάλλον για τις τεχνολογίες IoMT, καθώς είναι άγνωστος ο ρυθμός με τον οποίο ο αριθμός των απαιτούμενων αισθητήρων για έναν χρήστη και ο συνολικός αριθμός των χρηστών του θα αυξηθεί. Αποτέλεσμα αυτού, είναι η χρήση λιγότερων επιπρόσθετων μέτρων ασφάλειας απελευθερώνοντας ένα σημαντικό μέρος των ενεργειακών πόρων. Παρακάτω, αναλύονται οι προτεινόμενες λύσεις στη βιβλιογραφία χρησιμοποιώντας τη τεχνολογία Blockchain για τη διασφάλιση των συστημάτων IoT

Όπως παρατηρείται στον Πίνακα 6.2, τα προτεινόμενα μοντέλα χρησιμοποιούν σύγχρονες μεθόδους για την ενίσχυση της ασφάλειας των συστημάτων. Αναγράφονται οι απαιτήσεις που ενισχύονται στα συστήματα όπως η Μη-Άρνηση, η Αξιοπιστία, η Ευρωστία και η Διαθεσιμότητα (βλ. Κεφάλαιο 4). Φαίνεται, ότι χωρίς τη χρήση περίπλοκων τεχνολογιών όπως αυτά στο Κεφάλαιο 5 αντιμετωπίζονται τα ζητήματα της Επεκτασιμότητας, Ασφαλούς Δομής και Ασφαλών Καναλιών Επικοινωνίας. Η προτεινόμενη βιβλιογραφία παρουσιάζεται ελλιπής για την εξαγωγή ισχυρών συμπερασμάτων, καθώς δεν είναι έντονη η μελέτη της τεχνολογίας Blockchain στα συστήματα IoT ωστόσο, φαίνεται υποσχόμενη για την επίλυση των ζητημάτων ασφάλειας.

Ref.	Μέτρα Ασφάλειας	Απαιτήσεις Ασφάλειας
Yu et al., 2018	<i>RSA, 2/3 multi-signature, IDS (DNK-Means)</i>	<i>Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Αυθεντικότητα, Μη-Άρνηση</i>
Yu et al., 2018	<i>Smart Contracts</i>	<i>Ακεραιότητα, Εμπιστευτικότητα</i>
Banerjee et al., 2018	<i>Self-healing, RIM</i>	<i>Ακεραιότητα, Διαθεσιμότητα, Ευρωστία</i>
Dorri et al., 2017	<i>Περιορισμός συναλλαγών</i>	<i>Ευρωστία</i>

Πίνακας 6.2: Απαιτήσεις Ασφάλειας οι οποίες ικανοποιούνται από τα επιπρόσθετα μέτρα της προτεινόμενης βιβλιογραφίας.

Αρχικά, οι **Yu et al., 2018** προτείνουν ένα σύστημα αλληλεπίδρασης συσκευών IoT με τη χρήση της τεχνολογίας Blockchain, όπου στοχεύει στη δημιουργία ενός μοντέλου εμπιστοσύνης μεταξύ συσκευών-κόμβων. Η λύση που προτείνουν εφαρμόζει στο δεύτερο επίπεδο της προτεινόμενης αρχιτεκτονικής. Χρησιμοποιούν μεθόδους ανίχνευσης ανωμαλιών στο δίκτυο και με την μέθοδο DNK-Means, βαθμολογώντας και φιλτράροντας τους ενεργούς κόμβους. Εφαρμόζουν κρυπτογραφικές τεχνικές RSA και 2/3 Multi-signature για την διατήρηση της Ιδιωτικότητας των χρηστών και της ενίσχυσης της Ασφάλειας της πληροφορίας. Με τη συγκεκριμένη τεχνική ανιχνεύουν τους ανενεργούς κόμβους, αυξάνοντας τη δυσκολία για τους επιτιθέμενους και ταυτόχρονα προστατεύουν αποτελεσματικά την ασφάλεια και την ιδιωτικότητα των συσκευών IoT. Επιπλέον, χρησιμοποιώντας μόνο ενεργούς κόμβους για τη κρυπτογραφική διαδικασία Multi-signature, αντιμετωπίζοντας το ζήτημα της διαχείρισης των περιορισμένων πόρων. Για να επαληθευτεί μια συναλλαγή, τα δεδομένα που μεταδίδονται στον κόμβο-παραλήπτη αποκρυπτογραφούνται και εν συνεχεία επαληθεύεται η ψηφιακή υπογραφή. Έτσι, μέσω της προτεινόμενης μελέτης, η τριάδα CIA καθώς και η Αυθεντικότητα των δεδομένων προστατεύονται, ενώ ικανοποιείται και η ιδιότητα της Μη-Άρνησης. Ωστόσο, η παραπάνω μελέτη πραγματοποιήθηκε σε μη δυναμικό περιβάλλον, οπότε τα αποτελέσματα μπορεί να θεωρηθούν ιδανικά.

Επόμενα, προτείνεται από τους **Yu et al., 2018** το σύστημα TrustChain, όπου μέσω της τεχνολογίας Blockchain και με τη χρήση 'έξυπνων συμβολαίων' (Smart Contracts) κάθε οντότητα μπορεί να κάνει συναλλαγές, οι οποίες καταγράφονται στο δίκτυο Blockchain. Τα 'έξυπνα συμβόλαια' εφαρμόζουν πάνω στη τεχνολογία Blockchain, τα οποία περιγράφουν την συναλλαγή που προορίζεται να εκτελεστεί, διασφαλίζοντας την Αξιοπιστία του συστήματος και την Ακεραιότητα των δεδομένων. Ωστόσο, η φύση τους επιτρέπει την εκτέλεση τους, μόνο στη περίπτωση, που το δίκτυο Blockchain γνωρίζει ότι θα γίνει με επιτυχία. Φυσικά, υπάρχουν αρκετά ανοιχτά ζητήματα που αφήνει η εν λόγω τεχνολογία, από τα οποία διακρίνεται η Ιδιωτικότητα των δεδομένων, ο δυναμικός Έλεγχος Πρόσβασης και ζητήματα Εμπιστοσύνης.

Οι **Banerjee et al., 2018** προτείνουν ένα υλικολογισμικό, βασισμένο στη τεχνολογία Blockchain, με το οποίο εγγυώνται την Ασφάλεια των συσκευών και την Ακεραιότητα των δεδομένων, προσθέτοντας ένα μηχανισμό Ανίχνευσης Ανωμαλιών και εισάγοντας την έννοια της Αυτό-ίασης (Self-Healing) για τα συστήματα, το οποίο επιτυγχάνεται με το πλεονασμό, που υπάρχει στα Blockchain συστήματα. Έτσι, σε περίπτωση παραβίασης του, ανακτάται ο κώδικας του συστήματος από προηγούμενες εκδόσεις, με σκοπό τη διατήρηση της Ευρωστίας και Διαθεσιμότητας του συστήματος.

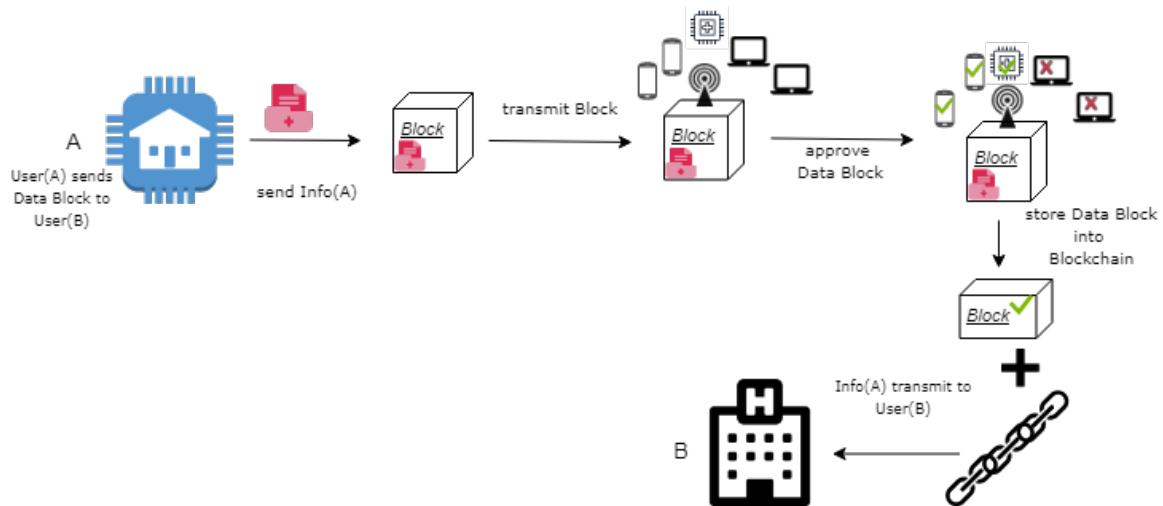
Χρησιμοποιούν την έννοια του Reference Integrity Metric (RIM), με το οποίο εξασφαλίζουν την Ακεραιότητα των δεδομένων του δικτύου Blockchain. Κάθε φορά που ένα χρήστης κατεβάζει το σει δεδομένων, αυτόματα η ακεραιότητα του ελέγχεται από το RIM. Το προτεινόμενο μοντέλο, μπορεί να χαρακτηριστεί ως μερικώς αποκεντρωμένο, καθώς χρησιμοποιεί μια οντότητα-hub, που περιέχει αναφορές για τη τοποθεσία των δεδομένων.

Οι **Dorri et al., 2017** προτείνουν ένα ολοκληρωμένο σύστημα Smart Home βασισμένο στην τεχνολογία Blockchain. Αρχικά, κάθε σπίτι είναι εξοπλισμένο με ένα σύνολο αισθητήρων, μια συσκευή-Miner και έναν χώρο αποθήκευσης δεδομένων σε υπολογιστικό νέφος. Κάθε Smart Home αποτελεί και έναν κόμβο του συνολικού δικτύου. Καθένα λειτουργεί αυτόνομα και αποθηκεύει για αρχή τα δεδομένα τοπικά, χρησιμοποιώντας την τεχνολογία του Blockchain. Κάθε συσκευή μπορεί να επικοινωνεί με άλλες συσκευές του τοπικού ή συνολικού δικτύου. Το χαρακτηριστικό για την αποφυγή κακόβουλων αιτημάτων είναι ο περιορισμός των συναλλαγών που γίνονται αποδεκτά. Έτσι, δείχνουν ότι παρά την υψηλή ενεργειακή ανάγκη, τα συστήματα IoT μπορούν να διαχειριστούν την υπολογιστική επιβάρυνση της τεχνολογίας Blockchain. Οι επιβαρύνσεις που δέχεται το δίκτυο δημιουργούν καθυστερήσεις στην ανταπόκριση. Το συγκεκριμένο χαρακτηριστικό για του γενικού τύπου συστήματα IoT μπορεί να μην δημιουργεί προβλήματα, ωστόσο για τη περίπτωση των IoMT είναι σημαντικό.

6.2 Η Τεχνολογία Blockchain και τα Συστήματα IoMT

Υποθετικά, σε ένα σύστημα Blockchain ο ασθενής (A) θέλει να στείλει τις ημερήσιες σωματικές μετρήσεις του στον θεράποντα γιατρό του (B), ο οποίος βρίσκεται στην νοσοκομειακή μονάδα της περιοχής του. Στη συνέχεια, ο ασθενής από το προσωπικό του δίκτυο προσθέτει στο δίκτυο το πακέτο πληροφορίας (send Info(A)) με τα απαραίτητα βιομετρικά δεδομένα, το οποίο αντιπροσωπεύεται σαν ένα 'Block'. Έπειτα, το 'Block' αναμεταδίδεται (transmit Block) στο σύνολο των χρηστών στο δίκτυο Blockchain. Στη συνέχεια, τη στιγμή που το 'Block' εγκρίθει από τους χρήστες-Miners του δικτύου (approve Data Block), τότε προστίθεται στο δίκτυο Blockchain (store Data Block into Blockchain) και ολοκληρώνεται η συναλλαγή με την αποστολή του πακέτου στον θεράποντα γιατρό (B) (Info(A) transmit to User(B)). Η λογική με την οποία λειτουργεί η τεχνολογία Blockchain ικανοποιεί τη πλειονότητα των απαιτήσεων ασφάλειας στα συστήματα IoMT.

Οι ικανότητες της τεχνολογίας Blockchain πληρούν τις πρωταρχικές απαιτήσεις τους. Οι μελέτες, που έχουν γίνει για τα συστήματα IoT στην υγεία είναι περιορισμένες, καθώς η τεχνολογία των IoT άρχισε να γίνεται ιδιαίτερα διαδεδομένη τα τελευταία χρόνια, πόσο μάλλον η μελέτη των απαιτήσεων που διαθέτουν σε επίπεδο ασφάλειας και ιδιωτικότητας. Παρά την έντονη ερευνητική δραστηριότητα, που έχει δημιουργηθεί για την εφαρμογή της τεχνολογίας Blockchain στα IoT, μικρή είναι ως προς τα συστήματα IoMT. Έτσι, λαμβάνοντας υπόψη τα παραπάνω σε συνδυασμό με την ανάγκη δημιουργίας ενός καθολικού προτύπου για την επικοινωνία των συσκευών (Banerjee et al., 2018), μελετάται ένα καινούργιο ερευνητικό πεδίο, του οποίου επίκεντρο είναι η βέλτιστη εφαρμογή της τεχνολογίας Blockchain στον χώρο των συστημάτων IoMT. Μια τυπική αναπαράσταση της εφαρμογής της τεχνολογίας του Blockchain παρουσιάζεται στο Σχ. 6.1.



Σχήμα 6.1: Τυπική αναπαράσταση της λειτουργίας Blockchain δικτύου στα ιατρικά συστήματα.

Όπως αναλύθηκε, η τεχνολογία Blockchain διαθέτει και το χαρακτηριστικό της Επεκτασιμότητας. Δηλαδή, η ιδιότητα να μπορεί να επεκτείνεται το σύστημα, προσθέτοντας στο δίκτυο της καινούργιους κόμβους. Για τα IoMT είναι θεμιτό, καθώς μπορεί να χρησιμοποιηθούν επιπλέον αισθητήρες από έναν χρήστη, όπως για παράδειγμα ιατροί, ή ακόμα και αισθητήρες που αφορούν το συνολικό δίκτυο. Επιπλέον, περισσότεροι χρήστες είναι πιθανό να προστίθενται ανά καιρούς στο σύστημα. Ωστόσο, το ίδιο χαρακτηριστικό αποτελεί και μια πρόκληση της Blockchain τεχνολογίας, η οποία αναφέρεται παρακάτω.

Όπως είναι διακριτό, υπάρχουν μόνον δύο ολοκληρωμένα μοντέλα που προτείνονται από την βιβλιογραφία. Μπορεί τα μοντέλα να αποδίδουν ιδανικά, εξασφαλίζοντας τη πλειονότητα των απαιτήσεων των συστημάτων IoMT που αναφέρονται στο Κεφάλαιο 4 ωστόσο, δεν είναι αρκετά έγκυρες λόγω του περιορισμένου πλήθους δοκιμών και ερευνητικών εργασιών. Η τεχνολογία Blockchain μπορεί να προσφέρει αρκετά πλεονεκτήματα στα συστήματα IoMT, καθώς εκτός από τις προαναφερόμενες απαιτήσεις ασφαλείας που ικανοποιούνται, χαρακτηρίζεται από:

- Ευρωστία,
- Ευελιξία,
- Επαληθευσιμότητα,
- Μη-συνδεσιμότητα,
- Μη-ανιχνευσιμότητα,

άλλα και από τη δυνατότητα Ανίχνευσης ανώμαλων συγκυριών στο σύστημα. Ωστόσο, υπάρχουν θέματα, που είναι κρίσιμα για τη λειτουργικότητα τους, τα οποία αναλύονται παρακάτω. Όπως αναφέρουν οι Christidis et al., 2016, ο συνδυασμός των συστημάτων IoT με την τεχνολογία Blockchain έχουν τη δυνατότητα να δημιουργήσουν ένα ισχυρό, αυτοματοποιημένο, αλλά κοστοβόρο σύστημα.

Όπως ειπώθηκε, οι μελέτες με ερευνητικό αντικείμενο τη διασφάλιση των συστημάτων IoMT με την τεχνολογία Blockchain είναι ελάχιστες. Παρακάτω, γίνεται η ανάλυση τους, ενώ σε ξεχωριστή ενότητα αναφέρονται οι προκλήσεις που αντιμετωπίζουν τα προτεινόμενα συστήματα.

Συγκεκριμένα, οι **Azaria et al., 2016** προτείνουν το MedRec, ένα σύστημα

διαχείρισης των Ηλεκτρονικών Αρχείων Υγείας, χρησιμοποιώντας την τεχνολογία Blockchain. Κάθε χρήστης έχει ως αντικείμενο τα προσωπικά του δεδομένα τα οποία αποθηκεύονται τοπικά, εκτελώντας τις συναλλαγές στο δίκτυο με τη χρήση των 'έξυπνων συμβολαίων'. Ταυτόχρονα, το δίκτυο Blockchain διαθέτει σύστημα διαχείρισης των δικαιωμάτων, που μπορεί να έχουν οι χρήστες σε κάθε σημείο του δικτύου και στα διαφορετικά δεδομένα. Ως Miners, θέτονται ενδιαφερόμενα μέρη, όπως ασφαλιστικές εταιρείες, νοσοκομεία κ.ο.κ, όπου προσφέροντας την υπολογιστική ισχύ τους για την επαλήθευση των συναλλαγών στο δίκτυο, παίρνουν ως αντάλλαγμα ανώνυμα δεδομένα ή μεταδεδομένα. Εγγυώνται ότι ενισχύεται η τριάδα CIA με την ασύμμετρη κρυπτογραφία, ενώ το σύστημα τους συνολικά προσφέρει μηχανισμούς Ελέγχου Πρόσβασης, Διαλειτουργικότητας και Διαθεσιμότητας. Για την ενίσχυση της Εμπιστευτικότητας, επιτρέπεται σε Αυθεντικοποιημένες οντότητες η περιορισμένη πρόσβαση σε σημεία του συστήματος που οι χρήστες είναι εξουσιοδοτημένοι.

Οι **Ouaddah et al., 2016** προτείνουν το FairAccess, μια δομή Framework ελέγχου πρόσβασης, βασισμένο στη τεχνολογία Blockchain, όπου είναι πλήρως αποκεντρωμένο, ενώ διαθέτει και την ικανότητα διατήρησης της ιδιωτικότητας των χρηστών. Το δίκτυο τους οργανώνεται σε ένα μεγάλο σύστημα Blockchain, το οποίο έπειτα χωρίζεται σε μικρότερα, τοπικά δίκτυα Blockchains για τα οποία κάθε χρήστης ή οργανισμός είναι υπεύθυνος για την διαχείρισή τους. Σε αυτά φιλοξενείται και ένας τοπικός Miner, μια συσκευή Raspberry Pi, η οποία εγκρίνει ή απορρίπτει την προβλεπόμενη συναλλαγή. Κάθε χρήστης είναι ιδιοκτήτης των δεδομένων του, και μπορεί να χορηγήσει τη πρόσβαση τους σε εξουσιοδοτημένες οντότητες του δικτύου, εφόσον το επιθυμεί. Χρησιμοποιούν την λογική του Organisation Based Access Control (OrBAC). Είναι ευέλικτο, με γνώμονα τον χρήστη, ελαφρύ και διαθέτει την ικανότητα της διαλειτουργικότητας μεταξύ των συσκευών και άλλων πρωτοκόλλων. Οι συγγραφείς με το προτεινόμενο μοντέλο, ικανοποιούν τις έννοιες της Επεκτασιμότητας και Διαθεσιμότητας των δικτύων IoMT, την Διαφάνεια των δεδομένων, ενώ είναι από τις προσεγγίσεις που λαμβάνει υπόψη τους όρους της Μη-συνδεσιμότητας και Μη-Ανιχνευσιμότητας.

Τέλος, οι **Karagiannis S. and Magkos E.** αναλύουν πως η τεχνολογία Blockchain μπορεί να ενισχύσει συστήματα, που η διατήρηση της Ιδιωτικότητας των δεδομένων είναι κρίσιμη. Εφαρμόζουν τη προσέγγιση τους στη περίπτωση των Ηλεκτρονικών Φακέλων Υγείας των ασθενών εντός των νοσοκομειακών μονάδων και παρατηρούν ότι οι χρήστες με καθημερινή διάδραση με το σύστημα, επωφελούνται. Έπειτα, με τη προσθήκη μέτρων για τη διατήρηση και ενίσχυση της Ιδιωτικότητας, ικανοποιούνται οι έννοιες της Μη-συνδεσιμότητας, Μη-παρατηρησιμότητας και Μη-ανιχνευσιμότητας. Ωστόσο, τονίζουν ότι με τη προσθήκη μέτρων ασφάλειας στη δομή της τεχνολογίας Blockchain αυξάνεται το latency και overhead του δικτύου. Απόρροια αυτού, είναι η καθυστέρηση της έγκρισης των συναλλαγών, ειδικά όταν γίνεται λόγος για τη περίπτωση των Multichain, όπου προκύπτουν και ζητήματα ιδιωτικότητας.

6.3 Προκλήσεις της Τεχνολογίας Blockchain στα Συστήματα IoMT

Η τεχνολογία Blockchain αν και δημιουργεί εύφορο περιβάλλον για τα συστήματα IoMT, αντιμετωπίζει ζητήματα τα οποία είναι κρίσιμα για την προστασία του συστήματος και των χρηστών. Αρχικά, δημιουργούνται ζητήματα ιδιωτικότητας. Όπως

αναφέρθηκε στο Κεφάλαιο 4.2, πρέπει στα συστήματα IoMT να μη διακρίνονται οι ενέργειες των χρηστών για τη διατήρηση του ιατρικού απορρήτου. Επιπλέον, επειδή η τεχνολογία Blockchain, έχει πάρει μεγάλες διαστάσεις, έχει γίνει αντικείμενο παραβίασης των επιτιθέμενων. Αποτέλεσμα αυτού, είναι η ανακάλυψη πολλών ευπαθειών, αλλά και η διαρκής παραβίαση εμπορικών πλατφορμών που χρησιμοποιούν τη τεχνολογία Blockchain.

Όσο προοδεύουν οι έρευνες στο αντικείμενο των συστημάτων IoMT με τη χρήση της τεχνολογίας Blockchain θα εντοπίζονται καινούργια ζητήματα. Όπως φαίνεται, οι προσεγγίσεις που μελετάνε τις εφαρμογές της Blockchain στα συστήματα IoMT είναι λίγες. Ωστόσο, αντί να προσπαθήσει η ερευνητική κοινότητα να λύσει τα ζητήματα της εφαρμογής της τεχνολογίας Blockchain ή να περιμένει να εξελιχθεί, θα ήταν επιθυμητό να δημιουργηθεί μια νέα προσέγγιση, στα πλαίσια της τεχνολογίας Blockchain, η οποία θα αφομοιώνει τα πλεονεκτήματα της και θα δομείται στις λύσεις, που θα μπορούσαν να εφαρμοστούν σε αυτήν. Χαρακτηριστικά οι Eyal et al., 2016 αναφέρουν τον επανασχεδιασμό της δομής της τεχνολογίας Blockchain, η οποία με τη μέθοδο της αντιμετωπίζει το ζήτημα μεταξύ το μέγεθος των πακέτων που διαμοιράζονται και της ασφάλειας του δικτύου. Έτσι, παρακάτω οι συγγραφείς της Πτυχιακής Εργασίας προτείνουν ένα καινούργιο μέτρο ασφάλειας για τα συστήματα IoMT με αποκεντρωμένο χαρακτήρα, το οποίο θα επιχειρήσει να ικανοποιήσει τις απαιτήσεις σε θέματα Ιδιωτικότητας, Απόδοσης και Επείγουσας αυθεντικοποίησης.

Φυσικά, τα θέματα της τεχνολογίας Blockchain δεν περιορίζονται στις προαναφερθέντες περιπτώσεις. Από την πρόσφατη βιβλιογραφία, φαίνεται ότι προκύπτουν ζητήματα Κατανάλωσης Πόρων και Απόκριση, αφού με την αυξημένη χρήση των πόρων από μέτρα ασφάλειας, μειώνεται η Απόκριση του δικτύου, αυξάνοντας το latency και overhead του δικτύου. Μεταξύ άλλων, οι Zheng et al., 2018, προσθέτουν τα προβλήματα που δημιουργούνται σε επίπεδο Απόδοσης και Ιδιωτικότητας.

- **Διαρροή της Ιδιωτικότητας:** Οι συναλλαγές εντός του Blockchain θεωρούνται ασφαλής, αφού δεν χρησιμοποιούνται πραγματικά στοιχεία, αλλά παραγόμενες διευθύνσεις. Μπορεί να προστατεύονται τα στοιχεία που συναλλάσσονται, ωστόσο δεν εγγυάται την Ιδιωτικότητα τους. Ένας επιτιθέμενος μπορεί να παρακολουθεί με επίθεση Eavesdropping βλέποντας την κίνηση του δικτύου. Έτσι, μπορεί να κερδίσει σε γνώση αντιστοιχώντας τα στοιχεία συναλλαγών με τις οντότητες τους, προσβάλλοντας την έννοια της Ιδιωτικότητας. Σημαντικό πρόβλημα για τα συστήματα IoMT, όπως αναλύθηκε στο Κεφάλαιο 3. Οι λύσεις που προτείνονται είναι αποτελεσματικές, ωστόσο μπορεί να αυξήσουν τις απαιτήσεις σε υπολογιστική ισχύ (Zheng et al., 2018),
- **Απόδοση:** Η δομή της τεχνολογίας Blockchain διαθέτει περιορισμούς, επιτρέποντας την διεκπεραίωση συγκεκριμένου αριθμού συναλλαγών τη φορά, εκπληρώνοντας τις ιατρικές υπηρεσίες με σχετική καθυστέρηση. Το συγκεκριμένο χαρακτηριστικό μπορεί να θεωρηθεί μέτρο ασφάλειας ενάντια σε απειλές κατά της Διαθεσιμότητας (βλ. Κεφάλαιο 3.1.3), ωστόσο τα δίκτυα IoMT, πρέπει να δρουν άμεσα και αποτελεσματικά. Η απόδοση συνδέεται έμμεσα με την ασφάλεια των συστημάτων, καθώς εξαρτώνται οι μηχανισμοί αντίδρασης,
- **Επείγουσα Αυθεντικοποίηση:** Σε συνέχεια της παραπάνω απαίτησης, η τεχνολογία Blockchain δεν υποστηρίζει μηχανισμούς, οι οποίοι θα παραλείψουν τα Πρωτόκολλα Συναίνεσης και θα περάσουν την συναλλαγή στην αλυσίδα. Επιπλέον, δεν έχει προταθεί στην βιβλιογραφία μέτρο το οποίο να αντιμετωπίζει το

ζήτημα των συστημάτων IoMT,

- **Επεκτασιμότητα:** Μπορεί ο χαρακτήρας της τεχνολογίας Blockchain να επιτρέπει την εισαγωγή αισθητήρων στο συνολικό δίκτυο με σχετική άνεση, ωστόσο η ποσότητα πληροφορίας, που κυκλοφορεί σε αυτό είναι μεγάλη, καθώς πρέπει να αποθηκεύονται όλες οι συναλλαγές που διεκπεραιώνονται στο δίκτυο. Έχουν προταθεί λύσεις, οι οποίες να προσπαθούν να αντιμετωπίσουν το εν λόγω ζήτημα, ωστόσο όχι με ικανοποιητικά αποτελέσματα.

6.4 Πρόταση Αποκεντρωμένου Μοντέλου Ασφάλειας για τα Συστήματα IoMT

Η ανάγκη δημιουργίας ενός προτύπου επικοινωνίας για τα συστήματα IoMT οδήγησε στη πρόταση ενός αποκεντρωμένου μοντέλου από τους συγγραφείς. Η τεχνολογία Blockchain δεν χρησιμοποιείται ως σύστημα ασφάλειας, αλλά σαν δομή δικτύου. Λαμβάνοντας υπόψη τις απειλές στην ασφάλειας και ιδιωτικότητας (Κεφάλαιο 3.1, 3.2), η αποκεντρωμένη προσέγγιση χρησιμοποιείται για την ασφαλή δομή που προσφέρει. Το μοντέλο προτείνεται με σκοπό τη διερεύνηση των πιθανών επεκτάσεων της τεχνολογίας Blockchain στα συστήματα IoMT, χωρίς να υπόσχεται την επίλυση των υπαρχόντων προβλημάτων. Εξετάζεται για τη περίπτωση των συστημάτων IoMT, καθώς όπως περιγράφεται η τεχνολογία Blockchain μπορεί να ικανοποιήσει εκ του σχεδιασμού πληθώρα απαιτήσεων (Κεφάλαιο 6.1). Έτσι, στην υποενότητα αναλύεται το προτεινόμενο αποκεντρωμένο μοντέλο για τη διασφάλιση των συστημάτων IoMT. Όπως φάνηκε, οι απαιτήσεις που ικανοποιεί η τεχνολογία Blockchain στα συστήματα IoMT δεν αρκούν (Κεφάλαιο 6.3).

6.4.1 Επισκόπηση Προτεινόμενου Μέτρου

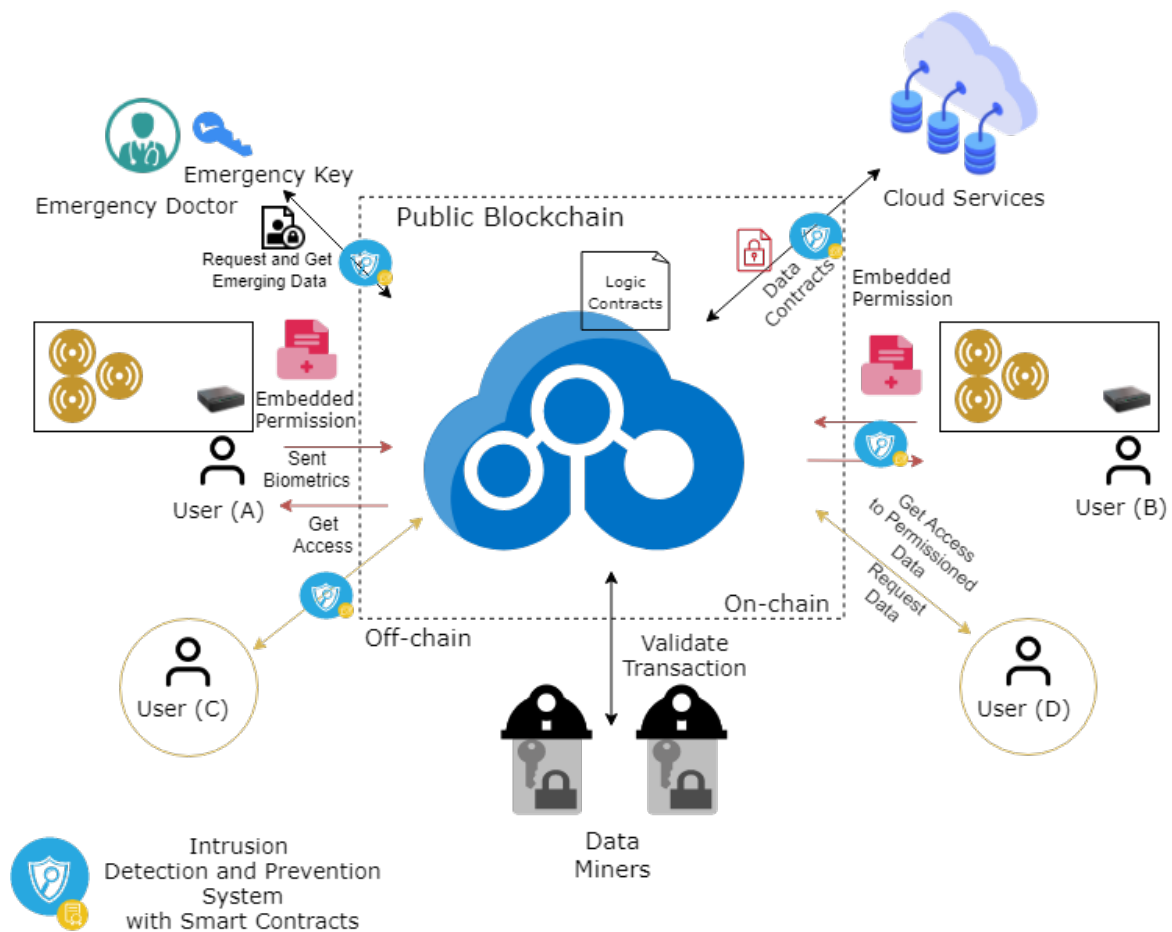
Το προτεινόμενο μοντέλο αποτελείται από τη κεντρική δομή ενός ιδιωτικού Blockchain, με το οποίο επικοινωνούν τα ιδιωτικά δίκτυα των χρηστών. Επιπλέον, επικοινωνεί με το υπολογιστικό νέφος του συστήματος, το οποίο προσφέρει υπολογιστικούς και αποθηκευτικούς πόρους. Οι χρήστες του δικτύου, οι οποίοι είναι αυθεντικοποιημένες οντότητες ανάλογα με την ιδιότητα τους, όπως γιατροί, επαγγελματίες υγείας (User C, D) και ασθενείς (User A, B) έχουν αντίστοιχα δικαιώματα, περιορίζοντας τη πρόσβαση τους σε συγκεκριμένες λειτουργίες του συστήματος. Οι γιατροί έχουν πρόσβαση στα ιατρικά δεδομένα των χρηστών τους, αλλά αυτά είναι περιορισμένα ανάλογα με την ειδικότητά τους. Από την άλλη, οι ασθενείς έχουν δικαιώματα μόνο στα προσωπικά δεδομένα τους.

Με τη παραπάνω οριοθέτηση στο προτεινόμενο μοντέλο δημιουργείται η επιθυμητή τμηματοποίηση του δικτύου (Yu et al., 2018). Αποτελεί μια σημαντική ιδιότητα για τα συστήματα IoMT, καθώς μεγάλος αριθμός των συσκευών βρίσκεται εκτεθειμένος και είναι ευάλωτος σε επιθέσεις. Με την τμηματοποίηση είναι δυνατό να απομονωθεί η κακόβουλη δραστηριότητα σε ένα μέρος του συστήματος, προτού προλάβει να γίνει επικίνδυνη για το συνολικό δίκτυο.

Τα δίκτυα των χρηστών, αποτελούνται από το σύνολο των συσκευών IoMT, οι οποίες λαμβάνουν τα βιομετρικά δεδομένα των χρηστών. Κάθε είδος συσκευής (Φορητές,

Εμφυτευμένες, ΣΑΠ - Κεφάλαιο 2.1) χρησιμοποιείται για τη συλλογή των δεδομένων. Όπως αναλύεται παρακάτω, τα βιομετρικά δεδομένα που μετρώνται από τις συσκευές IoMT συλλέγονται και επεξεργάζονται καταλλήλως από τους προσωπικούς διακομιστές των δικτύων με σκοπό την προετοιμασία και αποστολή τους στο σύστημα Blockchain. Με τη χρήση της τεχνολογίας Blockchain μετριάζονται τα προβλήματα που αντιμετωπίζουν τα κλασικά συστήματα IoMT (Κεφάλαιο 3.1, 3.2, 6.1, 6.2). Με το προτεινόμενο μοντέλο γίνεται προσπάθεια αντιμετώπισης των προκλήσεων που αντιμετωπίζει η τεχνολογία Blockchain στα συστήματα IoMT (Κεφάλαιο 6.3).

Το ιδιωτικό Blockchain επικοινωνεί με Data Miners, οικονομικά ενδιαφερόμενες οντότητες, οι οποίες διαθέτουν μεγάλη υπολογιστική δύναμη με την οποία υπολογίζουν το Πρωτόκολλο Συναίνεσης και εγκρίνουν τις συναλλαγές. Ασφαλιστικές εταιρείες, κρατικές υπηρεσίες, ερευνητικές ομάδες ή νοσοκομειακές μονάδες, που ως αντάλλαγμα δέχονται ανώνυμα δεδομένα (συλλογικά ή στατιστικά) των χρηστών, επιτρέποντας την ενδυνάμωση της Οικονομίας των Δεδομένων. Οι πληροφορίες προωθούνται στο ιδιωτικό Blockchain από τους χρήστες με το μπλοκ πληροφοριών να αποθηκεύεται. Τότε, οι ενδιαφερόμενες οντότητες μπορούν να αποκτήσουν πρόσβαση στην επιθυμητή πληροφορία κάνοντας αίτηση λήψης της. Όπως περιγράφεται παρακάτω, εάν έχουν πληρεξούσιο τότε εγκρίνεται η συναλλαγή και η οντότητα ανακτά την επιθυμητή πληροφορία. Στο Σχ. 6.2 συνοψίζεται η παραπάνω περιγραφή. Χρησιμοποιείται στο προτεινόμενο μέτρο ένα σύνολο παραλλαγών της τεχνολογίας Blockchain (Xu et al., 2018).



Σχήμα 6.2: Αναπαράσταση προτεινόμενου αποκεντρωμένου μοντέλου ασφάλειας για τα συστήματα IoMT

Στην επικοινωνία μεταξύ των χρηστών με το Blockchain χρησιμοποιούνται μπλοκ δεδομένων (Data Block) με ενσωματωμένο Έλεγχο Δικαιωμάτων (Embedded Permission) για να περιορίσουν την πρόσβαση σε μη-εξουσιοδοτημένες οντότητες. Τα μπλοκ δεδομένων μπορεί να περιέχουν ευαίσθητα στοιχεία των χρηστών. Ενώ βρίσκονται εκτεθειμένα στο ιδιωτικό Blockchain, αυθεντικοποιημένοι χρήστες χωρίς άδεια μπορούν να αποκτήσουν πρόσβαση, προσβάλλοντας έτσι την Εμπιστευτικότητα, Ακεραιότητα και Ιδιωτικότητα των δεδομένων. Με τη χρήση του Ελέγχου Δικαιωμάτων, κάθε οντότητα θα μπορεί να κάνει αίτηση για την απόκτηση της πληροφορίας, ωστόσο μόνον οι εξουσιοδοτημένες οντότητες θα ολοκληρώνουν την συναλλαγή, διασφαλίζοντας την τετράδα CIAA. Επιπλέον, αντιμετωπίζεται το πρόβλημα της **Διαρροής Ιδιωτικότητας** (Κεφάλαιο 6.3), καθώς δεν είναι διακριτό ποια υπηρεσία ή δεδομένα απέκτησε ο χρήστης, αφού τα επιλέγει μέσα από ένα μεγάλο σύνολο 'έξυπνων συμβολαίων' που είναι αποθηκευμένα στο ιδιωτικό Blockchain.

Στο σύστημα λειτουργούν τεχνικές Ανίχνευσης και Αντιμετώπισης παραβατικών συμπεριφορών (IDPS). Οι τεχνικές αναλύουν τη συμπεριφορά του χρήστη δημιουργώντας ένα προφίλ για το καθένα, αξιολογώντας και βαθμολογώντας τον. Έτσι, δημιουργείται ένα Μοντέλο Εμπιστοσύνης μεταξύ των κόμβων του δικτύου, πάνω στο οποίο βασίζεται το σύστημα IDPS. Λειτουργούν με βάση τις οδηγίες του Έξυπνου Συμβολαίου (Smart Contract). Έτσι, σε περίπτωση που ανιχνευθεί μια συμπεριφορά για έναν χρήστη που δεν συμμορφώνεται με το προφίλ του ειδοποιεί το σύστημα και πράττει αναλόγως. Φυσικά, οι τεχνικές IDPS ελέγχουν το σύστημα στο σύνολο του, ανιχνεύοντας παραδοσιακές επιθέσεις όπως DoS και Brute-force. Με την διευθέτηση των κλασικών απειλών στα συστήματα IoMT (Κεφάλαιο 3.1, 3.2) ενισχύονται οι έννοιες της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας.

Οι τεχνικές IDPS υιοθετούν την λειτουργικότητα της έννοιας Software Defined Network (SDN). Για το κομμάτι της ανίχνευσης παραβατικών συμπεριφορών, στα κανάλια επικοινωνίας, οι έλεγχοι τοποθετούνται στα κανάλια επικοινωνίας και λειτουργούν όπως αναφέρθηκε παραπάνω. Οι τεχνικές αντιμετώπισης με την ίδια λογική τοποθετούνται στα κανάλια επικοινωνίας με τεχνικές διχοτόμησης του δικτύου (microsegmentation). Έτσι, ανάλογα με τα δικαιώματα που διαθέτει κάθε κόμβος, οι τεχνικές επιτρέπουν ή περιορίζουν τη πρόσβαση σε δεδομένα και υπηρεσίες. Εάν εντοπιστεί κακόβουλη συμπεριφορά που δεν συνάδει με τα δικαιώματα του κόμβου οι μηχανισμοί IDPS αντιδρούν απορρίπτοντας την πρόσβαση και ενημερώνοντας το σύστημα για την παραβατική συμπεριφορά.

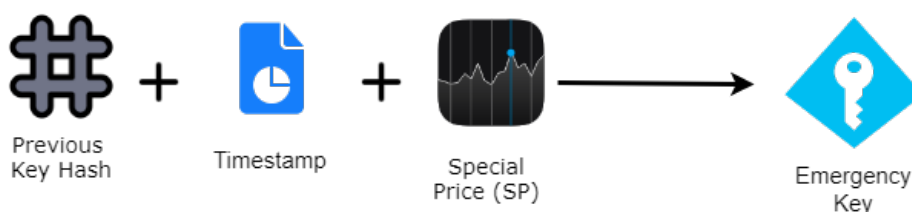
Ζητήματα **Απόδοσης** στη δομή Blockchain προκύπτουν από τη συσσώρευση δεδομένων. Τα μπλοκ δεδομένων (Data Block) στη περίπτωση των συστημάτων IoMT διαθέτουν μεγάλο όγκο βιομετρικών δεδομένων. Έτσι, επιβαρύνεται το σύστημα, μειώνοντας την λειτουργικότητά του. Στο προτεινόμενο μοντέλο, ύστερα από ένα σεβαστό χρονικό διάστημα, κατά το οποίο το σύστημα έχει επιβαρυνθεί τα μπλοκ δεδομένων σπάνε, δημιουργώντας τα Συμβόλαια Δεδομένων (Data Contracts) τα οποία περιέχουν τα βιομετρικά δεδομένα των χρηστών και τα Λογικά Συμβόλαια (Logic Contract) που διαθέτουν τα δεδομένα της συναλλαγής. Και τα δύο συμβόλαια διατηρούν τον ενσωματωμένο δικαίωμα πρόσβασης (Embedded Permission).

Στα συστήματα IoMT ο μεγάλος όγκος των διαμοιραζόμενων μπλοκ δεδομένων (Data Block) δημιουργεί αποθηκευτικά και υπολογιστικά προβλήματα στο Blockchain. Εντός του Blockchain διατηρούνται μόνο τα αρχεία των Λογικών Συμβολαίων (Logic Contract), τα οποία σχηματίζουν την αλυσίδα που διαμοιράζεται στους χρήστες, ελαχιστο-

ποιώντας το μέγεθος των μπλοκ που διατηρούνται εντός της δομής Blockchain.

Έπειτα, με τεχνικές κρυπτογράφησης εντός του Blockchain (On-chain) τα Συμβόλαια Δεδομένων, στέλνονται και αποθηκεύονται εκτός της δομής (Off-chain) στις υπηρεσίες υπολογιστικού νέφους (Cloud Services). Όποτε κρίνεται απαραίτητο χρησιμοποιώντας τους μηχανισμούς ενσωματωμένου ελέγχου οι εξουσιοδοτημένες οντότητες μπορούν να κάνουν αίτηση για να αποκτήσουν πρόσβαση στα βιομετρικά δεδομένα τους. Καθαυτό το τρόπο γίνεται προσπάθεια αντιμετώπισης των ζητημάτων **Επεκτασιμότητας** (Κεφάλαιο 6.3) της τεχνολογίας Blockchain.

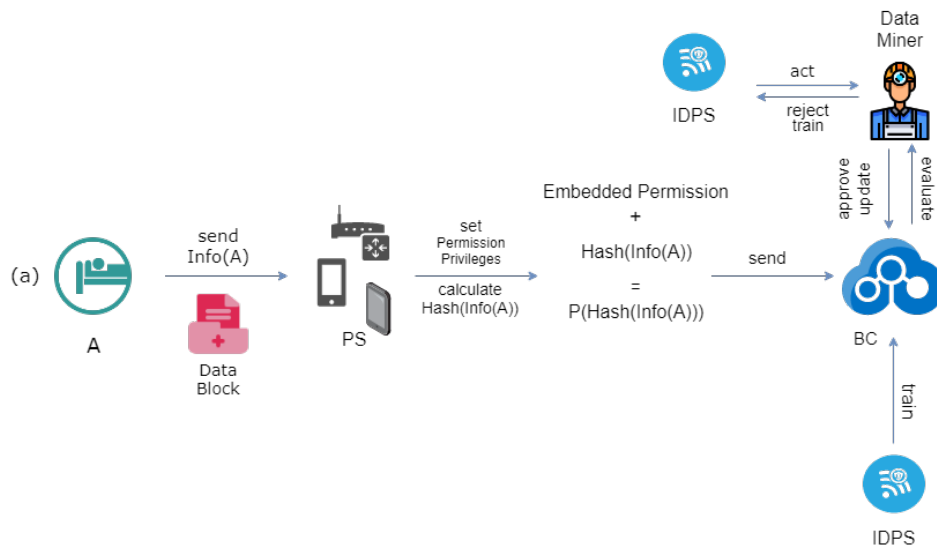
Για τη περίπτωση της **Επείγουσας Αυθεντικοποίησης** (Κεφάλαιο 6.3), χρησιμοποιείται η μέθοδος Πιστοποίησης δύο παραγόντων (2-Factor Authentication), με τη χρήση ενός ειδικού κλειδιού και του δαχτυλικού αποτυπώματος του γιατρού του τμήματος επειγόντων. Ένα διαφορετικό κλειδί χορηγείται στις οντότητες που χαρακτηρίζονται ως επείγοντες γιατροί με το οποίο έχουν άμεση πρόσβαση στα δεδομένα του ασθενούς (Emergency Key). Όπως φαίνεται στο Σχ. 6.3 το κλειδί υπολογίζεται με την τιμή του προηγούμενου κλειδιού (Previous Hash) σε συνδυασμό με έναν αριθμό, ο οποίος έχει πολύ μικρή πιθανότητα να αποκαλυφθεί πριν τον υπολογισμό της (π.χ το ποσοστό μεταβολής του χρηματιστηρίου Αθηνών μια μεταβλητή χρονική στιγμή - SP) και το χρονικό σημείο του υπολογισμού (timestamp). Ταυτόχρονα, με τη χρήση του δαχτυλικού αποτυπώματος γίνεται η ταυτοποίηση του γιατρού μέσω μιας εγγεγραμμένης συσκευής IoMT (π.χ Wristband, Smartphone, Smartwatch), ενισχύονται οι έννοιες της Αυθεντικοποίησης, Ελέγχου Πρόσβασης και Εξουσιοδότησης, Ευθύνης και Μη-άρνησης.



Σχήμα 6.3: Έκδοση επείγοντος κλειδιού.

Όπως προαναφέρθηκε ο κάθε γιατρός έχει δικαίωμα πρόσβασης μόνο στα ιατρικά δεδομένα των ασθενών του. Με τη παραπάνω διαδικασία, οι γιατροί του τμήματος επειγόντων μπορούν να αποκτήσουν πρόσβαση στα δεδομένα κάθε ασθενή που είναι αυθεντικοποιημένος χρήστης. Η τεχνική κρυπτογράφησης Hash διαθέτει υψηλές ενεργειακές απαιτήσεις, δημιουργώντας προβλήματα στην απόκριση του συστήματος. Έτσι, η ανανέωση του επείγοντος κλειδιού γίνεται σε ένα χρονικό διάστημα κατά το οποίο ένας επιτιθέμενος δεν θα μπορεί να το ανακτήσει και ταυτόχρονα θα χρησιμοποιείται με σκοπό τη μεγιστοποίηση της απόδοσης του. Για τη καλύτερη κατανόηση του προτεινόμενου μοντέλου, στα σχήματα που ακολουθούν αναλύεται η μελέτη περίπτωσης διαφορετικών ενεργειών στο σύστημα.

Στο Σχ. 6.4 παρουσιάζεται μία μελέτη περίπτωσης αποστολής μπλοκ δεδομένων από τις συσκευές IoMT του ασθενούς στο σύστημα Blockchain. Συγκεκριμένα ο χρήστης Α ως ασθενής έχει περιορισμένα δικαιώματα στο δίκτυο. Επιτρέπονται μόνο αιτήσεις ανάκτησης των δικών του ευαίσθητων πληροφοριών. Έτσι, ο χρήστης ξεκινάει να στείλει τα βιομετρικά του δεδομένα (σενδ Info(A)) στο σύστημα.

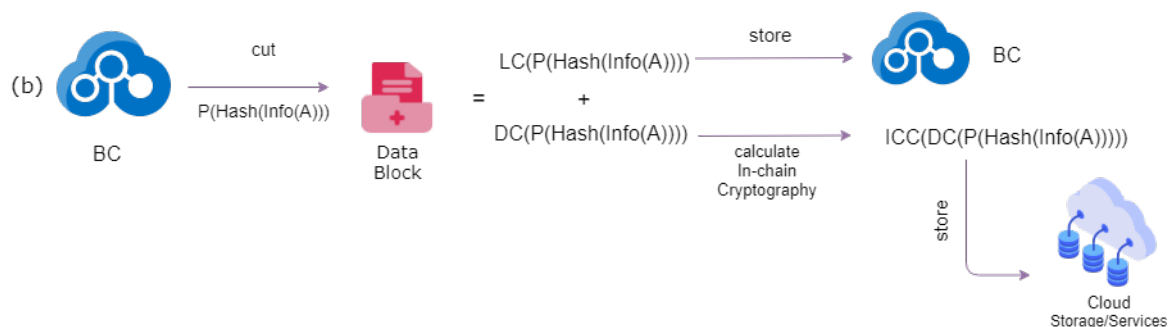


Σχήμα 6.4: Μελέτη περίπτωσης αποστολής μπλοκ δεδομένων από τις συσκευές IoMT ασθενούς στο σύστημα Blockchain

Ο προσωπικός διακομιστής (PS) του χρήστη μπορεί να είναι είτε συσκευές Router είτε συσκευές προσωπικής χρήσης όπως Tablet, Smartphone και Laptop. Προετοιμάζει το μπλοκ δεδομένων με τεχνικές κρυπτογράφησης Hash (calculate Hash(Info(A)) και οριοθετώντας τα δικαιώματα πρόσβασης σε αυτά με τα ενσωματωμένα δικαιώματα πρόσβασης (set Permission Privileges) υπολογίζεται το μπλοκ $P(\text{Hash}(\text{Info}(A)))$, όπου P το δικαίωμα πρόσβασης.

Έπειτα, το μπλοκ προωθείται (send) στο Blockchain, όπου αυτό με τη σειρά του το προωθεί στις οντότητες Data Miners. Αυτές τρέχοντας τα Πρωτόκολλα Συναίνεσης αξιολογούν (evaluate) και εγκρίνουν (approve) την συναλλαγή, με το μπλοκ δεδομένων να προστίθεται στο σύστημα ενημερώνοντας (update) το Blockchain. Σε περίπτωση απόρριψης (reject), η αποστολή των δεδομένων δεν αποθηκεύεται. Οι τεχνικές IDPS ενημερώνονται για την συναλλαγή (update), εκπαιδεύονται (train) και δρουν αναλόγως (act).

Εν συνεχεία στο Σχ. 6.5, αναλύεται η λειτουργία της δομής Blockchain κατά την παραλαβή και αποθήκευση του νέου μπλοκ δεδομένων. Όταν φτάνει το μπλοκ δεδομένων που έχει εγκριθεί ($P(\text{Hash}(\text{Info}(A)))$), αυτό χωρίζεται (cut) με τη χρήση του προτύπου Data Contracts(Xu et al., 2018). Με την διαδικασία αυτή προκύπτουν το Λογικό Συμβόλαιο ($\text{LC}(P(\text{Hash}(\text{Info}(A))))$ και το Συμβόλαιο Δεδομένων ($\text{DC}(P(\text{Hash}(\text{Info}(A))))$).



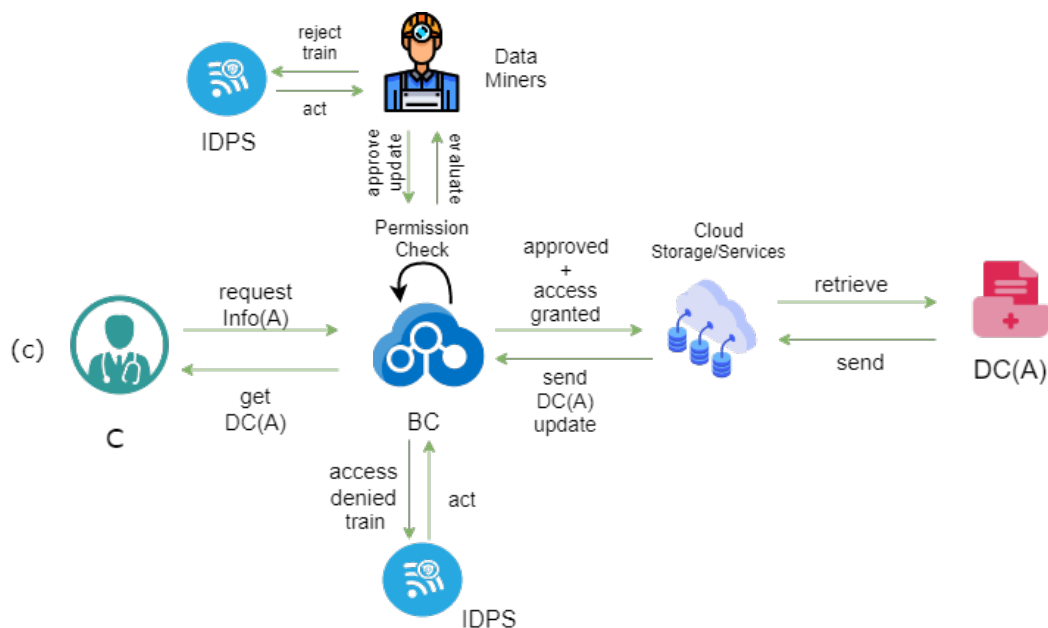
Σχήμα 6.5: Μελέτη περίπτωσης, κατά την αποθήκευση νέου μπλοκ δεδομένων στο σύστημα Blockchain

Το Λογικό Συμβόλαιο που περιέχει τα δεδομένα της συναλλαγής αποθηκεύεται

(store) άμεσα στο Blockchain. Με αυτό το τρόπο μειώνεται σημαντικά το μέγεθος των δεδομένων που διατηρούνται στη δομή Blockchain. Το Συμβόλαιο Δεδομένων διασφαλίζεται με τεχνικές κρυπτογράφησης εντός της δομής Blockchain (calculate In-chain Cryptography) δημιουργώντας ένα το νέο μπλοκ $ICC(DC(P(\text{Hash}(\text{Info}(A))))$, το οποίο προωθείται με ασφάλεια στο υπολογιστικό νέφος (store).

Στο Σχ. 6.6, εξετάζεται η περίπτωση ενός γιατρού χρήστη C, ο οποίος θέλει να αποκτήσει πρόσβαση στα δεδομένα του χρήστη ασθενή A. Στα συστήματα IoMT οι γιατροί έχουν περισσότερα δικαιώματα, καθώς τους επιτρέπεται η πρόσβαση στα προσωπικά δεδομένα των ασθενών τους, διατηρώντας το ιστορικό του καθενός. Ωστόσο, η πρόσβαση περιορίζεται στα δεδομένα που τον αφορούν. Για παράδειγμα, ο οδοντίατρος του χρήστη A δεν μπορεί να έχει δικαίωμα πρόσβασης στις οφθαλμολογικές εξετάσεις του ασθενή του.

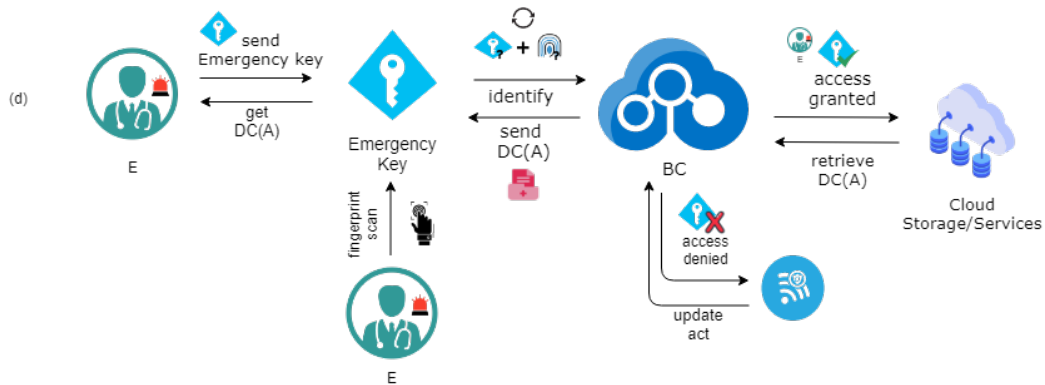
Σε συνέχεια του σχήματος, ο χρήστης C στέλνει το αίτημα (request Info(A)) στο Blockchain για την ανάκτηση του μπλοκ βιομετρικών δεδομένων του ασθενή A. Το Blockchain ελέγχει εάν ο χρήστης C έχει δικαιώματα πρόσβασης στα δεδομένα του χρήστη (Permission Check). Ταυτόχρονα, η συναλλαγή έχει προωθηθεί στις οντότητες Data Miners για την αξιολόγησή της (evaluate). Εφόσον έχει δικαίωμα πρόσβασης και ταυτόχρονα η συναλλαγή έχει εγκριθεί (access granted + approved), τότε το αίτημα προωθείται στο υπολογιστικό νέφος (Cloud Storage/Services), το οποίο ανακτά (retrieve) το Συμβόλαιο Δεδομένων του χρήστη A (DC(A)) και το προωθεί (send) στον χρήστη C με την αντίστροφη διαδικασία (send DC(A), get DC(A)). Το Blockchain ενημερώνεται για την συναλλαγή αποθηκεύοντας την (update). Εφόσον δεν έχει δικαιώματα πρόσβασης (access denied) ή δεν έχει εγκριθεί από τις Data Miners η συναλλαγή, τότε η διαδικασία σταματά στο Blockchain. Για την ολοκλήρωση της διαδικασίας απαιτείται η έγκριση και η αποδοχή της συναλλαγής. Εάν ισχύει μόνο μια περίπτωση τότε η συναλλαγή δεν προχωράει. Σε κάθε περίπτωση, οι τεχνικές IDPS εκπαιδεύονται και δρουν αναλόγως (train, act).



Σχήμα 6.6: Μελέτη περίπτωσης, κατά την οποία ο θεράπωντας γιατρός αποκτά πρόσβαση στα δεδομένα του ασθενούς του.

Τέλος, η παρακάτω λειτουργία αναφέρεται στη περίπτωση που ένας γιατρός

Ε του τμήματος των επειγόντων χρειάζεται τα βιομετρικά δεδομένα ενός ασθενή A, ο οποίος δεν έχει τις αισθήσεις του (Σχ. 6.7). Έτσι, ο γιατρός των επειγόντων στέλνει στο σύστημα το κλειδί (Emergency Key), το οποίο στην αρχή πρέπει το Blockchain να αναγνωρίσει (identify). Εφόσον εξακριβώνεται η ιδιότητα του γιατρού Ε και ταυτοποιείται σαν αυθεντικοποιημένος χρήστης του συστήματος με τη χρήση του δαχτυλικού αποτυπώματος (fingerprint scan), χορηγείται η άδεια πρόσβασης (access granted) και το σύστημα Blockchain στέλνει σήμα προς το υπολογιστικό νέφος (Cloud Storage/Services) με σκοπό την ανάκτηση των δεδομένων του ασθενούς A (retrieve DC(A)). Έπειτα, από το Blockchain προωθείται στον γιατρό Ε (send DC(A), get DC(A)). Στη περίπτωση που δεν επιτραπεί η πρόσβαση (access denied), τα συστήματα IDPS ενημερώνονται και πράττουν αναλόγως (update, act).



Σχήμα 6.7: Μελέτη περίπτωσης κατάστασης επειγόντως περιστατικού.

Συμπερασματικά, το προτεινόμενο μοντέλο δείχνει με τα προβλεπόμενα μέτρα να είναι ικανό να αντιμετωπίσει τα ζητήματα που δημιουργούνται από τη χρήση της τεχνολογίας Blockchain στα συστήματα IoMT. Ωστόσο, ένα σημαντικό ζήτημα είναι ο χρόνος έγκρισης των συναλλαγών από τις οντότητες Miners. Μέχρι πρότινος, τα Πρωτόκολλα Συναίνεσης που χρησιμοποιούνται για την έγκριση των συναλλαγών είναι χρονοβόρα, γεγονός μη αποδεκτό από τα συστήματα IoMT. Έτσι, έγκειται η ανάγκη δημιουργίας ενός Πρωτοκόλλου Συναίνεσης, το οποίο θα εξυπηρετεί τις ανάγκες των συστημάτων IoMT.

Κεφάλαιο 7

Σύνοψη, Προκλήσεις και Ανοιχτά Ζητήματα

7.1 Σύνοψη της Πτυχιακής Εργασίας

Οι συσκευές IoT έρχονται στον χώρο της ιατρικής για να ενισχύσουν την ιατρο-φαρμακευτική περίθαλψη, προσπαθώντας να λύσουν τα χέρια των επαγγελματιών υγείας από ζητήματα ρουτίνας, όπως η αναζήτηση και ενημέρωση του Ηλεκτρονικού Ιατρικού Φακέλου του ασθενούς. Παρά τις διευκολύνσεις η χρήση των συσκευών και συστημάτων IoMT παρουσιάζουν ένα σύνολο αδυναμιών, με τις οποίες έρχονται αντιμέτωποι οι σχεδιαστές των συστημάτων αυτών. Βλέποντας τα κενά που παραμένουν, μελετήθηκαν νέες αποκεντρωμένες προσεγγίσεις με βάση την τεχνολογία Blockchain.

Οι στόχοι των συγγραφέων επιτεύχθηκαν με την μελέτη των τύπων συσκευών IoMT και της αρχιτεκτονικής των δικτύων. Με γνώμονα τα παραπάνω ευρήματά, αναλύθηκαν τα προβλήματα ασφάλειας που αντιμετωπίζουν τα συστήματα IoMT όσον αφορά τις έννοιες της Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας. Έπειτα, αναλύθηκαν οι απαιτήσεις ασφάλειας, οι οποίες προκύπτουν τόσο από τις προκλήσεις του προηγούμενου κεφαλαίου όσο και από τη φύση των συστημάτων IoMT. Έχοντας υπόψη τις προβλεπόμενες απαιτήσεις αναλύθηκαν οι λύσεις που προτείνονται από τη βιβλιογραφία για την ικανοποίηση των απαιτήσεων. Από τη σχετική μελέτη, οι συγγραφείς κατέληξαν στην ανάγκη δημιουργίας ενός καθολικού προτύπου για τα συστήματα IoMT. Για το λόγο αυτό, μελετήθηκαν οι λύσεις με βάση τη τεχνολογία Blockchain, οι οποίες φαίνονται υποσχόμενες λόγω της ασφαλούς δομής τους. Ωστόσο, οι συγγραφείς συμπέραναν ότι δημιουργούνται ζητήματα απόδοσης και ιδιωτικότητας. Έτσι, πρότειναν ένα μοντέλο με βάση τη τεχνολογία Blockchain, το οποίο υπόσχεται να διευθετήσει τα ζητήματα που προκύπτουν και να ενισχύσει την έννοια της Επείγουσας Αυθεντικοποίησης.

Η εργασία απευθύνεται σε νέους ερευνητές, οι οποίοι μελετούν τη περίπτωση εφαρμογής της τεχνολογίας IoT στα ιατρικά συστήματα. Επιπρόσθετα, απευθύνεται σε άτομα, που μελετάνε την εφαρμογή της τεχνολογίας Blockchain στα ιατρικά συστήματα και σε άτομα, τα οποία ψάχνουν να λύσουν τα κενά που υπάρχουν στα συστήματα.

7.2 Ανοιχτά Ζητήματα και Μελλοντικές Επεκτάσεις

Τα ανοιχτά ζητήματα, που αναφέρονται παρακάτω στη Πτυχιακή Εργασία, είναι απόρροια της μελέτης των πηγών της βιβλιογραφίας, που τα αναπτύσσουν λεπτομερώς. Φαίνεται πως η πλειονότητα αυτών σχετίζεται με τις μεγάλες ποσότητες δεδομένων, που παράγονται από τις συσκευές IoT και διαμοιράζονται στα ιατρικά συστήματα. Οι Rathore et al., 2016 αναφέρονται στην εύρεση λειτουργικών, εύχρηστων και ενεργειακά αποδοτικών τεχνικών, που θα λειτουργούν με ακρίβεια σε πραγματικούς χρόνους, με σεβασμό προς την ιδιωτικότητα των χρηστών. Επιπλέον, αναφέρονται στην ανάγκη δημιουργίας μηχανισμών παρακολούθησης του συστήματος για την ανίχνευση παραβιάσεων στο σύστημα.

Οι Islam et al., 2015 την ανάγκη δημιουργίας ενός προτύπου, η ανάλυσή του κόστους ενός συστήματος IoMT, η κινητικότητα η οποία σαν χαρακτηριστικό είναι αναγκαία και οι υπηρεσίες αναλυτικής στους τελικούς κόμβους ή στα τοπικά δίκτυα των συστημάτων. Οι AlTawy and Youssef, 2016 εφιστούν τη προσοχή τους στη δημιουργία συστημάτων ανίχνευσης παραβιάσεων και απειλών στις συσκευές IMD, αλλά και στη μελέτη audit αρχείων για εγκληματολογικούς σκοπούς.

Οι Yu et al., 2018 αναφέρονται στην ανάγκη διευθέτησης των θεμάτων Ιδιωτικότητας των Δεδομένων και στις μεθόδους προστασίας τους από επικείμενες παραβιάσεις, στα ζητήματα εμπιστοσύνης που προκύπτουν, στον δυναμικό έλεγχο πρόσβασης και στη ταυτοποίηση των συσκευών IoT στα συστήματα. Οι Banerjee et al., 2018 αναφέρονται στον τρόπο με τον οποίο η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί βάση για την ασφάλιση των συσκευών IoT. Μια ενδιαφέρουσα προσέγγιση αποτελεί η μορφοποίηση της δομής της τεχνολογίας Blockchain, ώστε να προσφέρει μια αποδοτικότερη ενεργειακά και υπηρεσιακά μέθοδο για τα συστήματα IoMT.

Ένα σημαντικό θέμα έρευνας που προκύπτει είναι πώς μπορεί η τεχνολογία Blockchain να διασφαλίσει τις συσκευές IoT, που βρίσκονται σε δημόσιους και εύκολα προσβάσιμους χώρους. Το πρόβλημα που διέκριναν οι χρήστες στην εφαρμογή της τεχνολογίας Blockchain έγκειται στην έγκριση των συναλλαγών. Κρίνεται απαραίτητη ο σχεδιασμός ενός καινούργιου Πρωτοκόλλου Συναίνεσης για τη περίπτωση των συστημάτων IoMT, καθώς οι προτεινόμενες λύσεις είναι χρονοβόρες, χαρακτηριστικό το οποίο επιβαρύνει τη λειτουργικότητα των συστημάτων.

Κατάλογος Πινάκων

2.1	Αντιστοίχιση των επιπέδων αρχιτεκτονικής με τα στρώματα επικοινωνίας τους τύπους δικτύων και τις IoMT συσκευές.	22
2.2	Βιβλιογραφική ανασκόπηση των τελευταίων ερευνητικών εργασιών, που αναλύουν την αρχιτεκτονική των IoMT συστημάτων.	22
3.1	Συνοπτική παράθεση των απειλών στα συστήματα IoMT με βάση την Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα	32
3.2	Συνοπτική παράθεση των απειλών στα συστήματα IoMT με βάση την Ιδιωτικότητα	35
4.1	Αντιστοίχιση πρωτοκόλλων επικοινωνίας με το επίπεδο και στρώμα εφαρμογής τους σύμφωνα με την αρχιτεκτονική του Σχ 2.9	38
4.2	Σύνοψη των απαιτήσεων ασφάλειας στα τέσσερα στρώματα επικοινωνίας .	42
4.3	Σύνοψη των απαιτήσεων ιδιωτικότητας στα τέσσερα στρώματα επικοινωνίας	45
5.1	Σύνοψη των απαιτήσεων ιδιωτικότητας στα τέσσερα στρώματα επικοινωνίας	58
6.1	Απαιτήσεις Ασφάλειας τις οποίες καλύπτει Εκ του Σχεδιασμού η Τεχνολογία Blockchain.	65
6.2	Απαιτήσεις Ασφάλειας οι οποίες ικανοποιούνται από τα επιπρόσθετα μέτρα της προτεινόμενης βιβλιογραφίας.	66

Κατάλογος Σχημάτων

1.1	Τυπική απεικόνιση των εφαρμογών των Internet of Things (IoT) στις ιατρικές υπηρεσίες. Medical Internet of Things and Big Data in Healthcare - Scientific Figure on ResearchGate. Available from: www.researchgate.net/figure/An-illustration-of-how-this-revolution-in-medicine-will-look-in-a-typical-Internet-of_fig1_306022306	5
2.1	Φορητή IoMT συσκευή. Adapted from ‘The Internet of Things for Health Care - A Comprehensive Survey’, by S. M. R. Islam et al., 2015.	11
2.2	Χαρακτηριστικά παραδείγματα εμφυτευόμενων συσκευών. Adapted from ‘Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications’, by S. Al-Janabi et al., 2017. . .	12
2.3	Χαρακτηριστικό παράδειγμα απομακρυσμένης παρακολούθησης ασθενούς με υπνικά θέματα υγείας. Adapted from ‘Internet of Things for Sleep Quality Monitoring System A Survey’, N. Suratha et al., 2017.	13
2.4	Αναπαράσταση AAL λειτουργιών. Framework for QoS Performance Assessment on Biomedical Wireless Sensor Networks - Scientific Figure on ResearchGate. Available from: www.researchgate.net/figure/BWSN-applied-to-different-healthcare-scenarios-ambient-assisted-living-AAL-emergence_fig1_230580519	14
2.5	Η τυπική ροή των δεδομένων σε ένα σύστημα IoMT με τις αλληλεπιδράσεις των συστατικών του.	14
2.6	Αρχιτεκτονική στρωμάτων επικοινωνίας στις συσκευές IoMT. Biometric Security and Internet of Things(IoT) - Scientific Figure on ResearchGate. Available from: www.researchgate.net/figure/IoT-architecture-a-3-layer-b-4-layer-c-5-layer-and-d-SOA-based-5_fig1_328516514 [accessed 23 Jun, 2019]	15
2.7	Τύποι κόμβων και η μεταξύ τους συσχέτιση.	17
2.8	Κατανομή των διαφορετικών τύπων δικτύων που συμμετέχουν στα IoMT συστήματα.	18
2.9	Τυπική αναπαράσταση ενός IoMT συστήματος τριών επιπέδων.	19
3.1	Παραδείγματα επιθέσεων στα μοντέλο επικοινωνίας 4 στρωμάτων σε σχέση με τη τριάδα CIA. Adapted from ‘On threat modeling and mitigation of medical cyber-physical systems’, by H. Almohri et al., 2017.	28
4.1	Πρωτόκολλα επικοινωνίας των IoT. Adapted from ‘Choice of Effective Messaging Protocols - for IoT Systems MQTT, CoAP, AMQP and HTTP’, (by Nitin Naik, 2017.)	38
4.2	Το σύνολο των εννοιών που αντικρούονται στα συστήματα IoMT.	47

5.1 Διαχωρισμός των μέτρων ασφάλειας ανάλογα με το στάδιο εφαρμογής. .	50
5.2 Ανάλυση απόδοσης μεθοδολογιών ανίχνευσης επιθέσεων με βάση των Μηχανική Μάθηση.	52
6.1 Τυπική αναπαράσταση της λειτουργίας Blockchain δικτύου στα ιατρικά συστήματα.	68
6.2 Αναπαράσταση προτεινόμενου αποκεντρωμένου μοντέλου ασφάλειας για τα συστήματα IoMT	72
6.3 Έκδοση επείγοντος κλειδιού.	74
6.4 Μελέτη περίπτωσης αποστολής μπλοκ δεδομένων από τις συσκευές IoMT ασθενούς στο σύστημα Blockchain	75
6.5 Μελέτη περίπτωσης, κατά την αποθήκευση νέου μπλοκ δεδομένων στο σύστημα Blockchain	75
6.6 Μελέτη περίπτωσης, κατά την οποία ο θεράπωντας γιατρός αποκτά πρόσβαση στα δεδομένα του ασθενούς του.	76
6.7 Μελέτη περίπτωσης κατάστασης επειγόντως περιστατικού.	77

Βιβλιογραφία

- [1] Aafaf Ouaddah, Anas Abou Elkalam, Abdellah Ait Ouahman. FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Wiley Online Library, Security and Communication Networks* 9 (18) 5943-5964, 2016, 2016.
- [2] Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, Gregorio Martínez Pérez. Sustainable securing of Medical Cyber-Physical Systems for the healthcare of the future. *Elsevier*, 2018.
- [3] Ali Alzahrani, Abdullah Alqhtani, Haytham Elmiligi, Fayeze Gebali, Mohamed S. Yasein. NFC Security Analysis and Vulnerabilities in Healthcare Applications. *IEEE*, 2013.
- [4] Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. *IEEE*, 2017.
- [5] Amjad Gawanmeh, Ahmad Alomari. Taxonomy Analysis of Security Aspects in Cyber Physical Applications. *IEEE*, 2018.
- [6] Angel Perles, Eva Perez-Marin, Ricardo Mercado, J. Damian Segrelles, Ignacio Blanquer, Manuel Zarzo, Fernando J. Garcia-Diego. An energy-efficient internet of things (IoT) architecture for preventive conservation of cultural heritage. *Elsevier, Future Generation Computer Systems*, 2018.
- [7] Angela M. Lonzetta, Peter Cope, Joseph Campbell, Bassam J. Mohd, Thaier Hayajneh. Security Vulnerabilities in Bluetooth Technology as Used in IoT. *Journal of Sensor and Actuator Networks*, 2019.
- [8] Anup Burange, Harshal Misalkar, Umesh Nikam. Security in MQTT and CoAP Protocols of IOT's Application Layer. *Springer Nature Singapore Pte Ltd.*, 2018.
- [9] Ariel Ekblaw, Asaph Azaria, John D. Halamka, MD, Andrew Lippman. A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. *IEEE*, 2016.
- [10] Arijit Ukil, Soma Bandyopadhyay, Chetenya Puri, Arpan Pal. IoT Healthcare Analytics: The Importance of Anomaly Detection. *IEEE*, 2016.
- [11] Arsalan Mnajma, Noraj K. Jha. A Comprehensive Study of Security of Internet-of-Things. *IEEE*, 2017.
- [12] Arthur Gatouillat, Youakim Badr, Bertard Massot, Ervin Sejdic. Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine. *IEEE Internet of Things Journal*, 2018.
- [13] Axel Wirth. Cybercrimes Pose Growing Threat to Medical Devices. *Biomedical instrumentation and technology*, 2016.

- [14] Ayten Ozge Akmandor, Hongxu Yin, Niraj K. Jha. Smart, Secure, yet Energy-efficient, Internet-of-Things Sensor. *IEEE Transactions on Multi-Scale Computing Systems*, 2018.
- [15] Azaph Azaria, Ariel Ekblaw, Thiago Vieira, Andrew Lippman. MedRec: Using Blockchain for Medical Data Access and Permission Management. *IEEE*, 2016.
- [16] Bin Yu, Jarod Wright, Surya Nepal, Liming Zhu, Joseph Liu, Rajiv Ranjan. TrustChain: Establishing Trust in the IoT-based Applications Ecosystem Using Blockchain. *IEEE Cloud Computing*, 2018.
- [17] Bruno Bogaz Zarpelao, Rodrigo Sanches Miani, Claudio Toshio Kawakani, Sean Carlisto de Alvarenga. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 2019.
- [18] C. S. Krishna, T. Sasikala. Healthcare Monitoring System Based on IoT Using AMQP Protocol. *Springer Natuer Singapore Pte Ltd.*, 2019.
- [19] Chen Ying, Elenee Argentinis JD, Griff Weber. IBM WatsonL How Cognitive Computing Can Be Applied to Big Data Challenges in Life Sxiences Research. *Elvsier, Clinical therapeutics 38 (4)*, 688-701, 2016.
- [20] Daojing He, Ran Ye, Sammy Chan, Mohsen Guizani, Yanping Xu. Privacy in the Internet of Things for Smart Healthcare. *IEEE Communications Magazine*, 2018.
- [21] Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, Chi Yang. The Blockchain as a Decentralized Security Framework. *IEEE Consumer Electronics Magazine 7 (2)*, 18-21, 2018.
- [22] Elli Kartsakli, Aris S. Lalos, Angelos Antonopoulos, Stefano Tennina, Marco Di Renzo, Luis Alonso. End-to-End Communication Challenges in M2M Systems for mHealth Applications. *MDPI*, 2014.
- [23] Eyal Ronen, Colin O'Flynn, Adi Shamir, Achi-Or Weingarten. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. *IEEE*, 2017.
- [24] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi. Internet of Things Security: A Survey. *Journal of Network and Computer Applications*, 2017.
- [25] Faisal Alsubaei, Sajjan Shiva, Abdullah Abuhussein. Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. *IEEE 42nd Conference on Local Computer Networks Workshops*, 2017.
- [26] Fangyu Li, Yang Shi, Aditya Shinde, Jin Ye, WenZhan Song. Enhanced Cyber-Physical Security in Internet of Things through Energy Auditing. *IEEE*, 2019.
- [27] Frantz Cadet, Daniel T. Fokum. Coping with Denial-of-Service Attacks on the IP Telephony System. *IEEE*, 2016.
- [28] Gauri Kalnoor, Jayashree Agarkhed. Pattern Matching Intrusion Detection Technique Wireless Sensor Networks. *IEEE (AEEICB16)*, 2016.
- [29] Guanglou Zheng, Rajan Shankaran, Mehmet A. Orgun, Li Qiao, Kashif Saleem. Idead and Challenges for Securing Wireless Implantable Medical Devices: A Review. *IEEE Sensor Journal*, 2017.
- [30] Gulraiz J. Joyia, Rao M. Liaqat, Aftab Farooq, Saad Rejman. Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare

- Domain. *Journal of Communications* Vol. 12, No. 4, 2017.
- [31] Heena Rathore, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Mohsen Guizani. A Review of Security Challenges, Attacks and Resolutions for Wireless Medical Devices. *IEEE*, 2018.
 - [32] Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu. Security in Internet of Things: A Review. *IEEE*, 2012.
 - [33] Ioannis Andrea, Chrysostomos Chrysostomou, George Hadjichristofi. Internet of Things: Security Vulnerabilities and Challenges. *IEEE Symposium on Computers and Communication (ISCC)*, 180-187, 2015.
 - [34] Iuon-Chang Lin, Tzu-Chun Liao. A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, 2017.
 - [35] Jairo Giraldo, Esha Sarkar, Alvaro A. Cardenas, Michail Maniatakos, Murat Kantarcioglu. Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE*, 2017.
 - [36] Javan Mnjama, Greg Foster, Barry Irwin. A Privacy and Security Threat Assessment Framework for Consumer Health Wearables. *IEEE*, 2017.
 - [37] Jorge Granjal, Edmundo Monteiro, Jorge Sa Siva. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communication Surveys and Tutorials*, 2015.
 - [38] Kai Fan, Wei Jiang, Hui Li, Yintang Yang. Lightweight RFID Protocol for Medical Privacy Protection in IoT. *IEEE*, 2017.
 - [39] Kamanashis Biswas, Vallipuram Muthukkumarasamy. Security Smart Cities Using Blockchain Technology. *IEEE*, 2016.
 - [40] Kejun Chen, Shual Zhang, Yi Zhang, Qingxu Deng, Sandip Ray, Yier Jin. Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *Springer International Publishing AG*, 2017.
 - [41] Konstantinos Christidis, Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. *IEEE*, 2016.
 - [42] Kuan Zhang, Kan Yang, Xuemin (Sherman) Shen, Xiaohui Liang, Zhou Su, Henry H. Luo. Security and Privacy for Mobile Healthcare Networks: From a Quality of Protection Perspective. *IEEE Wireless Communications*, 2015.
 - [43] Laurie Pycroft, Tipu Z. Aziz. Security of implantable medical devices with wireless connections: The danger of cyber attacks. *Expert Review of Medical Devices*, 15:6, 403-406, DOI: 10.1080/17434440.2018.1383235, 2018.
 - [44] Longfei Wu, Xiaojiang Du, Mohsen Guizani, Amr Mohamed. Access Control Schemes for Implantable Medical Devices: A Survey. *IEEE Internet of Things Journal*, 2017.
 - [45] Mahmud Hossain, Yasser Jarim, Ragib Hasan. SecuPAN: A Security Scheme to Mitigate Fragmentation-Based Network Attacks in 6LoWPAN. *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, 307-318, 2018.
 - [46] Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo. A blockchain future for internet of things security: a position paper. *(DCN) Digital Communications and Networks*, 2018.

- [47] Mauro Conti, Ali Dehghantanha, Katrin Franke, Steve Watson. Internet of Things security and forensics: Challenges and opportunities. *Elsevier, Future Generation Computer Systems*, 2018.
- [48] Mehrnoosh Monshizadeh, Vikramajeet Khatri, Raimo Kantola. Detection as a Service: An SDN Application. *ICACT2017*, 2017.
- [49] Mei Yu, Jie Zhang, Jianrong Wang, Jie Gao, Tianyi Xu, Rui Deng, Yan Zhang, Ruiguo Yu. Internet of Things security and privacy-preserving method through node differentiation, concrete cluster centers, multi-signature, and blockchain. *International Journal of Distributed Sensor Networks*, 2018.
- [50] Minhaj Ahmad Khan, Khaled Salah. IoT Security: Review, blockchain solutions, and open challenges. *Elsevier Future Generation Computer Systems*, 2018.
- [51] Mohammad A. Salajudding, Ala Al-Fuqaha, Mohsen Guizani, Khaled Shuaib, Farag Sallabi. Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare. *IEEE Computer Magazine*, 2018.
- [52] Mohiuddin Ahmed, Jinpeng Wei, Yongge Wang, Ehab Al-Shaer. A Poising Attack Against Cryptocurrency Mining Pools. *Springer, Nature Switzerland AG*, 2018.
- [53] Montbel Thibaud, Huihui Chi, Wei Zhou, Selwyn Piramuthu. Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review. *Elsevier Decision Support Systems*, 2018.
- [54] Nico Suratha, Gede Putra Kusuma, Sani M. Isa. Internet of Things for Sleep Quality Monitoring System: A Survey. *IEEE*, 2016.
- [55] Nilanjan Dey, Amira S. Ashour, Fuqian Shi, Simon James Fong, Joao Manuel R. S. Tavares,. Medical cyber-physical systems: A survey. *Journal of Medical Systems*, 2017.
- [56] Nilanjan Dey, Amira S. Ashour, Fuqian Shi, Simon James Fong, Joao Manuel R.S. Tavares. Medical cyber-physical systems: A survey. *Journal of Medical Systems*, 2018.
- [57] Nimra Dilawar, Muhammad Rizwan, Fahad Ahmad, Saima Akram. Blockchain: Securing Internet of Medical Things (IoMT). *(IJACSCMA) International Journal of Advanced Computer Science and Applications*, 2019.
- [58] Nitin Naik. Choice of Effective Messaging Protocols for IoT SystemsL MQTT, CoAP, AMQP and HTTP. *IEEE*, 2017.
- [59] Olga Boric-Lubecke, Xiaomeng Gao, Ehsan Yavari, Mehran Baboli, Aditya Singh, Victor M. Lubecke. E-healthcare: Remote Monitoring, Privacy and Security. *IEEE*, 2014.
- [60] Ovunc Kocabas, Tolga Soyata, Mehmet K. Aktas. Emerging Security Mechanisms for Medical Cyber Physical Systems. *IEEE*, 2016.
- [61] Pavan Pongle, Gurunath Chavan. A survey: Attacks on RPL and 6LoWPAN in IoT. *IEEE*, 2015.
- [62] Raja Jain, Dev Kumar Chaudhary, Sanjiv Kumar. Analysis of Vulnerabilities in Radio Frequency Identification (RFID) Systems. *IEEE*, 2018.
- [63] Rayman Preet Singh, Benjamin Cassell, S. Keshav, Tim Brecht. TussleOS: Managing Privacy Versus Functionality Trade-Offs on IoT Devices. *ACM SIGCOMM Computer Communication Review Volume 46 Issue 3*, 2018.

- [64] Riham AlTawy and M. Youssef. Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. *IEEE Access*, 2016.
- [65] Rodrigo Roman, Jianying Zhou, Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. *Elsevier Computer Networks*, 2013.
- [66] Rohit Goyal, Nicola Dragoni, Angelo Spognardi. Mind The Tracker You Wear - A Security Analysis Of Your Wearable Health Trackers. *SAC '16 Proceedings of the 31st Annual ACM Symposium on Applied Computing*, 131-136, 2016.
- [67] S. M. Riazul Islam, Daehan Kwak, MD. Jumaun Kabir, Mahmud Hossain, Kyung-Sup Kwak. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE*, 2015.
- [68] S. Noimanee, K. Noimanee, S. Krisanachinda, W, Senavongse. Study of Cybercrime and Security in Medical Devices. *IEEE*, 2016.
- [69] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini. Security, privacy and trust in Internet of Things: The road ahead. *Elsevier Computer Networks*, 2015.
- [70] Samaher Al-Janabi, Ibrahim Al-Shourbaji, Mohammad Shojafar, Shahaboddin Shamshirband. Survey of Main Challenges (Security and Privacy) in Wireless Body Area Networks for Healthcare Applications. *Egyptian Informatics Journal*, 2017.
- [71] Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith. Wireless Body Area Network: A Survey. *IEEE*, 2014.
- [72] Samir V. Zanjali, Girish R. Tamlale. Medicine Reminder and Monitoring Systems for Secure Health Using IoT. *Elsevier Procedia Computer Science* 78 471-476, 2016.
- [73] Sandeep Pirbhulal, Oluwarotimi Williams Samuel, Wanqing Wu, Arun Kumar Sangaiah, Guanglin Li. A joint resource-aware and medical data security framework for wearable healthcare systems. *Elsevier, Future Generation Computer Systems*, 2019.
- [74] Sonal, SRN Reddy, Dinesh Kumar. Review of Smart Health Monitoring Approaches with Survey Analysis and Proposed Framework. *IEEE*, 2018.
- [75] Sravani Challa, Mohammad Wazid, Ashok Kumar Das, and Muhammad Khuram Khan. Authentication Protocols for Implantable Medical Devices. *IEEE Consumer Electronics Magazine*, 2018.
- [76] Stelios Karagiannis, Emmanouil Magkos. Decentralized Internet Privacy: Towards a Blockchain Framework for Healthcare. *MCIS*, 2017.
- [77] Syagnik (Sy) Banerjee, Thomas Hemphill and Phil Longstreet. Wearable devices and healthcare: Data sharing and privacy. *The Information Society - An International Journal*, 2016.
- [78] Tetsuya Yokotani, Yuya Sasaki. Comparison with HTTP and MQTT on Required Network Resources for IoT. *IEEE*, 2016.
- [79] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, Chenren Xu, . Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things. *Proceedings of the 14th ACM workshop on Hot Topics in Networks*, 5, 2015.

- [80] Wen Yao, Chao-Hsien Chu, Zang Li. The Adoption and Implementation of RFID Technologies in Healthcare: A Literature Review. *Springer*, 2011.
- [81] Xiaohua Feng, Babatunde Onafeso, Enjie Liu. Investigatin Big Data Security Issues with Raspberry Pi. *IEEE*, 2015.
- [82] Xiwei Xu, Cesare Pautasso, Liming Zhu, Qinghua Lu, Ingo Weber. A Pattern Collection for Blockchain-based Applications. *ACM*, 2018.
- [83] Xueqi Fan, Fransisca Susan, William Long, Shangyan Li. Security Analysis of Zigbee. *MIT. edu*, 2017.
- [84] Yassine Chahid, Mohamed Benabdellah, Abdelmalek Azizi. Internet of Things Protocols: Comparison, Architecture, Vulnerabilities and Security: State of the art. *ACM, ICCWCS*, 2017.
- [85] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Hsu, Chong-Kuan Chen, Shiu-hpyng Shieh, . IoT Security: Ongoing Challenges and Research Opportunities. *IEEE*, 2017.
- [86] Zhifeng Xiao, Yang Xiao. Security and Privacy in Cloud Computing. *IEEE*, 2013.
- [87] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang. Blockchain challenges and opportunitites: a survey. *International Journal of Web and Gried Services*, 2018.

Περιεχόμενα

1	Εισαγωγή	4
1.1	Τελευταίες Έρευνες	6
1.2	Μεθοδολογία	7
1.3	Στόχοι	8
1.4	Συνεισφορά	8
1.5	Ενδεικτική Δομή	9
2	Η Τύποι Συσκευών και η Αρχιτεκτονική των Συστημάτων IoMT	10
2.1	Τύποι Συσκευών στα Συστήματα IoMT	10
2.1.1	Συστήματα Υποβοηθούμενης Διαβίωσης - Ambient Assisted Living (AAL)	13
2.2	Αρχιτεκτονική των Συστημάτων IoMT	14
2.2.1	Η Δομή των Στρωμάτων Επικοινωνίας στα Συστήματα IoMT	15
2.2.2	Τύποι Δικτύων	16
2.2.3	Τα Επίπεδα της Αρχιτεκτονικής των Δικτύων IoMT	18
2.2.4	Συμπεράσματα	21
3	Απειλές Ασφάλειας και Ιδιωτικότητας στα Συστήματα IoMT	24
3.1	Απειλές Ασφάλειας στα Συστήματα IoMT	24
3.1.1	Απειλές Εμπιστευτικότητας στα Συστήματα IoMT	28
3.1.1.1	Απειλές στο Φυσικό Επίπεδο (Tier-1)	29
3.1.1.2	Απειλές στο Επίπεδο Δικτύου (Tier-2)	29
3.1.1.3	Απειλές στο Επίπεδο Εφαρμογής (Tier-3)	29
3.1.2	Απειλές Ακεραιότητας στα Συστήματα IoMT	30
3.1.2.1	Απειλές στο Φυσικό Επίπεδο (Tier-1)	30
3.1.2.2	Απειλές Επίπεδο Δικτύου (Tier-2)	31
3.1.2.3	Απειλές στο Επίπεδο Εφαρμογής (Tier-3)	31
3.1.3	Απειλές Διαθεσιμότητας στα συστήματα IoMT	31
3.1.3.1	Απειλές στο Φυσικό Επίπεδο (Tier-1)	33
3.1.3.2	Απειλές στο Επίπεδο Δικτύου (Tier-2)	33
3.1.3.3	Απειλές στο Επίπεδο Εφαρμογής (Tier-3)	33
3.2	Απειλές Ιδιωτικότητας στα Συστήματα IoMT	34
3.2.1	Διαρροή της Ιδιωτικότητας (Privacy Leakage - PL)	34
3.2.1.1	Απειλές στο Φυσικό Επίπεδο (Tier-1)	35
3.2.1.2	Απειλές στο Επίπεδο Δικτύου (Tier-2)	35
3.2.1.3	Απειλές στο Επίπεδο Εφαρμογής (Tier-3)	35
4	Απαιτήσεις Ασφάλειας και Ιδιωτικότητας στα Συστήματα IoMT	37
4.1	Απαιτήσεις Ασφάλειας στα Συστήματα IoMT	38

4.1.1	Απαιτήσεις στο Φυσικό Στρώμα (Sensing Layer)	39
4.1.2	Απαιτήσεις στο Στρώμα Δικτύου (Network Layer)	40
4.1.3	Απαιτήσεις στο Στρώμα Υπηρεσιών (Service Layer)	41
4.1.4	Απαιτήσεις στο Στρώμα Διεπαφής (Interface Layer)	41
4.2	Απαιτήσεις Ιδιωτικότητας στα συστήματα IoMT	42
4.2.1	Απαιτήσεις στο Φυσικό Στρώμα (Sensing Layer)	44
4.2.2	Απαιτήσεις στο Στρώμα Δικτύου (Network Layer)	44
4.2.3	Απαιτήσεις στο Στρώμα Διεργασιών (Service Layer)	44
4.2.4	Απαιτήσεις στο Στρώμα Διεπαφής (Interface Layer)	45
4.3	Συμβιβασμοί στα Συστήματα IoMT (Trade-offs)	45
5	Μέτρα για την Ενίσχυση της Ασφάλειας και της Ιδιωτικότητας στα Συστήματα IoMT	49
5.1	Προκαθορισμένες Λύσεις στην Ασφάλεια και Ιδιωτικότητα	49
5.1.1	Μέτρα Πρόληψης	50
5.1.1.1	Εκπαίδευση Χρηστών	50
5.1.1.2	Διαχείριση Κρίσεων	51
5.1.2	Μεθοδολογίες Ανίχνευσης	51
5.1.2.1	Μηχανισμοί Ελέγχου - Audit Mechanisms (AM)	51
5.1.2.2	Συστήματα Ανίχνευσης Παραβατικής Συμπεριφοράς (Intrusion Detection Systems - IDS)	52
5.1.3	Μεθοδολογίες Αντιμετώπισης Προβλημάτων στα Συστήματα IoMT	53
5.1.3.1	Κρυπτογράφηση	53
5.1.3.2	Τεχνικές Ελαχιστοποίησης Δεδομένων	54
5.1.3.3	Τεχνικές Ελέγχου Πρόσβασης	55
5.1.3.4	Μέτρα Ενίσχυσης της Ασφάλειας στο Κανάλι Επικοινωνίας	56
5.2	Προτεινόμενες Λύσεις στα Ζητήματα Ασφάλειας και Ιδιωτικότητας των Συστημάτων IoMT	57
5.3	Ανοιχτά Ερωτήματα και Προκλήσεις στα Συστήματα IoMT	60
6	Αποκεντρωμένες Προσεγγίσεις στην Ασφάλεια των Συστημάτων IoMT	63
6.1	Η Τεχνολογία Blockchain και τα Συστήματα IoT	63
6.2	Η Τεχνολογία Blockchain και τα Συστήματα IoMT	67
6.3	Προκλήσεις της Τεχνολογίας Blockchain στα Συστήματα IoMT	69
6.4	Πρόταση Αποκεντρωμένου Μοντέλου Ασφάλειας για τα Συστήματα IoMT	71
6.4.1	Επισκόπηση Προτεινόμενου Μέτρου	71
7	Σύνοψη, Προκλήσεις και Ανοιχτά Ζητήματα	78
7.1	Σύνοψη της Πτυχιακής Εργασίας	78
7.2	Ανοιχτά Ζητήματα και Μελλοντικές Επεκτάσεις	79
	Βιβλιογραφία	83