ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

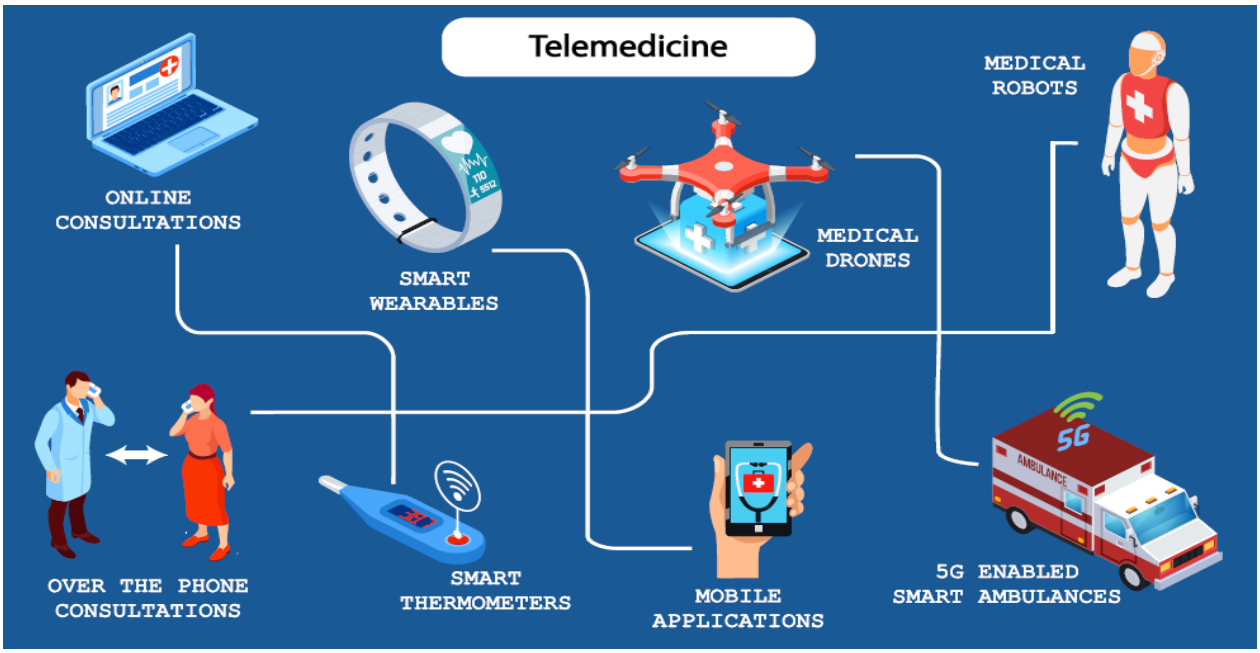
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΙΑΤΡΙΚΩΝ ΠΡΑΓΜΑΤΩΝ ΣΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΗΣ ΠΑΝΔΗΜΙΑΣ»



Των φοιτητών

Ιμάμ Χουσεΐν

Αρ. Μητρώου: 063142

Χατζηπουργάνη Δημητρίου

Αρ. Μητρώου: 063133

Επιβλέπουσα

Ασδρέ Αικατερίνη

Βαθμίδα: Ε.ΔΙ.Π.

Θεσσαλονίκη 10/01/2023

Τίτλος Δ.Ε.: Το διαδίκτυο των ιατρικών πραγμάτων στην αντιμετώπιση της πανδημίας

Κωδικός Δ.Ε.: 22214

Ονοματεπώνυμο φοιτητών: Ιμάμ Χουσεΐν - Χατζηπουργάνης Δημήτριος

Ονοματεπώνυμο εισηγητή: Ασδρέ Αικατερίνη

Ημερομηνία ανάληψης Δ.Ε.: 30/03/2022

Ημερομηνία περάτωσης Δ.Ε.: 20/01/2023

Βεβαιώνουμε ότι είμαστε οι συγγραφείς αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχαμε για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχουμε καταγράψει τις όποιες πηγές από τις οποίες κάναμε χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνουμε ότι αυτή η εργασία προετοιμάστηκε από εμάς προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

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

Η παρούσα διπλωματική εργασία αφιερώνεται στους φοιτητές που βρέθηκαν στη δεινή θέση να θέσουν σε δεύτερη μοίρα τη συνέχιση και ολοκλήρωση των σπουδών τους στη σχολή όπου φοιτούσαν, φτάνοντας στο σημείο να ενταχθούν στη κατηγορία των «αιώνιων φοιτητών». Οι λόγοι διακοπής των σπουδών μπορεί να ποικίλουν, ανεπάρκεια οικονομικών πόρων, εργασιακές υποχρεώσεις, οικογενειακοί και κοινωνικοί λόγοι, αλλά ποτέ το ξεθώριασμα της διάθεσης για ένα καλύτερο μέλλον μέσα από την τριτοβάθμια εκπαίδευση.

Πρόλογος

Η πανδημία του Covid-19 επέφερε πολλές αλλαγές στον τρόπο ζωής των ανθρώπων, αλλά ταυτόχρονα ώθησε την ενσωμάτωση της τεχνολογίας στον υγειονομικό κλάδο. Η τεχνολογία του Διαδικτύου των Πραγμάτων (IoT) σε συνεργασία με αυτή του Blockchain οδήγησε σε πολλές καινοτομίες που στόχο είχαν την μείωση της εξάπλωσης του ιού, μέσα από εφαρμογές ιατρικής παρακολούθησης ασθενών από το σπίτι, εντοπισμού και παρακολούθησης εστιών μόλυνσης, διασφάλισης τήρησης της καραντίνας, αυτοαξιολόγησης συμπτωμάτων ασθενών, ιχνηλάτησης επαφών, διαδικτυακής συμβουλευτικής και ενημέρωσης σε πραγματικό χρόνο κ.ά. Στο πλευρό αυτής της προσπάθειας στάθηκαν η τεχνητή νοημοσύνη (AI) και η ανάλυση δεδομένων μεγάλου εύρους (Big Data), προσθέτοντας υπεραξία στις διάφορες υπηρεσίες μέσα από την ανάλυση των πληροφοριών που συλλέγονταν σε καθημερινή βάση από τις συσκευές και τους αισθητήρες που αξιοποιούνται στο πλαίσιο του Διαδικτύου των Ιατρικών Πραγμάτων (IoMT). Η εξέλιξη αυτή στον υγειονομικό κλάδο θεωρείται από πολλούς εξαιρετικά σημαντική, καθώς στο μέλλον επιδημίες μικρής ή μεγαλύτερης εμβέλειας θα συμβαίνουν σε τακτικότερο βαθμό, φανερώνοντας το κομβικό ρόλο της τεχνολογίας στο μέλλον της ανθρωπότητας.

Περίληψη

Ο τεχνολογικός κλάδος μέσα από την υγειονομική κρίση του Covid-19 κατάφερε να ενδυναμωθεί κάτω από την καινοτομική ομπρέλα μετρίασης της εξάπλωσης του ιού. Στην παρούσα πτυχιακή εργασία γίνεται μια περιγραφή της τεχνολογίας του blockchain με επίκεντρο τη δομή και τις αρχές λειτουργίας της. Έπειτα, παρουσιάζεται μια ανάλυση της αρχιτεκτονικής και των τεχνολογιών που αξιοποιούνται στο Διαδίκτυο των Πραγμάτων (IoT) με κατεύθυνση την βελτιστοποίηση των υπηρεσιών του. Ακολουθεί μια εμβάθυνση στο οικοσύστημα του Διαδικτύου των Ιατρικών Πραγμάτων (IoMT), το πλαίσιο, την αρχιτεκτονική, την ασφάλεια και τις προκλήσεις διαλειτουργικότητας με τις τεχνολογίες blockchain, τεχνητής νοημοσύνης (AI) και δεδομένα μεγάλου εύρους (Big Data). Στην ενότητα της υγειονομικής επιτήρησης μέσω IoMT γίνεται μια αναφορά στις προηγούμενες υγειονομικές κρίσεις και την τεχνολογία που εφαρμόστηκε. Στη συνέχεια γίνεται εκτενής παρουσίαση του τρόπου αξιοποίησης της τεχνολογίας IoMT σε διάφορους τομείς κατά την διάρκεια της πανδημίας του Covid-19. Τέλος, πραγματοποιείται μια συγκριτική μελέτη 19 εφαρμογών έξυπνων κινητών που υλοποιήθηκαν στο πλαίσιο καταπολέμησης της πανδημίας, όπου αξιοποιούνται διάφορα εργαλεία αναφορικά με την αυτοαξιολόγηση και παρακολούθηση συμπτωμάτων, τη αξιολόγηση κινδύνου νόσησης, την παροχή έγκυρων και έγκαιρων πληροφοριών, την ανίχνευση και χαρτογράφηση επαφών, τη διαδικτυακή ιατρική συμβουλευτική, την οπτικοποίηση αναφορών.

Λέξεις-κλειδιά: Blockchain, IoT, IoMT, AI, Big Data, COVID-19, Covid Apps, Trace Apps

«Internet of Medical Things (IoMT) against Covid-19»

«Imam Housein and Chatzipourganis Dimitrios»

Abstract

The technology sector, through the health crisis of Covid-19, managed to strengthen itself under the innovative umbrella of mitigating the spread of the virus. In this thesis, a description of blockchain technology is made, focusing on its structure and operating principles. Then, an analysis of the architecture and technologies used in the Internet of Things (IoT) is presented with the aim of optimizing its services. This is followed by an in-depth survey into the Internet of Medical Things (IoMT) ecosystem, framework, architecture, security, and interoperability challenges with blockchain, artificial intelligence (AI), and Big Data technologies. In the section on IoMT-enabled healthcare surveillance, a reference is made to previous healthcare crises and the technology implemented, to transition then to the Covid-19 pandemic, where there is an extensive presentation of how IoMT technology is being used in various sectors. Finally, a comparative study of 19 smart mobile applications implemented in the context of pandemic combat is carried out, using various tools for self-assessment and symptom monitoring, disease risk assessment, provision of timely and accurate information, contact tracing and mapping, online medical consultation and visualization of reports.

Keywords: Blockchain, IoT, IoMT, AI, Big Data, COVID-19 mitigation, Covid Apps, Trace Apps

Ευχαριστίες

Με την ολοκλήρωση της πτυχιακής εργασίας κλείνει ο κύκλος σπουδών μας έπειτα από αρκετή μελέτη και προσπάθεια, περίοδο κατά τη διάρκεια της οποίας στάθηκαν στυλοβάτες οι γονείς και οι φίλοι μας. Είναι μοναδικό συναίσθημα όταν οι γύρω σου πιστεύουν στις δυνατότητές σου, προσφέροντας σου απλόχερα κουράγιο για να συνεχίσεις το εκπαιδευτικό ταξίδι με την ίδια θέληση με την οποία ξεκίνησες. Φυσικά, δεν θα μπορούσαμε να παραλείψουμε την καθηγήτριά μας, κα. Ασδρέ Αικατερίνη, για την συμβουλευτική υποστήριξη που μας παρείχε σε όλη την διάρκεια συγγραφής της παρούσας πτυχιακής εργασίας.

Περιεχόμενα

Κατάλογος Σχημάτων και Πινάκων

Συντομογραφίες

IoT → Internet of Things

P2P → Peer to Peer

PACS → Picture Archiving and Communication System

PoW → Proof of Work

PoS → Proof of Stake

PoET → Proof of Elapsed Time

PoB → Proof of Burn

EVM → Ethereum Virtual Machine

EMR → Electronic Medical Records

HDG → Healthcare Data Gateway

IoMT → Internet of Medial Things

ITU → International Telecommunication Union

SoA → Service oriented Architecture

UUID → Universal Unique Identifier

QoS → Quality of Service

WSN → Wireless Sensor Networks

API → Application Program Interface

IFP→ Interface Profile

UPnP → Universal Plug and Play

LoWPAN → Low power Wireless Personal Area Networks

M2M → Machine to Machine

LPWAN → Low Power Wide Area Network

WMN → Wireless Mesh Network

AHN → Ad Hoc Network

TEA → Tiny Encryption Algorithm

AES → Advanced Encryption Standard

ECC → Elliptic Curve Cryptography

GPS → Global Position System

DLT → Distributed Ledger Technology

FN → Full Node

LN → Lightweight Node

HIPAA → Health Insurance Portability and Accountability Act

EHR → Electronic Medical record

OSI → Open Systems Interconnection

LTE → Long Term Evolution

CIoT → Cognitive Internet of Things

CR → Cognitive Ratio

CIoMT → Cognitive Internet of Medical Things

EEG → Electroencephalography

ECG → Electrocardiogram

RASC → Reference Architecture for Smart City

IoC → Intelligence & Operations Centre

BAN → Body Area Network

ICN → Information Centric Networking

GIS → Geographic Information System

SORMAS → Surveillance Outbreak Response Management & Analysis System

PPE → Personal Protective Equipment

ML → Machine Learning

CT → Computerized Tomography

FDA → Food and Drug Administration

DoS → Denial of Service

SVM → Support Vector Machine

ICU → Intensive Care Unit

SDWSN → Software Defined Wireless Sensor Networks

UCI → University California Irvine

IEEE → Institute of Electrical and Electronics Engineers

RPM → Remote Patient Monitoring

SPHCC → Shanghai Public Health Clinical Center

BLE → Bluetooth Low Energy

UAV → Unmanned Aerial Vehicle

IIT → Indian Institute of Technology

SVI → Social Vulnerability Index

CVAC → COVID-19 Vaccine Coverage Index

HCW → Health Care Worker

ANFIS → Adaptive Neuro-fuzzy Inference System

KNN → K-Nearest Neighbor

BDN → Blockchain Distributed Network

Κεφάλαιο 1ο: Η τεχνολογία Blockchain

1.1 Εισαγωγή

Η τεχνολογία Blockchain είναι μια αποκεντρωμένη, κατανεμημένη, κρυπτογραφημένη βάση δεδομένων με μια συνεχώς αναπτυσσόμενη λίστα εγγραφών (block). Ενώ είναι μια σχετικά νέα τεχνολογία, έχει εφαρμοστεί με εκθετικό ρυθμό στον χρηματοπιστωτικό τομέα και τα τελευταία χρόνια έχει επεκταθεί και σε άλλους τομείς, συμπεριλαμβανομένης της υγειονομικής περίθαλψης. Σε μια πρόσφατη έρευνα σε εταιρείες startup που σχετίζονται με ακτινολογικά δεδομένα, η τεχνολογία Blockchain εμφανίστηκε ως η ταχύτερα αναπτυσσόμενη στον κλάδο [2].

Η Παγκόσμια Μελέτη Blockchain της Deloitte, το 2019, αποκάλυψε ότι πολλοί οργανισμοί από διαφορετικούς τομείς, συμπεριλαμβανομένου του τομέα της υγειονομικής περίθαλψης, επεκτείνουν τις πρωτοβουλίες τους στο Blockchain. Μάλιστα διατυπώνει την πρόβλεψη πως το 10% του παγκόσμιου Ακαθάριστου Εγχώριου Προϊόντος (ΑΕΠ) θα βασίζεται σε εφαρμογές Blockchain έως το 2025. Παρόλο που η τεχνολογία Blockchain γνωρίζει μεγάλο ενδιαφέρον την τελευταία δεκαετία, οι προκλήσεις που παρεμποδίζουν την ενσωμάτωσή της με συστήματα IoT και την εφαρμογή της στον τομέα της υγειονομικής περίθαλψης εξακολουθούν να είναι αρκετές και έντονες. Σε αυτό το κεφάλαιο θα επιχειρηθεί μια μικρή ιστορική αναδρομή, η παρουσίαση της δομής και των βασικών αρχών λειτουργίας της τεχνολογίας καθώς και τα πλεονεκτήματα της [6].

1.2 Ιστορία του Blockchain

Το θεμέλιο για την τεχνολογία Blockchain τέθηκε το 1991 σε ένα επιστημονικό άρθρο, το οποίο περιέγραφε ένα σύστημα για την επαλήθευση της αυθεντικότητας ψηφιακών εγγράφων μέσω συναρτήσεων κατακερματισμού (hash functions). Οι συγγραφείς κατέληξαν στο συμπέρασμα ότι θα ήταν δυνατόν να επιτευχθεί η πιστοποίηση της αυθεντικότητας των ψηφιακών εγγράφων είτε μέσω μιας κεντρικής αρχής, είτε μέσω της διανομής των χρονικών σημάνσεων των κατακερματισμών [17]. Ο όρος «Blockchain» εμφανίστηκε για πρώτη φορά τον Οκτώβριο του 2008, σε ένα άρθρο που έθεσε τη μαθηματική βάση για το κρυπτονόμισμα Bitcoin. Τα κρυπτονομίσματα δημιουργήθηκαν ως απάντηση στην παγκόσμια οικονομική κρίση του 2007, όπου το πρώτο ψηφιακό νόμισμα έκανε την εμφάνισή του ένα έτος μετά από την δημοσίευση του άρθρου [23]. Ο συντάκτης του άρθρου δημοσίευσε το άρθρο υπό το ψευδώνυμο Satoshi Nakamoto, ενώ μέχρι και σήμερα η ταυτότητα του συντάκτη παραμένει άγνωστη.

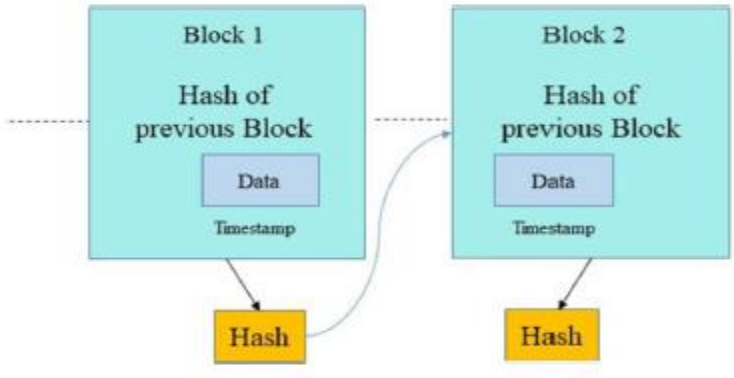
Εφόσον τα κρυπτονομίσματα είναι ψηφιακά και μπορούν εύκολα να αντιγραφούν, τα ίδια χρήματα θα μπορούσαν να διπλασιαστούν και να αποσταλούν σε δύο διαφορετικούς αποδέκτες, ένα πρόβλημα γνωστό ως «the double spending problem». Η επίλυση του προβλήματος της «διπλής δαπάνης» ήταν ένας

από τους αρχικούς παράγοντες που οδήγησαν στην ανάπτυξη της τεχνολογίας Blockchain. Πριν το Blockchain, η ασφάλιση της εγκυρότητας των συναλλαγών προϋπέθετε έναν κεντρικό διαμεσολαβητή (όπως μια τράπεζα), ο οποίος θα διαβεβαίωνε ότι τα χρήματα δεν έχουν σταλεί σε δύο διαφορετικά μέρη. Η τεχνολογία Blockchain, ωστόσο, επιλύει το πρόβλημα της διπλής δαπάνης αντικαθιστώντας την εμπιστοσύνη σε έναν κεντρικό διαμεσολαβητή, με την έννοια της κρυπτογραφικής απόδειξης.

Το Bitcoin ήταν το πρώτο κρυπτονόμισμα που ανέπτυξε τη λειτουργικότητα της τεχνολογίας Blockchain και κατηγοριοποιείται ως «αποκεντρωμένο εικονικό νόμισμα» από το Υπουργείο Οικονομικών των ΗΠΑ. Κατά τον Μάρτιο του 2021, το Bitcoin έχει συνολική κεφαλαιοποίηση άνω του ενός τρισεκατομμυρίου δολαρίων [23].

1.3 Δομή του Blockchain

Η δομή του Blockchain αποτελείται από τη κεφαλίδα και το σώμα του block που είναι διατεταγμένο με χρονολογική σειρά. Κάθε block αποθηκεύει την τιμή κατακερματισμού του προηγούμενου block, μια χρονική σήμανση (timestamp) και τη Merkel Root με τα δεδομένα του block. Κάθε block συναλλαγών στο Blockchain αποτελείται από την τιμή κατακερματισμού του προηγούμενου block, η οποία διασφαλίζει ότι όλα τα block συνδέονται, ενώ καμία αλλαγή δεν μπορεί να συμβεί σε block εκτός και αν αυτή επεκταθεί σε κάθε επόμενο block. Κάθε block περιέχει συναλλαγές και όλες οι συναλλαγές συνδέονται με μια τιμή κατακερματισμού, κάνοντας αδύνατη τη τροποποίηση δεδομένων. Ζεύγη τιμών κατακερματισμού ενώνονται για να υπολογιστεί η νέα τιμή, και η διαδικασία συνεχίζεται, δημιουργώντας ένα δέντρο τιμών κατακερματισμού. Η τιμή κατακερματισμού (hash) όλων των συναλλαγών που περιέχει ένα block ονομάζεται Merkel Root. Η Merkle Root διαφυλάσσει την ακεραιότητα των συναλλαγών του, καθώς οποιαδήποτε τροποποίηση συναλλαγής αλλάζει τη Merkle Root [4].



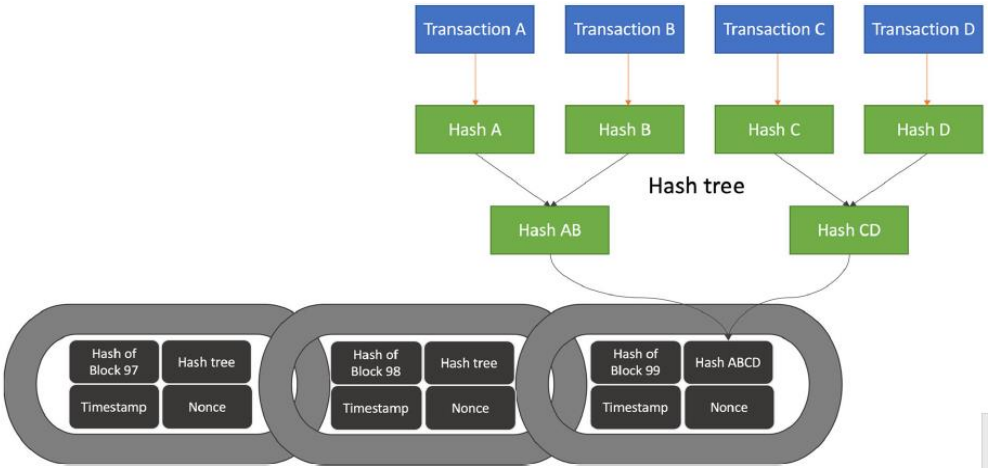
Εικόνα 1.1: Δομή του Blockchain (Πηγή: [4])

1.4 Αρχές λειτουργίας του Blockchain

1.4.1 Εισαγωγή

Η ανάπτυξη της θεωρίας της τεχνολογίας blockchain από τον Satoshi Nakamato, προσέλκυσε το έντονο ενδιαφέρον της κοινότητας των νέων τεχνολογιών ως μια εξελισσόμενη τεχνολογία peer-to-peer (P2P). Σήμερα, μπορούμε να ισχυριστούμε ότι η τεχνολογία blockchain εφαρμόζεται με επιτυχία σε όλους τους τομείς του διαδικτύου των πραγμάτων (IoT), όπως και στο κλάδο της υγείας (Internet of Healthcare Things). Η δομή blockchain συντίθεται από μια ακολουθία από blocks, δηλαδή μιας λίστας εγγραφών που είναι συνδεδεμένες μεταξύ τους με χρήση κρυπτογράφησης κατακερματισμού (hash). Στο δίκτυο blockchain ένα καθολικό εγγραφών διατηρεί δημόσια τις ψηφιακά υπογεγραμμένες συναλλαγές των χρηστών μεταξύ των ομότιμων χρηστών του δικτύου [15].

Η τεχνολογία Blockchain αναφέρεται σε ένα γενικότερο τεχνολογικό πλαίσιο και όχι σε μια συγκεκριμένη τυπική εφαρμογή. Αυτό σημαίνει, πως υπάρχουν κοινές αρχές στις οποίες βασίζονται οι διάφορες εφαρμογές, αλλά δεν είναι ίδιες για όλες. Κάθε μπλοκ (block) που ανήκει στην αλυσίδα περιέχει μια σειρά συναλλαγών. Ο απλούστερος τρόπος για να κατανοηθεί το τι συνιστά μια συναλλαγή, είναι να την δούμε ως οικονομική συναλλαγή, καθώς αυτής της μορφής ήταν και τα αρχικά διακεκριμένα στοιχεία δεδομένων που ανταλλάχθηκαν στην περίπτωση του Bitcoin [23]. Ωστόσο, οι συναλλαγές δεν είναι απαραίτητα οικονομικές και μπορεί να αποτελέσουν οποιοδήποτε γεγονός καταγράφεται και μεταβάλλει το Blockchain. Για παράδειγμα, η προσθήκη μιας μελέτης ιατρικής απεικόνισης σε ένα Blockchain θα μπορούσε να θεωρηθεί ως συναλλαγή. Στο δίκτυο Blockchain του Ethereum, μπορούν να αποθηκευτούν εφαρμογές και κάθε αποθήκευση (συναλλαγή) οδηγεί σε αλλαγή της κατανεμημένης εφαρμογής. Για παράδειγμα στο δίκτυο του Ethereum, ως συναλλαγή θα μπορούσε να θεωρηθεί η διανομή αλγορίθμων μηχανικής μάθησης σε όλους τους κόμβους του δικτύου.



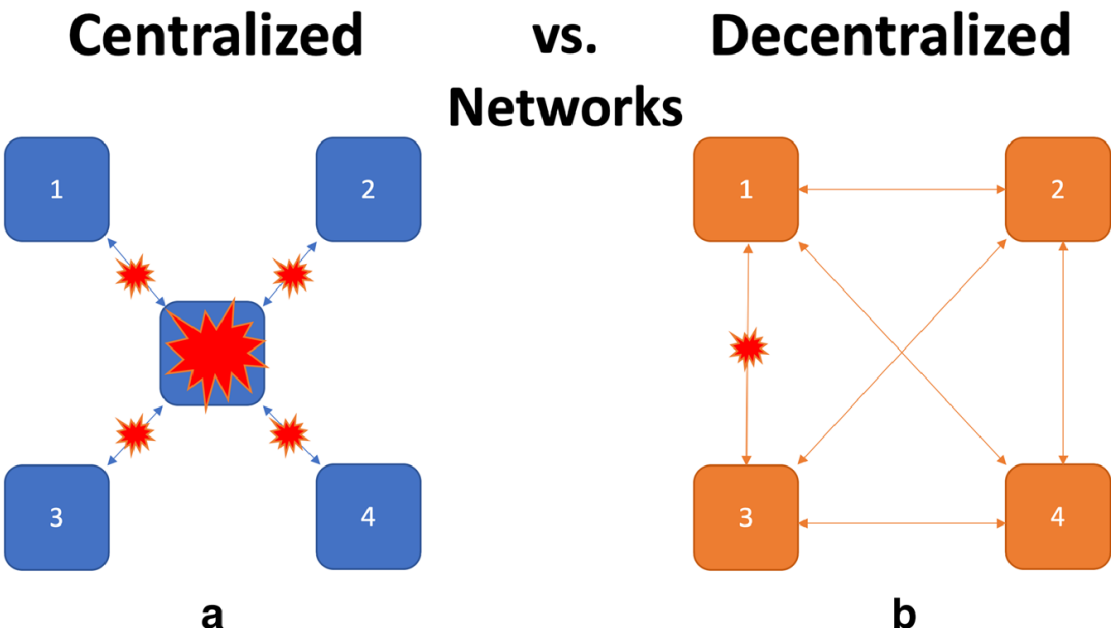
Σχήμα 1.2: Παράδειγμα Blockchain (Πηγή: [21])

Στο σχήμα 1.2 μπορούμε να δούμε την πραγματοποίηση πολλαπλών συναλλαγών στο Blockchain (π.χ. μεταφορά χρημάτων). Κάθε συναλλαγή κατακερματίζεται και οι κατακερματισμένες τιμές συνδυάζονται σε ένα δέντρο κατακερματισμού. Σε κάθε νέο block εισάγονται το δέντρο κατακερματισμού, ο κατακερματισμός του προηγούμενου μπλοκ και η χρονική σήμανση. Τα Nonces είναι τυχαίοι ακέραιοι αριθμοί 32bit (4 bytes) που χρησιμοποιούνται μόνο μία φορά και αποτελούν το κεντρικό μέρος του μηχανισμού Proof-of-Work, ως τιμές επαλήθευσης ενός μαθηματικού προβλήματος. Εφαρμόζεται κατά το κατακερματισμό της τιμής του μπλοκ, με το νέο μπλοκ να προστίθεται στο Blockchain, δημιουργώντας ένα πιο πολύπλοκο αλγόριθμο [21].

1.4.2 Blockchain και αποκέντρωση

Τα δίκτυα υπολογιστών μπορούν να κατηγοριοποιηθούν σε κεντρικά και αποκεντρωμένα ή κατανεμημένα (σχήμα 1.3). Τα κεντρικά δίκτυα έχουν μοναδικό σημείο αποτυχίας. Εάν ο κεντρικός κόμβος του δικτύου καταρρεύσει, αυτόματα το σύνολο του δικτύου γίνεται μη λειτουργικό, διότι όλες οι πληροφορίες περνούν μέσα από αυτό το κεντρικό κόμβο. Όλη η σχέση εμπιστοσύνης βασίζεται στον κεντρικό κόμβο, που είναι ο ρυθμιστής του δικτύου. Παραδείγματα κεντρικών δικτύων έχουμε σε κάποια εσωτερικά δίκτυα νοσοκομείων, τοπικής εικονικής αρχειοθέτησης και ενδοεπικοινωνίας (Picture Archiving and Communication System - PACS). Τα αποκεντρωμένα δίκτυα έχουν πολλούς κόμβους μέσω των οποίων μπορούν να επικοινωνούν τα δεδομένα και δεν βασίζονται σε ένα μοναδικό σημείο αποτυχίας ή επιτυχίας. Εάν ένας ή περισσότεροι κόμβοι τεθούν εκτός λειτουργίας, υπάρχει πλεόνασμα κόμβων έτσι ώστε το υπόλοιπο δίκτυο να παραμείνει λειτουργικό. Τα αποκεντρωμένα δίκτυα είναι αυτά με την υψηλότερη τοπολογική εφεδρεία, καθώς όλοι οι κόμβοι του δικτύου έχουν τη δυνατότητα να επικοινωνούν απευθείας μεταξύ τους [7].

Ένα δημόσιο Blockchain αποτελείται από μεμονωμένους κόμβους που ο καθένας μπορεί να αποθηκεύσει ολόκληρο το αντίγραφο της βάσης δεδομένων, αποτελώντας ένα παράδειγμα δικτύου αποκεντρωμένης τοπολογίας. Οι κόμβοι πρέπει να καταλήξουν σε «συναίνεση» ως προς το ποιο μπλοκ θα προστεθεί στη συνέχεια του Blockchain. Με αυτόν τον τρόπο, η τεχνολογία Blockchain επιτρέπει την διανομή των ψηφιακών λιστών και της βάσης δεδομένων. Ωστόσο, η αποκεντρωμένη λειτουργία δεν είναι απολύτως απαραίτητη για εφαρμογές Blockchain, καθώς προϋποθέτουν άδεια μιας μερίδας των χρηστών ή μιας κεντρικής αρχής για την αλλαγή και επικύρωση των δεδομένων.



Σχήμα 1.3: Κεντρικά και αποκεντρωμένα δίκτυα (Πηγή: McBee)

Στο σχήμα 1.3α παρατηρούμε το σχηματισμό της τοπολογίας των κεντρικών δικτύων, όπου υπάρχει ένα και μοναδικό σημείο επικοινωνίας με τους υπόλοιπους κόμβους. Έτσι, εάν ο κεντρικός κόμβος καταρρεύσει, ολόκληρο το δίκτυο δεν λειτουργεί. Στα αποκεντρωμένα δίκτυα του σχήματος 1.3b οι κόμβοι επικοινωνούν ανεξάρτητα μεταξύ τους, επομένως σε περίπτωση όπου κάποιος κόμβος τίθεται εκτός λειτουργίας, υπάρχουν εναλλακτικές διαδρομές ώστε το υπόλοιπο δίκτυο να παραμείνει λειτουργικό [21].

1.4.3 Αλγόριθμοι Συναίνεσης (consensus)

Η συναίνεση στην τεχνολογία Blockchain σημαίνει ότι όλοι οι αποκεντρωμένοι κόμβοι στο δίκτυο συμφωνούν για το τι αποτελεί αλήθεια του συστήματος. Έτσι, προκύπτει ότι θα προστεθούν στην αλυσίδα του Blockchain μόνο τα μπλοκ για τα οποία συμφωνούν όλοι οι κόμβοι, συνθέτοντας τον αλγόριθμο απόδειξης εργασίας (Proof of Work - PoW) που είναι ο πιο ευρέως χρησιμοποιούμενος μηχανισμός για την επίτευξη συναίνεσης σε Blockchain. Η απόδειξη εργασίας απαιτεί την επίλυση ενός δύσκολου μαθηματικού κρυπτογραφικού προβλήματος, με τη διαδικασία αυτή να ονομάζεται mining. Μόλις επιλυθεί το πρόβλημα, οι άλλοι κόμβοι του δικτύου επαληθεύουν τη λύση με έναν υπολογιστικό αλγόριθμο πολύ πιο απλό από αυτόν που απαιτείται για την επίλυση του προβλήματος [23].

Σε έναν αλγόριθμο PoW, η διαδικασία επαλήθευσης εξαρτάται από την δημιουργία ενός nonce, ενός μοναδικού τυχαίου αριθμού, ο οποίος με τη βοήθεια ενός αλγορίθμου υποβάλλεται σε επεξεργασία ή «κατακερματίζεται», ικανοποιώντας πάντοτε μια αυθαίρετη συνθήκη που έχει καθοριστεί από το Blockchain. Ένα nonce θα μπορούσε, παραδείγματος χάριν, να είναι μια τιμή που πρέπει να ξεκινάει από

έναν ορισμένο αριθμό μηδενικών και να επιτρέπει την προσθήκη των δεδομένων στο Blockchain. Το υπολογιστικό βάρος της εκπλήρωσης αυτής της διαδικασίας τοποθετείται σε αυτούς που επιδιώκουν να προσθέσουν μια συναλλαγή στην αλυσίδα των block, έτσι ενθαρρύνεται η προσθήκη καίριων δεδομένων. Η αλλαγή της αυθαίρετης συνθήκης που πρέπει να ικανοποιηθεί μπορεί να κάνει την ανακάλυψη του nonce πιο δύσκολη (μεγαλύτερη απαίτηση υπολογιστικής ισχύος) ή πιο εύκολη, ανάλογα με την ζητούμενη δραστηριότητα και το μέγεθος του Blockchain. Η μοναδική υπόσταση του nonce αποτρέπει επίσης τις διπλές προσθήκες στο Blockchain (διπλή δαπάνη), αφού κάθε απόδειξη εργασίας (PoW) καταγράφεται και διανέμεται σε όλους τους κόμβους του Blockchain. Τέλος, για να επιτευχθεί η συναίνεση της διαδικασίας θα πρέπει κάθε κόμβος να επαληθεύσει τη συμπερίληψη της απόδειξης εργασίας.

Άλλα παραδείγματα αλγορίθμων συναίνεσης αποτελούν η απόδειξη μεριδίου (Proof of Stake - PoS), η απόδειξη χρόνου που έχει παρέλθει (Proof of Elapsed Time - PoET), η απόδειξη καύσης (Proof of Burn - PoB) και η βυζαντινή ανοχή σφαλμάτων (Byzantine-fault-tolerance). Οι τεχνικές λεπτομέρειες του κάθε αλγορίθμου συναίνεσης είναι διαφορετικές, καθώς ο καθένας διαθέτει τα δικά του μοναδικά πλεονεκτήματα και μειονεκτήματα.

1.4.4 Αμεταβλητότητα (Immutability)

Ένα Blockchain είναι αμετάβλητο, καθώς νέα δεδομένα μπορούν μόνο να προστεθούν. Μόλις προσαρτηθούν τα δεδομένα, αποτελούν μόνιμο μέρος του Blockchain, ενώ τα μπλοκ δεν μπορούν ούτε να τροποποιηθούν, ούτε να αφαιρεθούν. Αυτό γίνεται αντιληπτό ως προσθήκη «συνδέσμων» στην αλυσίδα, η οποία αυξάνεται με κάθε νέο μπλοκ που περιλαμβάνει μια χρονική σφραγίδα, πλην της τιμής κατακερματισμού, της κορυφής του προηγούμενου μπλοκ, συνθέτοντας τα δεδομένα σε μια ενιαία αλυσίδα (Σχήμα 1.2).

Εάν ένας εισβολέας ήταν σε θέση να τροποποιήσει ένα μπλοκ, όλα τα επόμενα μπλοκ στην αλυσίδα θα έπρεπε επίσης να αλλάξουν την τιμή κατακερματισμού εφόσον η αλλαγή της τιμής κατακερματισμού του πρώτου θα επηρέαζε και τις επόμενες, εφόσον αυτή αποθηκεύεται στην κεφαλίδα του κάθε μπλοκ. Το υπολογιστικό κόστος μιας τέτοιας μετατροπής με την τρέχουσα τεχνολογία είναι αρκετά μεγάλο, πράγμα που αποτρέπει τις επιθέσεις [17].

1.4.5 Προέλευση των δεδομένων

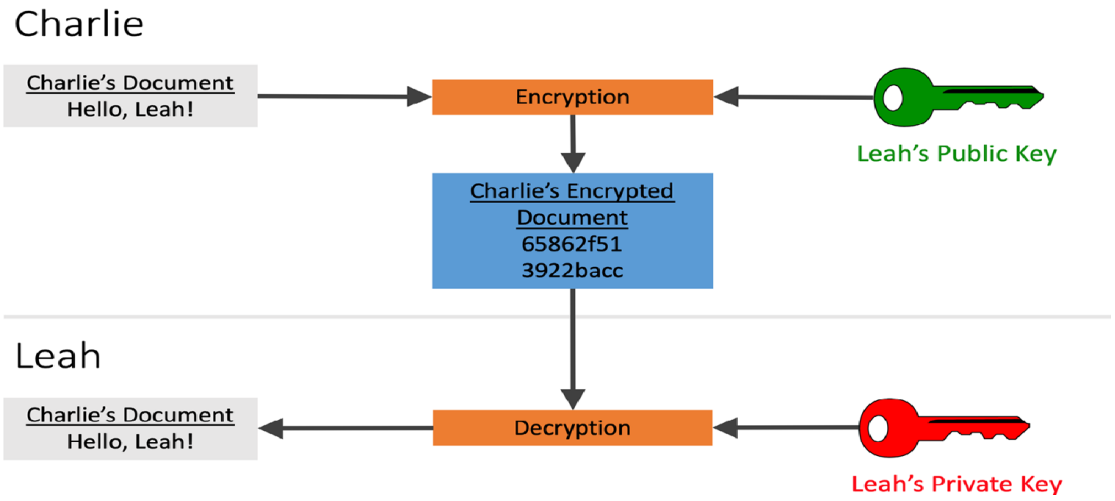
Η προέλευση ορίζεται στις κλασικές σπουδές ως «η καταγραφή της ιστορίας της ιδιοκτησίας, ενός αξιόλογου αντικειμένου ή έργου τέχνης». Η έννοια της προέλευσης των δεδομένων εφαρμόζει αυτή την ιδέα για την πιστοποίηση των δεδομένων και καθίσταται δυνατή διότι στην τεχνολογία Blockchain κάθε συναλλαγή είναι εγγενώς συνδεδεμένη με την προηγούμενη. Αυτό αποτελεί ένα βασικό συστατικό

της τεχνολογίας Blockchain καθώς κάθε μπλοκ της αλυσίδας περιέχει μια αναφορά στο προηγούμενο μπλοκ και ως εκ τούτου οι συναλλαγές μπορούν να εντοπιστούν έως και το γενετήριο block (το πρώτο block του Blockchain) [17].

1.4.6 Κρυπτογράφηση

Η τεχνολογία Blockchain βασίζεται στον κρυπτογραφικό μετασχηματισμό κάνοντας χρήση ενός δημοσίου-κλειδιού κρυπτογράφησης (Σχήμα 1.4) που χρησιμοποιεί ζεύγη κλειδιών. Τα δημόσια κλειδιά είναι διαθέσιμα δημοσίως, ενώ τα ιδιωτικά κλειδιά είναι μυστικά όπως οι κωδικοί πρόσβασης. Για κάθε αλληλεπίδραση με το Blockchain, ο εκάστοτε χρήστης έχει ένα ξεχωριστό δημόσιο και ιδιωτικό κλειδί. Έτσι, για παράδειγμα, ο χρήστης Α μπορεί να στείλει στον Β ένα κρυπτογραφημένο μήνυμα που είναι αναγνώσιμο μόνο από τον Β, το οποίο έχει κρυπτογραφηθεί με χρήση του δημόσιου κλειδιού του Β, ενώ μπορεί να αποκρυπτογραφηθεί μόνο με τη χρήση του ιδιωτικού κλειδιού του Β. Τα δεδομένα κρυπτογραφούνται και είναι αναγνώσιμα μόνο με το ιδιωτικό κλειδί του παραλήπτη.

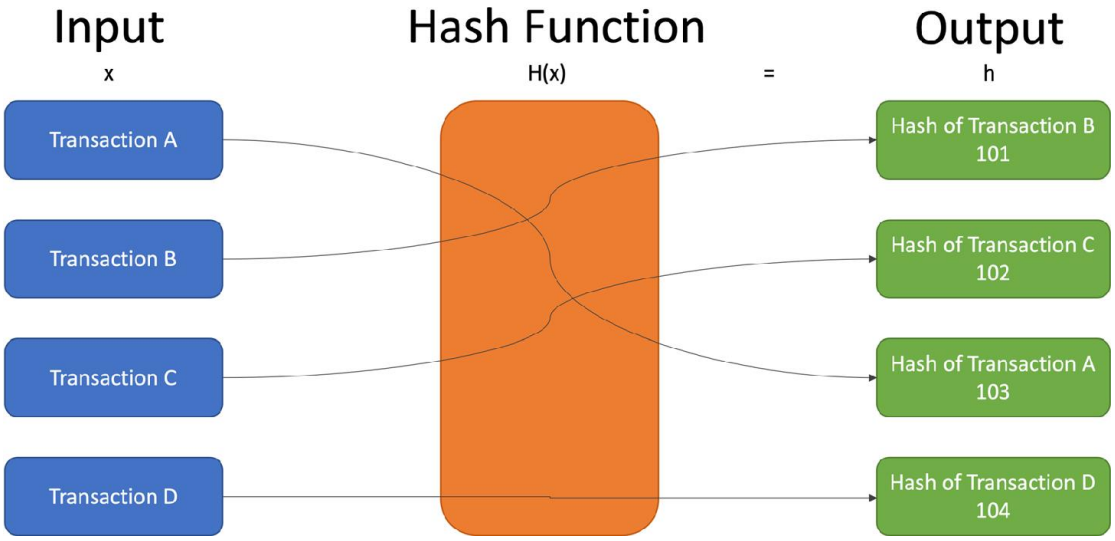
Οι συναρτήσεις Hash (Η) καταγράφουν τα δεδομένα εισόδου (x) σε εξόδους σταθερού μεγέθους (h) που ονομάζονται τιμές κατακερματισμού (Σχήμα 1.5). Οι συναρτήσεις κρυπτογραφικού κατακερματισμού είναι μη αναστρέψιμες (μονόδρομες), καθώς μια είσοδος αντιστοιχεί σε μια δεδομένη τιμή κατακερματισμού, αλλά όχι το αντίστροφο (δηλαδή, η αρχική είσοδος δεν μπορεί να ανακατασκευαστεί από την τιμή κατακερματισμού, αλλά τα δεδομένα εισόδου θα δίνουν πάντα την ίδια τιμή κατακερματισμού) [17].



Σχήμα 1.4: Κρυπτογράφηση δημόσιου κλειδιού (Πηγή: [17])

Το Blockchain βασίζεται στην κρυπτογράφηση δημόσιου κλειδιού που χρησιμοποιεί ζεύγη κλειδιών, όπου τα δημόσια κλειδιά είναι διαθέσιμα δημοσίως και τα ιδιωτικά κλειδιά διατηρούνται μυστικά.

Επομένως, εφαρμόζοντας το δημόσιο κλειδί της Leah, ο Charlie μπορεί να κρυπτογραφήσει ένα μήνυμα το οποίο μπορεί να αποκρυπτογραφηθεί και να αναγνωστεί μόνο από τη Leah μέσω του ιδιωτικού κλειδιού που διαθέτει [21].



Σχήμα 1.5: Συνάρτηση Hash (H) που αντιστοιχεί δεδομένα εισόδου (x) σε εξόδους σταθερού μεγέθους (h) που ονομάζονται τιμές κατακερματισμού (Πηγή: [17])

1.4.7 Δημόσια, Ιδιωτικά και Υβριδικά Blockchains

Σε κάθε εφαρμογή της τεχνολογίας Blockchain, υπάρχουν πολλές αποφάσεις που πρέπει να ληφθούν ως προς την λειτουργία του Blockchain. Μια σημαντική απόφαση, σχετίζεται με την προσβασιμότητα στις πληροφορίες του Blockchain, καθώς τα Blockchain μπορεί να λειτουργούν με άδεια ή χωρίς άδεια. Τα συστήματα Blockchain μπορεί να είναι δημόσια και προσβάσιμα από όλους ή ιδιωτικά όπου μπορούν να έχουν πρόσβαση όσοι πληρούν τα κριτήρια εισόδου. Στο δημόσιο blockchain, κάθε άτομο που έχει πρόσβαση σε σύνδεση στο διαδίκτυο μπορεί να συμμετάσχει στη διαδικασία επαλήθευσης συναλλαγών, ενώ το ιδιωτικό blockchain είναι ένα κεντρικό δίκτυο που διαχειρίζεται από μια αρχή που ελέγχει το επίπεδο ελέγχου ταυτότητας και εξουσιοδότησης των συμμετεχόντων πριν την εγγραφή τους στο σύστημα. Το blockchain κοινοπραξίας είναι ένα μερικώς κεντρικό δίκτυο, υλοποιημένο ως ιδιωτικός διαμοιρασμός blockchain μεταξύ πολλών εταιρειών.

Τα κρυπτονομίσματα Bitcoin και Ethereum αποτελούν παραδείγματα δημόσιων Blockchain όπου κάθε υπολογιστής με σύνδεση στο διαδίκτυο έχει πρόσβαση στα δεδομένα που είναι αποθηκευμένα στο Blockchain. Οι περισσότερες επιχειρηματικές εφαρμογές (π.χ. εκείνες που χρησιμοποιούν Hyperledger) χρησιμοποιούν ιδιωτικά Blockchain στα οποία ο μηχανισμός χορήγησης άδειας ελέγχει την πρόσβαση στα δεδομένα που είναι αποθηκευμένα στο Blockchain. Πέραν αυτών των δύο τύπων, υπάρχει και το υβριδικό (Hybrid) που αναφέρεται στη χρήση ενός συνδυασμού δημόσιας και ιδιωτικής αλυσίδας μπλοκ

ή κοινοπραξίας για τη διατήρηση του απορρήτου των ασθενών με την αποθήκευση ευαίσθητων δεδομένων (δηλαδή, διάγνωση γιατρού) σε ιδιωτικό blockchain, ενώ τα λιγότερο ευαίσθητα δεδομένα μπορούν να αποθηκευτούν δημόσια [32].

1.4.8 Smart Contracts

Ο κατακερματισμός δεδομένων μπορεί να οδηγήσει σε συγκρούσεις πληροφοριών μεταξύ των παρόχων υγειονομικής περίθαλψης και ανεπάρκεια πληροφοριών με συνέπεια να παρεμποδίζεται η διαδικασία θεραπείας. Η τεχνολογία Blockchain βοηθάει τα κέντρα υγειονομικής περίθαλψης να εγκαταστήσουν μια διασύνδεση μεταξύ του αποθετηρίου δεδομένων που υπάρχουν στο δίκτυο, διασφαλίζοντας την ασφαλή ανταλλαγή ευαίσθητων ιατρικών πληροφοριών, αυξάνοντας τη διαφάνεια μεταξύ των γιατρών και των ασθενών, προωθώντας παράλληλα τη συνεργασία μεταξύ παρόχων υγειονομικής περίθαλψης και οργανισμών με σκοπό τη διεξαγωγή ποιοτικών ερευνών.

Η ασφαλής μετάδοση μέσω της τεχνολογίας blockchain οφείλεται σε τρεις παράγοντες. Πρώτον, περιέχει ένα αμετάβλητο καθολικό το οποίο μπορούν να ελέγχουν και να έχουν πρόσβαση οι διάφοροι χρήστες, διασφαλίζοντας ότι όταν μια εγγραφή αποθηκεύεται στο καθολικό, ακολουθεί ορισμένους προκαθορισμένους κανόνες δίχως τη δυνατότητα τροποποίησης. Δεύτερον, το blockchain λειτουργεί ταυτόχρονα από πολλές συσκευές, αποτελώντας μια κατανεμημένη τεχνολογία, ενώ τρίτον ακολουθεί τους κανόνες ανταλλαγής δεδομένων με τη χρήση ενός μηχανισμού έξυπνων συμβολαίων [25].

Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για την εφαρμογή άλλων αποκεντρωμένων υπηρεσιών εκτός από οικονομικές συναλλαγές όπου η εμπιστοσύνη στο σύστημα είναι ενσωματωμένη λόγω των εγγενών ιδιοτήτων της τεχνολογίας Blockchain. Ένα από τα πιο σημαντικά πρόσθετα χαρακτηριστικά που μπορεί να ενσωματωθεί στο Blockchain είναι τα smart contracts.

Τα smart contracts είναι υπολογιστικά προγράμματα που εφαρμόζουν τους όρους συμφωνίας μεταξύ των διαφόρων μερών, χωρίς την ανάγκη ανθρώπινης παρέμβασης [10]. Αυτά τα συμβόλαια μπορούν να καταγραφούν και να επικυρωθούν από το Blockchain, το οποίο στη συνέχεια μπορεί να εκτελέσει με αυτόματο τρόπο, επιβάλλοντας τη κοινή σύμβαση συνήθως σύμφωνα με την δομή «if-then». Ένα έξυπνο συμβόλαιο επιτρέπει σε δύο ή περισσότερους χρήστες να πραγματοποιήσουν μια συναλλαγή με αξιοπιστία, δίχως την επικύρωση μεσάζοντα. Η διαδικασία επαλήθευσης και προσθήκης μιας συναλλαγής στο Blockchain εγγυάται ότι οι όποιες διαφορές ή ανακρίβειες μπορούν να συμβιβαστούν, καταλήγοντας στην ύπαρξη μόνο μίας έγκυρης συναλλαγής (χωρίς διπλές καταχωρίσεις).

Τα smart contracts έγιναν δημοφιλή λόγω του Ethereum, το οποίο χρησιμοποιεί την διανεμημένη ανοιχτού κώδικα (open source) υπολογιστική πλατφόρμα Ethereum Virtual Machine (EVM) που βασίζεται στην τεχνολογία Blockchain. Ο κύριος στόχος της EVM είναι να διατηρεί ένα κατανεμημένο

αρχείο συναλλαγών που εκτελούνται χρησιμοποιώντας το ψηφιακό νόμισμα Ethereum, Ether (ETH). Άλλες πλατφόρμες που προσφέρουν επίσης λειτουργίες smart contract είναι το umbrella project του Hyperledger. Οι βασικές αρχές παραμένουν οι ίδιες, ακόμη και αν σε ορισμένες περιπτώσεις η εφαρμογή και ο τρόπος χειρισμού των smart contracts διαφέρει.

Ωστόσο, ορισμένοι υποστηρίζουν ότι η ορολογία smart contracts «έξυπνα συμβόλαια» είναι στην πραγματικότητα λανθασμένη, υπό την έννοια ότι δεν είναι ούτε «έξυπνα» (ικανά να μεταφράσουν περίπλοκες νομικές συμφωνίες σε λογισμικό) ούτε «συμβόλαια» (δεν έχουν υποκείμενες νομικές ή συμβατικές διατάξεις), ενώ είναι προς το παρόν εφικτά και εφαρμόσιμα μόνο υπό αυστηρούς όρους. Προκλήσεις σχετικά με τα smart contracts ενδέχεται να προκύψουν εάν εξετάσουμε τις δυνατότητες για άτομα και οργανισμούς να δημιουργήσουν τα δικά τους συστήματα κανόνων ή έξυπνων συμβάσεων ως ένα είδος αυτοματοποιημένων ιδιωτικών κανονιστικών πλαισίων [14], [26].

Το έξυπνο συμβόλαιο διαχειρίζεται την ταυτότητα και καθορίζει τα δικαιώματα πρόσβασης του χρήστη σε διαφορετικές ηλεκτρονικές ιατρικές αναφορές (EMR) που είναι αποθηκευμένες στο blockchain. Έτσι, επιτρέπεται στο ιατρικό προσωπικό να προσπελάσει μόνο τις αναφορές EMR που έχει άδεια χρήσης. Πολλά έργα blockchain έχουν καθιερωθεί στη βιομηχανία υγειονομικής περίθαλψης τα τελευταία χρόνια για τη διαχείριση του ηλεκτρονικού ιατρικού φακέλου (EMR), της συνταγογράφησης φαρμάκων και των κλινικών πρωτοκόλλων. Οι Yue et al. έχουν αναπτύξει μια εφαρμογή που ονομάζεται πύλη δεδομένων υγειονομικής περίθαλψης (HDG) που αξιοποιεί την τεχνολογία blockchain και παρέχει τη δυνατότητα στους ασθενείς να ελέγχουν και να διαμοιράζονται τις πληροφορίες τους, χωρίς να παραβιάζεται η πολιτική απορρήτου [25].

1.5 Τρόποι υποστήριξης της τεχνολογίας Blockchain κατά του Covid-19

Η τεχνολογία Blockchain επιτρέπει σε άτομα και οργανισμούς από οποιαδήποτε σημείο στο κόσμο να αποτελέσουν κομμάτι ενός ενιαίου διασυνδεδεμένου δικτύου που διευκολύνει την ασφαλή κοινή χρήση δεδομένων. Η δυνατότητα προστασίας του blockchain από παραβιάσεις το καθιστά ανθεκτικό σε μη εξουσιοδοτημένες αλλαγές, ενώ η χρήση συναινετικών αλγορίθμων και έξυπνων συμβάσεων ελαχιστοποιεί τη δυνατότητα διάδοσης ψευδών δεδομένων και πλαστών πληροφοριών. Επίσης, βοηθάει στη διατήρηση της επεκτασιμότητας ελαχιστοποιώντας την πολυπλοκότητα ολοκλήρωσης, στην ελαχιστοποίηση των απαιτήσεων αποθήκευσης δεδομένων, στη διατήρηση της ισορροπίας μεταξύ της ευκολίας ενσωμάτωσης και των αναδυόμενων προβλημάτων ασφαλείας [15]. Παρακάτω παρουσιάζονται οι πιο σημαντικοί τρόποι καταπολέμησης της εξάπλωσης του Covid-19 μέσω της τεχνολογίας blockchain:

- **Υποστήριξη εκτεταμένων δοκιμών ελέγχου (testing) και αναφορών (reporting)**: Η Κίνα, η Γερμανία και η Δημοκρατία της Κορέας, είχαν τονίσει την ανάγκη για εκτεταμένους ελέγχους

τεστ ως το βασικό μέσο για τον περιορισμό εξάπλωσης του ιού. Ωστόσο, για να εξασφαλιστεί η αποτελεσματικότητα της διαδικασίας θα έπρεπε οι έλεγχοι να υλοποιούνται με έξυπνο τρόπο, διατηρώντας την ακρίβεια των δεδομένων όσον αφορά τον αριθμό των τεστ που διενεργούνται. Η τεχνολογία blockchain μπορεί να βοηθήσει στη δημιουργία κατανεμημένων σημείων ελέγχου για τον έλεγχο των ασθενών που εμφανίζουν συμπτώματα που σχετίζονται με τον COVID-19. Οι συντονιστές των σημείων ελέγχου μπορούν να λειτουργήσουν ως κόμβοι του ίδιου κατανεμημένου δικτύου blockchain, ενημερώνοντας συνεχώς τον αριθμό των δοκιμών που πραγματοποιήθηκαν και τον αριθμό των εργαστηριακά επιβεβαιωμένων περιπτώσεων, οδηγώντας σε αναφορές υψηλής ακρίβειας ανά περιοχή και υποστηρίζοντας τους φορείς υγειονομικής περίθαλψης στο σχεδιασμό στρατηγικής για την καταπολέμηση της εξάπλωσης της νόσου. Το κοινό δίκτυο blockchain μπορεί να λειτουργήσει ως μια ενιαία πηγή ενημέρωσης και ανάκτησης δεδομένων για όλους τους χρήστες, λόγω των εγγενών χαρακτηριστικών που φέρει το blockchain [11].

- **Καταγραφή στοιχείων των COVID-19 ασθενών**: Εκτός από την ασφαλή αποθήκευση των αναφορών ελέγχου (test), οι κατανεμημένες blockchain πλατφόρμες μπορούν να καταγράψουν τα στοιχεία των ασθενών COVID-19. Μόλις ένα άτομο βγει θετικό στον COVID-19, όλα τα στοιχεία του, συμπεριλαμβανομένου του φύλου, της ηλικίας, του ιατρικού ιστορικού, των υποκείμενων παθήσεων υγείας, της σοβαρότητας της νόσου, των συμπτωμάτων που παρουσίασε και των κατευθυντήριων οδηγιών θεραπείας, μπορούν να προστεθούν με ασφάλεια στο δίκτυο. Μια πλατφόρμα με ενημερωμένα δεδομένα για ασθενείς με COVID-19 μπορεί να βοηθήσει στη μελέτη των κλινικών χαρακτηριστικών και την κατανόηση του μοτίβου ανάπτυξης της νόσου. Στο εγγύς μέλλον, κάθε κέντρο υγείας COVID-19 θα μπορεί να ανατρέξει σε αυτές τις μελέτες και να προβλέψει το είδος των εγκαταστάσεων και φαρμάκων που απαιτούνται για την αντιμετώπιση της κατάστασης [11].
- **Διαχείριση του Lockdown**: Υπό συνθήκες καραντίνας οι βασικές ανάγκες των ανθρώπων πρέπει να καλυφθούν για να μπορέσουν να μείνουν στο σπίτι, ακολουθώντας αυστηρά τους περιορισμούς του lockdown. Μελέτες υποστηρίζουν ότι οι άνθρωποι που διαμένουν σε εύκολα προσβάσιμες περιοχές αξιοποιούν επιπλέον υπηρεσίες, από αυτούς που ζουν σε απομακρυσμένες περιοχές. Για το σκοπό αυτό, η τεχνολογία blockchain μπορεί να βοηθήσει στην επίβλεψη των απαιτήσεων των ανθρώπων ανά περιοχή και ως εκ τούτου στην αποτελεσματικότερη διαχείριση του lockdown. Το ρόλο των κόμβων σε αυτό το δίκτυο blockchain μπορούν να διατελέσουν οι εξουσιοδοτημένες ομάδες ή τα άτομα που συνδέονται με την επιβολή του lockdown, καταγράφοντας τις ανάγκες των κατοίκων στην καθορισμένη περιοχή του δικτύου. Όλοι οι συμμετέχοντες κόμβοι στο δίκτυο της αλυσίδας μπλοκ επιτρέπεται να ελέγχουν για τις απαιτήσεις

που παρατίθενται από τους κόμβους διαφορετικών περιοχών, ενώ έπειτα μπορούν να προβούν στις κατάλληλες ενέργειες για την ικανοποίηση αυτών των αναγκών, συμβάλλοντας στον περιορισμό της ανισορροπίας υπηρεσιών στους διαφορετικούς τομείς [11].

- **Πρόληψη της κυκλοφορίας ψευδών ειδήσεων**: Κατά τη διάρκεια της πανδημίας υπήρξε έντονο το φαινόμενο διασποράς ψευδών ειδήσεων και φημών, που αρκετές φορές περιείχαν επικίνδυνα μηνύματα για τους αναγνώστες. Ωστόσο, δεδομένου ότι πολλές πλατφόρμες κοινωνικής δικτύωσης χρησιμοποιούνται ως μέσο ενημέρωσης, καθίσταται ιδιαίτερα δύσκολη η παρακολούθηση της αυθεντικότητας των πληροφοριών που διαμοιράζονται σε καθεμία από αυτές. Ακόμα κι αν οι αρχές ανιχνεύσουν ένα μη πραγματικό μήνυμα, είναι σχεδόν αδύνατο να εντοπίσουν τον αρχικό διακινητή του. Η υλοποίηση ενός δημόσιου δικτύου blockchain ανταλλαγής πληροφοριών είναι μια πολλά υποσχόμενη λύση για τον περιορισμό της εξάπλωσης φημών, θεωριών συνωμοσίας, ψεύτικων ειδήσεων και επιθετικών παρατηρήσεων, καθώς όλα τα εμπλεκόμενα μέλη υπογράφουν με ψηφιακή υπογραφή το μήνυμά τους, ενώ οι αρχές διατηρούν το δικαίωμα ελέγχου και παρακολούθησης της ταυτότητας του αποστολέα και του περιεχομένου του μηνύματος. Αν και η χρήση συναινετικών αλγορίθμων διασφαλίζει ότι καμία ψευδή πληροφορία δεν θα εισχωρήσει στο δίκτυο, ακόμα κι αν συμβεί, οι αρχές μπορούν γρήγορα να εντοπίσουν τον αποστολέα του μηνύματος μέσω της ψηφιακής υπογραφής του [11].
- **Υποστήριξη μιας ασφαλούς πλατφόρμας δωρεών**: Στην Ινδία, μια ομάδα απατεώνων δημιούργησε ένα πλαστό τραπεζικό λογαριασμό με ίδιο όνομα με τον λογαριασμό που δημοσίευσε ο Ινδός πρωθυπουργός με σκοπό να αποσπάσει τις δωρεές που είχαν συγκεντρωθεί. Επομένως, απαιτείται μια ασφαλής και διαφανής πλατφόρμα δωρεών για την εξάλειψη κάθε αμφιβολίας γύρω από την εγκυρότητα και τη διαφάνεια των υφιστάμενων πλατφορμών δωρεών. Διάφορες πλατφόρμες crowdfunding που βασίζονται στη τεχνολογία blockchain έχουν προταθεί την περίοδο της πανδημίας, εξασφαλίζοντας μια ασφαλή και διαφανή συλλογή χρημάτων [11].
- **Περιορισμό διαταραχών στην εφοδιαστική αλυσίδα**: Η εμφάνιση του COVID-19 επέφερε αναταράξεις στο διεθνές εμπόριο και τις αλυσίδες εφοδιασμού. Εν μέσω των μέτρων lockdown που επιβλήθηκαν σε πολλές χώρες, οι περισσότεροι οργανισμοί σε όλο τον κόσμο αντιμετώπισαν σημαντικές δυσκολίες στη διατήρηση της ροής αγαθών και υπηρεσιών. Τεχνολογίες, όπως το blockchain, αναγνωρίζονται ως μεταρρυθμιστές των εμπορικών δικτύων και ως παράγοντες ανθεκτικότητας της αλυσίδας εφοδιασμού σε αντίστοιχες καταστάσεις έκτακτης ανάγκης στο μέλλον. Τα τελευταία χρόνια έχουν γίνει αρκετές προσπάθειες ενσωμάτωσης του blockchain στις αλυσίδες εφοδιασμού, σε μια προσπάθεια οι διάφοροι οργανισμοί να αυξήσουν την ορατότητα της εφοδιαστικής αλυσίδας. Στα υπάρχοντα συστήματα, ακόμα κι αν οι κατασκευαστές είναι εξοικειωμένοι με τις δυσκολίες που αντιμετωπίζουν οι προμηθευτές τους, ενδέχεται να αγνοούν

τις προκλήσεις που αντιμετωπίζουν οι συνεργάτες των προμηθευτών τους. Ωστόσο, λόγω της ανασφάλειας της απώλειας ανταγωνιστικού πλεονεκτήματος, οι προμηθευτές μπορεί να διστάζουν να επικοινωνήσουν τα στοιχεία του συνεργάτη τους. Για το λόγο αυτό, οι άδειες χρήσης του blockchain καθιστούν εφικτό το διαμοιρασμό δεδομένων από τον προμηθευτή δίχως να αποκαλύπτεται η πραγματική ταυτότητα του συνεργάτη του [11].

Κεφάλαιο 2ο: Διαδίκτυο των Πραγμάτων (IoT)

2.1 Εισαγωγή στην έννοια του IoT

Ο πρώτος που οραματίστηκε την έννοια του Διαδικτύου των Πραγμάτων ήταν ο Nikola Tesla, το 1926, όταν ανέφερε σε μια συνέντευξή του στο περιοδικό Colliers Magazine τον όρο «connected world». Πιο συγκεκριμένα, ο μεγάλος φυσικός διατύπωσε το εξής:

> «When wireless is perfectly applied, the whole Earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole [...] and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket»

Ο πρώτος που χρησιμοποίησε τον όρο Internet of Things (IoT) ήταν ο Kevin Ashton, το 1999, στο πλαίσιο της διαχείρισης της εφοδιαστικής αλυσίδας μέσω ραδιοσυχνοτήτων (RFID) – ετικέτες ή barcodes προσαρμοσμένες στα αντικείμενα (things) – με στόχο την βελτιωμένη αξιοπιστία και εγκυρότητα πληροφοριών στις επιχειρήσεις. Ο Βρετανός μηχανικός τεχνολογίας είχε γράψει στο RFID Journal:

> «If we had computers that knew everything there was to know about things – using data they gathered without any help from us – we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best»

Την ίδια χρονιά (1999) ο Neil Gershenfeld δημοσίευσε το έργο του «When Things Start to Think», στο οποίο οραματίστηκε την εξέλιξη του Παγκόσμιου Ιστού ως μια κατάσταση όπου «things start to use the Net so that people don't need to» (τα πράγματα θα αρχίσουν να χρησιμοποιούν το δίκτυο, έτσι ώστε οι άνθρωποι να μην χρειάζεται να το κάνουν οι ίδιοι) [27].

Αναλογιζόμενοι το ευρύ φάσμα των υλοποιήσιμων εφαρμογών, ο γενικότερος όρος «Net» (δίκτυο) φαίνεται να είναι καταλληλότερος από το «Internet» (διαδίκτυο), καθώς δεν πραγματοποιείται ολόκληρη η επικοινωνία μέσω του διαδικτύου. Συμπληρωματικά, η αλληλεπίδραση αυτή μπορεί να συμβαίνει αποκλειστικά μεταξύ πραγμάτων/συσκευών (things/devices), αλλά και μεταξύ πραγμάτων και ανθρώπων. Για να καταλήξουμε στο γεγονός ότι ο περισσότερο κατάλληλος όρος θα ήταν το «Internet of Everything» ή «Net of Everything», αντί για το «Internet of Things» που τελικά έχει επικρατήσει.

Ο πιο γνωστός οραματιστής του ψηφιακού και διασυνδεδεμένου φυσικού κόσμου, ο Mark Weiser, ισχυρίστηκε ότι ο κόσμος των πραγμάτων σχεδιάστηκε για να εξυπηρετεί τους ανθρώπους με διακριτικό τρόπο. Η αλληλεπίδραση αυτή μπορεί να συμβεί καθημερινά, με ψηφιακά επαυξημένο τρόπο, μέσω φυσικών αντιδράσεων, αισθήσεων και προφορικού λόγου. Η ολοένα και μεγαλύτερη συρρίκνωση των

τεχνολογικών στοιχείων (miniaturization) και η ενσωμάτωσή τους σε αντικείμενα δίχως παρεμβολές προς όφελος των χρηστών φαίνεται να γίνεται πραγματικότητα. Στο δοκίμιό του (1991) «The Computer for the 21st Century», ο Mark Weiser εξέφρασε για πρώτη φορά αυτό το όραμα ενώ ήταν επικεφαλής τεχνολογίας στο Ερευνητικό Κέντρο Xerox Palo Alto, το οποίο ο ίδιος αναφέρει ως «Ubiquitous Computing» ή «Ubicomp», με την εργασία του να κατατάσσεται μεταξύ των πιο συχνά αναφερόμενων ακαδημαϊκών εργασιών στους συναφείς κλάδους που προσβλέπουν σε ένα διασυνδεδεμένο κόσμο καθημερινών πραγμάτων.

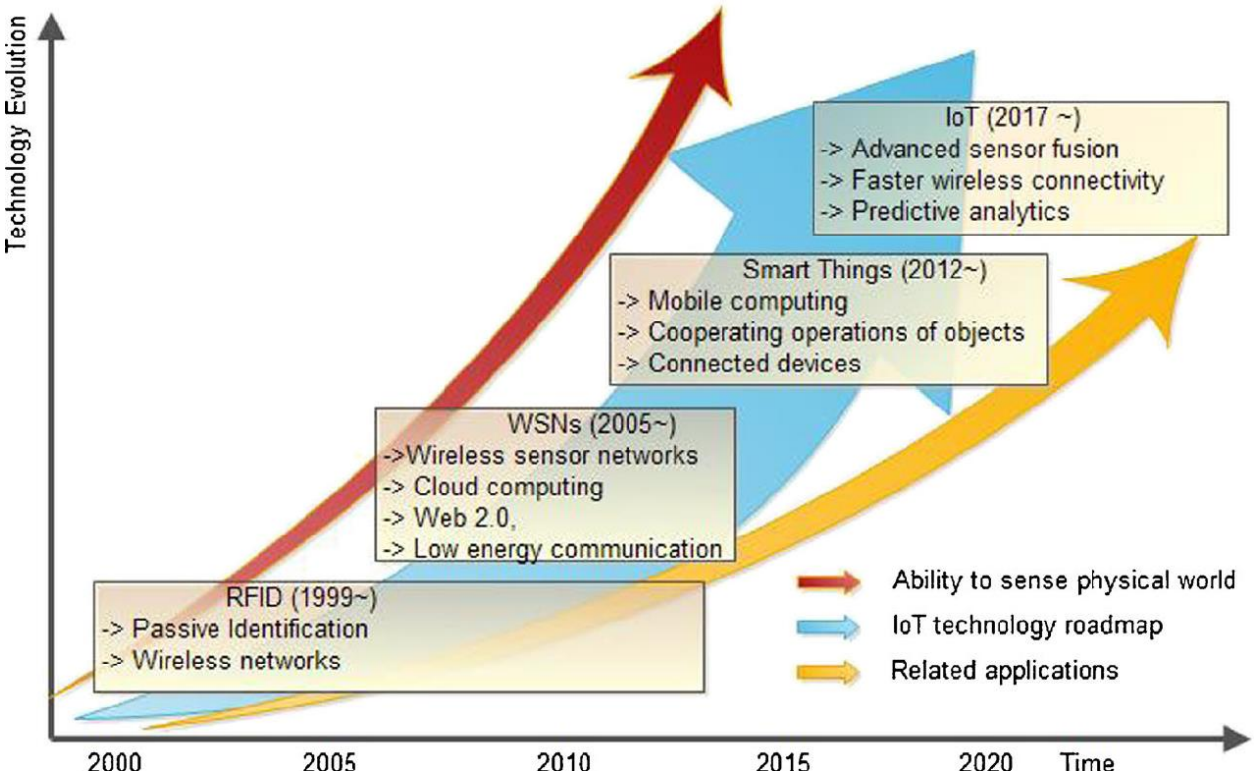
Το Διαδίκτυο των Πραγμάτων (IoT) βρίσκεται στο επίκεντρο επικαλυπτόμενων τεχνολογιών με προσανατολισμό στο διαδίκτυο (middleware), τα πράγματα (αισθητήρες) και τη σημασιολογική γνώση. Συγκεκριμένα, (i) ο προσανατολισμός στο Διαδίκτυο, δίνει έμφαση στο πρότυπο δικτύωσης, αξιοποιεί την καθιερωμένη δικτυακή υποδομή με βάση τις διευθύνσεις IP και αναπτύσσει πρωτόκολλα χαμηλών απαιτήσεων για την κάλυψη των ιδιαιτεροτήτων του IoT, προκειμένου να επιτευχθεί αποτελεσματική σύνδεση μεταξύ συσκευών, (ii) ο προσανατολισμός στα πράγματα, επικεντρώνεται σε φυσικά αντικείμενα και στην εύρεση μέσων με σκοπό την αναγνώριση και την ενσωμάτωση στον εικονικό κόσμο και (iii) ο προσανατολισμός στη σημασιολογική γνώση, στοχεύει στη χρήση σημασιολογικών τεχνολογιών, τη κατανόηση των αντικειμένων και των δεδομένων τους όσον αφορά την παρουσίαση, αποθήκευση, διασύνδεση και διαχείριση του τεράστιου όγκου πληροφοριών που παρέχεται από τον αυξανόμενο αριθμό αντικειμένων IoT.

Ο ορισμός του Διαδικτύου των Πραγμάτων (IoT), σύμφωνα με το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών, αρχικά είχε διαφοροποιηθεί σε δύο εκδοχές ανάλογα με το μέγεθος κλίμακας (μικρής και μεγάλης), που ενοποιήθηκαν στον παρακάτω:

> Το Διαδίκτυο των Πραγμάτων (IoT) είναι ένας κόσμος διασυνδεδεμένων αντικειμένων που είναι ικανά να ανιχνεύσουν, να ενεργοποιήσουν και να επικοινωνήσουν μεταξύ τους και με το περιβάλλον (δηλαδή, έξυπνα πράγματα ή έξυπνα αντικείμενα), ενώ παρέχουν τη δυνατότητα να μοιράζονται πληροφορίες, να ενεργούν εν μέρει αυτόνομα σε γεγονότα του πραγματικού/φυσικού κόσμου, να εκκινούν διαδικασίες και να δημιουργούν υπηρεσίες με ή χωρίς την άμεση ανθρώπινη παρέμβαση.

Σκόπιμα παραλείπεται να αποσαφηνιστεί εάν αυτό το πλαίσιο θα πραγματοποιηθεί απαραίτητα σε πρότυπα πρωτόκολλα επικοινωνίας ή σε ένα ενοποιημένο σχήμα, παρόλο που η δεύτερη επιλογή διαφαίνεται σίγουρα ως η βέλτιστη, μπορεί να μην είναι απαραίτητη ή ακόμη και εφικτή ως λύση, δεδομένων των διαστάσεων και της πολυπλοκότητας ενός εξαιρετικά ετερογενούς ψηφιακού κόσμου διασυνδεδεμένων πραγμάτων [27].

Παρά τις διαφωνίες αναφορικά με τον ορισμό του IoT, ο όρος έχει συζητηθεί ευρέως, ενώ σχετικές τεχνολογίες έχουν αναπτυχθεί ταχύτατα από διάφορα ιδρύματα, όπως η έξυπνη ανίχνευση και τεχνικές ασύρματης επικοινωνίας, που ενσωματώθηκαν στο Διαδίκτυο των Πραγμάτων και βοήθησαν στην ανάδυση νέων ερευνητικών οριζόντων και προκλήσεων. Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU) ανέλυσε τις συνδυαζόμενες τεχνολογίες, τις πιθανές αγορές, τις αναδυόμενες προκλήσεις και τις επιπτώσεις του IoT, με σκοπό να διερευνήσει τις μελλοντικές επεκτάσεις στην καθημερινή ζωή των ανθρώπων [20].



Σχήμα 2.1: Η εξέλιξη του Διαδικτύου των Πραγμάτων (IoT) (Πηγή: [20])

Το Διαδίκτυο των Πραγμάτων είναι ένας συνδυασμός της τεχνολογικής καινοτομίας και της ανθρώπινης έλξης για περισσότερη και συνεχώς αυξανόμενη συνδεσιμότητα με οτιδήποτε υπάρχει στο άμεσο και ευρύτερο περιβάλλον – επεκτείνοντας τη λογική της υπολογιστικής ισχύος σε ένα ενιαίο μηχανισμό περιβάλλοντος: «το περιβάλλον ως μια διεπαφή». Αυτός ο συνδυασμός push-pull πληροφοριών το καθιστά δυναμικό, γρήγορο, εξαιρετικά ανατρεπτικό και επί της ουσίας εξελικτικά ασταμάτητο [8].

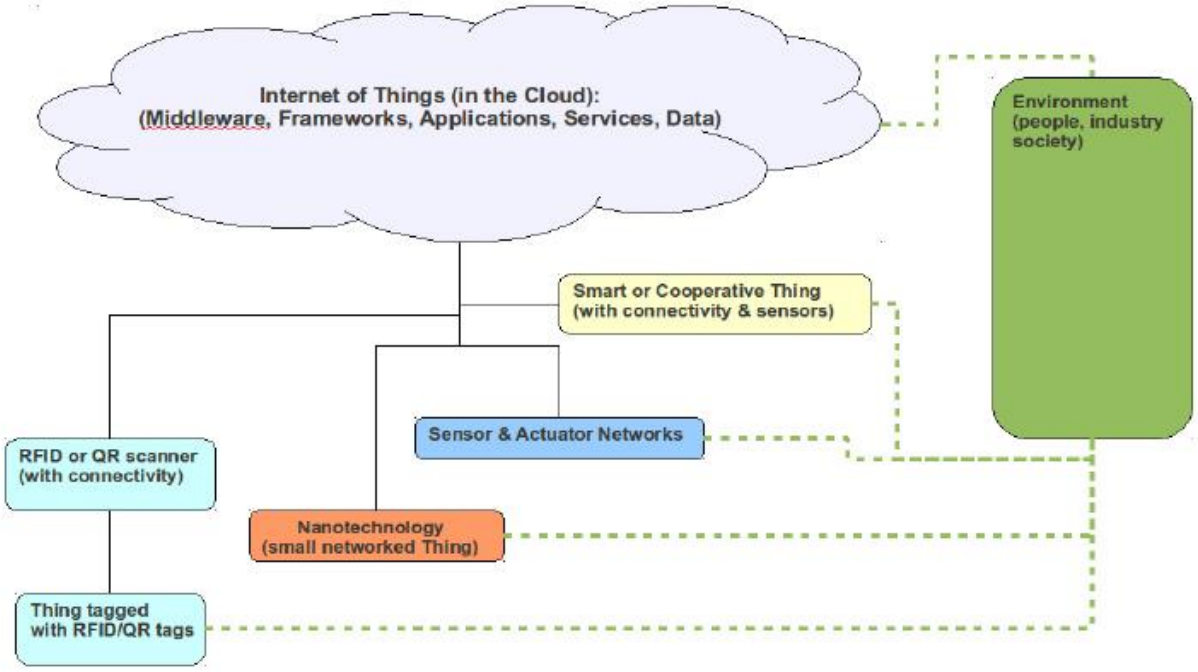
Η Mireille Hildebrandt, μια Ολλανδή καθηγήτρια πανεπιστημίου που ασχολείται με τις επιπτώσεις των αναδυόμενων τεχνολογιών και των κανονισμών δικαίου, είχε δηλώσει ότι «ίσως χρειαστεί να αναπτύξουμε έναν νόμο περί πραγμάτων (Ambient Law) που ενσωματώνεται στους αλγόριθμους και τις διεπαφές ανθρώπου - μηχανής που υποστηρίζουν την νοημοσύνη των πραγμάτων (Ambient Intelligence)

και για αυτό θα πρέπει να ξεπεράσουμε την παράλυσή μας, και να προετοιμαστούμε για τη συγγραφή ενός νέου σεναρίου».

Σε μια ομιλία στο Τεχνολογικό Συμβούλιο του Πίτσμπουργκ το 2009, ο Eric Schmidt, ένας Αμερικανός μηχανικός λογισμικού και εκτελεστικός διευθυντής της Google, εστίασε στις αρνητικές επιπτώσεις του (όπως το αποκάλεσε) θεσμικού κατακερματισμού στην καινοτομία και την τεχνολογική ολοκλήρωση. Αναρωτήθηκε εάν η διαδικασία χάραξης κυβερνητικής πολιτικής θα μπορούσε να επωφεληθεί από τους επαναληπτικούς κύκλους μέτρησης αποτελεσμάτων που χαρακτηρίζουν τους κύκλους της μηχανικής και το σχεδιασμό πρωτοτύπων. Με την παρακολούθηση αυτού του όγκου δεδομένων σε πραγματικό χρόνο και την ανάλυση συγκεντρωτικών αναφορών η πράξη διακυβέρνησης θα μπορούσε να επωφεληθεί. Συγκεκριμένοι νόμοι θα μπορούσαν να τεθούν σε ισχύ για 3 μήνες, να αξιολογηθούν και να προσαρμοστούν, ενώ στη συνέχεια, με βάση τα πραγματικά δεδομένα και όχι εκτιμήσεις, να προσαρμοστούν ξανά. Αυτή η διαδικασία θα μπορούσε να οδηγήσει σε συνδυαστική καινοτομία του συστήματος [8].

2.2 Το όραμα του IoT

Το όραμα IoT ενισχύει τη διασύνδεση από οποιοδήποτε μέρος, σε οποιοδήποτε χρόνο, για οποιονδήποτε χρήστη και για οποιαδήποτε συσκευή. Μόλις αυτά τα αντικείμενα συνδεθούν στο δίκτυο, είναι διαθέσιμες όλο και περισσότερες έξυπνες διαδικασίες και υπηρεσίες. Τα «πράγματα» θα μπορούσαν να επισημανθούν και μέσω σαρωτών, να αναγνωριστούν και να κοινοποιηθούν οι σχετικές πληροφορίες τοποθεσίας. Ομοίως, τα δικτυωμένα «πράγματα» με αισθητήρες γίνονται μικρότερα, εντάσσονται στην καθημερινότητά μας, ενώ οι αισθητήρες και ενεργοποιητές δικτύων ενεργούν στο τοπικό περιβάλλον, επικοινωνώντας την κατάσταση και τα γεγονότα σε μια υπηρεσία υψηλότερου επιπέδου. Τα έξυπνα «πράγματα» αντιλαμβάνονται τη δραστηριότητα και την κατάσταση του περιβάλλοντος μέσω της διασύνδεσής τους με το IoT. Το ενδιάμεσο λογισμικό και τα πλαίσια, που επιτρέπουν την ανάπτυξη εφαρμογών και υπηρεσιών, αξιοποιούν τα δεδομένα όπως αυτά λαμβάνονται από/για τα «πράγματα» και διατηρούνται στο cloud, προσθέτοντας νοημοσύνη και βελτιώνοντας τις παρεχόμενες υπηρεσίες, με το τελικό αντίκτυπο να αντικατοπτρίζεται στο γενικότερο περιβάλλον [13].



Εικόνα 2.2: Συστατικά στοιχεία του Διαδικτύου των Πραγμάτων (Πηγή: [13])

Η πρόβλεψη αναφέρει ότι σχεδόν τα πάντα θα είναι συνδεδεμένα στο δίκτυο. Μεμονωμένα αντικείμενα θα παρακολουθούνται, ενώ η κατάσταση και η θέση αυτών θα κοινοποιούνται σε πραγματικό χρόνο σε μια υπηρεσία υψηλότερου επιπέδου. Η ουσία έγκειται στην έξυπνη επεξεργασία του όγκου δεδομένων που συλλέγονται από την αλληλεπίδραση με το περιβάλλον, με στόχο την ενίσχυση των διαδικασιών λήψης αποφάσεων και εκτέλεσης ενεργειών [13].

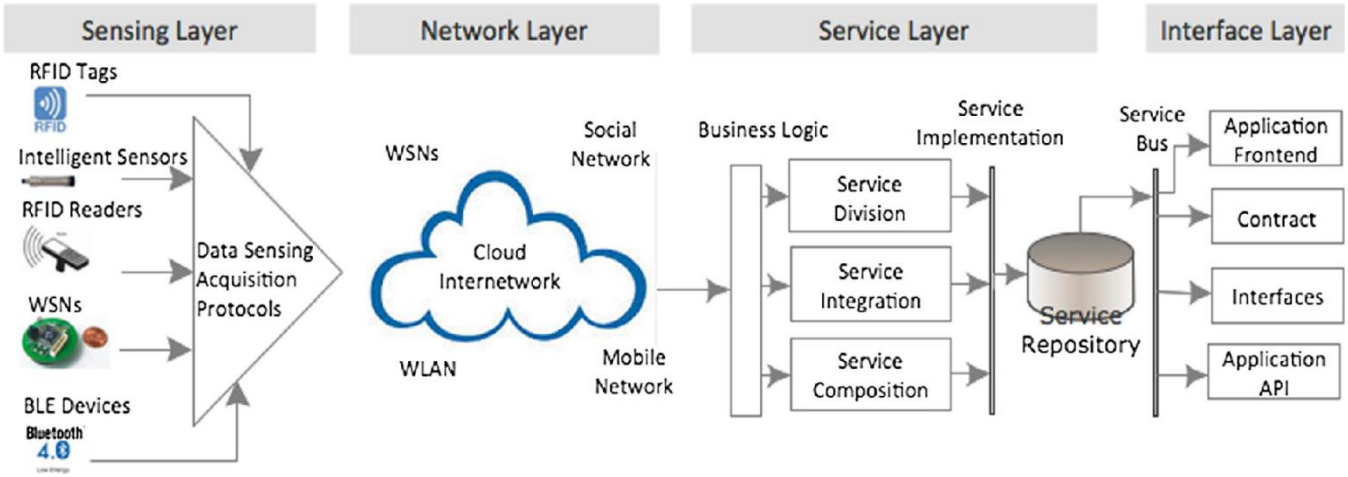
2.3 Αρχιτεκτονική IoT με προσανατολισμό στις υπηρεσίες

Η αρχιτεκτονική ενός συστήματος IoT πρέπει να εγγυάται την απρόσκοπτη λειτουργία του, η οποία γεφυρώνει το χάσμα μεταξύ του φυσικού και του εικονικού κόσμου. Ο σχεδιασμός της αρχιτεκτονικής IoT περιλαμβάνει παράγοντες όπως η δικτύωση, η επικοινωνία, τα επιχειρηματικά μοντέλα, τις διαδικασίες και την ασφάλεια, ενώ για την υλοποίησή της θα πρέπει να λαμβάνονται σοβαρά υπόψη η επεκτασιμότητα, η κλιμάκωση και η διαλειτουργικότητα μεταξύ των διαφόρων ετερογενών συσκευών και τεχνολογικών μοντέλων. Εξαιτίας του ότι τα «πράγματα» μπορεί να χρειάζεται να μετακινούνται γεωγραφικά και να αλληλεπιδρούν σε πραγματικό χρόνο, η αρχιτεκτονική του IoT θα πρέπει προσαρμόζεται με ευκολία έτσι ώστε να υποστηρίζεται η δυναμική αλληλεπίδραση και η σαφής επικοινωνία γεγονότων μεταξύ των συσκευών, διατηρώντας πάντοτε την αποκεντρωμένη και ετερογενή της φύση.

Στο Διαδίκτυο των Πραγμάτων, η αρχιτεκτονική με προσανατολισμό στις υπηρεσίες (Service-Oriented Architecture - SoA) μπορεί να καταστεί επιτακτική για τους παρόχους υπηρεσιών και τους χρήστες, με στόχο τη διασφάλιση της διαλειτουργικότητας μεταξύ των ετερογενών συσκευών με πολλούς τρόπους. Το παρακάτω σχήμα παρέχει ένα γενικό SoA, το οποίο αποτελείται από τέσσερα επίπεδα με διακεκριμένες λειτουργίες όπως παρουσιάζονται παρακάτω:

- Το επίπεδο αισθητήρων, όπου ενσωματώνονται τα διαθέσιμα αντικείμενα εξοπλισμού για την ανίχνευση της κατάστασης των πραγμάτων.
- Το επίπεδο δικτύου, που περιλαμβάνει τις υποδομές για την υποστήριξη της ασύρματης ή ενσύρματης σύνδεσης μεταξύ των συσκευών.
- Το επίπεδο υπηρεσιών, όπου αποτελείται από τη δημιουργία και διαχείριση των υπηρεσιών που απαιτούνται από τους χρήστες ή τις εφαρμογές.
- Το επίπεδο διεπαφής, που ενσωματώνει τις μεθόδους αλληλεπίδρασης με τους χρήστες ή τις εφαρμογές.

Η αρχιτεκτονική με προσανατολισμό στις υπηρεσίες (SoA) αποτελεί ένα σύνθετο σύστημα, που συντίθεται από ένα σύνολο καλά ορισμένων και απλών αντικειμένων ή υποσυστημάτων που μπορούν να διατηρηθούν και να λειτουργήσουν αυτόνομα. Ως εκ τούτου, τα συστατικά (λογισμικό και εξοπλισμός) σε ένα IoT μπορούν να επαναχρησιμοποιηθούν και να αναβαθμιστούν αποτελεσματικά, συντελώντας στην ευρεία εφαρμογή της αρχιτεκτονικής αυτής σε ασύρματα δίκτυα αισθητήρων. Η εφαρμογή της στο IoT παρέχει επεκτασιμότητα, κλιμάκωση, μεταβλητότητα και διαλειτουργικότητα μεταξύ ετερογενών πραγμάτων, συνοψίζοντας τις λειτουργίες και τις δυνατότητες του σε ένα κοινό σύνολο υπηρεσιών [20].



Σχήμα 2.3: Τα επίπεδα της αρχιτεκτονικής με προσανατολισμό στις υπηρεσίες στο Διαδίκτυο των Πραγμάτων (IoT) (Πηγή: [20])

2.3.1 Επίπεδο αισθητήρων

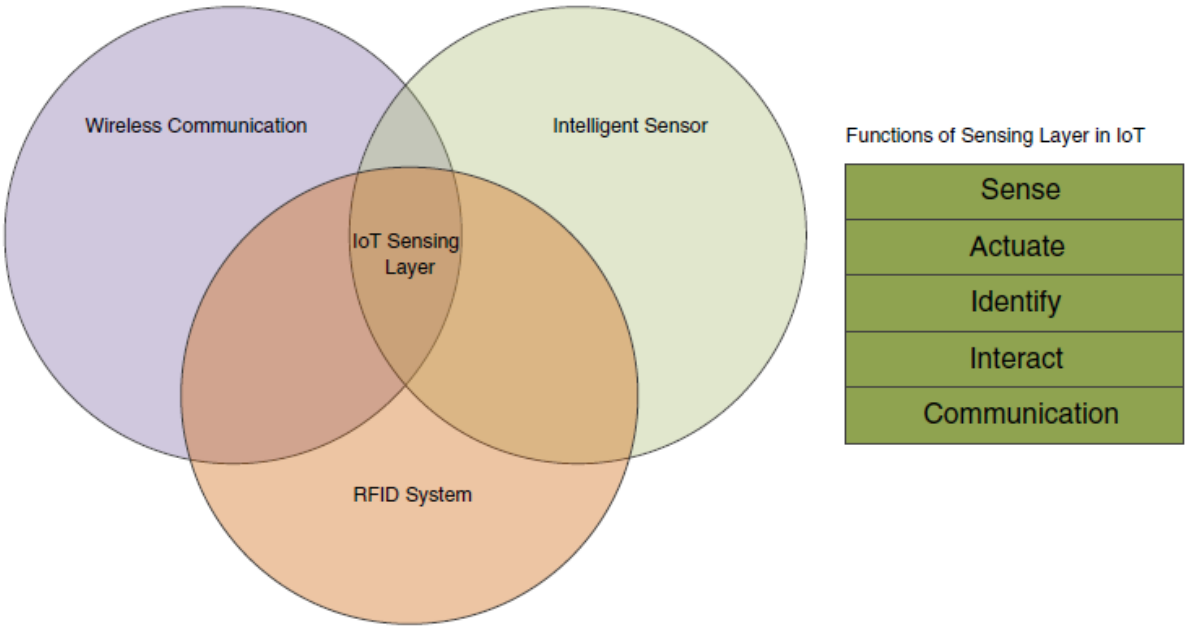
Τα τελευταία χρόνια, οι προηγμένες τεχνολογίες ανίχνευσης και επικοινωνίας έκαναν τις συσκευές με RFID ή αισθητήρες πιο ευέλικτες και προσβάσιμες, επεκτείνοντας σημαντικά τις ικανότητες του Διαδικτύου των Πραγμάτων, καθώς πλέον τα «πράγματα» μπορούν να αναγνωριστούν μοναδικά και να παρακολουθήσουν το περιβάλλον για διάφορους σκοπούς και εφαρμογές. Στον ψηφιακό κόσμο μέσω της τεχνικής εκχώρησης μοναδικής ταυτότητας που ονομάζεται Universal Unique Identifier (UUID), κάθε συσκευή στο IoT αποκτά μια ψηφιακή ταυτότητα, με τη συνδρομή της οποίας μπορεί να παρακολουθείται από το σύστημα με ευκολία. Συγκεκριμένα, το UUID είναι κρίσιμο για την επιτυχημένη ανάπτυξη υπηρεσιών σε ένα τεράστιο δίκτυο όπως αυτό του Διαδικτύου των Πραγμάτων. Επίσης, τα αναγνωριστικά ενδέχεται να αναφέρονται σε ονόματα και διευθύνσεις [20].

Σημαντικές πτυχές που θα πρέπει να προσδιοριστούν στο επίπεδο αισθητήρων είναι:

- το κόστος, το μέγεθος, οι πόροι και η κατανάλωση ενέργειας: Λόγω του μεγάλου αριθμού αισθητήρων σε ένα πολύπλοκο σύστημα IoT, οι έξυπνες συσκευές θα πρέπει να έχουν σχεδιαστεί με στόχο την ελαχιστοποίηση των απαιτούμενων πόρων.
- η ανάπτυξη: Τα αντικείμενα ανίχνευσης (ετικέτες RFID, αισθητήρες κ.ά.) μπορούν να αναπτυχθούν μία φορά, σταδιακά ή τυχαία ανάλογα με τις απαιτήσεις των εφαρμογών.
- η ετερογένεια: Η ποικιλία των «πραγμάτων» με διαφορετικές ιδιότητες μπορεί να κάνει το Διαδίκτυο των Πραγμάτων πολύ ετερογενές.
- η επικοινωνία: Οι αισθητήρες πρέπει να έχουν τη δυνατότητα επικοινωνίας έτσι ώστε να κάνουν τα «πράγματα» προσβάσιμα και ανακτήσιμα.
- το δίκτυο: Τα «πράγματα» είναι οργανωμένα σε δίκτυα multi-hop, mesh ή ad hoc.

Επιπλέον, καθώς το Διαδίκτυο των Πραγμάτων επεκτείνεται, ένας μεγάλος αριθμός στοιχείων λογισμικού και εξοπλισμού μπορεί να συμπεριληφθεί, γεγονός που κάνει επιτακτική την αξιοποίηση των ακόλουθων χαρακτηριστικών:

- Ενεργειακή απόδοση: Οι αισθητήρες θα πρέπει να είναι ενεργοί όλη την ώρα για να λαμβάνουν δεδομένα σε πραγματικό χρόνο. Αυτό αποτελεί μια πρόκληση όσον αφορά την παροχή ρεύματος στους αισθητήρες. Οι αισθητήρες λόγω της υψηλής ενεργειακής τους απόδοσης μπορούν να λειτουργήσουν για μεγαλύτερο χρονικό διάστημα δίχως διακοπή υπηρεσιών.
- Πρωτόκολλα: Διαφορετικά πράγματα που υπάρχουν στο IoT παρέχουν πολλαπλές λειτουργίες συστημάτων. Το IoT πρέπει να υποστηρίζει τη συνύπαρξη διαφορετικών επικοινωνιών όπως WLAN, ZigBee και Bluetooth.



Σχήμα 2.4: Λειτουργίες του επιπέδου αισθητήρων στο IoT (Πηγή: [20])

2.3.2 Επίπεδο δικτύου

Το επίπεδο δικτύου στο IoT συνδέει όλες τις συσκευές μεταξύ τους, επιτρέποντάς τους να γνωρίσουν το περιβάλλον τους. Μέσω του επιπέδου δικτύου, τα «πράγματα» μπορούν να διαμοιράζονται δεδομένα με τις συνδεδεμένες συσκευές, γεγονός που αποτελεί το πρωταρχικό στάδιο για την έξυπνη διαχείριση, επεξεργασία και επικοινωνία συμβάντων στο IoT. Επιπλέον, το επίπεδο δικτύωσης μπορεί να συλλέγει δεδομένα από άλλες υπάρχουσες υποδομές πληροφορικής, πληροφορίες που στη συνέχεια μεταδίδονται σε μονάδες λήψης αποφάσεων για τις πιο σύνθετες υπηρεσίες του υψηλότερου επιπέδου. Γενικά, τα «πράγματα» αναπτύσσονται σε ένα ετερογενές δίκτυο, στο οποίο μπορούν να ενσωματωθούν και άλλες συσκευές μέσω του διαδικτύου. Η επικοινωνία μέσω δικτύου ενδέχεται να περιλαμβάνει την Ποιότητα Υπηρεσιών (QoS) με σκοπό να εγγυηθεί την αξιοπιστία των σχετικών υπηρεσιών σε διαφορετικούς χρήστες ή εφαρμογές [20].

Από την άλλη μεριά, σημαντικά χαρακτηριστικά του δικτύου αποτελούν η αυτόματη ανακάλυψη και χαρτογράφηση των διαφόρων «πραγμάτων» στο δίκτυο, η αυτόματη ανάθεση ρόλων με σκοπό την ανάπτυξη, διαχείριση και προγραμματισμό της συμπεριφοράς των πραγμάτων, καθώς και η ικανότητα εναλλαγής ρόλων ανά πάσα στιγμή αυτό καταστεί απαιτητό. Έτσι, ενεργοποιείται η συνεργατικότητα κατά την εκτέλεση των διεργασιών.

Ανάμεσα στα ζητήματα που πρέπει να διευθετηθούν στο επίπεδο δικτύου, το απόρρητο των πληροφοριών και η ασφάλεια των προσωπικών δεδομένων είναι κρίσιμα λόγω της ανάπτυξης, της φορητότητας και της πολυπλοκότητάς τους. Για την εμπιστευτικότητα των πληροφοριών, η υπάρχουσα τεχνολογία κρυπτογράφησης που χρησιμοποιείται στα Wireless Sensor Networks (WSNs) μπορεί να επεκταθεί και να εφαρμοστεί στο IoT. Οι υπάρχουσες τεχνολογίες ασφάλειας δικτύων παρέχουν μια βάση για το απόρρητο και την ασφάλεια στο Διαδίκτυο των Πραγμάτων, αλλά η πρόοδος δεν έχει προσεγγίσει ακόμα το επιθυμητό επίπεδο [20].

2.3.3 Επίπεδο υπηρεσιών

Το επίπεδο υπηρεσιών βασίζεται στην τεχνολογία ενδιάμεσου λογισμικού (middleware), η οποία αποτελεί το κέντρο ενεργοποίησης των υπηρεσιών και εφαρμογών στο IoT, μια οικονομικά αποδοτική πλατφόρμα με επαναχρησιμοποιούμενο εξοπλισμό και λογισμικό.

Οι διεργασίες στο επίπεδο υπηρεσιών εκτελούνται απευθείας στο δίκτυο έτσι με στόχο τον αποτελεσματικό εντοπισμό των νέων υπηρεσιών μιας εφαρμογής και την δυναμική ανάκτηση των μετα-δεδομένων που σχετίζονται με αυτές. Διάφορα πρότυπα έχουν αναπτυχθεί από διαφορετικούς οργανισμούς εσωκλείοντας την πλειονότητα των προδιαγραφών, ενώ πρακτικά το επίπεδο υπηρεσιών αποτελείται από ένα σύνολο κοινών απαιτήσεων - με προσανατολισμό στην ελαχιστοποίηση αυτών - εφαρμογών, διεπαφών προγραμματισμού εφαρμογών (API) και πρωτοκόλλων, που υποστηρίζουν τις διάφορες εφαρμογές και υπηρεσίες.

Όλες οι δραστηριότητες με προσανατολισμό στις υπηρεσίες, όπως η ανταλλαγή και αποθήκευση πληροφοριών, η διαχείριση των δεδομένων, η βάση δεδομένων οντολογιών, οι μηχανές αναζήτησης και η επικοινωνία, εκτελούνται στο επίπεδο υπηρεσιών. Οι δραστηριότητες αυτές διεξάγονται βάσει των ακόλουθων στοιχείων:

- Η ανακάλυψη υπηρεσίας (service discovery) βρίσκει τα αντικείμενα που μπορούν να παρέχουν τις απαιτούμενες υπηρεσίες και πληροφορίες με αποτελεσματικό τρόπο.
- Η σύνθεση υπηρεσίας (service composition) επιτρέπει την αλληλεπίδραση μεταξύ συνδεδεμένων «πραγμάτων». Η ανακάλυψη εκμεταλλεύεται τις συσχετίσεις των «πραγμάτων» για να εντοπίσει την επιθυμητή υπηρεσία, ενώ η σύνθεση υπηρεσίας προγραμματίζει ή συνδυάζει μια πιο κατάλληλη υπηρεσία για να εξασφαλίσει τις υπηρεσίες με την υψηλότερη αξιοπιστία.
- Η διαχείριση αξιοπιστίας (trustworthiness management) προορίζεται για την κατανόηση του τρόπου σύνδεσης και επεξεργασίας των πληροφοριών που προέρχονται από άλλες υπηρεσίες.
- Οι διεπαφές προγραμματισμού εφαρμογών υπηρεσίας (Service APIs) παρέχουν τις αλληλεπιδράσεις αναφορικά με τις υπηρεσίες που απαιτούνται από τους χρήστες [20].

2.3.4 Επίπεδο διεπαφής

Στο Διαδίκτυο των Πραγμάτων (IoT), εμπλέκεται ένας μεγάλος αριθμός συσκευών, που μπορεί να προέρχονται από διαφορετικούς προμηθευτές και να μην ακολουθούν πάντα τα ίδια πρότυπα. Το ζήτημα της συμβατότητας μεταξύ των ετερογενών «πραγμάτων» (ανταλλαγή πληροφοριών, επικοινωνία και επεξεργασία γεγονότων) πρέπει να διευθετηθεί με στόχο την επιτυχή αλληλεπίδραση μεταξύ των συσκευών. Ως εκ τούτου, είναι εμφανής η ανάγκη για την εφαρμογή ενός αποτελεσματικού μηχανισμού διεπαφών που να απλοποιεί τη διαχείριση και διαλειτουργικότητα των «πραγμάτων».

Ένα προφίλ διεπαφής (IFP) μπορεί να ληφθεί ως ένα υποσύνολο του προτύπου υπηρεσιών, όπου είναι επιτρεπτή η ελάχιστη αλληλεπίδραση με τις εφαρμογές που εκτελούνται στο αντίστοιχο επίπεδο. Τα προφίλ διεπαφών χρησιμοποιούνται για την περιγραφή προδιαγραφών μεταξύ των διαφόρων εφαρμογών και υπηρεσιών. Μια υλοποίηση αυτού του επιπέδου είναι το Universal Plug and Play (UPnP), το οποίο προσδιορίζει ένα πρωτόκολλο για την απρόσκοπτη αλληλεπίδραση μεταξύ ετερογενών «πραγμάτων» [20].

2.4 Τεχνολογίες που αξιοποιούνται στο IoT

2.4.1 Τεχνολογία αναγνώρισης και εντοπισμού RFID

Η έννοια του IoT επινοήθηκε με βάση τις τεχνολογίες αναγνώρισης και παρακολούθησης με χρήση RFID. Εξαιτίας της ικανότητας να αναγνωρίζουν, ανιχνεύουν και παρακολουθούν, τα συστήματα RFID έχουν εφαρμοστεί ευρέως στη διαχείριση πόρων ή προϊόντων κατά την αποθήκευση και διαμετακόμιση, κοινώς ως logistics, όπως για παράδειγμα στη παρακολούθηση πακέτων, στη διαχείριση της εφοδιαστικής αλυσίδας, στις εφαρμογές υγειονομικής περίθαλψης κ.ά. Ένα σύστημα RFID θα μπορούσε να παρέχει επαρκείς πληροφορίες σε πραγματικό χρόνο σε συσκευές του IoT, οι οποίες θα καθίστανται ιδιαίτερα χρήσιμες για τους κατασκευαστές, τους διανομείς και τους μεταπωλητές. Για παράδειγμα, η ενσωμάτωση τεχνολογίας RFID στη διαχείριση της εφοδιαστικής αλυσίδας μπορεί να βελτιώσει τη διαχείριση αποθεμάτων, μειώνοντας το κόστος εργασίας, απλοποιώντας τις επιχειρηματικές διαδικασίες και βελτιώνοντας την απόδοση [20].

Το RFID χρησιμοποιείται για επικοινωνία μικρής εμβέλειας (10cm – 200m) και αποτελείται από έναν αναγνώστη και μια ετικέτα. Η ετικέτα υλοποιείται με χρήση ενός μικροτσίπ και μίας κεραίας. και προσδιορίζει μοναδικά ένα αντικείμενο/συσκευή (εξοπλισμός υγειονομικής περίθαλψης) στο περιβάλλον IoT. Ο αναγνώστης μεταδίδει ή λαμβάνει πληροφορίες επικοινωνώντας με την ετικέτα του αντικειμένου μέσω ραδιοκυμάτων. Σε ένα σύστημα Διαδικτύου των Πραγμάτων, τα δεδομένα που καταγράφονται στην ετικέτα έχουν τη μορφή ηλεκτρονικού κωδικού προϊόντος (EPC). Το RFID επιτρέπει τον άμεσο εντοπισμό και την συνεχή παρακολούθηση του εξοπλισμού υγειονομικής περίθαλψης από τους παρόχους

υγειονομικής περίθαλψης. Αποτελεί ένα εξαιρετικά ευάλωτο πρωτόκολλο όσο αφορά την ασφάλεια, που εμφανίζει προβλήματα συμβατότητας κατά τη σύνδεση με smartphone, με κύριο πλεονέκτημα της την ανεξαρτησία της από κάποια εξωτερική πηγή ενέργειας [25].

2.4.2 Ενσωμάτωση WSN και RFID

Αρκετοί τύποι έξυπνων αισθητήρων έχουν αναπτυχθεί στηριζόμενοι στις φυσικές αρχές υπέρυθρων, ακτινών γ, πίεσης, δονήσεων, ηλεκτρομαγνητικών, βιοαισθητήρων και ακτινών Χ, τα δεδομένα των οποίων μπορούν να ληφθούν και να ενσωματωθούν για αποθήκευση, λήψη αποφάσεων και ανάλυση. Η ενσωμάτωση αισθητήρων και RFID ενδυναμώνει το Διαδίκτυο των Πραγμάτων (IoT) στις υλοποιήσεις βιομηχανικών υπηρεσιών και στην περαιτέρω ανάπτυξη υπηρεσιών μέσω επεκτάσιμων εφαρμογών. Η ενοποίηση του IoT με RFID και WSN καθιστά δυνατή την ανάπτυξη εφαρμογών IoT στον τομέα της υγειονομικής περίθαλψη, τη λήψη αποφάσεων περίπλοκων συστημάτων και έξυπνων συστημάτων όπως έξυπνες μεταφορές, έξυπνες πόλεις ή έξυπνα συστήματα αποκατάστασης.

2.4.3 Πρωτόκολλα επικοινωνίας

Ο εξοπλισμός των συσκευών IoT περιλαμβάνει προδιαγραφές με σημαντικές διαφοροποιήσεις όσον αφορά την επικοινωνία, τον υπολογιστική λογική, τη μνήμη, τη χωρητικότητα αποθήκευσης δεδομένων και τη δυνατότητα μετάδοσής τους. Όλοι οι τύποι συσκευών (hardware) σε μια εφαρμογή IoT θα πρέπει να είναι καλά οργανωμένοι μέσω του δικτύου και να είναι προσβάσιμοι μέσω διαθέσιμης επικοινωνίας. Ακόμη, το Διαδίκτυο των Πραγμάτων μπορεί να είναι μια συνάθροιση ετερογενών δικτύων, όπως WSN, ασύρματα δίκτυα πλέγματος, δίκτυα κινητής τηλεφωνίας και WLAN. Επιπλέον, η αξιόπιστη επικοινωνία μεταξύ διαδικτυακής πύλης (gateway) και πραγμάτων είναι απαραίτητη για τη λήψη μιας κεντρικής απόφασης σχετικά με το IoT. Η πύλη έχει τη δυνατότητα να εκτελέσει τον αλγόριθμο περίπλοκης βελτιστοποίησης τοπικά εκμεταλλευόμενη τη γνώση του δικτύου της. Η υπολογιστική πολυπλοκότητα μετατοπίζεται από τα «πράγματα» στην διαδικτυακή πύλη, όπου μπορούν να διατηρηθούν οι βέλτιστες διαδρομές και τιμές παραμέτρων, λόγω του μεγέθους του τομέα πύλης σε σύγκριση με αυτό των «πραγμάτων» [20].

Τα χαρακτηριστικά εξοπλισμού και οι απαιτήσεις επικοινωνίας διαφέρουν από τον έναν τύπο συσκευής σε άλλο, όπως για παράδειγμα, ένα κινητό τηλέφωνο ή ένα tablet έχει πολύ καλύτερες δυνατότητες επικοινωνίας και υπολογιστικής ισχύος από μια άλλη ηλεκτρονική συσκευή συγκεκριμένης χρήσης, όπως ένα ρολόι παρακολούθησης καρδιακών παλμών. Έτσι, τα «πράγματα» μπορεί να έχουν πολύ διαφορετικές απαιτήσεις όσον αφορά την Ποιότητα της Υπηρεσίας (QoS), που μπορεί να συσχετίζονται με τους τομείς της χρονικής καθυστέρησης, της κατανάλωσης ενέργειας και της αξιοπιστίας. Επομένως, η ελαχιστοποίηση της κατανάλωσης ενέργειας για διεργασίες επικοινωνίας ή υπολογιστικών πράξεων

αποτελεί σημαντικό περιορισμό για τις συσκευές που τροφοδοτούνται από μπαταρία χωρίς εναλλακτικές τεχνικές συγκέντρωσης ενέργειας.

Το Διαδίκτυο των Πραγμάτων θα επωφεληθεί επίσης πολύ από τα υπάρχοντα πρωτόκολλα στο Διαδίκτυο όπως το IPv6. Τα πιο συχνά χρησιμοποιούμενα πρωτόκολλα και πρότυπα επικοινωνίας περιλαμβάνουν:

- RFID (π.χ. ISO 18000 6c EPC class 1 Gen2),
- NFC, IEEE 802.11 (WLAN), IEEE 802.15.4 (ZigBee),
- IEEE 802.15.1 (Bluetooth)
- Δίκτυα ασύρματων αισθητήρων/πλεγμάτων πολλαπλών βημάτων (Multihop Wireless Sensor/Mesh Networks)
- IETF Low power Wireless Personal Area Networks (6LoWPAN)
- Machine to Machine (M2M)
- Τεχνολογίες IP, όπως IP, IPv6, κ.ά. [20]

Communication Protocols	Transmission rate	Spectrum	Transmission range
RFID	424 kbps	135 Khz	>50 cm
		13.56 MHz,	>50 cm
		866–960 MHz	>3 m
		2.4 Ghz	>1.5 m
NFC	100 kbps–10 Mbps	2.45 GHz	
ZigBee	256 kbps/20 kbps	2.4 GHz/900 MHz	10 m
Bluetooth	1 Mbps	2.4 GHz	10 m
BLE	10 kbps	2.4 GHz	10 m
UWB	50 Mbps	Wide range	30 m
WiFi	50–320 Mbps	2.4/5.8 GHz	100 m
Wi-Max	70 Mbps	2–11 GHz	50 km
UMTS/CDMA/EDGE/MBWA	2 Mbps	896 MHz	~

Πίνακας 2.1: Πρωτόκολλα επικοινωνίας IoT και σχετικές πληροφορίες (Πηγή: [20])

Τα γνωστότερα πρότυπα επικοινωνίας για την ανταλλαγή δεδομένων μεταξύ εφαρμογών, συσκευών και αντικειμένων είναι το Bluetooth, το Wi-Fi και διάφορα πρότυπα κινητής επικοινωνίας, όπως το GSM που διέπουν τα δίκτυα δεύτερης γενιάς. Ωστόσο, οι περισσότερες εφαρμογές IoT αξιοποιούν συσκευές με περιορισμένους πόρους, γεγονός που οδήγησε στην τεχνολογία Δικτύων ευρείας περιοχής και χαμηλής ισχύος (LPWAN), που διακρίνεται για την ελάχιστη κατανάλωση ενέργειας και την χαρακτηριστική αυτονομία λειτουργίας τους. Το LPWAN είναι ένας διευρημένος όρος που εσωκλείει μια πληθώρα

τεχνολογιών που χρησιμοποιούνται για την επικοινωνία αισθητήρων και ελεγκτών στο διαδίκτυο, απαλλαγμένο από τα παραδοσιακά δικτύα Wi-Fi ή κινητής τηλεφωνίας.

Ταυτόχρονα, οι βιομηχανίες δικτύων κινητής τηλεφωνίας αναπτύσσουν περαιτέρω πρότυπα δικτύωσης κινητής τηλεφωνίας, όπως για παράδειγμα τα LTE-M και NB-IoT, με το τελευταίο να υποστηρίζεται από τους κορυφαίους κατασκευαστές και τους 20 μεγαλύτερους παρόχους κινητής τηλεφωνίας στον κόσμο. Περαιτέρω παραδείγματα δραστηριοτήτων που διαμορφώνουν νέα πρότυπα με καταλληλότητα χρήσης στο IoT περιλαμβάνουν το LoRa, το N-Wave και το Sigbox. Τα κυρίαρχα ζητήματα σχεδιασμού τους είναι η χαμηλή κατανάλωση ενέργειας (έως και περισσότερα από 10 χρόνια αυτονομίας), η ισχυρή ενσωμάτωση σε εσωτερικά περιβάλλοντα και η διασύνδεση μεγάλου αριθμού αισθητήρων και συσκευών με απαιτήσεις ζώνης χαμηλού εύρους [27].

Name	Frequency	Range	Examples	Standards
Bluetooth BLE	2.4 GHz	1–100 m >100 m	Headsets, wearables, sports and fitness, health care, proximity, automotive	IEEE 802.15.1[a] Bluetooth SIG [b]
EnOcean	315 MHz, 868 MHz, 902 MHz	300 m outdoor, 30 m indoors	Monitoring and control systems, building automation, transportation, logistics	ISO/IEC 14543-3-10[c]
GSM, LTE, LTE-M	Europe: 900 MHz and 1.8 GHz, USA: 1.9 GHz and 850 MHz		Mobile phones, asset tracking, smart meters, M2M	3GPP[d]
6LoWPAN	2.4 GHz	10–30 m	Automation and entertainment applications in home, office, and factory environments	Adaption layer for Ipv6 over IEEE802.15.4[e]
LoRa	Sub 1 GHz ISM band	2–5 km urban; 15 km suburban; 45 km rural	Smart city, long-range M2M	LoRaWAN[f]
NB-IoT (narrow-band-IoT)	700–900 MHz	10–15 km rural deep indoor penetration	Smart meters, event detectors, smart cities, smart homes, industrial monitoring	3GPP LTE Release 13[g]
NFC	13.56 MHz	Under 0.2 m	Smart wallets, smart cards, action tags, access control	ISO/IEC 18092[h] ISO/IEC 14443-2,-3,-4[i]
NWave	Sub 1 GHz ISM band	Up to 10 km	Agriculture, smart cities, smart meters, logistics, environmental	Weightless[j]
RFID	120–150 kHz (LF), 13.56 MHz (HF), 2450–5800 MHz (microwave), 3.1–10 GHz (microwave)	10 cm to 200 m	Road tolls, building access, inventory, goods tracking	ISO 18000[k]
DASH7	433 MHz (UHF), 865–868 MHz (Europe), 902–928 MHz (North America) UHF	0–5 km	Building automation, smart energy, smart city logistics	
SigFox[l]	900 MHz	3–10 km urban 30–50 km rural	Smart meters, remote monitoring, security	
Weightless	470–790 MHz	Up to 10 km	Smart meters, traffic sensors, industrial monitoring	Weightless[m]
Wi-Fi	2.4 GHz, 3.6 GHz, 4.9–5 GHz	Up to 100 m	Routers, tablets, smartphones, laptops	IEEE 802.11[n]
Z-Wave	ISM band 865–926 MHz	100 m	Monitoring and control for homes and light commercial environments	Z-Wave[o]; recommendation ITU G.9959[p]
ZigBee	2.4 GHz; 784 MHz in China, 868 MHz in Europe, and 915 MHz in USA and Australia	10–20 m	Home and building automation, WSN, industrial control	IEEE 802.15.4[q]

Πίνακας 2.2: Πρότυπα και πρωτόκολλα επικοινωνίας IoT (Πηγή: [27])

Bluetooth: Το Bluetooth είναι μια τεχνολογία ασύρματης επικοινωνίας μικρής απόστασης που χρησιμοποιεί ραδιοκύματα UHF (ultra-high frequency – υπερ-υψηλής συχνότητας) και επιτρέπει την ασύρματη σύνδεση μεταξύ δύο ή περισσότερων συσκευών. Το εύρος συχνοτήτων του πρωτοκόλλου Bluetooth είναι 2.4 GHz και το εύρος επικοινωνίας μπορεί να φτάσει έως και 100 m. Το Bluetooth παρέχει προστασία δεδομένων μέσω κρυπτογράφησης και ελέγχου ταυτότητας χρήστη, διακρίνεται για το χαμηλό κόστος και την υψηλή ενεργειακή του απόδοση, ενώ παράλληλα εξασφαλίζει σχετικά μικρή παρεμβολή κατά τη μετάδοση και λήψη δεδομένων μεταξύ των συνδεδεμένων συσκευών. Ωστόσο, όταν η εφαρμογή υγειονομικής περίθαλψης απαιτεί επικοινωνία μεγάλης εμβέλειας, δεν προτείνεται η χρήση αυτής της τεχνολογίας [25].

Zigbee: Το Zigbee είναι ένα από τα τυπικά πρωτόκολλα που διασυνδέει ιατρικές συσκευές, μεταδίδοντας πληροφορίες εκατέρωθεν, ενώ διαθέτει παρόμοιο εύρος συχνοτήτων με αυτό του Bluetooth (2.4 GHz) αλλά με υψηλότερο εύρος επικοινωνίας. Αυτή η τεχνολογία υιοθετεί μια τοπολογία δικτύου mesh, που αποτελείται από τερματικούς κόμβους (node), δρομολογητές και ένα κέντρο επεξεργασίας. Το κέντρο επεξεργασίας είναι υπεύθυνο για τη συγκέντρωση και ανάλυση δεδομένων, ενώ το δίκτυο mesh εξασφαλίζει την αδιάλειπτη σύνδεση μεταξύ των διαφόρων συσκευών ακόμα και όταν κάποιο σφάλμα εντοπιστεί σε αυτές. Τα πλεονεκτήματα αυτού του πρωτοκόλλου επικοινωνίας έγκεινται στη χαμηλή κατανάλωση ενέργειας, τον υψηλό ρυθμό μετάδοσης και την υψηλή χωρητικότητα δικτύου [25].

Near-Field Communication (NFC): Η βασική ιδέα του NFC είναι η ηλεκτρομαγνητική επαγωγή μεταξύ των κεραιών δύο κόμβων, τοποθετημένων σε κοντινή απόσταση. Αυτή η τεχνολογία είναι παρόμοια με την RFID που επίσης χρησιμοποιεί ηλεκτρομαγνητική επαγωγή για τη μετάδοση δεδομένων, αλλά διαθέτει πολύ μικρότερο εύρος επικοινωνίας. Οι συσκευές NFC μπορούν να λειτουργήσουν σε δύο καταστάσεις: ενεργή και παθητική λειτουργία. Στην κατάσταση της παθητικής λειτουργίας, μόνο μία συσκευή παράγει τη ραδιοσυχνότητα με την άλλη να λειτουργεί ως δέκτης, ενώ στην ενεργή λειτουργία και οι δύο συσκευές μπορούν να μεταδώσουν δεδομένα χωρίς σύζευξη. Προτείνεται για την εύκολη λειτουργία του και την αποτελεσματικότητα του ασύρματου δικτύου επικοινωνίας [25].

Wi-Fi: Το Wireless Fidelity (Wi-Fi) χρησιμοποιεί ραδιοκύματα για τη μετάδοση δεδομένων σε ένα δίκτυο, ακολουθεί το IEEE 802.11 b και IEEE 802.11 b/g/n πρότυπα, διαθέτει υψηλότερο εύρος μετάδοσης (έως 100 μέτρα) από το Bluetooth, έχοντας τη δυνατότητα δημιουργίας δικτύου εύκολα και γρήγορα. Η ευρεία εφαρμογή του Wi-Fi έγκειται στην υψηλή συμβατότητά του με έξυπνα κινητά και στην διασφάλιση ισχυρού επιπέδου ασφάλειας. Χαρακτηρίζεται από σχετικά υψηλότερη κατανάλωση ενέργειας και κάποια ασυνέπεια αναφορικά με τη σταθερότητα του δικτύου [25].

Δορυφορικά (Sateline): Η δορυφορική επικοινωνία φαίνεται να είναι πιο αποτελεσματική και ωφέλιμη σε απομακρυσμένες γεωγραφικές περιοχές (όπως αγροτικές περιοχές, βουνά, ωκεανοί κ.ά.) όπου άλλοι

τρόποι επικοινωνίας δεν μπορούν να λειτουργήσουν επαρκώς. Ο δορυφόρος λαμβάνει σήματα από το έδαφος, τα ενισχύει και στη συνέχεια τα αποστέλλει ξανά στη Γη. Το πλεονέκτημα της τεχνολογίας δορυφορικών επικοινωνιών περιλαμβάνει τη μεταφορά δεδομένων υψηλής ταχύτητας, την άμεση ευρυζωνική πρόσβαση, τη σταθερότητα και τη συμβατότητα της τεχνολογίας. Στα μειονεκτήματα εντάσσεται η υψηλή κατανάλωση ενέργειας συγκριτικά με τους άλλους τρόπους επικοινωνίας [25].

2.4.4 Πρωτόκολλα δικτύων

Πολλά πρωτόκολλα πολλαπλών επιπέδων για ασύρματα δίκτυα, όπως τα ασύρματα δίκτυα πλέγματος (WMNs) ή δίκτυα ad hoc (AHNs), δεν μπορούν να εφαρμοστούν στο Διαδίκτυο των Πραγμάτων. Αυτό οφείλεται στο γεγονός ότι η ετερογένεια του IoT έχει διαφοροποιήσει σε μεγάλο βαθμό τις ρυθμίσεις υλικού, τις απαιτήσεις QoS, τους στόχους και τις λειτουργίες του. Από την άλλη πλευρά, οι κόμβοι στο ασύρματο δίκτυο αισθητήρων (WSN) έχουν συνήθως παρόμοιες προδιαγραφές υλικού, παρόμοιες απαιτήσεις επικοινωνίας και κοινό στόχο. Επίσης, το Διαδίκτυο ενσωματώνεται στο IoT, κληρονομώντας μια κεντρική και ιεραρχική αρχιτεκτονική. Συγκριτικά, τα WSN, τα WMN και τα AHN έχουν σχετικά επίπεδες αρχιτεκτονικές δικτύου, καθώς σε αυτά τα δίκτυα οι κόμβοι επικοινωνούν με τη μέθοδο πολλαπλών βημάτων χωρίς την εμπλοκή του διαδικτύου [20].

2.4.5 Διαχείριση υπηρεσιών

Αναφέρεται στην υλοποίηση και διαχείριση των υπηρεσιών που συναντούν τις ανάγκες των χρηστών και των εφαρμογών, μέσω της αρχιτεκτονικής με προσανατολισμό στις υπηρεσίες (SoA) που προωθεί την ενθυλάκωση των υπηρεσιών. Η ενθυλάκωση επιτρέπει την λεπτομερή ανάλυση των υπηρεσιών, διατηρώντας τα συστατικά τους στην αφάνεια και κάτω από την ομπρέλα των ίδιων των υπηρεσιών. Η SoA, φανερώνοντας τη δυναμική φύση και την αξιοπιστία των εφαρμογών IoT, επιτρέπει σε αυτές την ενσωμάτωση ετερογενών αντικειμένων ως συμβατές υπηρεσίες, με γνώμονα την αποτροπή κάποιας πιθανής αποτυχίας του συστήματος από κατάργηση μιας συσκευής ή εξάντλησης της μπαταρίας του.

2.4.6 Προσδιορισμός χαρακτηριστικών υπηρεσίας

Οι υπηρεσίες προσδιορίζουν τη διαχείριση περιβάλλοντος και την ταξινόμηση αντικειμένων. Από οργανωτικής σκοπιάς, κάθε υπηρεσία μπορεί να αναγνωριστεί μοναδικά ως ένα εικονικό στοιχείο στο IoT, δημιουργώντας μια είδωλο για κάθε πραγματική συσκευή με τέτοιο τρόπο ώστε να είναι διαθέσιμος ο συνεχής συγχρονισμός τους. Επίσης, κάθε υπηρεσία IoT αποτελείται από ένα ή περισσότερα χαρακτηριστικά, τα οποία ορίζουν τις προδιαγραφές της υπηρεσίας, όπως δομή δεδομένων, άδεια, περιγραφικά στοιχεία κ.ά.

Στο πρότυπο Bluetooth SIG που κυκλοφορεί, μια υπηρεσία μπορεί να περιγραφεί με τη γλώσσα XML με στόχο την ευκολότερη ανταλλαγή με άλλο ενδιάμεσο λογισμικό. Το παράδειγμα της «Υπηρεσίας

Θερμομέτρου Υγείας», που φαίνεται στην παρακάτω εικόνα, παρέχει τις μετρήσεις του θερμομέτρου υγείας με ένα UUID (0x1809) χωρίς να γνωρίζει ο χρήστης πώς αποκτώνται τα σχετικά δεδομένα μέτρησης.

```
<?xml version="1.0" encoding="utf-8"?>
<service uuid = "1809">
  <uri>org.bluetooth.service.health_thermometer</uri>
  <description>Health Thermometer Service </description>
  <characteristic uuid = "2a1c", id = "xgatt_temperature_celsius">
    <description> Celsius temperature </description>
    <properties indicate = "true" />
    <value type = "hex"> 0000000000</value>
  </characteristic>
</service>
```

Εικόνα 2.5: Παράδειγμα υλοποίησης υπηρεσίας IoT με χρήση XML (Πηγή: [20])

Συνοψίζοντας, τα συστατικά μιας υπηρεσίας αποτελούνται από:

- τη δήλωση ορισμού, που περιγράφει τις ιδιότητες χαρακτηριστικών τιμών όπως η ανάγνωση, η εγγραφή, ο δείκτης, τους κανόνες και τους τύπους τιμών.
- τις εκχωρημένες τιμές για τις ιδιότητες.
- το περιγραφικό στοιχείο, που παρέχει βοηθητικές πληροφορίες σχετικά με τα χαρακτηριστικά.

2.4.7 Ασφάλεια και απόρρητο

Οι εφαρμογές του Διαδικτύου των Πραγμάτων (IoT) ενδέχεται να έρθουν αντιμέτωπες με διάχυτες απειλές, όπως επιθέσεις ετικετών RFID και διαρροές δεδομένων. Όσον αφορά τα συστήματα RFID, έχουν προταθεί διάφορα πρότυπα ασφαλείας και πρωτόκολλα επαλήθευσης ταυτότητας για την αντιμετώπιση απειλών ασφαλείας. Πιο συγκεκριμένα, ο Juels (2006) πρότεινε τη μέθοδο της «ετικέτας μπλοκ» για την πρόληψη ανίχνευσης δίχως εξουσιοδότηση. Από την άλλη πλευρά, χαμηλού κόστους αλγόριθμοι κρυπτογράφησης συμμετρικού κλειδιού, όπως ο Tiny Encryption Algorithm (TEA) και το Advance Encryption Standard (AES), έχουν προταθεί για την προστασία απορρήτου κατά την διαδικασία ανταλλαγής δεδομένων. Η χαμηλού κόστους ετικέτα RFID μέσω της εφαρμογής κάποιου αλγορίθμου κρυπτογράφησης ασύμμετρου κλειδιού, που ονομάζεται αλγόριθμος κρυπτογράφησης ελλειπτικής καμπύλης (ECC) κατάφερε να αναβαθμίσει το επίπεδο ασφαλείας. Επίσης, τα πρωτόκολλα ασφαλείας που αφορούσαν τα δίκτυα WSN μπορούν να ενσωματωθούν με ευκολία στα συστήματα IoT. Η προσαρμογή των υφιστάμενων προτύπων διαδικτύου στην εφαρμογή διαλειτουργικών πρωτοκόλλων καθώς και η διασφάλιση ασφάλειας σύνθετων υπηρεσιών χρήζουν περαιτέρω ανάλυσης. Οι προκλήσεις

που αφορούν την προστασία απορρήτου συνοψίζονται στην ανθεκτικότητα σε επιθέσεις, τον έλεγχο ταυτότητας δεδομένων, τον έλεγχο πρόσβασης και την προστασία του απορρήτου του χρήστη [20].

2.4.8 Γεωγραφικός εντοπισμός (localization)

Για τον τοπογραφικό προσδιορισμό μπορούν να χρησιμοποιηθούν τεχνικές εντοπισμού, που είτε εντοπίζουν το αντικείμενο με εξωτερικό τρόπο, είτε το ίδιο καθορίζεται μόνο του. Παραδείγματα συστημάτων εντοπισμού θέσης είναι το Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS) των Ηνωμένων Πολιτειών, το GLONASS (Ρωσία), το Galileo (Ευρωπαϊκή Ένωση) και το BeiDou (Κίνα). Ο γεωγραφικός εντοπισμός διακρίνεται σε τέσσαρις τύπους:

- Trilateration: οι αποστάσεις υπολογίζονται με τουλάχιστον τρία σημεία, η θέση των οποίων είναι γνωστή, ενώ για τον προσδιορισμό της θέσης γίνεται χρήση της γεωμετρικής τομής. Τον τύπο αυτό το συναντάμε σε απλά δίκτυα μέσω των χρόνων διάδοσης των εκπεμπόμενων σημάτων.
- Triangulation: ο υπολογισμός των αποστάσεων και των θέσεων γίνεται με χρήση γωνιών ή κατευθυντικών διαστάσεων.
- Next known point: η θέση καθορίζεται βάσει του επόμενου γνωστού σημείου του περιβάλλοντος. Αυτή η μέθοδος εφαρμόζεται ήδη σήμερα στη κινητή τηλεφωνία των δικτύων GSM, μέσω ανάθεσης σε μια κινητή ραδιοσυχνότητα.
- Footprint: η θέση καθορίζεται με βάση συγκεκριμένα χαρακτηριστικά της οπτικής γωνίας (αποτύπωμα) ως ανάλυση σκηνικού, που μπορεί να είναι πραγματικές εικόνες κάποιας θέσης, από κάποια συγκεκριμένη γωνία θέασης. Αυτά τα χαρακτηριστικά οπτικής γωνίας μπορούν να αποθηκεύσουν τις τιμές τους εκ των προτέρων σε έναν πίνακα, όπως συμβαίνει για παράδειγμα, με τις ηλεκτρομαγνητικές τιμές ή προδιαγραφές ακτινοβολίας σε ένα ή περισσότερα WLAN.

Προκλήσεις της διαδικασίας εντοπισμού αποτελούν η παρακολούθηση αντικειμένων σε κίνηση, η διαχείριση καλυμμένων ή εσωτερικών στοιχείων σε αντικείμενα (προβληματική με τον εντοπισμό θέσης GPS), η ακτινοβολία και η παραποίηση ραδιοκυμάτων. Ωστόσο, τα τελευταία χρόνια, έχει γίνει μεγάλη επένδυση σε τεχνολογίες εντοπισμού εσωτερικών χώρων [27].

Μέθοδοι γεωεντοπισμού εφαρμογών

Ο γεωεντοπισμός της τοποθεσίας των ανθρώπων μπορεί να πραγματοποιηθεί με πολλούς τρόπους, παρέχοντας ακριβείς εκτιμήσεις, εμφανίζοντας η κάθε μία μέθοδο τα πλεονεκτήματα και τα μειονεκτήματά της. Το παγκόσμιο σύστημα εντοπισμού θέσης (GPS) καταναλώνει μεγάλη ποσότητα ενέργειας. Ωστόσο, η ακρίβεια του GPS μπορεί να υποβαθμιστεί σοβαρά ανάλογα με τη θέση του δέκτη και των δορυφόρων, ειδικά σε εσωτερικούς χώρους. Στην έρευνα των Ng, Lam, Cheng και Shum αποδεικνύεται η χρησιμότητα του Received Signal Strength Indicator (RSSI) όσον αφορά τον εντοπισμό του χρήστη σε εσωτερικό περιβάλλον. Το κινητό του χρήστη είναι συνδεδεμένο στο Ασύρματο Τοπικό Δίκτυο (WLAN) και αποστέλλει ένα σήμα σε πολλά σημεία πρόσβασης σταθερής θέσης (APs), τα οποία στη συνέχεια συγχωνεύονται χρησιμοποιώντας έναν αλγόριθμο Center of Gravity (Κέντρο Βάρους). Ο αλγόριθμος αυτός, όταν είναι σωστά συντονισμένος, είναι ακριβής και αποτελεσματικός, αλλά μόνο εάν η κινητή συσκευή βρίσκεται μέσα στο κυρτό σκελετό που οριοθετείται από τα APs. Έτσι, εάν η πρώτη εκτιμώμενη τοποθεσία (με τη μέθοδο Center of Gravity) βρίσκεται εκτός της ζώνης πρωτεύουσας εκτίμησης, θα μεταβούμε σε άλλον αλγόριθμο εκτίμησης για τη θέση αυτή. Η αξιοπιστία των αποτελεσμάτων τοποθεσίας διασφαλίζεται μέσα από την ελαχιστοποίηση της κίνησης δεδομένων τοποθεσίας στο δίκτυο καθώς και κατά συνέπεια την μείωση της πιθανότητας υπερφόρτωσης του συστήματος εκτίμησης [24], [35].

Σε άλλη έρευνα ο Chawathe εξετάζει τη χρήση των φάρων Bluetooth-LE (Low Energy) – γνωστά και ως iBeacons - για την παρακολούθηση γεωγραφικής θέσης σε εσωτερικούς χώρους με εμπόδια και διαφορετικά κανάλια, συστήνοντας μια προσέγγιση βάσει δεδομένων και χρήση μεθόδων μηχανικής μάθησης για τη χαρτογράφηση ισχύος του σήματος. Το Bluetooth χρησιμοποιείται σχεδόν παντού, αλλά παρουσιάζει ένα πρόβλημα που σχετίζεται με την αντανάκλαση των σημάτων, καθιστώντας δύσκολη την ακριβή εκτίμηση των αποστάσεων [12].

Σε μια άλλη μελέτη παρουσιάζεται μια υπηρεσία παρακολούθησης χαμηλής ισχύος για συστήματα IoT, που ονομάζεται SensTrack και χρησιμοποιεί έναν αισθητήρα προσανατολισμού και ένα επιταχυνσιόμετρο για την παρακολούθηση της γεωγραφικής θέσης με πρόθεση να μειωθεί η χρήση της λειτουργίας GPS, το οποίο απαιτεί μεγαλύτερη κατανάλωση ενέργειας. Ο προσανατολισμός παρέχει τη δυνατότητα ανίχνευσης των σημείων αλλαγής κατεύθυνσης κατά τη διάρκεια της παρακολούθησης, ενώ η επιτάχυνση υποστηρίζει την εκτίμηση της τρέχουσας ταχύτητας του χρήστη και της απόστασης που έχει διανύσει από την τελευταία τοποθεσία του. Οι λειτουργίες αυτές βοηθούν το SensTrack να αποφασίσει πότε θα λάβει δειγματοληψία της θέσης μέσω GPS. Όσον αφορά τους εσωτερικούς χώρους το SensTrack ανακατασκευάζει τη διαδρομή με βάση τις καταγεγραμμένες δειγματοληψίες τοποθεσίας, συμπεριλαμβανομένων δειγματοληψιών GPS και WiFi. Πρόσφατα, η Apple και η Google ανακοίνωσαν

ότι θα χρησιμοποιούν το Bluetooth για τον εντοπισμό επαφών χρηστών iOS και Android, το οποίο οι χρήστες μπορούν να ενεργοποιήσουν ή απενεργοποιήσουν εύκολα και άμεσα [35], [39].

2.4.9 Τεχνολογία Blockchain

Το blockchain είναι μια αποκεντρωμένη τεχνολογία καθολικού (DLT) που χρησιμοποιεί κρυπτογραφία για την ασφαλή φιλοξενία εφαρμογών, αποθήκευση δεδομένων και ανταλλαγή πληροφοριών, αποκεντρωμένα και αμετάβλητα, χωρίς κεντρική αρχή. Η αποκεντρωμένη φύση της τεχνολογίας αυτής καθορίζει την επικοινωνία μεταξύ δύο μη αξιόπιστων συσκευών, με σκοπό την αποθήκευση των αλληλεπιδράσεων και της κατάστασης των ανταλλασσόμενων δεδομένων. Επίσης, το blockchain μπορεί να μειώσει σημαντικά τους κινδύνους που αντιμετωπίζουν οι χρήστες και να εξοικονομήσει κόστος από τις επιχειρηματικές διαδικασίες.

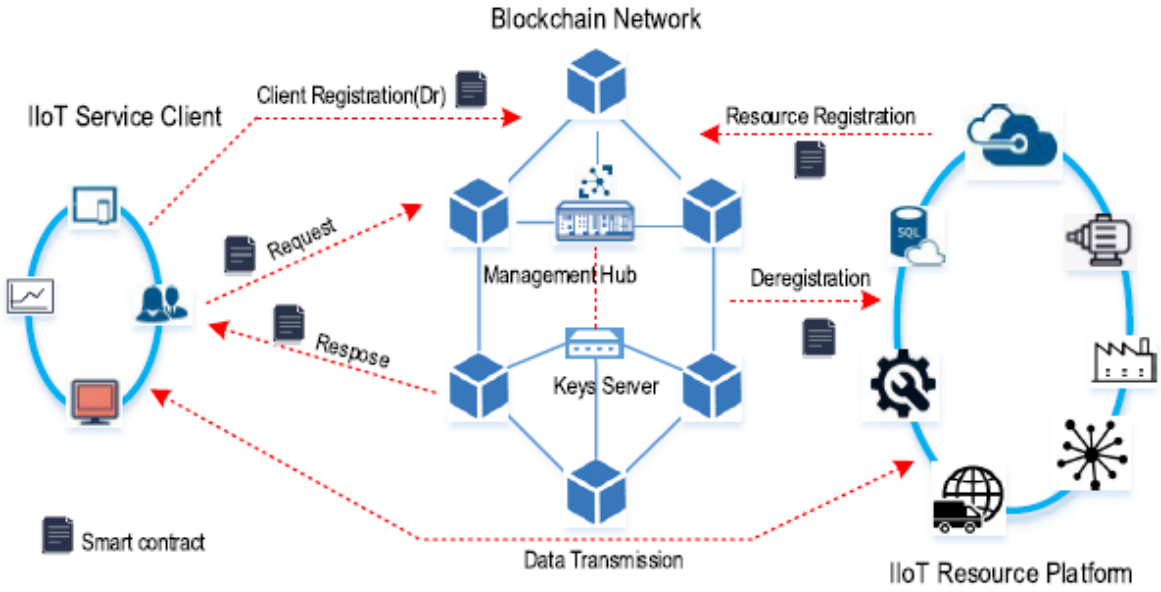
Γενικά, οι κόμβοι blockchain μπορούν να κατηγοριοποιηθούν σε πλήρη κόμβο (full node - FN) και κόμβο χαμηλών απαιτήσεων (lightweight node - LN), πιο συγκεκριμένα:

- FN: Μπορεί να κατεβάσει και να ελέγξει όλα τα μπλοκ (block) και τις συναλλαγές, ενώ μπορεί να λειτουργήσει ως κόμβος εξόρυξης και να δημιουργήσει μπλοκ για το blockchain.
- LN: Λόγω των περιορισμένων πόρων, ένα LN μπορεί να αποθηκεύσει και να επεξεργαστεί μόνο μέρος δεδομένων στο blockchain. Στο IoT, οι έξυπνες συσκευές (αισθητήρες) χαμηλών απαιτήσεων μπορούν να χρησιμεύσουν ως LN και να προτείνουν νέες συναλλαγές που θα διαδοθούν μεταξύ των κόμβων (nodes) και τελικά θα προστεθούν σε ένα μπλοκ στο blockchain.

Ένα σύστημα IoT περιλαμβάνει τόσο κόμβους χαμηλών απαιτήσεων (LN), όπως έξυπνους αισθητήρες, συσκευές ανάγνωσης και αναγνώρισης ραδιοσυχνοτήτων, έξυπνο μετρητή, όσο και δυναμικούς κόμβους (FN), όπως υπολογιστές βιομηχανικής χρήσης, διακομιστές ανάλυσης δεδομένων, διακομιστές υπολογιστικού πλέγματος. Οι κόμβοι LN μπορούν να συνδέσουν ομότιμους που εκτελούν ένα κόμβο FN έτσι ώστε να στείλει και να λάβει συναλλαγές, μπορούν να αποθηκεύσουν ελάχιστα δεδομένα σχετικά με το blockchain, αλλά μπορούν να στείλουν αιτήματα εξόδου, κωδικοποιημένα σε μηνύματα Πρωτοκόλλου Περιορισμένης Εφαρμογής σε ένα ή περισσότερα FN, κάνοντας χρήση JSON-RPC μέσω http, έτσι ώστε να γίνει κατανοητό από το δίκτυο blockchain. Στη συνέχεια, ο κόμβος FN στέλνει πίσω μια απάντηση που μπορεί να επαληθευτεί από το κόμβο LN, ελέγχοντας μόνο το δικό του διακριτικό (δεδομένα, καταστάσεις κ.τ.λ.), και εφόσον περάσει τον έλεγχο, ο κόμβος LN προχωρά στην κατασκευή των συναλλαγών. Εάν αποτύχει ο έλεγχος, ο κόμβος LN θα επιστρέψει μια μη έγκυρη απόκριση με τροποποιημένη έξοδο. Ο κόμβος LN μπορεί να ρωτήσει τον αντίστοιχο απομακρυσμένο FN για αποτελέσματα εξόδων και στη συνέχεια να μεταδώσει τις συναλλαγές του. Σε περιβάλλον IoT, ένα LN

μπορεί να δημιουργήσει συνδέσεις με πολλαπλούς μη αξιόπιστους κόμβους FN για να υποστηρίξει την ανάκτηση εξόδου, τη παραγωγή στοιχείων, τις δομικές ενημερώσεις και την επίλυση διενέξεων.

Ένα σύστημα blockchain-enabled IoT περιλαμβάνει τους δικτυακούς πόρους του IoT, το δίκτυο blockchain που καταγράφει όλες τις πληροφορίες του συστήματος, το κόμβο διαχείρισης (management hub), τους διακομιστές κλειδιών ασφαλείας που παράγουν τα απαραίτητα κλειδιά κρυπτογράφησης για την αυθεντικοποίηση των κόμβων και την κρυπτογράφηση των δεδομένων, τους χρήστες και τα έξυπνα συμβόλαια που παρέχουν τις διασυνδέσεις συστήματος μεταξύ των συστατικών IoT και Blockchain [41].



Εικόνα 2.6: Αρχιτεκτονική Blockchain-enabled IoT (Πηγή: [41])

Ένα έξυπνο συμβόλαιο είναι ένα αυτόματα εκτελέσιμο σενάριο και εφαρμόσιμο από FN και LN κόμβους που συμμετέχουν στη διαχείριση του blockchain. Στο IoT με δυνατότητα blockchain, η αλληλεπίδραση γίνεται μέσω διαμεσολάβησης των έξυπνων συμβάσεων, τα οποία μπορούν να κωδικοποιήσουν και να κατευθύνουν τις λογικές διαδικασίες με αποτελεσματικότητα και αξιοπιστία. Τα έξυπνα συμβόλαια στο Διαδίκτυο των Πραγμάτων ορίζουν τους κανόνες και τις κυρώσεις που σχετίζονται με μια συμφωνία, όπως ακριβώς κάνει μια παραδοσιακή σύμβαση χωρίς την παρεμβολή μεσάζοντα. Βασικά, ένα έξυπνο συμβόλαιο αποτελείται από τα παρακάτω κύρια στοιχεία: μέρη συμμετοχής (parties), συμβάντα ενεργοποίησης (triggering events) και ρυθμιστικές αρχές (regulators). Τα έξυπνα συμβόλαια μπορεί να προσφέρουν πολλά οφέλη στο IoT, όπως αυτονομία, εμπιστοσύνη, ιχνηλασιμότητα, ασφάλεια, αποτελεσματικότητα, ελεγκτική ικανότητα και ακρίβεια [41].

Κεφάλαιο 3ο: Διαδίκτυο των Ιατρικών Πραγμάτων (IoMT)

3.1 Εισαγωγή

Η αναγνώριση του IoMT ως ξεχωριστό τομέα του Διαδικτύου των Πραγμάτων, καθώς και οι προβλέψεις για εκτόξευση της αξίας του, σε συνδυασμό με την έξαρση της πανδημίας Covid-19, οδήγησε το 2021 στην επαναξιολόγησή της στα 136,8 δισεκατομμύρια δολάρια. Τα τελευταία χρόνια οι επιστήμονες της πληροφορικής προτείνουν την υλοποίησή της για την προστασία του απορρήτου των υγειονομικών αρχείων με την χρήση του IoMT [15].

Το σύστημα blockchain στον κλάδο της υγειονομικής περίθαλψης προτάθηκε για υψηλότερη ασφάλεια στο διαδίκτυο των πραγμάτων, με τη χρήση ιδιωτικού blockchain και έξυπνων συμβολαίων, ενώ οι αισθητήρες επικοινωνούν με την έξυπνη συσκευή και δημιουργούν εγγραφές με το πρωτόκολλο ethereum. Το μοντέλο συστήματος περιλαμβάνει τους παρακάτω κόμβους επικοινωνίας:

- Τον ασθενή που είναι εξοπλισμένος με διάφορες ιατρικές συσκευές, όπως ένα όργανο μέτρησης και έγχυσης ινσουλίνης ή ένα όργανο ελέγχου της πίεσης του αίματος.
- Μια έξυπνη συσκευή, όπως ένα έξυπνο τηλέφωνο ή tablet.
- Ένα έξυπνο συμβόλαιο, όπου μόνο καθορισμένοι κόμβοι μπορούν να εκτελέσουν και να επαληθεύσουν στο ιδιωτικό peer-to-peer δίκτυο blockchain.

Το μοντέλο IoMT, σε σύγκριση με τα παραδοσιακά μοντέλα, μπορεί να προστατεύσει το ιατρικό απόρρητο, μη επιτρέποντας τη συσχέτιση μεταξύ ασθενών και των δεδομένων τους [15].

Πρωταρχικό μέλημα των εφαρμογών υγειονομικής περίθαλψης αποτελεί το απόρρητο και η ασφάλεια λόγω της ευαίσθητης φύσης των δεδομένων που διακινούνται. Πολλοί νόμοι και ρυθμιστικά πρότυπα έχουν δημιουργηθεί για την εξασφάλιση του απορρήτου δεδομένων υγειονομικής περίθαλψης σε ηλεκτρονική μορφή, όπως πιο συγκεκριμένα ο νόμος περί φορητότητας και λογοδοσίας των πληροφοριών υγείας (HIPAA), που ψηφίστηκε από το Κογκρέσο των ΗΠΑ το 1996, ενσωματώνοντας ορισμένα βασικά μέτρα στην ασφάλεια των συστημάτων Ηλεκτρονικού Μητρώου Υγείας (EHR):

- Έλεγχος πρόσβασης: Περιλαμβάνει τους επιλεκτικούς περιορισμούς που σκοπό έχουν τον έλεγχο πρόσβασης σε δεδομένα, όπως οι κωδικοί πρόσβασης που μπορούν να εγγυηθούν ότι οι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε πληροφορίες ασθενών.
- Κρυπτογράφηση: Διαδραματίζει σημαντικό ρόλο στην ασφάλεια των δεδομένων κατά τη μετάδοση και αποθήκευση. Υλοποιείται με τη βοήθεια κρυπτογραφικών μεθόδων τόσο για την κωδικοποίηση όσο και την αποκωδικοποίηση των δεδομένων, παρέχοντας τη δυνατότητα προσπέλασης μόνο σε εξουσιοδοτημένους χρήστες που διαθέτουν το αντίστοιχο κλειδί.

- Ιχνηλάτηση καθολικού: Είναι ένα σύνολο χρονολογικών εγγραφών που χρησιμοποιούνται για τη δημιουργία ιστορικού χειρισμών που εφαρμόστηκαν στα δεδομένα, καταγράφοντας ποιος είχε πρόσβαση σε αυτά, ποιες αλλαγές πραγματοποιήθηκαν και πότε.

Οι κανόνες απορρήτου του HIPAA ώθησαν στη δημιουργία εθνικών προτύπων που αφορούσαν την προστασία δεδομένων των ασθενών, μεταξύ των οποίων συγκαταλέγονται οι παρακάτω:

- Οι ασθενείς έχουν τη δυνατότητα να αποφασίσουν αναφορικά με τη χρήση των δεδομένων τους από τρίτους, έχοντας τον πλήρη έλεγχό τους.
- Ορίζονται περιορισμοί στη χρήση δεδομένων.
- Ορίζονται ρυθμίσεις ασφαλείας που πρέπει να τηρούν οι πάροχοι υγειονομικής περίθαλψης για να διασφαλίσουν την ασφάλεια των δεδομένων.
- Καταγραφή των παραβιάσεων και θέσπιση κυρώσεων στους υπόλογους εφόσον παραβιάζουν τα δικαιώματα ιδιωτικότητας και απορρήτου των ασθενών [6].

3.2 Το IoMT οικοσύστημα

3.2.1 Το πλαίσιο (framework) IoMT

Οι ραγδαίες εξελίξεις στις επιστήμες, την τεχνολογία και την φαρμακευτική, ο πολλαπλασιασμός των έξυπνων ιατρικών συσκευών, η ανάπτυξη της επικοινωνίας μεταξύ των τεχνολογιών μετέτρεψαν τις διάφορες ιατρικές υπηρεσίες σε προσβάσιμα εικονικά συστήματα και απομακρυσμένες εφαρμογές, με στόχο να καταστήσουν την υγειονομική περίθαλψη καλύτερη, οικονομικότερη και πιο προσβάσιμη. Αυτές οι βελτιώσεις εφαρμόζονται σε όλα τα επίπεδα, τις εφαρμογές, τις αρχιτεκτονικές, την τεχνολογία, την επικοινωνία και την ασφάλεια.

Το πλαίσιο (framework) του υγειονομικού οικοσυστήματος αναφέρεται γενικά στο μοντέλο Διασύνδεσης Ανοικτών Συστημάτων (OSI), αλλά με σχετικές τροποποιήσεις που έγιναν για να ενσωματωθεί τεχνολογία του Διαδικτύου των Πραγμάτων (IoT). Η τεχνολογία του IoMT αναφέρεται στο υλικό (hardware - firmware), στο ενδιάμεσο λογισμικό (middleware) και στην πλατφόρμα cloud (λογισμικό), ενώ για την επικοινωνία εφαρμόζεται πρωτόκολλο μικρής ή μεγάλης εμβέλειας. Τα χαρακτηριστικά ασφαλείας περιλαμβάνουν τις απαιτήσεις ασφαλείας, τα μοντέλα απειλών και επιθέσεων, καθώς και τη διαχείριση κινδύνου [3].

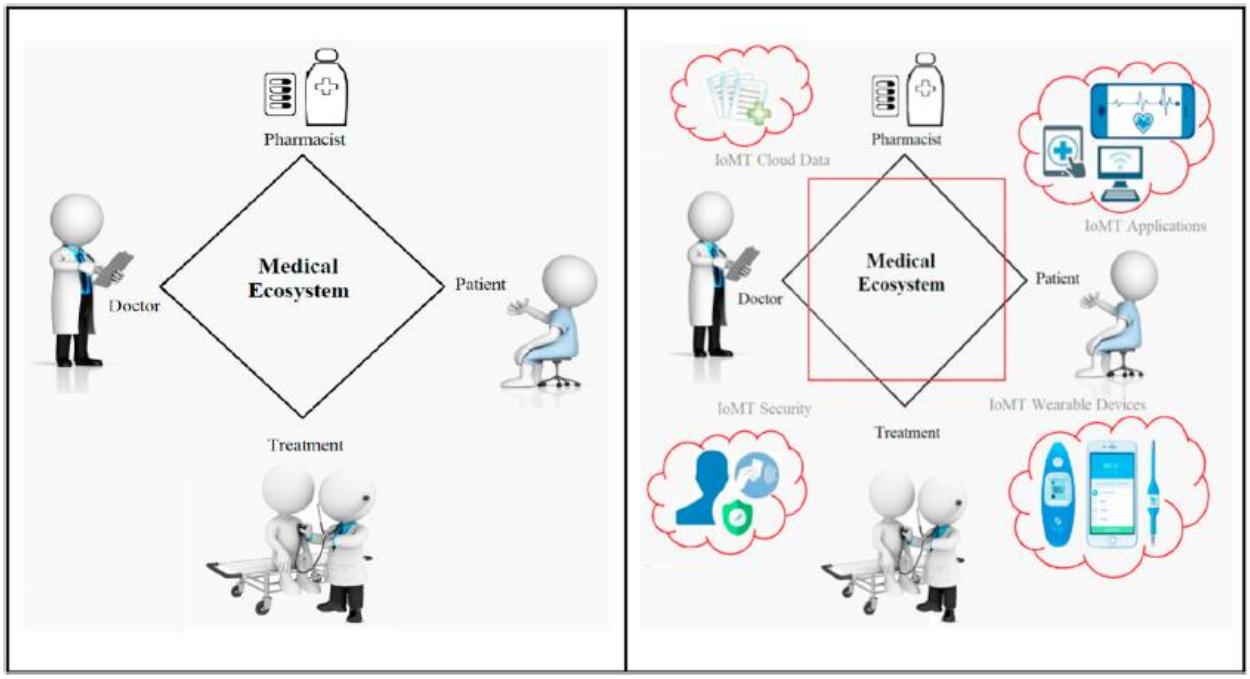
Προκειμένου να υποστηριχθεί ένα ασφαλές σύστημα IoMT αναπτύχθηκε μια προσέγγιση επαλήθευσης δεδομένων και αξιολόγησης κινδύνου, κατά την οποία ορίζονταν οι μέθοδοι ανάλυσης σε επιλεγμένες συσκευές IoT. Ένα σύστημα ιατρικής παρακολούθησης IoMT που διατηρεί το απόρρητο έχει σχεδιαστεί να προσαρτάται ως στοιχείο στο blockchain, με κατεύθυνση να καταστεί ασφαλής η ροή δεδομένων από

τους αισθητήρες στο ανθρώπινο σώμα, ενώ η μικρο-αρχιτεκτονική σχεδίαση μπορεί να συμπεριλάβει πλήθος εφαρμογών υγειονομικής περίθαλψης με ασφάλεια δεδομένων.

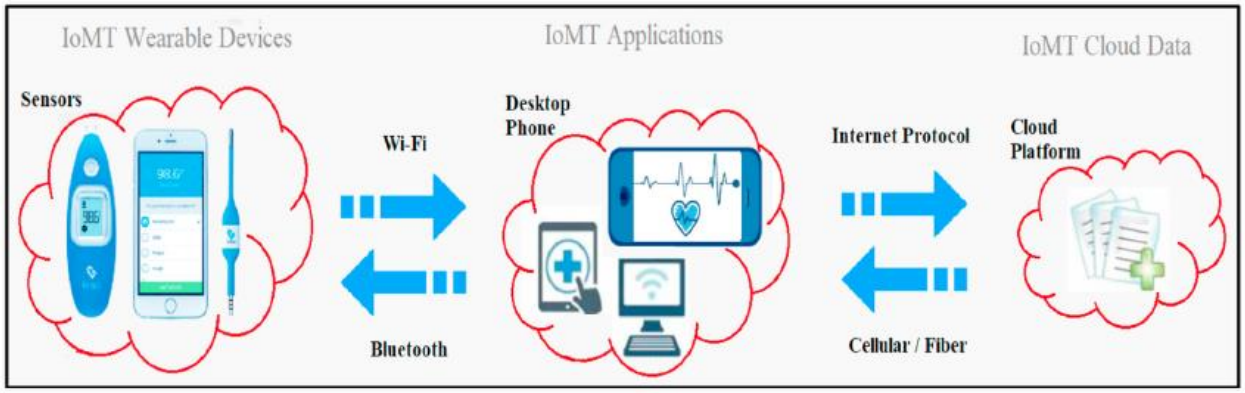
Η επικοινωνία αποτελεί ένα πολύ σημαντικό παράγοντα για το Διαδίκτυο των Ιατρικών Πραγμάτων (IoMT), καθώς ένα σύστημα IoMT μπορεί να χρησιμοποιεί το πρωτόκολλο Narrow Band IoT (NB-IoT), να επικοινωνεί μέσω Long-Term Evolution (LTE), να ενσωματώνει την τεχνολογία 5G για να υποστηρίξει ασύρματη επικοινωνία μεγάλης εμβέλειας, ή να αξιοποιεί το πρωτόκολλο ασύρματης επικοινωνίας μικρής εμβέλειας με χρήση Wi-Fi και Bluetooth.

Η τεχνολογία της cloud πλατφόρμας IoMT έχει βασιστεί στην αρχιτεκτονική πολλαπλού νέφους (multi-cloud) για να μπορέσει να υποστηρίξει την μαζική επέκταση του συστήματος, την προστασία του από αποτυχία αποκατάστασης δεδομένων, τη διαχείριση κλίμακας, τη δημιουργία αντιγράφων ασφαλείας και τη δρομολόγηση πόρων. Σε μια άλλη εξέλιξη, επισημαίνει ότι τα έξυπνα ρούχα που βασίζονται σε αισθητήρες, όπως φορητές συσκευές που βοηθούν στον απομακρυσμένο έλεγχο της υγείας μέσω διαγνωστικών υπηρεσιών. Οι αισθητήρες σώματος έχουν σχεδιαστεί έτσι ώστε να λειτουργούν ως ένα συνεχές IoMT σύστημα παρακολούθησης ασθενών, αποτελώντας τόσο το παραλήπτη όσο και τον πάροχο δεδομένων. Επίσης, έχει υποστηρίξει την αλληλεπίδραση γνωστικού υπολογιστή και τεχνητής νοημοσύνης μεταξύ ρομπότ και ασθενούς [3].

Από την άλλη μεριά, η ραγδαία ανάπτυξη φορητών συσκευών και εφαρμογών υγείας έχει δημιουργήσει μια τεράστια αγορά για την τεχνολογία του Διαδικτύου των Πραγμάτων, καθώς καινοτόμες εφαρμογές υγείας έχουν υλοποιηθεί για να εξυπηρετήσουν τις ανάγκες του υγειονομικού κλάδου, όπως η μέτρηση της αρτηριακής πίεσης, η καταγραφή της γλυκόζης στο αίμα κ.ά. Μια νέα ιδέα που ονομάζεται «Διαδίκτυο των Ιατρικών Πραγμάτων (IoMT)» προτάθηκε για την εκμετάλλευση τεχνολογιών αισθητήρων και ασύρματων δικτύων για την παρακολούθηση ιατρικών καταστάσεων [20].



Εικόνα 3.1: Σύγκριση παραδοσιακού και IoMT οικοσυστήματος (Πηγή: [3])



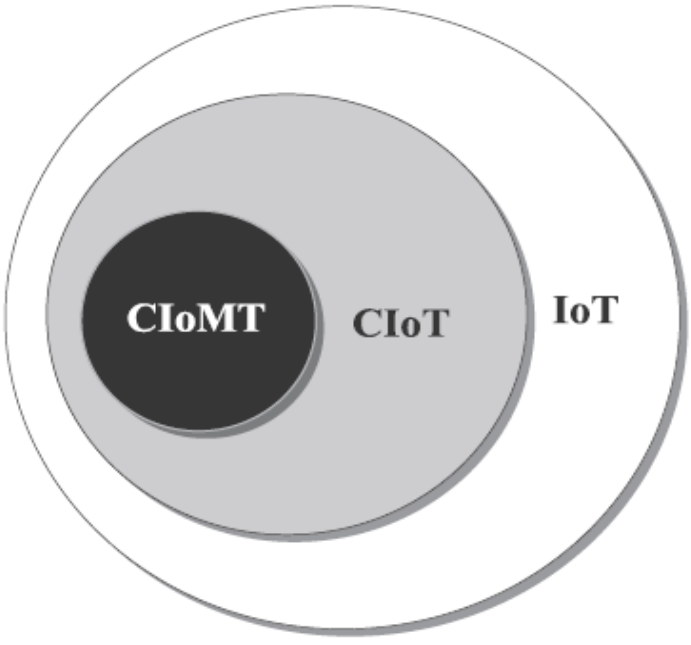
Εικόνα 3.2: Τεχνολογία IoMT και επικοινωνία των δεδομένων αισθητήρων (Πηγή: [3])

3.2.2 Cognitive Internet of Medical Things (CIoMT)

Το Διαδίκτυο των πραγμάτων (IoT) αναφέρεται σε ένα δίκτυο διασυνδεδεμένων φυσικών αντικειμένων όπως αισθητήρες, συσκευές παρακολούθησης της υγείας, έξυπνοι μετρητές, οικιακές συσκευές, αυτόνομα οχήματα κ.λπ. Αυτή η δυνατότητα διασύνδεσης επιτρέπει στα αντικείμενα να αισθάνονται, επεξεργάζονται, επικοινωνούν και αλληλεπιδρούν αυτόματα με τους ανθρώπους, παρέχοντας έξυπνες υπηρεσίες στους χρήστες. Εκτιμάται ότι λόγω της θεαματικής αύξησης των εφαρμογών και του αριθμού των διασυνδεδεμένων ασύρματων συσκευών στα συστήματα IoT, η κίνηση δεδομένων θα φτάσει τα 4394 EB έως το 2030 [33].

Για να ικανοποιηθεί αυτή η συνεχώς αυξανόμενη απαίτηση εύρους ζώνης, το IoT με βάση τη γνωστική συχνότητα που ονομάζεται Cognitive IoT (CIoT) αποτελεί μια εναλλακτική τεχνική βελτίωσης της αποτελεσματικότητας του περιορισμένου φάσματος χρήσης του. Η θεμελιώδης ιδέα πίσω από το CIoT είναι η δυναμική κατανομή των καναλιών συχνότητας κατά την ανταλλαγή πληροφοριών μεταξύ των διασυνδεδεμένων αντικειμένων.

Το Γνωστικό Διαδίκτυο των Πραγμάτων (CIoT) είναι μια τεχνολογία που επιτρέπει σε κάθε φυσική οντότητα την ενεργητική επικοινωνία και ανταλλαγή πληροφοριών, καθώς και την εγγυημένη διασφάλιση των απαιτήσεων Ποιότητας Υπηρεσιών (QoS). Το CIoT αναφέρεται στο IoT με δυνατότητα γνωστικής συχνότητας (Cognitive Ratio - CR), με τελικό σκοπό την υποστήριξη της επικοινωνίας συσκευής με συσκευή σε έναν διαρκώς αυξανόμενο αριθμό δικτύου ασύρματων συσκευών. Η τεχνική της δυναμικής κατανομής φάσματος συχνοτήτων βασίζεται στη γνωστική συχνότητα και αποτελεί τη λύση για την ενσωμάτωση ενός τεράστιου αριθμού συσκευών και εφαρμογών. Το Γνωστικό Διαδίκτυο Ιατρικών Πραγμάτων (CIoMT) ανήκει στη κατηγορία CIoT, εξειδικευμένη για τον ιατρικό κλάδο και την έξυπνη υγειονομική περίθαλψη. Έτσι, τα βιομετρικά δεδομένα του ασθενούς σε πραγματικό χρόνο, όπως η θερμοκρασία σώματος, η αρτηριακή πίεση, ο καρδιακός ρυθμός, το επίπεδο γλυκόζης, το Ηλεκτροκεφαλογράφημα (EEG), το Ηλεκτροκαρδιογράφημα (ECG), το επίπεδο οξυγόνου κ.λπ. καθώς και τα ψυχομετρικά δεδομένα όπως ομιλία, έκφραση κ.ά. είναι διαθέσιμα στο ιατρικό προσωπικό εξ αποστάσεως μέσω του συστήματος IoMT.



Σχήμα 3.3: Απεικόνιση του υποσυνόλου CIoMT, σε συσχέτιση με το CIoT και το IoT (Πηγή: [33])

Αυτή η ιδέα του CIoT ταιριάζει καλύτερα σε αυτήν την πανδημία, καθώς κάθε άτομο πρέπει να συνδέεται και να παρακολουθείται μέσω ενός τεράστιου δικτύου. Επίσης, λόγω του παγκοσμίου lockdown και των περιορισμών μετακίνησης και συγχρωτισμού, το μεγαλύτερο μέρος δραστηριοτήτων πραγματοποιείται διαδικτυακά, όπως το ηλεκτρονικό εμπόριο, η ηλεκτρονική μάθηση, η έξυπνη μέτρηση, η ηλεκτρονική επιτήρηση, η έξυπνη υγειονομική περίθαλψη και οι υπηρεσίες τηλεϊατρικής. Δραστηριότητες που πολλές φορές πραγματοποιούνται μέσω ασύρματης επικοινωνίας, καταναλώνοντας ορισμένο εύρος ζώνης. Το τεράστιο δίκτυο CIoT μεταδίδει μικρά πακέτα αναζητώντας περιστασιακά αδρανή κανάλια, με σκοπό να εξοικονομήσει εύρος ζώνης και να αξιοποιήσει αποτελεσματικά τους πόρους του φάσματος [33].

3.2.3 Προκλήσεις διαλειτουργικότητας Blockchain και IoMT

Η αποτελεσματικότητα εφαρμογής της τεχνολογίας blockchain στον κλάδο της υγείας βασίζεται σε τέσσερις προκλήσεις διαλειτουργικότητας:

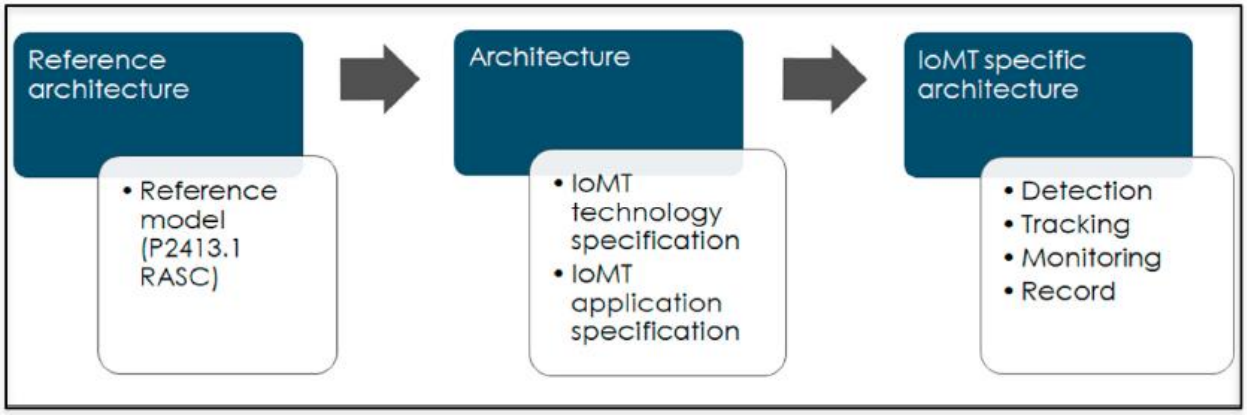
- Τη διατήρηση της εξελικτικότητας με ταυτόχρονη ελαχιστοποίηση της πολυπλοκότητας ενσωμάτωσης: στη τεχνολογία blockchain τα δεδομένα είναι αμετάβλητα και δύσκολο να τροποποιηθούν μαζικά, ενώ τα ιατρικά αρχεία πρέπει να είναι προσβάσιμα από μια ποικιλία συστημάτων που δεν μπορούν εύκολα να αλλάξουν με την πάροδο του χρόνου, διασφαλίζοντας ότι οι συμβάσεις που γράφονται στο blockchain διευκολύνουν την εξέλιξη όπου απαιτείται.
- Την ελαχιστοποίηση των απαιτήσεων αποθήκευσης δεδομένων: οι εφαρμογές στον κλάδο υγείας μπορούν να εξυπηρετήσουν χιλιάδες ή εκατομμύρια χρήστες, γεγονός που δυνητικά μπορεί να επιφέρει ένα τεράστιο φορτίο, όταν όλα αυτά τα δεδομένα αποθηκεύονται στο blockchain και ειδικότερα εάν δεν μελετηθούν επαρκώς οι τεχνικές ομαλοποίησης και αναδιαμόρφωσης δεδομένων. Επίσης, σημαντικό ζήτημα σχεδιασμού είναι η μεγιστοποίηση της ανταλλαγής δεδομένων, ενώ ταυτόχρονα διασφαλίζεται η ευελιξία στη διαχείριση περιστατικών υγειονομικής περίθαλψης. Έτσι, για παράδειγμα το μοτίβο Flyweight σε έξυπνα συμβόλαια, διατηρεί τα εγγενή δεδομένα που διαμοιράζονται οι ασθενείς στο κοινό συμβόλαιο, ενώ τα εξωγενή αποθηκεύονται σε ένα ξεχωριστό συμβόλαιο που αναφέρεται στο συγκεκριμένο ασθενή.
- Την εξισορρόπηση της ευκολίας ενσωμάτωσης με την ασφάλεια: τεχνικές απαιτήσεις όπως η αναγνώριση και ο έλεγχος ταυτότητας όλων των συμμετεχόντων, η ασφαλή υποδομή αποθήκευσης και ανταλλαγής δεδομένων, η εξουσιοδότηση και ο έλεγχος πρόσβασης των πηγών δεδομένων και η δυνατότητα διαχείρισης αυτών από διάφορες δομές φαίνεται ότι καλύπτονται λόγω της ασφαλής κρυπτογραφίας και του ανθεκτικού peer-to-peer δικτύου. Επιπλέον, οι ιδιότητες της τεχνολογίας blockchain για κοινή χρήση περιουσιακών στοιχείων, τη προστασία των πληροφοριών του χρήστη, τον έλεγχο των ιχνών πρόσβασης σε δεδομένα μπορούν να ωφελήσουν το κλάδο του IoMT, παρόλο που σημαντικοί κίνδυνοι εξακολουθούν να ελλοχεύουν.

- Την παρακολούθηση αλλαγών στο τομέα της υγείας σε μεγάλους πληθυσμούς ασθενών: τα κενά επικοινωνίας και οι προκλήσεις ανταλλαγής πληροφοριών αποτελούν σημαντικό εμπόδιο στη καινοτομία στην υγειονομική περίθαλψη, καθώς είναι γνωστό ότι οι ασθενείς φροντίζονται από διάφορους οργανισμούς και οι πάροχοι εξυπηρετούν εκατοντάδες ή περισσότερους ασθενείς. Το μοτίβο Publisher Subscriber στις συμβάσεις ethereum μπορεί να βελτιώσει την κλιμακωτή ανίχνευση αλλαγών συσχέτισης σε μεμονωμένες συμβάσεις [40].

3.3 Αρχιτεκτονική IoMT για την αντιμετώπιση της πανδημίας

Το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE), με στόχο την ετερογενή αλληλεπίδραση, την διαλειτουργικότητα συστημάτων και την υποστήριξη περαιτέρω επεκτασιμότητας της κλίμακας βιομηχανίας, ανακοίνωσε δύο νέα αρχιτεκτονικά πρότυπα αναφορικά με το Διαδίκτυο των Πραγμάτων (IoT), το P2413.1 RASC (πρότυπο αρχιτεκτονικής έξυπνης πόλης) και το P2413.1 PDIoT (πρότυπο αρχιτεκτονικής για τη διανομή ενέργειας στο Διαδίκτυο των Πραγμάτων). Η εγκαθίδρυση προτύπων παρέχει καθοδήγηση όσον αφορά την διαλειτουργικότητα των συστημάτων IoT και προορίζεται να ενοποιήσει και να ελαχιστοποιήσει τον κατακερματισμό της βιομηχανίας, θέτοντας τρεις στόχους:

1. την παροχή ενός ασφαλούς και διαλειτουργικού πλαισίου συστημάτων IoT για πολλαπλούς τομείς εφαρμογών.
2. την παροχή ενός πλαισίου συγκριτικών αξιολογήσεων μεταξύ των διαθέσιμων συστημάτων IoT και
3. την παροχή ενός πλαισίου με στόχο την υποστήριξη και επιτάχυνση του σχεδιασμού, της λειτουργίας και της ανάπτυξης συστημάτων IoT. Το παρακάτω σχήμα 3.4 αποτελεί το πλαίσιο καθοδήγησης που αξιοποιήθηκε για την ανάπτυξη εξειδικευμένης αρχιτεκτονικής με βάση το πρότυπο P2413.1 RASC.



Σχήμα 3.4: Πλαίσιο καθοδήγησης IoMT (P2413.1 RASC) (Πηγή: [3])

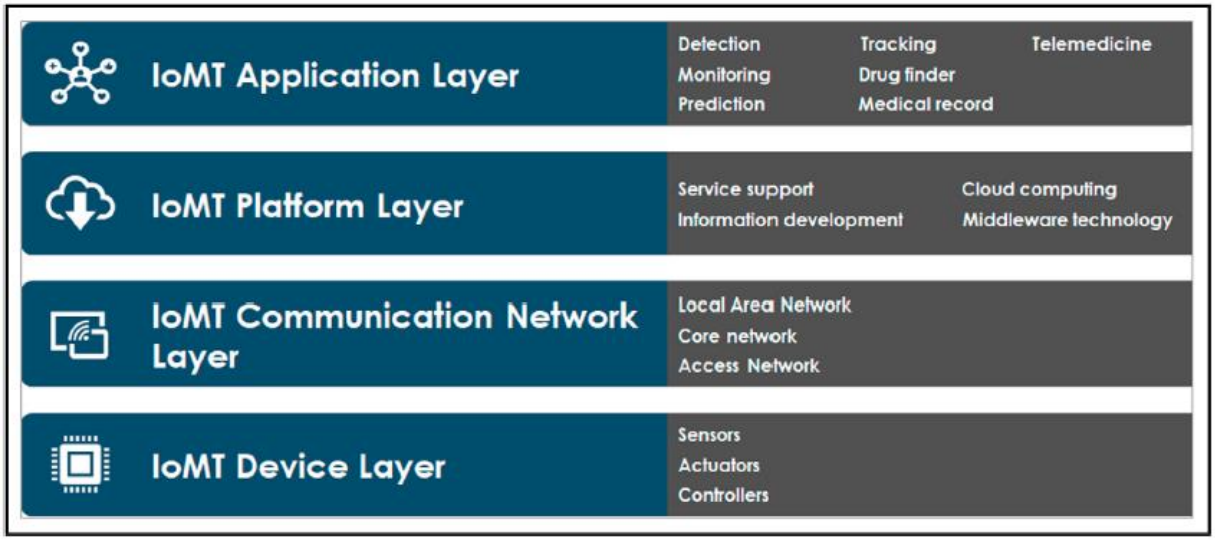
Το πρότυπο RASC ορίζει μια Αρχιτεκτονική Αναφοράς (Reference Architecture) τεσσάρων επιπέδων: επίπεδο συσκευής, επίπεδο δικτύου επικοινωνίας, επίπεδο πλατφόρμας IoT και επίπεδο εφαρμογής. Το πρότυπο περιλαμβάνει τη συσχέτιση τεχνολογιών, όπως τα δεδομένα μεγάλου εύρους (big data), το cloud computing και τη τεχνολογίας υπολογιστικών ακμών (Edge Computing), στο Ευφυές Κέντρο Εργασιών (IoC) κάτω από ένα ενοποιημένο πλαίσιο ασφαλείας. Μια πιθανή IoMT αρχιτεκτονική για την αντιμετώπιση της πανδημίας παρουσιάζεται παρακάτω στην εικόνα 3.5.

Το επίπεδο συσκευής περιλαμβάνει υλικό όπως αισθητήρες, ελεγκτές και ενεργοποιητές. Ο αναγνώστης και η ετικέτα RFID, η κάμερα αναγνώρισης προσώπου, το έξυπνο ρολόι γυμναστικής, οι ιατρικοί αισθητήρες, οι αντλίες ινσουλίνης και οι υπέρυθροι αισθητήρες μέτρησης θερμοκρασίας είναι μερικές από τις συσκευές που χρησιμοποιούνται σήμερα. Οι αισθητήρες μπορούν να ταξινομηθούν σε φορητές και εμφυτεύσιμες συσκευές, καθώς και συσκευές περιβάλλοντος.

Ακολουθεί το επίπεδο επικοινωνίας δικτύου, στο οποίο εφαρμόζονται μερικές από τις πιο πρόσφατες τεχνολογίες όπως το ασύρματο δίκτυο αισθητήρων (WSN), το Bluetooth, το ZigBee, το WiFi, το NB-IoT, το LTE, το 4G και το 5G, που αξιοποιούν πρωτόκολλα ελαφριάς χρήσης. Επίσης, προτείνονται για συσκευές χαμηλής ισχύος στα δίκτυα ασύρματης επικοινωνίας, όπως το Body Area Network (BAN) και το Personal Area Network (PAN). Επίσης, οι συσσωρευτές, όπως οι δρομολογητές WiFi, λειτουργούν ως πύλες πολλαπλής συνδεσιμότητας. Ένα παράδειγμα IoT επικοινωνίας αποτελεί το Information Centric Networking (ICN), η φύση του οποίου καθοδηγείται από τα δεδομένα και η επικοινωνία προσανατολίζεται στο περιεχόμενό τους. Το ICN προσφέρει επεκτασιμότητα, αποτελεσματική κινητικότητα δρομολόγησης, στρατηγικές προσωρινής αποθήκευσης και εργαλεία ασφάλειας στο IoMT.

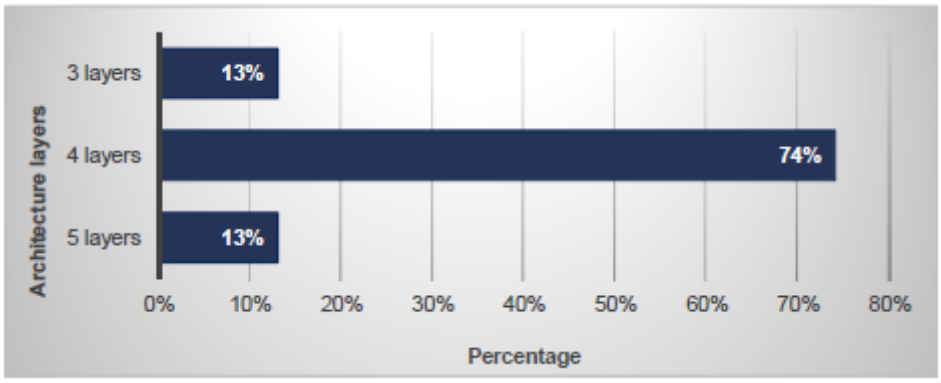
Το επίπεδο πλατφόρμας IoT υποστηρίζει τις υπηρεσίες, παρέχει ανάπτυξη πληροφοριών, υπολογιστική νέφους και τεχνολογία ενδιάμεσου λογισμικού. Οι πλατφόρμες cloud όπως το Microsoft Azure, το Oracle Cloud, το Amazon Web Services, το Google Cloud, το IBM Cloud και το Alibaba Cloud παρέχουν υπηρεσίες ανταλλαγής μηνυμάτων, αποθήκευσης, επεξεργασίας δεδομένων και στατιστικών αναλύσεων για εφαρμογές IoMT. Το υψηλότερο επίπεδο αρχιτεκτονικής IoT αποτελεί το επίπεδο εφαρμογής, το οποίο εφαρμόζεται σε οποιονδήποτε αριθμό συσκευών και περιλαμβάνει συστήματα ελέγχου, συστήματα παρακολούθησης/εντοπισμού, συστήματα φυσικής κατάστασης/υγείας, ηλεκτρονική καταγραφή ιατρικών δεδομένων, συστήματα απομακρυσμένης διάγνωσης, τηλεϊατρική κ.ά.

Το σύστημα υγείας που προσδιορίστηκε μεταξύ των εφαρμογών έξυπνων πόλεων που βασίζονται στη τεχνολογία IoT κατέληξε στο επίπεδο αρχιτεκτονικής τεσσάρων επιπέδων, το επίπεδο ανίχνευσης, το επίπεδο δικτύου, το επίπεδο υπολογιστικού νέφους και το επίπεδο εφαρμογής. [3]



Εικόνα 3.5: Συγκεκριμένη αρχιτεκτονική IoMT για την αντιμετώπιση της πανδημίας (Πηγή: [3])

Εστιάζοντας στη διασύνδεση στοιχείων μεταξύ του IPv6 και του φυσικού δικτύου, σχεδιάστηκε ένα απλοποιημένο πρωτόκολλο σε μορφή μηνυμάτων αντί της μετατροπής σε μορφή πακέτων. Με στόχο την ικανοποίηση των λειτουργικών απαιτήσεων του IoMT αναπτύχθηκε η αρχιτεκτονική πέντε επιπέδων (ανίχνευσης/εκτέλεσης, βοηθητικής επικοινωνίας, μετάδοσης δικτύου, ενοποίησης δεδομένων και εφαρμογής). Εναλλακτικά, με βάση την τεχνολογία του Διαδικτύου των Πραγμάτων (IoT) παρουσιάστηκε και μια αρχιτεκτονική τεσσάρων επιπέδων (εφαρμογής, δικτύου, ανάλυσης, ανίχνευσης), όπου στόχος ήταν να βελτιωθεί η μετάδοση απομακρυσμένης διάγνωσης και θεραπείας, λειτουργία που απαιτεί επεξεργασία και οπτικοποίηση δεδομένων από τρισδιάστατες εικόνες, ενώ ταυτόχρονα παρέχει ασφάλεια κατά τη μετάδοση των δεδομένων.



Εικόνα 3.6: Ποσοστιαία ανάλυση αρχιτεκτονικών ανά επίπεδο λειτουργίας (Πηγή: [3])

Μια αρχιτεκτονική IoMT με προδιαγραφές ασφαλείας μπορεί να οριστεί μεταγενέστερα με την προσθήκη συγκεκριμένων στοιχείων στο επίπεδο εφαρμογής, συστατικά τα οποία συναντάμε σε φορητά και μη

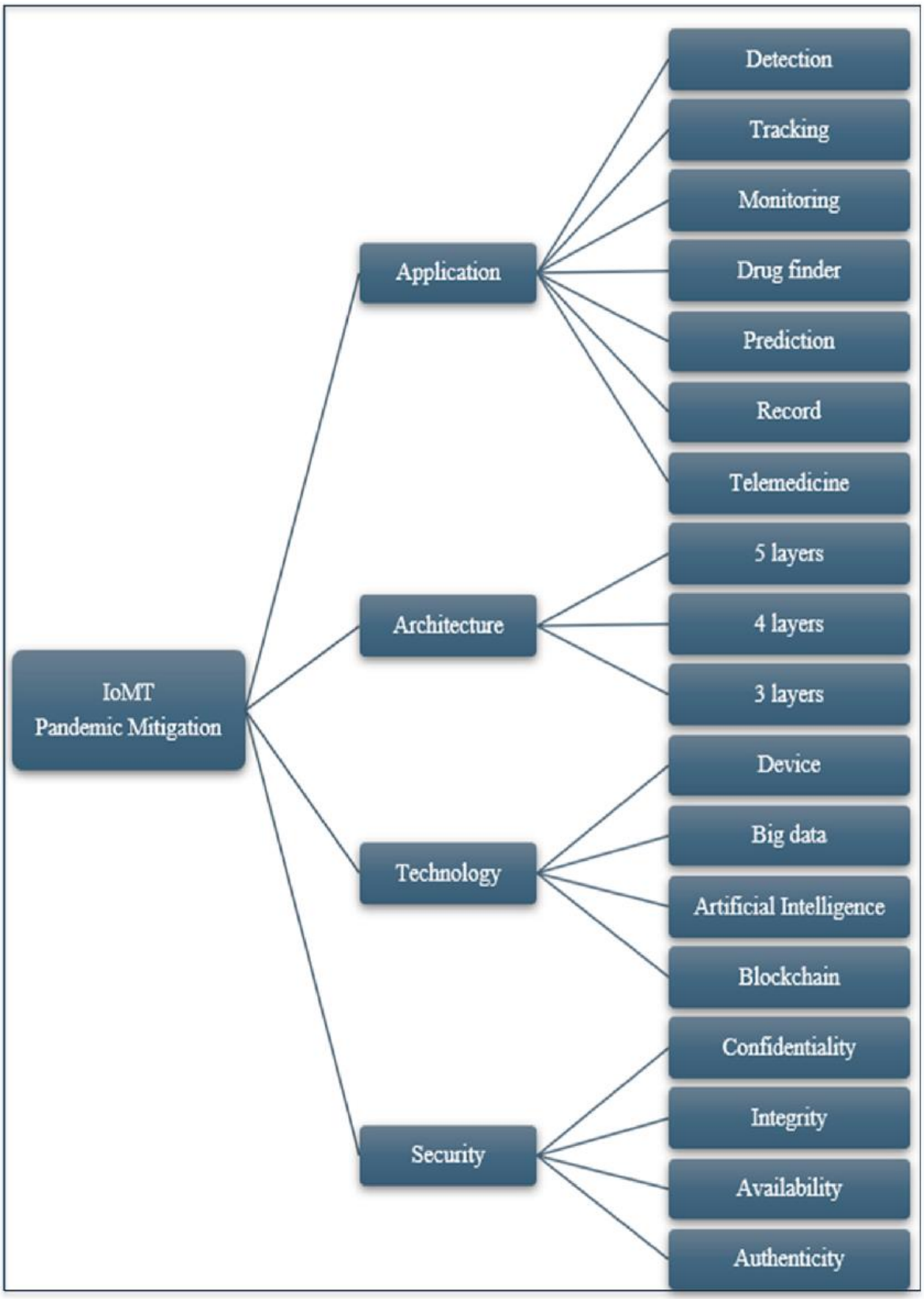
συστήματα IoT απομακρυσμένης υγειονομικής διάγνωσης, σε εφαρμογές υγείας και αισθητήρες περιβάλλοντος. Βάσει αυτής της προτεινόμενης αρχιτεκτονικής, η ασφάλεια του συστήματος IoMT θα εξακολουθεί να υπάρχει, παρότι έχουν ενσωματωθεί στα στοιχεία ασφαλείας του πλαισίου και τα υπόλοιπα επίπεδα. Επομένως, κάθε νέο σύστημα IoMT που κατασκευάζεται σύμφωνα με αυτήν την αρχιτεκτονική ασφαλείας έχει προ-εγκατεστημένο ένα αμυντικό μηχανισμό πολλαπλών επιπέδων.

Ο παρακάτω πίνακας συνοψίζει την ανάλυση των επιπέδων αρχιτεκτονικής, ενώ η εικόνα 3.6 παρουσιάζει τα ποσοστά εμφάνισης ανά επίπεδο, φανερώνοντας ότι η αρχιτεκτονική τεσσάρων επιπέδων είναι η πιο προσιτή, καθώς περιλαμβάνει ταξινόμηση εφαρμογής, εικονική πλατφόρμα, επικοινωνία δικτύου και φυσικές πτυχές του IoT [3].

Table 1
Summary of architecture layer analysis.

Architecture layer	5 layers	4 layers	3 layers	Ratio
Application	Liu et al. (2018)	Xu et al. (2019); Din et al., 2018; Sengupta et al. (2019); IEEE, 2020	Noor and Hassan, 2019	19%
Cloud computing		Zhang et al. (2018); Din et al., 2018		6%
Cloud-to-end-fusion		Ma et al. (2017)		3%
Cloud service		Ma et al. (2017)		3%
Platform		IEEE, 2020		3%
Processing		Sengupta et al. (2019)		3%
Data integration	Liu et al. (2018)			3%
Edge computing		Zhang et al. (2018)		3%
Transport		Ma et al. (2017)		3%
Network	Liu et al. (2018)	Xu et al. (2019); Din et al., 2018; Sengupta et al. (2019)	Noor and Hassan, 2019	16%
Analysis		Xu et al. (2019)		3%
Base station		Zhang et al. (2018)		3%
Communication	Liu et al. (2018)	IEEE, 2020		6%
Perception		Ma et al. (2017); Sengupta et al. (2019)	Noor and Hassan, 2019	9%
Sensing	Liu et al. (2018)	Xu et al. (2019); Din et al., 2018; Zhang et al. (2018)		13%
Device		IEEE, 2020		3%

Πίνακας 3.1: Συγκεντρωτική ανάλυση των επιπέδων αρχιτεκτονικής (Πηγή: [3])



Εικόνα 3.7: Κατηγορίες εφαρμογών IoMT για την αντιμετώπιση της πανδημίας (Πηγή: [3])

3.4 Τεχνητή νοημοσύνη και δεδομένα μεγάλου εύρους στο IoMT

Ένα σύστημα τεχνητής νοημοσύνης παρουσιάζει χαρακτηριστικά που ομοιάζουν με το ανθρώπινο εγκέφαλο, όπως η μάθηση και η επίλυση προβλημάτων. Μέθοδοι, όπως η μαθηματική υπολογιστική θεωρία πολυπλοκότητας, επικεντρώθηκαν στην ταξινόμηση προβλημάτων μέσα από τη διασύνδεση κλάσεων και πόρων μεταξύ τους υπό τη μορφή αλγορίθμου. Ένας από αυτούς μπορεί να είναι ένας αλγόριθμος βελτιστοποίησης που θα αφορά τον έλεγχο των εξάρσεων και της μετάδοσης του Covid-19, μέσω μοντελοποίησης του μηχανισμού διάδοσης του ιού σε πολλές χώρες ανά τον κόσμο, στοχεύοντας στην επίλυση του προβλήματος βελτιστοποίησης με χρήση των πιο αποδοτικών μεταβλητών διανομής. Η κατεύθυνση του μοντέλου εσωκλείεται στην απάντηση του παρακάτω σημαντικού ερωτήματος: πώς μπορούν οι υπεύθυνοι χάραξης πολιτικής και οι υγειονομικοί φορείς να είναι σε θέση να επαναφέρουν στην κανονικότητα τη ζωή των ανθρώπων την εποχή της διάδοσης του COVID-19;

Η εξόρυξη δεδομένων στο IoMT συμμετέχει στη διαδικασία προγνωστικών μοντέλων, παρέχοντας την πρώτη ύλη για την ακριβή πρόβλεψη του αντίκτυπου ασθενειών, όπως ο Covid-19. Τα δεδομένα που παράγονται από συσκευές IoT είναι δεδομένα ροής που αυξάνονται συνεχώς σε όγκο και ταχύτητα, όντας γνήσια δεδομένα μεγάλου εύρους (big data). Η ανάλυσή τους αποτελεί μια ανεξάρτητη μελέτη μοτίβων στατιστικών δεδομένων υγειονομικής περίθαλψης που θα οδηγήσει στη δημιουργία προγνωστικών μοντέλων. Η Μηχανική Μάθηση (ML), ως μέρος της τεχνητής νοημοσύνης, αποτελεί μια αναλυτική μεθοδολογία που μπορεί να προσομοιώσει ένα περιστατικό με ακρίβεια βάσει της προηγούμενης γνώσης και της ίδιας της διαδικασίας εκπαίδευσης του αλγορίθμου. Όπως είναι αναμενόμενο, ένας σημαντικός αριθμός μοντέλων μηχανικής μάθησης έχει αναπτυχθεί για την αναπαραγωγή περιπτώσεων COVID-19 [3].

Οι ιατρικές απεικονίσεις, όπως η ακτινογραφία και η αξονική τομογραφία (CT) διαδραματίζουν ουσιαστικό ρόλο στην αντιμετώπιση του COVID-19, ενώ οι πρόσφατα αναδυόμενες τεχνολογίες τεχνητής νοημοσύνης (AI) ενισχύουν περαιτέρω τη δύναμη των εργαλείων απεικόνισης. Έτσι, η λήψη ιατρικών απεικονίσεων με την υποστήριξη της τεχνητής νοημοσύνης μπορεί να ωθήσει σημαντικά στην αυτοματοποίηση της διαδικασίας σάρωσης αλλά και να αναδιαμορφώσει τη ροή εργασιών ελαχιστοποιώντας την επαφή με τους ασθενείς. Επίσης, η τεχνητή νοημοσύνη μπορεί να βελτιώσει την αποτελεσματικότητα της ιατρικής γνωμάτευσης με την ακριβή περιγραφή και ταξινόμηση των λοιμώξεων μέσω των απεικονίσεων X-ray και CT, διευκολύνοντας την οριοθέτηση της βαρύτητας της διάγνωσης, παρακολούθησης και πρόγνωσης της νόσου. Μια ολόκληρη σειρά ιατρικών απεικονίσεων και τεχνικών αναλύσεων εφαρμόζονται ευρέως στα νοσοκομεία πρώτης γραμμής για την καταπολέμηση του COVID-19 και περιλαμβάνουν την λήψη, τη τμηματοποίηση, τη διάγνωση, την ανατροφοδότηση και την

επαναξιολόγηση της διαγνωστικής απεικόνισης, με εστίαση στην ενσωμάτωση της τεχνητής νοημοσύνης [29].

Γενικά, η συγκριτική αξιολόγηση και δοκιμή διαγνωστικών μοντέλων για τον Covid-19 είναι μια σύνθετη διαδικασία, καθώς απαιτείται η αξιολόγηση πολλών κριτηρίων, ορισμένα από τα οποία έρχονται σε σύγκρουση μεταξύ τους. Απαιτείται ένας πίνακας αποφάσεων που συνδυάζει παραμέτρους αξιολόγησης και διαγνωστικά μοντέλα, για να ληφθεί η πολυπαραγοντική απόφαση με σεβασμό στα κριτήρια αξιολόγησης. Τα κριτήρια του διαγνωστικού μοντέλου καλύπτονται ελλιπώς από τις δοκιμαστικές προσεγγίσεις, που σε συνδυασμό με την περιορισμένη αποτελεσματικότητα των μεθόδων, οδηγούν στην αδυναμία εξίσωσης και συσχέτισης των διαφόρων ταξινομητών, βάσει των αποτελεσμάτων τους. Η παροχή ενός ολοκληρωμένου πλαισίου για την εκτίμηση και τη σύγκριση διαφόρων διαγνωστικών ταξινομητών κατά του Covid-19, ώθησε την ανάπτυξη ενοποιημένων ταξινομητών που θα καλύπτουν όλες τις διαστάσεις αποτελεσματικότητας των μοντέλων. Η τεχνική αυτή λειτούργησε ως υποστηρικτικός μηχανισμός υποβοήθησης των υπευθύνων λήψης αποφάσεων στον υγειονομικό τομέα, μέσω της σύγκρισης ανάμεσα στα βέλτιστα σχήματα ταξινόμησης που μπορούν να αξιοποιηθούν για τη διάγνωση του Covid-19 [3].

Σε μια πρόσφατη μελέτη (Jia et al., 2020), χρησιμοποιήθηκαν δεδομένα από το SARS του 2003 για τη ανάπτυξη τριών μαθηματικών μοντέλων, πιο συγκεκριμένα το Logistic, το Bertalanffy και το Gompertz, προκειμένου να συνταχθεί μια προγνωστική τάση για τον ιό. Στη συνέχεια, τα τρία αυτά μοντέλα εφαρμόστηκαν για την προσαρμογή και μελέτη της επιδημικής τάσης του Covid-19 στη Γουχάν (Wuhan), στην ηπειρωτική Κίνα και σε περιοχές εκτός της Χουμπέι (Hubei). Με βάση αυτή την έρευνα, οι επιστήμονες προέβλεψαν τον συνολικό αριθμό μολύνσεων και θανάτων που θα συνέβαιναν, καθώς και την ημερομηνία που θα τελειώσει η πανδημία στην Κίνα.

Σε άλλη μελέτη, αναπτύχθηκε ένα εργαλείο μηχανικής μάθησης που στόχευε στην ευαισθητοποίηση των μέτρων υγειονομικής προστασίας, με επίκεντρο το πλύσιμο των χεριών κατά τη περίοδο της πανδημίας του COVID-19. Με βάση δεδομένα υγείας 2799 ασθενών COVID-19, αναπτύχθηκε ένα μοντέλο πρόβλεψης που αξιοποιούσε τον αλγόριθμο μηχανικής μάθησης XGBoost και δοκιμάστηκε πρακτικά σε 29 ασθενείς, με στόχο την πρόβλεψη της σοβαρότητας της κατάστασης ασθενών με σοβαρή λοίμωξη COVID-19. Οι συντάκτες της μελέτης διαπίστωσαν ότι το μοντέλο έχει την ικανότητα αξιόπιστης πρόβλεψης του κινδύνου θνησιμότητας, όντας ένα κλινικό εργαλείο για την αναγνώριση των σοβαρότερων περιπτώσεων, με σκοπό τη μείωση του αριθμού των θανάτων. Επιπλέον, εφόσον δεν υπάρχει συγκεκριμένος βιοτικός δείκτης διάκρισης της σοβαρότητας νόσησης από COVID-19, αναδύεται δυναμικότερα η ανάγκη εκέλιξης αυτού του προβλεπτικού εργαλείου. Επίσης, σε άλλη μελέτη, υλοποιήθηκε μια μέθοδος μαθηματικής προσομοίωσης που αξιοποιούσε την τεχνολογία μηχανικής

μάθησης και στόχευε στην αναγνώριση των πιο σημαντικών βιοτικών δεικτών που συνδέονταν με την κατάσταση υγείας των ασθενών, διευκολύνοντας τη διαδικασία προτεραιοποίησης ασθενών όσον αφορά τη λήψη θεραπείας και την αποτροπή απώλειας της ζωής τους.

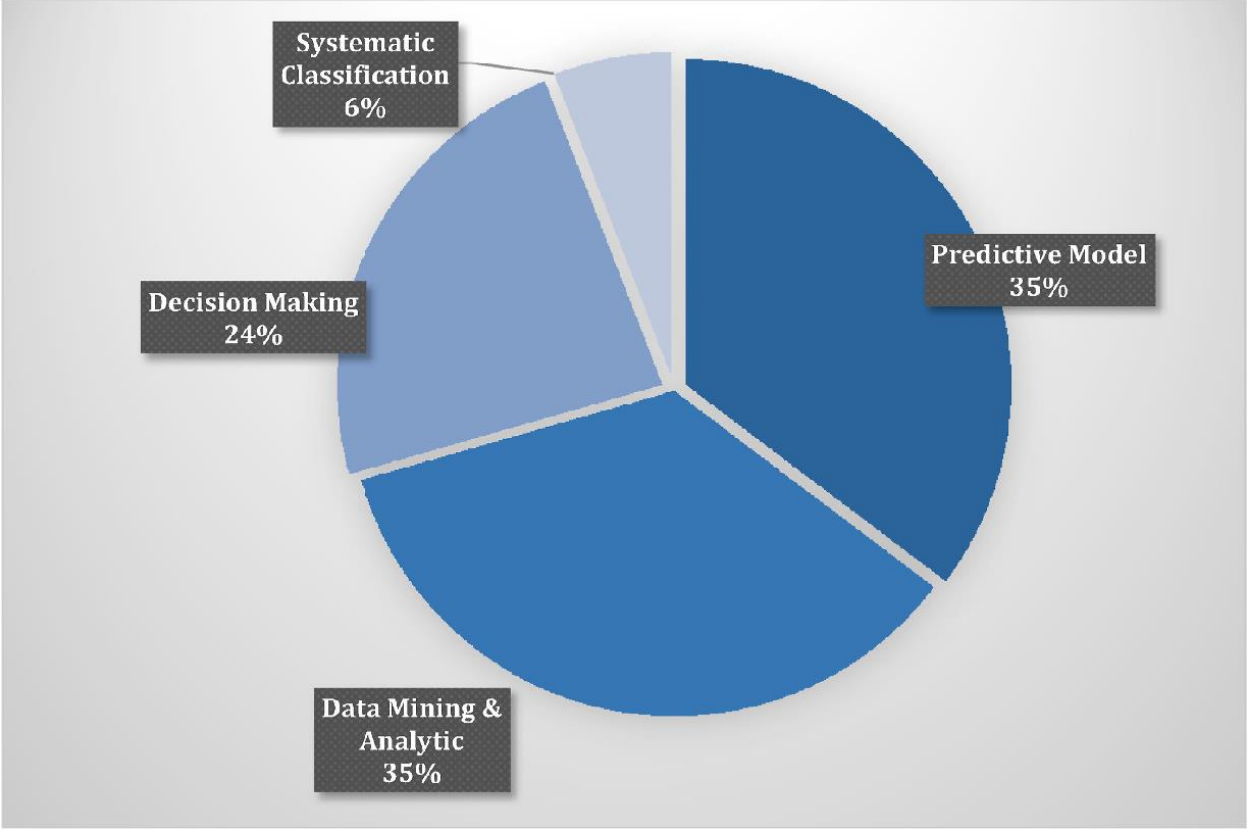
Άλλη έρευνα πραγματοποίησε μια επισκόπηση εξάπλωσης του COVID-19, καθώς και εκτίμηση της σοβαρότητάς της μέσα από τό ποσοστό θνησιμότητας, εφαρμόζοντας μεθόδους μηχανικής μάθησης και τεχνικές μαθηματικής προσομοίωσης όπως οι Rough Set-Support Vector Machine, Bayesian Ridge και Polynomial Regression, SIR Model και Recurrent Neural Network. Στόχος ήταν ο προσδιορισμός της σχέσης εξαρτημένης και ανεξάρτητης μεταβλητής σε ένα μοντέλο που περιγράφει το άτομο ως ευαίσθητο (δεν έχει προσβληθεί από τη νόσο αλλά μπορεί να μολυνθεί μέσω μετάδοσης από μολυσμένα άτομα), ή μολυσμένο (έχει προσβληθεί από τη νόσο) και την κατάσταση ως ανάρρωσε/απεβίωσε (ο ιός μπορεί να οδηγήσει σε μία από τις δύο καταστάσεις). Η μελέτη βασίστηκε στη συλλογή δεδομένων από το Johns Hopkins Corona Virus Resource Center, ενώ από τις μεθόδους μηχανικής μάθησης που χρησιμοποιήθηκαν στο πείραμα φάνηκε ότι το μοντέλο Recurrent Neural Network ήταν το πιο αποτελεσματικό.

Προηγμένες μέθοδοι μηχανικής μάθησης έχουν αξιοποιηθεί στη συστηματική ταξινόμηση των γονιδιωμάτων, στη δοκιμασία ανίχνευσης τεστ (με βάση το CRISPR) και στην αναζήτηση φαρμάκων κατά του COVID-19. Επίσης, ερευνητικές αναφορές αναδεικνύουν ότι το Διαδίκτυο των Πραγμάτων (IoT) και οι εξελιγμένες τεχνολογίες, όπως η τεχνητή νοημοσύνη (AI), η ανάλυση δεδομένων μεγάλου εύρους (big data analytics) και η επικοινωνία 5G, μπορούν να διαδραματίσουν σημαντικό ρόλο στην πρόληψη εξάπλωσης ασθενειών, υποστηρίζοντας διεργασίες όπως η συγκέντρωση δεδομένων, η ιατρική παρακολούθηση του ασθενούς και η εξόρυξη δεδομένων.

Σε χώρες, όπως η Κίνα και η Νότια Κορέα, διάφορες εφαρμογές που αξιοποιούν τη τεχνητή νοημοσύνη έχουν υλοποιηθεί κατά τη διάστημα έξαρσης της πανδημίας COVID-19. Μια τέτοια εφαρμογή Διαδικτύου των Ιατρικών Πραγμάτων ενάντια στον COVID-19 είναι ένα σύστημα υπέρυθρων καμερών και ανίχνευσης προσώπου, που έχει τη δυνατότητα αναγνώρισης ατόμων με υψηλή θερμοκρασία (πυρετό). Προκειμένου να μειωθεί η πιθανότητα μόλυνσης από COVID-19, η Κίνα κατασκεύασε ρομπότ εξοπλισμένα με τεχνητή νοημοσύνη για τη διεξαγωγή άμεσων μετρήσεων θερμοκρασίας σώματος. Η τεχνολογία αυτή βασίζεται στην επικοινωνία 5G, είναι εξοπλισμένη με 5 κάμερες υψηλής ανάλυσης και υπέρυθρα θερμόμετρα, έχοντας την ικανότητα λήψης μέτρησης θερμοκρασίας σώματος έως 10 ατόμων ταυτόχρονα σε απόσταση 5 μέτρων [3].

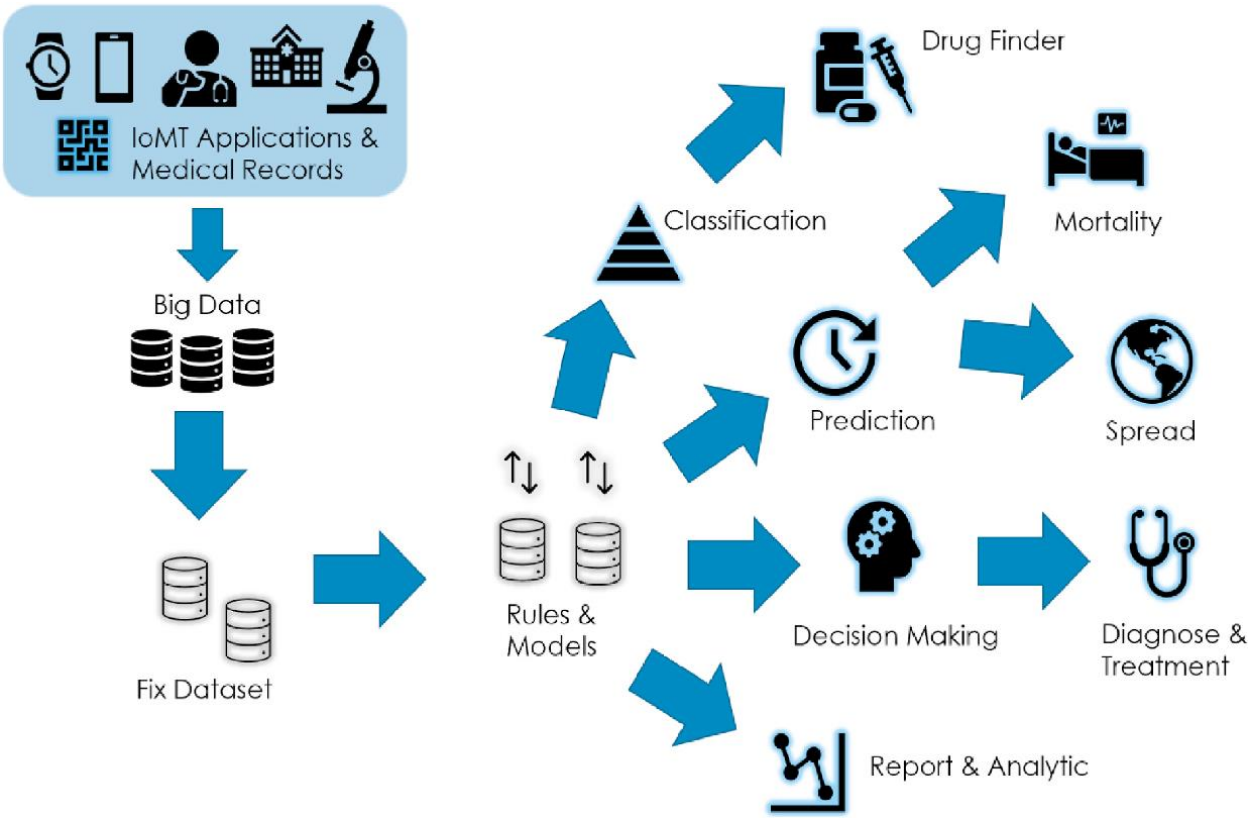
Αυτό το σύστημα IoT μπορεί να ανιχνεύσει τη θερμοκρασία με περιθώριο ακρίβειας 0.3C, ενώ επίσης μπορεί να αναγνωρίσει εάν τα άτομα φορούν την απαραίτητη προστατευτική μάσκα. Η εξελιγμένη

τεχνολογία αναγνώρισης προσώπου αναπτύχθηκε από την Sense Time και τη Megvii, κινεζικές εταιρείες υψηλής τεχνολογίας με εξειδίκευση στον τομέα του Διαδικτύου των Πραγμάτων [18].



Γράφημα 3.8: Ποσοστιαία ανάλυση της εφαρμογής τεχνητής νοημοσύνης και δεδομένων μεγάλου εύρους (big data) (Πηγή: [3])

Το παραπάνω γράφημα απεικονίζει την ποσοστιαία αναλογία των τεσσάρων πεδίων λειτουργίας των εφαρμογών IoMT. Από αυτό προκύπτει ότι το μοντέλο πρόβλεψης και εξόρυξης δεδομένων είναι τα συχνότερα χρησιμοποιούμενα, με το μοντέλο λήψης αποφάσεων να ακολουθεί.



Σχήμα 3.9: Γραφική απεικόνιση των τεχνολογιών IoMT, big data και τεχνητής νοημοσύνης στην αντιμετώπιση του Covid-19 (Πηγή: [3])

Είναι σαφές ότι η ανάλυση δεδομένων υγείας μεγάλου εύρους (big data) μπορεί να χρησιμοποιηθεί για την πρόβλεψη μοτίβων και κρυφών πληροφοριών μη ορατών με «γυμνό μάτι. Επιπλέον, το IoMT μπορεί να θεωρηθεί η εξέλιξη της βιομηχανίας υγείας που σε ορισμένες περιπτώσεις, μπορεί να βελτιώσει τους φορείς υγείας στη διάγνωση, τη θεραπεία και την πρόβλεψη άγνωστων ασθενειών, μέσα από την εξόρυξη δεδομένων. Ωστόσο, για να εξασφαλίσουμε αυτή τη δυναμική τεχνολογία, που συνδυάζει την ανάλυση δεδομένων μεγάλου εύρους και το Διαδίκτυο των Ιατρικών Πραγμάτων, υπάρχει η αναγκαιότητα τυποποίησης των αποκεντρωμένων δεδομένων. Η διαφοροποίηση ως προς τη μορφή και το μήκος των δεδομένων, καθώς και ο μεγάλος αριθμός μοντέλων μηχανικής μάθησης, μπορεί να επηρεάσει τις τιμές των διαφόρων μοντέλων και να φέρει στην επιφάνεια μια σημαντική πρόκληση όσον αφορά τις ομάδες διαχείρισης των υγειονομικών φορέων σχετικά με την επιλογή του καταλληλότερου.

Επιπροσθέτως, η επιλογή μιας μη βέλτιστης λύσης για το μοντέλο διάγνωσης COVID-19 μπορεί να εκτινάξει το κόστος για τους υγειονομικούς φορείς, σε μια εποχή όπου η ανάγκη για ένα αξιόπιστο και λειτουργικό μοντέλο διάγνωσης είναι τεράστια. Μια ευέλικτη προσέγγιση θα βοηθήσει στη δοκιμή και σύγκριση μιας σειράς διαγνωστικών μοντέλων για τον COVID-19, ενώ μετέπειτα στην επιλογή του

καταλληλότερου μοντέλου, που εναρμονίζεται με τις ανάγκες του ιδρύματος υγείας με στόχο την ελαχιστοποίση του χρόνου και του κόστους εφαρμογής, ακολουθώντας ένα αυστηρό πλαίσιο επιλογής αναφορικά με το μοντέλο μηχανικής μάθησης. Μια κλιμακωτή προσέγγιση που επεκτάθηκε στη συγκριτική ανάλυση διαγνωστικών μοντέλων από εργαστηριακά αποτελέσματα ακτινολογίας, όπως απεικονίσεις μαγνητικής τομογραφίας (CT), επέτρεψε στις διοικήσεις των νοσοκομείων να επιλέξουν το καταλληλότερο μοντέλο διάγνωσης του COVID-19, εφόσον οι απαιτήσεις και οι μεταβλητές των εφαρμογών παρέμεναν ενημερωμένες [3].

Το AI και τα Big Data φαίνεται να έχουν τεράστιες δυνατότητες στη διαχείριση του COVID-19 και άλλων καταστάσεων έκτακτης ανάγκης και ο ρόλος τους αναμένεται να αυξηθεί στο μέλλον. Η τεχνητή νοημοσύνη και τα δεδομένα μεγάλου εύρους μπορούν να χρησιμοποιηθούν για την παρακολούθηση της εξάπλωσης του ιού σε πραγματικό χρόνο, τον σχεδιασμό και την άρση των παρεμβάσεων στη δημόσια υγεία, την παρακολούθηση της αποτελεσματικότητάς τους, την επαναχρησιμοποίηση παλαιών συνθέσεων και την ανακάλυψη νέων φαρμάκων, καθώς και τον εντοπισμό δυνητικών εμβολίων και την ενίσχυση της ανταπόκρισης κοινοτήτων και περιοχών στην εξέλιξη της πανδημίας. Αυτές οι αναδυόμενες προσεγγίσεις μπορούν να αξιοποιηθούν μαζί με την κλασική επιτήρηση πλήθους, η οποία επιτρέπει την ανάλυση και την ερμηνεία δεδομένων, ενώ σε συνδυασμό με AI και Big Data μπορούν να αποκαλύψουν κρυφές τάσεις και μοτίβα, τα οποία μπορούν να χρησιμοποιηθούν για τη δημιουργία προγνωστικών μοντέλων. Τέλος, ο χρονικός ορίζοντας υλοποίησής τους διαφοροποιείται σε τρεις κατηγορίες: βραχυπρόθεσμος, μεσοπρόθεσμος και μακροπρόθεσμος σχεδιασμός, όπως φαίνεται στον παρακάτω πίνακα [9].

Time-Scale	Possible Application	Example
Short-term (weeks)	Rapid identification of an ongoing outbreak	AI can facilitate real-time epidemiological data collection, risk-assessment, decision-making processes, and design/implementation of public health interventions
	Diagnosis and prognosis of COVID-19 cases	Recognition of specific diagnostic and prognostic features
Medium-term (months)	Identification of a potential therapeutic option	Identify already existing drugs/discovering new molecules
Long-term (decades)	Enhancing cities and favoring the development of healthy, smart, resilient cites	Design new standardized protocols for sharing data and information during emergencies

Πίνακας 3.2: Εφαρμογές διαχείρισης του Covid-19 με χρήση AI και Big Data (Πηγή: [9])

3.5 Ασφάλεια στο IoMT

Σύμφωνα με μια πρόσφατη μελέτη, η μετάδοση δεδομένων συσκευών του Διαδικτύου των Πραγμάτων (IoT) είναι μη κρυπτογραφημένη πάνω από το 90%, ενώ περίπου το 57% αυτών είναι ευάλωτο σε επιθέσεις που έχουν στόχο την άντληση εμπιστευτικών πληροφοριών. Οι κυβερνοεπιθέσεις μπορεί να καταστούν βλαβερές για το ίδιο το σύστημα, αλλά μπορεί να θέσουν σε κίνδυνο και την ανθρώπινη ζωή.

Η ταχεία εξέλιξη και υιοθέτηση του IoMT, ειδικότερα σε περιόδους έξαρσης πανδημιών, είναι φυσιολογικό να εγείρει περαιτέρω ανησυχίες σε θέματα ασφαλείας, με αποτέλεσμα η διασφάλιση του απορρήτου των ευαίσθητων δεδομένων υγείας να αποτελεί μια πρόκληση για την αρχιτεκτονική του IoMT.

Οι προδιαγραφές ασφαλείας και απορρήτου σε ένα οικοσύστημα IoMT πρέπει να είναι αυστηρές, ενώ είναι απαραίτητη προσέγγιση η χρήση κρυπτογραφημένων αλγορίθμων για την αποτελεσματική ανίχνευση και πρόληψη εισβολών. Έτσι, η προτεινόμενη στρατηγική για τις μεθόδους ασφαλείας δίνει έμφαση στη διαχείριση κλειδιών, την ανίχνευση εισβολών, τον έλεγχο ταυτότητας και πρόσβασης του χρήστη.

Σε μια εφαρμογή IoMT, η ασφάλεια διαδραματίζει κρίσιμο ρόλο καθώς μπορεί να επηρεάσει με αρνητικό τρόπο τη ψυχολογική και βιολογική υγεία των χρηστών. Για παράδειγμα, επιθέσεις σε εμφυτεύσιμες συσκευές, όπως τα εμφυτεύματα εγκεφάλου, μπορεί να οδηγήσουν σε θάνατο του ασθενή. Επίσης, ο Οργανισμός Τροφίμων και Φαρμάκων των ΗΠΑ (FDA), το 2018, αναθεώρησε τις οδηγίες ηλεκτρονικής προστασίας των εφαρμογών ενσωμάτωσης ιατρικού εξοπλισμού, περιλαμβάνοντας ενημερωμένους κανονισμούς αναφορικά με την ασφάλεια των ιατρικών δεδομένων ασθενών.

Σύμφωνα με έρευνες αναφορικά με την ασφάλεια του IoMT, ο γεωγραφικός εντοπισμός μπορεί να υποστηρίξει τον προσδιορισμό hotspot μολύνσεων, αλλά θα πρέπει οι πληροφορίες τοποθεσίας του πύργου κινητής τηλεφωνίας να είναι προσβάσιμες από το Υπουργείο Υγείας, ενώ η πρόσβαση στη συλλογή δεδομένων να μην είναι δημόσια. Μια μελέτη που διεξήχθη από ειδικούς ασφαλείας ανακάλυψε περισσότερες από 68.000 διαδικτυακές υπηρεσίες υγείας εκτεθειμένες σε κυβερνοεπιθέσεις, με 12.000 από αυτές να ανήκουν σε έναν μόνο υγειονομικό φορέα. Ακόμη και ο πρώην Αντιπρόεδρος των ΗΠΑ, Dick Cheney, αφαίρεσε την ασύρματη επικοινωνία του εμφυτεύματος στην καρδιά του, λόγω αυξημένων ανησυχιών για πιθανή απειλή της ζωής του μέσω κυβερνοεπίθεσης μέσω της εμφυτευμένης συσκευής. Από τις δημοφιλέστερες απειλές στο IoMT αποτελούν οι επιθέσεις Denial-of-Service (DoS), Injection και η διαρροή δεδομένων (data leakage) [3].

3.5.1 Τύποι επιθέσεων σε IoMT

Επιθέσεις άρνησης υπηρεσίας (Denial-of-Service attacks): Αυτός ο τύπος επίθεσης συμβαίνει όταν ένα σύστημα IoT εμποδίζεται να αποστείλλει δεδομένα υγείας ασθενών στις αντίστοιχες υπηρεσίες που βρίσκονται στο cloud ή σε μια βάση δεδομένων, ή όταν ο επαγγελματίας υγείας δεν μπορεί να ανακτήσει πληροφορίες ασθενών. Τα συχνά αντίγραφα ασφαλείας δεδομένων μπορεί να είναι χρήσιμα για την ανάκτηση του ιστορικού εγγραφών, αλλά διαταράσσουν την αλληλεπίδραση επικοινωνίας σε πραγματικό χρόνο. Ο ισχυρός έλεγχος ταυτότητας και η χρονική σήμανση ενεργειών αλληλεπίδρασης θεωρείται από τους ειδικούς IoT ότι μπορεί να μειώσουν τη μορφολογία και την κινητικότητα των επιθέσεων.

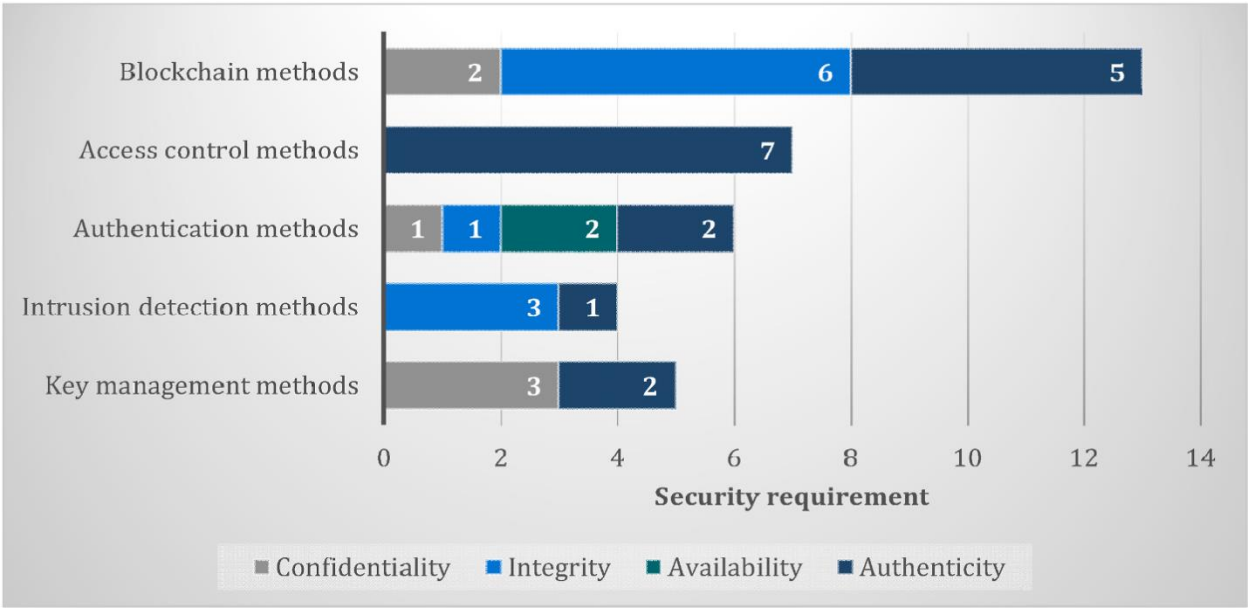
Επιθέσεις με έγχυση (Injection attacks): Η ακεραιότητα των δεδομένων διασφαλίζει ότι τα δεδομένα δεν έχουν αλλοιωθεί ή χειραγωγηθεί υπό οποιαδήποτε μορφή μέσα από τα κανάλια επικοινωνίας. Ένα παράδειγμα τέτοιας επίθεσης είναι η επίθεση έγχυσης ψευδών δεδομένων, που μπορεί να οδηγήσει στη μεταφορά ψευδών στοιχείων σε ένα κέντρο πληροφοριών υγειονομικού φορέα. Επίσης, άλλος συχνός τύπος επίθεσεων είναι η έγχυση SQL κώδικα που μπορεί να δώσει πρόσβαση σε κακόβουλους χρήστες σε βάσεις ιατρικών δεδομένων, χωρίς να μπορεί να γίνει αντιληπτό από τους διαχειριστές του συστήματος.

Διαρροή δεδομένων, απόρρητο και εμπιστευτικότητα (Data leakage, privacy & confidentiality): Η συλλογή, η αποθήκευση και μεταφορά αρχείων υγείας ενός χρήστη θα πρέπει να συμμορφώνεται με τους νομικούς και ηθικούς φραγμούς περί απορρήτου. Βέβαια, αυτό μπορεί να αποδειχθεί ανέφικτο, όταν αφορά την ανίχνευση επαφών για την μείωση έξαρσης της πανδημίας, όπου απαιτείται η παρακολούθηση της κινητικότητας χρηστών με συγκεκριμένα χαρακτηριστικά. Η διαφανής και προσπελάσιμη φύση της ασύρματης επικοινωνίας, μπορεί να καταστήσει τα συστήματα IoMT ευάλωτα σε διαρροή δεδομένων μέσω επιθέσεων sniffing, που σκοπό έχουν την υποκλοπή πληροφοριών, την ανάλυση κυκλοφορίας και την διενέργεια κακόβουλων επιθέσεων.

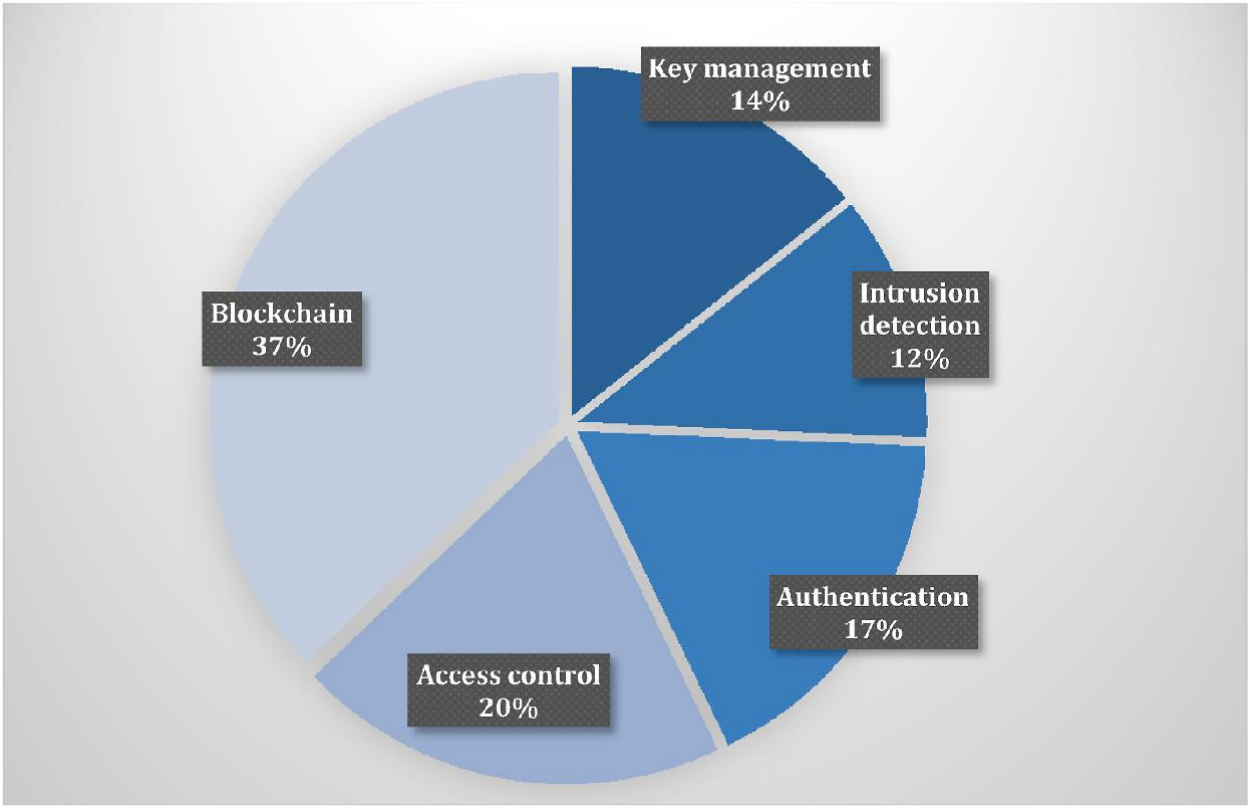
Ασφάλεια αισθητήρων/συσκευών IoMT (IoMT sensor/device safety): Η «ανοσολογική απόκριση» των ιατρικών συσκευών αποτελεί τη πιο κρίσιμη πτυχή των συστημάτων, λόγω των περιορισμών της υπολογιστικής ισχύος και των πόρων εξοπλισμού του Δαδικτύου των Ιατρικών Πραγμάτων. Γενικές λύσεις που σχετίζονται με προβλήματα ασφαλείας δεν μπορούν να εφαρμοστούν, καθώς η υλοποίησή τους σε αυτές τις συσκευές χαμηλής κατανάλωσης έχει αμφίβολα αποτελέσματα, ενώ ένα πιο ελαφρύ πλαίσιο λογισμικού ασφαλείας φαίνεται να έχει υψηλότερη συμβατότητα [3].

3.5.2 Τεχνολογία βελτίωσης ασφάλειας IoMT

Η εφαρμογή της ασφάλειας σε συσκευές IoMT είναι μια πρόκληση, εξαιτίας των περιοριστικών κριτηρίων στη χρήση συσκευών και τη κατανεμημένη αρχιτεκτονική του οικοσυστήματος IoMT. Επίσης, αυτές οι συσκευές συνήθως βρίσκονται στις τερματικές άκρες του δικτύου, λειτουργούν απομακρυσμένα ή εντός του ανθρώπινου σώματος, και επομένως δεν είναι πάντα προσβάσιμες. Απαιτείται πλαίσιο προστασίας δεδομένων και ασφαλούς επικοινωνίας που πληροί τις απαιτήσεις ασφαλείας και καταστεί τα συστήματα IoMT ασφαλή. Πιθανές παρεμβάσεις μπορεί να περιλαμβάνουν έλεγχο πρόσβασης μέσω επαλήθευσης ταυτότητας, προστασία κλειδιού κρυπτογράφησης και τεχνολογία blockchain. Το παρακάτω γράφημα απεικονίζει τις παρεμβάσεις και τις απαιτήσεις ασφαλείας του IoMT.



Γράφημα 3.10: Μέθοδοι και απαιτήσεις ασφαλείας IoMT (Πηγή: [3])



Γράφημα 3.11: Ποσοστιαία ανάλυση των μεθόδων ασφαλείας του IoMT (Πηγή: [3])

3.5.2.1 Αυθεντικοποίηση και κρυπτογράφηση

Πολλά συστήματα IoT εμφανίζουν ελλείψεις ή αδυναμίες ελέγχου ταυτότητας ως αποτέλεσμα των περιορισμών του τεχνολογικού εξοπλισμού, της κατανάλωσης ενέργειας και των άλλων υπολογιστικών πόρων. Δυστυχώς, η παραπάνω αδυναμία γεννά ευκαιρίες για κυβερνοεπιθέσεις, με σχετική έρευνα να παρουσιάζει δύο τύπους ελέγχου ταυτότητας μέσω συσκευής και χρήστη, με στόχο την ασφάλεια/κρυπτογράφηση των δεδομένων και τη διασφάλιση ακεραιότητας της επικοινωνίας.

Μια συχνή λύση ελέγχου ταυτότητας χρήστη σε ιδιωτικούς διακομιστές συστημάτων IoMT είναι η εφαρμογή βιομετρικής ασφάλειας. Τα βιομετρικά στοιχεία μπορούν να ληφθούν εύκολα από φορητό ή εμφυτεύσιμο εξοπλισμό στο ανθρώπινο σώμα και να χρησιμοποιηθούν ως εργαλεία αναγνώρισης για ασφαλή επικοινωνία.

Μελετώντας τους περιορισμούς εξοπλισμού, διαπιστώνουμε ότι οι προσεγγίσεις ασφαλείας χαμηλών απαιτήσεων, όπως η κρυπτογραφία, ο υβριδικός εντοπισμός ανωμαλιών και ο έλεγχος ταυτότητας πολλαπλών παραγόντων μπορούν να αναβαθμίσουν το επίπεδο ελέγχου ταυτότητας. Συγκεκριμένα, έχει προταθεί ένα υψηλής ασφάλειας και χαμηλών προδιγραφών σύστημα ελέγχου ταυτότητας για το WBAN, όπου η προστασία επικοινωνίας μπορεί να διασφαλιστεί χωρίς τη χρήση ασύμμετρης κρυπτογράφησης, ελαχιστοποιώντας σημαντικά το υπολογιστικό κόστος και τον κίνδυνο επιθέσεων.

Το έργο των Hossain et al. (2018) στόχευε σε ένα σύστημα ασφαλείας, που μπορεί να εγγυηθεί υψηλά επίπεδα ελέγχου ταυτότητας χρήστη με την αξιοποίηση ενός διακριτικού ασφαλείας (token) για υψηλότερη προστασία πρόσβασης σε ιατρικές συσκευές. Η κρυπτογραφημένη πρόσβαση αποτρέπει ενέργειες πλαστογραφίας, διασφαλίζοντας ασφαλή πρόσβαση σε ιατρικές συσκευές IoT. Επίσης, καταφέρνει να εντοπίζει κακόβουλες συσκευές, ανιχνεύοντας εισβολές με βάση την αξιοπιστία του συμπεριφορικού προφίλ αυτών των συσκευών στο οικοσύστημα IoMT.

Μια άλλη έρευνα ανέλυσε ένα πρωτόκολλο ελέγχου ταυτότητας πολλαπλών επιπέδων για το WBAN. Η σχεδίαση του πρωτοκόλλου πολλαπλής διανομής περιλαμβάνει ένα νέο πρωτόκολλο ελέγχου ταυτότητας χωρίς σύζευξη και πιστοποιητικό κρυπτογράφησης, καθώς και έναν αλγόριθμο εγκαθίδρυσης κοινού κλειδιού με κρυπτογράφηση αλγορίθμου ελλειπτικής καμπύλης.

Όσον αφορά την επικοινωνία μέσω αναγνώρισης ραδιοσυχνοτήτων (RFID), σε ένα σύστημα IOMT έχουν παρουσιαστεί αρκετές επιθέσεις που συνδέονται με ανωνυμία, μυστική αποκάλυψη, επανάληψη, ιχνηλασιμότητα και πλαστοπροσωπία. Για το λόγο αυτό, δημιουργήθηκε ένα νέο πρωτόκολλο αμοιβαίου ελέγχου ταυτότητας RFID με στόχο την ασφαλή επικοινωνία και τη προστασία απορρήτου ενσωματώνοντας τη λογική Burrows–Abadi–Needham (BAN), με την οποία επικυρώνονται τα χαρακτηριστικά ασφαλείας. Επιπλέον, ερευνητές ανέπτυξαν μια μέθοδο επαλήθευσης ταυτότητας μέσω του πρωτοκόλλου μεταφοράς ιδιοκτησίας σε εφαρμογές IoMT, έτσι ώστε να ικανοποιήσουν τις

απαιτήσεις ασφαλείας ελέγχου πρόσβασης και διατήρησης του απορρήτου και να ξεπεράσουν προβλήματα που συνδέονται με τον αποσυγχρονισμό, την ιχνηλασιμότητα, τις επιθέσεις εμπιστευτικών πληροφοριών και την άρνηση παροχής υπηρεσίας (DoS). Σε άλλη σχετική έρευνα, με χρήση της ίδιας λογικής BAN, προτάθηκε ένα πρωτόκολλο εγκαθίδρυσης επικυρωμένου κλειδιού χρησιμοποιώντας κρυπτογραφία ελλειπτικής καμπύλης (Elliptic Curve Cryptography) για την εξάλειψη των αδυναμιών ασφαλείας που εντοπίζονταν στα υπάρχοντα πρωτόκολλα επικοινωνίας IoMT.

Η έρευνα των Hussain et al. (2018) τόνισε ζητήματα ασφαλείας και απορρήτου ιατρικών δεδομένων που συναντώνται σε έξυπνα κινητά Android. Πραγματοποιήθηκε ανάπτυξη ενός συνόλου ελέγχων και πολιτικών ασφαλείας που στοχεύουν στη προστασία από διαφορετικές επιθέσεις και κακόβουλο λογισμικό, όπως περιορισμούς αδειών χρήσης, σκίαση δεδομένων και την ενεργοποίηση/απενεργοποίηση των περιφερειακών συσκευών του συστήματος.

Γενικότερα, οι απαιτήσεις απορρήτου τη εποχή της πανδημίας είναι ένα ζήτημα κρίσιμης σημασίας, με έμφαση στον εντοπισμό επαφών και τον έλεγχο της κινητικότητας. Αν και οι εφαρμογές ιχνηλάτησης επαφών είναι ζωτικής σημασίας για την υγειονομική επιτήρηση, πληροφορίες των χρηστών μπορεί να διαρρεύσουν σε τρίτους, δημιουργώντας σοβαρές ανησυχίες αναφορικά με το απόρρητο προσωπικών δεδομένων. Ως εκ τούτου, τα συστήματα IoMT πρέπει να αναπτύξουν μηχανισμούς βελτίωσης εμπιστοσύνης στους κεντρικούς διακομιστές ή να χρησιμοποιήσουν τις αποκεντρωμένες προσεγγίσεις που υποστηρίζονται από την τεχνολογία blockchain.

3.5.2.2 Τεχνολογία Blockchain

Το Blockchain βοηθά στη προστασία του απορρήτου δεδομένων σε ένα IoMT, καθώς ενσωματώνει μια αποκεντρωμένη αρχιτεκτονική, κρυπτογραγημένες συναλλαγές, αμετάβλητη και αξιόπιστη διασύνδεση με επαληθεύσιμη επιστροφή μετάδοσης και άμεση ταυτοποίηση συσκευής βάσει των μοναδικών αναγνωριστικών που διαθέτει. Η τεχνολογία Blockchain μετριάζει το ζήτημα των κατανεμημένων συσκευών μέσω της διαχείρισης πολλαπλών υπηρεσιών/πλατφορμών, βελτιώνει την προστασία απορρήτου κατά την ανταλλαγή δεδομένων, την αξιοπιστία των κατανεμημένων υπηρεσιών εξουσιοδότησης και επαλήθευσης ταυτότητας, καθώς και τη συνέπεια ανίχνευσης συναλλαγών σε συσκευές IoMT. Ωστόσο, δεδομένης της διαθεσιμότητας των δεδομένων σε όλα τα μέλη του blockchain, υπάρχει πάντοτε η πιθανότητα διαρροής πληροφοριών. Στις πιο συχνές επιθέσεις ενάντια συστατικών στοιχείων του blockchain ανήκουν η διαρροή απορρήτου πορτοφολιού (wallet privacy leakage), η επαναχρησιμοποίηση διευθύνσεων, οι επιθέσεις Sybil, η αναγνώριση χαρακτηριστικών του χρήστη (deanonymization), οι επιθέσεις σύνδεσης και η πλαστογράφηση μηνυμάτων. Είναι φυσιολογικό για τους χρήστες ενός συστήματος IoMT να χρησιμοποιούν το δημόσιο Wi-Fi (δημόσια διευθυνσιοδότηση)

νοσοκομείων, και ως εκ τούτου να εκτίθενται σε οποιονδήποτε κακόβουλο χρήστη έχει πρόσβαση σε αυτές τις διευθύνσεις μέσω του μη ασφαλούς δημόσιου ασύρματου δικτύου του υγειονομικού φορέα.

Τα blockchain wallets δημιουργήθηκαν για να ξεπεραστούν τα προβλήματα επαναχρησιμοποίησης διευθύνσεων, μέσα από τη αξιοποίηση προσωρινών διευθύνσεων μιας χρήσης σε κάθε μετάδοση δεδομένων. Το Blockchain wallet είναι ένα λογισμικό διαφανούς διαχείρισης διευθύνσεων, με δυνατότητα αποκάλυψης του απορρήτου συστήματος σύμφωνα με το βαθμό ασφαλείας του λογισμικού που το συνοδεύει. Οι επιθέσεις Sybil χαρακτηρίζονται από τη σκόπιμη δημιουργία πολλών ψεύτικων κόμβων (nodes) χρήστη με στόχο τον έλεγχο του δικτύου blockchain IoMT. Η εξαπάτηση μηνυμάτων (spoofing) οδηγεί σε πλαστογραφία μηνυμάτων στο δίκτυο IoMT, που ισοδυναμεί με επικοινωνία εσφαλμένων πληροφοριών και τη διαμόρφωση ενός σοβαρού πλήγματος στην ασφάλεια απορρήτου. Οι επιθέσεις διασύνδεσης προσανατολίζονται στα δεδομένα που αποθηκεύονται σε ένα IoMT, με σκοπό την εξωτερική σύζευξη προβληματικών δεδομένων με τις αξιόπιστες προστατευμένες πληροφορίες. Με κατεύθυνση την αντιμετώπιση του προβλήματος, οι προσεγγίσεις ταξινομήθηκαν σε 2 κατηγορίες: (i)Διατήρηση του απορρήτου ταυτότητας χρήστη και (ii)Διατήρηση του απορρήτου κατά τη μετάδοση ενός κόμβου στο IoMT. Γενικότερες προσεγγίσεις προστασίας απορρήτου στο blockchain αποτελούν η κρυπτογράφηση, τα έξυπνα συμβόλαια, η διατήρηση ανωνυμίας και οι διαφοροποιημένες πολιτικές απορρήτου [3].

Γενικά, η κρυπτογράφηση χρησιμοποιείται στην προστασία απορρήτου συσκευών, ενώ μπορεί να παραβιαστεί μόνο με διάσπαση κρυπτογράφησης του μαθηματικού αλγορίθμου. Ερευνητές, στηριζόμενοι στην τεχνολογία του blockchain, ανέπτυξαν μια κρυπτογραφημένη κοινή χρήση ηλεκτρονικών ιατρικών αρχείων, μέσω ενός συνδυασμού κρυπτογράφησης (Attribute-Based Encryption) και υπογραφής βάσει χαρακτηριστικών (Attribute-Based Signature). Ικανοποιεί τις απαιτήσεις περί μη πλαστογράφησης και ανωνυμίας, αντιστεκόμενη σε επιλεγμένες επιθέσεις αποκρυπτογράφησης. Το σύστημα τηλεϊατρικής υλοποιεί ενημέρωση πολλαπλών φορέων Attribute-Based Encryption, διατηρώντας την ανεξαρτησία του, με στόχο την αποφυγή λανθασμένης διάγνωσης από κακόβουλες επιθέσεις με προέλευση από το εσωτερικό του cloud. Επίσης, προτάθηκε ένα σχήμα κοινής χρήσης ιατρικών δεδομένων που χρησιμοποιεί αλυσίδες μπλοκ έπειτα από σχετική αδειοδότηση και περιλαμβάνει κρυπτογραφημένο κείμενο βάσει χαρακτηριστικών (Attribute-Based Encryption) για τον έλεγχο πρόσβασης και την εμπιστευτικότητα των ιατρικών δεδομένων.

Τα έξυπνα συμβόλαια αναπτύσσονται και εκτελούνται με βάση της λογικής των αποκεντρωμένων ιδιοτήτων του blockchain. Οι λεπτομέρειες της συναλλαγής καταγράφονται σαν κώδικας προγραμματισμού σύμφωνα με τις απαιτήσεις του συστήματος blockchain. Επίσης, ερευνητές σχεδίασαν έναν αξιόπιστο μηχανισμό ελέγχου πρόσβασης μέσω έξυπνων συμβάσεων για την ηλεκτρονική

καταγραφή ιατρικών δεδομένων στο blockchain και ένα αποκεντρωμένο διαλειτουργικό σύστημα αρχείων σε μια φορητή cloud πλατφόρμα. Σε άλλη έρευνα, οι έξυπνες συμβάσεις υλοποιούσαν μηχανισμούς επαλήθευσης ταυτότητας, μέσω της εφαρμογής κοινής χρήσης ιατρικών δεδομένων ενός συστήματος blockchain, με σκοπό την αποφυγή παραβίασης των αδειών χρήσης.

Οι Wang et al., το 2020, ανέπτυξαν μια ασφαλή μέθοδο μετάδοσης και αποθήκευσης δεδομένων blockchain σε συστήματα IoMT που λειτουργεί μέσω WBAN. Η υλοποίηση επικεντρώθηκε στην κοινή χρήση ιατρικών αρχείων με εφαρμογή blockchain κοινοπραξίας με κρυπτογράφηση. Πιο συγκεκριμένα, εισήγαγαν ένα σύστημα κοινής χρήσης προσωπικών ιατρικών αρχείων βασισμένο σε cloud με ακεραιότητα δεδομένων που επαληθεύεται μέσω έξυπνων συμβολαίων σε συνδυασμό με συμμετρική κρυπτογράφηση και τεχνικές Attribute-Based Encryption για την επίτευξη προστασίας απορρήτου και αδειών πρόσβασης. Επιπροσθέτως, μια άλλη μελέτη παρουσίασε ένα σύστημα blockchain διαχείρισης ιατρικών αρχείων που βασίζεται στη χρήση έξυπνων συμβολαίων που αξιοποιούν την εφαρμογή χρονικής σήμανσης και προηγμένων τεχνικών κρυπτογράφησης.

Η ανωνυμία (Anonymization) είναι μια ακόμη γνωστή τεχνική για τη προστασία του απορρήτου σε εφαρμογές blockchain IoMT. Το διαφοροποιημένο απόρρητο είναι μια μέθοδος που προστατεύει τους κόμβους IoMT προσθέτοντας θόρυβο μέσω μιας δυναμικής διατάραξης δεδομένων. Για την υλοποίηση χρησιμοποιήθηκε μια ελλειπτική υπολογιστική καμπύλη Diffie-Hellman σε ένα τυχαίο μοντέλο με στόχο να αναπτυχθεί μια αρχιτεκτονική cloud με αμοιβαία επαλήθευση ταυτότητας που διασφαλίζει την ανωνυμία του ασθενούς. Τα μηνύματα κάνουν χρήση δυναμικής κρυπτογράφησης, για να ενσωματωθούν σε ανώνυμα επαληθευμένους κόμβους [3].

Άλλη μελέτη πρότεινε ένα μοντέλο Μηχανικής Μάθησης (ML) για τη διατήρηση απορρήτου, το secure Support Vector Machine (SVM), που σκοπό έχει να εκπαιδεύσει τα κρυπτογραφημένα δεδομένα IoT της τεχνολογίας blockchain. Ο αλγόριθμος εκπαίδευσης υλοποιείται μέσα από το σχεδιασμό block με δομή ασφαλείας, με χρήση τεχνικών όπως ο πολλαπλασιασμός πολυωνύμων και η σύγκριση ασφαλείας, μέσω της εφαρμογής του ομοιομορφικού κρυπτοσυστήματος Paillier, που απαιτεί μόνο δύο αλληλεπιδράσεις σε μία επανάληψη, χωρίς την ανάγκη επικύρωσης από αξιόπιστο τρίτο παράγοντα. Η τεχνολογία blockchain εγγυάται την ασφάλεια και τη διαφάνεια δεδομένων του δικτύου όσον αφορά την αποθήκευση αυτών στους διάφορους παρόχους υπηρεσιών, μέσω της κρυπτογράφησης και της καταχώρησης τους σε ένα αποκεντρωμένο σύστημα [28].

Κεφάλαιο 4ο: Υγειονομική επιτήρηση Covid-19 και IoMT

4.1 Εισαγωγή

Τα νοσοκομεία σε όλο τον κόσμο αντιμετωπίζουν σημαντικές ελλείψεις συστημάτων εξαερισμού, μονάδων εντατικής θεραπείας (ICU), συστημάτων παροχής οξυγόνου και εξοπλισμού ατομικής προστασίας (PPE) που απαιτούνται για την περίθαλψη ασθενών με Covid-19. Τα συστήματα υγειονομικής περίθαλψης ακόμη και των πιο ανεπτυγμένων χωρών στον κόσμο βρίσκονται στα πρόθυρα κατάρρευσης λόγω του εκθετικά αυξανόμενου αριθμού ασθενών, γεγονός που καθιστά επιτακτική την ανάγκη διαχείρισης των νοσούντων απομακρυσμένα με αποτελεσματικό τρόπο [11].

Η ικανότητα των υπηρεσιών IoMT στην απομακρυσμένη συλλογή δεδομένων και παρακολούθηση ασθενών σε κατ' οίκον περιορισμό, ανέδειξε τον κομβικό τους ρόλο στην καταπολέμηση εξάπλωσης του ιού. Οι υγειονομικοί υπάλληλοι και οι αρχές χρειάζονται πληθώρα δεδομένων για τη διαχείριση μιας ραγδαία αναπτυσσόμενης πανδημίας, από το αρχικό στάδιο της διάγνωσης και του εντοπισμού εξάπλωσης στη κοινότητα. Στα απαραίτητα δεδομένα ανήκουν η θερμοκρασία του σώματος, η τοποθεσία και το ιστορικό μετακινήσεων, τα οποία συλλέγονταν αρχικά χειροκίνητα από τους ίδιους τους εργαζόμενους ενέχοντας υψηλή επικινδυνότητα λόγω αυξημένης επαφής με δυνητικά κρούσματα. Ακολούθησε η πρόταση των ερευνητών για χρήση του διαδικτύου των πραγμάτων μέσω ενός δικτύου ετερογενών αισθητήρων που συναντάμε σε φορητές συσκευές, κινητά τηλέφωνα, κάμερες και drones, καθώς τα μεγάλης εμβέλειας και χαμηλής κατανάλωσης ενέργειας πρωτόκολλα επικοινωνίας έχουν επιτρέψει την συλλογή και παρακολούθηση δεδομένων σε μεγάλη έκταση. Τα πρωτόκολλα LPWAN σε συνδυασμό με την ασύρματη δικτύωση αισθητήρων (SDWSN) μπορούν να βοηθήσουν στη μάχη καταπολέμησης του Covid-19 [16].

4.2 Προηγούμενες υγειονομικές κρίσεις, τεχνολογία και εφαρμογές

Ένα σύστημα που ενσωματώνει την αρχιτεκτονική IoMT και τεχνολογίες, συμπεριλαμβανομένων των RFID, WBAN και των υπηρεσιών cloud, είναι σε θέση να παρέχει αξιόπιστη παρακολούθηση της υγειονομικής περίθαλψης και έγκαιρη διάγνωση επιδημικών ασθενειών. Βεβαίως, σε τέτοιες περιπτώσεις, το σύστημα θα πρέπει να παρακολουθείται από άρτια εκπαιδευμένους επαγγελματίες λόγω της εξαιρετικά μολυσματικής φύσης αυτών των ιών. Το σύστημα καταγράφει τις στενές επαφές σε πραγματικό χρόνο και αποθηκεύει δεδομένα υγείας για τον μετριασμό εξάπλωσης του COVID-19. Ωστόσο, κατά τη διάρκεια του σοβαρού οξέος αναπνευστικού συνδρόμου (SARS-CoV), του κορωνοϊού του αναπνευστικού συνδρόμου της Μέσης Ανατολής (MERS-CoV) και της επιδημίας του Έμπολα, η τεχνολογία του Διαδικτύου των Πραγμάτων δεν ήταν ακόμη αναπτυγμένη, γεγονός που πιθανότατα αποτέλεσε ένα

σημαντικό λόγο ανάπτυξης ελάχιστων προσεγγίσεων αναφορικά με τη χρήση του στην αντιμετώπιση των προηγούμενων επιδημιών [3].

4.2.1 SARS-CoV – Ασία

Το 2002, ο ιός SARS-CoV εντοπίστηκε στη κινέζικη πόλη Γκουανγκντόνγκ (Guangdong) μέσω ιχνών ανθρώπινων λοιμώξεων, χωρίς ωστόσο να γίνει ποτέ ξεκάθαρη η πηγή αυτού του ιού. Ο SARS-CoV αναγνωρίστηκε ως το πρώτο ξεχωριστό στέλεχος κορωνοϊού το 2003, εμφανίζει συμπτώματα που θυμίζουν αυτά της γρίπης, εξαπλώθηκε σε 26 χώρες επιφέροντας την μόλυνση περισσότερων από 7000 ανθρώπων και τον θάνατο περίπου 800.

Μία από τις λίγες εφαρμογές IoT που αξιοποιήθηκαν για τον ιό SARS προήλθε από την κυβέρνηση της Σιγκαπούρης και αφορούσε μια εφαρμογή καραντίνας στο σπίτι για ύποπτα κρούσματα και μολυσμένα άτομα μέσω της χρήσης webcams. Εγκαταστάθηκαν ηλεκτρονικές κάμερες σε σπίτια ατόμων σε καραντίνα, ενώ σε περιπτώσεις άτυπης διακοπής της καραντίνας, δίνονταν γραπτές προειδοποιήσεις καθώς και ηλεκτρονικά βραχιολάκια καρπού προς συμμόρφωση των πολιτών. Οι αρχές ειδοποιούνταν εάν το ηλεκτρονικό βραχιόλι σπάσει ή όταν το άτομο απομακρυνθεί από το σπίτι καθώς η συσκευή ήταν συνδεδεμένη με μία συγκεκριμένη τηλεφωνική γραμμή ενημέρωσης.

Τα συστήματα γεωγραφικών πληροφοριών GIS χρησιμοποιήθηκαν στην επιδημία SARS-CoV το 2002 καθώς και στην εποχική γρίπη το 2020, παρέχοντας πολύτιμες πληροφορίες για την παρακολούθηση των μολυσμένων κρουσμάτων και την ανάλυση της νέας πηγής της νόσου.

4.2.2 MERS-CoV – Μέση Ανατολή

Το 2012, άτομα που παρουσίαζαν βήχα, δύσπνοια, διάρροια και πυρετό αναγνωρίστηκαν ως θύματα του MERS-CoV. Η ανάδειξη του νέου ιού διήρκεσε αρκετούς μήνες, καθώς το σύνδρομο εντοπίστηκε για πρώτη φορά στη Σαουδική Αραβία, με ενδείξεις που υποδείκνυαν τους δρομείς καμήλας ως πιθανή πηγή μόλυνσης, αλλά αυτό δεν επιβεβαιώθηκε ποτέ επίσημα. Η Ιορδανία, το Κατάρ, η Σαουδική Αραβία και τα Ηνωμένα Αραβικά Εμιράτα ήταν μεταξύ των χωρών που καταγράφηκαν μεταξύ των πρώτων κρουσμάτων. Όπως και ο SARS, ο νέος ιός προκαλούσε στους ασθενείς νεφρική ανεπάρκεια και σοβαρή πνευμονία.

Η δημοσίευση λεπτομερών πληροφοριών σε πραγματικό χρόνο, όπως ο κατάλογος των νοσοκομείων που διαχειρίζονται κρούσματα MERS-CoV, είναι σημαντική, καθώς έτσι αποφεύγεται η εξάπλωση των λοιμώξεων και ελαχιστοποιείται ο αριθμός των θετικών κρουσμάτων. Συνεπώς, η πρόταση αφορά τα στάδια πρώιμου ελέγχου της επιδημίας, μέσω ενός συστήματος έγκαιρης διάγνωσης των συμπτωμάτων, διαχωρισμού του πληθυσμού υψηλής επικινδυνότητας βάσει γεωγραφικής θέσης και ασφάλεια των προσωπικών δεδομένων των θετικών κρουσμάτων με στόχο την αποφυγή μαζικού πανικού.

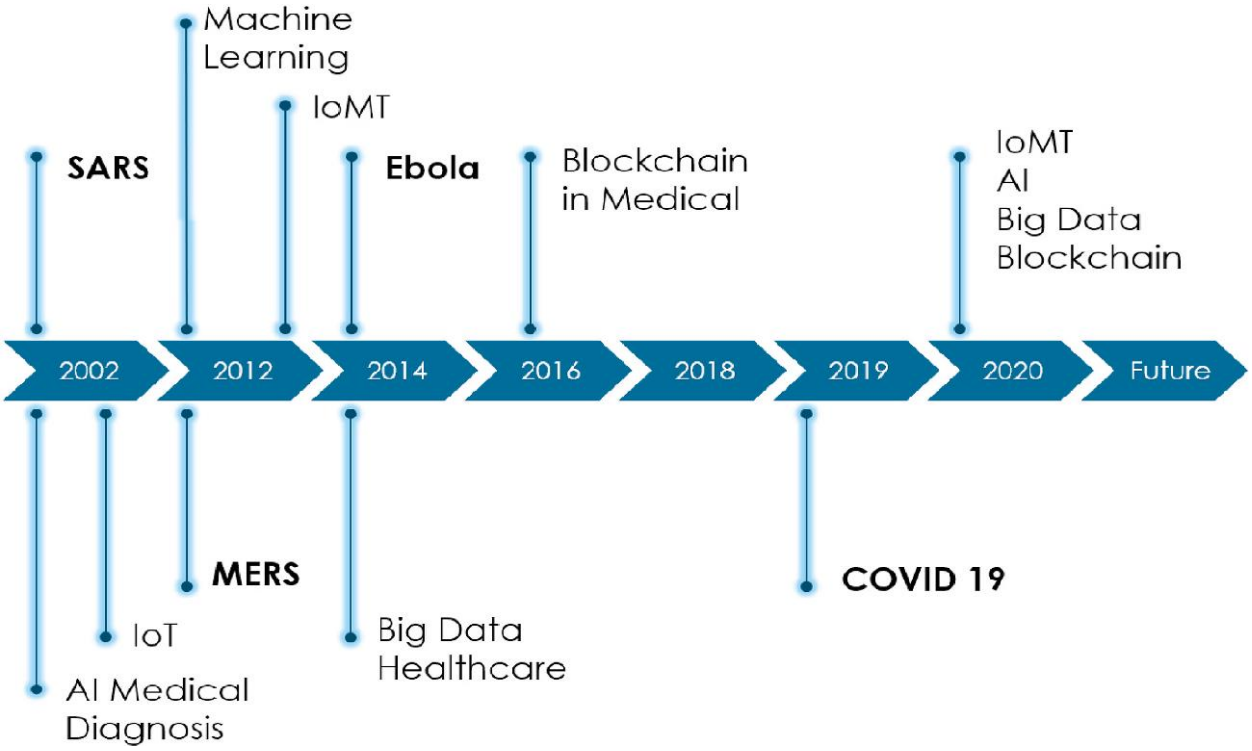
4.2.3 Επιδημία Ebola – Δυτική Αφρική

Η εμφάνιση του ιού Έμπολα (Ebola) ανακοινώθηκε τον Μάρτιο του 2014 από τον Παγκόσμιο Οργανισμό Υγείας (ΠΟΥ). Το πρώτο κρούσμα εντοπίστηκε κοντά στο χωριό Μελιάνδου (Meliandou), στη Γουινέα, αλλά εξαπλώθηκε γρήγορα σε άλλες τέσσερις άλλες χώρες, καθώς η γύρω περιοχή ήταν μια από τις πιο πυκνοκατοικημένες περιοχές της Δυτικής Αφρικής. Τον Αύγουστο του 2014, ο ΠΟΥ χαρακτήρισε την επιδημία αυτή ως «έκτακτη ανάγκη δημόσιας υγείας σε διεθνή κλίμακα ενδιαφέροντος».

Τον Σεπτέμβριο του 2014 επιβεβαιώθηκαν 4507 κρούσματα Έμπολα και 2296 θάνατοι σε πέντε χώρες, μεταξύ των οποίων η Γουινέα, η Νιγηρία, η Δυτική Αφρική, η Σιέρα Λεόνε και η Λιβερία. Αργότερα, ο αριθμός των κρουσμάτων αυξήθηκε σε 28.652, με 11.325 από αυτά να οδηγούν σε θάνατο. Το 2018, μια νέα επιδημία Έμπολα καταγράφηκε στη Mbandaka, της Λαϊκής Δημοκρατίας του Κονγκό.

Οι τεχνολογίες πληροφοριών και επικοινωνιών έχουν εισχωρήσει σε κάθε τομέα της ανθρώπινης ζωής, κυρίως στη δημόσια υγεία. Η χρήση κινητών τηλεφώνων είναι ευρέως διαδεδομένη σε ορισμένες αφρικανικές χώρες, όπως για παράδειγμα στη Μαδαγασκάρη όπου αξιοποιείται η υπηρεσία SMS ως μέθοδος αναφοράς για συστήματα επιτήρησης. Επιπλέον, ένας μεγάλος αριθμός επαγγελματιών υγείας στο σύστημα δημόσιας περίθαλψης της Ουγκάντας συλλέγει δεδομένα υγείας με τη βοήθεια έξυπνων συσκευών, όπως τα PDA. Υπάρχουν πολλές επιβεβαιωμένες αναφορές για τη χρήση τεχνολογιών πληροφοριών, όπως τα έξυπνα τηλέφωνα, τα δίκτυα επικοινωνίας, η τεχνητή νοημοσύνη, η ανίχνευση επαφών, τα γεωγραφικά συστήματα πληροφοριών (GIS) και τα μέσα κοινωνικής δικτύωσης κατά τη διάρκεια της επιδημίας Έμπολα στην Αφρική. Οι Boulos και Geraghty (2020) διεξήγαγαν έρευνα για να περιγράψουν μια σειρά από πρακτικά φορητά συστήματα γεωγραφικών πληροφοριών (GIS) και εφαρμογές για την καταγραφή θετικών κρουσμάτων κατά την περίοδο της επιδημίας. Το Worldpop.org κατέγραψε επίσης την κατανομή του πληθυσμού και τον χάρτη ροής κινητών τηλεφώνων στις αφρικανικές χώρες για να συμβάλει στον έλεγχο της επιδημίας του ιού Έμπολα το 2014.

Η ψηφιακή διαχείριση με χρήση κινητών τηλεφώνων είναι ένας άλλος τρόπος χρήσης της τεχνολογίας πληροφοριών για την ενίσχυση του ελέγχου και της αντιμετώπισης των ασθενειών. Μάλιστα, σε σχετική έρευνα αναλύθηκαν διάφορα συστήματα διαχείρισης, όπως το Σύστημα Διαχείρισης και Ανάλυσης Επιτήρησης και Απόκρισης Επιδημιών (SORMAS), το CommCare (Σύστημα για την απόκριση στον Έμπολα) και το AfyaData. Όλες αυτά τα συστήματα αναλύονται και αξιολογούνται με βάση κριτήρια όπως η ανίχνευση επαφών, η διαχείριση κρουσμάτων, η παρακολούθηση ασθενών και τα εργαστηριακά αποτελέσματα. Με βάση τα πορίσματα της ανάλυσης, το SORMAS, το οποίο είναι ένα σύστημα ανοικτού κώδικα που διενεργεί ανάλυση σε πραγματικό χρόνο μέσω μιας διαδικτυακής εφαρμογής, πληροί όλα τα κριτήρια που αναλύθηκαν. Η έκδοση 2015 του SORMAS έχει σχεδιαστεί για τον έλεγχο του ιού Ebola με τη συμμετοχή των κέντρων υγειονομικής περίθαλψης στη Νιγηρία [3].



Εικόνα 4.1: Χρονολογική σειρά εμφάνισης των τεχνολογιών IoMT για την αντιμετώπιση των επιδημιών (Πηγή: [3])

4.3 Εφαρμογές και τεχνολογία IoMT για την αντιμετώπιση του Covid-19

Η επεκτασιμότητα της τεχνολογίας IoT μπορεί να υποστηρίξει την παρακολούθηση μεγάλου αριθμού ασθενών από το σπίτι ή το νοσοκομείο. Οι βιομετρικές τους μετρήσεις, όπως η αρτηριακή πίεση, ο καρδιακός ρυθμός κ.ά. μπορούν να διαβιβάζονται στο cloud για ανάλυση χωρίς να εκτίθενται οι εργαζόμενοι στον τομέα της υγείας σε κίνδυνο. Το IoT έχει ήδη χρησιμοποιηθεί για τον εντοπισμό και την παρακολούθηση της προέλευσης μιας εστίας μόλυνσης, καθώς και για τη εξασφάλιση τήρησης της καραντίνας σε δυνητικά μολυσμένα άτομα.

Μια μελέτη χρήσης τεχνολογίας IoT για την ανίχνευση πυρετού, είχε προτείνει ένα φθηνό σύστημα IoT που ανέβαζε αυτόματα τα δεδομένα που συγκεντρώνονταν μέσω ασύρματης επικοινωνίας Bluetooth με ένα έξυπνο κινητό Android σε ένα παγκόσμιο δίκτυο. Κατά συνέπεια, τα αποτελέσματα ήταν άμεσα διαθέσιμα, οπουδήποτε στον κόσμο, καθιστώντας ένα αντίστοιχο σύστημα IoT πολύ χρήσιμο εργαλείο για το υγειονομικό προσωπικό προκειμένου να αντιμετωπίσουν μολυσματικές ασθένειες.

Μια άλλη μελέτη χρησιμοποίησε δεδομένα κινητών τηλεφώνων για την καταγραφή της εξάπλωσης του δάγκειου πυρετού στη Σιγκαπούρη το 2013 και το 2014 με λεπτομερείς αναλύσεις για κοντινές αποστάσεις και χρονικές περιόδους. Επομένως, η γεωγραφική επικάλυψη θέσης σε δεδομένα κινητής

τηλεφωνίας μέσω IoT από οποιονδήποτε μολυσμένο ασθενή μπορεί να οδηγήσει σε δύο πράγματα: να βοηθήσει τους επιδημιολόγους στην αναζήτηση του ασθενή μηδέν και να βοηθήσει στον εντοπισμό οποιουδήποτε είχε επαφή με κάποιο θετικό κρούσμα και διατρέχει υψηλό κίνδυνο να έχει μολυνθεί και ο ίδιος. Μια άλλη μελέτη συνέκρινε τις επιδημίες των τριών κορωνοϊών και κατέληξε στο συμπέρασμα ότι δεν υπήρξαν συχνές εκρήξεις κρουσμάτων από τους ιούς SARS και MERS, ενώ φαίνεται ότι οι εφαρμογές IoMT ενδέχεται να μειώσουν τη βαρύτητα του COVID-19 λόγω της υψηλότερης επιτήρησης και ελέγχου των λοιμώξεων στο ευρύ κοινό.

4.3.1 Covid-19 – Ταϊβάν

Λίγες ημέρες αφότου εντοπίστηκε το πρώτο κρούσμα του Covid-19 στις 21 Ιανουαρίου στην Ταϊβάν, οι κυβερνητικοί αξιωματούχοι ανέλαβαν διάφορες πρωτοβουλίες για την πρόληψη της εξάπλωσης του ιού, ιδίως για όσους είχαν επιστρέψει από την Κίνα μετά τις διακοπές του Σεληνιακής Πρωτοχρονιάς. Τα μέτρα αφορούσαν τον εντοπισμό και τον περιορισμό των κρουσμάτων, και την ανάπτυξη νέων τεχνολογιών.

Ψηφιακή επιτήρηση: Οι αρχές της Ταϊβάν, αξιοποιώντας την ανάλυση μεγάλων δεδομένων, τη δημιουργία ειδοποιήσεων σε πραγματικό χρόνο, τις σαρώσεις QR, τις πληροφορίες ταξιδιωτικού ιστορικού και άλλων πόρων κατάφεραν να εντοπίσουν και να κατατάξουν τα άτομα σε διάφορες διακριτές κατηγορίες κινδύνου. Τα άτομα που αναγνωρίστηκαν ως υψηλού κινδύνου κλήθηκαν να τεθούν σε καραντίνα στο σπίτι τους και να παραμείνουν καθ’ όλη τη διάρκεια επώασης της νόσου. Μέχρι τις αρχές Φεβρουαρίου 2020, είχε αναπτυχθεί και εφαρμοστεί ένα ψηφιακό σύστημα βασισμένο σε κινητά τηλέφωνα για την παρακολούθηση και τον εντοπισμό των ατόμων σε καραντίνα.

Το σύστημα, μια συνεργατική προσπάθεια μεταξύ πέντε μεγάλων εταιρειών τηλεπικοινωνιών και της κυβέρνησης της Ταϊβάν, ήταν σε θέση να παρακολουθεί άτομα σε καραντίνα τριγωνοποιώντας τη θέση των τηλεφώνων τους σε σχέση με τους κοντινότερους πύργους κινητής τηλεφωνίας. Εάν το κινητό τηλέφωνο ενός ατόμου ήταν απενεργοποιημένο ή εάν διαπιστωνόταν ότι ένα άτομο είχε παραβιάσει την καραντίνα, ενεργοποιούνταν συναγερμός εντός 15 λεπτών. Στη συνέχεια αναλάμβανε το προσωπικό πρώτης γραμμής (συνήθως αστυνομικοί), το οποίο είχε πρόσβαση σε cloud βάσεις δεδομένων (γνωστό ως σύστημα M-Police) με στόχο τον εντοπισμό αυτών και την επιβολή προστίμων. Αν και πληθαίνουν οι ανησυχίες για την προστασία της ιδιωτικής ζωής, μια πρόσφατη δημοσκόπηση έδειξε ότι η πλειοψηφία (84%) των Ταϊβανέζων υποστηρίζει σθεναρά την κυβερνητική πολιτική για την παρεμπόδιση της εξάπλωσης του ιού, η οποία έχει οδηγήσει σε σημαντικά λιγότερα κρούσματα σε σύγκριση με τη γειτονική Κίνα [3].

Φορητή τεχνολογία IoMT: Η εταιρεία iWEECARE της Ταϊβάν ανέπτυξε μια μικρή φορητή συσκευή IoMT, που ονομάζεται Temp Pal, η οποία είναι σε θέση να ανιχνεύει μη φυσιολογικές θερμοκρασίες και

να στέλνει σχετικές ειδοποιήσεις. Το σύστημα Temp Pal αποτελείται από ένα μαλακό αυτοκόλλητο μεγέθους γραμματόσημου, βάρους 3 γραμμαρίων και διάρκεια μπαταρίας 36 ωρών ανά φόρτιση, το οποίο είναι σε θέση να μεταδώσει συνεχή δεδομένα θερμοκρασίας μέσω Bluetooth Low Energy σε μια εφαρμογή για κινητά και εν συνεχεία στον πίνακα ελέγχου του cloud. Η συσκευή συγκεντρώνει δεδομένα ασύρματα μέσω εξειδικευμένων πυλών BLE/Wi-Fi και συλλέγει τις θερμοκρασίες των ασθενών μέσω έξυπνων επιθεμάτων Temp Pal που είναι προσαρτημένα στο σώμα τους. Το σύστημα IoMT, το οποίο αξιοποιείται τόσο από τα νοσοκομεία όσο και από άτομα σε καραντίνα, εξασφαλίζει την παρακολούθηση σε πραγματικό χρόνο, ενώ παράλληλα μειώνει τη συχνότητα της άμεσης επαφής μεταξύ ασθενών και νοσηλευτών, περιορίζοντας έτσι την εξάπλωση της ασθένειας. Σύμφωνα με το Νοσοκομείο Cheng Hsin της Ταϊβάν όπου εφαρμόστηκε η τεχνολογία, το cloud σύστημα παρακολούθησης θερμοκρασίας εξοικονόμησε χρόνο από το ιατρικό προσωπικό, μείωσε τα σφάλματα καταγραφής, την κατανάλωση εξοπλισμού ατομικής προστασίας (PPE) και το πιο σημαντικό τον κίνδυνο μόλυνσης για το προσωπικό πρώτης γραμμής.

IoMT με τεχνητή νοημοσύνη: Ένα σύστημα ανίχνευσης IoMT με τεχνητή νοημοσύνη έχει αναπτυχθεί στο νοσοκομείο Yonghe Cardinal Tien της Ταϊβάν. Ο έξυπνος ανιχνευτής που αναπτύχθηκε από κοινού μεταξύ της Microsoft Taiwan Azure και τοπικών παρόχων IoT, αξιοποίησε την τεχνητή νοημοσύνη, ένα έξυπνο σύστημα IoT edge και υπηρεσίες cloud για τη συνεχή σάρωση ατόμων, σε πραγματικό χρόνο, κατά την είσοδό τους στο χώρο του νοσοκομείου. Το σύστημα αναγνωρίζει τη θερμοκρασία του σώματος μέσω υπέρυθρης σάρωσης και μπορεί να εντοπίσει αν το άτομο φοράει προστατευτική μάσκα προσώπου μέσω τεχνολογίας τεχνητής νοημοσύνης. Το προσωπικό του νοσοκομείου πρώτης γραμμής ειδοποιείται αμέσως όταν ανιχνευθεί μη φυσιολογική θερμοκρασία ή απουσία προστατευτικής μάσκας σε οποιοδήποτε άτομο εισέρχεται στο νοσοκομείο, αυξάνοντας το επίπεδο υγειονομικής προστασίας προσωπικού και ασθενών, αλλά και απομακρύνοντας το βάρος του συνεχούς ελέγχου από το ανθρώπινο δυναμικό του νοσοκομείου.

4.3.2 Covid-19 – Νότια Κορέα

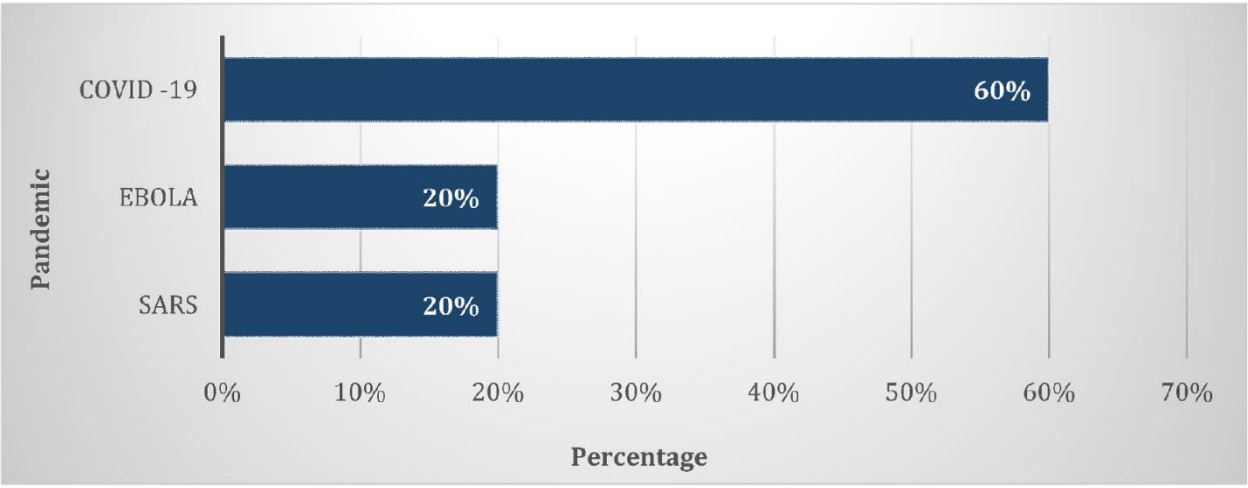
Μεταξύ των χωρών που έχουν πληγεί περισσότερο από τον Covid-19 είναι η Νότια Κορέα. Τον Ιανουάριο του 2020, αναφέρθηκε το πρώτο κρούσμα, μια γυναίκα από την πόλη Γουχάν, που είχε σταματήσει στο αεροδρόμιο της Νότιας Κορέας. Εκείνη την εποχή, η κατάσταση ήταν ακόμα υπό έλεγχο με ελαφρώς περισσότερα από 30 κρούσματα και οι ανησυχίες σχετικά με τη μεταδοτικότητα του COVID-19 πυροδότησαν σκέψεις για την ενίσχυση ελέγχου των συνόρων καθώς και για την ανάπτυξη κατάλληλων πρωτοκόλλων απολύμανσης. Ένα κρίσιμο γεγονός που εκτίναξε την επιδημία στη Νότια Κορέα σημειώθηκε τον Φεβρουάριο, όπου ένας κομιστής του ιού παρευρέθηκε στην εκκλησία

Shincheonji, στο Daegu της Σεούλ, έχοντας ως αποτέλεσμα την μόλυνση περισσότερων από 6000 ανθρώπους από ένα μόνο κρούσμα.

Η προσέγγιση της Νότιας Κορέας για την εξομάλυνση της καμπύλης χωρίς την επιβολή πλήρους αποκλεισμού έχει λάβει τα εύσημα πολλών χωρών σε όλο τον κόσμο. Η ιδέα βασίστηκε στη μείωση του αριθμού των νέων κρουσμάτων, ώστε να μην πιεστεί το σύστημα υγειονομικής περίθαλψης, καθώς και στη ταυτόχρονη μείωση της εξάπλωσης του ιού. Ο πλήρης αποκλεισμός θα ήταν επιζήμιος για την οικονομία της χώρας, καθώς θα μπορούσε να οξύνει τα φαινόμενα οικονομικής ύφεσης και ανεργίας. Η Νότια Κορέα κατόρθωσε να περιορίσει τη μετάδοση του ιού με την ενσωμάτωση και την υιοθέτηση πολλαπλών στρατηγικών που προέκυψαν έπειτα από συζητήσεις μεταξύ επαγγελματιών υγείας, τεχνικών επιτροπών και κυβερνητικών υπηρεσιών. Η προσέγγισή τους, γνωστή ως 3T, σημαίνει Trace, Test και Treat. Η τεχνολογία IoMT χρησιμοποιείται κυρίως στη στρατηγική Trace και για το λόγο αυτό παραλείπεται η ανάλυση των άλλων δύο στρατηγικών (Test και Treat).

Ιχνηλάτηση (Trace): Αυτή η στρατηγική περιγράφει λεπτομερώς τα μέτρα που σχετίζονται με ειδικές διαδικασίες εισόδου και ξεκινά με ένα πλήρες ερωτηματολόγιο για τη συλλογή πληροφοριών σχετικά με την υγεία των ατόμων που είχαν προηγούμενα ταξίδια ή ενδιάμεσους σταθμούς σε χώρες με υψηλό αριθμό επιβεβαιωμένων κρουσμάτων Covid-19. Οι εμπλεκόμενοι ταξιδιώτες πρέπει να υποβληθούν σε υποχρεωτική καραντίνα 14 ημερών πριν από την πραγματοποίηση κάποιου τεστ. Όσον αφορά την ατομική ευθύνη του καθενός, υπενθυμίζεται στα άτομα να τηρούν τις κοινωνικές αποστάσεις, να φορούν μάσκες και να εφαρμόζουν προσεκτικά τους κανόνες προσωπικής υγιεινής. Κάθε νέος επισκέπτης έπρεπε να κατεβάσει μια εφαρμογή αυτοδιάγνωσης στο smartphone του/της, ενώ μέσω αυτής μπορούσε να γίνει γεωγραφικός εντοπισμός του ατόμου.

Ο μηχανισμός εντοπισμού επαφών περιλαμβάνει 4 φάσεις, την αρχικοποίηση, την ενεργοποίηση, την αναφορά και την ανίχνευση. Η εφαρμογή διατηρεί όλα τα αρχεία κίνησης των ατόμων που βρίσκονται σε καραντίνα. Μόλις το άτομο έχει επιβεβαιωθεί ως κρούσμα Covid-19, όλες οι πληροφορίες της κίνησής του θα ληφθούν από την Υγειονομική Αρχή με σκοπό τον εντοπισμό των επαφών του/της. Πραγματοποιούνταν ακόμα και τηλεφωνικές κλήσεις για την ιχνηλάτηση ατόμων που δεν είχαν εγκαταστήσει την εφαρμογή, σε καθημερινή βάση για 14 ημέρες. Επίσης, λειτουργούσε τηλεφωνικό κέντρο για επικοινωνία με τα δημόσια κέντρα υγείας, το οποίο παρείχε συμβουλές υγειονομικής περίθαλψης και ήταν σε θέση να διαχειριστεί έως και 70.000 κλήσεις καθημερινά. Οι πληροφορίες σχετικά με τα επιβεβαιωμένα κρούσματα διαδίδονταν γρήγορα και με διαφάνεια στο κοινό, δύο φορές την ημέρα, έτσι ώστε να γνωρίζει τη θέση των περιοχών εξάπλωσης του ιού [3].



Εικόνα 4.2: Επιδημίες και χρήση τεχνολογικών εφαρμογών (Πηγή: [3])

4.3.3 Covid-19 – Γερμανία

Η Γερμανία, που αποτελεί μια από τις πιο προηγμένες τεχνολογικά χώρες, δημιούργησε μία δεξαμενή ιδεών με στόχο την επιτάχυνση της ψηφιοποίησης της υγειονομικής περίθαλψης, με στόχο την άμεση αντιμετώπιση του Covid-19. Ο υγειονομικός κόμβος καινοτομίας εισηγήθηκε μια λίστα υπηρεσιών τηλεϊατρικής (περιλαμβάνει πολιτική αποζημίωσης, κόστη υπηρεσιών και λειτουργίες), εύκολα προσβάσιμες από το προσωπικό υγείας, χωρίς να απαιτούνται σημαντικές προδιαγραφές σε υλικοτεχνικό εξοπλισμό.

Η Γερμανία εγκαινίασε μια εφαρμογή smartwatch για την ανίχνευση λοιμώξεων και τον μετριασμό της εξάπλωσης του Covid-19, η οποία συλλέγει ζωτικής σημασίας δεδομένα (όπως η θερμοκρασία του σώματος, ο καρδιακός ρυθμός και ο χρόνος ύπνου) από ασθενείς που φορούν ένα έξυπνο ρολόι, με σκοπό να προβλέψει εάν έχουν μολυνθεί από τον ιό. Αυτή η πρόγνωση, μαζί με άλλα δεδομένα που συλλέγονται από τις υγειονομικές αρχές, είναι προσβάσιμη μέσω ενός διαδικτυακού χάρτη για την εκτίμηση του επιπολασμού των λοιμώξεων. Επίσης, μια γερμανική νεοσύστατη εταιρεία, η DOCYET, δημιούργησε μια εφαρμογή που προβλέπει αν ένα άτομο έχει συμπτώματα τυπικής λοίμωξης από SARS-CoV-2. Η εφαρμογή ονομάζεται Corona-Bot και ενημερώνεται συχνά με βάση τις τελευταίες επιστημονικές δημοσιευμένες έρευνες και τα δεδομένα που παρέχουν τα επιστημονικά ιδρύματα.

Επίσης, η Bosch έχει δημιουργήσει μια ταχεία διαγνωστική συσκευή που είναι σε θέση να βεβαιώσει τη μόλυνση Covid-19 μέσα σε λίγες ώρες. Η συσκευή αυτή επιτρέπει την ταχεία ταυτοποίηση και απομόνωση των μολυσμένων ατόμων, μειώνοντας έτσι την εξάπλωση της ασθένειας. Ένα άλλο χαρακτηριστικό της εν λόγω συσκευής είναι ότι μπορεί να ανιχνεύσει άλλες αναπνευστικές ασθένειες, όπως η γρίπη Α και Β, και πρόκειται να είναι διαθέσιμη στη Γερμανία έως τον Απρίλιο του 2020. Επίσης, η Γερμανία έχει επιβάλει τη χρήση καρτών εντοπισμού επιβατών, συλλέγοντας τα στοιχεία επικοινωνίας

των επιβατών. Ο καθηγητής Jorg Debatin, επικεφαλής του Κόμβου Καινοτομίας στην Υγεία, επισήμανε ότι «δεν έχουμε προχωρήσει επαρκώς με την ψηφιακή ατζέντα στη Γερμανία για να ανταποκριθούμε πλήρως στην κρίση του Covid-19, ενώ πολλές καινοτομίες που θα μπορούσαν να συμβάλλουν έχουν προγραμματιστεί αλλά δεν έχουν ακόμη υλοποιηθεί» [3].

4.4 Πρόβλεψη εξέλιξης ασθενειών

Στη μελέτη των Kumar et al. έγινε η υλοποίηση μιας εφαρμογής υγειονομικής περίθαλψης που βασίζεται στο cloud και στο IoT που μπορεί να παρακολουθεί, να προβλέπει και να διαγνώσει σοβαρές ασθένειες. Παρουσίασαν μια πρόταση για την πρόβλεψη ατόμων με σοβαρά προβλήματα διαβήτη χρησιμοποιώντας ιατρικούς αισθητήρες και έναν αλγόριθμο ταξινόμησης που ονομάζεται νευρωνικός ταξινομητής ασαφούς κανόνα (Fuzzy Rule). Επιπλέον, πρότειναν τη χρήση του IoT, των φορητών ιατρικών συσκευών και του νευρωνικού δικτύου Boltzmann για τη συσσώρευση χαρακτηριστικών από προηγούμενες αναλύσεις και την πρόβλεψη καρδιακών παθήσεων. Στην έρευνά τους, αξιοποίησαν ένα φορητό ρολόι ως συσκευή IoT για τη συλλογή δεδομένων όπως ο καρδιακός ρυθμός και η σωματική δραστηριότητα. Οι συγγραφείς ανέλυσαν ένα σύνολο δεδομένων του Πανεπιστημίου της Καλιφόρνιας Irvine (UCI) που περιέχει πληροφορίες ασθενών (όπως ηλεκτροκαρδιογράφημα, αρτηριακή πίεση, τυπολογία θωρακικού πόνου, επίπεδα χοληστερόλης, αγγειακές πληροφορίες, ελάχιστο και μέγιστο καρδιακό ρυθμό) και συλλέγονται μέσω φορητών συσκευών IoT. Επίσης, χρησιμοποιήθηκε το σύστημα προσομοίωσης MATLAB για την αξιολόγηση της αποτελεσματικότητας του συστήματος. Η προτεινόμενη προσέγγιση επιτυγχάνει ακρίβεια 99,03% και ελάχιστη χρονική πολυπλοκότητα 8,5 δευτερόλεπτα [6].

Μια άλλη εργασία που προτάθηκε από τους Arulanthu et al. εισήγαγε ένα διαδικτυακό σύστημα υποστήριξης ιατρικών αποφάσεων για την πρόβλεψη της χρόνιας νεφρικής νόσου, μέσω συσκευών IoT συνδεδεμένες με το άτομο. Για να εξετάσουν την απόδοση του συστήματος, χρησιμοποίησαν ένα σύνολο δεδομένων αναφοράς για χρόνια νεφρική νόσο από το αποθετήριο UCI. Το μοντέλο που παρουσιάζουν προσφέρει ταξινόμηση με ακρίβεια πρόβλεψης 97,75% και τελικός στόχος είναι η ενίσχυση της απόδοσης του μοντέλου με χρήση τεχνικών επιλογής και ομαδοποίησης χαρακτηριστικών [6].

4.5 Απομακρυσμένος έλεγχος ασθενών

Η δημοτικότητα της απομακρυσμένης παρακολούθησης ασθενών αυξάνεται ραγδαία, ενώ το 2016 διαχειρίζονταν με αυτό το τρόπο την υγεία τους περίπου 7,1 εκατομμύρια ασθενείς και σήμερα φθάνουν τα 50,2 εκατομμύρια με την προσαρμοστικότητα του συστήματος blockchain στο τομέα της υγείας να αναμένεται υψηλή λόγω και του φόβου έξαρσης ανάλογων επιδημιών στο μέλλον. Η τεχνολογία blockchain έχει τη δυνατότητα να αυξήσει την ασφάλεια στα συστήματα απομακρυσμένης παρακολούθησης ασθενών και να αυτοματοποιήσει την παράδοση ειδοποιήσεων που σχετίζονται με την

υγεία των ασθενών με τρόπο συμβατό με τον νόμο περί Φορητότητας και Λογοδοσίας της Ασφάλισης Υγείας (HIPAA). Μπορεί να διορθώσει τα τρέχοντα προβλήματα ελλιπούς διαχείρισης δεδομένων των χρηστών, προσθέτοντας μορφοποιημένα και καθαρά δεδομένα στους ιατρικούς φακέλους (EHR) και τις λιμνάζουσες πληροφορίες υγειονομικής περίθαλψης, επιτρέποντας τη χρήση μεγάλου όγκου δεδομένων με αξιοπιστία και οδηγώντας σε σημαντικότερα αποτελέσματα [25].

Το Remote Patient Monitoring (RPM) αποτελεί ένα μοντέλο blockchain χαμηλών τεχνικών απαιτήσεων και υψηλής ασφάλειας προσωπικών δεδομένων, με επίκεντρο τις συσκευές IoT για απομακρυσμένο έλεγχο ασθενών. Για την ασφάλεια χρησιμοποιείται το πρωτόκολλο Ethereum, τα έξυπνα συμβόλαια και η κρυπτογράφηση δημόσιου και ιδιωτικού κλειδιού. Ο ασθενής είναι εξοπλισμένος με φορητές IoT συσκευές παρέχοντας τις απαραίτητες πληροφορίες στους υγειονομικούς φορείς μέσα από το τοπικό ιδιωτικό του blockchain σύστημα που διαχειρίζεται από τον εκάστοτε ιδιοκτήτη του έξυπνου σπιτιού. Ο ασθενής είναι υπεύθυνος για την χορήγηση ή όχι άδειας πρόσβασης στους παρόχους υγειονομικής περίθαλψης. Έτσι, όταν χρειάζεται θεραπεία κοινοποιεί τα δεδομένα του, ενώ όταν αυτή ολοκληρωθεί μπορεί να αποσύρει την πρόσβαση μέσω του δικτύου σε τρίτους [5].

4.5.1 Φορητές συσκευές

Οι φορητές συσκευές μπορούν να υποστηρίξουν τους επαγγελματίες υγείας και τους ασθενείς, να διαχειριστούν τα διάφορα ζητήματα υγειονομικής περίθαλψης με χαμηλότερο κόστος. Αποτελούν μη επεμβατικές λύσεις που μπορούν να υλοποιηθούν μέσω της ενσωμάτωσης διάφορων αισθητήρων σε διάφορα αξεσουάρ όπως ρολόι, βραχιόλι, κ.ά, με δυνατότητα σύνδεσης και παρακολούθησης σε πραγματικό χρόνο μέσω εφαρμογής του έξυπνου τηλεφώνου.

Στη κατεύθυνση αυτή, οι Castillejo et al. πρότειναν μια μέθοδο αναγνώρισης βιομετρικών στοιχείων μέσω μιας εφαρμογής ηλεκτρονικής υγείας για έξυπνα κινητά, με την ενσωμάτωση φορητών συσκευών σε ένα ασύρματο δίκτυο αισθητήρων απομακρυσμένης παρακολούθησης ασθενών. Σε μια αντίστοιχη μελέτη, οι Jie Wan et al. ανέπτυξαν μια συσκευή παρακολούθησης με τη βοήθεια αισθητήρων (συμπεριλαμβανομένων των καρδιακών παλμών, της θερμοκρασίας του σώματος, του ποσοστού οξυγόνου στο αίμα και της αρτηριακής πίεσης) για την απομακρυσμένη παρακολούθηση υγείας ασθενών. Εφαρμογές όπως οι παραπάνω θα αποδειχθούν ιδιαίτερα κρίσιμες σε υγειονομικές κρίσεις όπως η πανδημία Covid-19, όπου η διαθεσιμότητα των κλινών νοσηλείας είναι περιορισμένη και η έγκαιρη διακομιδή του ασθενή κατά την έξαρση της νόσου ιδιαίτερα κρίσιμη. Η συνδεσιμότητα αυτών των συσκευών με μια εφαρμογή κινητού ενισχύει την υπολογιστική της ισχύ, δίνοντας τη δυνατότητα για εύκολη επεξεργασία και οπτικοποίηση των πληροφοριών που συγκεντρώθηκαν [5].

Οι Otoom et al. πρότειναν ένα σύστημα ανίχνευσης και παρακολούθησης του COVID-19 που συλλέγει δεδομένα συμπτωμάτων σε πραγματικό χρόνο από τεχνολογίες φορητών αισθητήρων και από εφαρμογές

κινητών συσκευών. Ένα σύνολο δεδομένων 14251 επιβεβαιωμένων κρουσμάτων COVID-19 από το αποθετήριο Open Research Dataset του COVID-19 επεξεργάστηκε από αλγόριθμους μηχανικής μάθησης για τον εντοπισμό πιθανών κρουσμάτων κορωνοϊού. Μια άλλη μελέτη που δημοσιεύθηκε από τους Kumar et al. πρότεινε μια αρχιτεκτονική IoT για την ελαχιστοποίηση της εξάπλωσης του COVID-19, η οποία θα εκμεταλλευόταν τους υπάρχοντες αισθητήρες, όπως το υπέρυθρο θερμόμετρο, το έξυπνο ρολόι, τις οπτικές κάμερες και τις κάμερες IP. Οι Baskaran et al. παρουσίασαν ένα σύστημα βασισμένο στο IoT για την αποτροπή του COVID-19 στο εργασιακό περιβάλλον. Πρότειναν να χρησιμοποιηθεί η αναγνώριση προσώπου για να επιβεβαιωθεί η παρουσία ατόμων αντί του χειροκίνητου βιομετρικού συστήματος, τη χρήση ανέπαφων υπέρυθρων αισθητήρων για τον έλεγχο της θερμοκρασίας σώματος των ατόμων και την αποστολή ειδοποιήσεων στις αρχές υγειονομικής επιτήρησης όταν η θερμοκρασία υπερβαίνει τις επιτρεπτές τιμές.

Πρόσφατα, ερευνητές πρότειναν ένα σύστημα βασισμένο στο IoT και την τεχνητή νοημοσύνη για την έγκαιρη εξ αποστάσεως ανίχνευση της νόσου COVID-19. Το σύστημά τους αποσκοπεί στη μείωση της άμεσης επαφής με ασθενείς με COVID-19, αξιοποιώντας διάφορους έξυπνους ιατρικούς αισθητήρες, όπως αισθητήρες σφυγμού, θερμοκρασίας και αίματος, που μπορούν να λειτουργούν αυτόματα χωρίς ανθρώπινη αλληλεπίδραση και το σύστημα να λειτουργεί και να εκπαιδεύεται σύμφωνα με τα δεδομένα που συγκεντρώνονται. Έτσι, το πρώτο βήμα σε αυτόν τον αλγόριθμο είναι ο έλεγχος της θερμοκρασίας του ασθενούς με τη χρήση του θερμικού αισθητήρα. Στη συνέχεια, εάν υπάρχει πυρετός, οι αισθητήρες παλμών μετρούν τον καρδιακό ρυθμό και εάν αυτός ξεπερνά τους 100 παλμούς, ο αισθητήρας αίματος μετρά τα αιμοσφαίρια (λευκά και ερυθρά) και τα αιμοπετάλια. Στο τέλος, εάν ο ασθενής βγει θετικός από αυτόν τον αλγόριθμο, θα πρέπει να απομονωθεί για περαιτέρω εργαστηριακές εξετάσεις [6].

Έλεγχος θερμοκρασίας: Η θερμοκρασία του ανθρώπινου σώματος είναι ένας παράγοντας διατήρησης της ομοιόστασης αλλά και πολλών άλλων διαγνωστικών διαδικασιών. Επιπροσθέτως, μια αλλαγή της θερμοκρασίας αποτελεί προειδοποιητικό σημάδι για κάποια ασθένεια, ίωση κτλ. Η μέτρησή της γίνεται μέσω φορητής συσκευής IoT (3D εκτύπωσης) που προσαρμόζεται στο αυτί και εντοπίζει την θερμοκρασία του σώματος από τη μεμβράνη του τυμπάνου με τη βοήθεια αισθητήρα υπερύθρων. Τα δεδομένα αποθηκεύονται στη βάση δεδομένων και εμφανίζονται σε διαδικτυακή εφαρμογή, ενώ το σύστημα ελέγχου έχει αναπτυχθεί σε Arduino και Raspberry Pi.

Έλεγχος πίεσης του αίματος: Με τη βοήθεια του IoT η μέτρηση της πίεσης, τόσο της συστολικής όσο και της διαστολικής, μπορεί να γίνει μέσω ενός φορητού gadget χωρίς πρόσδεση στο μανίκι, ενώ τα αποτελέσματα πραγματικού χρόνου μπορούν να αποθηκευτούν στο cloud για μακρά περίοδο. Σε παρόμοια μελέτη, η μέτρηση γίνεται μέσω του δακτύλου χρησιμοποιώντας μια μονάδα μικροελεγκτή και τα δεδομένα να αποθηκεύονται και πάλι στο cloud.

Έλεγχος κορεσμού οξυγόνου: Η παλμική οξυμετρία αποτελεί ζωτική παράμετρο της υγειονομικής ανάλυσης. Η πρόοδος προήλθε από την ενσωμάτωση της τεχνολογίας IoT και με τη χρήση των τεχνολογιών επικοινωνίας Zigbee και WiFi για την μετάδοση των πληροφοριών. Επιπλέον, υπάρχει σύστημα συναγερμού που μπορεί να ειδοποιεί τους ασθενείς όταν ο κορεσμός οξυγόνου φτάσει σε κρίσιμο επίπεδο, στοιχείο ιδιαίτερα χρήσιμο για τη διαχείριση ασθενών που νοσούν από Covid-19 [5].

4.5.2 Έξυπνες συσκευές

Έξυπνα θερμόμετρα: Πριν από 8 χρόνια, μια Αμερικάνικη εταιρεία τεχνολογίας που ονομάζεται Kinsa Health κυκλοφόρησε θερμόμετρα εντοπισμού ατόμων με υψηλό πυρετό με δυνατότητα σύνδεσης στο διαδίκτυο. Αν και τα θερμόμετρα αυτά αναπτύχθηκαν αρχικά για την παρακολούθηση ιών υψηλής συχνότητας εμφάνισης, αποδεικνύονται εξαιρετικά χρήσιμα για την ανίχνευση εστιών του Covid-19. Η Kinsa Health έχει αναπτύξει περισσότερα από ένα εκατομμύριο έξυπνα θερμόμετρα σε κτίρια διαφόρων πόλεων στις ΗΠΑ, θερμόμετρα που διέθεταν τη δυνατότητα σύνδεσης με μια εφαρμογή κινητών τηλεφώνων για την άμεση μετάδοση των μετρήσεων τους στην εταιρεία. Στη συνέχεια τα δεδομένα εξομοιώνονται από την Kinsa σε καθημερινή βάση για τη ανάπτυξη χαρτών που φανερώνουν σε ποιες από τις περιοχές των ΗΠΑ παρατηρούνται υψηλές θερμοκρασίες, επιτρέποντας έτσι στις αρχές των ΗΠΑ να εντοπίσουν πιθανά hotspot. Τα τελευταία χρόνια, οι διαδραστικοί χάρτες της Kinsa έχουν αποδείξει την εξαιρετική ακρίβεια και εγκυρότητα πρόβλεψης της εξάπλωσης της γρίπης στις ΗΠΑ, ξεπερνώντας ακόμη και τον επίσημο κρατικό φορέα όσον αφορά την ταχύτητα της πρόβλεψης [11].

SPHCC IoT wearable: Το Δημόσιο Κέντρο Κλινικής Υγείας της Σαγκάης (SPHCC) έχει χρησιμοποιήσει τη χρήση πυλών Bluetooth IoT που αναπτύχθηκαν από την Cassi Network μέσω φορητών αισθητήρων που υλοποιήθηκαν από τη VivaLNK, με στόχο την παρακολούθηση ασθενών με COVID-19 ελαχιστοποιώντας τις ανθρώπινες επαφές. Η Κίνα έχει καταφέρει να μειώσει τον αριθμό των κρουσμάτων COVID-19 χάρη στην εφαρμογή τέτοιων τεχνολογιών. Στον μηχανισμό αυτό, οι φορητοί αισθητήρες της VivaLNK παρέχουν συνεχώς δεδομένα σε πραγματικό χρόνο σχετικά με τις αλλαγές στη θερμοκρασία του σώματος του ασθενούς. Στη συνέχεια, οι πύλες της Cassia συγκεντρώνουν αυτά τα δεδομένα και τα μεταδίδουν ασύρματα στο σταθμό υγειονομικής επιτήρησης, όπου οι εργαζόμενοι παρακολουθούν την υγεία των ασθενών τους χωρίς να χρειάζεται να τους επισκέπτονται προσωπικά. Οι πύλες Cassia IoT επιτρέπουν τη σύζευξη σχεδόν 40 συσκευών Bluetooth Low Energy (BLE) ταυτόχρονα, διευκολύνοντας τη συνδεσιμότητα μεταξύ πολλών δωματίων του SPHCC. Η αξιοποίηση αυτών των τεχνολογιών στο SPHCC έχει μειώσει σημαντικά τον κίνδυνο έκθεσης των εργαζομένων στον τομέα της υγειονομικής περίθαλψης στον ιό, εξασφαλίζοντας παράλληλα μειωμένο φόρτο εργασίας [11].

Κουμπιά IoT: Για να διατηρήσουν υψηλά πρότυπα καθαριότητας και να περιορίσουν τον αριθμό των νοσοκομειακών λοιμώξεων (HAIs), αρκετά νοσοκομεία στο Βανκούβερ έχουν εγκαταστήσει κουμπιά IoT

που λειτουργούν με μπαταρίες. Αυτά τα κουμπιά, με το όνομα Wanda QuickTouch, σχεδιάστηκαν για γρήγορη ανάπτυξη σε οποιαδήποτε εγκατάσταση, ανεξάρτητα από το μέγεθός της, προκειμένου να στέλνουν άμεσες ειδοποιήσεις στη διοίκηση, προειδοποιώντας για οποιοδήποτε θέμα υγιεινής ή συντήρησης που μπορεί να θέσει σε κίνδυνο τη δημόσια ασφάλεια. Ένα χαρακτηριστικό αυτών των κουμπιών είναι η ανεξαρτησία τους από την εξωτερική επιφάνεια, καθώς έχουν την ικανότητα να προσκολλώνται σε οποιαδήποτε επιφάνεια [11].

IoT ασθενοφόρα: Το ιατρικό προσωπικό επειγόντων περιστατικών που σχετίζεται με ασθενοφόρα συνήθως αντιμετωπίζει καταστάσεις πολύ υψηλής πίεσης και ενδεχόμενου σφάλματος. Κατά τη διάρκεια της τρέχουσας πανδημίας του Covid-19, οι καταστάσεις έχουν γίνει ακόμη πιο έντονες και πιεστικές για το ιατρικό προσωπικό που διαχειρίζονται ασθενείς με Covid-19. Τα IoT ασθενοφόρα προσφέρουν μια αποτελεσματική λύση κατά την οποία το ιατρικό προσωπικό προτείνει απομακρυσμένα τις απαραίτητες ενέργειες στο προσωπικό που βρίσκεται στο ασθενοφόρο με τον ασθενή. Αυτό οδηγεί στην έγκαιρη απόκριση και την αποτελεσματική διαχείριση του ασθενούς. Τα οχήματα WAS αποτελούν μια έξυπνη λύση για τα ασθενοφόρα πρώτων βοηθειών. Ο εξοπλισμός αναγνώρισης ραδιοσυχνοτήτων (RFID) συνδέεται στο ασύρματο τοπικό δίκτυο (WLAN) έτσι ώστε να αποκτήσει απομακρυσμένη πρόσβαση στις πληροφορίες του ασθενούς το κατάλληλο ιατρικό προσωπικό [16].

4.5.3 Drone (UAVs - Unmanned Aerial Vehicle)

Σε περιόδους έκτακτης ανάγκης για τη δημόσια υγεία, όπως η πανδημία Covid-19, τα UAV (μη επανδρωμένα εναέρια οχήματα) δηλαδή τα drones, μπορούν να προσφέρουν αρκετά συγκριτικά πλεονεκτήματα, όπως η ελαχιστοποίηση των ανθρώπινων επαφών, η βελτίωση της προσβασιμότητας σε δυσπρόσιτες περιοχές κ.ά. Η Κίνα, που ήταν η πρώτη χώρα που ήρθε αντιμέτωπη με την επιδημία του Covid-19, έκανε εκτεταμένη χρήση της τεχνολογίας των μη επανδρωμένων αεροσκαφών για την καταπολέμηση του Covid-19. Στη συνέχεια, ερευνητές από σε όλο τον κόσμο ένωσαν τις δυνάμεις τους μέσω καινοτόμων προσπαθειών έτσι ώστε να βρουν έξυπνους τρόπους χρήσης drones για την καταπολέμηση του Covid-19.

Επιτήρηση πλήθους

Η Κίνα και η Ινδία ήταν οι πρωταρχικές χώρες που υιοθέτησαν την επιτήρηση πλήθους με χρήση της τεχνολογίας drone. Η MicroMultiCopter, ένας από τους κορυφαίους κατασκευαστές βιομηχανικών drone με έδρα το Shenzhen της Κίνας, ανέπτυξε πάνω από 100 drones σε αρκετές περιοχές της Κίνας στη κατεύθυνση αποτελεσματικής επιτήρησης περιοχών. Τα μη επανδρωμένα αεροσκάφη, διέθεταν ηχητικό εξοπλισμό, για την επικοινωνία οδηγιών και συμβουλών σε άτομα που δεν συμμορφώνονταν με τους κανονισμούς της κινεζικής κυβέρνησης.

Στην Ινδία, μια εταιρεία τεχνολογικών λύσεων με την ονομασία Cyient προμήθευσε την αστυνομία της Telangana με τεχνολογία μη επανδρωμένης εναέριας επιτήρησης με στόχο την υποστήριξη διαχείρισης του lockdown στη υγειονομική κρίση του Covid-19. Επιπλέον, τα drones ήταν εξοπλισμένα με κάμερες επιτήρησης και μπορούσαν να παρακολουθούν αποτελεσματικά επικίνδυνες υγειονομικά περιοχές, ενημερώνοντας άμεσα τις αστυνομικές αρχές για λήψη των σχετικών μέτρων και την πρόληψη ανεπιθύμητων καταστάσεων [11].

Μετάδοση δημόσιων ανακοινώσεων

Τα drones αποδείχθηκαν χρήσιμα για τη μετάδοση κρίσιμων πληροφοριών, ιδιαίτερα σε περιοχές που δεν διέθεταν άλλους τρόπους επικοινωνίας. Οι αστυνομικές αρχές στη Μαδρίτη της Ισπανίας χρησιμοποίησαν ένα drone με μεγαφωνική εγκατάσταση προς ενημέρωση του κοινού, σύμφωνα με τις υγειονομικές κατευθύνσεις που τέθηκαν σε ισχύ αναφορικά με τη διαχείριση καταστάσεων έκτακτης ανάγκης. Επιπροσθέτως, άλλες χώρες της Ευρώπης χρησιμοποιούν τακτικά μη επανδρωμένα αεροσκάφη για να προβούν σε δημόσιες ανακοινώσεις, στην προσπάθειά τους να επικοινωνήσουν τους κανόνες κοινωνικών αποστάσεων και να λάβουν όλα τα απαραίτητα μέτρα προφύλαξης αναφορικά με τον περιορισμό εξάπλωσης της νόσου.

Παρακολούθηση μάζας

Αρκετές δημόσιες αρχές στην Κίνα έχουν χρησιμοποιήσει μη επανδρωμένα αεροσκάφη με εξοπλισμό υπέρυθρων καμερών, για τη διενέργεια μετρήσεων θερμοκρασίας μεγάλης κλίμακας σε κατοικημένες περιοχές. Οι αρχές στο Νέο Δελχί της Ινδίας, έθεσαν σε εφαρμογή ένα drone πολλαπλών χρήσεων για τον περιορισμό εξάπλωσης του Covid-19. Το drone είχε την ονομασία "corona combat", διέθετε μια θερμική κάμερα, μια κάμερα νυχτερινής όρασης, ένα φορητό κουτί ιατροφαρμακευτικού υλικού, ένα μεγάφωνο ανακοινώσεων και μια δεξαμενή αποθήκευσης απολυμαντικού υγρού 10 λίτρων. Σε αντίθεση με τα θερμόμετρα υπέρυθρων μετρήσεων που μπορούσαν να λάβουν τη θερμοκρασία ενός μόνο ατόμου τη φορά, αυτού του τύπου τα drones είχαν την ικανότητα μέτρησης θερμοκρασιών πολλών ανθρώπων ταυτόχρονα.

Επίσης, ερευνητές από το Πανεπιστήμιο της Νότιας Αυστραλίας, σε συνεργασία με τον κατασκευαστή εμπορικών UAVs από τον Καναδά, DraganFly, ανέπτυξαν ένα «pandemic drone» για την εξ αποστάσεως παρακολούθηση και αναγνώριση ατόμων με μολυσματικές αναπνευστικές ασθένειες. Τα μη επανδρωμένα αεροσκάφη ενσωμάτωσαν έναν εξειδικευμένο αισθητήρα και ένα σύστημα παρακολούθησης μέσω υπολογιστή για την παρακολούθηση της θερμοκρασίας και των καρδιακών παλμών των ανθρώπων, έχοντας την δυνατότητα να εντοπίζουν ακόμη και άτομα που φτερνίζονται ή βήχουν σε δημόσιους χώρους. Η επιτυχία εφαρμογής τους θα φέρει επανάσταση στη διάγνωση του Covid-19 μέσω της έγκαιρης ανίχνευσης πιθανών ασθενών του ιού [11].

Απολυμαντικός ψεκασμός

Τα μη επανδρωμένα αεροσκάφη μπορούν να χρησιμοποιηθούν για την είσοδο σε μολυσμένες τοποθεσίες και την απολύμανση του χώρου μέσω ψεκασμού, περιορίζοντας στο ελάχιστο τον κίνδυνο περαιτέρω εξάπλωσης του ιού και μειώνοντας παράλληλα την έκθεση των υγειονομικών υπαλλήλων της πρώτης γραμμής στον ιό. Η Ισπανία είναι η πρώτη ευρωπαϊκή χώρα που επιστράτευσε μη επανδρωμένα αεροσκάφη για τη διαχείριση της πανδημίας. Ο στρατός της Ισπανίας υιοθέτησε τη χρήση γεωργικών drones που κατασκευάζονται από την κινέζικη εταιρεία DJI, για να απολυμάνουν δημόσιους χώρους μέσω ψεκασμού, έχουν χωρητικότητα 16 λίτρων και μπορούν να ολοκληρώσουν το ένα δέκατο του χιλιομέτρου σε μια ώρα.

Παράδοση ιατρικών προμηθειών και ειδών πρώτης ανάγκης

Τα drones μπορούν να χρησιμοποιηθούν για την ταχύτατη μεταφορά φαρμάκων από ένα ιατρικό φορέα σε ένα άλλο, αλλά και από κάποιο ιατρικό κέντρο σε ασθενείς που αντιμετωπίζουν τον ιό σε ήπια μορφή στο σπίτι τους. Πράγμα που συνέβη κατά τη διαδικασία μεταφοράς προμηθειών ιατροφαρμακευτικής περίθαλψης από το κέντρο ελέγχου ασθενειών στο τοπικό νοσοκομείο της περιοχής Xinchang, δίχως να εκτεθεί η ανθρώπινη ζωή στον κίνδυνο μόλυνσης.

Η Marut Drones, μια startup που αποτελείται από μια ομάδα επιστημόνων του Ινδικού Ινστιτούτου Τεχνολογίας (IIT), ανέπτυξε μια ολόκληρη σειρά drones για την αντιμετώπιση της πανδημίας COVID-19 στην Ινδία. Η εταιρεία διαθέτει μη επανδρωμένα αεροσκάφη για απολύμανση, διανομή φαρμάκων, θερμική ανάλυση, παρακολούθηση κυκλοφορίας και επιτήρηση πλήθους. Τα drones της εταιρείας είναι εξοπλισμένα με προηγμένη τεχνολογία πλοήγησης και αποφυγής εμποδίων, έχοντας τη δυνατότητα κάλυψης αποστάσεων 12 χιλιομέτρων σε μόλις 8 λεπτά, καταφέρνοντας χρόνους παράδοσης 80 φορές μικρότερους από τις συμβατικές μεθόδους. Σύμφωνα με τις εκτιμήσεις της ίδιας της εταιρείας, τα μη επανδρωμένα αεροσκάφη απολύμανσης έχουν ήδη προχωρήσει σε απολύμανση εκτάσεων πάνω από 1900 χιλιόμετρα.

Εκτός του ότι αποτελούν έναν ασφαλή τρόπο για την διανομή ιατρικών προμηθειών, τα μη επανδρωμένα αεροσκάφη μπορούν να βοηθήσουν στην παράδοση ειδών πρώτης ανάγκης, όπως έχει πραγματοποιηθεί σε ορισμένες περιοχές της Αυστραλίας, της Κίνας και των ΗΠΑ. Ο κινέζικος γίγαντας ηλεκτρονικού εμπορίου JD.com πλέον χρησιμοποιεί αρκετά drones για την πραγματοποίηση παραδόσεων βασικών αγαθών κατά το τελικό στάδιο αποστολής (last-mile delivery).

4.6 Έξυπνες εφαρμογές

Στην προσπάθεια αντιμετώπισης του Covid-19, πολλές εταιρείες δημιούργησαν εφαρμογές με χρήση της τεχνολογίας blockchain, λύνοντας το κρίσιμο πρόβλημα της έλλειψης ενοποίησης πιστοποιημένων πηγών δεδομένων. Η τεχνολογία blockchain ενσωματώθηκε σε διάφορες λύσεις για να διασφαλιστεί η ασφάλεια ανταλλαγής ιατρικών δεδομένων που συνδέονται με τον Covid-19. Σύμφωνα με ειδικούς, ένα από τα κύρια πλεονεκτήματα της χρήσης εφαρμογών blockchain είναι η ικανότητα του να επικυρώνει διαρκώς μεταβαλλόμενα δεδομένα. Δύο εφαρμογές blockchain ακολουθούν παρακάτω.

4.6.1 Civitas

Μια νεοσύστατη επιχείρηση από τον Καναδά, που ειδικεύεται σε τεχνολογίκές λύσεις blockchain ανέπτυξε ένα σύστημα ασφαλείας, υπό της μορφής εφαρμογής, με το όνομα Civitas, με κατεύθυνση την υποστήριξη των τοπικών αρχών ανά τον κόσμο στον έλεγχο επιπτώσεων από τον Covid-19. Αυτή η εφαρμογή συσχετίζει τις επίσημες ταυτότητες των ατόμων με αρχεία blockchain, με σκοπό την επαλήθευση ή όχι εγκεκριμένης άδειας απομάκρυνσης του ατόμου από το σπίτι. Αυτή η εφαρμογή προσδιορίζει ακόμη και την κατάλληλη ώρα και ημέρα εξόδου για τα άτομα που εμφανίζουν συμπτώματα Covid-19 για την αγορά βασικών ειδών, ελαχιστοποιώντας τον κίνδυνο επιπολασμού της ασθένειας σε τρίτους. Επιπλέον, το Civitas διαθέτει μια ενσωματωμένη λειτουργία τηλεϊατρικής, που επιτρέπει την παρακολούθηση και αξιολόγηση των συμπτωμάτων των ασθενών, την αποστολή συμβουλών σχετικά με τη φαρμακευτική αγωγή και τις προτεινόμενες στρατηγικές υγειονομικής περίθαλψης από το εξειδικευμένο υγειονομικό προσωπικό. Η εταιρεία ισχυρίζεται ότι η εφαρμογή διασφαλίζει με ακεραιότητα και την ιδιωτικότητα των προσωπικών δεδομένων των χρηστών [11].

Το Civitas είναι μια εφαρμογή επίλυσης της ιχνηλασιμότητας για τον COVID-19, που αναπτύχθηκε από την startup Emerge με στόχο τη δημιουργία ενός ψηφιακού διαβατηρίου COVID-19 και την βελτιωμένη παρακολούθηση της μετάδοσης του COVID-19 στην κοινότητα. Βασίζεται στην τεχνολογία Blockchain για τη δημιουργία ενός επαληθεύσιμου ψηφιακού αρχείου που περιλαμβάνει τα αποτελέσματα των δοκιμών ελέγχου και των σημείων μετάδοσης COVID-19 [6].

Οι Torky και Hassanien παρουσίασαν ένα πλαίσιο βασισμένο σε Blockchain για την εξακρίβωση και τον εντοπισμό άγνωστων μολυσμένων κρουσμάτων COVID-19, καθώς και την πρόβλεψη του κινδύνου μετάδοσης σε τρίτους. Το σύστημα αποτελείται από τέσσερα τμήματα:

1. Υποσύστημα Επαλήθευσης Λοιμώξεων (Infection Verifier Subsystem) που αναπαριστά ψηφιακά τα μοτίβα και τις περιπτώσεις μόλυνσης.
2. Σύστημα Blockchain για την αποθήκευση δεδομένων με επιβεβαιωμένες περιπτώσεις COVID-19.
3. Εφαρμογή P2P-Mobile για απεικόνιση πληροφοριών και εντοπισμό των μολυσμένων περιπτώσεων με βάση την επικοινωνία P2P (Peer to Peer).
4. Σύστημα Μαζικής Επιτήρησης (Mass-Surveillance System) για τη χαρτογράφηση των επαφών μεταξύ πολιτών, με στόχο την παρακολούθηση και τον εντοπισμό ατόμων και τοποθεσιών με τα οποία ήρθε σε επαφή κάποιο επιβεβαιωμένο κρούσμα COVID-19.

Πρόσφατα, οι Xu et al. παρουσίασε ένα πλαίσιο διατήρησης απορρήτου που βασίζεται στο Blockchain για τον εντοπισμό επαφών της πανδημίας COVID-19, που ονομάζεται BeepTrace και βασίζεται σε δύο αλληλοεπιδρώντα συστήματα blockchains. Το πρώτο διατηρεί τη γεωγραφική θέση και χρησιμοποιείται για τον εντοπισμό προσωπικών δεδομένων τοποθεσίας, ενώ το δεύτερο διατηρεί ειδοποιήσεις και χρησιμοποιείται για την αποθήκευση συμπιεσμένων αποτελεσμάτων (ένα ζεύγος ψευδώνυμου και γεωγραφικών δεδομένων). Τα δεδομένα κρυπτογραφούνται και μόνο εξουσιοδοτημένοι χρήστες/εξυπηρετητές μπορούν να έχουν πρόσβαση σε αυτά [6], [36].

4.6.2 MiPasa

Το MiPasa είναι μια ανοιχτή πλατφόρμα ροής και ανάλυσης δεδομένων, δημιουργήθηκε πάνω στο Hyperledger Fabric και βασίζεται στις υπηρεσίες blockchain και το cloud της IBM, για την διευκόλυνση ανταλλαγής πιστοποιημένων πληροφοριών υγείας μεταξύ ατόμων, κρατικών αρχών και νοσοκομείων. Η εφαρμογή αυτή λειτουργεί μέσω συλλογής πληροφοριών που παρέχονται από διάφορους οργανισμούς υγειονομικής περίθαλψης, αξιωματούχους δημόσιας υγείας και άλλα άτομα. Ο ΠΟΥ πρόσφατα αναγνώρισε αυτήν την εφαρμογή ως μια αποτελεσματική πλατφόρμα για να βοηθήσει τους επιστήμονες να αποκτήσουν πρόσβαση σε πιστοποιημένες πληροφορίες. Οι πληροφορίες που είναι διαθέσιμες σε αυτή την πλατφόρμα υποστηρίζουν τη λήψη αποφάσεων αναφορικά με τη μελλοντική στρατηγική δράσης και την αποτελεσματική διάθεση των πόρων των νοσοκομείων στην αντιμετώπιση των επιπτώσεων της πανδημίας του Covid-19 [11].

Το MiPasa έχει σχεδιαστεί για να καθιστά δυνατή τη σύνθεση πηγών δεδομένων, την διευθέτηση των ασυνεπειών τους, τη υποβοήθηση στον εντοπισμό σφαλμάτων ή λανθασμένων αναφορών και την απρόσκοπτη ενσωμάτωση αξιόπιστων νέων πληροφοριών. Υποστηρίζεται από μια διεπιστημονική ομάδα επαγγελματιών υγείας, προγραμματιστών λογισμικού και εφαρμογών, καθώς και ειδικών σε θέματα

προστασίας της ιδιωτικότητας, οι οποίοι συνεργάζονται για να διευκολύνουν τη συλλογή αξιόπιστων και ποιοτικών δεδομένων και να τα καταστήσουν προσβάσιμα στους κατάλληλους φορείς. Η ένταξη γίνεται μέσω του δικτύου Unbounded Network, το οποίο τρέχει μια έκδοση παραγωγής του Hyperledger Fabric σε πολλαπλά νέφη. Η IBM είναι μεταξύ των πρώτων υποστηρικτών του Unbounded Network, το οποίο βοηθά περισσότερους συμμετέχοντες να συνεργάζονται ανοιχτά, μέσω blockchains με και χωρίς άδεια, ενώ βρίσκεται σε παραγωγή από το 2018 [43].

Κάθε ειδικευμένος οργανισμός είναι σε θέση να ενσωματώσει εύκολα νέες δικές του πηγές δεδομένων από άλλες πλατφόρμες με την απλή χρήση APIs, διευκολύνοντας σημαντικά τη συλλογή, την ταξινόμηση και τη μελέτη πληροφοριών σχετικά με την εξάπλωση και τον περιορισμό της πανδημίας. Το MiPasa μπορεί να βοηθήσει στην παρακολούθηση και πρόβλεψη τοπικών και παγκόσμιων επιδημιολογικών τάσεων και να ανιχνεύσει πιθανούς ασυμπτωματικούς φορείς του ιού, αξιοποιώντας δεδομένα μεγάλου εύρους σχετικά με τις διαδρομές και τα περιστατικά μόλυνσης σε ένα ισχυρό σύστημα επεξεργασίας με τεχνητή νοημοσύνη κατανεμημένο σε όλο τον κόσμο [44].

Μελέτη Περίπτωσης MiPasa

Το εμβόλιο κατά του Covid-19 αντιμετωπίστηκε με δυσπιστία από τους πολίτες. Στις Ηνωμένες Πολιτείες, έπειτα από έρευνα που έγινε σε 7000 ενήλικες, έδειξε ότι ο δισταγμός αυτός απέναντι στο εμβόλιο μειώθηκε στις αρχές του 2021, φανερώνοντας ότι η αποδοχή του εμβολίου εξαρτάται από το βάρος που βίωσαν οι διάφορες ομάδες ανθρώπων λόγω σοβαρής ασθένειας και θανάτου από Covid-19. Στο παράρτημα Α παρουσιάζεται ο κώδικας που χρησιμοποιήθηκε στην εφαρμογή του MiPasa.

Η μελέτη περίπτωσης αφορά τη διστακτικότητα απέναντι στο εμβόλιο του Covid-19 και δύο είναι οι δείκτες που εντοπίζονται σε αυτήν. Ο **Δείκτης Κοινωνικής Ευπάθειας (SVI)** περιγράφει συνοπτικά τον βαθμό στον οποίο μια κοινότητα είναι ευάλωτη στις καταστροφές. Οι συντελεστές που λαμβάνονται υπόψη κατά την ανάπτυξη του SVI περιλαμβάνουν οικονομικά δεδομένα, καθώς και δεδομένα σχετικά με την εκπαίδευση, τα οικογενειακά χαρακτηριστικά, τη στέγαση, τη γλωσσική ικανότητα, την εθνικότητα και την πρόσβαση σε οχήματα. Οι τιμές του SVI κυμαίνονται από 0 (λιγότερο ευάλωτος) έως 1 (πιο ευάλωτος), ενώ μπορούν να εντοπιστούν οι εξής κατηγορίες: πολύ χαμηλός (0,0-0,19), χαμηλός (0,20-0,39), μέτριος (0,40-0,59), υψηλός (0,60-0,79), πολύ υψηλός (0,80-1,0).

Η πιο πρόσφατη ενημέρωση δεδομένων από την Household Pulse Survey – η οποία συλλέγει στατιστικά στοιχεία για τον τρόπο με τον οποίο επηρεάστηκαν οι ζωές των ανθρώπων από την πανδημία του Covid-19 – δείχνει ότι η διστακτικότητα σε εθνικό επίπεδο συνεχίζει να μειώνεται, από 21.6% μεταξύ 6 έως 18 Ιανουαρίου σε 10.8% μεταξύ 23 Ιουνίου έως 5 Ιουλίου. Τα ποσοστά όμως παραμένουν υψηλά σε ορισμένες πολιτείες, με τους πιο διστακτικούς πληθυσμούς να βρίσκονται στο Wyoming (25,6%), τη West Virginia (22,4%), τη North Dakota (22,2%) και την Αλάσκα (20,5%). Το γεγονός ότι η

διστακτικότητα παραμένει σε μέρη της χώρας σε υψηλά επίπεδα αντικατοπτρίζεται στον αριθμό των κρουσμάτων που εντοπίζονται.

Ο έτερος δείκτης είναι ο **Δείκτης Κάλυψης Εμβολίων (CVAC)** που καταγράφει τις προκλήσεις που σχετίζονται με τη προσφορά και τη ζήτηση, παρεμποδίζοντας την ταχεία, άμεση και εκτεταμένη κάλυψη εμβολίων κατά του Covid-19 στις πολιτείες των Η.Π.Α. μέσα από πέντε συγκεκριμένους παράγοντες, το ιστορικό εμβολιασμών, τα κοινωνικοδημογραφικά εμπόδια, τους πόρους του υγειονομικού συστήματος περίθαλψης, τη προσβασιμότητα στην υγειονομική περίθαλψη και την παράτυπη συμπεριφορά αναζήτησης φροντίδας. Το CVAC μετρά το επίπεδο ανησυχίας σε μια προβληματική κατάσταση για ένα εύρος από 0 (χαμηλότερη ανησυχία) έως 1 (υψηλότερη ανησυχία), ενώ αναλυτικότερα παρατηρούνται οι παρακάτω κατηγορίες: πολύ χαμηλή (0,0-0,19), χαμηλή (0,20-0,39), μέτρια (0,40-0,59), υψηλή (0,60-0,79), πολύ υψηλή (0,80-1,0) ανησυχία [42].

Δημογραφική ανάλυση: Αν και η πανδημία δεν έχει αφήσει κανένα ανεπηρέαστο, το βάρος της νόσου COVID-19 έπεσε δυσανάλογα στα μέλη φυλετικών μειονοτήτων. Οι έγχρωμοι, οι ισπανόφωνοι και οι Λατίνοι έχουν σχεδόν 3 φορές μεγαλύτερες πιθανότητες να νοσηλευτούν λόγω COVID-19 και περίπου 2 φορές μεγαλύτερες πιθανότητες να απεβιώσουν σε σύγκριση με λευκούς μη ισπανόφωνους πολίτες. Με 3 εγκεκριμένα εμβόλια SARS-CoV-2 διαθέσιμα για χρήση έκτακτης ανάγκης στις ΗΠΑ, είναι σημαντικό να αυξηθεί η πρόσβαση στα εμβόλια για τον COVID-19 και να αντιμετωπιστεί ο δισταγμός κατά του εμβολίου COVID-19 σε κοινότητες όπου είναι ακόμη υψηλός.

Η διαδικασία κατανομής εμβολίων στις ΗΠΑ έδωσε προτεραιότητα στους εργαζόμενους του τομέα υγειονομικής περίθαλψης (HCW) και στους πολίτες εγκαταστάσεων μακροχρόνιας περίθαλψης. Καθώς ο εμβολιασμός κατά του COVID-19 επεκτείνεται, είναι σημαντικό να συνεχιστεί η διαδικασία αξιολόγησης όσον αφορά την δεκτικότητα εμβολιασμού και να διασφαλιστεί η δίκαιη κατανομή των εμβολίων. Οι εργαζόμενοι στον τομέα υγείας αντιμετωπίζουν επαγγελματική και κοινωνική έκθεση στον ιό, ενώ η θέση τους είναι κομβική στην απόκριση της δημόσιας υγείας στην πανδημία. Αν και ο κίνδυνος λοίμωξης μέσω της εργασίας είναι χαμηλός έχοντας λάβει τα σωστά μέτρα ατομικής προστασίας, μελέτες έχουν δείξει ότι οι έγχρωμοι, οι ισπανόφωνοι και οι λατίνοι του κλάδου υγείας έχουν υψηλότερο περιθώριο μόλυνσης, που σχετίζεται με αυξημένη έκθεση της κοινότητας στον ιό. Σε μια μεγάλη μελέτη, φανερώθηκε η συσχέτιση του αριθμού των λοιμώξεων στον κλάδο των υγειονομικών με την διαβίωση σε περιοχές με αυξημένο επιπολασμό του ιού. Οι πιθανότητες μόλυνσης από τον COVID-19 αυξήθηκαν 2 φορές μεταξύ των έγχρωμων υγειονομικών, αλλά και αυτών με πολυφυλετικό υπόβαθρο σε σύγκριση με τους λευκούς. Η διαφοροποίηση του κινδύνου νόσησης από Covid-19 στην κοινότητα των υγειονομικών σε φυλετικές/εθνικές μειονότητες πιθανότατα προέρχεται από ιστορικές και συστημικές πρακτικές που έχουν μειονεκτήσει τις έγχρωμες κοινότητες και οδήγησαν σε οικιστικό διαχωρισμό, ο οποίος σχετίζεται με

αυξημένη έκθεση στον ιό. Συνεπώς, η απορρόφηση των εμβολίων COVID-19 είναι ιδιαίτερα σημαντική για τους εργαζόμενους στον τομέα της υγειονομικής περίθαλψης που ζουν σε κοινότητες με αυξημένη επιβάρυνση από τη νόσο.

Συμπέρασμα: Με τη μελέτη αυτή διαπιστώθηκε ότι περίπου οι μισοί εργαζόμενοι στον τομέα της υγειονομικής περίθαλψης ήταν διστακτικοί απέναντι στον εμβολιασμό κατά του COVID-19, με τα υψηλότερα ποσοστά να εντοπίζονται στις κοινότητες των έγχρωμων και των ισπανόφωνων ή λατινοαμερικάνικων κοινοτήτων. Τα αποτελέσματα της έρευνας έδειξαν ότι απαιτείται περισσότερη δουλειά για να διασφαλιστεί η εμπιστοσύνη στον εμβολιασμό κατά του COVID-19, ιδιαίτερα μεταξύ των έγχρωμων και ισπανόφωνων ή Λατίνων κοινοτήτων. Η επικοινωνία μηνυμάτων που δίνουν έμφαση στα ατομικά, οικογενειακά και κοινωνικά οφέλη από τη λήψη του εμβολίου, καθώς και η παροχή διαρκούς διαφάνειας αναφορικά με την αξιοπιστία των εμβολίων COVID-19 είναι απλές προσεγγίσεις που μπορούν να διαδοθούν γρήγορα στα συστήματα υγειονομικής περίθαλψης με στόχο τη προώθηση αποδοχής των εμβολίων μεταξύ των υγειονομικών [42].

4.7 Διαχείριση εφοδιαστικής αλυσίδας εμβολίων

Από τους πρώτους μήνες που ιός Covid-19 εισήλθε στη ζωή μας και την επιβολή περιοριστικών μέτρων παγκοσμίως, οι πολιτικοί και οι πολίτες εναπόθεσαν τις ελπίδες τους στην ανακάλυψη του εμβολίου, για την επαναφορά στην κανονικότητα του τρόπου ζωής τους. Στο άκουσμα της θετικής είδησης πολλοί είχαν προβληματιστεί με τις χαμηλές θερμοκρασίες που έπρεπε να συντηρηθεί το εμβόλιο της Pfizer από -60 έως -80 βαθμούς κελσίου, τον εξοπλισμό που θα απαιτούνταν καθώς και την εξασφάλιση των σταθερών συνθηκών μεταφοράς στις διάφορες χώρες ανά τον κόσμο. Επίσης, ο κλάδος υγειονομικής περίθαλψης έχει ολοένα και αυξανόμενο αριθμό πλαστών φαρμάκων, με το ποσοστό αυτών να φθάνει το 10% στις πιο ανεπτυγμένες χώρες.

Έτσι, προτάθηκε ένα πλαίσιο blockchain και IoT που θα καταγράφει και θα χρονολογεί τη μεταφορά φαρμακευτικών σκευασμάτων και εμβολίων σε κάθε σημείο της εφοδιαστικής αλυσίδας. Καθώς τα εμβόλια ταξιδεύουν, κάθε συναλλαγή έχει μια χρονική σήμανση και τον τρέχοντα υπεύθυνο μεταφοράς. Επομένως, το εφοδιαστικό κέντρο, οι γιατροί και οι ασθενείς έχουν πλήρη πρόσβαση στο ιστορικό του προϊόντος που έλαβαν, καθώς και τα επίπεδα θερμοκρασίας κατά τη μεταφορά που διασφαλίζουν την ενεργή δραστικότητα του σκευάσματος.

Το παραπάνω πλαίσιο blockchain – IoT περιλαμβάνει τα ακόλουθα συστατικά:

- Σαρωτή QR κωδικού: Για να διαβαστούν οι πληροφορίες των πακέτων και να αποθηκευτούν στο blockchain είναι απαραίτητο να υπάρχει σαρωτής κωδικών QR ή smartphone με εφαρμογή σάρωσης κωδικών QR.

- Δημιουργία στοιχείου: Μόλις ένα προϊόν εισέλθει για πρώτη φορά στην αλυσίδα εφοδιασμού, δημιουργείται ένα νέο στοιχείο, με όλες οι πληροφορίες του προϊόντος να αποθηκεύονται στον κωδικό QR.
- Αισθητήρας: Απαιτείται για την ένταξη προϊόντων ψυχρής αποθήκευσης που είναι απαραίτητη η παρακολούθηση της θερμοκρασίας τους. Χρησιμοποιούνται κυρίως κατά το στάδιο διαμετακόμισης του προϊόντος και πιο συγκεκριμένα κατά την παραλαβή του προϊόντος από την επόμενη οντότητα της αλυσίδας εφοδιασμού, όπου ο κωδικός QR του αισθητήρα σαρώνεται και ελέγχεται η τήρηση του πρωτοκόλλου θερμοκρασίας, για να ακολουθήσει στη συνέχεια η αποδοχή ή άρνηση του προϊόντος από τον παραλήπτη.
- Μεταφορά στοιχείου: Εάν το προϊόν μεταβιβαστεί από έναν προμηθευτή σε έναν άλλο ή από μία οντότητα σε μία άλλη στην αλυσίδα εφοδιασμού, κάθε αλλαγή και προσθήκη πληροφοριών αποθηκεύεται στην αλυσίδα των block.
- Προβολή προϊόντος μέσω σάρωσης QR κώδικα: Όλοι οι συμμετέχοντες μπορούν να δουν τις λεπτομέρειες του προϊόντος στην εφοδιαστική αλυσίδα μέσω εγγραφής στην εφαρμογή έξυπνων κινητών. Με την σάρωση του κωδικού QR ή των αισθητήρων που συνδέονται με τις συσκευασίες εμβολίων, ο χρήστης λαμβάνει όλες τις πληροφορίες σχετικά με τη διαδρομή και τις συνθήκες μεταφοράς.

Το σύστημα μεταφοράς και αποθήκευσης εμβολίων σε ορισμένες θερμοκρασίες από το στάδιο παρασκευής έως τον τελικό καταναλωτή ονομάζεται Cold Chain. Κατά τη διαδικασία μεταφοράς των εμβολίων απαιτείται ένα έξυπνο κουτί μεταφοράς, το οποίο διατηρεί τη θερμοκρασία και καταγράφει όλες τις αλλαγές σε ένα αισθητήρα, ενώ μέσω της τεχνολογίας Blockchain και των έξυπνων συμβολαίων εξασφαλίζεται η αξιοπιστία και η διαθεσιμότητα των δεδομένων σε όλα τα μέλη του συστήματος.

Ο κωδικός QR αποθηκεύει όλες τις απαραίτητες πληροφορίες σχετικά με τον αισθητήρα, το εύρος θερμοκρασίας, το όριο θερμοκρασίας, τις πληροφορίες ιδιοκτήτη κ.ά., ενώ διατηρεί και δύο κενά κελιά πληροφοριών για την ένδειξη χαμηλής και υψηλής θερμοκρασίας. Κατά τη διάρκεια της μεταφοράς, εάν η θερμοκρασία μεταβληθεί πέραν ενός συγκεκριμένου ορίου για κάποιο πακέτο, η θερμοκρασία αυτή αποθηκεύεται στα κενά κελιά του κώδικα QR. Ο αισθητήρας εμφανίζει επίσης μια κόκκινη λυχνία αν η θερμοκρασία έχει υπερβεί το όριο σε οποιαδήποτε στιγμή και αναβοσβήνει με πράσινο χρώμα αν η θερμοκρασία έχει διατηρηθεί εντός των ορίων. Μόλις ολοκληρωθεί η παράδοση, τα δεδομένα αισθητήρων μπορούν να μεταφερθούν στο σύννεφο μέσω προγράμματος ανάγνωσης κωδικών QR και ο κατακερματισμός του κώδικα QR αποθηκεύεται σε μια αλυσίδα μπλοκ.

Σήμερα, πολλές φορητές συσκευές smartphone χρησιμοποιούνται ως σαρωτές και αναγνώστες κωδικών QR. Για την ασφάλεια αυτών των αισθητήρων απαιτείται ένα σύστημα ψηφιακής υπογραφής που θα

επιβεβαιώνει ότι τα δεδομένα δεν έχουν τροποποιηθεί από κάποιον τρίτο. Επίσης, στα δίκτυα αισθητήρων οποιαδήποτε μορφής συγχώνευση δεδομένων αισθητήρα απαιτεί χρονικό συγχρονισμό όλων των αισθητήρων και για το λόγο αυτό αναπτύχθηκε ο διάσημος αλγόριθμος Berkeley από τους Gusella και Zatti στο Πανεπιστήμιο της Καλιφόρνια.

Οι συσκευές IoT παράγουν μεγάλο όγκο δεδομένων και το blockchain δεν μπορεί να τον διαχειριστεί λόγω του χαμηλού ρυθμού εκτέλεσης των συναλλαγών. Παρόλο που υπάρχουν αρκετοί αλγόριθμοι συναίνεσης διαθέσιμοι για το blockchain που υποστηρίζουν υψηλές επιδόσεις, δεν μπορούν να εφαρμοστούν εξαιτίας του ότι αυτοί προϋποθέτουν ταυτόχρονα και εξαιρετικά υψηλές επιδόσεις δικτύου. Στο προτεινόμενο μοντέλο, χρησιμοποιήθηκαν οι αλγόριθμοι συναίνεσης Raft υψηλών επιδόσεων, αν και θεωρούνται περισσότερο κατάλληλοι για μικρό αριθμό συμμετεχόντων στο δίκτυο. Λόγω της χαμηλής επεκτασιμότητας του δικτύου, μια αύξηση του αριθμού των κόμβων στο δίκτυο θα μειώσει την αποδοτικότητα και την απόδοση του αλγορίθμου Raft. Ο αλγόριθμος Raft αναμένει πολύ γρήγορη μετάδοση δεδομένων για να επιδείξει υψηλή απόδοση, το οποίο επιτυγχάνεται μέσω του Blockchain Distributed Network (BDN) με διακομιστή bloXroute. Οι διακομιστές bloXroute διαδίδουν μόνο κρυπτογραφημένα μπλοκ (block) πολύ γρήγορα στο δίκτυο, γεγονός που εμποδίζει τη διακοπή διάδοσης του εκάστοτε block με βάση το περιεχόμενό του και αποτρέπει τη διάκρισή του από τους διακομιστές. Οι διακομιστές (servers) του BDN χρησιμοποιούν προηγμένες τεχνικές δικτύου, που επιτρέπουν την άμεση μετάδοση δεδομένων στο υπόλοιπο δίκτυο όταν το blockchain λαμβάνει ένα νέο πακέτο, πολλαπλασιάζοντας την ταχύτητά του έως και 100 φορές, αποτρέποντας παράλληλα την εμφάνιση του φαινομένου bottleneck στο δίκτυο.

Ουσιαστικά, το bloXroute δεν είναι ένα blockchain σύστημα από μόνο του, αλλά ένα εξαιρετικά επεκτάσιμο κατανεμημένο δίκτυο. Το ζήτημα που αναδύεται είναι το πώς θα πραγματοποιηθεί η συλλογή κρυπτογραφημένων δεδομένων από συσκευές με περιορισμένους πόρους, καθώς σήμερα πολλές εφαρμογές, όπως δίκτυα αισθητήρων ή RFID, υλοποιούνται σε συσκευές με πολύ περιορισμένες δυνατότητες και απαιτούν χαμηλών προδιαγραφών κρυπτογράφηση. Πολλοί γνωστοί καθιερωμένοι αλγόριθμοι, όπως ο AES, δεν ικανοποιούν τις βασικές απαιτήσεις αυτών των συσκευών, όπως η ελαχιστοποίηση του κόστους εξοπλισμού, της κατανάλωσης ενέργειας και των καθυστερήσεων. Στην κατεύθυνση αυτή, έχουν προταθεί ελαφρά πρωτόκολλα κρυπτογράφησης, με αλγόριθμους που είναι συνήθως μικρότεροι και ταχύτεροι στην υλοποίηση λογισμικού για το Διαδίκτυο των Πραγμάτων (IoT).

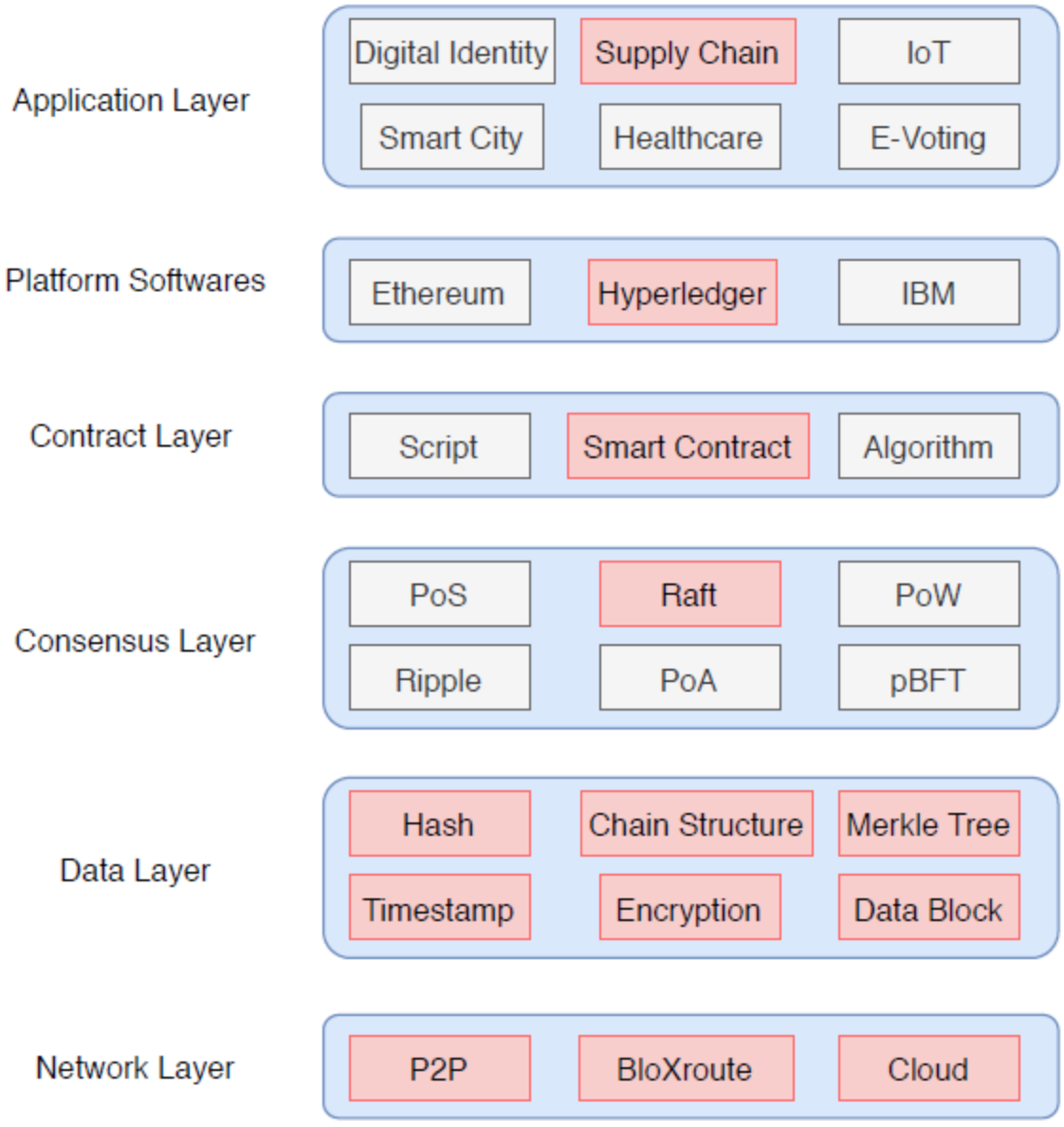
Ένα ακόμη σημαντικό ζήτημα που χρειάζεται να αντιμετωπιστεί είναι η ασφάλεια των συσκευών - αισθητήρων με «ελαφριά» σχήματα ψηφιακών υπογραφών. Ένα δίκτυο blockchain αποτελείται από διάφορους κόμβους IoT περιορισμένων πόρων, με χαμηλή χωρητικότητα αποθήκευσης, περιορισμένη ταχύτητα επεξεργασίας και χαμηλό εύρος ζώνης επικοινωνίας, σημεία που θέτουν περιορισμούς χαμηλής

ενεργειακής κατανάλωσης. Ο κατάλληλος αλγόριθμος κρυπτογράφησης για συσκευές IoT χαμηλών δυνατοτήτων ανήκει στην οικογένεια ARX, η οποία κρυπτογραφεί το απλό κείμενο με σταθερό μέγεθος block (αντί της κλασικής bit-by-bit), όπως για παράδειγμα οι SPECK και LEA, με το πρώτο να αποτελεί τον πιο αποδοτικό αλγόριθμο κρυπτογράφησης. Η οικογένεια ARX διαθέτει τρεις θεμελιώδεις λειτουργίες, την αρθρωτή προσθήκη (modular addition), τη δυαδική περιστροφή (bitwise rotation) και την αποκλειστική OR (exclusive OR). Σε περίπτωση που κάποιος οργανισμός επιθυμεί να διατηρήσει απόρρητες και κρυφές τις πληροφορίες του από άλλους τρίτους γίνεται χρήση του Hyperledger, όπου διαχωρίζεται το εκάστοτε κανάλι από τα υπόλοιπα [30].

Το σύστημα περιλαμβάνει δύο επίπεδα τοπολογικού δικτύου:

- Διακομιστές blockchain με προδιαγραφές χαμηλής καθυστέρησης και υψηλής χωρητικότητας, που στοχεύουν στη βελτιστοποίηση της διάδοσης συναλλαγών και μπλοκ σε πολλαπλά συστήματα υψηλής ταχύτητας. Λειτουργούν σαν διακομιστές πλέγματος που συνδέονται με άλλα πλέγματα (clusters) και μειώνουν την επιβάρυνση και την καθυστέρηση του δικτύου. Επιπλέον, το σύστημα δεν έχει τη λειτουργία κεντρικού διακομιστή που διαχειρίζεται άλλους μικρούς κόμβους, αλλά σκοπός του είναι η αύξηση της ταχύτητας διάδοσης των block.
- Ομότιμα δίκτυα που είναι δίκτυα P2P κόμβων που χρησιμοποιούν διακομιστές blockchain για τη διάδοση συναλλαγών και block, ενώ παράλληλα ελέγχουν τη συμπεριφορά του. Αυτά τα ομότιμα δίκτυα χρησιμοποιούν έναν συγκεκριμένο αλγόριθμο συναίνεσης, ομαδοποιούνται σε μορφή πλεγμάτων και κάθε πλέγμα έχει έναν διακομιστή blockchain που διαδίδει συναλλαγές και block για λογαριασμό άλλων κόμβων που ονομάζονται επίσης ομότιμοι.

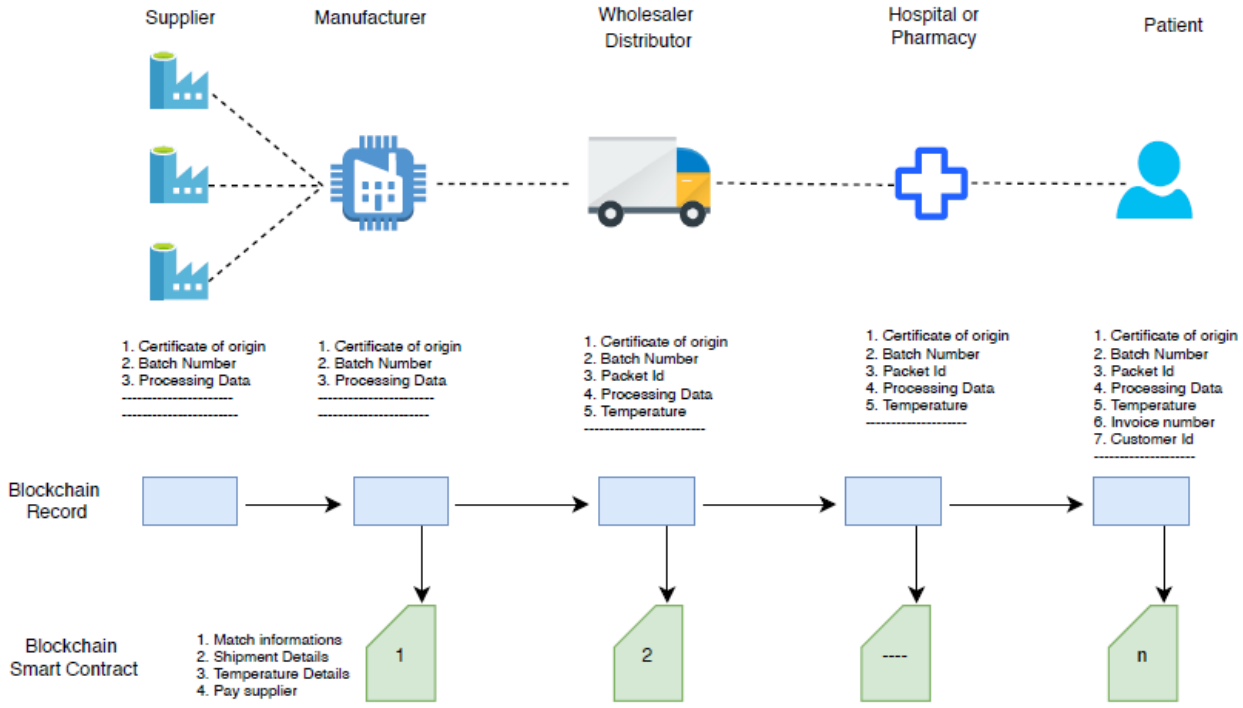
Διαφορετικά ομότιμα μέλη του δικτύου μπορούν να στείλουν κρυπτογραφημένα block σε διακομιστές blockchain δίχως την εμπλοκή κεντρικού διακομιστή. Λόγω αυτής της ρύθμισης, ο διακομιστής blockchain δεν μπορεί να εξαπατήσει κάποιο συγκεκριμένο κόμβο (node) ή πλέγμα (cluster). Ο διακομιστής blockchain εξυπηρετεί τυφλά τους κόμβους στο δίκτυο χωρίς να γνωρίζει το περιεχόμενο του κρυπτογραφημένου block, βελτιώνοντας σημαντικά την ταχύτητα διάδοσης, καθώς αυτά προωθούνται σε άλλα δίκτυα για επαλήθευση χωρίς καθυστέρηση δικτύου. Για τον έλεγχο της συμπεριφοράς οποιουδήποτε διακομιστή blockchain, τα ομότιμα μέλη του δικτύου μπορούν να στείλουν δοκιμαστικά block στον διακομιστή blockchain και να επιβεβαιώσουν εάν οι ομότιμοι τα έλαβαν γρήγορα. Η πλήρης αρχιτεκτονική blockchain παρουσιάζεται στο παρακάτω σχήμα 4.3 [30].



Σχήμα 4.3: Η αρχιτεκτονική του συστήματος Blockchain (Πηγή: [30])

Το προτεινόμενο πλαίσιο περιλαμβάνει ένα σύστημα βασισμένο σε blockchain και IoT που καταγράφει και επισημαίνει χρονικά (timestamps) τη μεταφορά των ιατρικών σκευασμάτων σε κάθε σημείο της εφοδιαστικής αλυσίδας. Καθώς τα φάρμακα και τα εμβόλια ταξιδεύουν μέσω της αλυσίδας εφοδιασμού, κάθε συναλλαγή φέρει μια χρονική σήμανση με τον τρέχοντα ιδιοκτήτη της αλυσίδας εφοδιασμού. Το καθολικό που αποθηκεύεται στο blockchain χρησιμοποιείται για τη διασφάλιση της ασφάλειας του συστήματος και της ποιότητας των φαρμακευτικών προϊόντων. Οι ασθενείς, τα νοσοκομεία, τα φαρμακεία, αλλά και κάθε ενδιαφερόμενος μπορεί να έχει πρόσβαση στο πλήρες ιστορικό των φαρμακευτικών προϊόντων που έλαβε, όπως για το παράδειγμα των εμβολίων, που είναι βιώσιμα σε ένα

συγκεκριμένο εύρος θερμοκρασίας και το φάρμακο παύει να είναι ενεργό σε περίπτωση που υπάρξει διάλειμμα στην ψυχρή αλυσίδα. Η χρήση οχημάτων ψυγείων, κιβωτίων διατήρησης θερμοκρασίας κ.ά, επιτρέπουν τη συνεχή ψυχρή διάχυση και διατήρηση ενός ομοιόμορφου επιπέδου θερμοκρασίας [30].



Εικόνα 4.4: Σύστημα blockchain διαχείρισης εφοδιαστικής αλυσίδας φαρμακευτικών προϊόντων (Πηγή: [30])

Κεφάλαιο 5ο: Συγκριτική μελέτη εφαρμογών κατά του Covid-19

5.1 Συγκριτική ανάλυση μεθόδων ανίχνευσης επαφών

5.1.1 Εισαγωγή στην ψηφιακή ανίχνευση επαφών

Η ψηφιακή ανίχνευση επαφής είναι η μέθοδος αναγνώρισης και προσδιορισμού της επαφής μεταξύ 2 ή περισσότερων χρηστών με τη χρήση ενός τεχνολογικά υποστηριζόμενου συστήματος εντοπισμού. Στο πλαίσιο του COVID-19, η επαφή ορίζεται ως η παρουσία σε απόσταση 6 μέτρων από ένα άτομο για διάστημα άνω των δέκα λεπτών. Ο χειροκίνητος εντοπισμός επαφής είναι χρονοβόρος και απαιτεί πολύωρη εργασία, ο οποίος σε συνδυασμό με την ασθενή απομνημόνευση των κοινωνικών συναντήσεων στο πρόσφατο παρελθόν δημιουργεί πιθανότητα ελλιπή και αναποτελεσματική ανίχνευση επαφών [34].

Αυτοί οι περιορισμοί μπορούν να ξεπεραστούν με τα ψηφιακά συστήματα εντοπισμού επαφών, με τα κύρια πλεονεκτήματα τους να συνοψίζονται στα εξής:

- Δημιουργία ενός αρχείου καταγραφής της τοποθεσίας (απόλυτης ή σχετικής) και του χρόνου παραμονής.
- Η παθητική καταγραφή δεν απαιτεί ανθρώπινη παρέμβαση.
- Η επεκτασιμότητα σε ένα ευρύ κοινό.
- Η πρόβλεψη για εύκολη και γρήγορη ειδοποίηση.

Το βασικό εργαλείο για τον ψηφιακό εντοπισμό επαφών είναι το κινητό τηλέφωνο και με βάση τα χαρακτηριστικά του, η ανίχνευση επαφών μπορεί να σχεδιαστεί με βάση το GPS, το Bluetooth, το WiFi κ.ά., προσφέροντας τα ανάλογα πλεονεκτήματα και περιορισμούς. Όλα τα ψηφιακά συστήματα εντοπισμού επαφών μπορούν να ταξινομηθούν σε συστήματα που συλλέγουν δεδομένα απόλυτης θέσης (GPS, αρχεία καταγραφής Wi-Fi κ.α.) και σχετικής θέσης (Bluetooth), με τη λειτουργικότητα του εκάστοτε συστήματος να διαφοροποιείται ανάλογα με την κατηγορία που εντάσσεται. Συστήματα που συλλέγουν απόλυτα δεδομένα τοποθεσίας μπορούν επίσης να βρουν επαφές που επισκέφτηκαν τον ίδιο τόπο σε διαφορετικό χρόνο, εκτός από τις επαφές που βρέθηκαν στο ίδιο μέρος την ίδια χρονική περίοδο, καθιστώντας τα ιδιαιτέρως χρήσιμα απέναντι σε μολυσματικές ασθένειες έμμεσης εξάπλωσης. Όταν ένας ασθενής επισκέπτεται μια τοποθεσία, εξαπλώνει τους παθογόνους μικροοργανισμούς σε αυτήν, οι οποίοι παραμένουν ενεργοί στην τοποθεσία για ορισμένο χρονικό διάστημα. Ακόμη και αν ο ασθενής εγκαταλείψει την τοποθεσία, ένας άλλος επισκέπτης μπορεί να μολυνθεί εάν έρθει σε επαφή με μολυσμένες επιφάνειες στον ίδιο χώρο. Από την άλλη πλευρά, τα συστήματα που βασίζονται στη σχετική θέση δύο συσκευών, υποστηρίζουν τον εντοπισμό του ατόμου Α από το άτομο Β, χωρίς να προσδιορίζουν την ακριβή του θέση, διασφαλίζοντας την ιδιωτικότητα των πληροφοριών τοποθεσίας [34].

Στη συνέχεια θα προσδιορίζουμε τις βασικές παραμέτρους για τη μέτρηση της αποτελεσματικότητας ενός συστήματος εντοπισμού επαφών.

Ακρίβεια (Accuracy): Μια ψηφιακή λύση εντοπισμού επαφών πρέπει να έχει υψηλή ακρίβεια για τον ορθό εντοπισμό της. Τυπικά, η μέτρηση της ακρίβειας υπολογίζεται μέσω των ψευδώς θετικών και των ψευδώς αρνητικών του συστήματος, όπου τα ψευδώς θετικά προσδιορίζουν τον αριθμό των ατόμων που αναγνωρίστηκαν εσφαλμένα ως άτομα επαφής (δεν ήρθαν ποτέ σε επαφή με έναν ασθενή με θετικό COVID, αλλά αναγνωρίστηκαν ως επαφή), ενώ τα ψευδώς αρνητικά προσδιορίζουν τα άτομα που ήρθαν σε επαφή με ασθενή θετικό στο COVID, αλλά δεν ταυτοποιήθηκαν ως επαφές. Για το πλαίσιο αυτό, τόσο τα ψευδώς θετικά όσο και τα ψευδώς αρνητικά έχουν βαρύνουσα σημασία. Από τη μία πλευρά, εάν ο αριθμός των ψευδώς θετικών είναι υψηλός, το σύστημα θα εντοπίσει πολύ περισσότερους ανθρώπους που έχουν ανάγκη εξετάσεων αποστέλλοντας ψευδείς ειδοποιήσεις, μειώνοντας την εμπιστοσύνη του κοινού προς την εφαρμογή και επιβαρύνοντας τους πόρους υγειονομικής περίθαλψης. Από την άλλη πλευρά, μία υψηλή ψευδώς αρνητική τιμή υποδηλώνει ότι το σύστημα δεν μπορεί να εντοπίσει επαρκώς τους χρήστες που βρίσκονται στο ίδιο σημείο, αυξάνοντας έτσι τον κίνδυνο μόλυνσης για τον γενικό πληθυσμό.

Απόρρητο (Privacy): Κάθε εφαρμογή εντοπισμού επαφών πρέπει να αλληλεπιδρά με τον χρήστη πληροφορίες, όπως δεδομένα υγείας και τοποθεσία, γεγονός που καθιστά την προστασία της ιδιωτικής ζωής μια πολύ σημαντική παράμετρο. Οι ανησυχίες για την προστασία της ιδιωτικής ζωής είναι σχεδόν εξίσου σημαντικές με την ακρίβεια καταγραφής. Τα συστήματα που συλλέγουν ακριβείς πληροφορίες θέσης θα μπορούσαν διαρρεύσουν λεπτομέρειες σχετικά με την κινητικότητα του χρήστη αποκαλύπτοντας λεπτομέρειες σχετικά με το ιστορικό επισκέψεων, την απόλυτη τοποθεσία και συχνότητα επισκέψεων αυτής [34].

Ευρεία υιοθέτηση (Ubiquity): Σύμφωνα με μελέτες, για να είναι αποτελεσματικό ένα σύστημα ανίχνευσης επαφών περίπου το 80% του πληθυσμού των χρηστών πρέπει να ενσωματώσει κάποια εφαρμογή εντοπισμού επαφών. Μια τέτοια μεγάλης κλίμακας υιοθέτηση από τους χρήστες χρειάζεται:

- **Συμβατότητα**: Η τεχνολογία ανίχνευσης θέσης θα πρέπει να είναι συμβατή με τα smartphones που χρησιμοποιούν ξεπερασμένο λογισμικό. Για παράδειγμα, το 25% των χρηστών Android παγκοσμίως δεν είναι σε θέση να χρησιμοποιήσουν εφαρμογές σχεδιασμένες σε εκδόσεις χαμηλότερες από το Android 8.0 που κυκλοφόρησε το 2017. Ως εκ τούτου, τυχόν εφαρμογές που χρησιμοποιούν δυνατότητες διαθέσιμες μόνο σε σύγχρονα λειτουργικά συστήματα κινητών τηλεφώνων δεν θα είναι συμβατές με συσκευές μεγάλου αριθμού χρηστών και ως εκ τούτου θα παρουσιάζεται ελλιπής εκπροσώπηση του πληθυσμού.
- **Επεκτάσιμος σχεδιασμός**: Η εφαρμογή πρέπει να είναι σε θέση να εντοπίζει επαφές και να προσδιορίζει την απόστασή τους όχι μόνο σε χώρους όπου λίγα smartphones ανταλλάσσουν

πληροφορίες μεταξύ τους, αλλά και σε πολυσύχναστα περιβάλλοντα όπως το μετρό, και το σούπερ μάρκετ, που έχουν εκατοντάδες ανθρώπους να κυκλοφορούν. Η σχεδίαση αυτών των εφαρμογών θα πρέπει να μπορεί να υποστηρίξει τη διαχείριση της υψηλής κινητικότητας και τη μέτρηση της ακριβής απόστασης μεταξύ μιας μεγάλης ομάδας ανθρώπων, ελαχιστοποιώντας παράλληλα τη πιθανότητα κατάρρευσης όταν το σύστημα δέχεται έντονες πιέσεις από τους χρήστες της εφαρμογής.

Η επίσημη εφαρμογή της ινδικής κυβέρνησης για την ψηφιακή ανίχνευση επαφών ξεπέρασε τις 100 εκατομμύρια λήψεις. Αντίστοιχου μεγέθους κλίμακας εφαρμογές οφείλουν να ακολουθούν βελτιωμένες πρακτικές μηχανικής. Η πρόκληση αυτή ενισχύεται επειδή όχι μόνο οι χρήστες πρέπει να κατεβάσουν, να εγκαταστήσουν, να συναινέσουν στη συλλογή δεδομένων αλλά και σε ορισμένες περιπτώσεις (π.χ. εφαρμογές που βασίζονται σε Bluetooth) να διατηρήσουν την εφαρμογή ενεργή στο παρασκήνιο. Τέτοιες εφαρμογές μπορεί να καταναλώνουν ενέργεια πολύ γρήγορα με αποτέλεσμα οι χρήστες να απενεργοποιούν τις εφαρμογές και ως εκ τούτου να οδηγούμαστε σε ένα αναποτελεσματικό σύστημα ανίχνευσης επαφών [34].

5.1.2 Σύγκριση μεθόδων ψηφιακής ανίχνευσης επαφών

Bluetooth: Σε μια πυκνοκατοικημένη τοποθεσία, όπως ένα μεγάλο κατάστημα λιανικής πώλησης ή ένα συγκρότημα κατοικιών με στενά συνδεδεμένους μικρούς χώρους διαμερισμάτων, όλοι όσοι βρίσκονται εντός της ακτίνας 100 μέτρων από μια συσκευή Bluetooth μπορεί να χαρακτηριστούν ως επαφές κοντινής απόστασης, παρόλο που μπορεί να μη βρέθηκαν στο ίδιο κατάστημα ή διαμέρισμα και να μην είχαν κάποια φυσική επαφή. Για να μετριαστεί αυτό το πρόβλημα, οι εφαρμογές Bluetooth συνδυάζονται με τη χρήση της ισχύος σήματος για την αναγνώριση συσκευών κοντινής απόστασης. Επίσης, οι συσκευές θα πρέπει να είναι σε θέση να συνδεθούν μέσω Bluetooth και η ισχύς του σήματος να είναι πάνω από ένα όριο, δηλαδή η συσκευή δεν θα βρίσκεται απλώς στην ακουστική εμβέλεια, αλλά και αρκετά κοντά για να παρέχει ισχυρό σήμα, επιτρέποντας την αναγνώρισή της ως επαφή. Το Bluetooth σε συνδυασμό με την ισχύ του σήματος είναι η πιο κοινή προσέγγιση που υπάρχει σήμερα, ωστόσο όπως επεσήμαναν οι ίδιοι οι ιδρυτές του Bluetooth, αυτή η προσέγγιση έχει επίσης ψευδώς θετικά και ψευδώς αρνητικά αποτελέσματα. Η προσέγγιση αυτή προϋποθέτει ότι η ισχύς του σήματος είναι συνάρτηση της απόστασης, επομένως μπορεί να χρησιμοποιηθεί ως αντιπροσωπευτικό μέτρο για την απόσταση. Όμως, η ισχύς του σήματος εξαρτάται και από άλλους παράγοντες όπως το περιβάλλον και τα εμπόδια που παρεμβάλλονται μεταξύ των συσκευών. Αυτό οδηγεί σε μεγάλα σφάλματα στην εκτίμηση της απόστασης, όπως για παράδειγμα μπορεί δύο συσκευές να απέχουν 3 μέτρα μακριά και να φαίνεται ότι η απόσταση είναι 30 μέτρα και το αντίστροφο, στοιχειοθετώντας ανακρίβειες που είναι ευρέως γνωστές μεταξύ των ερευνητών στην κοινότητα του ασύρματου εντοπισμού θέσης μέσω Bluetooth [34].

GPS: Το Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS) παρέχει γεωγραφικές πληροφορίες θέσης και ώρας σε συσκευές εξοπλισμένες με δέκτη GPS μέσω ενός συνόλου δορυφόρων πλοήγησης GPS. Το GPS αποτελεί ένα μέσο για την παρακολούθηση κάθε smartphone και τον εντοπισμό δύο τηλεφώνων ως επαφές όταν παραμένουν πολύ κοντά για πολύ ώρα, καθώς τα περισσότερα smartphones διαθέτουν GPS, ενώ ως λύση μπορεί να λειτουργήσει σε παγκόσμια εμβέλεια και να επεκταθεί με ευκολία. Για παράδειγμα, το CovTracer που χρησιμοποιήθηκε στην Κύπρο, συλλέγει δεδομένα GPS για τον υπολογισμό της απόστασης συσκευών. Ωστόσο, η προσέγγιση εμφανίζει δύο μειονεκτήματα. Πρώτον, εγείρει σοβαρά ερωτήματα σχετικά με την προστασία της ιδιωτικής ζωής, και δεύτερον αποτυγχάνει όσον αφορά την ακρίβεια καταγραφής της τοποθεσίας, ιδίως σε εσωτερικούς χώρους και σε υπαίθριες αστικές σήραγγες. Το GPS σε εσωτερικούς χώρους ακόμη και όταν λειτουργεί επιτυχώς, μπορεί να εμφανίσει σφάλματα εντοπισμού θέσης γύρω στα 10 μέτρα, που θεωρούνται πολύ υψηλά για εφαρμογές εντοπισμού επαφών, καθώς επαφή μπορεί να χαρακτηριστεί όταν η απόσταση μεταξύ των συσκευών είναι μικρότερη των 2 μέτρων. Ένα σφάλμα 30 μέτρων θα αποπροσανατολίσει αυτές τις εκτιμήσεις και θα οδηγήσει σε υψηλό ψευδώς θετικό ή ψευδώς αρνητικό ποσοστό, ανάλογα με τον τρόπο σχεδιασμού του συστήματος. Γενικά, η ακρίβεια του GPS είναι χαμηλή για τον εντοπισμό επαφών με σφάλματα των 20-30 μέτρων, ειδικά σε εσωτερικούς χώρους όπου οι άνθρωποι περνούν ένα μεγάλο μέρος του χρόνου τους, οπότε η χρήση του δεν θα βοηθήσει πολύ ούτως ή άλλως. Επίσης, η κοινή χρήση των πληροφοριών θέσης με μια κεντρική οντότητα απαιτεί προσεχτική διαχείριση, καθώς τεχνική αδυναμία μπορεί να οδηγήσει σε διαρροή και κατάχρηση δεδομένων. Ωστόσο, με τη ρητή συγκατάθεση του χρήστη μπορεί να προσφέρει άλλα οφέλη, όπως βοήθεια στις κυβερνήσεις να απεικονίσουν τις τοποθεσίες των ατόμων υψηλού κινδύνου και να κατανέμουν τους πόρους υγειονομικής περίθαλψης, αποτρέποντας έτσι το ξέσπασμα της επιδημίας [34].

Wi-Fi: Οι άνθρωποι περνούν περίπου το 80% του χρόνου τους σε εσωτερικούς χώρους, σε σπίτια και επιχειρήσεις, όπου τα δίκτυα Wi-Fi παρέχουν μια εναλλακτική προσέγγιση. Τα δίκτυα Wi-Fi αποτελούνται από πολλά σημεία πρόσβασης δικτύου (AP), μέσω των οποίων οι συσκευές των χρηστών μπορούν να συνδεθούν, αποσυνδεθούν και μετακινηθούν ανά πάσα στιγμή. Όλα αυτά τα συμβάντα συνδέσεων, αποσυνδέσεων, εξουσιοδοτήσεων και μετακινήσεων μεταξύ των AP καταγράφονται εσωτερικά από το κάθε σημείο πρόσβασης (AP) σε ένα αρχείο καταγραφής συστήματος που ονομάζεται «syslog». Αναλύοντας τα συμβάντα που καταγράφονται στο αρχείο αυτό για κάθε συσκευή μπορούμε να προσδιορίσουμε την κινητικότητά της και μαζί και του χρήστη καθώς η συσκευή βρίσκεται συνεχώς πάνω του. Έτσι, σε ένα δίκτυο Wi-Fi, μπορούμε να αντλήσουμε την κινητικότητα όλων των χρηστών που είναι συνδεδεμένοι στο δίκτυο χρησιμοποιώντας τα αρχεία καταγραφής Wi-Fi.

Τα κύρια πλεονεκτήματα της εν λόγω ανίχνευσης επαφών με βάση το Wi-Fi είναι:

- Η πρόβλεψη για ανίχνευση επαφών σε εσωτερικούς χώρους.
- Η αποφυγή εγκατάστασης νέων αισθητήρων ή νέων συσκευών, καθώς λειτουργεί με τα υπάρχοντα δίκτυα Wi-Fi και τα αρχεία καταγραφής τους για την ασφάλεια του δικτύου και την ανάλυση της κυκλοφορίας.
- Η παροχή λεπτομερειών σχετικά με την ώρα επίσκεψης και τη διάρκειά της.
- Δεν απαιτείται εγκατάσταση κάποιας εφαρμογής σε κινητά τηλέφωνα για τη χρήση Wi-Fi [34].

Ακουστική εμβέλεια (Acoustic-ranging): Ο πρωταρχικός σκοπός των τηλεφώνων είναι να εκπέμπουν, να καταγράφουν και να μεταφέρουν ήχο, καθιστώντας την εκτίμηση εμβέλειας με βάση τον ήχο μια ακόμη ανταγωνιστική προσέγγιση. Ο εντοπισμός επαφών με βάση τον ήχο βασίζεται στην ιδέα ότι κάθε συσκευή εκπέμπει έναν τυχαίο αλλά μοναδικό ήχο που μπορεί να χρησιμοποιηθεί για τον υπολογισμό της απόστασης. Η ακουστική συχνότητα και το πλάτος επιλέγονται έτσι ώστε να βρίσκονται εκτός του εύρους της ανθρώπινης ακοής. Σε αντίθεση με το Bluetooth, το GPS και το WiFi, ο ήχος είναι ένα μηχανικό κύμα που ταξιδεύει πολύ πιο αργά από τα ραδιοκύματα (106 φορές πιο αργός), προσδίδοντας στην ακουστική αναγνώριση την εκτίμηση του χρόνου μετάδοσης. Συγκεκριμένα, δεδομένου ότι οήχος ταξιδεύει ως κύμα, δύο συσκευές μπορούν με ακρίβεια να μετρήσουν το χρόνο που χρειάζεται ένας ήχος για να πάει από τη μία συσκευή σε μια άλλη. Έτσι, για τον υπολογισμό της απόστασης, πρέπει να πολλαπλασιάσουμε το χρόνο που χρειάζεται για να ταξιδέψει μεταξύ των συσκευών με την ταχύτητα του ήχου. Για παράδειγμα, αν ένας ήχος χρειαζόταν σήμα 4 χιλιοστά του δευτερολέπτου για να πάει από το σημείο 1 στο σημείο 2, σημαίνει ότι αυτά βρίσκονται σε απόσταση περίπου 4,5 μέτρων. Επίσης, ένα σφάλμα ενός χιλιοστού του δευτερολέπτου ή δύο στη μέτρηση του χρόνου μετάδοσης δεν θα έκανε τα σφάλματα να είναι μεγάλα. Παρόλο που τα συστήματα με βάση την ακουστική εμβέλεια έχουν τα πλεονεκτήματα της υψηλής ακρίβειας και της ευρείας υιοθέτησης, υπάρχουν 3 βασικές παγίδες στην ηχητική μέτρηση:

- Κλίμακα: Ο αριθμός των συσκευών που μπορούν να εντοπίσουν ταυτόχρονα επαφές με βάση τον ήχο είναι μικρός, με την επικοινωνία μεταξύ 2 μόνο συσκευών να χαρακτηρίζεται ως αποδοτική, αλλά να αποκτά σημαντικό θόρυβο καθώς αυξάνεται ο αριθμός των συσκευών που εντάσσονται στη δραστηριότητα. Έτσι, σε πολυσύχναστους χώρους το σύστημα καθίσταται αναξιόπιστο, λόγω του ότι οι παρεμβολές περιβάλλοντος προσθέτουν περαιτέρω θόρυβο.
- Απόρρητο: Η εφαρμογή ενός συστήματος με βάση τον ακουστικό εντοπισμό μέσω smartphones είναι μια λύση ευρείας αποδοχής, αλλά προϋποθέτει ότι τα μικρόφωνα των συσκευών πρέπει να είναι ενεργοποιημένα σε όλη τη χρονική διάρκεια. Η δειγματοληψία θέσης σε υψηλή συχνότητα συνεπάγεται την αύξηση του κινδύνου αποκάλυψης απορρήτου και της ιδιωτικότητας, τον οποίο οι περισσότεροι χρήστες δεν είναι πρόθυμοι να αποδεχτούν.

- Ακουστική δυσφορία: Τα σήματα ακουστικής εμβέλειας είναι αθόρυβα στο ανθρώπινο αυτί, καθώς δεν εμπίπτουν στο εύρος συχνοτήτων της ανθρώπινης ακοής. Παρόλα αυτά, μεγάλο μέρος του ζωικού βασιλείου μπορεί να προσλάβει αυτές τις συχνότητες, προκαλώντας τους σχετική δυσφορία, γεγονός που σημαίνει ότι πρέπει να εφαρμοστούν αυστηρότερες δοκιμές για να διασφαλιστεί η γενικότερη ασφάλεια.

Πολλοί σχεδιαστές εφαρμογών σήμερα εξερευνούν τη χρήση διαφορετικών τρόπων, όπως ο συνδυασμός ήχου και Bluetooth, έτσι ώστε η μία τεχνολογία να μπορεί να βοηθήσει στην εξάλειψη των αδυναμιών της άλλης. Τέτοιες προσεγγίσεις έχουν μεγάλη απήχηση και χρησιμοποιούνται σε πολλές από τις εφαρμογές που κυκλοφορούν, ωστόσο, βρίσκονται ακόμη σε προκαταρκτικά στάδια έρευνας και δεν έχουν δοκιμαστεί ενδελεχώς [34].

Technology	Proximity Accuracy	Privacy	Ubiquity	Scalability
Bluetooth	Low accuracy(errors 10-20 feet).	Privacy preserving solution	Yes	Yes
GPS	Low accuracy (errors 30 feet)	Privacy concerns for absolute location	Yes	Yes
Acoustic	High accuracy	Privacy concerns for microphone access	Yes	No
WiFi Logs	Low Accuracy (errors 10-15 meters)	Privacy preserving solution	Yes	Yes
Advanced	High accuracy (0-5 feet)	Privacy concerns exist	No	No

Πίνακας 5.1: Σύγκριση τεχνολογιών με βάση τις παραμέτρους (ακρίβεια, ιδιωτικότητα, ευρεία υιοθέτηση και επεκτασιμότητα) (Πηγή: [34])

5.2 Συγκριτική ανάλυση εφαρμογών κατά του Covid-19

Στο σημείο αυτό θα παρουσιάσουμε μια μελέτη 12 δωρεάν εφαρμογών που χρησιμοποιήθηκαν στη Σαουδική Αραβία, την Ιταλία, την Σιγκαπούρη, το Ηνωμένο Βασίλειο, τις Ηνωμένες Πολιτείες της Αμερικής και την Ινδία και αφορούσαν την πανδημία του Covid-19. Οι 12 εφαρμογές για κινητές συσκευές ήταν: Mawid, Tabaud, Tawakkalna, Sehha, Aarogya setu, TraceTogether, COVID safe, Immuni, COVID symptom study, COVID watch, NHS COVID-19 και PathCheck.

Αναλύθηκαν οι ακόλουθες δυνατότητες και λειτουργίες:

- επισκόπηση εφαρμογών και γενικές πληροφορίες (τιμή, αξιολογήσεις, android, iOS, προγραμματιστής/κάτοχος, χώρα, κατάσταση),
- εργαλεία υγείας (αξιολόγηση κατάστασης-κινδύνου χρήστη, αυτοαξιολόγηση, ενσωμάτωση e-pass, έκδοση αναφορών αποτελεσμάτων τεστ, διαδικτυακή συμβουλευτική, ιχνηλάτηση επαφών),
- εργαλεία εκμάθησης και ενημέρωσης (εξατομικευμένες σημειώσεις, εκπαιδευτικοί πόροι, πληροφορίες για τον COVID-19),
- εργαλεία επικοινωνίας (επίλυση ερωτημάτων, ραντεβού, κοινωνικά δίκτυα, ειδοποιήσεις),
- σχεδιασμός εφαρμογής (οπτικοποίηση δεδομένων, σχεδιασμός προγράμματος),
- εργαλεία δικτύωσης (χαρτογράφηση τοποθεσίας – GPS, συνδεσιμότητα με άλλες συσκευές) και
- επιλογές ασφάλειας και απορρήτου προσωπικών δεδομένων (ειδοποιήσεις, προστασία δεδομένων), με στόχο την διερεύνηση της αποτελεσματικότητας της εκάστοτε εφαρμογής [1].

Feature Type	Features	Mawid	Tabaud	Tawakkalna	Sehha	Aarogya Setu	TraceTogether
App Overview	Price	Free	Free	Free	Free	Free	Free
	Rating: Android (No. of Ratings)/iOS (No. of Ratings)	4.5 (80,440)/ 4.5 (8200)	4.3 (7074)/ 4.5 (323)	4.6 (51,611)/ 4.0 (2200)	4.1 (5425)/ 4.3 (492)	4.4 (1.4 million)/ 4.5 (3100)	3.7 (11,065)/2.7 (33)
	Android	Yes	Yes	Yes	Yes	Yes	Yes
	iOS	Yes	Yes	Yes	Yes	Yes	Yes
	Developer/Owner	Ministry of Health	Ministry of Health	Ministry of Health	Ministry of Health	National Informatics Centre	Government Technology Agency
	Country	Saudi Arabia	Saudi Arabia	Saudi Arabia	Saudi Arabia	India	Singapore
	Status	In use	In use	In use	In use	In use	In use
Health Tools	User Status (Risk Assessment)	Yes	Yes	Yes	No	Yes	Yes
	Self-Assessment	Yes	No	No	No	Yes	No
	E-Pass Integration	No	No	Yes	No	Yes	No
	Test Results Reporting	Yes	Yes	No	No	Yes	Yes
	Online Consultation	Yes	No	No	Yes	Yes	No
	Contact Tracing	No	Yes	Yes	No	Yes	Yes
Learning	Personalized Notes	Yes	No	No	Yes	Yes	No
	Educational Resources	No	No	No	Yes	Yes	No
	COVID-19 Information	Yes	No	Yes	No	Yes	Yes
Communication	Query Resolution	Yes	No	No	Yes	Yes	No
	Appointments	Yes	No	No	Yes	No	No
	Social Network	No	No	No	No	No	No
	Notifications	Yes	Yes	Yes	Yes	Yes	Yes
App Design	Data Visualisation	Yes	Yes	Yes	Yes	Yes	Yes
	Program Plan	No	Yes	No	Yes	Yes	No
Networking	Location Mapping (GPS)	Yes	No	Yes	No	Yes	Yes
	Connectivity with Other Devices	No	Yes	No	No	Yes	Yes
Safety & Security	Alerts	Yes	Yes	Yes	Yes	Yes	Yes
	Data Protection	Low Risk	Low Risk	Medium Risk	High Risk	Medium Risk	Low Risk

Πίνακας 5.2.i: Χαρακτηριστικά και λειτουργίες των 6 εφαρμογών (Apps) κατά του Covid-19 (Πηγή: [1])

Feature Type	Features	COVID Safe	Immuni	COVID Symptom Study	NHS COVID-19	COVID Watch	PathCheck SafePlaces
App Overview	Price	Free	Free	Free	Free	Free	Free
	Rating: Android (No. of Ratings)/iOS (No. of Ratings)	2.8 (13,696)/ 4.1 (12,100)	2.6 (41,612)/ 3.8 (49)	4.7 (128,037)/4.7 (17,000)	4.0 (89,977)/ 4.7 (707)	4.1 (31)/4.3 (57)	4.1 (74)/4.5 (55)
	Android	Yes	Yes	Yes	Yes	Yes	Yes
	iOS	Yes	Yes	Yes	Yes	Yes	Yes
	Developer/Owner	Australian Department of Health	Ministero della Salute	Zoe Global Limited & Kings College	NHS England	Arizona Department of Health Services	PathCheck, Inc.
	Country	Australia	Italy	UK	UK	USA	USA
	Status	In use	In use	In use	In use	In use	In use
Health Tools	User Status (Risk Assessment)	Yes	Yes	No	Yes	Yes	Yes
	Self-Assessment	No	No	No	Yes	No	Yes
	E-Pass Integration	No	No	No	No	No	No
	Test Results Reporting	Yes	Yes	No	Yes	No	Yes
	Online Consultation	No	No	No	No	No	Yes
	Contact Tracing	Yes	Yes	No	Yes	Yes	Yes
Learning	Personalized Notes	No	No	No	Yes	No	Yes
	Educational Resources	No	No	Yes	Yes	No	Yes
	COVID-19 Information	No	Yes	Yes	Yes	No	Yes
Communication	Query Resolution	No	No	No	No	No	Yes
	Appointments	No	No	No	Yes	No	Yes
	Social Network	No	No	No	No	No	No
	Notifications	Yes	Yes	Yes	Yes	Yes	Yes
App Design	Data Visualisation	Yes	Yes	Yes	Yes	Yes	Yes
	Program Plan	Yes	No	No	Yes	No	Yes
Networking	Location Mapping (GPS)	No	No	No	Yes	No	Yes
	Connectivity with Other Devices	Yes	Yes	No	Yes	Yes	Yes
Safety & Security	Alerts	Yes	Yes	Yes	Yes	Yes	Yes
	Data Protection	Medium Risk	Low Risk	Low Risk	Medium Risk	Low Risk	Low Risk

Πίνακας 5.2.ii: Χαρακτηριστικά και λειτουργίες των 12 εφαρμογών (Apps) κατά του Covid-19 (Πηγή: [1])

Μερικά από τα συμπεράσματα που προέκυψαν παρουσιάζονται παρακάτω:

- Όλες οι εφαρμογές μπορούν να χρησιμοποιηθούν από την πλειοψηφία των χρηστών κινητών συσκευών σε όλο τον κόσμο, είναι δωρεάν και διαθέσιμες στις πλατφόρμες Android και iOS. Ωστόσο, οι λειτουργίες των εφαρμογών διαφέρουν σε σχέση με τα διαθέσιμα εργαλεία υγείας.
- Δέκα από τις δώδεκα εφαρμογές (Mawid, Tabaud, Tawakkalna, Aarogya Setu, TraceTogether, COVIDSafe, Immuni, NHS COVID-19, COVID Watch, PathCheck SafePlaces) έχουν τη δυνατότητα αξιολόγησης της κατάστασης ή κινδύνου του χρήστη, διαθέτουν την επιλογή αναφορών αποτελεσμάτων των τεστ Covid-19 (βοηθά στην ανάλυση της εξάπλωσης του ιού) και αποστέλλει ειδοποιήσεις στους χρήστες που έχουν έρθει σε στενή επαφή με μολυσμένο άτομο έτσι ώστε να λάβουν προληπτικά μέτρα.
- Τέσσερις από τις εφαρμογές (Mawid, Aarogya Setu, NHS COVID-19 και PathCheck SafePlaces) που εξετάστηκαν παρείχαν τεστ αυτοαξιολόγησης, μέσα από τα οποία οι χρήστες μπορούν να αξιολογήσουν την κατάστασή τους και να λάβουν ανατροφοδότηση σχετικά με τα απαραίτητα προληπτικά μέτρα.
- Δύο από τις εφαρμογές (Tawakkalna, Aarogya Setu) παρείχαν υπηρεσίες e-pass ή ταξιδιωτικών αδειών κατά τη διάρκεια της επιδημίας COVID-19.
- Εννέα από τις δώδεκα εφαρμογές (Tabaud, Tawakkalna, Aarogya Setu, TraceTogether, COVID Safe, Immuni, NHS COVID-19, COVID Watch και PathCheck SafePlaces) παρείχαν μια λειτουργία ανίχνευσης επαφών.
- Μία μόνο εφαρμογή (Mawid) επέτρεπε αναφορές ελέγχων τεστ, έτσι ώστε οι χρήστες να μπορούν να κλείσουν κάποιο ραντεβού ή να λάβουν υπηρεσίες υγειονομικής περίθαλψης, αλλά δεν διέθετε λειτουργίες ανίχνευσης επαφών [1].

Εστιάζοντας στην ενσωμάτωση των εργαλείων υγείας, μπορεί να παρατηρηθεί ότι:

- Η πλειονότητα των εφαρμογών διέθεταν ανίχνευση επαφών, αναφορές αποτελεσμάτων τεστ και τεστ αυτοδιάγνωσης, αντικατοπτρίζοντας τον βασικό στόχο τους, που ήταν ο περιορισμός της εξάπλωσης του κορωνοϊού.
- Κάποιες εφαρμογές όπως οι Mawid, Sehha, Aarogya Setu και PathCheck παρείχαν διαδικτυακές συμβουλευτικές υπηρεσίες, διευκολύνοντας πρακτικά τις διαδικασίες κοινωνικού συγχρωτισμού και καραντίνας στο σπίτι, διασφαλίζοντας την αδιάκοπη παροχή υπηρεσιών υγειονομικής περίθαλψης για διάφορες καταστάσεις/παθήσεις.
- Θα πρέπει να σημειωθεί ότι η εγκατάσταση διαφορετικών εφαρμογών για τις διάφορες υπηρεσίες, όπως συμβουλευτική, ενημέρωση πληροφοριών, ιχνηλάτηση επαφών και ταξιδιωτικών αδειών μπορεί να προκαλέσει σύγχυση και ασάφεια στους πολίτες σχετικά με τη χρήση τους. Επομένως,

μια ενιαία εφαρμογή που ενσωματώνει πολλές υπηρεσίες όπως στο Aarogya Setu και το PathCheck μπορεί να διευκολύνουν τους πολίτες, επιτρέποντάς τους την πρόσβαση σε υπηρεσίες από μία μόνο εφαρμογή.

Αναφορικά με τα εργαλεία ενημέρωσης, εκμάθησης και επικοινωνίας, παρατηρήθηκε ότι:

- Πέντε (Mawid, Sehha, Aarogya Setu, NHS COVID-19, PathCheck SafePlaces) από τις δώδεκα εφαρμογές παρείχαν επιλογές για εξατομικευμένες σημειώσεις.
- Πέντε από αυτές εφαρμογές (Sehha, Aarogya Setu, COVID-Symmptom Study, NHS COVID-19 και PathCheck SafePlaces) παρείχαν πρόσβαση σε εκπαιδευτικούς υγειονομικούς πόρους και πληροφορίες σχετικά με τον COVID-19. Με την ταχεία εξάπλωση των ψευδών ειδήσεων για τον COVID-19 σε όλο τον κόσμο, είναι υψίστης σημασίας οι άνθρωποι να εκπαιδεύονται κατάλληλα και να ενημερώνονται για προληπτικά μέτρα, άλλες θεραπείες και διαδικασίες ασφαλείας.
- Τέσσερις από τις δώδεκα εφαρμογές (Mawid, Sehha, Aarogya Setu, PathCheck SafePlaces) πρόσφεραν επιλογές για την επίλυση ερωτημάτων.
- Τέσσερις εφαρμογές (Mawid, Sehha, NHS COVID-19, PathCheck SafePlaces) πρόσφεραν διαδικτυακή κράτηση ραντεβού.
- Σε καμία από τις εφαρμογές δεν εντοπίστηκε ενσωμάτωση λειτουργιών κοινωνικής δικτύωσης, ενώ όλες παρείχαν σχετικές ειδοποιήσεις [1].

Όσον αφορά το σχεδιασμό, τη δικτύωση και την ασφάλεια των εφαρμογών, μπορεί να σημειωθεί ότι:

- Όλες οι εφαρμογές παρείχαν τη δυνατότητα οπτικοποίησης δεδομένων και γραφικής αναπαράστασης πληροφοριών σχετικά με τις λοιμώξεις COVID-19. Από αυτές, οι μισές (Tabaud, Sehha, Aarogya Setu, COVID Safe, NHS COVID-19 και PathCheck SafePlaces) πρόσφεραν τη δυνατότητα επιλογής σχεδιασμού παρουσίασης, ενώ οι άλλες μισές όχι.
- Οι μισές από τις εφαρμογές που εξετάστηκαν (Mawid, Tawakkalna, Aarogya Setu, TraceTogether, NHS COVID-19, PathCheck SafePlaces) χρησιμοποιούσαν τη λειτουργία εντοπισμού τοποθεσίας μέσω GPS, ενώ οι άλλες μισές (Tabaud, Sehha, COVID Symptom Study, Immuni, COVID Safe, COVID Watch) δεν ενσωμάτωναν αυτήν τη λειτουργία λόγω αυξανόμενων ανησυχιών για το απόρρητο.
- Οκτώ από τις δώδεκα εφαρμογές (Aarogya Setu, TraceTogether, NHS COVID-19, PathCheck SafePlaces, Tabaud, Immuni, COVID Safe, COVID Watch), υλοποιήθηκαν με βάση την τεχνολογία Bluetooth Low Energy, η οποία είναι ιδιαίτερα αποτελεσματική εξαιτίας της χαμηλής κατανάλωσης ενέργειας για τον εντοπισμό επαφών κοντινών αποστάσεων. Για τον παραπάνω λόγο, η πλειονότητα των εφαρμογών προτίμησε την εν λόγω τεχνολογία.

- Παρά την ευρεία χρήση των εφαρμογών διαχείρισης του COVID-19, ζητήματα όπως το απόρρητο, η ασφάλεια, η ασφάλεια και η προστασία δεδομένων συνεχίζουν να απασχολούν την διεθνή κοινότητα. Παρόλο που εφαρμογές όπως το TraceTogether, το Immuni, το COVID Watch, το PathCheck κ.λπ. έχουν προβεί σε ενημέρωση και εφαρμογή σαφής πολιτικής απορρήτου αναφορικά με τη χρήση και καταστροφή δεδομένων, με στόχο την αποφυγή συλλογής προσωπικών πληροφοριών που ενδέχεται να αποκαλύψουν την ταυτότητα του χρήστη, παρατηρούνται ακόμα ζητήματα που παραμένουν θολά και αναζητούν επίλυση [1].

5.2.1 Mawid App

Η εφαρμογή Mawid είναι ένα κεντρικό σύστημα κράτησης ιατρικών ραντεβού από το Υπουργείο Υγείας της Σαουδικής Αραβίας, μέσω του οποίου οι ασθενείς μπορούν να κλείσουν, να ακυρώσουν και να τροποποιήσουν το ραντεβού τους σε 2400 κέντρα πρωτοβάθμιας φροντίδας. Μέσω του GPS και της λειτουργίας χαρτών, οι ασθενείς μπορούν να δουν τα κέντρα πρωτοβάθμιας περίθαλψης που βρίσκονται πλησιέστερα στην τοποθεσία τους. Η εφαρμογή ειδοποιεί επίσης τον χρήστη σε περίπτωση που υπάρξει κενή θέση ραντεβού νωρίτερα από το προγραμματισμένο, ελαχιστοποιώντας έτσι το χρόνο αναμονής σε ασθενείς που αναζητούν άμεσα ραντεβού. Επίσης, διαθέτει λειτουργία αυτοαξιολόγησης για τον COVID-19, προσφέροντας συμβουλευτικές υπηρεσίες προς τους χρήστες. Από την κυκλοφορία της, τον Μάιο του 2019, η εφαρμογή έχει ενσωματωθεί στο 98% των νοσοκομείων και κέντρων πρωτοβάθμιας περίθαλψης, εξυπηρετώντας περισσότερους από 6,5 εκατομμύρια εγγεγραμμένους χρήστες. Η εφαρμογή παρέχει ιατρικές συμβουλές σε περισσότερους από μισό εκατομμύριο ανθρώπους, έχοντας καταγράψει περισσότερα από 250.000 τεστ αυτοαξιολόγησης [1].

5.2.2 Tabaud App

Η εφαρμογή Tabaud αναπτύχθηκε για τον έλεγχο εξάπλωσης του COVID-19, προκειμένου να χαλαρώσουν οι περιορισμοί στις κοινωνικές και επιχειρηματικές δραστηριότητες στη Σαουδική Αραβία. Η εφαρμογή σχεδιάστηκε κυρίως για τον εντοπισμό επαφών, καθώς ειδοποιεί τους χρήστες όταν έρχονται σε στενή επαφή με άλλα μολυσμένα άτομα που έχουν εγγραφεί και χρησιμοποιούν την ίδια εφαρμογή. Χρησιμοποιεί το Google Apple API για τον εντοπισμό επαφών, το οποίο προστατεύει αυστηρά το απόρρητο και την ασφάλεια των χρηστών, ενώ για τον εντοπισμό κοντινών smartphone αξιοποιεί την τεχνολογία Bluetooth και όχι την χαρτογράφηση τοποθεσίας. Εάν ένας χρήστης ενημερώσει την εφαρμογή ότι μολύνθηκε, στη συνέχεια η πληροφορία αποστέλλεται στο Υπουργείο Υγείας, και εφόσον επιβεβαιωθεί όλοι οι χρήστες smartphone με την εφαρμογή Tabaud που βρέθηκαν κοντά στο μολυσμένο άτομο το διάστημα των 14 ημερών πριν από τη μόλυνση, θα λάβουν ειδοποίηση για να λάβουν τα απαραίτητα μέτρα προφύλαξης. Επιπλέον, η εφαρμογή αναλύει την εγγύτητα των άλλων smartphone στο μολυσμένο άτομο, βοηθώντας στην εκτίμηση της ικανότητας και του κινδύνου μόλυνσης. Ωστόσο, η

ταυτότητα των προσώπων αποκρύπτεται και η ανωνυμία διατηρείται κατά την επικοινωνία με άλλες εφαρμογές smartphone, υιοθετώντας αυστηρές πολιτικές απορρήτου. Περισσότερα από 15.000 θετικά κρούσματα έχουν αναφερθεί μέσω των χρηστών της εφαρμογής [1].

5.2.3 Tawakkalna App

Το Tawakkalna, είναι η επίσημη εφαρμογή για κινητά από το Υπουργείο Υγείας της Σαουδικής Αραβίας, με στόχο τη διευκόλυνση των μετακινήσεων των ανθρώπων κατά τη διάρκεια του lockdown. Επιπλέον, παρέχει πληροφορίες σχετικά με τον COVID-19, όπως τον αριθμό των μολύνσεων σε διαφορετικές τοποθεσίες, και επιτρέπει στους πολίτες της χώρας να ζητούν ταξιδιωτικές άδειες λόγω έκτακτης ανάγκης κατά τη διάρκεια της απαγόρευσης μετακινήσεων και κυκλοφορίας. Η εφαρμογή ειδοποιεί επίσης τους χρήστες εάν βρίσκονται κοντά σε μολυσμένες ζώνες, ενώ η κατάσταση του κάθε χρήστη εμφανίζεται μέσω ενός έγχρωμου QR κωδικού, όπου η πράσινη εκδοχή του δείχνει ότι το άτομο είναι υγιές και έχει άδεια να ταξιδέψει, η κίτρινη ότι το άτομο είναι ύποπτο κρούσμα COVID-19 και δεν επιτρέπεται να κινηθεί και η κόκκινη δείχνει ότι το άτομο έχει μολυνθεί και οφείλει να παραμείνει σε καραντίνα [1].

5.2.4 Sehha App

Η εφαρμογή Sehha είναι μια από τις πιο καινοτόμες εφαρμογές υγείας για κινητές συσκευές στη Σαουδική Αραβία. Η εφαρμογή αναπτύχθηκε για την παροχή ηλεκτρονικής συμβουλευτικής μέσω βίντεο και ηχητικών μηνυμάτων από την άνεση του σπιτιού των χρηστών. Αξιοποιεί την τεχνολογία τεχνητής νοημοσύνης (AI), δίνοντας τη δυνατότητα στους χρήστες να λαμβάνουν ασφαλείς ιατρικές πληροφορίες και βελτιώνοντας την εμπειρία τους κατά τη συμβουλευτική διαδικασία. Επίσης, διαθέτει ένα εργαλείο αξιολόγησης της υγείας, όπου οι χρήστες απαντούν σε ορισμένες ερωτήσεις και βάσει των αποτελεσμάτων, αναπτύσσεται μια βαθμολογία αναφορικά με την κατάσταση υγείας του χρήστη, τη διάγνωση της πιθανής πάθησης, παρέχοντας παράλληλα και τη σχετική ανατροφοδότηση. Η εφαρμογή Sehha είναι παρόμοια με την εφαρμογή Mawid όσον αφορά την κράτηση ραντεβού, αλλά διαφέρει από τη Mawid καθώς διευκολύνει την ηλεκτρονική συμβουλευτική διαδικασία ατόμων, ενώ η Mawid παρέχει συμβουλές σε κέντρα πρωτοβάθμιας περίθαλψης [1].

5.2.5 Aarogya Setu App

Το Aarogya Setu είναι μια επίσημη εφαρμογή για κινητά που κυκλοφόρησε στις 2 Απριλίου 2020 από τη κυβέρνηση της Ινδίας για την παρακολούθηση και τον περιορισμό εξάπλωσης του COVID-19. Από τις 26 Μαΐου, η εφαρμογή έχει πάνω από 114 εκατομμύρια χρήστες, περισσότερους από οποιαδήποτε παρόμοια εφαρμογή στον κόσμο και είναι διαθέσιμη σε 12 γλώσσες σε πλατφόρμες Android, iOS και KaiOS. Το AarogayaSetu, σε αντίθεση με άλλες παρόμοιες εφαρμογές, είναι μια τεράστια υλοποίηση all-in-one που όχι μόνο παρακολουθεί την τοποθεσία και τις επαφές μέσω Bluetooth (όπως και το Tawakkalna), αλλά

εκχωρεί χρωματικά κωδικοποιημένα σήματα που υποδεικνύουν τον κίνδυνο μόλυνσης. Παρέχει πρόσθετες λειτουργίες, όπως τεστ αυτοαξιολόγησης, αναφορές ελέγχων τεστ, ηλεκτρονικές ταξιδιωτικές άδειες, πληροφορίες σχετικά με τον COVID-19 και προληπτικά μέτρα, διαδικτυακή συμβουλευτική κ.ά. Η εφαρμογή έχει ειδοποιήσει περισσότερους από 1,4 εκατομμύρια χρήστες για πιθανό κίνδυνο μόλυνσης και συνέβαλε στη δημιουργία 697 hotspot κορωνοϊού στη χώρα. Ωστόσο, σε σχέση με τη χρήση δεδομένων, εκφράστηκαν ορισμένες ανησυχίες σχετικά με το απόρρητο, όπως η συλλογή και αποθήκευση πληροφοριών, οι θεσμικές αποκλίσεις, η έλλειψη νομοθεσίας, η διαφάνεια και η δυνατότητα ελέγχου. Η κυβέρνηση επίλυσε αυτά τα ζητήματα και η εφαρμογή χρησιμοποιείται επί του παρόντος από την πλειοψηφία των πολιτών [1], [18].

Η Ινδία είναι η μοναδική δημοκρατική χώρα στον κόσμο, που επέβαλλε τη χρήση της εφαρμογής του κορωνοϊού για τους πολίτες της. Ωστόσο, στη χώρα παρατηρούνται ελλείψεις στην εθνική νομοθεσία περί προσωπικού απορρήτου και, ως εκ τούτου, υπάρχει ασάφεια ως προς το ποιος μπορεί να έχει πρόσβαση στα δεδομένα της εφαρμογής. Η εφαρμογή χρησιμοποιεί τη «συνδρομητική χαρτογράφηση» και βασισμένη στα δεδομένα στοχεύει στον περιορισμό του ιού, παρέχοντας συμβουλές για καραντίνα, τεστ ή μέτρα προφύλαξης. Επίσης, έχει εντοπίσει σχεδόν 3500 hotspot σε όλη την Ινδία χρησιμοποιώντας την παραπάνω προσέγγιση, τα οποία και επιβεβαιώθηκαν στην πραγματικότητα έπειτα από 17-25 ημέρες. Τέλος, το συνολικό ποσοστό θετικού κρούσματος COVID-19 είναι περίπου 4,65% και μεταξύ εκείνων που έλαβαν οδηγίες για άμεση υποβολή σε τεστ, το 24% βρέθηκε θετικό [18].

5.2.6 TraceTogether

Το TraceTogether είναι μια εφαρμογή ανίχνευσης επαφών για έξυπνες συσκευές που ξεκίνησε από την κυβέρνηση της Σιγκαπούρης το Μάρτιο του 2020. Όπως και η εφαρμογή Aarogya Setu, χρησιμοποιεί την τεχνολογία Bluetooth για να αναγνωρίσει πότε ένας χρήστης βρίσκεται σε κοντινή απόσταση από ένα θετικό κρούσμα, στέλνοντας σχετικές ειδοποιήσεις στο χρήστη. Χρησιμοποιεί ανώνυμα αναγνωριστικά, τα οποία ανταλλάσσονται μεταξύ των συσκευών με εγκατεστημένο το TraceTogether. Το μόνο που απαιτεί η εφαρμογή είναι η δήλωση ενός έγκυρου τηλεφωνικού αριθμού. Κατά τον σχεδιασμό της εφαρμογής δόθηκε ιδιαίτερη σημασία στη διατήρηση απορρήτου και την ασφάλεια δεδομένων. Τα δεδομένα που αποθηκεύτηκαν μέσω Bluetooth στα smartphone διαγράφονται αυτόματα μετά από 21 ημέρες, εφόσον ο χρήστης δεν έχει έρθει σε επαφή με κάποιο ασθενή Covid-19, ενώ οι χρήστες διατηρούν το δικαίωμα διαγραφής δεδομένων, διασφαλίζοντας το επίπεδο απορρήτου υψηλό [1], [18].

5.2.7 COVIDSafe App

Στις 14 Απριλίου 2020, η ομοσπονδιακή κυβέρνηση ανακοίνωσε την εφαρμογή εντοπισμού COVIDSafe που βασίστηκε στη φαινομενική επιτυχία της εφαρμογής TraceTogether της Σιγκαπούρης και στο υποκείμενο πρωτόκολλο Bluetooth OpenTrace/BlueTrace. Η πρώτη έκδοση του COVIDSafe

υλοποιήθηκε από το Υπουργείο Υγείας της Αυστραλίας και ήταν διαθέσιμη για λήψη στα App Store της χώρας για συσκευές iOS και Android, αποτελώντας τη μόνη εφαρμογή που έχει εγκριθεί από την αυστραλιανή κυβέρνηση. Σκοπός της είναι η παρακολούθηση των μετακινήσεων των ανθρώπων και ο εντοπισμός στενών επαφών με μολυσμένα άτομα, αποστέλλοντας σχετικές ειδοποιήσεις, πληροφορίες και συμβουλευτική υποστήριξη. Η εφαρμογή εκτελείται στο παρασκήνιο, χρησιμοποιώντας τεχνολογία Bluetooth 4.0 για επικοινωνία (με χρήση ψηφιακής χειραψίας) με άλλες συσκευές που έχουν εγκαταστήσει την εφαρμογή COVIDSafe. Η λειτουργία της εφαρμογής απαιτεί την ενεργοποίηση των σχετικών ενημερώσεων από το COVIDSafe, εφόσον έχει προηγηθεί η επαλήθευση του χρήστη μέσω αυθεντικοποίησης δύο παραγόντων [1], [37].

Το COVIDSafe αποφεύγει τις διασυνδέσεις προσωπικών δεδομένων με μεμονωμένους πολίτες, παράγοντας τυχαία αναγνωριστικά που ανανεώνονται κάθε 2 ώρες. Οι χρήστες μπορούν να εγγραφούν χρησιμοποιώντας κάποιο ψευδώνυμο, προστατεύοντας την ταυτότητά τους, ενώ καταχωρούν τον αριθμό του κινητού τηλεφώνου τους. Αυτά τα αναγνωριστικά μεταδίδονται μεταξύ των διαφόρων συσκευών, ενώ αυτές καταγράφουν την ισχύ των συγκεκριμένων σημάτων Bluetooth, αποθηκεύοντας τις κρυπτογραφημένες πληροφορίες, όπως η ημερομηνία, η ώρα και οι αριθμοί επικοινωνίας, στη συσκευή για 21 ημέρες. Έπειτα από την πάροδο αυτού του διαστήματος, οι χρήστες μπορούν να διαγράψουν τα δεδομένα, ενώ το σύνολο αυτών που αποθηκεύονται στο National Covid Safe Data store θα καταστραφούν μετά το τέλος της πανδημίας. Η διαδικασία ενεργοποιείται μόνο υπό την προϋπόθεση ότι ένας χρήστης (α) επικοινωνήσει με έναν υγειονομικό υπάλληλο για να κοινοποιήσει ένα θετικό τεστ COVID και στείλει ένα μοναδικό κωδικό ενεργοποίησης μέσω SMS και (β) στη συνέχεια αποκτά τη δυνατότητα να ανεβάσει τα τοπικά αποθηκευμένα αναγνωριστικά (IDs) ως κρυπτογραφημένα δεδομένα στο κυβερνητικό διακομιστή, που υποστηρίζεται από την Amazon Web Services. Η εισαγωγή του ληφθέντος κωδικού (PIN) παρέχει λειτουργικά την ενεργή συγκατάθεση του χρήστη για την προβλεπόμενη χρήση της εφαρμογής δημόσιας υγείας [1], [37].

Εικόνα 5.1: Γραφική απεικόνιση εφαρμογής COVIDSafe (a) Μενού εισόδου, (b) Σελίδα γενικών πληροφοριών, (c) ραντάρ εντοπισμού επαφών, (d) Μενού παρακολούθησης υγείας, (e) δείκτης κινδύνου νόσησης (Πηγή: [35])

Με την εγκατάσταση του COVIDSafeApp σε ένα έξυπνο κινητό, παράγεται ένα ζεύγος δημόσιου και ιδιωτικού κλειδιού, έπειτα από τη λήψη ενός επικυρωμένου αριθμού OTP στο τηλέφωνο, ο οποίος προέρχεται από την εισαγωγή του χρήστη στην εφαρμογή. Επομένως, ο αριθμός τηλεφώνου δεν αποθηκεύεται, ούτε χρησιμοποιείται για άλλους σκοπούς, ενώ ο χρήστης χρησιμοποιεί ως ταυτότητα το δημόσιο κλειδί [4].

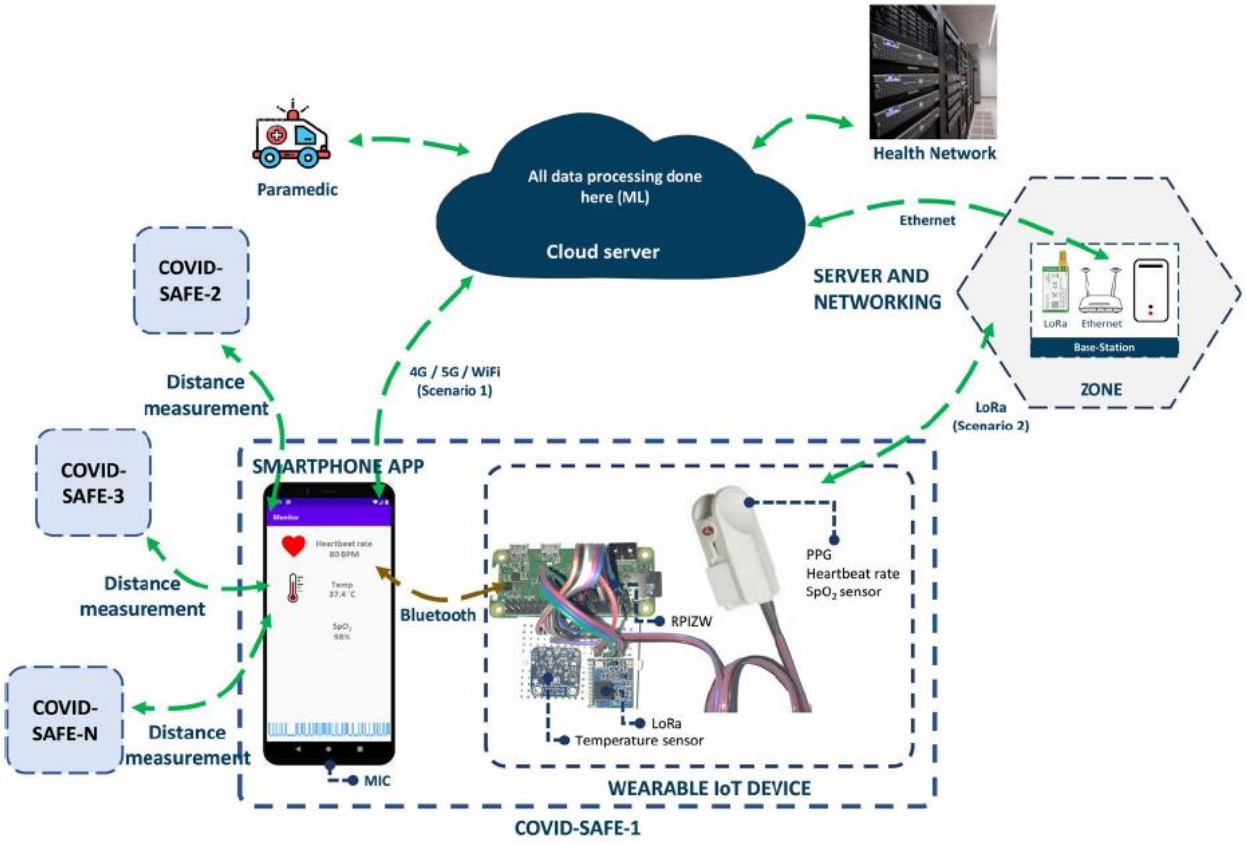
Η πλατφόρμα COVIDSafe συντίθεται από τη φορητή IoT συσκευή, την εφαρμογή (app) του κινητού και τον διακομιστή ομίχλης (fog), προσφέροντας χαμηλού κόστους και χαμηλών απαιτήσεων IoT nodes που αναπτύχθηκαν στο Raspberry Pi Zero (RPIZ), για την συνεχή παρακολούθηση της θερμοκρασίας του σώματος, του καρδιακού ρυθμού, του κορεσμού οξυγόνου στο αίμα και την περιοδικότητα του βήχα. Τα δεδομένα που συλλέγονται από τους IoT nodes αποθηκεύονται σε ένα διακομιστή ομίχλης, ενώ στη συνέχεια εφαρμόζεται ένας αλγόριθμος μηχανικής εκμάθησης για να στείλει τις απαραίτητες πληροφορίες στους χρήστες. Το λογισμικό περιλαμβάνει μια διεπαφή προγράμματος εφαρμογής (Application Program Interface - API) για την αλληλεπίδραση με τους χρήστες και ένα σύστημα λήψης αποφάσεων Fuzzy στον διακομιστή ομίχλης. Τα nodes συλλέγουν δεδομένα και αναβαθμίζουν τους κανόνες λήψης αποφάσεων με στόχο την υποστήριξη των χρηστών σε διάφορες περιπτώσεις, όπως η ανάγκη επίσκεψης σε κάποιο γιατρό, η διατήρηση αποστάσεων και οι ειδοποιήσεις σχετικά με περιοχές υψηλού κινδύνου μόλυνσης [35].

Α. Φορητή IoT συσκευή

Το IoT node λειτουργεί συνδυαστικά με το έξυπνο κινητό του χρήστη, συλλέγοντας δεδομένα εγγύτητας μέσω Bluetooth και επικοινωνώντας με το διακομιστή μέσω του δικτύου κινητής τηλεφωνίας. Αποτελείται από έναν Raspberry Pi Zero (RPIZ) κεντρικό επεξεργαστή, δύο αισθητήρες θερμοκρασίας και φωτοπληθυσμογραφήματος (PPG), και το πρόσθετο LoRa για επικοινωνία δεδομένων όταν δεν είναι εφικτή η σύνδεση στο δίκτυο κινητής τηλεφωνίας ή στο WiFi. Ο αισθητήρας PPG είναι ένα μη επεμβατικό εργαλείο που προσαρμόζεται ανώδυνα στο άκρο του δακτύλου του χρήστη, στέλνοντας δύο μήκη κύματος φωτός στο δάκτυλο και συλλέγοντας το ανακλώμενο μέσα από μια δίοδο μεγέθους καρφίτσας. Η έξοδος αυτού του αισθητήρα καταγράφεται αναλογικά και μετατρέπεται σε ψηφιακό σήμα (ADC). Επίσης, παρακολουθεί συνεχώς τη φωνή του χρήστη για να καταγράψει τον ρυθμό και τη σοβαρότητα του βήχα. Τέλος, λογισμικό και σύστημα συγχρονίζονται με κατεύθυνση την παρακολούθηση του χρήστη κατά τη διάρκεια των καθημερινών του δραστηριοτήτων.

Η λειτουργία του υποστηρίζεται με δύο τρόπους, όπου στον πρώτο το IoT node αποστέλλει τα δεδομένα του αισθητήρα στην εφαρμογή smartphone μέσω σύνδεσης Bluetooth και στη συνέχεια στον διακομιστή μέσω 4G/5G ή WiFi. Ο διακομιστής τροφοδοτεί την εφαρμογή με τις πιο πρόσφατες ενημερώσεις και ειδοποιήσεις αναφορικά με νέους περιορισμούς και χρήσιμες συμβουλές από τις υπηρεσίες υγείας και τις κυβερνήσεις. Η εφαρμογή αποστέλλει τις παραμέτρους σώματος των χρηστών για περαιτέρω επεξεργασία στο διακομιστή cloud, για να επιστρέψει αυτός στη συνέχεια το βαθμό επικινδυνότητας νόσησης του χρήστη. Ο δεύτερος τρόπος λειτουργίας είναι ένα δίκτυο που βασίζεται στο LoRa, μια τεχνολογία ασύρματης συχνότητας ήχου που λειτουργεί σε ένα φάσμα ραδιοσυχνοτήτων απαλλαγμένο από άδειες. Το LoRa είναι ένα πρωτόκολλο φυσικού επιπέδου που χρησιμοποιεί διαμόρφωση ευρέως φάσματος και υποστηρίζει επικοινωνία μεγάλης εμβέλειας μέσα από ένα στενό εύρος ζώνης εκπομπής, καθιστώντας το ανθεκτικό στις παρεμβολές. Το IoT node εισέρχεται σε αυτήν τη λειτουργία όταν δεν είναι διαθέσιμη η σύνδεση μέσω 4G/5G/WiFi [35].

Ο Raspberry Pi Zero (RPIZ) διαθέτει μια κεντρική μονάδα επεξεργασίας (CPU) ενός πυρήνα 1 GHz με 512 MB μνήμη τυχαίας πρόσβασης (RAM), αρκετές εισόδους/εξόδους (Global Purpose Input/Outputs - GPIOs), ασύρματο δίκτυο LAN και συνδεσιμότητα Bluetooth, καθιστώντας την πλατφόρμα ως την καταλληλότερη επιλογή για συστήματα που βασίζονται στο Διαδίκτυο των Πραγμάτων. Το IoT node σχεδιαστηκε με την βοήθεια ενός τρισδιάστατου εκτυπωτή στη μορφή κλιπ δακτύλου, λειτουργεί με μπαταρία και εσωκλείει όλα τα απαραίτητα στοιχεία, δίχως να απολέσει τη φιλικότητά του προς τον χρήστη [35].



Εικόνα 5.2: Το πλαίσιο αρχιτεκτονικής της εφαρμογής COVIDSafe, όπου COVIDSafe-1 είναι ο χρήστης (Πηγή: [35]).

Β. Σύστημα Λήψης Αποφάσεων

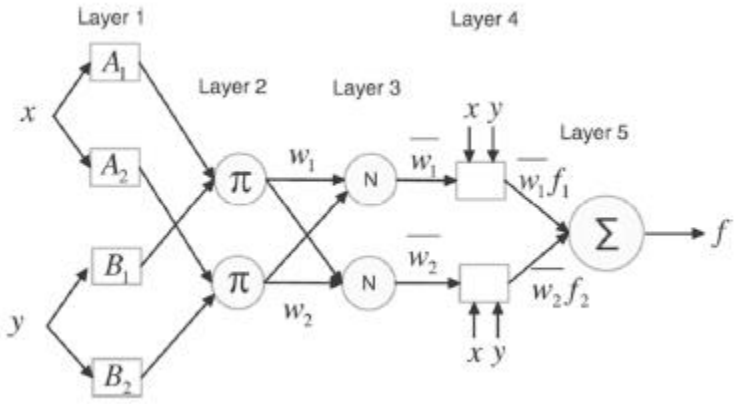
Ένα fuzzy σύστημα τεκμηρίων αποτελεί ένα σύστημα λήψης αποφάσεων που χρησιμοποιείται για την πρόβλεψη του κινδύνου εξάπλωσης του ιού. Το μοντέλο εκτιμά έναν παράγοντα κινδύνου που περιέχει τρεις ποιοτικές τιμές (χαμηλή, μέτρια και υψηλή), οι οποίες μπορούν να βοηθήσουν τους χρήστες να αντιληφθούν εάν βρίσκονται σε ασφαλή κατάσταση ή εάν μπορεί να μεταδώσουν και οι ίδιοι την ασθένεια. Το προτεινόμενο πλαίσιο προσομοίωσης πραγματοποιείται σε MATLAB. Ο σκοπός αυτής της εφαρμογής είναι να σχεδιάσει ένα σύστημα όπου τα ίδια τα άτομα προβλέπουν την θετικότητα ή μη στον Covid, αφού εισάγουν συμπτώματα σε μια εφαρμογή που βασίζεται σε Blockchain και IoT.

Οι είσοδοι του fuzzy συστήματος τροφοδοτούνται από τα χαρακτηριστικά υγείας και τις πληροφορίες που σχετίζονται με την τοποθεσία του χρήστη. Τα χαρακτηριστικά υγείας περιλαμβάνουν τον αναπνευστικό ρυθμό, τη συχνότητα του βήχα, τη θερμοκρασία, το δείκτη μάζας σώματος (BMI) και το επίπεδο κορεσμού οξυγόνου στο αίμα, ενώ ο βαθμός κινδύνου βάσει περιοχής υπολογίζεται στον διακομιστή με χρήση παραμέτρων, όπως η τελευταία φορά που εκτέθηκε ο χρήστης σε επαφή με κάποιο θετικό κρούσμα και το ποσοστό θετικότητας στην περιοχή [35].

B1. Προσομοίωση ANFIS

Πρώτον, χρησιμοποιούμε το Adaptive Neuro-fuzzy Inference System (ANFIS) για την πρόβλεψη θετικότητας ή μη στον Covid και το K-Nearest Neighbor (KNN) για τη βελτίωση του ποσοστού ακρίβειας. Δεύτερον, χρησιμοποιούμε ένα σύνολο αριθμητικών δεδομένων σε πραγματικό χρόνο που αποτελείται από συμπτώματα COVID-19 για το KNN. Το KNN αποτελείται από τα Ensemble KNN, Cousine KNN και Fine KNN. Με βάση αυτό το σύνολο δεδομένων αποτελείται από συμπτώματα Covid, το σύστημα θα προβλέψει το ποσοστό ακρίβειας έπειτα από εκπαίδευση και δοκιμές με όλους τους τύπους του KNN. Το προτεινόμενο σύστημα προβλέπει την κατάσταση του Covid με βάση όλα τα καταγεγραμμένα συμπτώματα και το KNN ενισχύει το ποσοστό ακρίβειας με το Ensemble KNN [4].

Στο σύστημα ANFIS, το σύνολο δεδομένων χωρίζεται σε δύο τμήματα με 80% για εκπαίδευση και 20% για δοκιμές, εφαρμόζοντας το μοντέλο Sugeno που αποτελείται από ένα σύνολο αριθμητικών δεδομένων με έξι παραμέτρους εισόδου (ηλικία, βήχας, πυρετός, διάρροια, γρίπη, πονοκέφαλος) και μόνο μία καθαρή έξοδο ναι/όχι που αφορά τη θετικότητα στον ιό. Η συμπεριφορά ενός πολύπλοκου συστήματος περιγράφεται από την διύλιση των ασαφών κανόνων IF-THEN.



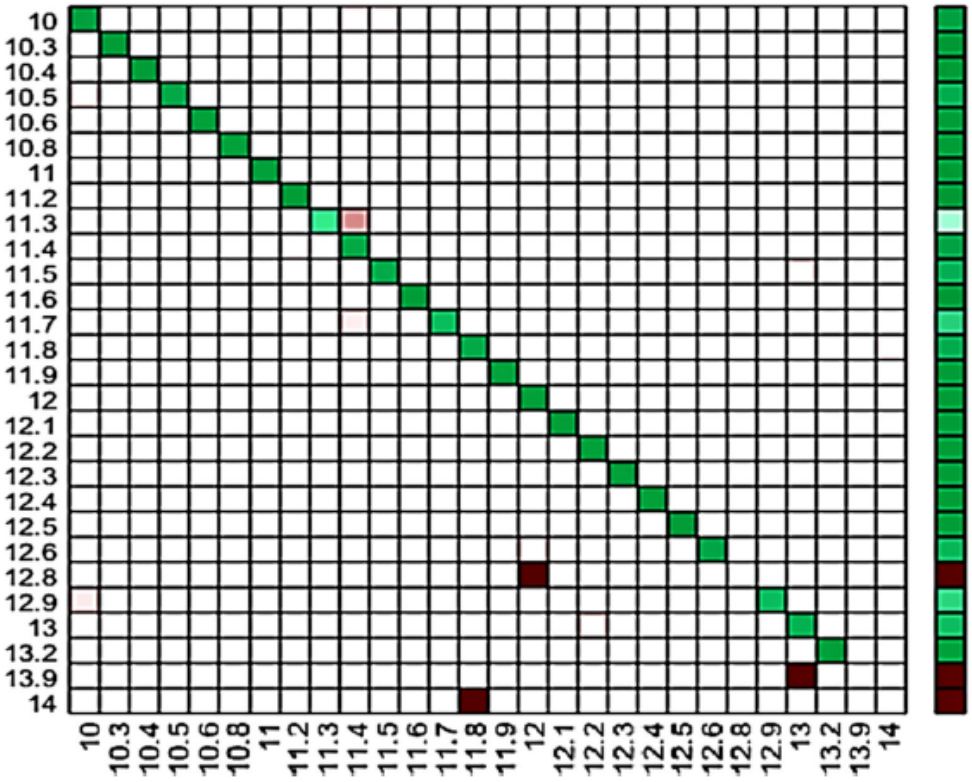
Εικόνα 5.3: Η Αρχιτεκτονική του αλγόριθμου ANFIS

B2. Προσομοίωση KNN

Ο αλγόριθμος KNN χρησιμοποιείται για την ταξινόμηση του αριθμητικού συνόλου δεδομένων για την πρόβλεψη μόλυνσης ή μη του ατόμου με βάση τα υπάρχοντα συμπτώματα. Σκοπός του KNN είναι να αυξήσει το ποσοστό ακρίβειας μετά την εκπαίδευση του συνόλου δεδομένων σε αλγόριθμους KNN, που περιλαμβάνει 415 σειρές και 16 στήλες. Στη συνέχεια, επιλέγουμε τον αλγόριθμο KNN για υλοποίηση και εισάγουμε τα δεδομένα σε όλους τους τύπους του (Fine KNN, Cousine KNN και Ensemble KNN). Μετά την εκπαίδευση του συνόλου δεδομένων σε όλους τους αλγόριθμους KNN, συμπεραίνουμε ότι το Ensemble KNN έχει επιτύχει το καλύτερο ποσοστό ακρίβειας. Το συνολικό ποσοστό ακρίβειας είναι

95,9%, ενώ έχει παρατηρηθεί ότι το Ensemble KNN επιτυγχάνει το υψηλότερο ποσοστό ακρίβειας. Το σχήμα 13 αντιπροσωπεύει το γράφημα της καμπύλης ROC του προτεινόμενου πλαισίου.

Στην εικόνα 5.4, ο πίνακας σύγχυσης αποτελείται από το ορθό ποσοστό θετικότητας και το ψευδές ποσοστό θετικότητας στον ιό, διαχωρίζοντας δύο τύπους κλάσεων όπου η μία είναι η πραγματική και η άλλη η προβλεπόμενη τάξη. Μπορούμε να υπολογίσουμε την ακρίβεια, το ποσοστό ακρίβειας, την ορθή και την εσφαλμένη ταξινόμηση μέσω αυτού του ορθού και ψευδούς ποσοστού θετικότητας. Ο πίνακας σύγχυσης φανερώνει ότι όλες οι παράμετροι προβλέπονται με ακρίβεια [4].



Εικόνα 5.4: Πίνακας σύγχυσης για τον αλγόριθμο KNN (Πηγή: [4])

Γ. Αξιολόγηση εφαρμογής

Η εφαρμογή COVIDSafe αποτελεί το πιο ολοκληρωμένο πλαίσιο IoT που μπορεί να χρησιμοποιηθεί για τον έλεγχο της μόλυνσης και την επιτήρηση της πανδημίας. Πολλές χώρες έχουν εφαρμόσει εφαρμογές ανίχνευσης επαφών που εντοπίζουν το ιστορικό της τοποθεσίας ενός ασθενούς και ειδοποιούν τους χρήστες εάν κάποιος έχει προσβληθεί από τον COVID-19 στα μέρη που έχουν επισκεφτεί πρόσφατα. Από την άλλη πλευρά, το σύστημα COVIDSafe, όπως παρουσιάζεται παραπάνω, παρέχει υλικό, αισθητήρες και λογισμικό (Μηχανικής Μάθησης (ML) και το app για κινητές συσκευές), προσφέροντας ορισμένα πλεονεκτήματα, όπως (βλ. Πίνακα 5.3):

- Αυτοαξιολόγηση αλλά και αυτόματη καταγραφή συμπτωμάτων του χρήστη μέσω αισθητήρων.
- Παροχή διάγνωσης σύμφωνα με τα χαρακτηριστικά της κατάστασης του χρήστη και τοπολογικά δεδομένα.
- Παροχή ειδοποιήσεων τόσο στο χρήστη όσο και σε υγειονομικούς φορείς.
- Τακτική ανανέωση πληροφοριών σε πραγματικό χρόνο.
- Υποστήριξη απομακρυσμένης παρακολούθησης ασθενών.

Description / Scope	**Service offered**					
	COVID symptoms	***Hardware offered?***	***Diagnosis***	***Notification to person/ HA***	***Update real-time?***	***Remote monitoring***
COVID-SAFE – a complete IoT system	Yes (fever, cough, SpO_2, HR, BMI, hotspots)	Yes (both smartphone and sensors to collect real-time data)	Yes (personal and regional data)	Yes, Yes	Yes	Yes

Πίνακας 5.3: Αξιολόγηση COVIDSafe App βάσει των προσφερόμενων υπηρεσιών (Πηγή: [35])

5.2.8 Immuni App

Το Immuni είναι μια πολυγλωσσική εφαρμογή ανίχνευσης επαφών που κυκλοφόρησε από την ιταλική κυβέρνηση τον Ιούνιο του 2020. Λειτουργεί παρόμοια με άλλες εφαρμογές ανίχνευσης επαφών, ειδοποιώντας τους χρήστες εάν έρθουν σε στενή επαφή με ένα άτομο που χρησιμοποιεί την ίδια εφαρμογή και έχει εγγραφεί ως μολυσμένο. Η ιδιαιτερότητα της εφαρμογής συνδέεται με τη χρήση της τεχνολογίας Bluetooth Low Energy, εξασφαλίζοντας χαμηλή κατανάλωση ενέργειας, καθώς και με την αποτροπή συλλογής προσωπικών στοιχείων όπως όνομα, ημερομηνία γέννησης, διεύθυνση, αριθμό τηλεφώνου ή διεύθυνση email. Εάν δύο χρήστες smartphone με εγκατεστημένη την εφαρμογή Immuni έρθουν σε στενή επαφή, τα smartphone τους ανταλλάσσουν αυτόματα κωδικούς, βοηθώντας στον εντοπισμό προηγούμενων επαφών εάν κάποιος από τους χρήστες διαγνωστεί με τον ιό. Πιο συγκεκριμένα, αυτός ο κωδικός εισάγεται στο κεντρικό σύστημα υγείας με τη συγκατάθεση των ασθενών και χρησιμοποιείται για την ειδοποίηση των χρηστών που ήρθαν σε στενή επαφή, δίχως την καταγραφή κινήσεων αλλά διαμοιρασμό μόνο των σχετικών κωδικών υποστήριξης της διαδικασίας εντοπισμού επαφών [1].

5.2.9 COVID Symptom Study App

Η εφαρμογή COVID Symptom Study αναπτύχθηκε από τους ερευνητές του King's College London Guys, του St Thomas' Hospitals και της Zoe Global Limited, μιας εταιρείας τεχνολογίας υγείας. Ο σκοπός αυτής της εφαρμογής είναι η ανάλυση της εξάπλωσης του ιού, ο εντοπισμός περιοχών υψηλού κινδύνου στο Ηνωμένο Βασίλειο, η αξιολόγηση ευάλωτων τμημάτων της κοινωνίας και η κατανόηση των συμπτωμάτων που συνδέονται με υποκείμενες παθήσεις υγείας. Δεν παρέχει πληροφορίες ή συμβουλές για την υγεία, αλλά προορίζεται για συγκέντρωση δεδομένων προκειμένου να προωθήσει την έρευνα που

σχετίζεται με τον COVID-19 στο Ηνωμένο Βασίλειο και ως εκ τούτου τη λήψη καλύτερων προληπτικών μέτρων. Οι άνθρωποι συμμετέχουν εθελοντικά στη μελέτη και μοιράζονται γενικές πληροφορίες, όπως ηλικία, πληροφορίες υγείας και τυχόν υποκείμενες παθήσεις, καθώς και συμπτώματα που μπορεί να εμφανίζουν. Περισσότεροι από 4 εκατομμύρια άνθρωποι από το Ηνωμένο Βασίλειο συμμετέχουν εθελοντικά στην εφαρμογή, συνεισφέροντας στη δημιουργία μιας αποτελεσματικής βάσης δεδομένων που μπορεί να χρησιμοποιηθεί για την ανάλυση πληροφοριών που σχετίζονται με τον COVID-19 [1].

5.2.10 NHS COVID-19 App

Η εφαρμογή NHS COVID-19 κυκλοφόρησε από το NHS Test and Trace, UK και αξιοποιεί την τεχνολογία χαμηλής κατανάλωσης Bluetooth μαζί με GPS για την ιχνηλασιμότητα των μετακινήσεων των χρηστών. Λειτουργίες της αποτελούν η ειδοποίηση του χρήστη σε περίπτωση στενής επαφής με άλλους εγγεγραμμένους χρήστες της εφαρμογής που βρέθηκαν θετικοί στον COVID-19, η αναφορά συμπτωμάτων και η κράτηση ενός δωρεάν τεστ COVID-19 από τις διαθέσιμες υπηρεσίες. Επίσης, ενημερώνει εάν έχει εντοπιστεί μεγάλος αριθμός θετικών κρουσμάτων σε τοποθεσίες (μέσω της καταγραφής των check-in που έχουν κάνει οι χρήστες), παρέχει συμβουλές υγείας και επιτρέπει στους χρήστες να παρακολουθούν την αντίστροφη μέτρηση για τη λήξη της καραντίνας τους. Η εφαρμογή δεν συλλέγει προσωπικές πληροφορίες που μπορεί να οδηγήσουν στην αναγνώριση του χρήστη, παρά μόνο αποθηκεύει πληροφορίες όπως η τοποθεσία, ο ταχυδρομικός κώδικας, το check-in σε κάποιο χώρο κ.ά. με στόχο την ιχνηλάτηση των επαφών του [1].

5.2.11 COVID Watch App

Η εφαρμογή COVID Watch (ΗΠΑ), αναπτύχθηκε από το Πανεπιστήμιο της Αριζόνα με την υποστήριξη του Τμήματος Υπηρεσιών Υγείας της περιοχής. Χρησιμοποιήθηκε από το πανεπιστήμιο και το σχέδιο ήταν να κυκλοφορήσει σε φάσεις σε ολόκληρη την Αριζόνα. Σκοπός της εφαρμογής είναι η παροχή ειδοποιήσεων στους χρήστες που ήρθαν σε στενή επαφή με οποιοδήποτε εγγεγραμμένο μολυσμένο άτομο που χρησιμοποιεί την εφαρμογή. Αξιοποιώντας την τεχνολογία Bluetooth, δεν εφαρμόζει υπηρεσίες παρακολούθησης τοποθεσίας και δεν συλλέγει προσωπικές πληροφορίες που ταυτοποιούν τον χρήστη. Το ιδιαίτερο χαρακτηριστικό της εφαρμογής είναι ότι κανένα μέλος ή φορέας δεν μπορεί να εντοπίσει την ταυτότητα των εγγεγραμμένων χρηστών, ενώ αποτέλεσε μια από τις πρώτες εφαρμογές που κυκλοφόρησε με προδιαγραφές ανοιχτού κώδικα [1].

5.2.12 PathCheck App

Το PathCheck (Η.Π.Α.) είναι μια εφαρμογή ανίχνευσης επαφών που αναπτύχθηκε από το MIT και το TripleBlind, οι οποίοι συνεργάστηκαν για να σχηματίσουν έναν μη κερδοσκοπικό οργανισμό που ονομάζεται PathCheck Foundation. Η εφαρμογή χρησιμοποιεί το Google Apple Exposure Notification

API, το οποίο διασφαλίζει το απόρρητο και την ασφάλεια των χρηστών, δίνοντάς τους τη δυνατότητα να αποθηκεύσουν την τοποθεσία και το ημερολόγιο συμπτωμάτων στο τηλέφωνό τους. Η εφαρμογή ενσωματώνει διάφορες υγειονομικές υπηρεσίες και οι χρήστες μπορούν να επιλέξουν το τμήμα όπου θα διαμοιραστούν οι πληροφορίες τους. Ο στόχος υλοποίησης του PathCheck είναι να επιταχύνει την επαναλειτουργία της οικονομίας και των κοινωνικών δραστηριοτήτων [1].

5.3 Ανάλυση πρόσθετων εφαρμογών κατά του Covid-19

Πάρα πολλές χώρες στον κόσμο έχουν αναπτύξει και κυκλοφορήσει εφαρμογές με σκοπό τον έλεγχο εξάπλωσης του COVID-19. Σύμφωνα με τη Διεθνή Αμνηστία, οι εφαρμογές «BeAware» του Μπαχρέιν και «Smittestopp» της Νορβηγίας είναι τα περισσότερο ανησυχητικά εργαλεία μαζικής παρακολούθησης. Θέτουν σε κίνδυνο το απόρρητο των χρηστών καθώς οι εφαρμογές εκτελούν ενεργά και σε ζωντανή μετάδοση της τοποθεσίας των χρηστών, ανεβάζοντας συχνά συντεταγμένες GPS σε έναν κεντρικό διακομιστή. Η πρόσφατη επιδημία του κορωνοϊού έχει επηρεάσει την παγκόσμια κοινότητα, επομένως θα μπορούσε να αναπτυχθεί ένα καθολικό σύστημα εφαρμογών για κινητά που θα ενσωματώνει όλες τις απαραίτητες λειτουργίες για τον εντοπισμό, την παρακολούθηση και την αποστολή ειδοποιήσεων και διασύνδεσης με τις υγειονομικές αρχές και τους κυβερνητικούς φορείς, ώστε να μπορούν να λάβουν άμεσα μέτρα για τον έλεγχο εξάπλωσης της μόλυνσης [18].

Η πλειονότητα των εφαρμογών υποστηρίζονταν από τις αγορές των Apple και Google Play και δημιουργήθηκαν στις ομιλούμενες γλώσσες των χωρών καθώς και στα αγγλικά, με τη μόνη εφαρμογή να σπάει τον κανόνα την AarogayaSetu με 12 διαθέσιμες γλώσσες. Ωστόσο, η στρατηγική αυτή διέγειρε τις ανησυχίες σχετικά με την ανωνυμία, το απόρρητο και τη χρήση δεδομένων, κυρίως λόγω της συμμετοχής των εταιρειών Google και Apple, οι οποίες θα μπορούσαν να έχουν πρόσβαση στη βάση δεδομένων, καθώς και η έλλειψη πολιτικής απορρήτου κατά το σχεδιασμό εφαρμογών ανίχνευσης επαφών. Φυσικά, πάντα ελλοχεύει ο κίνδυνος παραγωγής ανακριβών δεδομένων κατά τον εντοπισμό ασθενών COVID-19, ενώ σε ορισμένες περιπτώσεις η χρήση της εφαρμογής μπορεί να καταστεί ενοχλητική. Η συντήρηση αυτών των συστημάτων είναι δύσκολη και απαιτεί εφεδρικά συστήματα σε περίπτωση προβλημάτων επικοινωνίας. Γενικά, είναι απαραίτητη προϋπόθεση τα συστήματα να πληρούν τις κατευθυντήριες γραμμές προστασίας δεδομένων, καθώς και τις απαιτήσεις απορρήτου και εμπιστευτικότητας. Τέλος, οι εφαρμογές εγκαθίστανται έχοντας την αποδοχή του χρήστη, αλλά δεν διασφαλίζουν την πλήρη συμμετοχή του, ούτε την τακτική του χρήση. Επιπλέον, οι εφαρμογές για κινητά βρίσκονται σε μια συνεχή επεξεργασία, σε μια διαρκή εξέλιξη μέσω περιοδικών ενημερώσεων [18].

5.3.1 BeAware App

Οι αρχές του Βασιλείου του Μπαχρέιν ανέπτυξαν την εφαρμογή BeAware τόσο για Android όσο και για iOS, η οποία έχει τη δυνατότητα να παρακολουθεί ασθενείς με COVID-19 χρησιμοποιώντας φορητά ηλεκτρονικά βραχιολάκια, να ειδοποιεί τους αρμόδιους κυβερνητικούς φορείς για οποιαδήποτε ύποπτη δραστηριότητα και να εντοπίζει την κινητικότητά τους μέσω Bluetooth και GPS. Όσον αφορά τα άτομα που βρίσκονται σε απομόνωση συνίσταται ο ορισμός της ακριβής θέσης τους, ενώ στην κατεύθυνση αυτή, το Υπουργείο Υγείας απαιτεί από τους χρήστες την αποστολή φωτογραφιών που δείχνουν το πρόσωπο και το βραχιόλι τους. Επίσης, το κέντρο παρακολούθησης ειδοποιείται εάν ο χρήστης απομακρυνθεί 15 μέτρα από το τηλέφωνό του, ενώ οι παραβάσεις τιμωρούνται με ποινή ή/και φυλάκιση. Τέλος, οι χρήστες πρέπει να φορτίσουν τις συσκευές τους και να βεβαιωθούν ότι η τοποθεσία και η σύνδεση στο διαδίκτυο είναι ενεργοποιημένα [18].

5.3.2 GH COVID-19 Tracker App

Η Γκάνα ανέφερε το πρώτο κρούσμα COVID-19 στις 12 Μαρτίου και ένα μήνα αργότερα τα υπουργεία Επικοινωνιών και Υγείας κυκλοφόρησαν μια εφαρμογή για κινητά Android, iOS και USSD (πρωτόκολλο για το παγκόσμιο σύστημα επικοινωνίας κινητών με χρήση μηνυμάτων κειμένου - Unstructured Supplementary Service Data) για τον εντοπισμό επαφών, γνωστή ως «GH COVID-19 Tracker App». Η εφαρμογή εντοπίζει ύποπτα κρούσματα με διενέργεια τεστ και παρακολούθηση των επαφών με επιβεβαιωμένα θετικά κρούσματα COVID-19. Η εφαρμογή λειτουργεί μέσω του δικτύου κινητής τηλεφωνίας, μπορεί να εντοπίσει τις πρόσφατες τοποθεσίες που επισκέφτηκε το άτομο και να αποστείλει ειδοποιήσεις εάν το άτομο πρέπει να τεθεί σε καραντίνα. Η συλλογή και η διαθεσιμότητα δεδομένων μέσω της εφαρμογής ήταν μια σημαντική βοήθεια στη μάχη της Γκάνα κατά του COVID-19 [18].

5.3.3 Smittestopp

Από το πρώτο κρούσμα COVID-19 που εντοπίστηκε στη Νορβηγία τον Φεβρουάριο του 2020, οι αρχές δημόσιας υγείας παρείχαν συμβουλές για τα ευρέως γνωστά μέτρα ελέγχου λοιμώξεων, όπως η υγιεινή των χεριών, το φτέρνισμα και ο βήχας, η απομόνωση ατόμων με συμπτώματα COVID-19, η αποφυγή περιττών μετακινήσεων, η τηλεργασία και ο εντοπισμός επαφών θετικών κρουσμάτων. Με κατεύθυνση τον περιορισμό μετάδοσης του κορωνοϊού, οι υγειονομικές αρχές ανέπτυξαν την εφαρμογή Smittestopp, η οποία είναι μια εφαρμογή που υποστηρίζεται από τις αγορές της Apple και Google Play. Η εφαρμογή Smittestopp συλλέγει δεδομένα σχετικά με το μοτίβο κινητικότητας των χρηστών και σε περίπτωση που κάποιος από αυτούς έχει έρθει σε στενή επαφή με άλλον χρήστη της εφαρμογής που έχει διαγνωστεί με COVID-19, αναλαμβάνει να παρέχει συμβουλές περιορισμού της μετάδοσης. Διατηρείται η ανωνυμία των χρηστών, ενώ δεδομένα που παραμένουν στη βάση περισσότερο του ενός μήνα διαγράφονται [18].

5.3.4 Virus Radar

Το Υπουργείο Καινοτομίας και Τεχνολογίας της Ουγγαρίας ανακοίνωσε την επίσημη εφαρμογή παρακολούθησης COVID-19 που ονομάζεται «VirusRadar» στις 13 Μαΐου 2020. Αναπτύχθηκε από την Nextsense, η εφαρμογή αξιοποίησε την τεχνολογία ανίχνευσης επαφών της εταιρείας και δωρίθηκε στις αρχές ως στήριξη στην αντιμετώπιση του COVID-19. Λειτουργεί για κινητά Apple iOS και Android και εφαρμόζει τα υψηλότερα πρότυπα ασφαλείας, παρέχει πλήρη έλεγχο των προσωπικών δεδομένων και εγγυάται την προστασία του απορρήτου. Η εφαρμογή χρησιμοποιεί τεχνολογία Bluetooth Low Energy και ανταλλάσσει κρυπτογραφημένα, ανώνυμα δεδομένα με άλλους χρήστες αυτής, μετρώντας την απόσταση μεταξύ των τηλεφώνων. Εάν ένα άτομο έχει μολυνθεί, ο χρήστης της εφαρμογής θα κληθεί να μοιραστεί τις πληροφορίες με τις υγειονομικές αρχές. Τα δεδομένα που συλλέγονται μέσω της συσκευής αποθηκεύονται για 2 εβδομάδες σε έναν ασφαλή διακομιστή υπό την διαχείριση των υγειονομικών αρχών, δίχως να καταγράφεται η τοποθεσία ή άλλα προσωπικές πληροφορίες [18].

5.3.5 HAMAGEN

Αποτελεί μια εφαρμογή ανίχνευσης επαφών που αναπτύχθηκε από το Υπουργείο Υγείας του Ισραήλ, κυκλοφόρησε στις 22 Μαρτίου 2020 και ονομάζεται «HAMAGEN» και λειτουργεί τόσο σε συσκευές Android και iOS. Χρησιμοποιεί την εύρεση τοποθεσίας μέσω GPS της συσκευής για να ειδοποιεί τον χρήστη εάν τυχαίνει να διασταυρωθεί με θετικό κρούσμα COVID-19, ενημερώνοντας τον για την ακριβή ώρα και τοποθεσία συνάντησης. Στη συνέχεια, ο χρήστης μπορεί να ελέγξει, να επιβεβαιώσει ή να απορρίψει την ειδοποίηση με μη αυτοματοποιημένο τρόπο. Το ιστορικό τοποθεσίας GPS διασταυρώνεται με τα επιδημιολογικά δεδομένα του Υπουργείου Υγείας και αποθηκεύεται μόνο στο τηλέφωνο του χρήστη δίχως να δίνεται πρόσβαση σε τρίτους. Το σύστημα ελέγχου της εφαρμογής είναι ανοιχτό και παρέχει τον απόλυτο έλεγχο στον χρήστη [18].

5.3.6 Rakning C-19

Το Rakning C-19 κυκλοφόρησε στις αρχές Απριλίου στην Ισλανδία με σκοπό την παρακολούθηση των δεδομένων GPS των χρηστών, τη συλλογή πληροφοριών σχετικά με τις συναντήσεις τους και τον εντοπισμό εκτεθειμένων ατόμων στον ιό. Η εφαρμογή λειτουργεί τόσο σε συσκευές Android και iOS και έχει σχεδόν 40% αποδοχή από τους πολίτες, διαθέτει το πιο σημαντικό ποσοστό διείσδυσης από όλα τα προγράμματα παρακολούθησης επαφών παγκοσμίως. Με την ολοκλήρωση της εγκατάστασης, η εφαρμογή εκτελείται στο παρασκήνιο, αποθηκεύοντας τη θέση της συσκευής πολλές φορές σε μια ώρα. Γενικότερα, τα δεδομένα αποθηκεύονται αποκλειστικά στο τηλέφωνο για 2 εβδομάδες και είναι προσβάσιμα μόνο από τον χρήστη, για να διαγραφούν στη συνέχεια [18].

5.3.7 COVID Symptom Tracker

Η εφαρμογή παρακολούθησης συμπτωμάτων του Ηνωμένου Βασιλείου που ονομάζεται C-19 COVID Symptom Tracker, αναπτύχθηκε από την εταιρεία Zoe με τη συμβολή του King's College του Λονδίνου και του Γενικού Νοσοκομείου της Μασαχουσέτης. ενώ παρέχεται δωρεάν. Έγινε ιδιαίτερα αποδεκτή από το κοινό, έχοντας 2.979.018 συμμετέχοντες έως τις 6 Μαΐου 2020. Η εφαρμογή αποδείχτηκε ιδιαίτερα χρήσιμη καθώς βοήθησε στον εντοπισμό ενός στους δέκα ανθρώπους που εμφάνιζαν συμπτώματα κορωνοϊού. Σκοπός της εφαρμογής ήταν η καλύτερη κατανόηση των συμπτωμάτων του Covid-19, ο προσδιορισμός περιοχών υψηλού κινδύνου στη χώρα και η αναγνώριση των ευάλωτων ατόμων βάσει των συμπτωμάτων και της κατάστασης της υγείας τους [31].

5.4 Συγκριτική ανάλυση εφαρμογών κατά του Covid-19

Με σκοπό την διατήρηση κοινών κριτηρίων μεταξύ των διαφόρων μελετών, συνεχίζουμε την ανάλυση εφαρμογών που διατίθενται δωρεάν τόσο σε συσκευές Android όσο και iOS. Η μόνη εφαρμογή που είναι διαθέσιμη για καθολική χρήση σε παγκόσμια κλίμακα είναι το COVID Symptom Tracker, επιτρέποντας στους χρήστες να αναφέρουν τυχόν συμπτώματα σε καθημερινή βάση. Οι χρήστες οφείλουν να καταχωρήσουν τα προσωπικά τους στοιχεία όπως ηλικία, φύλο, ύψος, βάρος και ταχυδρομικό κώδικα, ενώ οι υγειονομικές αρχές μπορούν να επεξεργαστούν τις πληροφορίες αυτές. Με βάση τα αποτελέσματα της αξιολόγησης των βασικών χαρακτηριστικών, το COVID Symptom Tracker απαιτεί σύνδεση στο διαδίκτυο για την ομαλή λειτουργία της εφαρμογής αλλά δεν περιλαμβάνει εκπαιδευτικό υλικό. Επίσης, στην αξιολόγηση λειτουργικότητας, η εφαρμογή συγκέντρωσε 3 στα 5, λόγω της έλλειψης αρκετών λειτουργιών, συμπεριλαμβανομένων των υπηρεσιών ιατρικής παρακολούθησης στο σπίτι και ιατρικής συμβουλευτικής με κάποιο επαγγελματία υγείας.

Η εφαρμογή COVA Punjab σημείωσε τη δεύτερη υψηλότερη βαθμολογία στην αξιολόγηση βασικών χαρακτηριστικών, με τη χρήση του Διαδικτύου να αποτελεί έναν σταθερό περιοριστικό παράγοντα ομαλής λειτουργίας. Γενικά, οι περισσότερες από τις εφαρμογές mHealth στο Apple App Store και στο Google Play Store καταστούν απαιτητή προϋπόθεση τη σύνδεση στο Διαδίκτυο, καθώς σημαντικό κανόνα για την κοινότητα προγραμματιστών αποτελεί ο συγχρονισμός δεδομένων σε πραγματικό χρόνο με την εφαρμογή με στόχο την αποτροπή παρουσίασης ξεπερασμένων πληροφοριών. Ωστόσο, ο αξιολογητής της έρευνας δεν κατάφερε να έχει πρόσβαση στην εφαρμογή, λόγω του ότι για την εγγραφή χρήστη απαιτείται η καταχώρηση ενός τοπικού αριθμού τηλεφώνου. Επομένως, δεν υπάρχουν σχετικές πληροφορίες διάθεσης εκπαιδευτικών πόρων για τον ιό από την εν λόγω εφαρμογή. Όσον αφορά την αξιολόγηση λειτουργικότητας, τόσο το COVA Punjab όσο και το TraceTogether σημείωσαν βαθμολογία 4 στα 5, με το TraceTogether να μην διαθέτει δυνατότητα ιατρικής παρακολούθησης από το σπίτι και εκπαιδευτικό περιεχόμενο, ενώ για το COVA Punjab δεν υπάρχουν διαθέσιμες πληροφορίες για τα

συγκεκριμένα χαρακτηριστικά. Ωστόσο, το TraceTogether σημείωσε υψηλότερη (5/5) αξιολόγηση από το COVA Punjab (4/5) όσον αφορά τα βασικά χαρακτηριστικά τους [22].

Το TraceTogether παρουσιάζει την υψηλότερη βαθμολογία στην αξιολόγηση βασικών χαρακτηριστικών, αλλά διαθέτει επίσης την υψηλότερη βαθμολογία στην αξιολόγηση λειτουργικότητας τόσο στο App Store όσο και στο Play Store. Χρησιμοποιείται κυρίως για τον εντοπισμό επαφών κρουσμάτων COVID-19 στη Σιγκαπούρη και επιτρέπει την έγκαιρη ενημέρωση των χρηστών όσον αφορά την επαφή τους με κάποιο θετικό κρούσμα COVID-19. Έτσι, εάν υπάρχει υποψία ότι ένας χρήστης έχει μολυνθεί με COVID-19, τα δεδομένα του συλλέγονται από την υγειονομική αρχή με στόχο τον εντοπισμό επαφών, επιτρέπουν μόνο στους ίδιους να αλληλεπιδρούν και να μεταφορτώνουν σχετικά αρχεία, όπως εικόνες και έγγραφα. Επίσης, το TraceTogether παρέχει πληροφορίες αναφορικά με τις διαθέσιμες λειτουργίες σε κάθε νέο χρήστη που επισκέπτεται για πρώτη φορά την εφαρμογή.

Από την άλλη μεριά υπάρχει επίσης ένας αριθμός εφαρμογών που σημείωσαν χαμηλή βαθμολογία στην αξιολόγηση λειτουργιών, αλλά η υλοποίησή τους δεν περιλάμβανε και τα δύο λειτουργικά συστήματα. Έτσι, το CoronaChecker αναγνωρίστηκε ως εφαρμογή χαμηλής αξιολόγησης με βαθμολογία 0 στα 5 στο Apple App Store, καθώς ο βασικός της προορισμός είναι η παροχή προτάσεων σχετικά με την αναγκαιότητα διενέργειας τεστ COVID-19 από τον εκάστοτε χρήστη. Αξιοποιώντας την τεχνολογία της τεχνητής νοημοσύνης, ξεκινά μια συνομιλία με τον χρήστη, αναπτύσσοντας μια αλληλεπίδραση μέσω κλειστών ερωτήσεων για την αναγνώριση τυχόν κλινικών συμπτωμάτων. Παρά τη χαμηλή αξιολόγηση λειτουργικότητας που συγκέντρωσε, βαθμολογήθηκε με 5 στα 5 από 298 χρήστες, φανερώνοντας ότι οι χρήστες έμειναν απόλυτα ικανοποιημένοι από τη λειτουργική απόδοση της εφαρμογής, καθώς ο σχεδιασμός του στόχευε στην επιβεβαίωση της κατάστασης υγείας του χρήστη και όχι τη χρήση του ως εκπαιδευτικό εργαλείο αναφορικά με τον COVID-19 [22].

Κριτήρια αξιολόγησης των εφαρμογών

Για την αξιολόγηση των εφαρμογών συμπεριλήφθηκαν τα επτά βασικά χαρακτηριστικά που συνοψίζονται στα παρακάτω:

(1) μη απαίτηση σύνδεσης στο διαδίκτυο
(2) μέγεθος εγκατάστασης εφαρμογής μικρότερο από 50 MB
(3) μη απαίτηση συνδρομής (δηλαδή δωρεάν)
(4) παροχή εκπαιδευτικού περιεχομένου (αναφορικά με τον COVID-19)
(5) υποστήριξη εξαγωγής δεδομένων (κοινή χρήση δεδομένων χρήστη με άλλες πλατφόρμες)
(6) αυτοματοποιημένη εισαγωγή και ενημέρωση δεδομένων (χωρίς παρέμβαση χρήστη) και
(7) συμβουλευτική υποστήριξη [22].

Επιπλέον, πραγματοποιείται αξιολόγηση με βάση τις πέντε κατηγορίες λειτουργιών των εφαρμογών όπως παρουσιάζονται παρακάτω:

(1) παροχή πληροφοριών για τον COVID-19
(2) ανίχνευση ή χαρτογράφηση περιπτώσεων με COVID-19
(3) επιτήρηση και έλεγχος του κατ' οίκον περιορισμού
(4) διαδικτυακή συμβουλευτική με τις υγειονομικές αρχές και
(5) επίσημη έκδοση εφαρμογής για κινητές συσκευές υπό την διαχείριση υγειονομικού φορέα.

No	Name of mobile apps	No internet requirement	Size of app <50 MB	No subscription requirement (ie, free)	Educational content	Export data	Automated data entry	Advisory	Total score
Universal COVID-19[a] apps									
1	COVID Symptom Tracker	N/A[b]	✓	✓	N/A	✓	✓	✓	5
Country-specific apps									
2	BC COVID-19	N/A	✓	✓	✓	N/A	✓	✓	5
3	Canada COVID-19	N/A	✓	✓	✓	N/A	✓	✓	5
4	Coronavirus Australia	N/A	✓	✓	✓	✓	N/A	✓	5
5	COVA[c] Punjab	N/A	✓	N/A	—[d]	✓	✓	✓	4
6	HSE[e] COVID-19	N/A	✓	N/A	N/A	✓	✓	N/A	3
7	NCOVI	—	✓	✓	✓	—	—	✓	4
8	TraceTogether	N/A	✓	✓	N/A	✓	✓	✓	5
9	자가격리자 안전보호 (Self-Isolator Safety & Protection)	—	✓	✓	✓	—	—	✓	4
10	자가격리자 전담공무원 (Self-isolating Government Officials)	—	✓	✓	✓	—	—	✓	4

Πίνακας 5.4: Αξιολόγηση βασικών χαρακτηριστικών των εφαρμογών κατά του Covid (iOS και Android) (Πηγή: [22])

No	Name of mobile apps	Knowledge	Tracing/mapping of COVID-19[a] cases	Home monitoring surveillance	Online consultation with health authority	Official mobile app maintained by health authority	Total score
Universal COVID-19 apps							
1	COVID Symptom Tracker	✓	✓	N/A[b]	N/A	✓	3
Country-specific apps							
2	BC COVID-19	✓	N/A	N/A	N/A	✓	2
3	Canada COVID-19	✓	✓	N/A	N/A	✓	3
4	Coronavirus Australia	✓	✓	N/A	N/A	✓	3
5	COVA[c] Punjab	✓	✓	—[d]	✓	✓	4
6	HSE[e] COVID-19	✓	N/A	✓	N/A	✓	3
7	NCOVI	✓	✓	—	—	✓	3
8	TraceTogether	✓	✓	N/A	✓	✓	4
9	자가격리자 안전보호 (Self-Isolator Safety & Protection)	✓	—	✓	—	✓	3
10	자가격리자 전담공무원 (Self-isolating Government Officials)	✓	—	✓	—	✓	3

Πίνακας 5.5: Αξιολόγηση λειτουργιών των εφαρμογών κατά του Covid-19 (iOS και Android) (Πηγή: [22])

5.5 Πορίσματα και τελική αξιολόγηση εφαρμογών κατά του Covid-19

Έχοντας προβεί στην ανάλυση αρκετών εφαρμογών από διάφορες έρευνες επιστημόνων και με την κριτική ματιά των συγγραφέων αυτής της πτυχιακής εργασίας συμπεραίνουμε ότι κάθε εφαρμογή έχει έναν συγκεκριμένο στόχο και ένα κοινό στο οποίο απευθύνεται. Έπειτα από λεπτομερή αξιολόγηση των διαθέσιμων εφαρμογών παρατηρήθηκε ότι λίγες εφαρμογές μπορούν να εφαρμοστούν σε παγκόσμια κλίμακα για εκπαίδευση και αυτοαξιολόγηση σχετικά με τον COVID-19. Μία από αυτές τις εφαρμογές έξυπνων κινητών και η μοναδική με λειτουργικότητα παγκόσμιας εμβέλειας είναι το COVID Symptom Tracker, που υποστηρίζεται τόσο σε συσκευές Apple όσο και Android. Βέβαια, στην αξιολόγηση λειτουργικότητας βρίσκεται στη μέση της βαθμολογίας (3 στα 5) φανερώνοντας κάποιες αδυναμίες που αφορούσαν το εύρος των υπηρεσιών που παρείχε.

Η εφαρμογή που διασφαλίζει με ακεραιότητα το απόρρητο των χρηστών είναι η TraceTogether της Σινγκαπούρης, η οποία ταυτόχρονα συμπεριλαμβάνει τις πιο κοινές λειτουργίες, όπως αξιολόγηση κατάστασης κινδύνου, παρουσίαση αναφορών αναφορικά με τα τεστ, ανίχνευση επαφών και αποστολή σχετικών ειδοποιήσεων. Αξιοποιεί τον υβριδικό τρόπο γεωγραφικού εντοπισμού, συνδυάζοντας GPS και Bluetooth Low Energy, αποθηκεύοντας τις πληροφορίες στη συσκευή για 21 ημέρες, ενώ οι χρήστες διατηρούν το δικαίωμα να διαγράψουν τα δεδομένα ανά πάσα στιγμή. Με βαθμολογία 4 στα 5 στην

αξιολόγηση λειτουργικότητας φαίνεται ότι η εφαρμογή καλύπτει ένα μεγάλο φάσμα λειτουργιών, ενώ συγκεντρώνει την υψηλότερη βαθμολογία στην αξιολόγηση χρηστών τόσο σε συσκευές Android όσο και iOS.

Η εφαρμογή AarogayaSetu από την Ινδία αποτελεί την πληρέστερη υλοποίηση βάσει του συνόλου εργαλείων αξιολόγησης (υγείας, εκπαίδευσης, επικοινωνίας, δικτύωσης και ασφάλειας), με πολυγλωσσική δυνατότητα 12 διαθέσιμων γλωσσών και τις υψηλότερες αξιολογήσεις από τους χρήστες τόσο σε Android όσο και iOS. Από τις παρεχόμενες υπηρεσίες εξαιρούνται η ενσωμάτωση των κοινωνικών δικτύων και η κράτηση ραντεβού, ενώ όσον αφορά την προστασία του απορρήτου παρουσιάζει χαμηλό επίπεδο κινδύνου που στην ουσία δεν ανταποκρίνεται στην πραγματικότητα καθώς η χώρα στερείται στιβαρής νομοθεσίας και πολιτικής ασφάλειας προσωπικών δεδομένων.

Επίσης, η εφαρμογή GH COVID-19 Tracker της Γκάνας ήταν η μόνη που υποστήριζε κινητά USSD, δηλαδή το πρωτόκολλο επικοινωνίας με χρήση μηνυμάτων κειμένου, με στόχο να καλύψει υψηλότερο ποσοστό του πληθυσμού και να επιτύχει αποτελεσματικότερη ανίχνευση επαφών. Συνολικά από τις 19 εφαρμογές, οι 15 διέθεταν τη λειτουργία ανίχνευσης επαφών, γεγονός που καταδεικνύει τη σπουδαιότητά της στην μείωση της εξάπλωσης του ιού.

Γενικότερα, προτείνεται η χρήση εφαρμογών που υλοποιούνται κάτω από την αιγίδα των υγειονομικών αρχών της εκάστοτε χώρας, καθώς έτσι αποφεύγεται η διάδοση παραπλανητικών πληροφοριών στο ευρύ κοινό, ενώ παράλληλα αυξάνεται η αξιοπιστία των εφαρμογών και η διασφάλιση της ιδιωτικότητας των χρηστών. Για την καταπολέμηση της παραπληροφόρησης σχετικά με την πανδημία, πολλοί οργανισμοί, συμπεριλαμβανομένων των δύο κολοσσών ανάπτυξης εφαρμογών για κινητά - Apple και Google - κατέβαλαν σημαντικές προσπάθειες συμμετοχής στην υλοποίησή τους, γεγονός που παράλληλα γέννησε και αρκετές ανησυχίες που αφορούσαν την προστασία του απορρήτου. Επιπλέον, με στόχο την αύξηση του ποσοστού δέσμευσης των πολιτών με αυτές τις εφαρμογές, θα πρέπει να παρέχονται βασικές πληροφορίες για τον COVID-19, οδηγίες και προληπτικά μέτρα, υποστηρίζοντας ένα ευρύτερο φάσμα υπηρεσιών και όχι απλά μια εστιασμένη λειτουργία που σχετίζεται με τον COVID-19 (π.χ. λειτουργία αξιολόγησης συμπτωμάτων). Φυσικά, προτείνεται οι εφαρμογές αυτές να διατίθενται δωρεάν τόσο στο Apple App Store όσο και στο Google Play Store, έτσι ώστε να καταστούν εύκολα προσβάσιμες από το σύνολο των δυνητικών χρηστών. Έχει διαπιστωθεί ότι η κατάταξη των εφαρμογών σε κατάλληλες κατηγορίες πλαισιώνει τα κριτήρια επιλογής του χρήστη σχετικά με το ποια εφαρμογή αρμόζει καλύτερα στις ανάγκες του, ενώ ταυτόχρονα βελτιώνει το βαθμό χρήσης και δέσμευσης προς την εφαρμογή [22].

Οι εφαρμογές θα έπρεπε να είναι διαθέσιμες για καθολική χρήση και όχι μόνο για τους κατοίκους μιας συγκεκριμένης χώρας, γεγονός που σε πολλές περιπτώσεις οφείλεται στην αυστηρή διαδικασία επαλήθευσης, που εκτελείται με δήλωση ενός τοπικού αριθμού κινητού τηλεφώνου, αλλά και στην

έλλειψη ενοποιημένης πολιτικής προστασίας απορρήτου και προσωπικών δεδομένων σε ηπειρωτικό ή/και παγκόσμιο επίπεδο. Η ύπαρξη μηδαμινού, χαλαρού ή αυστηρού πλαισίου για την προστασία της ιδιωτικότητας και η διασφάλιση των προσωπικών δεδομένων των χρηστών αποτελεί κομβικό κομμάτι για την αξιολόγηση των εφαρμογών, καθώς θα πρέπει να τηρούνται υψηλά πρότυπα ασφαλείας, προστατεύοντας την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών [22].

Βασική προϋπόθεση για την έγκυρη ενημέρωση του κοινού είναι ο συγχρονισμός των δεδομένων σε πραγματικό χρόνο, πλαίσιο που συμπεριλαμβάνει τις στατιστικές αναλύσεις γεωγραφικού εντοπισμού των κρουσμάτων Covid-19, των ασθενών που ανάρρωσαν αλλά και αυτών που απεβίωσαν, με κατεύθυνση την άμεση ενημέρωση αναφορικά με την πανδημία σε παγκόσμιο επίπεδο. Επίσης, η προσθήκη άλλων προηγμένων λειτουργιών θα βελτιώσει σημαντικά την ποιότητα και την πληρότητα μιας εφαρμογής, όπως η λειτουργία ειδοποιήσεων αναφορικά με περιοχές κοινωνικού συγχρωτισμού υψηλής επικινδυνότητας, η παρακολούθηση της κατάστασης των ατόμων που βρίσκονται σε καραντίνα, η διαδικτυακή διαβούλευση με επαγγελματίες υγείας, η ανίχνευση επαφών με μολυσμένους χρήστες της εφαρμογής και η αποστολή ειδοποιήσεων διενέργειας τεστ νόσησης για COVID-19. Με στόχο την επιβράδυνση της επιδημίας του ιού, ένας ανιχνευτής συμπτωμάτων είναι χρήσιμος για την ανίχνευση περιοχών υψηλής επικινδυνότητας, την ταχύτητα μετάδοσης του ιού ανά περιοχή και την αναγνώριση ατόμων που παρουσιάζουν τον υψηλότερο κίνδυνο αναφορικά με τις βιομετρικές μετρήσεις της κατάστασης υγείας τους [22].

Όσον αφορά τις μεθόδους ανίχνευσης επαφών, ο εντοπισμός μέσω Bluetooth είναι μακράν ο πιο δημοφιλής τρόπος, διασφαλίζοντας την αποτελεσματικότητα της εφαρμογής μέσω της τεχνολογίας Bluetooth Low Energy που διακρίνεται για τη χαμηλή κατανάλωση ενέργειας. Διασφαλίζει τη προστασία του απορρήτου, καθώς εντοπίζει τη σχετική θέση του χρήστη, ωστόσο, μπορεί να παρουσιάσει ορισμένα σφάλματα στην εκτίμηση των αποστάσεων μεταξύ των συσκευών κυρίως σε εσωτερικούς χώρους, όπου υπάρχουν φυσικά εμπόδια και αντανακλάσεις σημάτων. Γενικότερα, προτείνεται η υβριδική χρήση μεθόδων ανίχνευσης επαφών, καθώς ο γεωεντοπισμός θέσης μέσω GPS χαρακτηρίζεται από υψηλή κατανάλωση ενέργειας και ανακρίβεια αποτελεσμάτων σε εσωτερικούς χώρους, ενώ ο συνδυασμός GPS με τη χρήση Wi-Fi (APs) ή ακουστικής εμβέλειας ή iBeacons ή αισθητήρες SensTrack, μπορεί να βελτιώσει την απόδοση της εν λόγω λειτουργίας.

Καθώς η τεχνολογία αναβαθμίζεται, ο αλγόριθμος εντοπισμού συμπτωμάτων μπορεί να βελτιωθεί και να προσαρμοστεί, βελτιώνοντας τη διαγνωστική του ακρίβεια. Επίσης, οι φορητές συσκευές όπως τα έξυπνα ρολόγια και οι έξυπνες ζώνες θα γίνουν ακόμα πιο συνηθισμένες και θα ενσωματωθούν στην καθημερινή μας ζωή, εδραιώνοντας μια προσέγγιση που φέρει τη δυναμική να βοηθήσει στη ζωτική παρακολούθηση της υγείας των ευάλωτων πληθυσμών. Η ολοκληρωμένη εφαρμογή που αναπτύσσεται αυτήν τη στιγμή από την Apple και την Google μπορεί να βοηθήσει στον περιορισμό της εξάπλωσης του ιού σε παγκόσμια

κλίμακα, προσφέροντας μια μοναδική ευκαιρία προετοιμασίας για παρόμοιες μελλοντικές επιδημιολογικές κρίσεις. Η ενσωμάτωση μεθόδων μηχανικής μάθησης και τεχνητής νοημοσύνης, θα βελτιώσει την ακρίβεια και ταχύτητα της διαδικασίας ανίχνευσης και αναγνώρισης ύποπτων λοιμώξεων. Οι ενοποιημένες πληροφορίες που παρέχονται από αξιόπιστους οργανισμούς, όπως ο ΠΟΥ, θα μπορέσουν να αποφύγουν κάθε περιττή σύγχυση όσον αφορά τις οδηγίες και τις συμβουλές που επικοινωνούνται σε μια κατάσταση πανδημίας. Η προσαρμογή των πληροφοριών αυτών, στη συνέχεια, επίκειται στην αρμοδιότητα των εκάστοτε κυβερνήσεων ώστε να ταιριάζουν με την πολιτισμική κουλτούρα της χώρας [31].

Δύο μόνο εφαρμογές (Tawakkalna, Aarogya Setu) από τις 19 που μελετήθηκαν παρείχαν υπηρεσίες e-pass ή ταξιδιωτικών αδειών κατά τη διάρκεια της επιδημίας COVID-19, που κατά κάποιο τρόπο ομοιάζουν με το Covid Free App που κυκλοφόρησε στην Ελλάδα για τον έλεγχο των πιστοποιητικών εμβολιασμού ή νόσησης, τα οποία υποχρεούνται να επιδεικνύουν οι πολίτες προκειμένου να εισέλθουν σε εστιατόρια, καταστήματα, σινεμά κ.ά. Στην χώρα μας δεν εντοπίσαμε κάποια εφαρμογή που να τέθηκε σε λειτουργία, όπως αυτές που αναλύθηκαν στη συγκριτική ανάλυση εφαρμογών κατά του Covid-19.

Κεφάλαιο 6ο: Συμπεράσματα

Το πρωταρχικό συμπέρασμα που αναδύθηκε από την παρούσα πτυχιακή εργασία είναι ότι εφαρμογές eHealth για κινητές συσκευές με σκοπό την παρακολούθηση συμπτωμάτων, την παροχή έγκυρων και έγκαιρων πληροφοριών, την αυτοαξιολόγηση νόσησης, τον εντοπισμό και την ανίχνευση επαφών μπορούν πλέον να υλοποιηθούν και να τεθούν σε εφαρμογή σε σύντομο χρονικό διάστημα, αποδεικνύοντας τα άμεσα αντανακλαστικά των επιστημόνων του τεχνολογικού κλάδου. Εφαρμογές που μπορούν να παρέχουν πολύτιμες πληροφορίες σε κυβερνήσεις, υγειονομικούς φορείς και ιδιώτες όσον αφορά τον έλεγχο, την παρακολούθηση, την εκπαίδευση, τη διάγνωση, τη πρόβλεψη, τη λήψη αποφάσεων και ανάλυση των δεδομένων που προκύπτουν από το εύρος όλου αυτού του φάσματος που σχετίζεται με τον Covid-19, αλλά μπορούν να φανούν εξίσου χρήσιμες σε οποιαδήποτε άλλη μελλοντική επιδημία.

Εφαρμογές, όπως αυτές που παρουσιάζονται στην εργασία, μπορούν να δώσουν στην ερευνητική κοινότητα την ευκαιρία να παρακολουθεί τις μακροπρόθεσμες επιπτώσεις του COVID-19, απαντώντας σε ερωτήσεις όπως ο αριθμός των ανθρώπων που έχουν μολυνθεί πραγματικά, την αιτία που μερικοί άνθρωποι αρρωσταίνουν βαρύτερα από άλλους, το διάστημα που μπορεί ένα άτομο να διατηρεί ανοσία στην ασθένεια και τον βέλτιστο τρόπο κατανομής των πόρων ιατρικού εξοπλισμού. Ωστόσο, υπάρχουν ακόμα αρκετά σημεία που χρήζουν περαιτέρω διερεύνησης, όπως η ακριβέστερη ανίχνευση γεωγραφικής θέσης, η έγκαιρη ενημέρωση πληροφοριών, η ανάπτυξη εφαρμογών για συσκευές που δεν εντάσσονται στα έξυπνα κινητά, η βελτιωμένη οπτικοποίηση δεδομένων, η πρόβλεψη περιστατικών Covid-19 καθώς και η υψηλότερης κλίμακας ενσωμάτωση της ψηφιακής υγείας από όλα τα ενδιαφερόμενα μέλη [19].

Οι έρευνες θα πρέπει να κατευθυνθούν στον επανασχεδιασμό των μοντέλων Blockchain προκειμένου να καταστούν περισσότερο κατάλληλα για τα συστήματα IoT. Πιο συγκεκριμένα, θα μπορούσαν να αναπτυχθούν νέες αρχιτεκτονικές blockchain και σύγχρονοι αλγόριθμοι συναίνεσης ειδικά προσανατολισμένοι στις απαιτήσεις των συσκευών IoT. Αυτό σημαίνει ότι θα δοθεί προτεραιότητα σε καινοτομίες που θα ελαχιστοποιήσουν την κατανάλωση ενέργειας, καθώς για την επίλυση των πολύπλοκων μαθηματικών υπολογισμών του μηχανισμού απόδειξης εργασίας των συναλλαγών απαιτείται σημαντική ποσότητα ενέργειας για την τροφοδοσία του συστήματος blockchain. Βέβαια, το blockchain είναι μια ταχέως αναπτυσσόμενη τεχνολογία που η υλοποίησή της προϋποθέτει υψηλό προϋπολογισμό κεφαλαίου, γεγονός που καθιστά δύσκολη την συχνή ανανέωση των τεχνολογικών πόρων, αλλά και βαρύτερο το περιβαλλοντικό αποτύπωμα όταν καθίσταται απαραίτητη η αντικατάστασή τους. Όπως προκύπτει από το παραπάνω, η επεκτασιμότητα του συστήματος εξαρτάται από την εφαρμοζόμενη πολυπλοκότητά του, αφού η επικύρωση της εκάστοτε συναλλαγής πρέπει να διενεργηθεί από την πλειονότητα των κόμβων (nodes) [6], [38].

Εκτός από το IoT και το Blockchain, μπορούν να δημιουργηθούν συστήματα που αξιοποιούν επίσης τα πλεονεκτήματα της τεχνητής νοημοσύνης, των δεδομένων μεγάλου εύρους (big data), του fog και cloud computing. Με τη βοήθεια της τεχνητής νοημοσύνης θα μπορούσε να βελτιωθεί ο αλγόριθμος εντοπισμού συμπτωμάτων, αυξάνοντας τη διαγνωστική του ακρίβεια. Επίσης, θα μπορούσε να δημιουργηθεί ένα σύστημα υγειονομικής περίθαλψης που χρησιμοποιεί συσκευές IoT για τη συλλογή ιατρικών δεδομένων, όπου οι πληροφορίες θα φιλτράρονταν στο fog computing πριν υποβληθούν σε επεξεργασία στο αντίστοιχο cloud. Ο τεράστιος όγκος δεδομένων θα αναλυόταν με τη βοήθεια τεχνητής νοημοσύνης και φυσικά, η επικοινωνία και ο έλεγχος πρόσβασης θα διατηρούνταν με χρήση της τεχνολογίας Blockchain. Με αυτή τη συγχώνευση τεχνολογιών, θα μπορούσε να αναπτυχθεί ένα πλήρες σύστημα υγείας που ενσωματώνει τις πιο πρόσφατες τεχνολογικές καινοτομίες. Επιπροσθέτως, πρέπει να καθοριστούν ρυθμιστικοί κανόνες και νομικές κατευθύνσεις που διασφαλίζουν τη χρήση του Blockchain στον τομέα της υγειονομικής περίθαλψης, γεγονός που θα ωθήσει σε μια υψηλότερου επιπέδου σύγκλιση τεχνολογιών και ως εκ τούτου στη θετική επίδρασή τους στον κλάδο της υγείας. Γεγονός που απαιτεί μεγάλη προσοχή στη γενίκευση της χρηστικότητας των εφαρμογών και την διευθέτηση των ανησυχιών που συνδέονται με την ανωνυμία δεδομένων, το απόρρητο, τη χρήση και τα δικαιώματα κτήσης τους [6].

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Alanzi, T. (2021). A review of mobile applications available in the app and google play stores used during the COVID-19 outbreak. *Journal of multidisciplinary healthcare*, *14*, 45.

[2] Alexander, A., McGill, M., Tarasova, A., Ferreira, C., & Zurkiya, D. (2019). Scanning the future of medical imaging. *Journal of the American College of Radiology*, *16*(4), 501-507.

[3] Aman, A. H. M., Hassan, W. H., Sameen, S., Attarbashi, Z. S., Alizadeh, M., & Latiff, L. A. (2021). IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. *Journal of Network and Computer Applications*, *174*, 102886.

[4] Aslam, B., Javed, A. R., Chakraborty, C., Nebhen, J., Raqib, S., & Rizwan, M. (2021). Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic. *Personal and ubiquitous computing*, 1-17.

[5] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. *In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.*

[6] Azbeg, K., Ouchetto, O., Andaloussi, S. J., & Fetjah, L. (2021). A taxonomic review of the use of IoT and blockchain in healthcare applications. *Irbm*.

[7] Baran, P. (1964). On distributed communications networks. *IEEE transactions on Communications Systems*, *12*(1), 1-9.

[8] Bassi, A., Bauer, M., Fiedler, M., Kramp, T., Van Kranenburg, R., Lange, S., & Meissner, S. (2013). *Enabling things to talk* (p. 379). Springer Nature.

[9] Bragazzi, N. L., Dai, H., Damiani, G., Behzadifar, M., Martini, M., & Wu, J. (2020). How big data and artificial intelligence can help better manage the COVID-19 pandemic. *International journal of environmental research and public health*, *17*(9), 3176.

[10] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*, *3*(37).

[11] Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. Ieee access, 8, 90225-90265.

[12] Chawathe, S. S. (2018, November). Indoor Localization Using Bluetooth-LE Beacons. In *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 262-268). IEEE.

[13] Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things-promise for the future? An introduction. In *2011 IST-Africa Conference Proceedings* (pp. 1-9). IEEE.

[14] De Filippi, P., & Hassan, S. (2018). Blockchain technology as a regulatory technology: From code is law to law is code. *arXiv preprint arXiv:1801.02507*.

[15] Ferrag, M. A., Maglaras, L., & Janicke, H. (2019). Blockchain and its role in the internet of things. In Strategic Innovative Marketing and Tourism (pp. 1029-1038). Springer, Cham.

[16] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). *Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems, 42(7), 1-7.*

[17] Haber, S., & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer, Berlin, Heidelberg.

[18] Jalabneh, R., Syed, H. Z., Pillai, S., Apu, E. H., Hussein, M. R., Kabir, R., ... & Saxena, S. K. (2021). Use of mobile phone apps for contact tracing to control the COVID-19 pandemic: A literature review. *Applications of Artificial Intelligence in COVID-19*, 389-404.

[19] Kondylakis, H., Katehakis, D. G., Kouroubali, A., Logothetidis, F., Triantafyllidis, A., Kalamaras, I., ... & Tzovaras, D. (2020). COVID-19 mobile apps: a systematic review of the literature. *Journal of medical Internet research*, *22*(12), e23170.

[20] Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: a survey. *Information systems frontiers*, *17*(2), 243-259.

[21] McBee, M. P., & Wilcox, C. (2020). Blockchain technology: principles and applications in medical imaging. *Journal of digital imaging*, *33*(3), 726-734.

[22] Ming, L. C., Untong, N., Aliudin, N. A., Osili, N., Kifli, N., Tan, C. S., ... & Goh, H. P. (2020). Mobile health apps on COVID-19 launched in the early days of the pandemic: content analysis and review. *JMIR mHealth and uHealth*, *8*(9), e19796.

[23] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

[24] Ng, J. K. Y., Lam, K. Y., Cheng, Q. J., & Shum, K. C. Y. (2013). An effective signal strength-based wireless location estimation system for tracking indoor mobile users. *Journal of Computer and System Sciences*, *79*(7), 1005-1016.

[25] Pradhan, B., Bhattacharyya, S., & Pal, K. (2021). IoT-Based Applications in Healthcare Devices. *Journal of Healthcare Engineering*, *2021*.

[26] Quintais, J. P., Bodo, B., Giannopoulou, A., & Ferrari, V. (2019). Blockchain and the law: A critical evaluation.

[27] Schoder, D. (2018). Introduction to the Internet of Things. *Internet of things A to Z: technologies and applications*, 1-50.

[28] Shen, M., Tang, X., Zhu, L., Du, X., & Guizani, M. (2019). Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet of Things Journal*, *6*(5), 7702-7712.

[29] Shi, F., Wang, J., Shi, J., Wu, Z., Wang, Q., Tang, Z., ... & Shen, D. (2020). Review of artificial intelligence techniques in imaging data acquisition, segmentation, and diagnosis for COVID-19. *IEEE reviews in biomedical engineering*, *14*, 4-15.

[30] Singh, R., Dwivedi, A. D., & Srivastava, G. (2020). Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. Sensors, 20(14), 3951.

[31] Singh, H. J. L., Couch, D., & Yap, K. (2020). Mobile health apps that help with COVID-19 management: scoping review. *JMIR nursing*, *3*(1), e20596.

[32] Sookhak, M., Jabbarpour, M. R., Safa, N. S., & Yu, F. R. (2021). Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues. *Journal of Network and Computer Applications*, *178*, 102950.

[33] Swayamsiddha, S., & Mohanty, C. (2020). Application of cognitive Internet of Medical Things for COVID-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, *14*(5), 911-915.

[34] Trivedi, A., & Vasisht, D. (2020). Digital contact tracing: technologies, shortcomings, and the path forward. *ACM SIGCOMM Computer Communication Review*, *50*(4), 75-81.

[35] Vedaei, S. S., Fotovvat, A., Mohebbian, M. R., Rahman, G. M., Wahid, K. A., Babyn, P., ... & Sami, R. (2020). COVID-SAFE: an IoT-based system for automated health monitoring and surveillance in post-pandemic life. *IEEE access*, *8*, 188538.

[36] Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W. J., & Imran, M. A. (2020). BeepTrace: blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond. *IEEE Internet of Things Journal*, *8*(5), 3915-3929.

[37] Yang, F., Heemsbergen, L., & Fordyce, R. (2021). Comparative analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: a new corona of public health governmentality?. *Media International Australia*, *178*(1), 182-197.

[38] Zahoor, K., Bawany, N. Z., & Hameed, A. (2022). BLOCKCHAIN APPLICATIONS FOR COVID-19–A SURVEY. *Suranaree Journal of Science & Technology*, *29*(5).

[39] Zhang, L., Liu, J., & Jiang, H. (2012, October). Energy-efficient location tracking with smartphones for IoT. In *SENSORS, 2012 IEEE* (pp. 1-4). IEEE.

[40] Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2017). Applying software patterns to address interoperability in blockchain-based healthcare apps. *arXiv preprint arXiv:1706.03700.*

[41] Zhao, S., Li, S., & Yao, Y. (2019). Blockchain enabled industrial Internet of Things technology. *IEEE Transactions on Computational Social Systems*, *6*(6), 1442-1453.

Διαδίκτυο

[42] Mipasa Notebooks, «Covid-19 Vaccine Hesitancy», Νοέμβριος 2022. Διαθέσιμο: https://mipasa.unbounded.network/hrs1994/notebooks/7d68173e-bb68-403a-b9e9-0f28653089bd

[43] Levi, J. & Singh, G. (2020). MiPasa - an Open Data Platform to Support COVID-19 Response. Ανακτήθηκε στις 20 Νοεμβρίου 2022 από: https://hacera.com/blog/mipasa-and-ibm-blockchain-platform/

[44] Haig, S. (2020). World Health Organization Launches Blockchain Platform to Fight COVID-19. Ανακτήθηκε στις 25 Νοεμβρίου 2022 από: https://cointelegraph.com/news/world-health-organization-launches-blockchain-platform-to-fight-covid-19