ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΕΥΦΥΗΣ ΥΓΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΙΑΤΡΙΚΩΝ ΠΡΑΓΜΑΤΩΝ: ΖΗΤΗΜΑΤΑ ΤΟΥ ΟΙΚΟΣΥΣΤΗΜΑΤΟΣ, ΤΕΧΝΟΛΟΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ ΚΑΙ ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ

SMART HEALTH IN THE INTERNET OF MEDICAL THINGS: ECOSYSTEM ISSUES, ENABLING TECHNOLOGIES AND PROPOSED SOLUTIONS

Διπλωματική Εργασία

της

Μοναστηρλή Χρυσάνθης

Θεσσαλονίκη, 10/2022

ΕΥΦΥΗΣ ΥΓΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΙΑΤΡΙΚΩΝ ΠΡΑΓΜΑΤΩΝ: ΖΗΤΗΜΑΤΑ ΤΟΥ ΟΙΚΟΣΥΣΤΗΜΑΤΟΣ, ΤΕΧΝΟΛΟΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ ΚΑΙ ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ
SMART HEALTH IN THE INTERNET OF MEDICAL THINGS: ECOSYSTEM ISSUES, ENABLING TECHNOLOGIES AND PROPOSED SOLUTIONS

Μοναστηρλή Χρυσάνθη
Πτυχίο Πληροφορικής, Πανεπιστήμιο Ιωαννίνων, 2020

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Ψάννης Κωνσταντίνος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25/10/2022:

Ψάννης Κωνσταντίνος Παναγιώτης Φουληράς Αλεξανδροπούλου Ευγενία

Μοναστηρλή Χρυσάνθη

Περίληψη

Η έννοια της ευφυούς υγείας (smart health) και του Διαδικτύου των Ιατρικών Πραγμάτων (Internet of Medical Things - IoMT) έχουν ανακύψει τα τελευταία χρόνια ως πιθανές λύσεις σε διάφορα ζητήματα των συστημάτων παροχής υγείας αφού επιτρέπουν, μεταξύ άλλων, την απομακρυσμένη παρακολούθηση ασθενών, την τήρηση ηλεκτρονικών φακέλων υγείας και την εφαρμογή εργαλείων τεχνητής νοημοσύνης σε ιατρικά δεδομένα. Σε αυτή την εργασία παρουσιάζονται τα εγγενή ζητήματα σε ένα οικοσύστημα IoMT, όπως η ασφάλεια και η εμπιστευτικότητα των δεδομένων, οι τεχνολογίες που στηρίζουν την υλοποίηση όπως το Blockchain και η μηχανική μάθηση αλλά και κάποιες ολοκληρωμένες προτάσεις που έχουν τεθεί από ερευνητές στο πεδίο.

Λέξεις Κλειδιά: Διαδίκτυο των Ιατρικών Πραγμάτων, ευφυής υγεία, Blockchain, μηχανική μάθηση, ασφάλεια, εμπιστευτικότητα

Abstract

Smart health and the Internet of Medical Things have lately emerged as potential solutions for issues plaguing health systems worldwide such as remote patient monitoring, switching to electronic health records and using artificial intelligence tools on large sets of medical data. This thesis presents the core issues in an Internet of Medical Things ecosystem such as data privacy, safety and security and enabling technologies such as Blockchain and machine learning, as well as selected integrated framework proposals by researchers in the field.

Keywords: Internet of Medical Things, smart health, Blockchain, machine learning, privacy, security.

Foreword & acknowledgements

I would like to thank Associate Professor Psannis Konstantinos for suggesting this very interesting topic for my thesis and for his cooperation during its undertaking. His course was very inspirational to me and opened up an entire research field before my eyes with a large potential for research and real word applications.

Contents

Table of figures

Table of tables

1 Introduction

1.1 The issue of smart health/ smart hospitals

The word smart is lately used in combination with many terms to identify devices or functions that possess what is perceived as a level of intelligence. Smart health is a term used to indicate a large set of devices and technologies that automate or enhance the provision of health services and the overall quality of care offered to patients. The Internet of Medical Things is a collection of diverse devices that have networking capabilities whose function is related to an aspect of health. Smart health as implemented in the Internet of Medical Things is the topic of this thesis. The related challenges, the core ecosystem issues, enabling technologies and tools as well as integrated framework proposals are presented.

1.2 Goals of the thesis

This thesis aims to serve as a comprehensive reference for people that are looking to start studying on issues related to smart health and the Internet of Medical Things. By highlighting the core concepts and pinpointing the major issues at hand tackled by researchers, this thesis is ideal to set the theoretical foundations for further study.

1.3 Contribution

The main contribution of the thesis is that it stands as a complete introduction to concepts related to smart health and the Internet of Medical Things without requiring previous knowledge of the field. Furthermore, the list of references is an excellent starting point for further study as they are recent publications, in well known journals and conferences with significant impact.

1.4 Structure of the thesis

The structure of the thesis is as follows: Chapter 2 is a concise introduction to basic terminology and a brief description of the structure of the Internet of Medical Things. Following that, Chapter 3 delves into the core challenges of the ecosystem, namely privacy, safety and security of the medical data and the devices operation in general. The

confidential nature of health related information leaves no room for omissions when it comes to privacy and informed consent of the patient that can at any stage be revoked is the basic function that needs to be supported. It must be 100% clear to the patient which data is captured, where it is stored and who has access to it and what it is used for. Additionally, although security needs in the IoMT resemble those of traditional networks, there is another parameter/ mode of operation that requires extensive advanced planning that is unique in medical scenarios, namely emergency operation and this is also discussed.

Chapter 4 presents the enabling technologies that can provide solutions in the implementation of the Internet of Medical Things. The two most important ones are Blockchain and machine/ deep learning. The inherent properties of Blockchain which make it a good solution are discussed, as well as the types of machine learning/ deep learning tools that can be used with medical data.

Chapter 5 presents three types integrated framework proposals in the context of the Internet of Medical Things. The first one is a relatively generic framework for remote patient monitoring focusing while the second one is related to the Covid-19 pandemic. The final type of proposals presented is related to the combination of deep learning networks with a Blockchain storage infrastructure.

Chapter 6 contains reference tables for the publications on the Internet of Medical Things included in the thesis bibliography. Tables are provided for each of the core topics discussed and additional information is provided per publication in order to enable researchers to locate publications of interest. Chapter 7 presents our integrated proposal for electronic health records management at a state level, while Chapter 8 compares this proposed platform with existing approaches and points where it is superior. Chapter 9 discusses deep learning approaches to natural language processing and describes a code implementation in Python we undertook, whose performance can be estimated when data from electronic health records become available.

Lastly, Chapter 10 presents a summary of the thesis and highlights future research directions while Chapter 11 11 includes all references.

2 Background

Predictions for the size of the market related to the Internet of Medical Things are not easy, especially during the last two years with the unexpected turn of events related to the Covid-19 pandemic. More specifically, 2015 predictions by Forbes predicted that at 2020 the Internet of Things (IoT) will contribute $1.9 trillion to the global economy and $117 billion to the IoT-based healthcare industry [Hossain and Muhammad, 2016]. More recent figures by Deloitte [Forbes, 2022] estimate the 2022 IoMT market at 158.1 billion dollars. The precise monetary figures may vary but the number of sensors which is a good indicator of popularity is expected to rise to 22 billion when now it is estimated at 10 billion.

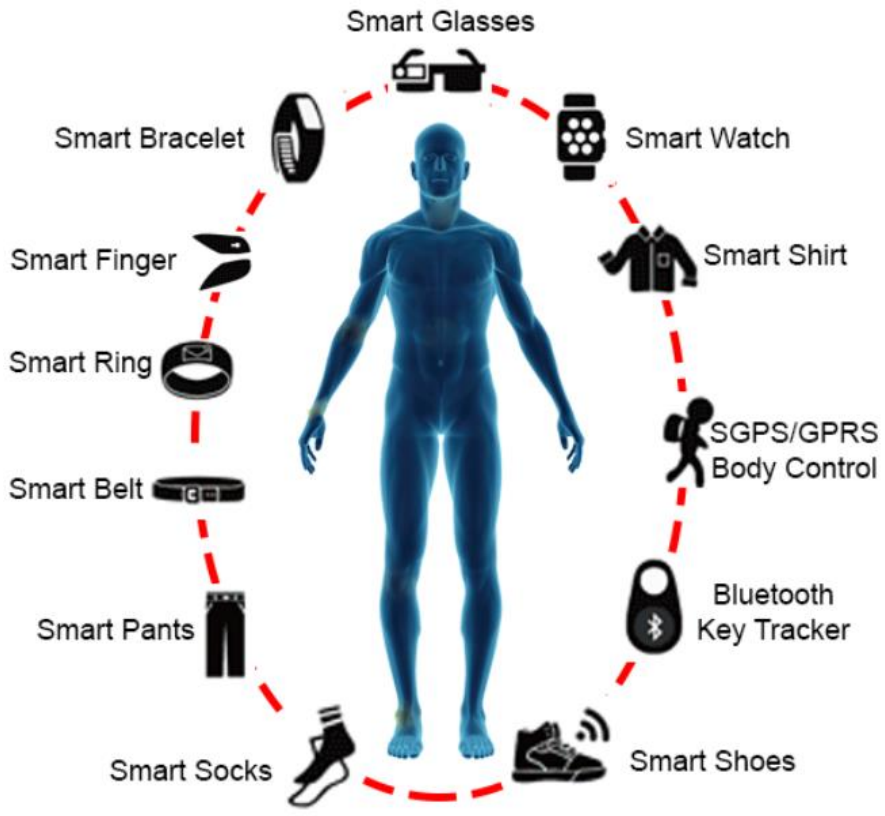

Figure 2.1: Examples of wearable devices

Figure 2.1 includes examples of wearable devices that can be used for various types of applications, including smart health. “Smart” clothes or accessories can provide insights

into a person health status. Accuracy of measurements varies but wearables can definitely offer helpful information. Figure 2.1 cites examples of smart health applications

Figure 2.2: Examples of IoMT applications

These include remote patient monitoring and telehealth, assisted living where devices help ageing individuals with everyday tasks, effective chronic disease management with fewer visits to professionals and hospitals but also applications related to facilities operation such as asset (equipment) and drug tracking and management.

The covid-19 pandemic was an unprecedented turn of events and caused a massive healthcare crisis, testing the limits of traditional services. The benefits of remote patient monitoring became even more apparent and new tools and applications were developed to shield, especially those at a higher risk, i.e., the elderly and those with underlying conditions. The management of chronic disease consists not only of reacting to adverse events detected (for example, detecting an imminent heart attack based on the data from a pacemaker) by providing emergency services on location, but also by programmable devices that automatically intervene such as a defibrillator in the case described above. This device can jolt the patient's heart with a jolt to restore its normal rhythm. Another

very interesting set of medical applications includes remote diagnostic services. The vast amounts of data generated by medical devices can be processed and combined to detect associations between conditions, new risk factors and, of course, monitor outcomes based on the given treatment plan. Machine learning tools have a pivotal role in such applications.

Next generation telecommunication networks which combine fiber backbone networks with advanced mobile ones (5G) are combined with other new technologies such as big-data analytics, artificial intelligence, as it is implemented by machine learning and blockchain. The vast number of interconnected devices of different types, devices which were not networked until recently form what is referred to as the Internet of Things (IoT). Among the several related applications, the Internet of Medical Things (IoMT) stands out, both for its significance for health monitoring given the present health crisis.

The Internet of Medical Things (IoMT) is composed of heterogenous devices which are either worn or implanted in participating individuals. These devices have some form of networking abilities, typically via Bluetooth or similar protocols such as ZigBee, to enable short range communications with minimal power consumption. On the other communicating end, one can find mobile devices (phones), computers of specialized based stations which gather, store and upload the data to the Internet. These paired devices may also be used to issue commands to the medical device, for instance to dispense medication according to a doctor specified schedule.

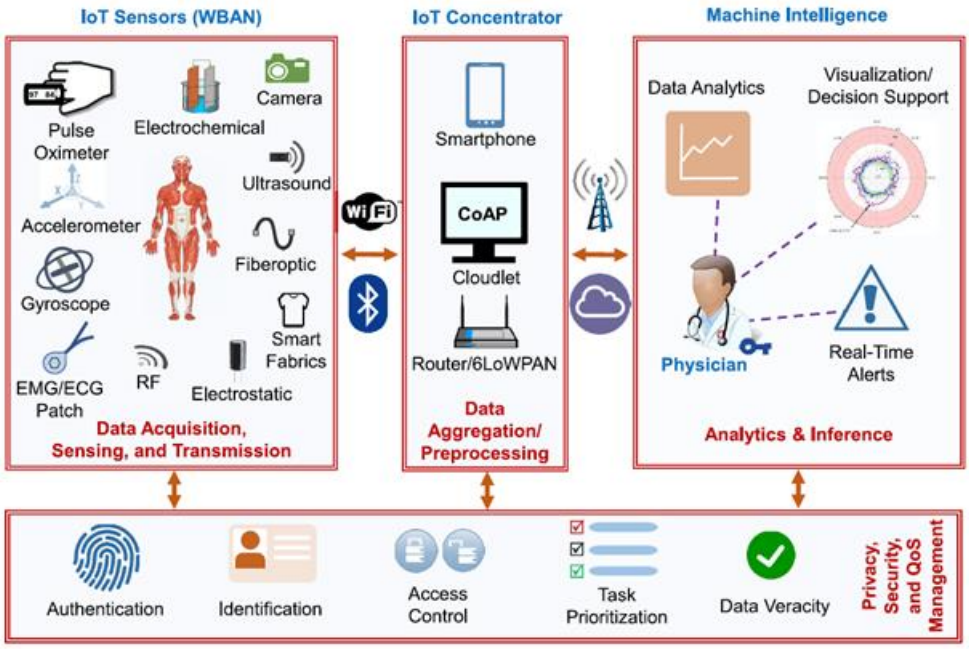

Figure 2.3: A high level architecture of the Internet of Medical Things

A high level architecture of the Internet of Medical Things is depicted in Figure 2.3. In this scenario, sensors and other medical devices monitor and record a host of vital signs that correspond to the current health status of the individual. Thus, a wireless body area network is formed around the patient. Data is collected via other devices like base stations and subsequently forwarded in servers, potentially located in the cloud. These sets of data can then be processed to mine information using big data analytics techniques and machine learning, to extract knowledge and support physicians in their decision-making processes.

Furthermore, when a state of emergency is detected (for instance trouble in heart function or a fall), the connected devices can issue alarms in interconnected medical facilities in the vicinity of the patient. The volume of data recorded is obviously large given that the number of patients monitored is increasing. Apart from monitoring data obtained directly from devices, medical data may include images and videos from scans or past doctor visits, which further increases its volume. Besides volume, velocity and variety are also main concerns since the speed data is obtained increases as does the inherent heterogeneity in a complete medical history. It goes without saying, that data privacy and secure access are also paramount due to the sensitive nature of medical data.

In the remainder of the thesis, we explore the core issues that emerge in the Internet of Medical Things, the enabling technologies that provide solutions and present recent integrated framework proposals published by researchers in the field.

3 Core ecosystem issues

This chapter presents three issues that are pivotal for smart health. For the Internet of Medical Things is to be widely accepted, there need to be guarantees for privacy, safety and security. This chapter explains each principal and explores potential issues and solutions.

3.1 Privacy

The transmission, management and storage of sensitive information related to people's health has highlighted privacy and confidentiality as core issues in any smart healthcare implementation. This section summarizes relevant challenges and proposed solutions.

From the very early days of e-healthcare, attempts to compromise privacy were observed. For instance, O' Connor et al., in a 2017 paper describe a botnet found in an IoT scenario that was collecting personal information and monitoring user activities without the users being informed of such operations, fortunately not in a platform providing healthcare related services. A core privacy concept in any IoT context is informed consent. The user/ patient needs to be fully informed and have a clear understanding of how their data will be utilized, the goals of data storage and processing, what can be achieved by using their data and how they will benefit. They must also be aware of all related risks. These are challenges that exist in all types of networks but the ubiquitous nature of the Internet of Things exacerbates the situation. The person whose data is being collected in a healthcare IoT scenario (e.g. in a smart hospital) is often referred to as a digital health citizen.

The General Data Protection Regulation (GDPR), which applies to citizens of countries in the European Union dictates that data controllers and processors are obliged to emphasize transparency, security and accountability during data handling or incur financial penalties. This, in essence, means that they must embrace the concept of "Privacy by Design" [O' Connor et al., 2017]. In this direction, privacy concerns are addressed proactively on any new or upgraded healthcare IoT system or procedure which involves data, throughout the lifecycle, from conception, to planning, implementation and upgrade.

Digital citizens in general and digital health citizens in particular are envisaged in GDPR to be fully aware and having consented to data processing and usage. Giving informed consent requires adequate information (full disclosure) and is typically given with a signature. In an IoT scenario, however, physical signatures have been replaced by electronic signatures (or ticking boxes) which gives rise to the concept of electronic consent (eConsent), expected to displace other types of signatures/ permissions.

As it was previously mentioned, informed consent requires adequate and accurate information. Additionally, GDPR explicitly specifies that consent may be modified or revoked at any time and this should also be supported by providers. Four distinct levels of consent have been identified and face different technical challenges in their implementation [O'Connor et al., 2017].

1. General Consent: full access to health data is granted by the digital health citizen.

2. General Consent with specific conditions: there is general agreement to data processing but restrictions are specified.

3. General Denial with specific conditions: complementary to type 2 where only what is allowed is specified.

4. General Denial: no access to health data is granted.

In a proposed practical approach [O'Connor et al., 2017], eConsent when registering for a Health Social Network was investigated and it was found that users had very little understanding of the Privacy Policy and Terms and Conditions of the website. Participants were clear that they welcome improvements on transparency and understandability and enhanced control on their data.

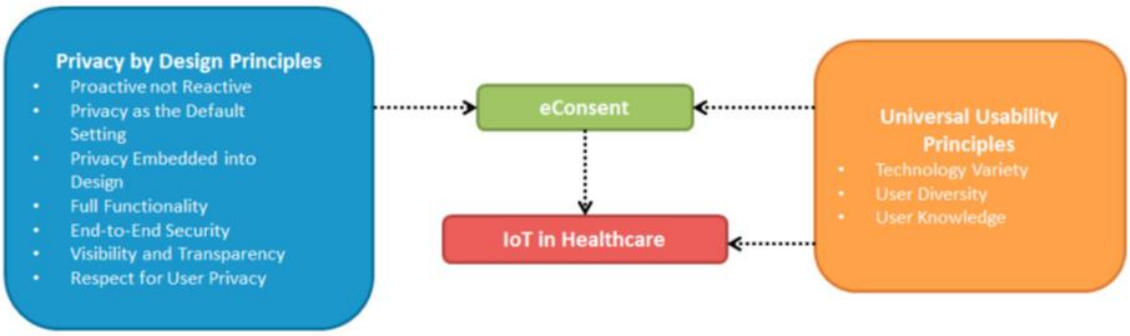

Figure 3.1: Leveraging privacy by design and usability in a healthcare IoT

Figure 3.1 illustrates the basic principles of privacy by design and their relationship with eConsent in a healthcare IoT, where usability is also an important concern. In terms of the privacy by design principles, we have the following issues and proposed solutions:

Proactive not reactive strategy: events need to be anticipated before they occur and the system needs to be prepared. A proposed solution is to have all installed software such as such as antivirus and antimalware up-to-date.

Privacy is the default behavior: Data is automatically protected, access is monitored and only provided to authenticated entities.

Privacy embedded into design: eConsent process is transparent, clearly defined and easy to locate for the user.

Full functionality: all legitimate interests are accommodated, i.e., all "players" are granted appropriate permissions.

End-to-end security: can be implemented using encryption for the entire data path.

Privacy and consent need to be leveraged with usability. Relevant principles include:

- Variety of technology: support for various devices in terms of hardware and software.
- User diversity: user background, skills, knowledge vary. The process needs to be inclusive and accessible, adaptable for older users.
- Gaps in user knowledge: the users may need to learn entirely new things. The language needs to be as simple as possible and initial knowledge of users may need to be assessed (e.g., via a short quiz).

The data protection authorities in several European countries have issued directives, clarifying the topic of digital consent and authentication via electronic means such as certificates. For example, the Greek Data Protection Authority issued directive 2 in 2011, on the topic of digital consent in the context of Article 11 of 2006 Law 3471. In the directive it is clearly specified that any communication with an individual, even one using automated means (without human intervention) should be attempted only after explicit consent has been granted (opt-in system). This consent should be requested at the first contact, before the target individual is handed information. Exceptions to this regulation, also specified in the article, require the sender to include opt-out links and information is short messages or e-mails sent without prior consent.

Per the directive, consent can be retracted at any point, without retroactive consequences for the individual. Consent is given in written form or via digital means. In the case of a digital communication, the provided contact information (e.g., e-mail address) need to be verified as belonging to the individual who gave consent for the communication. Furthermore, digital signatures based on trusted certification authorities are given the same legal basis as traditional signatures.

3.2 Safety

In a scenario where medical devices (wearable or implanted) are used for health monitoring and, potentially, interventions, safety issues arise when a device malfunctions and interacts in an undesired way with the patient or fails to act when such a need arises. Under safety issues, we categorize adverse events that do not involve other entities apart from the patient and the device. Issues involving third parties (potentially malicious) are discussed in the security section.

Figure 3.2: Potential adverse events in implanted medical devices [Camara et al., 2015].

Figure 3.2 illustrates potential adverse events for four popular types of implanted devices, a pacemaker/ defibrillator, a neurostimulator, a drug delivery system and a cochlear implant. Adverse events range from mild discomfort to severe impact to the patient's life and well-being.

In general, safety related issues surrounding networked medical devices are related to wireless safety, namely the way wireless radiation interacts with body tissues, battery issues which may impact device performance, failure or subpar performance detection and interference with other devices. The last issue of devices coexistence is expected to become more critical as the number of devices rises and their popularity soars. An additional point that needs to be made concerning battery issues is that battery replacement in an implant typically requires surgery, which is invasive and unpleasant for the patient.

3.3 Security

Security is a very important issue in all computer networks and in scenarios where there is any exchange of valuable information. When medical devices with networking capabilities are involved the stakes become even higher as security holes can even threaten human lives. Cyber physical systems are defined as electronic systems that are aware of their physical surroundings and can interact with them [AlTawy and Youssef, 2016]. Implanted medical with networking capabilities are popular examples of cyber physical

systems and they are vulnerable to both cyber and physical threats. As shown in Figure 3.3, physical threats are mostly related to environmental and social factors, can compromise availability and safety but are mostly events of large scale and out of the patient's or physician's control.

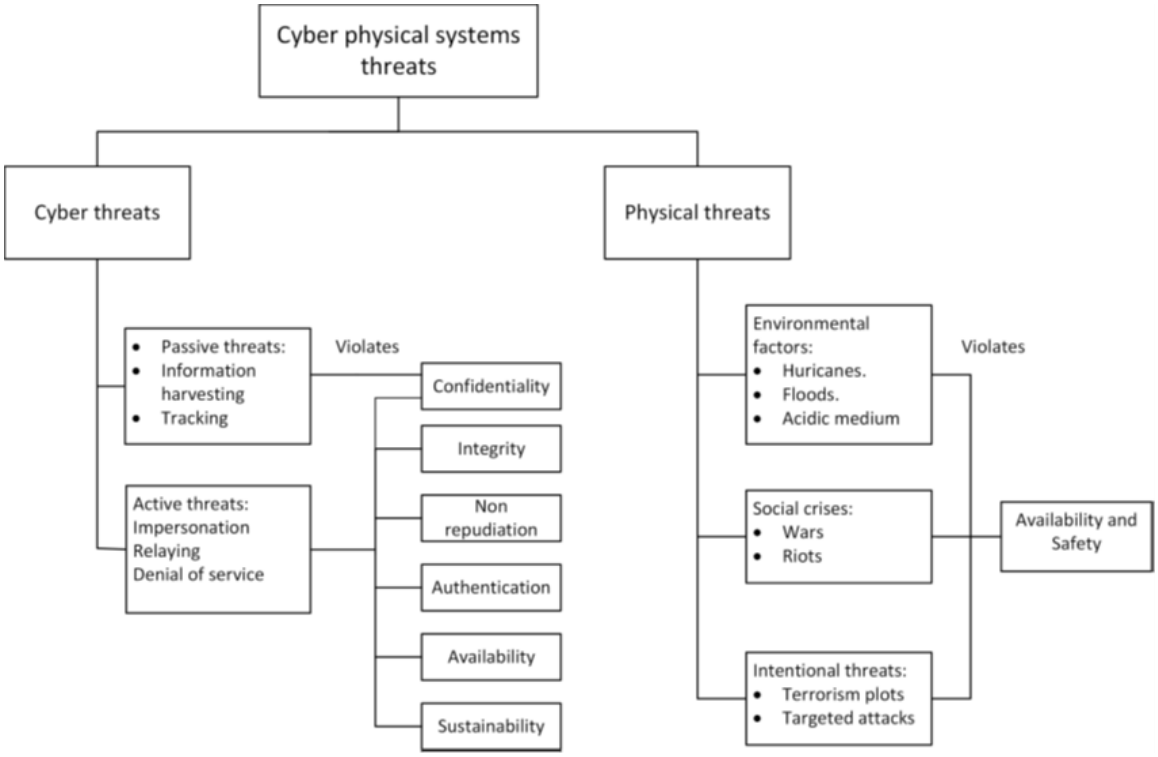

Figure 3.3: Types of security threats in cyber-physical systems

Cyber threats on the other hand are types of threats against which manufacturers, facilities and practitioners need to take specific actions. Cyber security threats can be classified as passive or active. In passive threats, the attackers try to remain undetected while harvesting usable information about the patient and the device or track the device operation or the patient's whereabouts and actions without interfering. In active threats, attackers attempt to either take over the device or compromise its operation while remaining undetected for as long as it takes to complete their task. While passive threats compromise confidentiality and can expose information that can be used in active attacks in the future, active threats also challenge the device availability first and foremost, i.e., may hinder the device normal operation and put the patient's life at risk.

In general, implanted medical devices are vulnerable to the following types of active attacks [AlTawy and Youssef, 2016]:

- Impersonation: if the wireless channel over which communication is conducted is not properly secured, an adversary may interject himself between the implant and its base station/ programmer and impersonate either end. The intruder can forward the communications eavesdropped to the legitimate receiver or feed false information to a physician, to hide, for example, an adverse event that requires immediate intervention.
- Relaying: these attacks are a special type of impersonation attacks which exploit proximity to the medical device to trick it into believing the intruder is a legitimate programmer. Thus the device may carry out instructions that actually harm the patient.
- Denial-of-service: attacks in this category target device availability, i.e., their aim is to render the device working sub-optimally or not at all. For instance, an attacker can feed a device commands that drain its battery, interfere with communications using signal jammers or use magnetic fields near the patient to have sensitive devices turn themselves off.

From the example of attacks cited above, the pivotal role of security in the Internet of Medical Things is very clear. Although research in network security has evolved significantly and strong cryptographic algorithms have been implemented, they are not always suitable for IoMT scenarios. Additional challenges that arise when discussing security of implanted medical devices are related to the critical physical environment (interaction with body tissues, size limitations), the constrained resources (tiny size of devices and constrains on power and processing abilities), the limitations in deploying updates or new software on previously implanted devices and, most importantly, the requirement for emergency authentication. Although, authenticated and controlled access to the device is required in patient monitoring scenarios, in the case of emergencies where a different doctor in a different hospital than the usual needs to access the device to treat the patient or even save his life. This means that security algorithms and authentical protocols need to have taken this case into account in their design. Potential solutions have been presented but each comes with inherent weaknesses.

Figure 3.4 summarizes the types of protection mechanisms that can be implemented in an implanted medical device as single measures or combined. Auditing refers to detailed logging of device actions and patient status and can be effective in detecting anomalies in operation and/ or security breeches. Given the constrains on device memory size, logging may be better implemented in an external device where the implant transmits its data periodically.

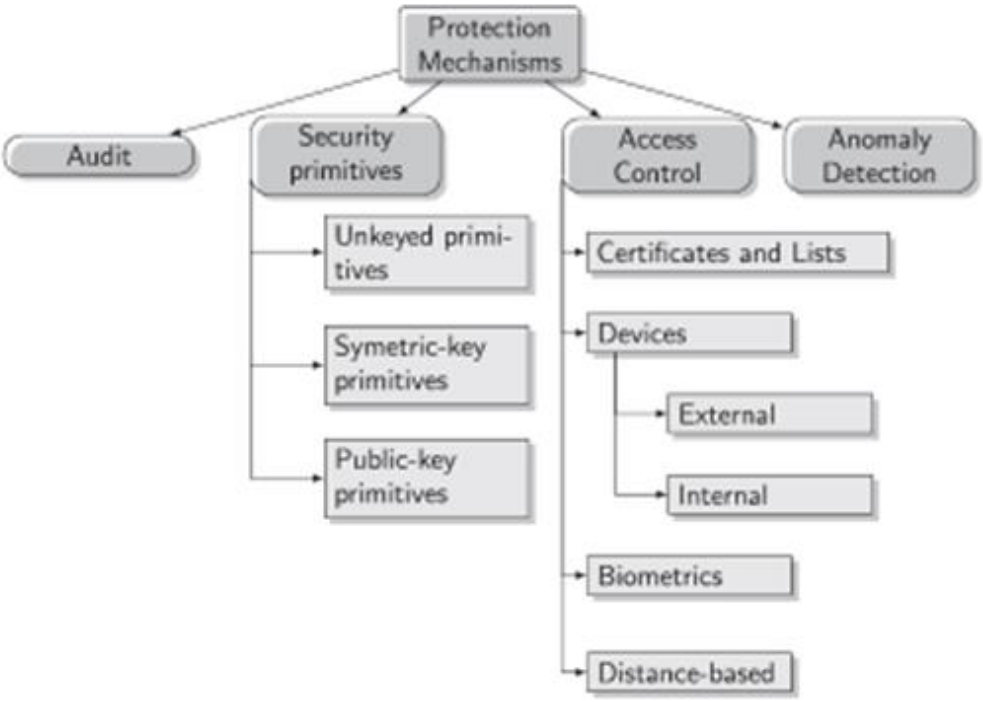

Figure 3.4: Protection mechanisms for medical devices

Cryptographic primitives are well known measures to protect a communications channel, but as mentioned above, restrictions regrading computational power and battery make complex schemes unsuitable and issues such as key management and secure storage arise, especially in emergency situations where the patient may be incapacitated. Access control mechanisms prevent unauthorized and inappropriate usage of the implant. Again, solutions that are widely employed in traditional networks are not suitable for e-health scenarios where emergency authentication is critical.

4 Enabling technologies and tools for the Internet of Medical Things

This chapter presents technologies and software related tools that are essential for the future, global and scalable Internet of Medical Things.

4.1 Sensors, actuators and connected devices

This refers to the devices that actually perform medical data collection and through some form of networking capabilities (e.g., WiFi connection or Bluetoothe/ Zigbee etc.) forward them to storage servers or processing facilities. Apart from devices worn by people or implants in patients under observation, this type of infrastructure includes environmental monitoring tools (for example devices evaluating air quality in crowded places or temperature monitors) and their base stations.

Devices performing data collection in an IoMT scenario are often required to be able to issue alerts and forward them to attending physicians or emergency responders. For example, a common use is a wearable device that can detect a fall, worn by elderly people under close monitoring.

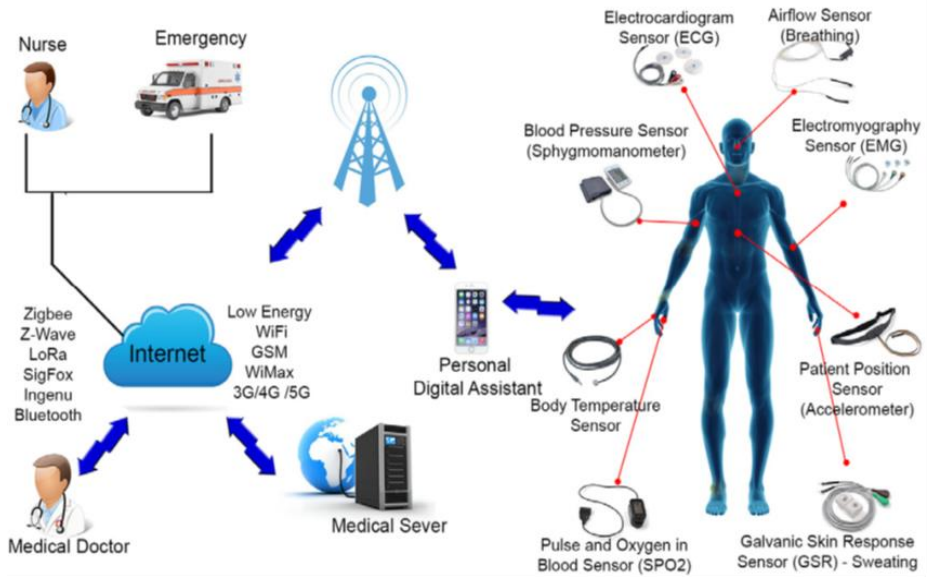

Figure 4.1: Architecture for a remote healthcare monitoring system

Figure 4.1 [Rodrigues et al., 2018] illustrates the architecture of a remote healthcare monitoring system that is based on a number of diverse sensors, implanted or wearable, monitoring bodily functions. Examples include, electrocardiogram sensors monitoring heart rate, airflow sensors monitoring respiration, temperature and perspiration sensors, accelerometers monitoring body position, checking for potential falls and many others.

The technical details of operation of such devices are out of the scope of this thesis but it must be noted that their heterogeneity, lack of interoperability between manufacturers, lack of standards in the industry and network "pollution" caused by crowding and devices in close proximity that generate interference are significant challenges that need to be addressed in the effort for a safe and dependable Internet of Medical Things. Additionally, security, as detailed in the previous chapter is a huge concern, since a minor security flaw in a single component may be exploited by a knowledgeable intruder to jeopardize the entire system.

4.2 Blockchain

As its name suggests, Blockchain is essentially a sequence of blocks (Figure 4.2). The first block is referred to as the Genesis block and every other block *i* is connected to the previous (*i*-1) and the next block (*i*+1), if it exists.

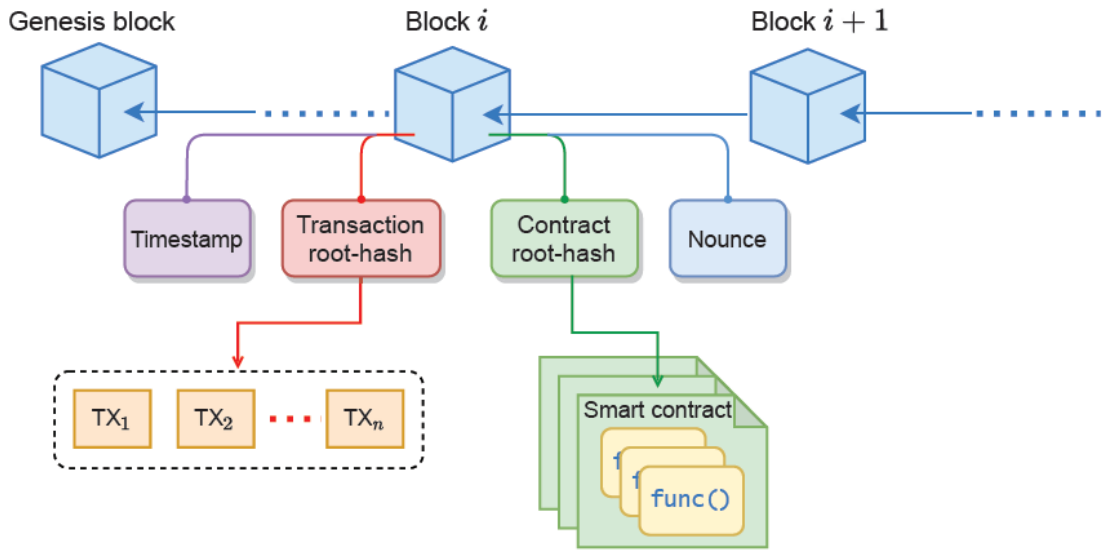

Figure 4.2: A generic Blockchain structure

The connections between blocks (backward and forward references) are established using hash values. This means that each block contains hash values of the full contents of their neighboring blocks. This is very important as it prevents the modification of their contents, thus guaranteeing immutability. Immutability is a very important property of Blockchain and the basis of many of its inherent security and privacy features. Each block also contains a root hash of all the transactions, and a root hash of all the contracts. Modifying even one bit of this data alters the hash value and is thus detectable.

Another important concept that can be implemented on top of a Blockchain infrastructure are smart contracts. These contracts automate the execution of tasks once certain conditions are met or disruptions occur (such as deadlines expiring or breach of a contract). Because of the inherent immutability, smart contacts greatly simplify the administration process, reduce workloads in business activities and alleviate certain risks.

The key features of Blockchain as a technology that make it very attractive as a storage engine for the medical data in IoMT are as follows:

Immutability: as mentioned above, this refers to the fact that data stored in a Blockchain cannot be modified and the modification goes unnoticed. Such probability is extremely low, due to the hash values used throughout the chain, so it is considered that none can tamper stored data without being caught.

Non-repudiation of transactions: entities performing transactions may be required to use digital signatures and transactions may be validated using a distributed consensus mechanisms. These features combined with strong cryptographic algorithms guarantee that no one can refute a recorded transaction (since multiple parties have confirmed it) and no one can deny having performed one since their digital signature was used, thus ensuring non-repudiation of transaction.

Traceability: this concept referred to tracing the origin of data added to the blockchain by analyzing publicly available blockchain data. Interested parties can determine who performed a particular transaction and when.

Decentralization: the distributed nature of blockchain means that there is no central authority (single point of failure/ workload) and enables the validation of transactions by a majority of peers distributed throughout the system. This enhancing reliability and availability.

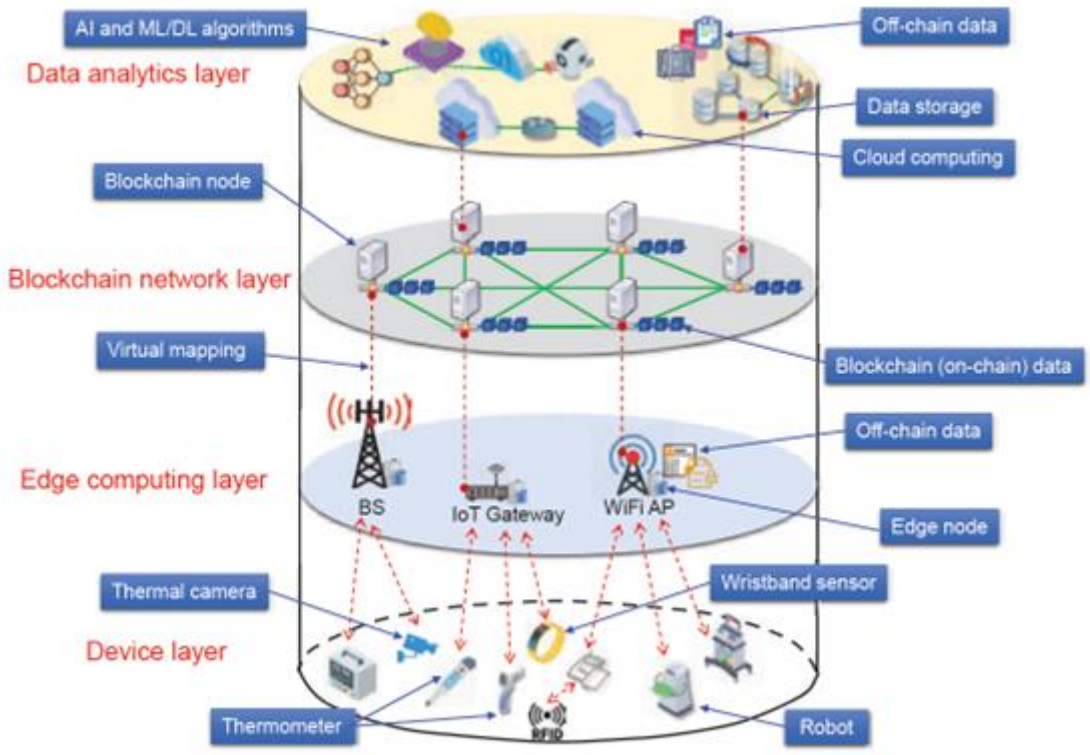

Figure 4.3: A blockchain enabled Internet of Medical Things

Dai et al. in their 2020 paper [Dai et al., 2020] describe the architecture of a blockchain enabled Internet of Medical Things depicted in Figure 4.3. In the proposed architecture, the following layers are identified:

1. Device layer: this layer contains the devices actually capturing health related data
2. Edge computing layer: this layer is the bridge between devices and edge computing facilities (located at base stations/ access points/ gateways) that gather and preprocess IoMT data).
3. Blockchain network layer: this layer functions as the middleware between the lower layers and the data analytics layer and guarantees trustworthy management of resources, authentication and access control.
4. Data analytics layer: this is the layer where artificial intelligence (machine learning and deep learning) tools are used to extract usable information from the massive volumes of data produced from the underlying layers.

The advantages of the confluence of IoMT and Blockchain are listed in [Indumathi et al., 2020] as follows:

- Affordability/ reductions in operational costs.
- Uninterrupted real-time monitoring, e.g., for children and the elderly/ automatic alerts
- Simplicity, ease of use and energy efficiency

4.3 Machine learning tools & Deep learning

Massive data generated from medical sensors, wearable and implanted devices, and other Internet of Things technologies provide rich information about the health status and context of users/ patients. Such incredible volumes of data can be very useful in patient monitoring and assisting doctors to detect conditions and make accurate diagnoses but they require automated processing techniques such as those related to traditional machine learning (ML) and deep learning (DL). For instance, when processing chest X-rays or CT scans, a machine learning algorithm can classify them as infected or normal. The decision

requires several steps where, for example, features of input images are extracted during preprocessing and fed into a machine learning model to be used in the final decision. Another potential application for machine learning techniques, besides classification is to detect the start and evolution of a potential pandemic outbreak and detect possible future hot-zones [Alyasseri et al., 2021].

Machine learning is a powerful tool that facilitates the process of mining massive amount of data that have been collected from different sources and turn data into usable information. This is accomplished by applying a model that was previously learned from a set of observed data examples referred to as a training set.

Machine learning techniques used in e-health applications include the following (Figure 4.4):

1. Supervised learning: is based on a set of labeled training data, i.e., pairs of input and output data where the correct result is tagged.
2. Unsupervised learning: in contrast to supervised learning, there are no previously tagged data to serve as the basis for learning.
3. Semi-supervised learning: as its name suggests, this approach falls between supervised and unsupervised learning, utilizing a small set of labeled training data to improve learning accuracy and speed.
4. Reinforcement learning: algorithms in this category were inspired by behavioral psychology. In such as scenario, intelligent software agents take actions aimed at maximizing a cumulative reward. Normally, there is no a priori knowledge and optimal policies have to be discovered from the training data [Qolomany et al., 2019].

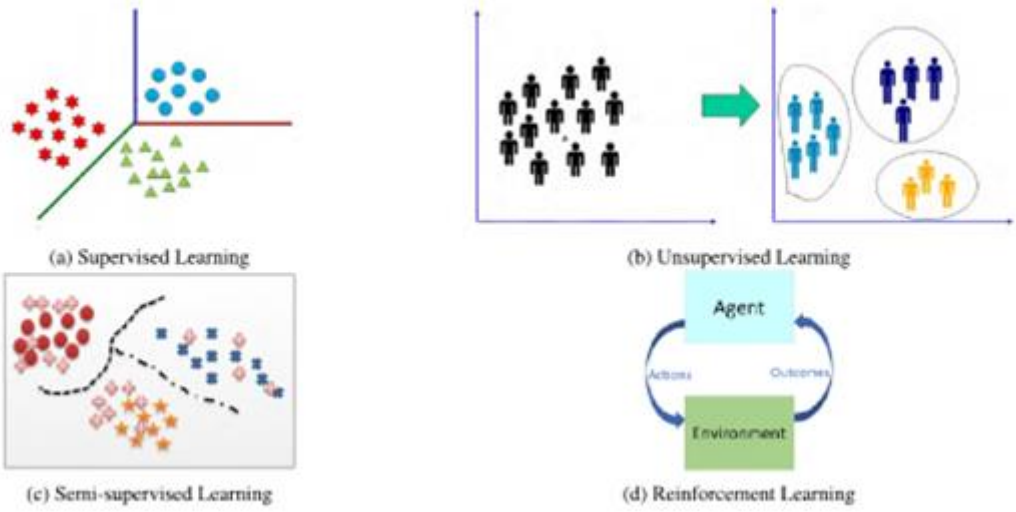

Figure 4.4: Types of machine learning

In deep learning, a model attempts to learn the abstract representations of data. The most typical feature of deep learning models is that they contain a number of hidden layers (at least one hidden layer exists), as well as the standard input and output layers. The number of layers is referred to as the depth of the model. Each hidden layer may contain a number of neurons, and neurons with each neuron having multiple inputs and a single output, connecting to inputs of neurons in lower layers. Each neuron is associated with a weight and a bias whose values are determined and updated during the training.

The way most deep learning models typical learn is via back-propagation. In this approach, there is a feed forward step and a back-propagation step. Initially, the outputs at each layer are calculated based on previous and current layer parameters. These intermediate results determine whether a neuron will be activated. Precise mathematical functions depend on the problem at hand.

As it is clear, such a complex model with multiple layers requires massive computational resources in order to be accurately trained. In this direction, distributed deep learning training may split the load between many collaborating parties. Parallelism may be achieved either in the model (split the model) or the data (split the training data) direction. In the data parallelism approach, which is more common, all parties maintain copies of the model training parameters derived from a centralized parameter server. The local machines then upload their own training gradients and collaboratively update the model which is then available to all.

Popular deep learning algorithms/ network categories include:

1. Convolutional Neural Networks: best suited for analyzing images therefore used in scenarios where x-rays or other types of scans are the basis for diagnosis. Also suitable for computer vision applications.
2. Deep Neural Networks: a subclass of artificial neural networks, i.e., networks that attempt to imitate the function of the human brain.
3. Recurrent Neural Networks: suitable for natural language processing applications.
4. Generative Adversarial Networks: as the name suggests, in these models there are two networks competing against one another with each opponent benefiting from the other one's losses.

5 Integrated framework proposals for Health IoT

In this section, integrated proposals on implementations of smart healthcare that have been presented in literature are presented.

5.1 A high level proposal for multiple scenarios

One of the first complete proposals for an integrated Health Internet of Things and smart healthcare was presented by Hossain and Muhammad in 2016. In their seminal paper [Hossain and Muhammad, 2016], the authors present a scenario for a healthcare IoT ecosystem, discuss its structure and data flow in detail and discuss a specific application for electrocardiogram monitoring in detail.

The conceptual illustration for the ecosystem is shown in Figure 5.1 where the participating players are involved devices are depicted.

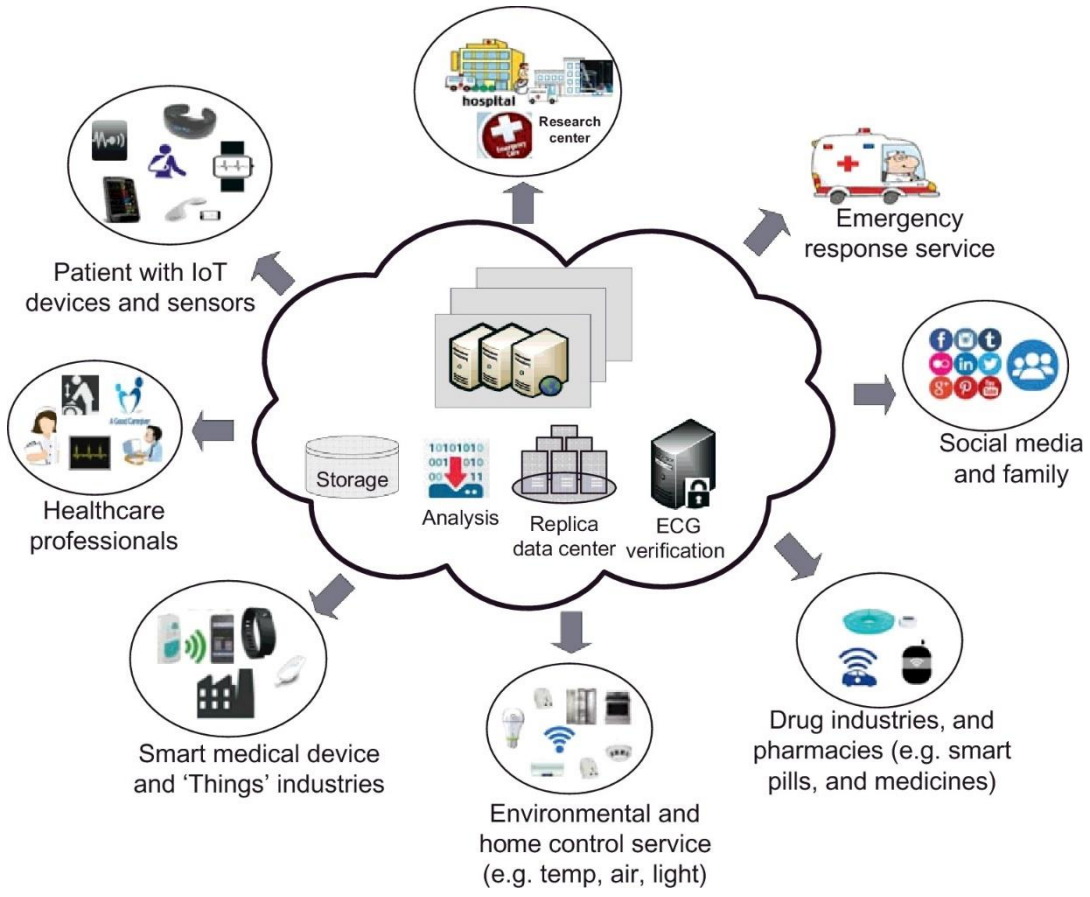

Figure 5.1: A healthcare Internet of Things illustration.

As shown in the figure, patients with IoT devices and sensors are connected with healthcare professionals, smart hospitals, drug stores and emergency responders. Other participants/ stakeholders include medical research centers and pharmaceutical industries. Family and friends may also be connected and kept in the loop, possibly via social media. In this ecosystem, patient information can be transferred seamlessly and securely among the interested parties, such that specific patient data are available only to a designated authorized healthcare team. For instance, prescribed drugs are automatically forwarded to the drug store selected and delivered to the patient. Additionally, big data analytics (and potentially artificial intelligence) enables analyzing, storing, closely monitoring, and securely sharing the data for further review and medical recommendations or medical research.

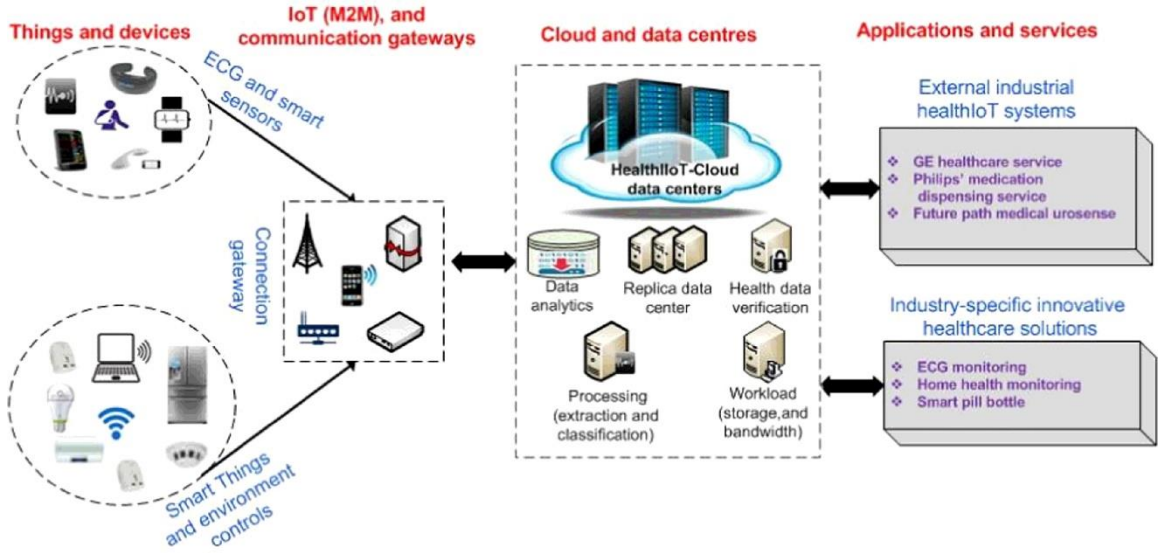

Figure 5.2: The flow of data in an internet of medical things architecture.

A very important issue in an internet of medical things architecture is the paths through which data flows. These paths for an application related to electrocardiogram signal monitoring are depicted in Figure 5.2. Mapping the paths is very important in order to identify potential points of signal interception and other security related issues. As mentioned above, the readings captured from the sensors are seamlessly transferred to cloud servers where they are processed and securely stored. This chain of collected data is either accessed by healthcare professionals, or delivered to external systems for further industry-specific specialized processing. The original signal processing consists of several

steps whose aim is to increase signal quality and remove errors that may trigger alarms. More specifically, signals are enhanced to remove physiological defects such as those due to muscular activity or motion as well as non-physiological defects commonly caused by electrical interference or electrode malfunction. These defects or combinations of them can result in ECG resembling cardiac abnormalities like ectopic rhythm. Other processing steps include the detection of peak amplitude (peak R) and watermarking to protect the signal from forgery. Selected features of interest are extracted from the signal and stored in the IoMT infrastructure to be later used as input to machine learning software such as a vector machine classifier.

5.2 Proposals related to the Covid-19 pandemic

The coronavirus pandemic caught humanity by surprise, not because it was the first recorded pandemic or the one with the highest mortality rate, but because the very contagious virus tested the limits of healthcare systems and challenged assumptions regarding everyday life. Concepts such as distance learning and remote working became very popular to assist with limiting the spread of the virus and, of course, technology played a significant role. The fact that hospitals and other care facilities were swamped with potential and confirmed cases was also a powerful motive to adopt telemedicine, especially for vulnerable patients, so as to keep people at risk of severe disease as far away from outbreak epicenters as possible. It was only natural that researchers would explore solutions related to utilizing the Internet of Medical Things for applications related to the Covid-19 pandemic and this section summarizes relevant publications and highlights all the ways in which a smart hospital and smart health in general could provide solutions.

In [Dai et al., 2020], researchers identify the following applications for IoMT as related to Covid-19:

1. **Tracing pandemic origin**: this refers to the use of technology such as thermal cameras and sensors in places where there is crowding such as transportation media stations, in order to identify potential cases (via detecting elevated body temperature, for example) and follow the chain of transmission to people that were in close proximity to a Covid-19 positive person. In this scenario, the Blockchain enabled IoMT guarantees data privacy and traceability of

transactions. It must be noted that detection equipment does not have to be installed in fixed locations but can instead be mounted on unmanned arial vehicles (drones) to cover, for example, gatherings of large crowds in sports stadiums or concerts.

2. **Quarantine and social distancing**: isolation from other people for a possible case during an outbreak has been proven to be the most effective measure to limit the Covid-19 pandemic. Social distancing has, likewise, been proven to limit transmission from asymptomatic individuals during the time between they contacted the disease and the time they became sick. Quarantine restrictions typically require dedicated facilities and staff for supervision but such solutions are not cost-effective or scalable during the worst phases of the pandemic. Technology such as wristbands allows people (for example travelers) to quarantine at home or at hotels while periodically reporting their exact locations. As far as social distancing is concerned, wristbands can issue alerts when distance is below a specified threshold or crowd density is unacceptable in a venue and/ or keep track of distances from other wristbands in close proximity. The role of Blockchain in such scenarios is mainly data privacy protection.
3. **Smart hospital**: a Blockchain enabled Internet of Medical Things can support practically every function of a smart hospital. In such a medical facility, for instance, material resources/ assets in every scale and of every type (from beds and ambulances to imaging equipment and respirators) can be monitored for availability and proper operation by using RFID tags and smart sensors. The usage data and malfunction logs can be used for predictive cost analysis and procurements related decision making. Within a hospital building, IoMT devices can be used to monitor environmental conditions such as temperature and air quality, generate alerts or even take relevant actions. In the near future IoMT devices used may not be passive such as sensors but also include devices that perform actions such as cleaning or disinfecting thus reducing manual labor and cost. In all the scenarios described, Blockchain guarantees the privacy and immutability of data, protects the chain of transactions from tampering and thus ensures non repudiation of transactions.

4. **Remote healthcare and telemedicine**: the Covid-19 pandemic really highlighted virtually all shortcomings of traditional healthcare systems. Vulnerable people such as the elderly or the chronically ill were forced to stay away from hospitals overflowing with patients for fear of infection. A Blockchain enabled IoMT can enable remote monitoring of patients via wearable or implanted devices that securely share the data they record with physicians and issue alerts in case of emergencies. The most important concern in this process has traditionally been data privacy and security and this is exactly where Blockchain comes into play, ensuring data provenance and allowing data access only to authorized personnel and prohibiting its modification [Abdulkareem et al., 2021], [Shamsabadi et al., 2021].

5.3 Proposals combining deep learning with Blockchain

This section contains recent proposals by researchers that combine deep learning with Blockchain in applications related to the Internet of Medical Things that introduce innovations in Blockchain implementation and inherent mechanisms.

5.3.1 DeepChain

DeepChain [Weng et al., 2019] was proposed as an approach to building a safe, distributed and fair deep learning framework in an IoMT ecosystem. The most novel aspect of DeepChain is its Blockchain based incentive mechanism that evaluates the contributions of participating parties and encourages them to adopt proper (honest) behaviors. DeepChain also guarantees data confidentiality and auditability of actions and transactions during the training process.

Figure 5.3 illustrates the difference between traditional deep learning and DeepChain. In all types of collaborative deep learning, local parties generate intermediate or partial results (gradients) based on the training data they have available and upload them to a local parameter server to obtain updated model parameters. This mechanism, however, has serious security flaws (analyzed in subsequent paragraphs) and DeepChain resolves the issues by implementing Trading Contracts and Processing Contracts as smart contract

in the Blockchain, and with them guides the secure training process. In the figure, T_x refers to transaction.

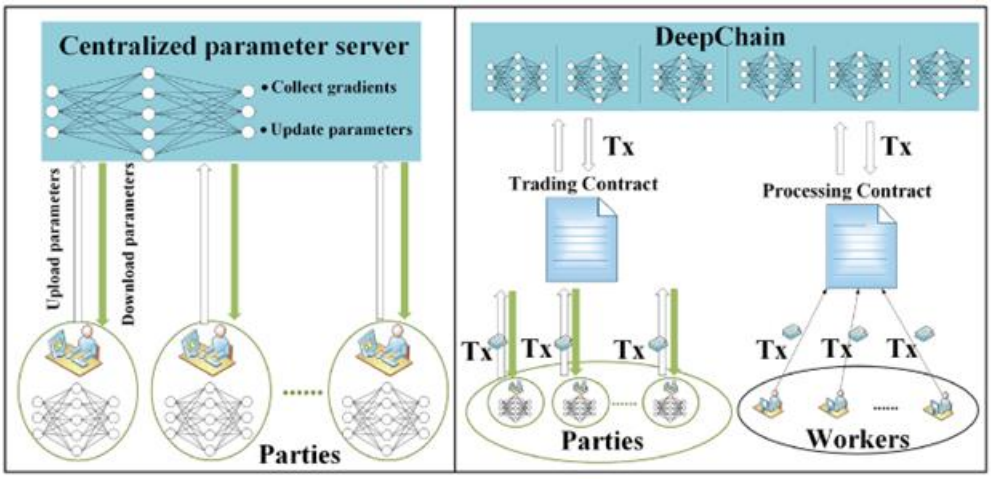

Figure 5.3: Traditional distributed deep learning vs. DeepChain

Figure 5.4 illustrates the operation of the DeepChain novel incentive mechanism. Cooperative parties and workers (= entities that complete tasks) contribute to the training of a model and get rewarded with high quality results from the training. In the figure, contributions are denoted by ω and rewards by π.

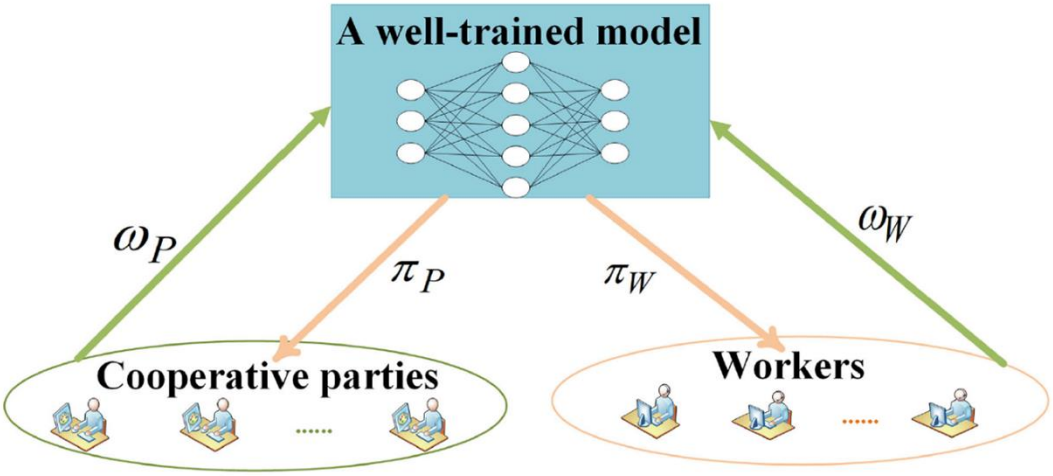

Figure 5.4: DeepChain incentive mechanism

Parties with high volumes of data are encouraged to contribute their data for model training because the incentive mechanism values data quantity and offer substantial rewards for large data sets. If a party's behavior is deemed to be dubious, the party gets a

penalty. The training of local models also needs to be accurate and workers who process and validate transactions also need to be honest. For example, two cooperating parties who want to obtain results pay a fee that is inversely proportional to the volume of data they contribute. An agreed upon reward for completion of processing is awarded to the party who will create a new block in the Blockchain, i.e., to the party that will finish processing their transactions first.

Because of the nature of Blockchain, transaction auditability is guaranteed and fabrication of input data or intermediate results is dateable and punishable (via the incentive mechanism). It must be noted that data volume (quantity) is the single criterion used for contribution evaluation, hence there is room for improvement in the incentive mechanism if it is altered to take quality into account as well.

Collaborative deep learning, which is the basis of DeepChain is faced with several challenges related to security due to its inherent data/ gradients disclosure. These challenges are addressed in DeepChain via specific mechanisms. The first threat has to do with the disclosure of local data and model when they are uploaded to the parameter server. Despite the fact that each party only uploads local gradients (intermediate results) to the parameter server, potential attackers may attempt to infer and steal the input data that led to these gradients, thus exposing private training data. Confidentiality of local gradients is achieved in DeepChain by requiring at least a number of participants collude to reveal local gradients. In other words, in DeepChain, participants encrypt their local gradients using their own private keys and upload them to the parameter server but decryption requires all participants to collaborate. It is considered highly unlikely that the number of participants that are required for decryption are all dishonest. Other challenges are related to potentially malicious behaviors by participants who either attempt to upload erroneous gradients or attempt to falsify their proof-of-work to save on processing time and get results. These are dealt via the auditability mechanisms mentioned above, which are again based on participant consensus. A final challenge is fairness guarantee for participants. This is achieved by setting strict time out deadlines and inflicting monetary penalties to members that were either not punctual or dishonest via smart contracts. The money from penalties incurred by dishonest members are transferred to honest parties, thus guaranteeing fairness.

5.3.2 BinDaaS

BinDaaS (Blockchain-Based Deep Learning as-a-Service) was proposed by Bhattacharya et al. in 2021 as a potential solution for security and privacy issues that emerge when storing Electronic Health Records [Bhattacharya et al., 2021]. As its full name suggests, BinDaaS integrates BlockchaiIN with deep learning as a Service.

The BinDaaS system architecture is illustrated in Figure 5.5 and is composed of 4 layers, numbered from 0 to 3, with data moving from the lowest index layer to the highest (from 0 to 3). The lowest layer (0) contains the network users/ players such as physicians and patients, but also administrative staff and third-parties, lab technicians and researchers. Data flowing in the network may be generated automatically by (bio)sensors monitoring vital patient signs such as blood glucose levels or manually, by recording for example test results, diagnoses, medications administered and others. It must be noted that the collected raw data undergoes homogenization and classification using Bayesian classifiers. Layer 1 contains authorities (such as hospitals and laboratories) and companies (insurance and pharmaceutical). Data gathered in this Authoritative Organizational Layer is subsequently forwarded to Layer 2, which is the Analytics Layer via distributed network infrastructures to be processed for knowledge management purposes. This is the layer where deep learning as a service if offered to extract usable information from the data. The outcomes of the deep learning network is then fed as an input to layer 3 which contains the Electronic health record Servers (ES).

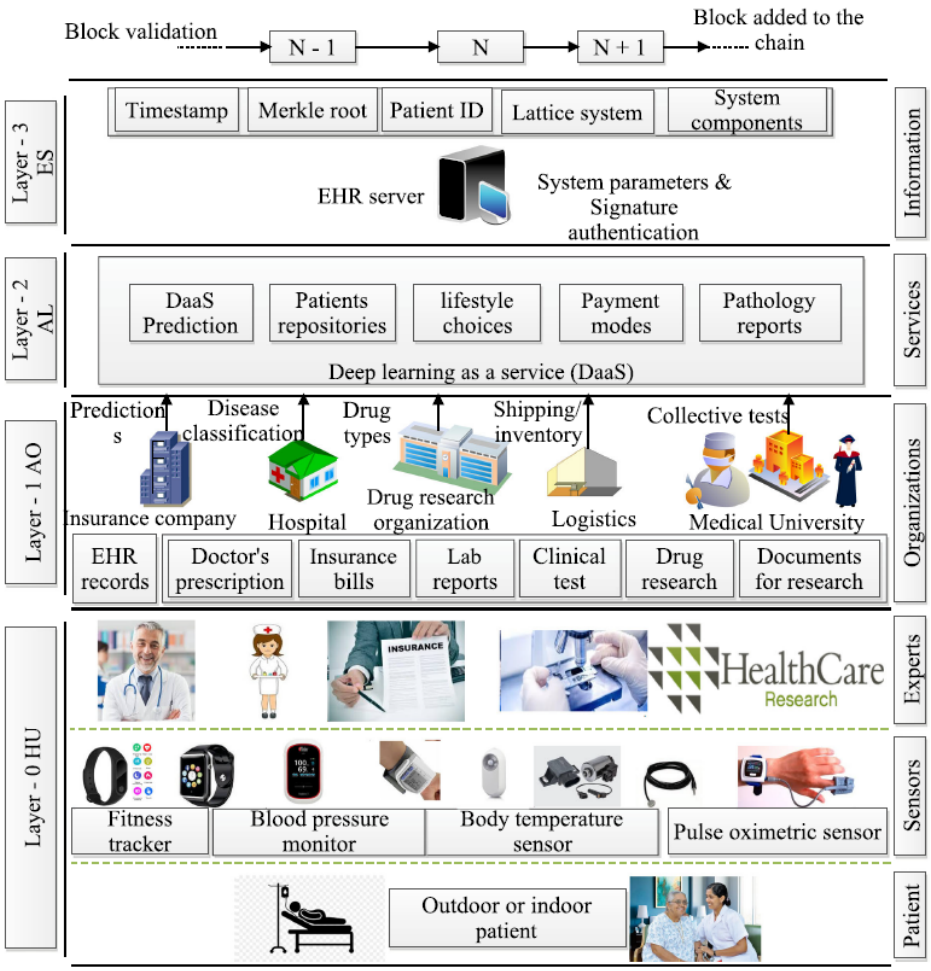

Figure 5.5: BinDaaS system architecture

The ES layer actually determines the process via which blocks are added to the Blockchain and is responsible for guaranteeing security and integrity both for data and transactions. An important tool employed in this direction is lattice cryptography that improves resilience to several types of attacks (side channel attacks, quantum forgeries, collusion).

Medical data stored in electronic health records in BinDaaS include symptoms, clinical observations, data captured from devices (monitored) and patient hospital visits or hospitalizations which may both be planned or emergency. Every piece of relevant information (date/ time of admission/ discharge, lab reports, diagnoses, etc) is contained in the patient's file along with lifestyle choices that may affect health. This in-depth information can be used to predict future illness by feeding a prediction model. The

researchers behind BinDaas validate both the security scheme and the prediction model against existing state-of-the art infrastructures for comparison.

6 Publications on the Internet of Medical Things – Current literature reference tables

In this chapter we will attempt to organize recent papers on the general topic of the Internet of Medical Things in tables listing the main properties of each publication. These tables aim to serve as concise sources of information for researchers that wish to study the area in depth.

The first table lists all papers contained in the list of references that were published during the last 5 years (since 2017), with the type of paper (overview, implementation prototype, integrated proposal), its main topic, and additional selected keywords.

Table 1: Recent publications reference

Reference	Publication Type	Main Topic	Selected keywords
Abdulkareem et al., 2021	Software prototype	COVID-19 diagnosis system	Machine learning, smart hospital
Ahad et al., 2019	Overview	5G-based smart healthcare network	Smart healthcare, device-to-device communication
Ahmed et al., 2021	Software prototype	Patient discomfort detection	Deep learning, computer vision
Albesher, 2019	Overview	Smart cyber-physical ubiquitous environments	Sensors, wearable devices
Alqaralleh et al., 2021	Implementation model	Secure image transmission and diagnosis model	Blockchain, deep belief network
Alyasseri et al., 2022	Overview	COVID-19 diagnosis models	Machine learning, deep learning
Ben Ida et al., 2020	Implementation model	Early warning scoring system	Smart hospital, self-adaptative system, vital signs monitoring
Bhattacharya et al., 2019	Prototype	BinDaaS: Blockchain-based deep-learning as-a-service	Electronic health records, disease prediction
Bigini et al., 2020	Overview	Blockchain for the internet of medical things	Distributed Ledger Technology, Blockchain

Dai et al., 2020	Integrated proposal	Blockchain-enabled IoMT to combat COVID-19	Blockchain, COVID-19
Dilawar et al., 2019	Integrated proposal	IoMT security	Blockchain, proof of work
Ellouze et al., 2020	Overview	Blockchain for IoMT	Security, proposed architectures
Fang et al., 2020	Integrated proposal	Privacy protection	Watermarking, data sharing, access control
Guinard, 2006	Prototype	Assets tracking system	Smart hospital, RFID, workflow optimization
Habibzadeh et al., 2019	Overview	IoT from a clinical perspective	Health monitoring, healthcare analytics, medical decision support
Hussain et al., 2019	Prototype	Baby behavior monitoring	Computer vision, alerts
Indumathi et al., 2020	Integrated proposal	Blockchain IoMT	Real-time health monitoring
Jamil et al., 2019	Integrated proposal	Drug supply chain integrity management	Blockchain, smart contracts
Jia et al., 2022	Comparative analysis	Hospital performance metrics prediction	Machine learning
Isravel & Silas,2020	Overview	IoT-cloud based technologies smart healthcare	Health data, machine learning
Khan et al., 2021	Overview	Reliability in the IoT	Machine learning, 6G communications, Blockchain based security
Lakhan et al., 2021	Integrated proposal	Sensor data aggregation and study	Ethereum, smart contract, Blockchain
Mansour et al., 2021	Prototype	Diagnosis model for heart disease and diabetes using AI and IoT	Machine learning, classification of the medical data
Maxwell & Grupac, 2021	Integrated proposal	Virtual care technologies for Covid-19 patients	Artificial intelligence, Covid screening and diagnosis
Moro Visconti & Morea, 2020	Integrated proposal	Smart hospital project financing	Healthcare digitalization, pay-for-performance incentives

Naresh et al., 2020	Overview	The advent of IoMT	Enabling technologies, key applications, proposed architecture
O'Connor et al., 2017	Integrated proposal	Privacy by design	Informed consent, GDPR, digital consent
Pan et al., 2019	Overview	Intentions of medical practitioners towards smart technologies	Technology transfer, subjective norm, perceived risk
Połap et al., 2020	Integrated proposal	Blockchain and neural networks	Patient monitoring, assisted diagnosis, federated learning
Rayan et al., 2019	Overview	Machine learning in smart health	
Rodrigues et al., 2018	Overview	Enabling technologies for IoMT	Assisted living, mobile health
Said et al., 2020	Prototype	Rank attack detection	Machine learning, smart hospital, security, intrusion detection
Samanta et al., 2021	Prototype	Secure cloud services	Support vector machines based cryptography
Seliem & Elgazzar, 2019	Proposal	Blockchain based IoMT	Lightweight security scheme, smart hospital, bolster
Shamsabadi et al., 2022	Overview	Management of chronic diseases	Covid-19
Sharma et al., 2020	Integrated proposal	Blockchain based smart contracts	
Stanley & Kucera, 2021	Integrated proposal	Real-Time Medical Data Analytics in the Covid-19 pandemic	Detection, monitoring, response to treatment
Sundaravadivel et al., 2017	Overview	Smart healthcare	Products, cost analysis
Taiwo & Ezugwu, 2020	Proposal	Remote patient monitoring	Covid-19, sensors, mobile application
Tian et al., 2019	Overview	Smart healthcare	Technologies
Tokognon et al., 2017	Proposal	Health monitoring framework	Big Data, sensors
Turner & Pera, 2021	Integrated proposal	Real-Time Covid-19 Detection	Big Data, wearable devices
Weng et al., 2019	Prototype	Blockchain based collaborative deep learning	Incentive mechanism, privacy, DeepChain
Yamashita et al., 2021	Prototype	Medical workers and objects tracking	Smart hospital, geomagnetic

			positioning algorithms, beacons
Yaqoob et al., 2019	Overview	Security vulnerabilities of networked medical devices	Attacks, countermeasures, regulations
Zeadally et al., 2019	Overview	Smart healthcare	Big Data analytics
Zhang et al., 2020	Integrated proposal	Diagnosis based on medical image analysis	Deep learning, cardiac monitoring, Big Data analytics

The second table lists selected references that entail the topics of privacy, safety and security. Its columns include the type of paper, the type of device/ network, the key issue(s) and core topics.

Table 2: References on privacy, security or safety

Reference	**Type**	**Devices/ networks/**	**Key Issue(s)**	**Topics**
AlTawy & Youssef, 2016	Overview	Cyber physical systems	Security Safety	Implantable devices, security tradeoffs
Dilawar et al., 2019	Integrated proposal	IoMT	Security Privacy	Blockchain secured IoMT architecture
Fang et al., 2020	Proposals	Smart hospitals network	Privacy	Data-sharing framework and access control mechanism based on watermarking
O'Connor et al., 2017	Proposal	General	Privacy	Informed consent and retraction/ modification of consent by digital citizens
Said et al., 2020	Protype	IoT in smart hospital	Security	Intrusion detection system based on support vector machines
Samanta et al., 2021	Prototype	Secure cloud services for medical data	Security	Improvements in strength to support vector machines based cryptography

The third classification includes selected papers in the area of machine or deep learning.

Table 3: Publications in the area of machine/ deep learning

Reference	Type	Specific tool	Mode of operation	Results
Abdulkareem et al., 2021	ML	Naive Bayes model Random Forest model Support vector machine model	Covid-19 diagnoses based on original and normalized datasets and feature selection	SVM model performance 95%
Ahmed et al., 2021	DL	Deep convolutional neural networks	Video analysis	True-positive 94% False-positive 7%.
Bhattacharya et al., 2019	DL	Deep long short-term memory model	Analysis and classification of electronic health records	Precision score: 0.7244, recall: 0.7078, obtained F1-score: 0.7118
Jia et al., 2022	DL	Deep long short-term memory model	Forecast multiple streams of healthcare timeseries data	Outperforms similar models for predicting daily patient visits, number of daily medical examinations and prescriptions
Mansour et al., 2021	ML	Cascaded Long Short Term Memory Model	Classification of medical data	Maximum accuracies of 96.16% and 97.26% in diagnosing heart disease and diabetes
Said et al., 2020	ML	Support Vector Machines	Intrusion detection/ rank attack	High detection accuracy, low false positive rates
Weng et al., 2019	DL	Trading and processing contracts	Collaborative deep learning	Fair incentive mechanism that encourages honest participation

The fourth table lists indicative proposals related to the Covid-19 pandemic.

Table 4: Publications related to the Covid-19 pandemic

Reference	Type of tool	Approach
Abdulkareem et al., 2021	Diagnosis system	Clinical decision support system based on machine learning and IoMT devices
Alyasseri et al., 2022	Overview of diagnosis models	Publications classification, public datasets

Maxwell & Grupac, 2021	Virtual care technologies	Artificial intelligence-enabled wearable medical devices, virtualized care systems, and wireless biomedical sensing devices for COVID-19 screening, testing, and treatment
Shamsabadi et al., 2022	Management of chronic disease	Using sensors and the IoMT to obtain data from chronically ill patients in the context of the Covid-19 pandemic
Stanley & Kucera, 2021	Integrated tool for detection, diagnosis and monitoring	Management of healthcare, AI-based diagnostic algorithms, real-time medical data analytics
Taiwo & Ezugwu, 2020	Remote smart home healthcare support system	Android application for doctor-patient communication + sensors recording physiological data + smart home features
Turner & Pera, 2021	Real-time detection and monitoring system	Integration of wearable medical devices data with clinical data leads to increased informed diagnostics and treatment decisions

The fifth and final table contains selected proposals that include Blockchain as storage or sharing mechanism.

Table 5: Publications incorporating Blockchain in an IoMT environment

Reference	**Other tools/ Implementation specific**	**Use of Blockchain**
Bhattacharya et al., 2019	Deep learning	Storing electronic health records
Indumathi et al., 2020	Encryption	Health information data exchange between patients and doctors, drugs management, Personal Health Records management
Jamil et al., 2019	Smart contracts	Drug supply chain integrity management, counterfeit drugs detection
Lakhan et al., 2021	Ethereum based proposal	Using a Blockchain-Enabled Smart-Contract Cost-Efficient Scheduling Algorithm Framework
Seliem & Elgazzar, 2019	Smart hospital	Lightweight Blockchain scheme consisting of a cloud server, network cluster, medical facility, and smart medical devices
Sharma et al., 2020	Smart contracts	Proposed architecture for the use of smart contracts in Blockchain based e-healthcare
Weng et al., 2019	Trading and processing contracts	Novel incentive mechanism for collaborating parties

7 Electronic health records management at a state level – A proposal

This chapter presents an integrated proposal for electronic health records management at a state level, having Greece as an implementation example. Several inherent challenges are discussed, along with potential solutions. The proposal is generally presented at a functional requirements and design level, but several technological implementation details are discussed, in the context of the Internet of Medical Things.

7.1 Current status & inherent challenges

A web application akin to an electronic health record manager was recently (in 2022) launched by the Greek government. The main focus of this application is online drug prescriptions but there are also records of hospitalizations, doctors' visits, diagnoses and future appointments. Authentication is based on accounts from the General Secretariat of Information Systems and additional one-time passwords sent via SMS in the prespecified and validated user mobile phone number. Data already in the application databases is limited both in the time domain (the exact time frame is not specified) and in terms of origin (generally from public sector health facilities), so its far from a complete Electronic Health Record (EHR). The major inherent challenges in the attempt to build and operate an EHR management platform at a state level are:

- **Security and privacy**: the very sensitive nature of the information contained in an EHR means that security and privacy need to be guaranteed in the system. Apart from being impervious to any form of attack, the system needs to have a flexible e-consent mechanism that allows an individual to consent and retract consent for a number of functions at any time.
- **Scale**: although Greece is a relatively small country, the scale of a platform at a state level is still daunting, especially if data from IoMT devices is to be included. Availability needs to be guaranteed, if health services are to rely on the platform for treatment, especially in emergency situations.
- **State of e-literacy of the population**: although the Covid-19 pandemic has forced Greeks to use online platforms and e-banking for operations previously

performed in person, the population is still relatively illiterate in electronic services, trust levels in such platforms are low and many are susceptible to fraud attempts.

7.2 Stakeholders – requirements

The EHR management platform will have several different types of users and there are many types of stakeholders. The main types of users will be:

- Patients. Includes adults and minors who are not managing their accounts on their own.
- Health professionals with varying levels of access (e.g. doctors are expected to have additional privileges compared to nursing staff).
- Administrative employees of public and private health facilities (related to billing functions).
- Researchers in various fields (medicine, biology, sensor devices, networks and many more). They need access mostly to anonymized data.
- Policy makers: they need access to aggregate statistics for audit and resources dimensioning purposes.

7.3 Volume of data - input methods

The volume of input data will naturally be very big and there are also issues related to time sensitivity, i.e., data needs to be updated, current and complete at all times in order to support medical decisions but these updates shouldn't take much of the doctor's time (for example). A potential solution for data input are speech to text tools and in particular deep learning tools in this category. Data dictated should be processed by specialized software to extract information for symptoms that correspond to diagnostic criteria according to international standards for classification of diseases (ICD), maintained by the World Health Organization. Additionally, lab and imaging results should also be incorporated into the EHR and potentially processed by other machine/ deep learning tools.

7.4 Distributed storage – processing

A centralized solution for the type of platform discussed in this chapter has many drawbacks. Having a single point of failure is a crucial vulnerability for the availability of the application as well as a target for malicious attackers. Therefore, a solution with distributed storage and control is preferable. Blockchain is a technology that offers many advantages in this direction that have been pointed out in preceding sections. The storage engine does not need to be in a single physical location and attention must be given to the backup policy as well. Replication and redundancy seem like natural solutions but they imply a high infrastructure cost.

7.5 Deep learning applications in EHR management

Many potential machine learning/ deep learning applications are worth implementing in an EHR management platform. Having complete health data on an individual enables "automated" diagnoses based on specific criteria and classification tools. Drug-drug interactions can also be investigated as the complete prescriptions history is also included. Prediction tools based on input data can make accurate assessments about the patient prognosis but also suggest and monitor therapeutic schemas.

When data from large numbers of patients is pooled together, it can drive research in several fields related to biology and medicine, especially after anonymization. Additionally, aggregate data can be used for administrative purposes and policy design, e.g., for dimensioning of resources (including human resources or staffing), automating processes and, of course, monitoring. Another very important potential application is fraud detection, where drugs, exams or procedures are prescribed to individuals that do not need them or could not possibly have them (for example, prostate exams on females).

7.6 Incentive mechanisms

Our envisioned platform will have many parties collaborating in the processing of the data, either at the stage before they are added to the main database, or afterwards, for research purposes. Examples of such parties may include, for instance, Greek universities. These parties need to be rewarded for their participation which involves using their own

processing and storage resources or, conversely, to pay for using state resources. The commodity in our scenario is the intermediate deep learning results (gradients), much like it is described in the incentive mechanism implemented in the context of DeepChain, described in Chapter 5 . In that collaborative deep learning network, parties were reward on the basis of the volume of data they provided, i.e. on data quantity. In our platform, we propose that the incentive mechanism be extended to consider the quality of data as well. Quality of data can be assessed on the basis of several parameters, such as the rarity of data (data on population segments that are under represented in the data pool), the originating device (data from particular sensors or exams may be more valuable) or the past results of the given party (if their previous data yielded worthwhile findings).

7.7 A working scenario

In a typical working scenario of our electronic health records management platform, a patient visits a regional state health care facility, such as the emergency section of a small hospital. The doctor, already having access to the platform via authentication when she started her shift, examines the patient and discusses his symptoms while having his detailed history available at a table provided by the hospital (the patient is identified via his social security number, which is unique). The patient is connected to a hearth monitor for an electrocardiogram, which is also recorded to be stored and processed by the system at a later time when the load is lighter. During the electrocardiogram, the doctor observes the signals and “takes notes” of patient condition and results by dictating on a recorder that converts speech to text. If there is an abnormality detected, the machine may also issue a warning. The doctor then prescribes some bloodwork via the tablet and the patient is forwarded to another department with his updated health record. The other department performs the tests and the original doctor sees the results on her tablet and prescribes medication for the patient who has left the hospital premises but receives notification of the prescription and instructions on his registered mobile phone.

Some time later, when the system load is sufficiently low, the audio dictation is processed by the EHR management system and the patient record is updated with the visit, medication and diagnosis. An agent detects that the combination of drugs the patient is now on, along with its demographics, fits the criteria for a running trial conducted by a

collaborating party on a research facility and alerts the facility about the new data. The facility volunteers to facilitate the processing of the electrocardiogram in exchange for any data that may be entered in the system regarding the patients next doctor visit, his future drug prescriptions, etc. Results from deep learning software processing the ECG are subsequently uploaded to the platform and both the doctor and the patient are notified, along with any insurance companies involved.

8 Comparison of proposed platform with existing approaches

In this chapter, we are highlighting, mostly using tables, the novel features of our proposed integrated platform for electronic health records management. The comparison is based on two recently proposed architectures combining deep learning and Blockchain, namely DeepChain [Weng et al., 2019] and BinDaaS [Bhattacharya et al., 2021], as well as the current systems for electronic health records management in Greece. We provide separate tables for each pair of systems under comparison and then we conclude with a sum up of the comparison outcomes.

Table 6 summarizes the comparison of DeepChain with our proposed platform. In essence, our platform includes all the features of DeepChain that enable collaborative deep learning while making improvements of the incentive mechanism which encourage participation of additional members and improve fairness. The scale of the two systems is also obviously different, ours being larger from the start.

Table 6: Comparison of our proposal with DeepChain

Feature	**DeepChain**	**Integrated Proposal**
Implementation/ Purpose	Collaborative deep learning	Collaborative deep learning for given projects and general knowledge extraction
Safety of data	Guaranteed by Blockchain	Guaranteed by Blockchain
Performance	Depends on collaborating parties	Also includes state server infrastructures
Collaboration	Parties work on a given project and share computing burden and results	Parties are free to collaborate as they please
Fairness	Members who contribute work obtain results depending on their contributions	Member contributions are evaluated more fairly (quality is also weighed)
Incentive mechanism	Based solely on data quantity	Also considers data quality
Accuracy of results	Validated by collaborative members	Validated by collaborative members and dedicated servers

Table 7 summarizes the comparison of BinDaaS with our proposed platform. Again, our platform includes all the features of BinDaaS that enable a deep learning application related to health data, such as the one described in the paper, but at a much larger scale and including actually creating the electronic health records.

Table 7: Comparison of our proposal with BinDaaS

Feature	BinDaaS	Integrated Proposal
Implementation/ Purpose	Blockchain based storing and processing of electronic health records	Collaborative deep learning for given projects and general knowledge extraction from health data
Safety of data	Guaranteed by Blockchain	Guaranteed by Blockchain
Security	Lattices-based cryptography	Can implement any selected method/ not restricted by processing power
Performance	Depends on the given infrastructure	Also includes state server infrastructures and collaborating parties (not limited to healthcare providers)
Collaboration	Parties work on a given project and share computing burden and results	Parties are free to collaborate as they please
Incentive mechanism	Members are working on the same project	Incentive mechanism to promote collaboration from members in different projects
Accuracy of results	Validated by collaborative members	Validated by collaborative members and dedicated servers

Table 8 is an attempt for a comparison between our proposal and the newly launched state information system for storing medical data. Apart from this state system, numerous physicians use typically web-based software systems to store and share patient data, with dubious security and privacy features and no data post-processing for information extraction.

Table 8: Comparison of our proposal with current state information system and privately used systems

Feature	Current systems	Integrated Proposal
Implementation/ Purpose	Storing patient data to maintain history between examinations	Collaborative deep learning for given projects and general knowledge extraction from health data
Safety of data	Depends on platform implementation, generally not guaranteed	Guaranteed by Blockchain

Security	State IS ids and two factor authentication for patients, separate registrations/ authentication for health professionals	Can implement any selected method/ not restricted by processing power
Performance	Varies significantly according to load	Uses additional servers (besides state ones)
Collaboration	Data is shared among health professionals	Parties are free to collaborate as they please
Types of data stored	Limited, text based data	Any form of data, including multimedia files
Post-processing	None, data validation is limited to input	Deep learning applications

To sum up the comparison, our proposed integrated platform essentially combines all the features of DeepChain and BinDaaS, while extending these proposals at the scale of a country, where both the infrastructure and the volume of data scale accordingly. Because of the proposed change in the incentive mechanism, even more parties are expected to collaborate. Current state information system for electronic health records mainly attempts to record basic data such as doctor's visits, prescriptions, hospital stays and operations, generally for auditing and regulatory reason. It remains to be seen if it will be extended in some form, with AI features added, and how well it will scale.

9 A deep learning implementation for natural language processing in electronic health records

In this chapter, we describe the functionality and the Python libraries involved in a deep learning application that can work on electronic health data to extract information and predict the likelihood of future disease. Once relevant data becomes available and publicized after anonymization, a prototype of the proposed application can be used to test its predictive accuracy.

Machine learning essentially involves solving a problem solving by instructing the computer how to learn from experience. This means that the software could reach a decision that could be right or wrong after performing a set of tasks and requires a dataset with potential for teaching and learning. Common tasks implemented by machine learning algorithms include classification and regression, ranking and clustering. Popular algorithms are typically based on statistics and regression, use decision trees, clustering and rule-based learning. Artificial neural networks (ANNs) are a distinctive class of machine learning algorithms with many applications in fields such as speech and audio (speech and music recognition and synthesis), image and video (image classification and object detection, visual similarity assessment, people recognition etc.). As it was outlined in our integrated proposal, several types of such applications could be integrated in the platform, for example, speech recognition ANNs for parsing dictations by doctors during patient examination, or image labelling for detecting abnormalities in ultrasounds or x-rays.

For a practical application, however, we chose to focus on the parsing of electronic health records using natural language processing artificial neural networks. Natural language processing (NLP) entails tasks such as text recognition and semantic parsing, machine translation, automatic text summarization, automatic paraphrasing, information retrieval and sentiment analysis (for example, in customer reviews). Popular indicative applications include text and document classification, e-mail classification and spam filtering, news filtering, native language identification and text or document similarity estimation.

Natural language processing tools typically perform some standard tasks at the beginning, aimed to clean up the original text for better and quicker results. Preprocessing

and parsing are performed before the original (native) text is handed over for computational handling in order to transform the original sequence of characters to a cleaner form. Tokenization involves splitting the text into self-contained semantic units such as words or sentences. Normalization is the removal of morphological variations from words such as capitalization, plural number or tenses in order to detect similarities in meaning while lemmatization involves using a preconstructed dictionary. Parsing can be described as the morphological and syntactical analysis of tokens in order to identify their role within sentences, i.e., the part of speech (noun, verb, adjective).

In natural language processing, word senses are the meanings of words, but many words have different meanings when used in different contexts and this is referrec as polysemy. Words and senses do not have a 1-1 matching as there are multiple words with the same meaning (synonyms). This implies that word-sense disambiguation may be required to identify the particular meaning of a word based on the way it is used in a sentence and its context. Another category of terms that require special treatment are named entities such as people names, organizations and geographical locations within the text. The basis of NLP are word embeddings which are mappings between words or phrases from the vocabulary and vectors of real numbers because they capture various linguistic properties of the text and enable feature extraction or feature encoding.

Bag-of-words (BoW) is a simple and popular method of feature extraction. In this approach, documents are viewed as containers where (for simplicity) the order of items does not matter. In this context, documents are similar if they have similar content and the meaning of the document can be extrapolated from its content. The basic BoW implementation considers unigrams, i.e., single words or tokens. n-grams use multiple consecutive words as tokens and thus change the size of the vocabulary to capture more meaning. n-gram models can be used to calculate probabilities for words based on the words already encountered on the basis of the assumption that each word depends only on the last n-1 words.

Another effective method of preprocessing involves using Term Frequency-Inverse Document Frequency (TF-IDF) to compute the importance of a gram for information retrieval. TF-IDF is the product of two factors Term Frequency and Inverse Document Frequency. Term Frequency refers to how often a given word appears in a document and is a measure of its importance. A very high frequency, though, in the entire corpus (set of

documents) means that it is a common word for the given topic therefore its score should be penalized. Inverse Document Frequency is calculated by counting the number of documents that contain a term and computing a ratio of the total number of documents divided by this value and then inverting. An important gram would have a high term frequency and a low document frequency of the term in the entire corpus (thus a high product). Common terms tend to have low weights and are filtered out. TF-IDF is often used for stop-words filtering for various applications such as text summarization and classification. Stop words are, for example, articles, propositions etc.

A fundamental functional in natural language processing is the discovery of word embeddings. The objective is to obtain vector representations of words based on the observation that similar/ related words tend to be close to each other in vector representations and similarity of word representations goes beyond simple syntactic regularities. A well known example of algebraic operations on word vectors is that the formula vector(“King”) - vector(“Man”) + vector(“Woman”) results in a vector that is closest to vector(“Queen”). Word2vec is a very popular open source software created by researchers in Google that computes distributed vector representations of words from very large data sets. Output: vector space with each word corresponding to a vector positioned in such a way that words that share common contexts in the corpus are close to one another. Word2Vec includes efficient implementations of Continuous Bag-of-Words and Continuous Skip-gram Models and can be used to predict surrounding words (context) given the current word.

Regarding programming tools with NLP capabilities, the Python programming language is the obvious choice, hence its popularity in the field. The Natural Language Toolkit (NLTK) is a Python set of libraries for symbolic and statistical natural language processing that also is Free and Open Source software and has built-in functions for tokenization, part-of-speech tagging along with dictionaries, thesaurus, array of stop words for several languages as well as visualization tools (parse trees). Gensim is free and open source vector space modeling and topic modeling toolkit implemented in Python that is widely used by researchers in related fields and companies.

As part of the NLP functions implemented in this thesis, we wrote and tested Python scripts that read the text of an article (we conducted tests with publications on long Covid), preprocess it with the methods described in previous paragraphs and then use the

Gensim doc2vec and word2vec models to parse it. It can then either locate similar documents (if we construct a corpus consisting of many papers) or calculate the similarity between two terms (distance in the document). In a larger practical application of the concepts described in previous paragraphs, out deep learning tool could be used to filter patients whose electronic health records indicate they were diagnosed with long Covid and analyze their EHRs to pinpoint symptoms of their condition that led to the diagnosis. Since we are discussing information recorded in the past, the results from the linguistic analysis of the electronic health records leading up to the diagnosis can be stored on disk and reused in future models. In such models, we could construct a tool that will guide physicians in new diagnoses of the same condition.

10 Summary and conclusions

This chapter summarizes the topics discussed in the thesis and presents potential future directions of research.

10.1 Summary

This thesis focuses on the Internet of Medical Things (IoMT) as the basis for implementing smart health. The IoMT is an environment where wearable or implanted medical devices with networking capabilities interact with base stations, mobile devices or other programmers to hand over their recorded data and receive instructions. The data captured is then stored in an appropriately protected storage infrastructure and used as a basis for treatment decisions or medical research. Following a concise introduction to basic terminology, we delved into the core challenges of the ecosystem, namely privacy, safety and security of the medical data and the devices operation in general. The confidential nature of health related information leaves no room for omissions when it comes to privacy and informed consent of the patient that can at any stage be revoked is the basic function that needs to be supported. It must be 100% clear to the patient which data is captured, where it is stored and who has access to it and what it is used for. Safety issues are related to how a medical device interacts with body tissues and are important concerns but mostly out of scope for this thesis while security involves such issues as attacks by malicious third parties which aim to compromise device availability, data confidentiality, normal operation and non-repudiation of transactions. Although security needs in the IoMT have a lot in common with traditional networks, there is an additional parameter/ mode of operation that requires extensive advanced planning that is unique in medical scenarios, namely emergency operation. In the case a medical emergency, all security features may need to be disabled so that physicians may have access to the device to treat the patient and such a feature needs to not only be in place beforehand, but not compromise the overall security of the implemented solution.

After the core ecosystem issues discussed in Chapter 3 , Chapter 4 presents the enabling technologies that can provide solutions. The two most important ones are Blockchain and machine/ deep learning. The inherent properties of Blockchain, namely the consensus needed by multiple parties in order to add information guarantee the

immutability, non repudiation and integrity of the data, as multiple culprits have to form a malicious alliance and this is considered highly unlikely. Furthermore, artificial intelligence tools can process the massive amounts of data stored in a Blockchain (or cloud) infrastructure to acquire knowledge, for instance related to new treatments, diagnoses or interrelations between conditions and medications. In this direction, several machine learning and deep learning tools/ frameworks have been proposed and are discussed in this thesis.

Chapter 5 presents three types integrated framework proposals in the context of the Internet of Medical Things. The first one is a relatively generic framework for remote patient monitoring focusing on the operation of the heart via an electrocardiogram signal. The second one is related to the Covid-19 pandemic and shows how technology can be used for functions such as cases and origin detection, quarantine monitoring and telemedicine. The final type of proposals presented is related to the combination of deep learning networks with a Blockchain storage infrastructure. The first solution is related to distributed deep learning to securely share the workload of training a model with large data sets while the second one presents a framework for storing electronic health records and provide authenticated access to all interested parties without compromising privacy and security.

Chapter 6 contains reference tables for current publications related to the Internet of Medical Things, listed in the References chapter of this thesis. The first table is a reference of recent (post 2017) publications while the second table lists papers on privacy, security or safety. The third table contains publications in the area of machine and deep learning while the fourth one lists papers related to the Covid-19 pandemic and the 5^{th} and final one includes publications incorporating Blockchain in an IoMT environment. Relevant information is provided in columns of each table, so as a researcher interested in delving in a topic deeper can easily find suitable papers to study.

Chapter 7 contains our approach at an integrated proposal for electronic health records management, at a country level, incorporating Blockchain and deep learning and providing an incentive mechanism for participants (health professionals and patients) which rewards contributions with results. This integrated proposal is then compared to existing deep learning over Blockchain proposals in Chapter 8, which also includes a comparison table with the current state information systems for electronic health records.

Lastly, Chapter 9 presents the functionality and the Python libraries involved in the implementation of a deep learning application that attempts to extract knowledge from patients' electronic health records. A specific application regarding long Covid is described.

10.2 Future research directions

Like every other new technology, the opportunities for further research in the field of smart health and the Internet of Medical Things are abundant. Virtually every issue discussed in this thesis is open for discussion, trials and, of course, standardization. In this section, we will attempt to highlight major issues whose resolution could give an extra boost to smart health applications.

One of the issues first encountered in the field is related to the challenges of device diversification and the heterogeneity of the environments in which they have to adequately operate. The number of devices deployed is expected to rise rapidly as more and more patients adopt mobile lifestyles and are reluctant to pay regular visits to specific locations. Ageing of global population is also an important concern as well as the possibility to support multiple devices on the same body and they way the will operate and interact.

Data security and privacy solutions are also fields for further research and standardization, especially in the field of informed electronic consent. Emergency operation/ overrides built in the devices is another required feature and, of course, implementing solutions at an affordable cost is also worthy of research.

Specialized machine learning/ deep learning tools designed specifically for medical data are another interesting research direction. Collaborative or distributed deep learning is a promising approach in this direction, as it seems very suitable for handling the large volumes of data. Incentive mechanisms inherent in such tools to encourage participating parties to contribute may also need to be studied and improved, for instance to not only consider quantity as a measure of a contribution (and thus reward), but also quality, as expressed by accuracy of captured data, rarity of demographic features of the patients and other factors.

11 References

Abdulkareem, K. H., Mohammed, M. A., Salim, A., Arif, M., Geman, O., Gupta, D., & Khanna, A. (2021). *Realizing an effective COVID-19 diagnosis system based on machine learning and IOT in smart hospital environment*. IEEE Internet of Things Journal, 8(21), 15919-15928.

Ahad, A., Tahir, M., & Yau, K. L. A. (2019). *5G-based smart healthcare network: architecture, taxonomy, challenges and future research directions*. IEEE access, 7, 100747-100762.

Ahmed, I., Jeon, G., & Piccialli, F. (2021). *A deep-learning-based smart healthcare system for patient's discomfort detection at the edge of Internet of Things*. IEEE Internet of Things Journal, 8(13), 10318-10326.

Albesher, A. A. (2019). *IoT in health-care: Recent advances in the development of smart cyber-physical ubiquitous environments*. IJCSNS, 19(2), 181.

Alqaralleh, B. A., Vaiyapuri, T., Parvathy, V. S., Gupta, D., Khanna, A., & Shankar, K. (2021). *Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment*. Personal and ubiquitous computing, 1-11.

AlTawy, R., & Youssef, A. M. (2016). *Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices*. IEEE Access, 4, 959-979.

Alyasseri, Z. A. A., Al-Betar, M. A., Doush, I. A., Awadallah, M. A., Abasi, A. K., Makhadmeh, S. N., ... & Zitar, R. A. (2022). *Review on COVID-19 diagnosis models based on machine learning and deep learning approaches*. Expert systems, 39(3), e12759.

Ben Ida, I., Balti, M., Chabaane, S., & Jemai, A. (2020, June). *Self-adaptative early warning scoring system for smart hospital*. In International Conference on Smart Homes and Health Telematics (pp. 16-27). Springer, Cham.

Bhattacharya, P., Tanwar, S., Bodkhe, U., Tyagi, S., & Kumar, N. (2019). *BinDaaS: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications*. IEEE transactions on network science and engineering, 8(2), 1242-1255.

Bigini, G., Freschi, V., & Lattanzi, E. (2020). *A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision*. Future Internet, 12(12), 208.

Camara, C., Peris-Lopez, P., & Tapiador, J. E. (2015). *Security and privacy issues in implantable medical devices: A comprehensive survey*. Journal of biomedical informatics, 55, 272-289.

Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., & Tarricone, L. (2015). *An IoT-aware architecture for smart healthcare systems*. IEEE Internet of Things journal, 2(6), 515-526.

Dai, H. N., Imran, M., & Haider, N. (2020). *Blockchain-enabled internet of medical things to combat COVID-19*. IEEE Internet of Things Magazine, 3(3), 52-57.

Dilawar, N., Rizwan, M., Ahmad, F., & Akram, S. (2019). *Blockchain: securing internet of medical things (IoMT)*. Int. J. Adv. Comput. Sci. Appl, 10(1), 82-89.

Ellouze, F., Fersi, G., & Jmaiel, M. (2020, June). *Blockchain for internet of medical things: A technical review*. In International Conference on Smart Homes and Health Telematics (pp. 259-267). Springer, Cham.

Fang, L., Yin, C., Zhu, J., Ge, C., Tanveer, M., Jolfaei, A., & Cao, Z. (2020). *Privacy protection for medical data sharing in smart healthcare*. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 16(3s), 1-18.

Forbes, 2022. Last retrieved, June 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/04/01/the-internet-of-medical-things-its-role-in-healthcare-and-how-to-implement-it/

Guinard, P. F. D. (2006). *Building a smart hospital using RFID technologies*. In European Conference on eHealth 2006. Gesellschaft für Informatik eV.

Habibzadeh, H., Dinesh, K., Shishvan, O. R., Boggio-Dandry, A., Sharma, G., & Soyata, T. (2019). *A survey of healthcare Internet of Things (HIoT): A clinical perspective*. IEEE Internet of Things Journal, 7(1), 53-71.

Hellenic Data Protection Authority (2011), *Directive 2/2011 Digital consent in the context of article 11, Law 3471/2006*. Last retrieved , October 2022, available at:

https://www.dpa.gr/sites/default/files/2020-01/2994_2_2011.PDF

Hossain, M. S., & Muhammad, G. (2016). *Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring*. Computer Networks, 101, 192-202.

Hussain, T., Muhammad, K., Khan, S., Ullah, A., Lee, M. Y., & Baik, S. W. (2019). *Intelligent baby behavior monitoring using embedded vision in IoT for smart healthcare centers*. Journal of Artificial Intelligence and Systems, 1(1), 110-124.

Indumathi, J., Shankar, A., Ghalib, M. R., Gitanjali, J., Hua, Q., Wen, Z., & Qi, X. (2020). *Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services* (BC IoMT U 6 HCS). IEEE Access, 8, 216856-216872.

Jamil, F., Hang, L., Kim, K., & Kim, D. (2019). *A novel medical blockchain model for drug supply chain integrity management in a smart hospital*. Electronics, 8(5), 505.

Jia, Q., Zhu, Y., Xu, R., Zhang, Y., & Zhao, Y. (2022). *Making the hospital smart: using a deep long short-term memory model to predict hospital performance metrics*. Industrial Management & Data Systems.

Isravel, D. P., & Silas, S. (2020, March). *A comprehensive review on the emerging IoT-cloud based technologies for smart healthcare*. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 606-611). IEEE.

Khan, M. Z., Alhazmi, O. H., Javed, M. A., Ghandorh, H., & Aloufi, K. S. (2021). *Reliable Internet of Things: Challenges and Future Trends*. Electronics, 10(19), 2377.

Lakhan, A., Mohammed, M. A., Rashid, A. N., Kadry, S., Panityakul, T., Abdulkareem, K. H., & Thinnukool, O. (2021). *Smart-contract aware ethereum and client-fog-cloud healthcare system*. Sensors, 21(12), 4093.

Mansour, R. F., El Amraoui, A., Nouaouri, I., Díaz, V. G., Gupta, D., & Kumar, S. (2021). *Artificial intelligence and Internet of Things enabled disease diagnosis model for smart healthcare systems*. IEEE Access, 9, 45137-45146.

Maxwell, S., & Grupac, M. (2021). *Virtual Care Technologies, Wearable Health Monitoring Sensors, and Internet of Medical Things-based Smart Disease Surveillance Systems in the Diagnosis and Treatment of COVID-19 Patients*. American Journal of Medical Research, 8(2), 118-131.

Moro Visconti, R., & Morea, D. (2020). *Healthcare digitalization and pay-for-performance incentives in smart hospital project financing*. International Journal of Environmental Research and Public Health, 17(7), 2318.

Naresh, V. S., Pericherla, S. S., Murty, P. S. R., & Sivaranjani, R. (2020). *Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions*. Comput. Syst. Sci. Eng., 35(6), 411-421.

O'Connor, Y., Rowan, W., Lynch, L., & Heavin, C. (2017). *Privacy by design: informed consent and internet of things for smart health*. Procedia computer science, 113, 653-658.

Qolomany, B., Al-Fuqaha, A., Gupta, A., Benhaddou, D., Alwajidi, S., Qadir, J., & Fong, A. C. (2019). *Leveraging machine learning and big data for smart buildings: A comprehensive survey*. IEEE Access, 7, 90316-90356.

Pan, J., Ding, S., Wu, D., Yang, S., & Yang, J. (2019). *Exploring behavioural intentions toward smart healthcare services among medical practitioners: A technology transfer perspective*. International Journal of Production Research, 57(18), 5801-5820.

Połap, D., Srivastava, G., Jolfaei, A., & Parizi, R. M. (2020, July). *Blockchain technology and neural networks for the internet of medical things*. In IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS) (pp. 508-513). IEEE.

Rayan, Z., Alfonse, M., & Salem, A. B. M. (2019). *Machine learning approaches in smart health*. Procedia Computer Science, 154, 361-368.

Rodrigues, J. J., Segundo, D. B. D. R., Junqueira, H. A., Sabino, M. H., Prince, R. M., Al-Muhtadi, J., & De Albuquerque, V. H. C. (2018). *Enabling technologies for the internet of health things*. IEEE Access, 6, 13129-13141.

Said, A. M., Yahyaoui, A., Yaakoubi, F., & Abdellatif, T. (2020, June). *Machine learning based rank attack detection for smart hospital infrastructure*. In International Conference on Smart Homes and Health Telematics (pp. 28-40). Springer, Cham.

Samanta, D., Alahmadi, A. H., Karthikeyan, M. P., Khan, M. Z., Banerjee, A., Dalapati, G. K., & Ramakrishna, S. (2021). *Cipher block chaining support vector machine for secured decentralized cloud enabled intelligent IoT architecture*. IEEE Access, 9, 98013-98025.

Sánchez, D., Tentori, M., & Favela, J. (2008). *Activity recognition for the smart hospital. IEEE intelligent systems*, 23(2), 50-57.

Seliem, M., & Elgazzar, K. (2019, June). *BIoMT: Blockchain for the internet of medical things*. In 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) (pp. 1-4). IEEE.

Shamsabadi, A., Pashaei, Z., Karimi, A., Mirzapour, P., Qaderi, K., Marhamati, M., & Dadras, O. (2022). *Internet of things in the management of chronic diseases during the COVID-19 pandemic: A systematic review*. Health Science Reports, 5(2), e557.

Sharma, A., Tomar, R., Chilamkurti, N., & Kim, B. G. (2020). *Blockchain based smart contracts for internet of medical things in e-healthcare*. Electronics, 9(10), 1609.

Silva, B. N., Khan, M., & Han, K. (2018). *Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable Cities and Society*, 38, 697-713.

Stanley, A., & Kucera, J. (2021). *Smart Healthcare Devices and Applications, Machine Learning-based Automated Diagnostic Systems, and Real-Time Medical Data Analytics in COVID-19 Screening, Testing, and Treatment*. American Journal of Medical Research, 8(2), 105-117.

Sundaravadivel, P., Kougianos, E., Mohanty, S. P., & Ganapathiraju, M. K. (2017). *Everything you wanted to know about smart health care: Evaluating the different technologies and components of the internet of things for better health*. IEEE Consumer Electronics Magazine, 7(1), 18-28.

Taiwo, O., & Ezugwu, A. E. (2020). *Smart healthcare support for remote patient monitoring during covid-19 quarantine*. Informatics in medicine unlocked, 20, 100428.

Tian, S., Yang, W., Le Grange, J. M., Wang, P., Huang, W., & Ye, Z. (2019). *Smart healthcare: making medical care more intelligent*. Global Health Journal, 3(3), 62-65.

Tokognon, C. A., Gao, B., Tian, G. Y., & Yan, Y. (2017). *Structural health monitoring framework based on Internet of Things: A survey*. IEEE Internet of Things Journal, 4(3), 619-635.

Turner, D., & Pera, A. (2021). *Wearable Internet of Medical Things Sensor Devices, Big Healthcare Data, and Artificial Intelligence-based Diagnostic Algorithms in Real-Time COVID-19 Detection and Monitoring Systems*. American Journal of Medical Research, 8(2), 132-145.

ul Huque, M. T. I., Munasinghe, K. S., & Jamalipour, A. (2014). *Body node coordinator placement algorithms for wireless body area networks*. IEEE internet of things journal, 2(1), 94-102.

Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., & Luo, W. (2019). *Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive*. IEEE Transactions on Dependable and Secure Computing, 18(5), 2438-2455.

Yamashita, K., Oyama, S., Otani, T., Yamashita, S., Furukawa, T., Kobayashi, D., ... & Shiratori, Y. (2021). *Smart hospital infrastructure: Geomagnetic in-hospital medical worker tracking*. Journal of the American Medical Informatics Association, 28(3), 477-486.

Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). *Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review*. IEEE Communications Surveys & Tutorials, 21(4), 3723-3768.

Yu, L., Lu, Y., & Zhu, X. (2012). *Smart hospital based on internet of things*. Journal of Networks, 7(10), 1654.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). *Internet of things for smart cities*. IEEE Internet of Things journal, 1(1), 22-32.

Zeadally, S., Siddiqui, F., Baig, Z., & Ibrahim, A. (2019). *Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics*. PSU research review.

Zhang, T., Sodhro, A. H., Luo, Z., Zahid, N., Nawaz, M. W., Pirbhulal, S., & Muzammal, M. (2020). *A joint deep learning and internet of medical things driven framework for elderly patients*. IEEE Access, 8, 75822-75832.