Internet of Things Based E-health Systems: Ideas, Expectations and Concerns

Mirjana Maksimović and Vladimir Vujović

Abstract Even the interaction between technology and healthcare has a long history, the embracing of e-health is slow because of limited infrastructural arrangements, capacity and political willingness. Internet of Things (IoT) is expected to usher in the biggest and fastest spread of technology in history, therefore together with e-health will completely modify person-to-person, human-to-machine and machine-to-machine (M2M) communications for the benefit of society in general. It is anticipated that the IoT-based e-health solutions will revolutionize the healthcare industry like nothing else before it. The rapid growth of IoT, Cloud computing and Big data, as well as the proliferation and widespread adoption of new technologies and miniature sensing device, have brought forth new opportunities to change the way patients and their healthcare providers manage health conditions, thus improving human health and well-being. The integration of IoT into the healthcare system brings numerous advantages, such as the availability and accessibility, the ability to provide a more "personalized" system, and high-quality cost-effective healthcare delivery. Still, the success of the IoT-based e-health systems will depend on barriers needed to overcome in order to achieve large-scale adoption of e-health applications. A large number of significant technological improvements in both hardware and software components are required to develop consistent, safe, effective, timely, flexible, patient-centered, power-efficient and ubiquitous healthcare systems. However, trust, privacy and security concerns, as well as regulation issues, identification, and semantic interoperability are pivotal in the widespread adoption of IoT and e-health together. Therefore, developing a climate of trust is one of the most important tasks that must be accomplished for successful e-health implementations. This chapter analyzes the ideas and impacts of

M. Maksimović (✉) · V. Vujović
Faculty of Electrical Engineering, University of East Sarajevo,
Vuka Karadzica 30, 71123 East Sarajevo, Bosnia and Herzegovina
e-mail: mirjana@etf.unssa.rs.ba

V. Vujović
e-mail: vladimir_vujovich@yahoo.com

S.U. Khan et al. (eds.), *Handbook of Large-Scale Distributed Computing in Smart Healthcare*, Scalable Computing and Communications,
DOI 10.1007/978-3-319-58280-1_10

IoT on the design of new e-health solutions and identifies the majority of challenges that determine successful IoT-based e-health system adoption.

Keywords Internet of Things · E-health · Expectations · Concerns

1 Introduction

Healthcare, as an essential human right, is in the interest of every human being and can be considered as fundamental for a functioning society. The research of healthcare systems' role and the importance in the quality of life and social welfare in modern society nowadays is broadly performed in order to help produce better decisions on policy design and implementation of healthcare systems at global, national and sub-national scales [6, 116]. Longer and healthier human's life makes the population more productive what implies the important contribution of health to economic well-being.

Healthcare systems and services in a new era in medicine and technology are essential for accomplishing the healthcare needs of individuals and populations. Thus, effective public health systems are designed to take care of the health of target populations which constant growth requires new, more advanced and efficient healthcare solutions [91]. To develop and evaluate innovative approaches for improving the quality of healthcare, innovations in the organization, funding, roles of health professionals as well as the use of technology, are equally important. With the present Information and Communication Technology (ICT) development, healthcare, as well as every aspect of human life today, has been revolutionized. In other words, the impact of technology in healthcare is immense—the rapid advancements in the ICT have changed healthcare systems locally and globally. Hence, a fundamental change over the last decades in both ICT and the medical sector, has switched the traditional view of health, where healthcare delivery has been designed around the provider (located in hospitals or clinics), to a new and multifaceted scenario, where the care goes to the patient, instead of the patient going to the care [38, 75]. The application of ICT to human health is one of the leading research goals for the 7th and 8th Framework Programs of European Union (EU). Beyond the technological factors, it is important to highlight that socioeconomic and political factors have also a significant influence on the evolution of digital healthcare (Fig. 1).

As can be seen in Fig. 1 healthcare is outstandingly affected by technological advancements [61]. Technological breakthroughs change healthcare in all its areas, creating a new vision of healthcare known as e-health. E-health with the help of ICTs creates novel opportunities for information distribution, interaction and joining forces of all participants in healthcare sector (the public, institutions, health professionals and healthcare providers). E-health, despite its social, political, ethical, technological and economic constraints, became a major part of a modern 21st Century society [38]. Development of new technologies, particularly the Internet

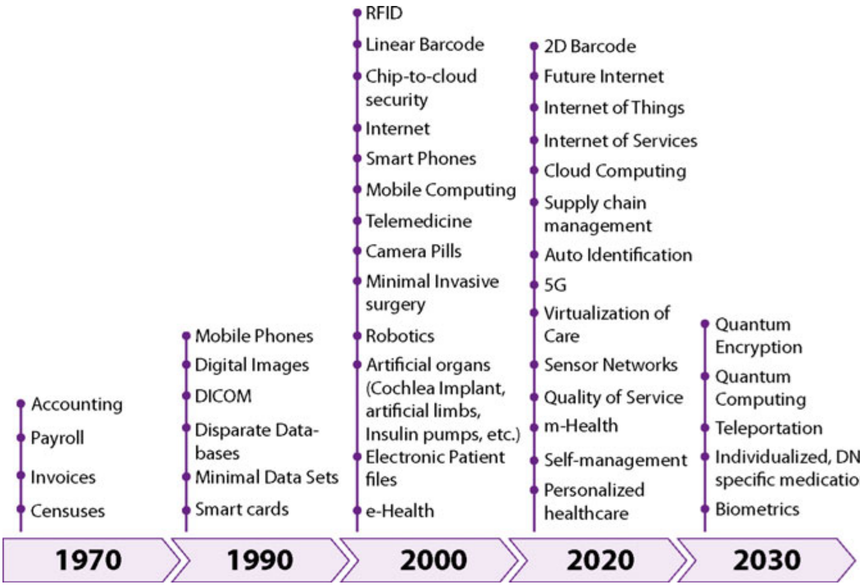


Fig. 1 Digital health evolution [36]

and Wireless Sensor Networks (WSNs) that together make the new unique concept called "Internet of Things" (IoT), has created a new horizon in the healthcare sector. As an emerging paradigm and a cutting edge technology, IoT connects the world via smart objects [56] and holds enormous potential for transforming the healthcare delivery system in the modern healthcare systems of 21st Century. Communications in IoT vision relates to communications among devices and objects, as well as among diverse devices (machine-to-machine (M2M) communications), supporting people daily patterns within a smart environment. These principles provide abilities to human to interact with various types of smart (intelligent) devices, converge and make applications, and commonly participate without outstanding interworking technologies [62]. It is considered that the IoT has greatest potential in the healthcare sector. This can be seen in many current healthcare solutions, which are already applied to enhance the availability and quality of care, and above all to avoid unnecessary healthcare costs and efforts. Using smart IoT devices, remote health monitoring and notification can be done easily, accurately and in a timely manner, what is essential in emergency cases [60, 103]. In theory, emergency admissions could be reduced with the help of proactive IoT-driven e-health systems which should be able to address the problems before they become more serious or irreversible. Relying on these facts, new concepts and technologies like network architectures, services, applications, interoperability, and security and privacy issues represent leading research trends in the IoT-based healthcare. In addition, there is a need for continuous work on legislation, policies, and guidelines in order to successfully implement the IoT principles in the medical field [59].

From an economic point of view, healthcare, as the global largest and fastest growing industry, is one of the areas that are expected to progress notably over years to come. McKinsey Global Institute [80] reveal prognosis and economic feasibility of the IoT-based healthcare. Figure 2 shows that by 2025 the highest percentage of the IoT incomes will go to the healthcare sector and hopefully will lead to fully customized, available, and on-time healthcare services for everyone.

Evidently, technology is increasingly playing a role in almost all healthcare processes, creating e-health services which provide better healthcare accompanied with improved availability, efficiency, responsibility and satisfaction of consumers. However, with the e-health industry growth more questions and challenges are faced in healthcare research. In other words, despite the potential of IoT-based e-health systems and services to improve the quality of healthcare, its wider uptake is hampered by a number of factors, such as the lack of access to capital by healthcare providers, resistance to change on the part of healthcare professionals and patients as well, standardization issues connected with security, privacy and confidentiality concerns, legal barriers and lack of technical skills.

To get as much as possible insights into the IoT role in progressive healthcare, this chapter examines the ideas and current impacts of IoT on the design of new e-health solutions and future directions for incorporating IoT into the clinical practice of medicine. It begins with a recapitulation of the literature, which includes the currently available systems on the market, as well as technological approaches for their implementation. A detailed analysis of the e-health system benefits, together with the objectives which must be fulfilled for their progress and significant improvement, are presented too. Relying on these objectives and modern technologies, a comprehensive analysis of applying the IoT in healthcare has been given. The study also includes the technological and methodological approach for the implementation of IoT-based healthcare systems. Alongside this, the IoT-based e-health system architecture was presented coupled with analysis of numerous recent studies that include the latest trends and challenges for integrating the modern technology in the IoT healthcare system. As a part of the performed research, benefits and expectations are especially highlighted, and challenges, risks and concerns which deal with various factors that have a direct or indirect impact on

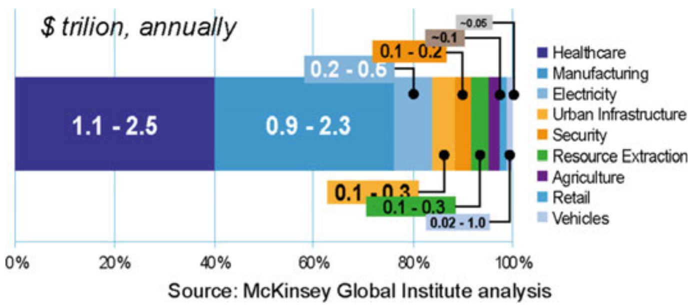


Fig. 2 The IoT leading applications and their economic impact in 2025 [55]

the implementation of IoT in healthcare are discussed as well. The chapter is concluded with summary representation of facts and includes SWOT analysis to evaluate the Strengths, Weaknesses, Opportunities, and Threats of presented concepts which determine successful IoT-based e-health system adoption.

2 E-health

E-health, as one of the results of the Internet expansion and appearance of e-terms during the 1990s, becomes an indispensable term which represents a mean of improving health services access, efficiency and quality by applying ICTs to health. Nowadays, e-health as a way of achieving healthcare reform represents one of the main research goals by many academic institutions, professional bodies and funding organizations. There are various currently used forms of e-health:

- Electronic Health Record (EHR)—an electronic version of a comprehensive report of the patient's overall health that make all information available immediately and in a secure way to authorized users [20],
- Electronic Medical Record (EMR)—a digital report that encompasses all of patient's medical history from one practice [50],
- Personal Health Record (PHR)—a health report where the patient keeps his health-related data in a private, secure, and confidential environment [70],
- Virtual healthcare teams and decision support teams—teams of healthcare professionals who cooperate, exchange information on patients through digital equipment with aim to improve their knowledge and make better decisions [40, 128],
- e-prescribing—a technology framework that allows writing and sending prescription electronically and directly from the healthcare institution to the pharmacy [20],
- e-appointments—an online service that makes scheduling an appointment for any health institution fast and easy, while reducing waiting time [135],
- m-health (mobile health)—a universal term that encompasses health practices enabled by mobile devices and other wireless technology [70, 74],
- Telemedicine—the ICT based remote delivery of healthcare information and services [51, 78, 131, 132],
- Telehealth—the distribution of health-related services and information via ICTs [25],
- Internet-based technologies and services, and more.

These are some of the many digital health technologies that serve to make easier the health-related data aggregation, storage, transfer, retrieval and processing; improve interaction between patients and healthcare providers; monitor various (biological and physiological) parameters, and ensure distant healthcare services [36].

Some of well-known intelligent pervasive healthcare systems, among others, are [86, 94, 125]: @*Home system* (enables remote monitoring of patient's vital parameters); *HEARTFAID* (enables on-time diagnosis and more effective insights in heart diseases within old people); *ALARM-NET* (an Assisted-Living and Residential Monitoring Network for ubiquitous, adaptive healthcare); *CAALYX* (Complete Ambient Assisted Living Experiment based on the usage of wearable lightweight devices that measure vital signs of a patient and automatically alert care provider in an emergency case); *TeleCARE* (enables the development of a configurable common infrastructure useful for the elderly people and the healthcare providers); *CHRONIC* (an integrated IT (Information Technology) environment for the care of chronic patients); *MyHeart* (with the help of smart electronic and textile systems and adequate services offers the means for dealing with cardiovascular diseases); *OLDES* (enables a wider range of services to old people using an innovative low-cost technology); *SAPHIRE* (implements the patient monitoring by using agent technology and intelligent decision support systems); *MobiHEALTH* (facilitates the online, continuous monitoring of vital signs, via GPRS (General Packet Radio Service) and UMTS (Universal Mobile Telecommunications System) technologies); *SAPHE* (allows intelligent, unobtrusive continuous healthcare monitoring via telecare networks with small wireless body sensors and sensors integrated in homes); *DITIS* (an e-health mobile application which supports networked collaboration for home healthcare); *AXARM* (an extensible remote assistance and monitoring tool for neurodegenerative disease telerehabilitation); *VirtualECare* (an intelligent multi-agent system for health monitoring and interacting with elderly people). The list of pervasive healthcare systems grows constantly along with the rapid advancements in ICTs and their widespread adoption can benefit patients, healthcare providers, managers and policy makers as well (Fig. 3) [2].

From a patient's point of view, e-health makes easier access to quality healthcare services through associated networked-monitoring equipment, particularly to

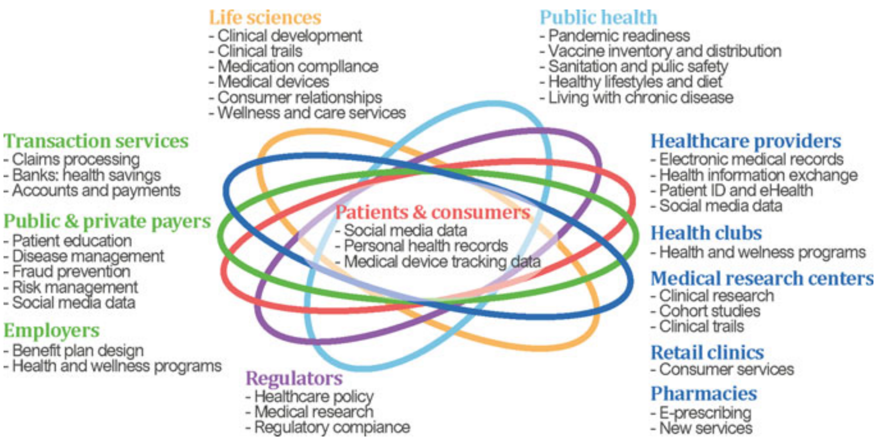


Fig. 3 The role and importance of participants in healthcare sector [2]

people in remote, rural and isolated communities. The old and less “physically” mobile patients, especially benefit from these health services over distance because they require fewer visits to the healthcare professional and institutions and thus they are more capable of living on their own. In the case of a potentially dangerous situation or detected anomalies (when dataset goes beyond the normal range, approaching to potential emergency), the system can generate an alarm [21]. Thus, e-health gives health professionals faster, secure access to all the data they need to care for the patient (Fig. 4). Recent surveys on patients' behavior to digital health (according to Frost & Sullivan) show that about 16% of them use wearable sensors, 24% use mobile applications to track their health and wellness, and 29% use electronic PHR. It is anticipated that this tendency will continue as 47% of patients would consider using wearable devices in the closest future [26]. The benefits of these self-monitoring devices are the removal of the need to run expensive and long tests as well as the realized connection with healthcare expert systems. These systems are essential in providing accurate information for diagnosis, decision-making, reducing medical errors and enabling prompt healthcare [91].

Since relevant health data are available to healthcare providers when required, e-health is seen as an opportunity to make healthcare more efficient by facilitating communication and enhancing patient care offering new services and types of treatments, alongside reduced delays, errors and administrative costs [47]. Multidisciplinary teams of health professionals, through e-health, have faster and secure access to all the information required to treat the patients in an adequate and timely manner. They can exchange health information and arrange health interventions in an effective way, thereby avoiding tasks duplications and cutting costs. Possible errors and complications, especially medication errors and adverse drug reactions, can be deflected through the role of e-prescribing systems. If an order is made for medications to which a patient is known to be allergic or there are potential contra-indications and drug interactions, this system flags alerts. Consequently, the less time is spent to clarifying and rewriting illegible prescriptions, and thus can be better used. However, Li et al. [71] identify and synthesize factors which influence healthcare providers' acceptance of e-health vision: healthcare provider characteristics (experience and knowledge in IT sector, gender, age, race, professional role and experience); medical practice characteristics (practice size and level, single or multi-specialty, location, teaching status, patient age range); voluntariness of use;

Fig. 4 The massive aggregation of healthcare data in the healthcare ecosystem

performance expectancy (the usefulness and needs, relative advantage, job-fit, payment and financial stimulus); effort expectancy (simplicity of usage and complexity); social influence (the subjective norm, competition, supportive organizational culture for change, and friendship network) and facilitating or inhibiting conditions (legal concerns, patient privacy issues, financial limitations, IT support). Having in mind that healthcare providers are the key enablers of e-health initiatives, their acceptance of e-health systems and applications is essential to reform and revolutionize healthcare.

Easy access, dissemination, use and exchange of accurate and reliable information, enable policy makers to made correct healthcare investment decisions (Fig. 4). In this way, health service interventions are conducted to where they are instantly required. Managers, through access to national health data summaries, can better supervise and evaluate health intervention programs.

Therefore, e-health has many benefits to offer. Organizations and governments worldwide are choosing to implement e-health in order to enhance quality of care as well as the patient experience. The major benefits can be summarized in [65]:

- Technology usage effectively saves time (increased timeliness of treatment and decreased transfer rates) and eases financial pressures.
- Quality of care is enhanced through more informed decision making processes. Diagnoses are on-time and more accurate.
- Online healthcare services are provided for members, employers, providers and brokers. Wireless devices' usage enables real-time treatment, while telemedicine and remote in-home monitoring support senior wellness and preventative care, as well as expert diagnosis and treatment to rural residents. Remote consultations, whether urgent or diagnostic saves lives.
- Delivery of care is more efficient, cost-effective and convenient. Customer experience is more satisfied while staff and doctor satisfaction is also improved.
- ICTs usage can enable health processes to cover more cases without raising staff numbers or related costs. Thus, costs are reduced and administrative efficiency and coordination are improved.
- Revenue cycle management is speeded through electronic payment technology.
- Enhanced access to a patient's health information decreases the incidence of medical errors.

As can be noticed, e-health is rapidly growing and changing and owns the enormous potential to improve the quality and efficiency of healthcare. However, its widespread use is obstructed by a number of barriers, ranging from technical to financing to political issues (Fig. 5) [30].

As technology is rapidly changing, new e-health solutions are constantly progressing to satisfy the needs of current practice. Appropriate technology infrastructure, systems integration, standardization as well as social, ethical, and economic questions, represent the main challenges for ubiquitous e-health adoption and achieving higher quality and more productive healthcare. To achieve healthcare

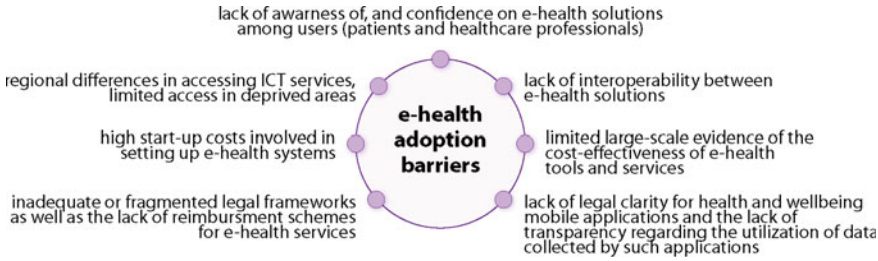


Fig. 5 The major barriers to wider uptake of e-health

improvements, it is recognized that every healthcare system should accomplish next six goals [57], Steinwachs and Hughes (2008):

- *Patient safety*—includes the prevention of errors and adverse effects to patients associated with healthcare. To accomplish this goal, it is necessary to perform certain actions such as correct identification of the patient, enhancing communication, enabling adequate care and reducing the risk of undesired outcomes.
- *Effective care*—is based on scientific evidence (laboratory experiments, clinical research, epidemiological studies…) that treatment will lead to desired health outcomes.
- *Timeliness*—considers that healthcare organization should be organized to provide care to patients in a timely manner. Although occasionally harmless, a misdiagnoses or failure to timely diagnose a medical condition, illness, or injury could lead to worsening of the condition and outcomes to worsen.
- *Efficiency*—is based on identifying and eliminating waste of resources (equipment, energy, supplies and ideas).
- *Patient-centered* healthcare—involves the creation of individualized healthcare services according to the patient's needs, values, and preferences.
- *Equity*—means providing the same quality of care regardless of personal characteristics such as gender, race, education, geographic location, and socioeconomic status.

These six goals represent a guideline for creating a contemporary, Internet-based healthcare system, and in the rest of this chapter a discussion will show their significance.

3 The IoT Based E-health Systems and Services

In the past, sensing in the healthcare was applicable mainly in healthcare institutions, and rarely outside of hospitals. Additionally, sensing unit at an early stage, were simple devices for measuring parameters of interest and creating some form of the output signal (mechanical, electrical, or optical). Nowadays, a development of

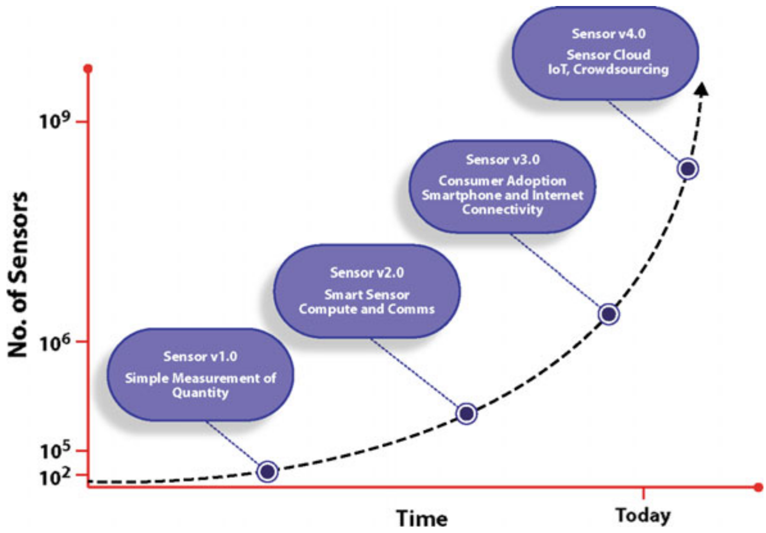


Fig. 6 Evolution of sensors [79]

computing and pervasive communications, connectivity to the Internet and Cloud integration as well as use of mobile smart devices, have added outstandingly to the capabilities of sensor devices, their number and scope (Fig. 6) [79].

Society is currently witnessing ICT influences on the evolution of sensors and their applications which can be almost everywhere: from health and fitness, aging demographics, personalized healthcare, public health, national security, IoT, water and food traceability and production. Consequently, using new concepts and approaches like IoT, Big data and Cloud computing, novel healthcare solutions have a huge potential to easily meet all of six improvements goals.

IoT-powered healthcare systems of 21st Century rely on the fundamental definition of the IoT as a network of intelligent, interconnected devices (which are usually equipped with microcontrollers or microprocessors, memory, wireless transceiver, sensing unit and autonomous power supply) based on existing and evolving interoperable ICTs [56]. To realize the integration of IoT principles in e-health, a variety of sensors (wearables and ingestible devices) gather patient's health-related data; microcontrollers process and wirelessly transmit those data; microprocessors provide user interfaces and displays while healthcare-specific gateways and the Cloud are used to analyze and store the data. The analyzed data are then transmitted wirelessly to medical professionals for further medical analysis, the remote control of certain medical treatments or parameters or real-time feedback [69, 89, 121].

To continuously monitor several vital signs of patients and transmit the data to the server, different health sensors either embedded in some device, like a smartphone, or wearable by users, are utilized. Ideally, the chosen sensors should be invisible, unobtrusive and non-invasive, able to protect user privacy and data confidentiality, to consume low-power and demand minimal computational resources, to be cheap and easy to install and have low-maintenance overhead [130]. For example, various sensors like temperature sensors, voice-sensors (microphone), video sensors, image sensors, IR (infrared) sensors, optical sensors, ultrasonic sensors, piezoelectric sensors, accelerometer, and more, can be used to address the same or different problems (fall detection, child care, disabled care, etc.) [120]. Connecting diverse medical devices (e.g., thermometers, glucometers, smart heart rate monitors, fitness tracking device, blood pressure cuffs, asthma inhalers, etc.) creates a new paradigm commonly referred the "Internet of Medical Things" (IoMT) [108]. To allow synchronization of the real world with its virtual representation and therefore enable enhanced process and decision-making support, these smart objects used for medical purposes should be unique in its context or system (to have an identity), have abilities to gather the information and to interact with environment (sensors and actuators), determine the current position, communicate with other objects, store data (memory) and act autonomously to accomplish a predefined goal [127]. Relying on these principles, according to report by the Atlantic Council [44] a four categories of medical devices led by IoT concepts are identified: consumer-based (e.g., fitness tracking devices), wearable, external devices (e.g., insulin pumps), internally embedded devices (e.g., pacemakers, within the body sensors) and stationary devices (e.g., home-monitoring devices, IV (intravenous) pumps and fetal monitors). These four categories of medical devices may be considered as the foundation of any modern healthcare system nowadays.

With the rapid technological advancements, the new generation of "medical" or "clinical wearables" has more advanced performances in the sense of sensing, capturing and analyzing, making them more clinical useful [76]. Using a new type of networks, various communication technologies like GSM (General System for Mobile communication), RFID (Radio Frequency Identification), GPS (Global Positioning System), Bluetooth, Wi-Fi, ZigBee and NFC (Near Field Communication) for interconnecting wearable health sensors, and transferring sensor data to the central server [100, 120] enables making the human body as a part of the IoT, bringing in such way integration to a completely new level. Following these principles, in the next few years it is expected that the 5G network, with its superfast connectivity, intelligent management, and data capabilities, will provide new possibilities in healthcare, including diagnostics, data analytics, and treatment [126]. More specifically, the IETF (Internet Engineering Task Force) has standardized 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), ROLL (Routing over Low power and Lossy-networks), and CoAP (Constrained Application Protocol) to equip constrained devices used in IoT vision [72].

How to deal and process a large amount of gathered data is one of the biggest challenges in present healthcare systems. The large quantity of data is usually stored in the Cloud where they are reachable worldwide, by a virtually unlimited number of participants, even simultaneously. Private information of a patient, are usually accessible to himself and to the healthcare givers but they are also anonymously available to anyone, so that can be effectively aggregated for research or statistical worldwide analysis [38]. A variety of techniques, such as artificial intelligence, machine learning, intelligent data mining, computer vision, Big data and analytics and more, are used to discover hidden patterns, anomaly detection, perform predictive modeling and to make actionable decisions. In this way, using smart devices equipped with evidence-based algorithms increase the possibility to significantly reduce the number of medical errors. Alongside this, information regarding health should be always accessible to both healthcare provider and patient in the most understandable formats for each [42]. In order to understand the life cycle of the device, researchers propose the usage of six C's: Connection (the path showing how device is connected to the ecosystem); Collection (how data are collected from the sensing element); Correlation (mapping the data to a context and perform correlation to produce relevant and concise data); Calculation (making a decision based on filtered and processed data); Conclusion (taking appropriate actions); and Collaboration (the patient and the healthcare teams' work together). Relying on six C's definition, the architecture for e-health must support diverse devices, applications, and backend systems to enable the free information flow (satisfying the needs of six C's life cycle) in order to make on-time and right decisions [69]. Therefore, gateways, medical servers, and health databases, are crucial in making medical records and bringing health services to authorized stakeholders whenever required [59].

The elements defined above for gathering, storing, transmitting and analyzing data are essential regardless of different technologies and architectures of IoT healthcare solutions that can be found in a review of literature [4, 21, 46, 82, 84, 86, 90, 93, 97, 104, 110, 134]. In addition to technology, that creates the capacity to provide health services, the structure of healthcare also includes the facilities (e.g., hospitals and clinics) and personnel (e.g., physicians and nurses) [109]. Enabling simple and cost-effective collaboration of patients, hospitals and healthcare organizations, via smooth and secure connectivity, is a significant trend [59].

The representative cases of IoT/IoMT include remote monitoring of people health (chronic or long-term conditions); tracking patient medication orders and the location of patients admitted to hospitals; and patients' wearable mobile health devices, which can send data of interest to healthcare providers. In other words, nowadays the Internet and smart mobile devices provide a quite simple interactive environment for all, fulfilling the principles of IoT-based e-health: to enable anyone to access e-health services anytime, anyplace and on any device (Fig. 7). Mobile medical devices (e.g., wearable sensors, bands, watches) and smart applications facilitate continuous self-monitoring of various vital parameters while Cloud-based architectures enable storing and sharing large amounts of data in an effective and easy manner [19]. Therefore, the presented architecture consists of three basic layers:

- Sensing/perception layer: the most basic layer which key component is sensing device for capturing and presenting the physical in the digital world. The essential data sensing/gathering from sensing devices and some controlling actions and communications are the main functions of this layer.

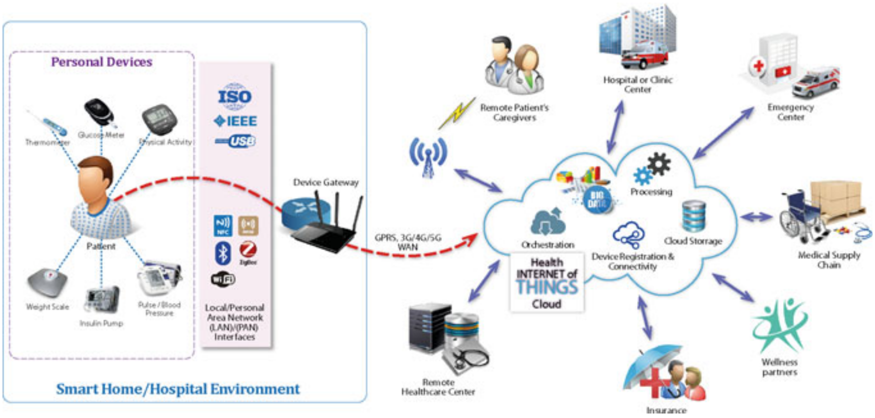


Fig. 7 The IoT-based e-health system architecture

- Network layer: the middle layer which includes all kinds of access networks, protocols, communication devices and routing modules.
- Application layer: includes operating modules for analyzing sensed data, computation, and actions.

Bearing in mind the importance of new healthcare solutions, a variety of recent studies accentuate tendency and challenges for ubiquitous health technologies in the IoT. Over the last years, academic researchers have paid increasing attention to this field, proposing numerous more or less similar solutions, based on the basic three layers IoT architecture, highlighting: the usage of smart, intelligent, wireless sensor devices to perceive utilization of the appliances necessary for daily living and in this way determine the lifestyle of old people living alone [41, 83, 112]; an IoT low-cost technology solution for observing human vital parameter [76, 97, 111, 114]; a simple and secure IoT for creating a general and pervasive Ambient Assisted Living framework to be used by m-health applications [37, 41, 74, 103]; IoT-based e-health solutions, creating a M2M system based on a Cloud computing [102, 110, 123], and more. In addition, one of the most important trends in 2015 became the development of Do It Yourself (DIY) healthcare platforms [24]. With the help of inexpensive hardware and open-source software, a DIY system which satisfies the user's specific needs can be easily created. The created solution can be used to monitor human vital parameters as well as some of the environmental parameters affecting health. Providing techniques and the customizable solutions to the consumers is valuable for both end-users and product developers [76]. Some of the IoT e-health solutions currently present on the market are [105, 115]: *Empatica Embrace* (a sleek watch that collects data regarding to epilepsy, autism and other chronic disorders, makes it available to caregivers and creates alerts in case of emergency); *Lumo Lift* (a discreet lightweight wearable that tracks patient's posture and activity); *Philips Respironics* breathing masks and *SleepMapper* application (an interactive self-management system that tracks user's sleeping patterns); *Chrono*

SmartStop (a wearable lightweight transdermal device that relies on nicotine replacement therapy); *Real Time Healthcare* (a platform that helps the patient follow their medication routines, informs healthcare professionals about important information, including location details if the patient becomes confused and lost); *Scanadu Scout* (an electronic device which enables quickly check of patient's vital signs by placing the device on patient's temple); *iOTOS* (a wireless device which have possibility to be integrated in all kinds of devices used from diagnostics to home monitoring). At the hospital side, it is important to highlight [105]: smart IV pumps (intelligent infusion devices which can preset doses and have ability to communicate with electronic medication administration records); robotic-assisted surgery; wireless capsule endoscopy (as an alternative to the tube-based endoscope where the patient swallows camera in a pill and it moves through the gastrointestinal track taking pictures); tracking medications administered to patients and assets via RFID. Based on currently available IoT-powered healthcare solutions, Islam et al. [59] categorize services (used to develop applications) and applications of IoT in healthcare sector (Fig. 8), where applications are further classified into two groups: single- (a specific disease or infirmity) and clustered-condition applications (a number of diseases or conditions together as a whole).

Despite the way IoT-based e-health systems are realized, they all should provide the effective and efficient healthcare for anyone, anytime and anywhere. Therefore, regarding data, the IoT-driven e-health solution must:

- Collect patient health data from a various types of sensors remotely and in a secure and safe way,
- Apply complex algorithms from a broad scope of pattern recognition and machine learning techniques, to analyze the gathered data, and
- Exchange the data through wireless networks (satisfying privacy and security demands) with who can make real-time feedback.

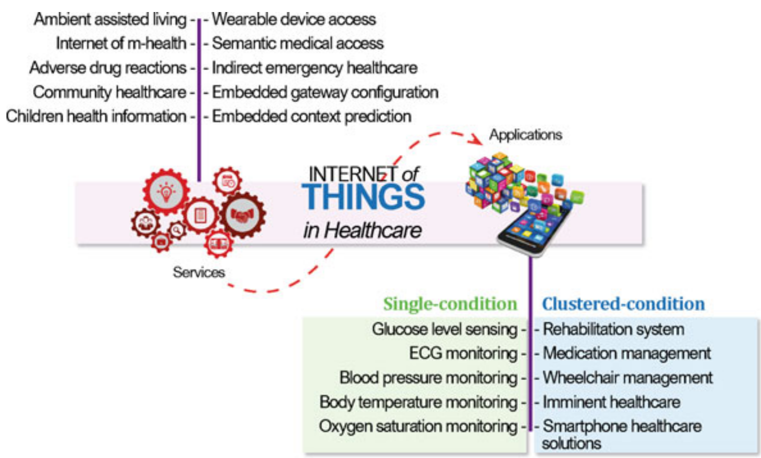


Fig. 8 Services and applications of IoT-powered healthcare

As ICT is used to support the core processes of healthcare, in the first step a prodigious amount of data has been produced. Due to datasets volume, variability, and velocity, there is a need to filter out relevant, differentiating information from the voluminous datasets. This implies a quick growth of Big data analytics, which gives an opportunity to healthcare organizations to improve care and profitability. With the limitless potential to effectively store, process and analyze medical data, the Big data in healthcare are being applied in many prevention and personalization purposes. In other words, successfully dealing with a huge volume of data can improve profits, and effectively reduce the cost of healthcare. Furthermore, the rapid development of IoT healthcare is accompanied with the increased risk of security and privacy. Therefore, security and privacy are crucial design goals that should be taken into consideration. To receive as much as possible benefits of the IoT-based e-health system, devices must connect to networks and the Cloud in ways that are interoperable and secure. It implies that generated, assembled, and shared data must be protected with appropriate authentication methods. The additional important factor is the data access control, which prevents unauthorized accesses to the patient's data. Healthcare providers and patients will be able to experience the advantages of digital modernization for wellness and healthcare only satisfying essential demands for IoT-driven healthcare system development and Quality of Services (QoS) requirements. In order to measure QoS of IoT-based e-health system, various QoS parameters and QoS metrics must be considered. They can be classified according to three layers' structure of IoT [13]:

- Sensing/perception layer: reliability, throughput, real-time, sampling parameters, time synchronization, location/mobility, sensing and actuation coverage.
- Network layer: lifetime of sensing networks, utilization of network resources, bandwidth, delay, packet loss rate, jitter, services perform cost, perform time, load, reliability, fault tolerance.
- Application layer: service issues (time, delay, priority, availability, accuracy, load), information accuracy, costs (network deployment, service usage).

As tracking, identification, authentication, data collection and sensing are essential characteristics of IoT-driven e-health, among various QoS metrics, several of them can be considered as of special interest in IoT healthcare applications: reliability, throughput, delay, energy consumption, system lifetime, network coverage, packet loss rate, scalability. However, QoS support provided in IoT-based e-health systems varies and targets different QoS levels for specific uses (e.g., emergency case, intensive care).

In summary, using smart IoT devices, comprehensive physiological information is collected and shared directly with each other and the Cloud, enabling to gather, store and analyze a mixture of health status indicators faster and more accurately [89]. Therefore, the idea of IoT-based e-health solutions is to accomplish all six goals for health improvements and QoS requirements, by enhancing life quality, providing medical support and life-saving care, decreasing barriers for monitoring important patient health data, reducing the cost of care and providing the on-time and right prevention and treatment.

3.1 Benefits and Expectations

New approaches to the procedures, equipment, and processes by which medical care is delivered have led to impressive achievements in health worldwide during the past few decades. With the power of ICT, healthcare becomes more efficient as well as cheaper and more reliable. In e-health, the IoT's connectivity provides means to monitor, record and transmit health data on a 24/7 basis from a patient home to the healthcare providers (using sensors in mobile devices, within bodies sensors or sensors attached to clothing) and enable the IoT-related data and services to be pervasive and personalized [97].

The IoT-powered e-health systems, using small, lightweight wireless approaches connected through the IoT, have potential to enable remote monitoring and secure capturing of a great wealth of patient health data and fitness information. In other words, medical devices such as wearables and home health monitoring devices (e.g., wirelessly connected thermometers, glucometers, heart rate or blood pressure monitors) can be connected to the IoT technology enabling remote, timely and comfortable monitoring of patient's vital signs from a hospital environment. The device which uses the IoT scheme is unique to the world and identifiable at anytime and anywhere through the Internet. The IoT-powered health devices in distance health monitoring systems, alongside the traditional sensing tasks, can also share health-related data with each other, as well as with hospitals or clinics through the Internet, outstandingly facilitating setup and administration work [49]. The collected health information, stored in a central data server, can be intelligently analyzed to identify patterns and trends and represents a basis for the statistical and epidemiological researches (e.g., disease and epidemic outbreak prediction, tracking and controlling in an efficient manner) [97]. Using gathered information and applying complex algorithms and evidence-based models in order to perform certain actions, significantly improve health by enhancing the access to healthcare and quality of care alongside drastically costs cutting (Fig. 9).

The most promising IoT-based e-health use cases are preventive health actions, proactive monitoring, follow-up care and management of chronic care diseases. The benefits of IoT-driven e-health as a technique to improve the quality of healthcare are recognized worldwide. Opposed to traditional paper-based practice and expensive physical interactions between healthcare givers and patients, the IoT-based e-health solution provides a faster, easier and cost-effective ways to accessing healthcare [119]. The important modifications that IoT has already brought in diverse areas of healthcare are noticeable in [15, 93]:

- Patient tracking, monitoring and diagnostics (e.g., preventive care, monitoring patient's health, chronic disease self-care),
- Sharing and recording health-related data, and collaboration,
- Smart healthcare devices and tools (e.g., smart wheelchair, sensors),
- Cross-organization integration (e.g., connected emergency units, response vehicles, and healthcare institutions).

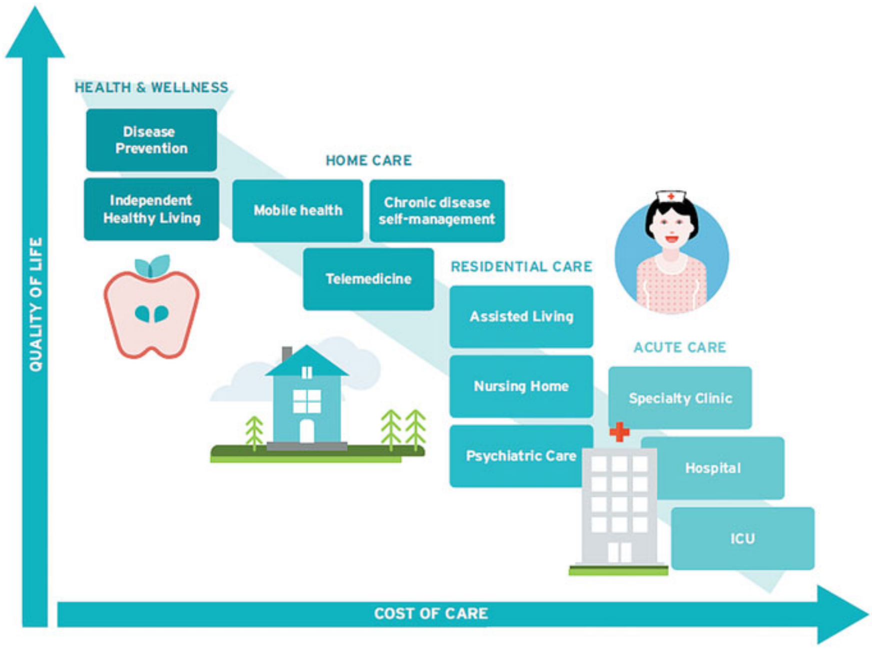


Fig. 9 Improved quality of life followed with reduced cost of care [75]

To develop a successful IoT-driven e-health system, it is necessary to satisfy following demands:

- To effectively manage healthy living, the system must be unobtrusive and comfortable as possible and available 24/7.
- Ubiquitous technology should be used for sensing, monitoring, analyzing, and communicating. Telemedicine advancements, videoconferencing and the IoT, provide means for monitoring patients' health at home, virtually from anywhere. Therefore, using digital communication technologies and virtualization, the appropriate healthcare can be provided anytime and anywhere.
- Any medical device (wearable or portable) must be connected to the Cloud, pulled and be capable of analyzing a vast range of collected health markers of a patient in real time and to identify important signs of possible health risk.
- The connected devices must be able to speak the same language using protocols and collaborate with each other without human involvement. Connected devices should be ubiquitous and a programmable platform.
- Monitoring of vital health indicators collected by portable devices (e.g., smartphones and tablets) must be realized. The data gleaned from the smart IoT devices are used by healthcare professionals to figure out who needs the most hands-on attention and to help diagnose the patient so they can get the best treatment as quickly as possible. Data collected from health monitoring devices

should be visualized in easy understandable charts and diagrams. Thus, providing visualization of the voluminous data and analysis results accessible to healthcare practitioners in an understandable and adjustable format, regardless of the underlying development platform, are essential.

- Shifting reactive treatment towards precise, predictive and preventive should significantly reduce the number of alerts. In the case of emergency (when any abnormality is detected) intelligent notifications must be enabled and sent to a caregiver.
- The growth of medical devices at a hospital and clinical side requires stabilization of existing wired and wireless infrastructure as well as pervasive Wi-Fi connectivity and bandwidth for clinician workflow and communications. Automated and secure provisioning and control of medical devices on the wired/wireless network, staff supporting and consulting, and technical support 24/7 are mandatory.
- Authorization processes, data exchange and privacy must be compliant with EU Data Protection Directive (Europe) or HIPAA (Health Insurance Portability and Accountability Act) in the USA (United States of America) as well as national regulations [88].
- Reduce costly and unnecessary medical services.
- Deliver personalized experiences to users, which meet their specific needs through flexibility, convenience and technologies.
- Scaling sensors down to the nanoscale, and reduce energy consumption.

Remote monitoring, real-time monitoring and online medical consultations are major benefits patients experience in the IoT-driven e-health vision. These benefits are the consequence of growing number of technological solutions aimed to help save lives and improve the health of humans on a global scale. With the help of such IoT-powered e-health systems, patients better understand their health status and much more participate in the healthcare decisions affecting them. An active participation ensures their well-being through access to a summary of their health information (from anywhere), giving them more insight into their health by tracking of their medications, immunizations and allergies. It is believed that web portals, the Internet and social media, improve access to health-related information [19]. Using the IoT-based e-health systems and services the point of care is shifted towards patients, placing the patient in the center of the treatment process followed with the reduced demand for physical contact between patients and healthcare givers [36]. Moreover, in the IoT-based e-health system, where smart (intelligent) devices can bring decisions and perform actions without human intervention, impact of racial bias and any kind of discrimination in healthcare (income, gender, age, education, race, etc.) patient can face with health professionals or anyone else can be minimized [42]. Hence, with the help of the IoT-driven e-health patients can receive better and safer healthcare, anywhere and at any time as needed by them. Fast and more quality healthcare is based on more complete patient information availability. The IoT nature of e-health systems enables data exchange between smart devices as well as between devices and health institutions and professionals automatically through the Internet. Collected and analyzed data facilitate fast and safe treatment decisions. Some of the benefits healthcare professionals achieve are: remote access to the patient chart; identifying necessary laboratory tests; being alerted in case of critical laboratory values or possible medication errors; being reminded to provide preventive care, facilitated direct communications with patients as well as the ability to cope easier with increases in patient numbers. To point out, the IoT has potential to revolutionize how healthcare is delivered and operationalized, by radically reducing costs and improving the availability and quality of healthcare by focusing on the way all participants in healthcare processes, devices and applications are connected and cooperate with each other. Currently applied IoT-driven e-health applications already show the tremendous benefits IoT brings to health services.

Maximization of socioeconomic benefits through the implementation of e-health systems is a goal of the new European e-health Action Plan for the period 2012–2020. It defines the vision for novel healthcare for the 21st Century where physicians will spend more time with their patients and reduce unnecessary administrative tasks. According to the plan, during the period 2014–2020, research and innovation will be supported in the field of IoT in order to develop digital, personalized and predictive, patient-centric and cost-effective healthcare, focusing on the embedded and cyber-physical systems, operating platforms, network technologies, semantic interoperability, and security and privacy issues [30]. Moreover, by 2020, it is expected that shrinking sensors to the nanometer scale will imply nanotechnology widespread use and its involvement in every aspect of life. Embedding nano-devices in the environment creates a new vision—the "Internet of Nano Things" (IoNT). The IoNT in the field of medicine creates a new term—"nanomedicine", which has potential to make diagnoses and treatment less invasive and more intelligent. The elimination of many invasive procedures will be realized with the help of smart pills and nanoscale robotics. Beyond numerous benefits nanomedicine has to offer, big challenges will have to be met: the linkage of the nanoscale networks to the Internet, communication issues between the nano- and micro networks, privacy and safety issues, potential toxic and hazardous effects of nanoparticles, generation of large amounts of data, etc. [91]. Nevertheless, the use of nanotechnology in medicine opens a whole new world of exciting possibilities, and it is expected to revolutionize the healthcare over decades to come.

Beyond the technical/scientific factors, it is important to address and non-technical challenges of different nature, such as socioeconomic challenges during the IoT domains and technologies' progress [36]. Hence, the incredible benefits of the IoT integration into the healthcare system for both an individual and a society will be achieved only when most of these concerns and risks are overcome. Thus, the success of the IoT-powered healthcare depends on the overall ecosystem development, embraced by an adequate regulations and appropriate level of trust. Accomplished identification, privacy and security, confidentiality, trust and semantic interoperability issues can lead to wisely used and widely applied IoT-driven e-health, therefore improving access, availability, and increasing the financial efficiency of healthcare systems in general.

3.2 Challenges, Risks and Concerns

Despite the opportunities and benefits, e-health widespread adoption is facing with numerous barriers. On the other side, the realization of the IoT vision, in order to create adjustable, secure, ubiquitous and non-invasive solution, requires significant modifications of systems, architectures and communications [133]. In general, the challenges IoT faces are: availability of Internet at any place and without costs, development of low-cost smart sensing platforms, scalability, energy consumption, computational capacity, fault tolerance, security and privacy issues and a climate of trust [85]. Alongside technology impacts to the IoT development and usage, it is important to point out and social and economic factors. All these facts make the IoT-driven e-health systems a complex and exciting field. The challenges IoT-based e-health vision deals with may result significantly slower than anticipated adoption of the IoT-powered e-health systems and services as well as nullify any or all of the identified benefits.

In the rest of the chapter main challenges, risks and concerns of modern IoT healthcare system are discussed.

Government action

Governments are responsible for providing fundamental services, such as healthcare and ICTs infrastructure, continuity of funding, accessible education as well to support services around personal health issues including implementation of standards and protecting privacy and security rights.

Technology issues

The technology domains that will provide the IoT practicable and reliable solutions' wider uptake, including healthcare sector, are: (i) identification, (ii) IoT architecture, (iii) communication, (iv) network, (v) network discovery, (vi) software and algorithms, (vii) hardware, (viii) data and signal processing, (ix) discovery and search engine technology, (x) relationship network management technology, (xi) power and energy storage, (xii) security and privacy, and (xiii) standardization [12]. In other words, the experts assume that the progress and mature of IoT technologies will require continuous and intense work in data protection, ethical issues, architecture, identification of networked objects, standards and regulations, and governance [81]. As a consequence, the IoT-driven e-health adoption on a large scale is being hindered by a variety of factors. Successful IoT applications in the area of personalized advanced healthcare require home diagnostic kits, healthcare monitoring and the low-cost collection of medical data shared with the patient's healthcare providers through the Cloud. Medical devices, opposite to office computer systems, are often used in a harsh environment. Therefore, the hardware components of medical devices should have higher physical tolerance against environmental conditions. To prevent wrong measurements or treatment parameters, medical devices often use a dual communication channel design, in order to detect and correct wrong transmission and ensure the totality of the transmitted information [117].

Hence, availability of required data is essential for making right and timely health-related decisions [88]. Therefore, IoT medical devices must: (i) gather data and analyze real-time data, (ii) monitor device operation for faults and prevent malfunctions, (iii) remote control and device configuration, (iv) enable devices to broadcast results and notifications to other devices, (v) maintain an active device inventory and track assets, and (vi) enable remote software/firmware updates. Having in mind that one of the obstacles to healthcare technology embracement is that healthcare professionals and patients often resist technology, the IoT smart medical devices must be easy to handle devices, customized, affordable, powerful, safe and comfortable. With technology advancements, creating hardware and wireless connectivity equipment becomes cheaper and more efficient, enabling connection of a whole range of objects together. As a result, healthcare-related information systems and hardware are now omnipresent. With the help of small, powerful and cheap devices, and medical software applications, people are able to monitor themselves on a daily basis and share their health information with healthcare providers when needed and start to become more responsible for their own care along with a deeper understanding of own illness. To achieve these benefits, interoperability appears as a key challenge. Therefore, an interoperable ecosystem of many heterogeneous sorts of systems (devices, sensors, equipment, etc.), services and applications, to provide the free health-related information stream for accurate and on time decision is crucial.

Human factors

People are key components to the creation and use of e-health products and services. Cognitive, social, and cultural barriers can enable patients and consumers to benefit from rapidly changing and growing e-health systems. These barriers include cultural and language differences, lack of knowledge and access to technology. Even the lack of IT knowledge may be one of the main barriers, the data scandals that regularly occur represents a higher obstacle. Some potential patients of the IoT-driven e-health services, feel their lives are being controlled and therefore have resistance and may reject them. Also, some professionals are mainly focused to give their best to treat the patient and other activities usually consider as a loss of control over their patients' care. Consequently, technology rejection by influential healthcare givers affects other healthcare staffs [35]. One of the ways to deal with these barriers is to give an opportunity for healthcare professionals and customers to participate in designing and adopting technologies, improving system development and facilitating them to control the effects of the information system based on their engagement [95]. Computer and web technology skills, the organizational and managerial competencies and leadership, as well as the awareness of the associated legal, ethical, and economic issues, are necessary for the changes IoT brings in e-health tasks, processes and job roles. Only through the continuous and reactive work on overcoming these barriers e-health strategies can be customized in order to satisfy a wide scope of society demands [47].

Big data and analytics

According to Cisco predictions, by 2020, 50 billion diverse devices will be connected to the Internet [32]. Consequently, the IoT growth will imply the large-volume, complex, growing data sets. Some estimates states that the amount of generated data will be 507.5 ZB (zettabyte = 1 trillion gigabyte) of data per year or 42.3 ZB per month by 2019. It is expected that the data produced by IoT connected devices in 2019 will be 269 times greater than the data being transmitted from end-user devices to data centers and 49 times higher than total data center traffic [27]. Regarding produced healthcare data on a global scale, in 2012 the amount of generated data was 500 petabytes (10^{15} bytes), while 25000 petabytes can be expected in 2020 [34]. Evidently, a voluminous nature of data produced by the IoT-driven e-health systems represents a big challenge. A large, rapidly growing, and mostly unstructured medical data are the consequence of increased digitalization of formerly analogue media (images, reports, lab results, etc.), the continuous optimization of diagnostic laboratory and imaging sensors, increased monitoring with sensors of all kinds, etc. However, voluminous data alone doesn't do much, but IoT collected health data and algorithms together, are exceptionally valuable. Thus, the main question is how to analyze, capture, search, share, store, and visualize data which have a tendency to grow. In the modern approach, a solution can be found in the concept of "Big data", which is primarily used to describe large sets of data. Opposite to traditional datasets, Big data usually encompasses voluminous sets of unstructured data. These data require real time analysis, and any of required operation can't be performed using existing IT and software/hardware tools [22]. Concepts and technologies which are usually closely related to Big data are almost always [22, 101, 107]:

- Cloud computing (provide reliable storage for data),
- IoT (gathering prodigious amount of data from real world—sensors and actuators),
- Data center (acquiring, managing, organizing, and leveraging the data), and
- Hadoop (data storage and processing, system management, and incorporation of variant modules).

One of the essential concepts in Big data is "Not Only Structured Query Language" (NoSQL) which represents a well-known set of non-relational data management systems. Unlike traditional Relational Database Management Systems (RDBMS) which use table-based approach and SQL for accessing data, NoSQL systems are not table-based and do not depend on SQL. Instead, these systems are based on a key-value storage. NoSQL database management systems are useful when working with masses of data which nature does not demand a relational model [7, 33, 43, 113]. Today, there are a various NoSQL database types, such as the Key Value Pairs, Column, Document, and Graph-based databases [107].

Volume, variety, velocity, value and veracity, as the foundational characteristics of Big data, discussed through application in healthcare, justify application of Big data for this purpose [11, 96]:

- *Volume*: As time goes on, a high quantity of health-related data is produced and accumulated, resulting in terabytes and petabytes of data. These systems include medical and healthcare information such as: personal information, radiology images, personal medical records, 3D imaging, genomics, and biometric sensor readings. Nowadays, relying on advances in data management, healthcare systems have the potential for manipulation, storage and use of such a complex data structure by using virtualization and Cloud computing.
- *Variety*: The most challenging aspect of Big data appliance in healthcare consists of joining traditional data with new data forms to get the most closer to the right solution for a specific patient. Structured information, such as clinical data, can be stored, processed and manipulated by machine in an easy way. However, most of health-related data, such as office medical records, doctor handwritten or machine-written notes and prescriptions, images and radiograph films, e-mail messages and attachments are unstructured or semi-structured. From that reason, healthcare applications demand more efficient ways to merge and convert various types of data, in particular to convert structured to unstructured data.
- *Velocity*: Most healthcare data has been traditionally static, but today velocity of data increases with massive data that are the results of continuous regular monitoring. The information stored in healthcare systems is often correct, but not always even if it is updated on a regular basis. Thus, Big data must be retrieved, analyzed and compared to make time and accurate decisions based on real-time data processing, which sometimes can make decision between life and death.
- *Value*: Advances in Big data is process of creating value which can be translated into understanding new diseases and therapies, predicting outcomes at earlier stages, making real-time decisions, promoting patients' health, enhancing medicine, reducing cost and improving healthcare value and quality.
- *Veracity*: Quality of data is of primary concern in health sector because the quality of offered healthcare as well as life or death decisions depends on having the accurate health-related data. In order to achieve effective results with data analytics, it is necessary to provide health-related information of high-quality.

In the summary, Big data analytics, as a top issue in the healthcare industry, are needed to extract useful information from the collected voluminous datasets, and, based on this, adapt the therapy according to the needs. Hence, in the IoT world, health-related data is transmitted to patient' EHR system automatically. The IoT solutions in healthcare enable health practitioners to merge the IoT data from various medical devices. In this way healthcare professionals obtain a complete picture of patient's health status [68]. Possible benefits of Big data application in healthcare include detecting diseases at earlier stages, predicting epidemics, curing disease, avoiding preventable deaths and therefore improving the quality of life and support prevention and personalization. With the help of Big data and analytics, healthcare institutions get an opportunity to create more affordable and better healthcare, moving reactive treatment towards predictive and preventive medicine. However, there are a lot of challenges that hinder the development of Big data in healthcare. Difficulties lie in technical issues (to successfully deal with growing amounts of great variety of data and high speed of data generation and processing—data recording, gathering, analyzing, manipulating and visualization) and security issues (to secure personal data as well as corporate data from unauthorized access or from loss) [45]. So, besides physical sensor development, the IoT-driven e-health system growth relies on the development of Big data analytics tools, interfaces, and systems that will allow healthcare providers to observe and apply the resulting information.

Security and privacy

Matched to the traditional definition of security (which includes secure communication, cryptography and guaranteed privacy), security in the IoT vision involves information integrity, confidentiality of data, availability of services, anti-malware, privacy protection, access control, etc. [72]. Consequently, IoT presents new challenges to network and security architects.

Security, as one of the top challenges IoT faces with, involves the security issues on sensing, communication, and application level as well as overall system security [72]. At the sensing layer, an IoT sensing infrastructure/device/technologies (which have low power and constrained resources, limited connectivity and computing capabilities) don't have the power to provide appropriate security protection. The IoT at middle layers (network and service layers) is based on networking and communications which make easier eavesdropping, interception and Denial of Service (DoS) attacks. The information collection and encryption at the upper (application) layer, which is the topmost and terminal level, help obtaining the security requirements at all layers [66, 72]. In summary, each layer has the ability to provide corresponding security controls, while the security requirements between layers are of the great importance as well. Security threats in IoT layers, as well as those between layers, are shown in Table 1 [72].

The Open Web Application Security Project [92] defines top ten IoT vulnerabilities as:

- Insecure Web interface (e.g., default accounts, SQL injection),
- Insufficient authentication/authorization (e.g., weak passwords, no two-factor authentication),
- Insecure network services (e.g., ports open, DoS attacks),
- Lack of transport encryption/integrity verification (e.g., misconfigured or no use of Transport Layer Security (TLS), custom encryption),
- Privacy concerns,
- Insecure Cloud interface (e.g., default accounts, no lockout),
- Insecure mobile interface (e.g., account enumeration, no account lockout),

Table 1 Security threats in IoT

Sensing/perception layer	Middle layers		Application-interface layer	Between layers
	Network layer	Service layers		
• Unauthorized access • Availability • Spoofing attack • Selfish threat • Malicious code • DoS • Transmission threats • Routing attack	• Data breach • Transmission threats • DoS • Public key and private key • Malicious code • Routing attack	• Privacy threats • Services abuse • Identity masquerade • Service information • Manipulation • Repudiation • DoS • Replay attack • Routing attack	• Remote configuration • Misconfiguration • Security management • Management system	• Sensitive information leakage at border • Identity spoofing • Sensitive information spreads between layers

- Insufficient security configurability (e.g., lack of password security options, no security monitoring and logging),
- Insecure software/firmware (e.g., old device firmware, unprotected device updates), and
- Poor physical security (e.g., accessed or removed data storage media, easily disassembled device itself).

When it comes to healthcare and e-health applications in an IoT environment, there is a need to pay more attention to the security design than in many other IoT networks because the medical data (all data related to a person's health and medical history) are exceptionally sensitive and need to be protected in appropriate way. The exploitation of vulnerabilities mentioned above represents a risk to the safety and effectiveness of IoT-based e-healthcare. The success of healthcare application is determined by the achieved level of patient security and privacy. IoT-based e-health applications operate on a variety of elements: sensor devices, actuators, processing, networking and memory components. The general security level is determined by the weakest element of the system. Therefore, the security must be built into each component, and the overall system (Fig. 10).

With regards to security, data, communication channels and the medical device itself, are the weakest points [69]. In other words, during plugging a large number of diverse connected devices into the IoT system they should be securely identified and have the ability to be discovered. Even most of today's IoT medical devices use secure communication methods, they could still be vulnerable to hackers since communications are mostly wireless (e.g., stealing information, disruption of

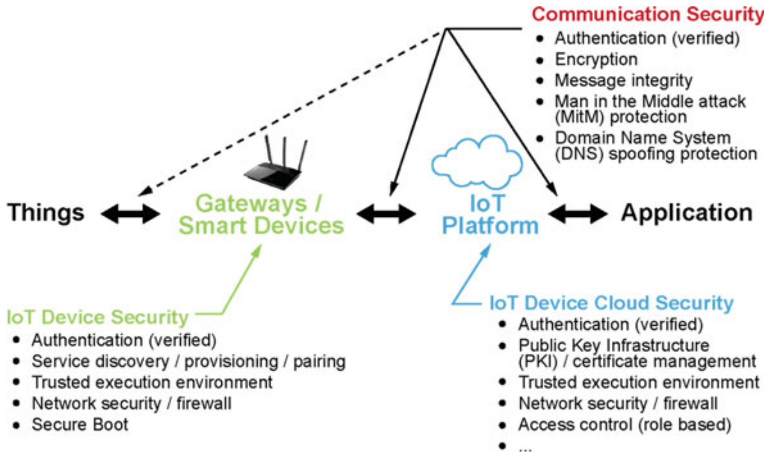


Fig. 10 IoT security points [8]

services like pacemakers, remote hacking of a vehicle control system, remotely unlocking locked door) while unattended elements are mainly unprotected from physical attacks [63]. The additional problem is the fact that execution of complex security-enabling algorithms in IoT devices requires their significant energy, communications, and computation capabilities. Hence, by connecting more intelligent devices to the Internet, the privacy and security issues become critical, representing the major challenges in realization of IoT vision. Considering that the information collected by the IoT system might reveal personal information, the security issues (protection of data and privacy) arise during aggregation of data and their exchange. In other words, with the larger transfer of sensitive data over IoT devices, there is more risk of data to be leaked, falsified or manipulated. Untraceability, unlinkability, unobservability, anonymity and pseudonymity, are mandatory to satisfy privacy issues. Thus, private information from patients, which makes e-health as a highly sensitive yet personal area, appears as an essential component in the widespread adoption of IoT principles in healthcare. The relationship between security and privacy concepts is data protection. Hence, the special interest during the healthcare security architecture design must be given to confidentiality and protection of information. Other factors such as information security, trust, end-to-end personal data privacy and protection should be also systematically and carefully addressed at the conception phase of each component and overall IoT-based e-health system. Figure 11 shows the relationship between information security and present healthcare research problems [9].

The security requirements and challenges of the IoT e-health applications are shown in Fig. 12 [59].

As the first step in the entire health information access procedure, user authentication is essential in healthcare information systems. Some of the authentication mechanisms used to verify the user's identity are: password, PIN (Personal

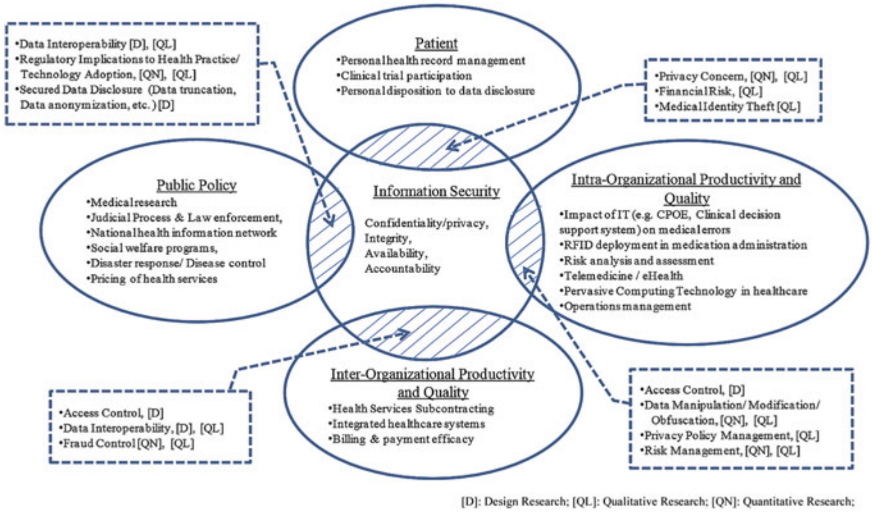


Fig. 11 Research areas in the healthcare information security [9]

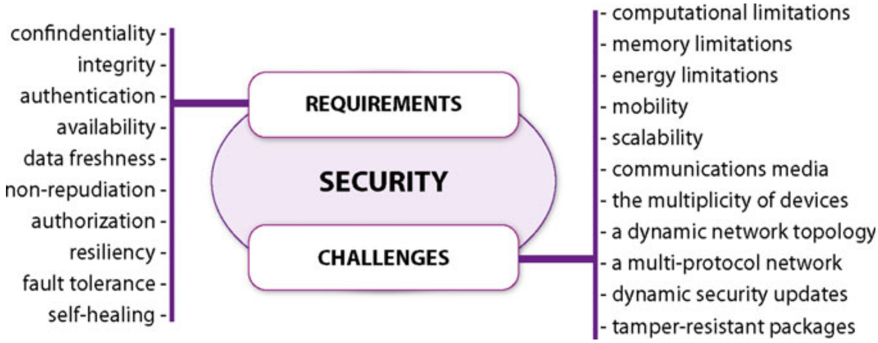


Fig. 12 Security requirements and challenges for the IoT-based healthcare solutions

Identification Number), fingerprint, signature, voice pattern, smart card, token, etc. Only in this way it can be assured that the information is sent by the trusted sender [76]. Moreover, networked devices that exchange data with other IoT devices need to be properly authenticated to avoid security problems. This may need to include certain authentication protocols, and to use integrity-secured or encrypted channels of communication [31]. Interoperability, as an essential characteristic of the IoT-driven e-health system, enables diverse things to better cooperate and integrate in order to produce the desired outcome [18]. In order to make an interoperable system, its elements have to be designed according to standards satisfying their properties on: (i) technical (interoperability achieved using compatible hardware interfaces), (ii) syntactical (compatible data exchange protocols and data containers), and (iii) semantical (the same understanding of the meaning of data) levels [88]. When health-related sensitive data are shared across the network, authentication, availability, confidentiality, and integrity are mandatory in order to realize secure communications in IoT. With patient data integrity, the received medical reports can't be altered in transit. In this way, patient' medical data, transferred to the medical personal, can't be modified, changed or interpreted by any unauthorized source. Additionally, data confidentiality ensures that a patient's health-related records are secured from passive attacks [29]. Availability, as another security requirement (Fig. 12), ensures the continuity of the IoT healthcare services to authorized person upon demand. Due to the sensitive nature of health data, bounded latency and reliability of the IoT-based e-health system are crucial to effective intervention, especially in a case of emergency. It is important to highlight that data or messages sent earlier can't be denied by a node (non-repudiation). Employed system security scheme must protect the data, device and network from any attack as well as to provide respective security services at any moment, even some interconnected health devices are harmed, failed, run out of energy or there is a software glitch [59].

Clearly, to enable at least a minimum level of security, IoT healthcare services are facing with numerous challenges (Fig. 12). Bearing in mind that a typical IoT healthcare system consists of small health-related devices of limited computational performances, memory and battery power, finding a security solution that overcomes these computational, memory and energy limitations and maximizes security performance is a challenging task [59]. To secure devices in sensing layer of IoT, all devices should be produced according to specific security criteria and implement security standards for IoT. A trustworthy data sensing system, ability to detect and identify the source of users and securely designed software or firmware at IoT end-node are mandatory as well [72]. Other serious challenges are focused on develop a mobility-compliant security algorithm and design highly scalable security scheme applicable to the simplest of devices, and be appropriate for dynamic network topology as well. An overall security protocol that has ability to equally deal with both wired and wireless channel characteristics represents important challenges security specialists facing with. Dynamic security updates and tamper-resistant packages of IoT health devices are nothing less challenging to implement [59]. Therefore, to implement the IoT-powered e-health system, using portable health devices to collect, store, and transfer patient health-related sensitive data to a central server, requires secure manners to rapidly transfer recorded data so that patient's personal information can't be compromised at any stage. Only satisfying requirements defined above and successfully dealing with mentioned challenges, this goal can be accomplished. A large number of research is devoted to the integration of enormous streams of real-time data from the IoT with all of existing data, preserving and protecting user security with the help of pervasive sensing and analytics systems and choice of hardware and software which will contribute to development of new intelligent, secure, easy and modern IoT applications. Novel research regarding security topics in IoT-driven e-health are also based on improving several algorithms in medical applications that can be supported by the IoT technology and security issues and on defining new cryptographic protocols that are able to work on tiny, low-power devices [1, 28, 64, 87, 98]. The ways of reducing and solving the risk of security and privacy in an e-health environment are discussed in many works [5, 9, 53, 54, 59, 67, 69, 73, 106, 118, 122, 129].

Nevertheless, protecting privacy and security and assuring fairness in the IoT is a critical, yet complex task. As a very important and full of challenges, security and privacy issues must be taken into account during the whole IoT lifecycle, from the design phase to the services running. To protect privacy, in order to facilitate the overall adoption of the IoT, following tasks must be performed [48, 124]:

- Take into account technical solutions,
- Encompass regulatory considerations,
- Include market-based aspects, and
- Incorporate socio-ethical issues.

However, it has been proven that, regarding privacy, a technical solution is not an unattainable goal. On the contrary, political and economic factors are much greater constraints society is facing with regard the level of privacy [52].

In summary, the security and privacy issues of IoT-powered e-health systems must be threatened on many levels, what is essential for the success of IoT implementation in healthcare. Confidentiality, data integrity, accountability, availability of services and access control are the essential goals that systems have to achieve in order to satisfy certain security and safety demands [88]. Since an IoT-driven e-health system store and process data of special interest, they should be equipped with appropriate mechanisms of their protection. Security should be built hierarchal into the whole healthcare ecosystem. Still, there are many open problems in areas of security and privacy protection, network protocols, standardization, identity management, etc. [72]. Assured privacy, security and consumer trust are the keys to realizing the full potential of the IoT application in healthcare. This highlights the fact that novel security protocols and identification techniques are mandatory, as well as more intelligent security systems that include managed threat detection, anomaly detection, and predictive analysis [23].

Regulations and standardization

The IoT success depends on the standardization issues, which provide secured interoperability, compatibility, reliability, and effective operations on a global level [72]. Therefore, standards, simply put as a list of agreed-upon rules and guidelines, are considered as fundamental for facilitating e-health system interoperability, providing adherence to current privacy and security legislation as well as ensuring the ability to successfully leverage various devices and applications. Not only are they important with regards to traditional e-health systems, standards also playing a role in the success of the novel IoT-based e-health solutions. In other words, taking into account that a patient may necessitate the services of various healthcare providers, uses various devices, many different electronic systems and information systems while used devices and information systems may use disparate (communications) protocols and messaging formats, the IoT-driven e-health must be supported with numerous standards. Lake et al. [69] classify standards used in e-health applications in: data, message, document and process standards. The standards are also classified into syntax, semantics, relationship, purpose and classification based. However, standards for the IoT-based e-health together with technology are key enablers of the transformation and revolutionizing healthcare. To deal with deployments and utilization of diverse products, global interoperability standards are necessary. These standards enable that variety of devices, systems and applications for health monitoring and preventive care talk the same language and intercommunicate. To provide a common methodology for specifying sensor performance and facilitate integration for multi-vendor sensors, the IEEE 2700–2014 "Standard for Sensor Performance Parameter Definitions" has been developed as the result of the IEEE Standards Association and MEMS Industry Group collaboration [10]. Moreover, due to the sensitivity of medical data and required strong legal regulation, healthcare-related systems are significantly harder to develop. Safety and performance of products on the EU market are determined either by Directive 2001/95/EC 11 on general product safety or by specialized medical device directive in case of medical products [36]. Telemedicine, e-health and IoT technologies are advancing rapidly, requiring new generations of communication protocols, provisions for the service layer and interoperability guidelines. Work in standardization of this area is continuous and intense. An IEEE active project P2413 "Draft Standard for an Architectural Framework for the Internet of Things (IoT)," [58] defines an architectural framework proposing cross-domain interaction, system interoperability and functional compatibility for the IoT [10]. As the Cloud is one of the major building blocks of the IoT-based e-health vision, Cloud-related standards at various layers of Cloud infrastructure and services as well as some level of confluence of e-health and Cloud-related standards are essential too. Moreover, the processes and services automation is not feasible without adequate data standards that permit communication through open access Internet-oriented software languages. Some of the common e-health data standards include [69]: ICD (International Classification of Disease)—international standard codes for diagnoses; LOINC (Logical Observation Identifiers Names and Codes)—a universal coding system for the reporting of laboratory and clinical measurements; CPT (Current Procedural Terminology)—standard for coding medical procedures; SNOMED CT (Systematized Nomenclature Of Medicine)—widely used hierarchical healthcare terminology; NDC (National Drug Codes)—Food and Drug Administration's numbering system for medications. It is important to mention and following standards: HL7 (Health Level System 7)—a standard for exchanging integration, sharing, and retrieval information between medical applications; CCR (Continuity of Care Record) and CCD (Continuity of Care Document)—standards for solving the problem of patient-data portability and interoperability; DICOM (Digital Imaging and Communications in Medicine)—the international standard for the communication and management of medical imaging related information; IHE (Integrating the Health Enterprise)—an initiative to improve the way computer systems in healthcare sector exchange information. Furthermore, adequate regulative and standards (necessary to ensure that information systems can exchange and share the patient information in order to provide appropriate and timely care) like the ISO/IEC 27,000-series which encompasses information security standards, must be satisfied [76]. There is also the Federal Information Processing Standard (FIPS 140), a USA government computer security standard, which deals with security in the transmission of information, what is a crucial in the successful deployment of medical IoT applications. The ISO/IEEE 11073 family of standards has potential to provide complete and interoperable health IoT architecture. In this way, the applications in the Cloud are able to supervise and gather health-related information from personal health devices, enabling health professionals to access remotely and directly to the newest measurement values of each patient from the Cloud [77]. A comprehensive review of widely adopted e-health interoperability standards has been presented in [3]. As can be seen, the collection, processing, recording and dissemination of medical patient data are under the control of many laws and regulations. Even these regulations and laws vary greatly between different countries and continents, authorization procedures, data interchange and privacy must be compliant with EU Data Protection Directive (e.g. Directive 2011/24/EU—the application of patients' rights in cross-border healthcare; Directive 2000/31/EC—electronic commerce; Directive 95/46/EC—Data Protection) and the national Patients' Rights Laws (Europe) or the HIPAA in the USA [39].

It is worth to note that the IoT-driven e-health systems create complete new challenges in sense of legislation and policy issues. From a standards perspective, the IoT-based e-health systems represent a huge challenge for standardization. Standardization, as a time-lagged and long-term process, is a complex task that has to involve all participants. Moreover, standards development and implementation lag behind technological development, making this process slow and may require concerted regulatory action. Nevertheless, the success of IoT-powered e-health vision relies mainly on standardization, which provides reliability, compatibility, interoperability, and effectiveness of the operations on a worldwide scale.

Investment

Growing demand for real-time disease management, improved patient care services, effective and efficient treatment outcome implies investors, providers, and developers rising interest in the IoT appliance in the healthcare. The IoT in the healthcare market is segmented based on application, into telemedicine, inpatient monitoring, clinical operations, medication management, and connected imaging. Regardless of the applications, the basic requirement for implementing the IoT e-health services is the access to the Internet. Besides rapid Internet growth, Internet access is not still available to every place in the world. This implies a need to largely invest in IT infrastructure and resources. The private companies will invest only if they can make a profit. Hence, at this point the government comes in play [85]. On the other side, many companies and organizations largely invest in adopting new technologies in order to gain patients' attention and deliver actionable insights for their personalized care. One of the leading trends in the market is the result of high consumerization. Patients want to have insight in their health condition as well as to take control of it [99]. Even BI Intelligence [14] predicts that on a global scale 73 million IoT devices will be installed for the healthcare sector by 2016 and 161 million by 2020, the IoT-based healthcare isn't just about devices. Instead of hardware devices, more investment will be aimed at developing appropriate software and services of IoT healthcare solutions [14]. The development of Big data analytics, Cloud services and artificial intelligence are in the center of healthcare industry's investments. According to multiple market reports, the investments in Big data analytics platforms and tools, the IoT, Cloud computing technologies, and business intelligence tools in healthcare sector will continue their rapid growth. It is anticipated that the healthcare-specific IoT market will expand from $32.47 billion in 2015 to $163.24 billion by 2020 [16]. In other words, the immense interest in completely connected health and supporting devices, sensors, and clinical tools, will imply new and numerous investment in many key market segments that will integrate to create the healthcare-specific IoT [17].

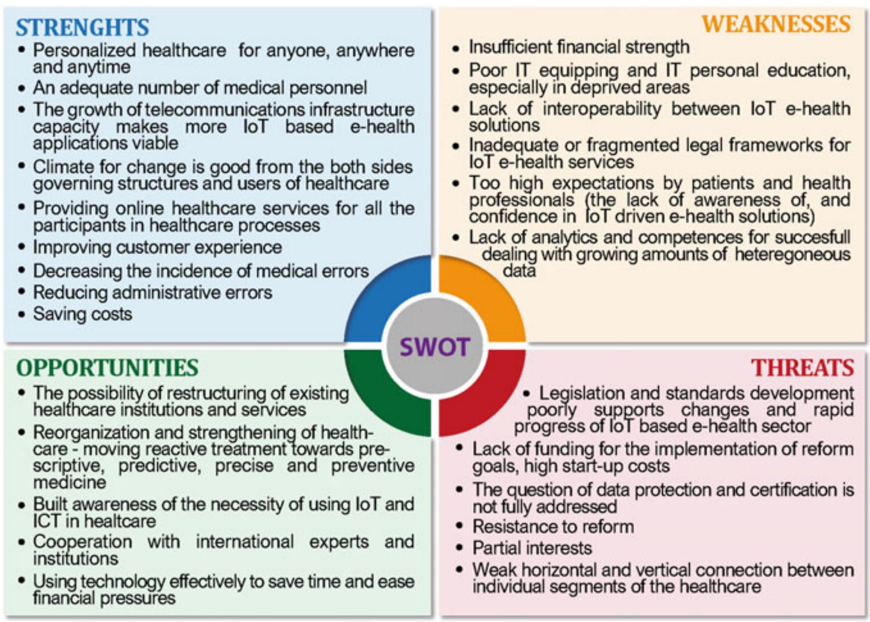
4 Discussion And Concluding Remarks

With the technology-driven developments, people in the 21st Century via more effective and efficient healthcare systems and services are able to have insight and proactively manage their health conditions. The IoT and e-health are keystone technologies which together entirely change person-to-person, human-to-machine and M2M communications, revolutionizing healthcare in all its aspects. IoT smart devices applied in healthcare provide novel and attractive ways to monitor, record patients' data in home and work environments, and automatically transmit gathered information to electronic systems. Data analyzed and delivered in easily understandable formats, enable healthcare practitioners to quick and easy gain insights into the health conditions of patients and start using the collected data in their clinic practice, providing in such way a faster, easier and cost-effective means to accessing healthcare. Even the IoT integration in healthcare is still early in the maturity, it can be expected that connected medical devices will become ubiquitous and programmable, with the possibility to talk to each other while improving quality of care and consequently patients' personal health. In other words, in both hospitals and at home, the possibilities of IoT-based e-health solutions are endless.

With this in mind, it can be pointed out that the advantage of IoT-based e-health system is in possibility of smart objects to continuously monitor the health condition of a patient and exchange information with other devices and health institutions via the Internet, in order to help make correct and personalized treatment decisions. An intelligent infrastructure for personal health management through smart devices and technologies accessible to all citizens, enable omnipresence of many medical applications such as remote health monitoring, fitness and wellness programs, chronic diseases, and care of old and disabled people. Reducing the costs and the time to perform health tasks and processes, more quality health decisions and activities at the operational, managerial and policy levels and dealing with an increasing number of cases without raising staff numbers or associated costs, are the main advantages IoT brings in the healthcare domain.

This chapter, in addition to a performed review of the literature and existing solutions, highlights six objectives for improving the current e-health system. Guided by the improvements' objectives and the new concepts, primarily IoT, Big data and Cloud computing, the IoT-based e-health system architecture that includes key elements of the modern healthcare system is presented as well. The conducted analysis has confirmed that potential outcomes are significant. Still, there is a number of possible challenges, risks and concerns that may prevent the full adoption of IoT-powered healthcare. It is important to note technological, managerial, organizational and ethical challenges, as well as standardization, interoperability, security and privacy issues, and economic factors which all together represent the major challenges and barriers to revolutionize the healthcare processes, increasing the availability and quality of medical care embraced with dramatically lowering costs.

Understanding the IoT-driven e-health may perhaps best be achieved by reviewing a SWOT analysis to evaluate the Strengths, Weaknesses, Opportunities, and Threats of the IoT-based healthcare at the present time.



Hence, to develop and integrate effective ubiquitous IoT-powered healthcare, it is essential to recognize and deal with many ethical concerns, equal rights in accessing to healthcare services and receiving care, accountability, the effectiveness of patient involvement and quantity and quality of online health-related information. Successfully dealing with numerous challenges IoT-based healthcare services are faced with, should enable reduced costs, increased the quality of life, and enrich the both patients and healthcare providers' experience. Even the IoT is immensely changing healthcare, those changes are barely starting. Satisfying essential demands, immensely improving existing healthcare systems and continuously looking for entirely novel ways of monitoring and delivering healthcare will lead to experience the maximal benefits IoT-based e-health has to offer.

References

1. Acharjee, S. et al. (2014) Watermarking in Motion Vector for Security Enhancement of Medical Videos, Control, International Conference on Instrumentation, Communication and Computational Technologies (ICCICCT).
2. Adebesin, F., Kotzé, P., Van Greunen, D. and Foster, R. (2013a) Barriers and Challenges to the Adoption of E-Health Standards in Africa, Health Informatics South Africa (HISA).
3. Adebesin, F., Foster, R., Kotzé, P. and Van Greunen, D. (2013b) A review of interoperability standards in e-Health and imperatives for their adoption in Africa, Research Article – SACJ No. 50, pp. 55–72.
4. Adibi, S. (2015) Mobile Health. A Technology Road Map. Springer International Publishing Switzerland.
5. Agrawal, V. (2014) Security and Privacy Issues in Wireless Sensor Networks for Healthcare. Internet of Things User-Centric IoT. First International Summit, IoT360. Rome, Italy, pp. 223–228.
6. Alliance for Health Policy and Systems Research (2004) Strengthening health systems: the role and promise of policy and systems research, Geneva, Switzerland.
7. Amato, A. and Venticinque, S. (2014) Big Data Management Systems for the Exploitation of Pervasive Environments, Bessis, N. and Dobre, C. (eds.), Big Data and Internet of Things: A Roadmap for Smart Environments, Studies in Computational Intelligence 546, pp 67–90.
8. Andres, R. (2015) Eurotech's Everyware IoT Security Elements Overview, [Online]: http://www.slideshare.net/Eurotechchannel/iot-security-elements.
9. Appari, A. and Johnson, M.E. (2008) Information Security and Privacy in Healthcare: Current State of Research. [Online]: http://www.ists.dartmouth.edu/library/416.pdf.
10. Ash, B. and Bennett, K. (2014) Expanding Wellness Monitoring and Care with e-Health, [Online]: https://www.mdtmag.com/blog/2014/12/expanding-wellness-monitoring-and-care-e-health.
11. Asri, H., Mousannif, H., Moatassime, H. A. and Noel, T. (2015) Big Data in healthcare: Challenges and Opportunities, International Conference on Cloud Technologies and Applications (CloudTech), pp. 1–7.
12. Bandyopadhyay, D. and Sen, J. (2011) Internet of Things - Applications and Challenges in Technology and Standardization, Wireless Personal Communications, Vol. 58, Issue 1, pp 49–69.
13. Bhaddurgatte, R.C. and Kumar, V. (2015) A Review: QoS Architecture and Implementations in IoT Environment, Research & Reviews: Journal of Engineering and Technology, pp. 6–12.

14. BI Intelligence (2016) The global market for IoT healthcare tech will top $400 billion in 2022, [Online]: http://www.businessinsider.com/the-global-market-for-iot-healthcare-tech-will-top-400-billion-in-2022-2016-5.
15. Brasseal, M. (2015) Realtime Technology and the Healthcare Internet of Things, [Online]: https://www.pubnub.com/blog/2015-06-19-realtime-technology-and-the-healthcare-internet-of-things/.
16. Bresnick, J. (2015) Healthcare Big Data Analytics, IoT, Cloud Markets Set for Growth, [Online]: http://healthitanalytics.com/news/healthcare-big-data-analytics-iot-cloud-markets-set-for-growth.
17. Bresnick, J. (2016) Healthcare Internet of Things Investment is Just Getting Started, [Online]: http://healthitanalytics.com/news/healthcare-internet-of-things-investment-is-just-getting-started.
18. Bui, N. and Zorzi, M. (2011) Health Care Applications: A Solution Based on The Internet of Things. Proceedings of the 4th International symposium on Applied Sciences in Biomedical and Communication Technologies – ISABEL 2011.
19. Buzzi, M.C. et al. (2016) Facebook: a new tool for collecting health data? Multimed Tools Appl, Springer Science + Business Media New York.
20. Car, J. et al. (2008) The Impact of eHealth on the Quality & Safety of Healthcare, A Systemic Overview & Synthesis of the Literature, Report for the NHS Connecting for Health Evaluation Programme.
21. Chatterjee, P. and Armetano, R. L. (2015) Internet of Things for a Smart and Ubiquitous eHealth System, International Conference on Computational Intelligence and Communication Networks (CICN - 2015), At Jabalpur, India.
22. Chen, M. et al. (2014) Big Data: Related Technologies, Challenges and Future Prospects, Springer.
23. Cisco (n.d.) Securing the Internet of Things: A Proposed Framework, [Online]: http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html.
24. Comstock, J. (2015) PwC predicts "DIY Healthcare" will be the top trend of 2015. [Online]: http://mobihealthnews.com/39747/pwc-predicts-diy-healthcare-will-be-the-top-trend-of-2015.
25. Conrad, S. K. (1998) Making telehealth a viable component of our national health care system. Prof. Psychol. Res. Pract. 29(6):525–526.
26. Das, R. (2015) Top 10 Healthcare Predictions for 2016, [Online]: http://www.forbes.com/sites/reenitadas/2015/12/10/top-10-healthcare-predictions-for-2016/#146f174c2f63.
27. Daecher, R. and Schmid, R. (2016) Internet of Things: From sensing to doing, Deloitte University Press, [Online]: http://dupress.com/articles/internet-of-things-iot-applications-sensing-to-doing/.
28. Dey, N. et al. (2012) Stationary Wavelet Transformation Based Self-Recovery of Blind-Watermark from Electrocardiogram Signal in the Wireless Telecardiology, Recent Trends in Computer Networks and Distributed Systems Security, Vol., 335 of the series Communications in Computer and Information Science, pp. 347–357.
29. Divi, K., Kanjee, M.R. Liu, H. (2010) Secure Architecture for Healthcare Wireless Sensor Networks. Sixth International Conference on Information Assurance and Security.
30. eHealth Action Plan 2012–2020 - Innovative healthcare for the 21st century (2012), European Commission [Online]: https://ec.europa.eu/digital-single-market/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century.
31. European Commission (2016) Advancing the Internet of Things in Europe, Commission Staff Working Document accompanying document Communication from the commission to the European parliament, the Council, The European economic and social committee and the committee of the regions, Digitising European Industry - Reaping the full benefits of a Digital Single Market, Brusseless.
32. Evans, D. (2011) The Internet of Things - How the Next Evolution of the Internet Is Changing Everything, Cisco Internet Business Solutions Group (IBSG), [Online]: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

33. Feinleib, D. (2014) Big Data Bootcamp - What Managers Need to Know to Profit from the Big Data Revolution, Apress.
34. Feldman, B., Martin, E.M., Skotnes, T. (2012) Big Data in Healthcare, Hype and Hope, Dr. Bonnie 360.
35. Fichman, R.G., Kohli, R. and Krishnan, R. (2011) The Role of Information Systems in Healthcare: Current Research and Future Trends, Information Systems Research, Vol. 22 Issue 3, p 419.
36. Fricker, S.A. et al. (eds.) (2015) Requirements Engineering for Digital Health, Springer International Publishing Switzerland.
37. Forsstrom, S., Kanter, T., Johansson, O. (2012) Real-time distributed sensor-assisted m-health applications on the internet-of-things. In: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1844–1849.
38. Gaddi, A., Capello, F. and Manca, M. (2014) eHealth, Care and Quality of Life, Springer-Verlag Italia.
39. George, C., Whitehouse, D. and Duquenoy, P. (eds.) (2013) eHealth: Legal, Ethical and Governance Challenges, Springer-Verlag Berlin Heidelberg.
40. Georgiadis et al. (2010) An Intelligent Web-based Healthcare Systems: The case of DYMOS. Web-based applications in Healthcare and Medicine (A. Lazadikou (ed.)) Annals of Information System, Vol.7, Springer Science + Business Media LLC.
41. Giaffreda, R. et al. (eds.) (2015) Internet of Things - User-Centric IoT (IoT360 2014), Part I, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer Cham Heidelberg New York Dordrecht London.
42. Gibbons, M. C. (2008) eHealth Solutions for Healthcare Disparities, Springer Science + Business Media, LLC.
43. Ghavami, P. K. (2015) BIG DATA GOVERNANCE: Modern Data Management Principles for Hadoop, NoSQL & Big Data Analytics, CreateSpace Independent Publishing.
44. Glaser, J. (2014) How The Internet of Things Will Affect Health Care, [Online]: http://www.hhnmag.com/articles/3438-how-the-internet-of-things-will-affect-health-care.
45. Goyen, M. (2016) Big Data and Analytics in Healthcare, Vol. 16, Issue 1, [Online]: https://healthmanagement.org/c/healthmanagement/issuearticle/big-data-and-analytics-in-healthcare.
46. Habib, K., Torjusen, A. and Leister, W. (2015) Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth, eTELEMED 2015: The Seventh International Conference on eHealth, Telemedicine, and Social Medicine, 73–78.
47. Harrison J.P. and Lee A. (2006) The Role of E-Health in the Changing Health Care Environment, Nurs Econ. 24(6):283–288.
48. Hasić, H. and Vujović, V. (2014) Civil law protection of the elements comprising the “Internet of Things” from the perspective of the legal owner of the property in question. Infoteh-Jahorina, Vol. 13. pp. 1005–1011.
49. Hassanalieragh, M. et al. (2015) Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges, IEEE International Conference on Services Computing, pp. 285–292.
50. Hillestad, R. et al. (2005) Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, And Costs, Health Affairs 24, no.5 (2005):1103–1117.
51. Hjelm, N.M. (2005) Benefits and drawbacks of telemedicine, J Telemed Telecare. 11(2): 60–70.
52. Hohmann, J. and Benzschawel, S. (2013) Data Protection in eHealth Platforms, R.G. Beran (ed.), Legal and Forensic Medicine, DOI 10.1007/978-3-642-32338-6_81, # Springer-Verlag Berlin Heidelberg.
53. Hossain, Md. M., Fotouhi, M. and Hasan, R. (2015) Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things, IEEE World Congress on Services, pp. 21–28.
54. Hu, F. (2016) Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, CRC Press, Taylor & Francis Group.

55. Intel (n.d.) The Internet of Things and Healthcare Policy Principles [Online]: http://www.intel.eu/content/dam/www/public/emea/xe/en/documents/iot-healthcare-policy-principles-paper.pdf.
56. Internet Society (2015) The Internet of Things: An Overview, Understanding the Issues and Challenges of a More Connected World, [Online]: https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf.
57. Institute of Medicine (2001) Crossing the Quality Chasm: A New Health System for the 21st Century, Academies Press.
58. IoT Architecture (2016) P2413 - Standard for an Architectural Framework for the Internet of Things (IoT), [Online]: http://standards.ieee.org/develop/project/2413.html.
59. Islam, S.M.R. et al. (2015) The Internet of Things for Health Care: A Comprehensive Survey, IEEE Access (Vol. 3), pp. 678–708, ISSN: 2169-3536.
60. Jog, Y. et al. (2015) Internet of Things as a Solution Enabler in Health Sector, International Journal of Bio-Science and Bio-Technology, Vol.7, No.2, pp. 9–24.
61. Kabene, S. M. (2010) Healthcare and the Effect of Technology: Developments, Challenges and Advancements, Premier Reference Source.
62. Kang, H. et al. (2015) A conceptual device-rank based resource sharing and collaboration of smart things, Multimed Tools Appl, Springer Science + Business Media New York.
63. Kansal, S. and Kaur, N. (2016) Multi-level Authentication for Internet of Things to Establish Secure Healthcare Network –A Review, International Journal of Advance Research, Ideas and Innovations in Technology, Vol. 2., Issue. 3, pp. 1–5.
64. Katagi, M. and Moriai, S. (n.d.) Lightweight Cryptography for the Internet of Things [Online]: https://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf.
65. Kendler, P.B. (n.d.) Trends in e-health, Wipro Technologies, [Online]: http://www.ehealthnews.eu/images/stories/pdf/trends_in_ehealth.pdf.
66. Keoh, S.L., Kumar, S.S., Tschofenig, H. (2014) Securing the Internet of Things: A Standardization Perspective, IEEE Internet of things Journal, 1(3), 265–275.
67. Kim, J. T. (2014) Privacy and Security Issues for Healthcare System with Embedded RFID System on Internet of Things. Advanced Science and Technology Letters. Vol.72. (Healthcare and Nursing). pp. 109–112.
68. Kirk, S. (2015) Healthcare: A $117B opportunity for the Internet of Things [Online]: https://www.ariasystems.com/blog/healthcare-a-117b-opportunity-for-the-internet-of-things/#sthash.VByNaXsz.dpuf.
69. Lake, D. et al. (2013) Internet of Things: Architectural Framework for eHealth Security, Journal of ITC Standardization.
70. Laxman, K., Krishnan and S.B., Dhillon, J.S. (2015) Barriers to Adoption of Consumer Health Informatics Applications for Health Self Management, Health Science Journal, Vol. 9, No. 5:7.
71. Li, J. et al. (2013) Health Care Provider Adoption of eHealth: Systematic Literature Review, Interact J Med Res. 2013 Jan-Jun; 2(1): e7.
72. Li, S., Tryfonas, T., and Li, H. (2016) The Internet of Things: A Security Point of View. Internet Research, 26(2), 337–359. 10.1108/IntR-07-2014-0173.
73. Löhr, H., Sadeghi, A.-R. and Winandy, M. (2010) Securing the E-Health Cloud. Proceedings of the 1st ACM International Health Informatics Symposium.
74. Lv, Z., Chirivella, J. and Gagliardo, P. (2016) Big data Oriented Multimedia Mobile Health Applications, J Med Syst, 40: 120.
75. MacIntosh, E., Rajakulendran, N. and Salah, H. (2014) Transforming Health: Towards Decentralized and Connected Care, MaRS Market Insights.
76. Maksimović, M., Vujović, V. and Perišić, B. (2016) Do It Yourself solution of Internet of Things Healthcare System: Measuring body parameters and environmental parameters affecting health, Journal of Information Systems Engineering & Management, Vol. 1, No. 1, pp. 25–39.

77. Martins, A.F. (2014) IEEE 11073 and Connected Health: Preparing Personal Health Devices for the Internet, IEEE International Conference on Consumer Electronics (ICCE), pp. 274–275.
78. Matusitz, J., and Breen, G. M. (2007) Telemedicine: Its effects on health communication. Health. Commun. 21(1):73–83.
79. McGrath, M. J., Scanaill, C. N. (2013) Sensor Technologies, Healthcare, Wellness and Environmental Application, Apress.
80. McKinsey Global Institute (2013) Big Data at Center of Disruptive Technologies [Online]: http://www.mckinsey.com/insights/business_technology/disruptive_technologies.
81. Meier-Hahn, U. (2013) European Commission publishes report on Internet of Things, [Online]: http://policyreview.info/articles/news/european-commission-publishes-report-internet-things/114.
82. Mukherjee, S., Dolui, K. and Datta, S. K. (2014) Patient Health Management System using e-Health Monitoring Architecture. IEEE International Advance Computing Conference (IACC). pp. 400–405.
83. Mukhopadhyay, S. C. and Leung H. (2010) Advances in Wireless Sensors and Sensor Networks. Springer-Verlag Berlin Heidelberg.
84. Mukhopadhyay, S. C. and Lay-Ekuakille, A. (2010) Advances in Biomedical Sensing, Measurements, Instrumentation and Systems. Springer-Verlag Berlin Heidelberg.
85. Mukhopadhyay, S. C. (2014) Internet of Things Challenges and Opportunities, Smart Sensors, Measurement and Instrumentation, Vol. 9, Springer International Publishing Switzerland.
86. Nakashima, H., Aghajan, H. and Augusto, J. C. (2010) Handbook of Ambient Intelligence and Smart Environments. Springer Science + Business Media.
87. Nandi, S. et al. (2014) Cellular Automata based Encrypted ECG-hash Code Generation: An Application in Inter-Human Biometric Authentication System, I.J. Computer Network and Information Security, 11, 1–12.
88. Neuhaus, C., Polze, A. and Chowdhuryy, M.M.R. (2011) Survey on Healthcare IT Systems: Standards, Regulations and Security, Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam.
89. Niewolny, D. (2013) How the Internet of Things Is Revolutionizing Healthcare - White Paper, [Online]: https://cache.freescale.com/files/corporate/doc/white_paper/IOTREVHEALCARWP.pdf.
90. Nugent C., Coronato, A. and Bravo, J. (2013) Ambient Assisted Living and Active Aging. 5th International Work-Conference, IWAAL 2013 Carrillo, Costa Rica.
91. Omanović-Mikličanin, E., Maksimović, M. and Vujović, V. (2015) The Future of Healthcare: Nanomedicine and Internet of Nano Things, Folia Medica, Facultatis Medicinae, Universitatis Saraeviensis, Vol. 50, No. 1.
92. OWASP (2014) Internet of Things Top ten [Online]: https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf.
93. Pang, Z. (2013) Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being, PhD Thesis in Electronic and Computer Systems, KTH – Royal Institute of Technology, Stockholm, Sweden.
94. Pitsillides, A. et al. (2006) DITIS: Virtual Collaborative Teams for Home Healthcare, Journal of Mobile Multimedia, Vol. 2, No.1, pp. 023–036, Rinton Press.
95. Qureshi, Q. A. et al. (2013) Infrastructural Barriers to e-Health Implementation in Developing Countries, European Journal of Sustainable Development (2013), 2, 1, 163–170.
96. Raghupathi, W. and Raghupathi, V. (2014) Big data analytics in healthcare: promise and potential, Health Information Science and Systems.
97. Rahmani, A.M. et al. (2015) Smart e-Health Gateway: Bringing Intelligence to Internet-of-Things Based Ubiquitous Healthcare Systems, 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), 826–834.
98. Raza, S. (2013) Lightweight security solutions for the Internet of Things, PhD thesis, School of Innovation, Design and Engineering, Malardalen University, Sweden.

99. Research and Markets (2016) IoT in Healthcare - Types, Technologies & Services, Applications, By Regions, Global Market Drivers, Opportunities, Trends, and Forecasts, 2016–2022, [Online]: http://www.researchandmarkets.com/research/8pjcct/iot_in_healthcare.
100. Rezvan, M. and Barekatain, M. (2015) The Sensors Are Innovative in Internet of Things, S. Mumtaz et al. (eds.): WICON 2014, LNICST 146, pp. 253–261, Springer Cham Heidelberg New York Dordrecht London.
101. Rodríguez-Mazahua, L. et. al. (2015) A general perspective of Big Data: applications, tools, challenges and trends, The Journal of Supercomputing, vol. 2, no. 8, pp. 3073–3113.
102. Said, O. and Tolba, A. (2012) SEAIoT: Scalable E-Health Architecture based on Internet of Things, International Journal of Computer Applications (0975–8887) Volume 59– No.13.
103. Santos, A., Macedo, J., Costa, A., Nicolau, M.J. (2014) Internet of Things and Smart Objects for M-Health Monitoring and Control, CENTERIS 2014 - Conference on ENTERprise Information Systems/ ProjMAN 2014 - International Conference on Project MANagement/ HCIST 2014 - International Conference on Health and Social Care Information Systems and Technologies, Procedia Technology 16:1351–1360.
104. Salvi, D., Villalba Mora, E. and Arredondo Waldmeyer, M. T. (2010) An architecture for secure e-Health systems. Universidad Politecnica de Madrid, Spain. Vol.1, pp. 2–4.
105. Sharp, J. (2013) Health Start-Ups! - The Internet of Things Creeps into Healthcare, [Online]: http://www.healthworkscollective.com/sharpjw1/112411/health-start-ups-internet-things-creeps-healthcare.
106. Shih, F. and Zhang, M. (2010) Towards Supporting Contextual Privacy in Body Sensor Networks for Health Monitoring Service. [Online]: http://www.w3.org/2010/policy-ws/papers/09-Shih-Zhang-MIT.pdf.
107. Stackowiak, R., Licht, A., Mantha, V. and Nagode, L. (2015) Big Data and The Internet of Things, Enterprise Information Architecture for a New Age, Apress.
108. Stein, J. (2015) The Emergence of the 'Internet of Medical Things'. Huffpost Tech. [Online]: http://www.huffingtonpost.com/josh-stein/the-emergence-of-the-inte_b_6801714.html.
109. Steinwachs, D. M. and Hughes, R.G. (2008) Patient Safety and Quality: An Evidence-Based Handbook for Nurses: Health Services Research: Scope and Significance (Chapter 8), Agency for Healthcare Research and Quality (US).
110. Suciu, G. et al. (2015) Big Data, Internet of Things and Cloud Convergence – An Architecture for Secure E-Health Applications, J Med Syst 39:141.
111. Suryadevara, N. K., Kelly, S. and Mukhopadhyay, S. C. (2014) Internet of Things Challenges and Opportunities: Ambient Assisted Living Environment Towards Internet of Things Using Multifarious Sensors Integrated with XBee Platform, Springer International Publishing Switzerland.
112. Suryadevara, N. K. and Mukhopadhyay S. C. (2015) Smart Homes, Design, Implementation and Issues, Smart Sensors, Measurement and Instrumentation, Volume 14, Springer International Publishing Switzerland.
113. Ta, V.-D., Liu, C.-M., Nkabinde, G. W. (2016) Big Data Stream Computing in Healthcare Real-Time Analytics, International Conference on Cloud Computing and Big Data Analysis, pp. 37–42.
114. Takpor, T.O. and Atayero, A.A. (2015) Integrating Internet of Things and EHealth Solutions for Students' Healthcare, Proceedings of the World Congress on Engineering Vol I WCE 2015, London, U.K.
115. Telefónica IoT Team (2015) 5 Amazing Things come true thanks to the IoT: eHealth Edition, [Online]: https://iot.telefonica.com/blog/5-amazing-things-come-true-thanks-to-the-iot-ehealth-edition.
116. Theodoropoulos, S. (n.d.) On the effectiveness of Publicly or Privately produced Health care services, [Online]: www.vsfs.cz/…/1_ws_3_1_theodopulos.doc.
117. Ting, D. (2015) The Internet of Things Can Revolutionize Healthcare, But Security is Key. [Online]: http://histalk2.com/2015/05/28/readers-write-the-internet-of-things-can-revolutionize-healthcare-but-security-is-key/.

118. Tsai, F. S. (2010) Security Issues in E-Healthcare, Journal of Medical and Biological Engineering, 30(4): 209–214.
119. Turner, J.W., Thomas, R. J., and Reinsch, N. L. (2004) Willingness to try a new communication technology: Perpetual factors and task situations in a health care context. J. Bus. Comm. 41(1):5–26.
120. Uniyal, D. and Raychoudhury, V. (2014) Pervasive Healthcare: A Comprehensive Survey of Tools and Techniques, arXiv:1411.1821 [cs.CY].
121. Vermesan, O. and Friess, P. (2014) Internet of Things – From Research and Innovation to Market Deployment, Rivers Publishers Series in Communication.
122. Waegemann, C. P. (n.d.) Confidentiality and Security for e-Health. CEO, Medical Records Institute (MRI). [Online]: https://www.itu.int/itudoc/itu-t/workshop/e-health/s5-05.pdf.
123. Wang, L. et al. (2012) Technology Enabled Knowledge Translation for eHealth: Principles and Practice, Healthcare Delivery in the Information Age (K. Ho et al. (eds.),) - Chapter 23: Low-Cost Health Care: Improving Care to Rural Chinese Communities Through the Innovations of Integrated Diagnostic Terminals and Cloud Computing Platforms, Springer Science + Business Media.
124. Weber, R. H and Weber, R. (2010) Internet of Things: Legal Perspectives. Springer-Verlag Berlin Heidelberg.
125. Weerasinghe, D. (ed.) (2009) eHealth - Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Germany.
126. West, D. M. (2016) How 5G technology enables the health Internet of Things, Center for technology innovation at Brookings.
127. Wickramasinghe, N. et al. (eds.) (2012) Critical Issues for the Development of Sustainable E-health Solutions, Healthcare Delivery in the Information Age, Springer Science + Business Media, LLC.
128. Wiecha, J. and Pollard, T. (2004) The Interdisciplinary eHealth Team: Chronic Care for the Future, J Med Internet Res 2004; 6(3): e22.
129. Wilkowska, W. and Ziefle, M. (2012) Privacy and data security in E-health: Requirements from the user's perspective. Health Informatics Journal 18(3) pp. 191–201.
130. Wilson, D.H. and Atkenson, C. (2005) Simultaneous Tracking and Activity Recognition (STAR) Using Many Anonymous, Binary Sensors. In Proceedings of the Springer Berlin Heidelberg, Pervasive computing, pp. 62–79.
131. Wootton, R. (2001) Telemedicine. Br. Med. J. 323:557–560.
132. Wright, D. (1998) Telemedicine and developing countries. J. Telemed. Telecare. 4(2) L2–37.
133. Yan, L. et al. (2008) The Internet of Things, From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications, Taylor & Francis Group.
134. Yang, G. et al. (2014) A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor and Intelligent Medicine Box, IEEE Transactions on Industrial Informatics.
135. Zhang, X., Yu, P. and Yan, J. (2014) Patients' adoption of the e-appointment scheduling service: A case study in primary healthcare, Investing in E-Health: People, Knowledge and Technology for a Healthy Future, H. Grain et al. (eds.), pp. 176–181, The authors and IOS Press.