*i*Journals: International Journal of Software & Hardware Research in Engineering (IJSHRE)
ISSN-2347-4890
Volume 10 Issue 1 January 2022

IoT (Internet Of Things) in Health Care (HIoT) Based on Cloud Infrastructure. HIoT Security Challenges

Authors: MSC. Malvina XHABAFTI[1]; MSC. Veranda SYLA[2]; MSC.Gerild QORDJA[3]

Mediterranean University of Albania[1,2,3], Department of Informatics and Scientific Education[1,2]; Department of Informatics and Scientific Fourmer[3]
malvinaxhabafti@umsh.edu.al[1]; verandasyla@umsh.edu.al[2]; gerildqordja@umsh.edu.al[3]

***Abstract*- The last decade has witnessed extensive research in the field of healthcare services and their technological upgradation. The Internet of Things (IoT) has shown potential application in connecting various medical devices, sensors, and healthcare professionals to provide quality medical services in a remote location. In combination with current sociological trends, the maturing development of IoT devices is projected to revolutionize healthcare. A network of body-worn sensors, each with a unique ID, can collect health data that is orders-of-magnitude richer than what is available today from sporadic observations in clinical/hospital environments. In this paper, we survey existing and emerging technologies that can enable this vision for the future of healthcare, particularly in the clinical practice of healthcare. Alsowe will see network security as a whole as well as medical equipment but also identifying risks and recommendations in relation to these issues.**

***Keywords* -IoT, HIoT; network security;health care IoT;clinical HIoT; healthcare analytics;digital health devices; cloud-based health care systems**

I. INTRODUCTION

Nowadays, Internet of Things (IoT) promises market potential in the field of e-health services and the telecommunication industry (Vermesan, 2014). The IoT can improve business intelligence in hospitals and facilitate patient service in the health sectors (Roman, 2011). Also it can improve health basics and prevent disease by providing ongoing monitoring activities for ordinary people or prone patients and moreover, it empowers patients and helps businesses benefit from this innovation (Bandyopadhyay, 2011). It further improves the patient's social problems, people's concerns about their health and quality of life (Helal, 2009) also contributes to economic prosperity in the health sector (Haller, 2009). With the help of this technology, hospital activities affect the environment (such as the production and disposal of hospital waste) and it can be better managed and less likely to harm the environment (Perera, 2014). IoT applications can develop several platforms that provide smart and innovative services for patients and people in need of medical care. Furthermore, it improves their health, safety, ease of access to emergency medical care, ongoing care and prompt support, while also improving their quality of life (Vermesan, 2014).A lot of benefits that IoT application offers in the healthcare sector is most categorized into tracking of patients, staff, and objects, identifying, as well as authenticating, individuals, and the automatic gathering of data and sensing. Hospital workflow can be significantly improved once patients flow is tracked. Additionally, authentication and identification reduce incidents that may be harmful to patients, record maintenance and fewer cases of mismatching infants. In addition, automatic data collection and transmission is vital in process automation, reduction of form processing timelines, automated procedure auditing as well as medical inventory management. Sensor devices allow functions centered on patients, particularly, in diagnosing conditions and availing real-time information about patients' health indicators.

The focus of our study will be on network security as a whole as well as medical equipment but also identifying risks and recommendations in relation to these issues. We first conduct a presentation of general information in the literature review section based on various researchers and then a study focusing on the safety of medical devices.In the following we analyze the challenges and risks faced by HIoT as well as recommendations regarding the practices to be followed to minimize the impact of these risks.

This study aims to answer the following questions:

• What is HIoT and how is it affecting our daily lives?

• What are some of the benefits of implementing HIoT?

• Are we safe from this technology and what are the risks we have to face?

II. LITERATURE REVIEW

A. IoT, definition and concept

The term "IoT" was spread from the research work done by the Auto-ID Center at the Massachusetts Institute of Technology (MIT) in 1999 (S.Sarma, 2000). IoT includes two concepts: "Internet" and "Thing", where "Internet" refers to "the world wide web of interconnected computer networks", based on a standard communication protocol, while "Thing" refers to "an object not exactly identifiable"(Commission, 2016). These concepts mean that any object can be addressed by an IP (Internet Protocol) and can act in a smart space, such as a health environment.

Another definition of IoT is "a dynamic self-configured dynamic network infrastructure with interoperable communication standards and protocols, where" physical and virtual "things have identities, physical attributes and virtual personalities and also integrate into the information infrastructure" (D . Metcalf, 2016). Indeed, the IoT is the global network that results in the interconnection of smart objects via Internet technologies, i.e. a set of supporting technologies needed to realize such a vision (including, for example, RFID, sensors, devices machine-to-machine communication, etc.) and the ensemble of applications and services that utilize such technologies to open new business and market opportunities (L.Atzori, 2010)

B. IoT Architecture and Features

The overall architecture and features of the IoT are quite different from the internet in terms of communication. For us it is normal that communication can be created anytime and anywhere, however, IoT has additional dimensions. So, the concept of IoT has some features that show multi-dimensional inclusion, information sharing and intelligent processing, which are:

- *Interconnected* - IoT helps people with devices and devices with other devices.
- *Smart Sensing* - Most devices and actuators have sensors embedded or connected to detect current conditions.
- *Intelligence*- IoT devices have several computing units and software used for smart decisions, forecasting and automation control.
- *Energy efficiency*-All IoT devices must be efficient and able to use recyclable energy, increase its energy utilization, if device application requires and permits it.
- *Expression (or data sharing)* - IoT-related devices have the ability to express and share their current state on all other connected devices. This allows for better flow of communication between the user and the machine.
- *Security*- IoT devices should help ensure the security of individual life. All smart medical devices are a good example of this feature.

Furthermore, IoT has functional features:

- Function to get information from things.
- Information exchange function.
- Function to process and control information intelligently.
- Large-scale function.

IoT is defined by its architecture, which is able to gather all the features and functions and make them function correctly and smoothly in a unique architecture.

There are two types of known architectures, 3-layer and 5-layer. We will look at the expanded architecture (5-layer) as it also covers business issues.

Figure 1 shows the architecture of the 5-layer type and includes the following layers (Gang, 2011):

- *Perception layer* (sometimes device layer or coordination and collaboration data collection). This layer deals with the data collected from things. For example, sensitivity devices. Physical layer analogy in the OSI networking model.
- *Network layer* (sometimes transmission layer). Transfers information from things to other things and to information processing systems.
- *Middle layer.* This layer is responsible for processing information and making decisions based on the analysis performed.
- *Application layer.* Provides applications based on object information processed in the middle layer.

- *Business layer*. Responsible for IoT ecosystem management.

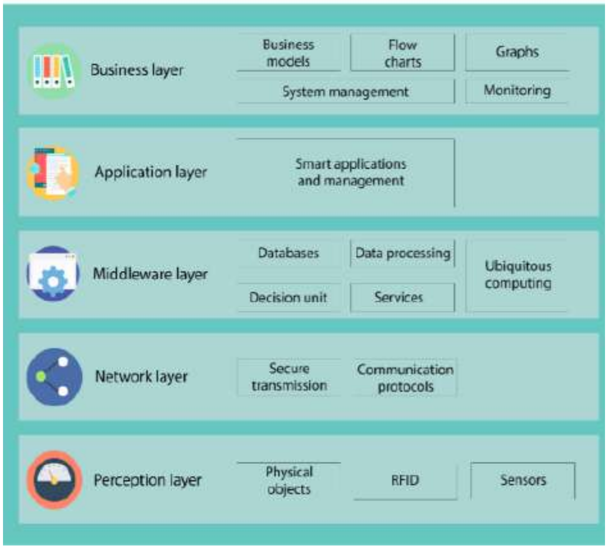

Figure 1: Architecture of IoT, (Gang, 2011)

C. Healthcare IoT

IoT in Healthcare

IoT health care support is increasing every day to improve access to care, increase the quality of care and most importantly reduce the cost of care (David Niewolny, 2013).

Based on the unique, biological, behavioral, social, and cultural characteristics of an individual, the integrated practice of well-being, health care, and patient support is referred to as personalized health care. This empowers each individual by following the basic principle of health care "proper care for the right person at the right time", which leads to better results and improved satisfaction thus making healthcare cost effective (I.Ungurean, 2013). A consistent service focuses on prevention, early detection of pathology, and home care rather than an expensive clinic, and controls overall well-being to anticipate needs and ensure compliance with health care plans. The IoT promises to manage the personalization of care services and can retain the digital identity of each person. Various devices are used in healthcare, to communicate and to make the system universal. Classifications of personalized IoT-based health care systems are Clinical Care and Remote Monitoring (Mikhail Simonov, 2010).

Cloud-based Health Care Systems

Cloud technologies have been extensively researched because of their usefulness in managing, processing, and analyzing big data.The literature on the use of cloud technologies for IoT Internet purposes has also been researched, such as smrat grid (S. Bera, S. Misra, and JJPC Rodrigues, 2015) and mobile computing for smartphones (P. Mach and Mr. Becvar, 2017). These works consider data storage and processing as the main advantages of cloud technologies. The use of cloud technology for storing health records is considered (N. Sultan, 2014) also part of cloud technology which examines this technology as a complete field. Preservation is further considered, with particular focus on how a large database can be used for data analysis and trend determination (L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, 2016). While each of these related works provides valuable insights into the field of cloud technologies, there is no known article that considers all the advantages, disadvantages, challenges, and opportunities that the cloud presents in WBANs and IoT-based health care systems. In this section, we bridge the gap in the literature by presenting recent works related to cloud-based healthcare, analyzing key challenges, and making recommendations for future research directions.

Much research has been done in recent years regarding the benefits of cloud systems for healthcare applications. These benefits stem from the three primary services that cloud technologies can provide in healthcare settings (Stephanie Baker, Wei Xiang, Senior Member, IEEE, and Ian Atkinson, 2018):

- *Software as a Service (SaaS)* - provides applications for healthcare providers that will enable them to work with health records or perform other relevant tasks.
- *Service Platform (PaaS)* - provides tools for virtualization, networking, database management, and more.
- *Service Infrastructure (IaaS)* - provides physical infrastructure for storage, servers and more.

These services can be used to accomplish a variety of tasks, but two main uses are easily identified in the literature; big data management and data processing.

Architecture of Healthcare Mobile-IoT

The Mobile-IoT architecture can remotely monitor patients using mobile devices to receive data from medical sensors via ECG signals, without the need for the patient to be present in the physician's office (Mr. Young, 2016).

This architecture consists of four levels:

a) *Sensing*
b) *Middleware gateway*
c) *Storage*
d) *Application*

In this architecture, it is necessary to use a mobile device, therefore a device has been designed and developed in order to meet the requirements of the current architecture which provides multiple communication interfaces to have multiple alternatives for internet connection (I.Ungurean, 2009).

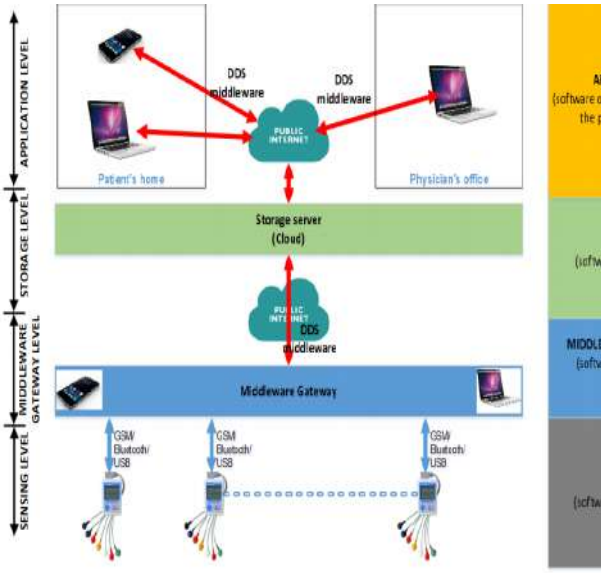

Figure 2: Architecture of HIoT,(C. Arcadius, B. Gao, G. Tian & Y. Yan, 2017)

1. *Sensing level* consists of devices that receive ECG signals. The ECG mobile device is used at home by the patient to receive and transmit ECG data to the central server via an Internet connection. If there is no Internet connection, the data is stored in an internal flash memory and transmitted to the storage server always if there is an active Internet connection (Ghasemzadeh, 2010).
2. *Middleware Gateway level* allows the transmission of data received from the mobile device to a central server where the data is stored. This level contains all the software infrastructure for mobile devices (smartphones, notebooks) needed to retrieve data from the ECG mobile device and transmit data to the central server. The MODBUS protocol is used to receive data in Bluetooth (Virtual COM), USB and GSM (SMS) command interfaces. This data is packaged and sent to the central server using the Data Distribution Service for real-time intermediation systems (DDS) (I.Ungurean, 2009).
3. At the *Storage level*, the patient's ECG data is stored for later viewing and analysis by the physician. In this case, a virtual cloud computing system is used that is focused on data storage. The system runs a server that allows data transfer from patients to be stored and respond to physician and patient requests.

4. At the *Application level* is the application for the m-IoT architecture. In this case, there are two software applications: one in the doctor's office and one in the patient's mobile device. For each request, doctors and patients must use authentication data to access the server (D.Kwon, 2011).

For each of the levels we present its specific characteristics and in this section we will avoid presenting examples.

Benefits of implementing Health Internet of Things

Clinical HIoT systems can have a substantial impact on medical quality and safety by integrating relevant decision-making automation tools and knowledge acquisition into medical providers' practices, reducing omissions resulting from gaps in provider knowledge or failing to and applied that knowledge to clinical practice. These systems, when integrated into larger HIoT systems, can improve medical decision-making and the proper use of diagnostic tests and therapeutic agents.

In the outpatient healthcare facilities, the use of HIoT offers many benefits (Catteddu D, Hogben G, 2009).

First, it can improve the efficiency and financial health of the practice. For years, many offices have used computer planning and financial systems to improve office processes by pursuing internship productivity and automating reimbursement processes.

Second, the use of electronic outpatient health records (EHRs) also provides an opportunity to monitor and improve clinical quality by improving access to information and reducing duplicate documentation. And tools based on "e-descriptive" technology can improve the effectiveness and safety of outpatient-prescribed practices as they have done in hospital facilities.

Following research based on some scientific literature we concluded that a summary of the main basic benefits are:

- The IoT promises market potential in the field of e-health services and the telecommunications industry (Vermesan, O. &Friess. 2014).
- The IoT can improve business intelligence in hospitals and facilitate patient service in the health sectors (Roman, R., Najera, P. & Lopez, 2011).
- The IoT can improve the health and disease prevention by providing ongoing monitoring activities for ordinary patients and also helping

businesses benefit from this market innovation. (Bandyopadhyay, D. & Sen, 2011).

- Further improves the patient's social problems, people's concerns about their health and quality of life also contributes to economic prosperity in the health sector (Haller, Karnouskos, S. &Schroth, 2009).
- IoT applications can develop several platforms that provide smart and innovative services for patients and people in need of medical care. Furthermore, it improves their health, safety, ease of access to emergency medical care, ongoing care, and rapid support, while also improving their quality of life (Vermesan, O. &Friess, 2014).

III. HIoT SECURITY, RISKS AND RECOMMENDATIONS

Since individuals' health records are often a target for malicious attacks leading to the exposure of this sensitive information, some problems may arise if patients can not believe that their personal information will be provided and used solely for the purpose of required. Patients may intentionally hide or not seek medical help to avoid the consequences that may come from disclosing this information (Salama, U., 2018).

The protection of health data obtained from various sensors and devices makes illegal access critical to the adaptation of an HIoT model. Therefore, strict security policies and technical measures should be introduced to share health data with authorized users, organizations and applications. (Islam, S.R, 2015)

Also the healthcare domain can be a target of attackers because the devices and applications are related to personal information, presenting healthcare data. To have a full adaptation to HIoT, it is of particular importance to identify: security requirements, vulnerabilities, threat patterns, countermeasures. (Milanovic, D. et al. 2017).

In this section we will present some of the vulnerabilities or risks to be considered in cloud-based architecture and also in smart medical devices. In addition to the risks, some recommendations will be given that are derived from the study of works as the most appropriate to be considered.

A. Cloud IoT Security

Cloud computing provides the optimal solution that meets the health system requirements for both on-demand storage and processing services. It provides a healthcare environment with an affordable and easy-to-manage infrastructure that is available anytime, anywhere, which is also highly scalable to facilitate large numbers of actors and millions of data. But, on the other hand, the issue of providing this health sensitive information to cloud providers leads to some serious privacy concerns.

The architecture reviewed in this paper presents how HIoT components interact with each other and how information flows based on the cloud. But despite the advantages and new developments in technology, cloud security remains a hot issue regarding unauthorized access, security breach attacks and privacy of personal data. Here we will present some attacks and how they can be avoided or solved.

According to Zhou, J. (2017) the main areas that provide threats and recommendations should be provided are:

Identity privacy, location privacy, Node Compromise Attack, Layer Removing / Adding Attack, secure Forward and backward, Semi-Trusted and / or Malicious Cloud Security. As part of our overall analysis of security issues and challenges in the architecture that unites IoT, Cloud, and smart medical devices, we will consider identity privacy,Node Compromise Attack, and forward-backward security.

- *Identity privacy:* Conditional identity privacy refers to the fact that the true identity of the IoT user must be well protected by the public; on the other hand, when any dispute arises in an emergency, the tracing must also be done effectively by the authority. To achieve this goal the nickname technique has been widely adopted, but periodically updated nicknames and certificates lead to high and sometimes intolerable costs for nodes implementing IoT. In the worst case it can not resist the physical attack of dynamic tracking (Zhou, J., 2017).On the other hand in a review by Cook, A. et al (2018), identity privacy is seen as an important point. Encoding and encryption of identity is recommended. This is efficient in terms of audit time and communication cost but does not take into account traceability.
- *Node Compromise Attack:* This means extracting and attacking resource-restricted IoT devices. Thus it obtains access to all private information including the secret key used to encrypt packages, the private key to generate signatures, and so on, and then reprograms or replaces IoT devices (Zhou, J., 2017). Furthermore in HIoT, compromising a device can lead to chain compromises and can lead to interception of communication and packet flow where we have privacy breaches. In the case of maliciousattacks it can cause damage to the system and to people whose health is monitored.

- *Forward and backward security:* Due to the mobility and dynamic movements that occur in groups and networks on the Internet of Things, it is necessary to achieve forward and backward security. The first means that users who have just joined IoT can only decrypt encrypted messages received afterwards, but not before they become part of the network; while the second means that it is the revoked or canceled user that can only decrypt encrypted messages before leaving but not after leaving (Zhan, J. et al, 2017).This type of security is effective in terms of computer complexity, communication costs, and confidentiality of user access privileges, but on the other hand attacker prediction models are limited (Cook, A. et al, 2018).

This may be related to Healthcare so that the information communication encryptions from the application to the data collection node are not decrypted and are secure even in the case of the introduction of a new user or the removal of an existing one.Given the architecture presented in this paper, in the data of a patient or elderly we may have some accepted and authenticated users who receive encrypted data so this analysis is important.

B. Safety of smart medical devices

In this chapter, we will talk about the potential risks of IoT Health Care and their correlation with the benefits to society. Previously, many different advantages of telemedicine were introduced, but in this chapter we will analyze the risk landscape behind the good promises of digital healthcare, understand the sources of risk in modern network medical devices, and finally prepare recommendations to maximize value for patients by minimizing the security risks posed by software, hardware, firmware, and communication technologies across personal medical devices. The purpose of this chapter is to find the balance between clear benefits and the ability to defend the technology and communication bases of modern equipment.

To understand the risks, we will first briefly analyze the purpose of digital medical technologies to show the roots of security problems.

One of the main ideas of the HIoTis to individualize medicine by allowing people to choose the equipment and systems needed to meet their health goals, which poses the first risk - now every medical device owner can be personally attacked. Another advantage of digital healthcare is the constant monitoring and large amounts of statistical data. Health monitoring products provide real-time feedback on nutrition, heart rate, blood pressure and other vital signs. All data collected must be provided. Finally, IoT brings automation as part of digitalization, enabled by artificial intelligence, consequently the system can make mistakes, followed by wrong injections or wrong medication recommendations, which can affect the patient's condition or even kill him .

Concerns about the safety of HIoT equipment

Society's desire and technological ability to use networking technologies always exceeds their ability to control the security of these technologies. Medical devices on the net are no exception. They offer great benefits to the modern healthcare system, so that developers and adopters turn a blind eye and try not to notice serious safety gaps in new products. The situation will remain the same or worsen if security officials and equipment makers do not take the steps that need to be integrated.

There are four main and related areas of health care that pose concerns for the Internet of Things (Harries, 2014):

a) Accidental failures;
b) Protection of patient privacy;
c) Intentional termination;
d) Widespread disruption;

- *Accidental failures* are the most obvious problem, which reduces the overall trust of users, because if any major failure occurs, society will reject medical devices in the network, delaying the evolution of healthcare and medicine for years. People can trust doctors, but it is always difficult to trust the device if there is a mechanical fault that then leads to an irreversible consequence. Medical devices on the network are vulnerable for more than just criminal purposes. Like any other mechanical device, digital or technological, they can be completely destroyed or their behavior can be changed to a more suitable format. This is not the result of inadequate engineering or poor equipment. This is the result of manufacturing defects, software errors or other circumstances affected by millions of conditions. The complexity of the equipment and operating technology that controls physical processes, such as pumps, creates exponential opportunities for defects in design, implementation, or operation, any of which can lead to dramatic accidental failure. The probability of failure should be small when it comes to medical devices compared to other network technologies.
- *Protecting patient privacy* is another issue to be concerned about. According to the Global State of Information Security survey, the number of security breakdowns reported by healthcare providers increased dramatically by

60% from 2013 to 2016, which is almost double the risk increase, compared to with other industries and systems. The main point and second concern is the protection of the patient's personal and private data, as it is considered to be the most valuable information for attackers and other threats, (PwC, 2016). Danger to medical devices on the network poses great difficulties for the owners of these devices, as they monitor, access and store patients most personal information - biological and medical records. To meet the IoT paradigm, all devices must have a wireless communication module to be able to transfer data anytime and anywhere, so the ability of wireless networks is one of the key points of Smart Health Care to achieve high efficiency.On the other hand, as with any wireless solution, the user wants to be sure that there is no transmission of unencrypted personal data, or that there is no backdoor on the device from the network. In addition, some smart devices are capable not only of health monitoring but also of billing (doing financial operations online), used as a separate feature or as an extension for medical purposes. The riskiness of such solutions puts patients at risk of losing medical and banking information; both types are also private. Since HIoT is still in its infancy, no one knows how information can be used by criminals however there is a solid understanding about what needs to be ensured to avoid eavesdropping or data loss.

- *Intentional termination* is another concern. Racketeers, terrorists and other criminals seek to exploit as many vulnerabilities in the entire IT infrastructure as possible to commit crimes and cause chaotic situations. When it affects banks or transportation systems, the consequences are manageable by the government, however, when a device is on a person or even under his skin, the consequences of cybercrime committed using that device can be particularly personal and threatening. A pacemaker is a good example. It is possible for criminals to associate with him and kill the person. The same thing can happen with insulin pumps or any medication delivery system.
- *Widespread disruption* is a very suspicious risk, but since medical devices are connected to the global network, some targeted malware can spread on the Internet and act against only selected medical devices, so all with vulnerable devices affected by this malware. This is a rather dubious scenario; however, it still needs to be considered.

Although HIoT poses many risks, almost half of PwC respondents have integrated medical devices into their enterprise information systems, however, they have not optimized the security and privacy of these smart devices.

- 37% said they contacted the manufacturers encountered in the user manual to understand the safety capabilities of medical devices and the potential risks to users, only 59% of the previous 37% conducted a solution risk assessment.
- 56% of this 59% implemented some additional security checks, which is a small amount of all respondents, which confirms that people want to use new devices much more than to ensure that they are safe(Lee, 2016).

To summarize, we will demonstrate an example situation, which shows the lack of safety in insulin pumps, which are the most widely used solutions for monitoring / automating smart health solutions. Two analysts, Jay Radcliffe and Barnaby Jack, have analyzed insulin pumps. In 2011, Radcliffe discovered that knowing the serial number of the insulin pump would allow connection to it from 100-150 meters. Since these devices have almost no security today, an attacker can turn off the pump or cause an insulin overdose with cheap and common electronic devices. Later, Jack discovered a way to compromise an insulin pump even without the serial number. This would allow an attacker to scan for any nearby device, rather than targeting a specific device identified in advance. (Finkle, 2016).

Risks, recommendations for adjustments and safety

The sources of safety risks in smart healthcare devices are quite general, as a range of technologies is the same for many technological solutions of recent years. However, medical devices are well regulated, consequently this produces a new range of risks due to these concisely defined rules but, which may have an improper approach that can be exploited.

The software and firmware used in medical devices are a different and completely inconsistent mix of different standards, their versions and connection methods, where the one who enters the market first gains a good reputation, the preferences of the manufacturer or the patient.

Mostly, the size of the device is critical to the choice of technology and standard, which makes our analysis more difficult, as small specific devices, tend to perform accurate monitoring. Furthermore, battery life is critical for devices that will be attached to the body such as those body sensor device.So, for example "pacemakers" operate with custom processing units and personalized operating systems, which almost guarantees security, as device makers can not work on a product for a long time, investing big money. It is quite surprising because people would prefer the high security device, which is even more expensive, instead of the cheap work solution with poor safety capabilities.

Since smart healthcare devices must be connected to the internal world, the communication technologies used are more standardized than the other components of the devices, due to existing communication protocols and regulated technologies.

While in a network of a local hospital with stationary equipment there are some defined boundaries and permanent, consistent needs, network professionals can monitor and update security in a fairly easy way, ranging from simple ACLs and traffic jamsto some advanced hardware and constant hardware and firmware updates. For smart medical devices, which are placed on the body and held, the situation is different - there is the challenge of regulating vulnerability as they are detected and fall prey to attack. If, for example, a device is surgically installed, adjusting the software or firmware is not always possible, while changing the hardware requires a risky operation.

Moreover, updating normal network equipment does not require rules, when some manufacturers avoid changes and even security updates, as re-approval of the audit agency is required. So, patching a medical device remains costly and difficult, as device makers must prove that the patched device still meets all installed medical requirements.

To complete the risk source analysis, access control management is a major dilemma for device makers, as greater access to personal data is done by the device, therefore, the healthcare device must be well secured and protected from unauthorized access and intrusion. This question is very hot especially for automation systems and equipment for monitoring chronic diseases. Different manufacturers have different approaches to finding the perfect balance in security and accessibility for authorized personnel. Some companies restrict all types of access except the data master. In this case, all the credentials are stored somewhere, and patients prefer to keep them close in case of an emergency situation so that doctors can easily access the equipment. The main obstacle here is that criminals are also able to gain access to this information. Other manufacturers increase the emphasis on security by avoiding such encrypted credentials, but they have a high risk that personnel will not receive the right information in extreme situations.

IV. RECOMMENDATIONS

Some recommendations for further device innovation at Healthcare Internet of Things and for risk minimization are:

1. *The first requirement for medical device manufacturersto build a good and smart solution is the "secure-by-design" approach to research and development.* This means that safety should be the number one issue when designing and building the product. It should not be added later, as it was in the past, what caused various challenges. For example very often security experts had to face well-closed points by developers who were trying to implement security on a device after it was added.Adding safety features to the product after its engineering is a job that leads to loss, because it is completely ineffective to try to secure systems that are already in use.
2. *Improving the cooperation of public organization with public and public with private is another recommendation*.HIoT and medical device management are overcrowded with various regulations which do not fit the real needs of the evolution of medicine in the digital age. Adding more regulations will only make the situation worse and greater coordination is important. The truth is that regulators are not as fast with technological innovation. To deal with rapid change, regulators seek feedback from all actors involved through transparent, collaborative forums, which ensure the independent function of regulators.The safety improvement process requires discussions and places to talk about them, providing clarity in terms of the proposed arrangements, reaching agreement on how to promote innovation and produce a safe product that serves the public interest. Manufacturers should also continue to improve communication between them. For example, the Industrial Internet Consortium (IIC), formed by Intel, IBM, Cisco, AT&T, and Microsoft, is an example of how industry collaboration can help unlock business value while improving security.The EU may consider such models for adopting new rules. The current EU procedures for the approval of digital medical devices are quite short and outdated. The European Parliament is considering new regulations that will promote security as well as innovation. However, some manufacturers worry that such rules will create unnecessary layers of bureaucracy and delay patient access to new products, which is the number one issue to avoid.
3. *Current regulatory methods and the whole paradigm need to be adapted to encourage innovation in this area, while still meeting security and public needs.* Most regulations

give officials only a brief look at the new medical device before it goes directly to consumers. The good method here is to compare new solutions with existing ones and determine the risks and benefits of treating identical problems. There is a need to classify the proposed product and review its risks and benefits to society. Such processes already exist. For example, the FDA 510 (k) process, the Dutch European agencies and the international Continua alliance. All regulations need to be modern and meet current technologies, as some equipment manufacturers use older technologies because they are sure they will obtain the approval of officials. This shrinks innovation dramatically, which in turn reduces security and increases vulnerabilities. One possible solution here is a simplified approval process, suggested by McAfee.

4. *It is necessary for a proposed model to provide a voice for the public, especially for patients and other users involved in the process.* In most countries, governments and private companies do not consider the public interest in medical matters. This dramatically affects the quality of service by not making the right jokes and searches for usability, effectiveness and safety.Regulators have already recognized the value of public input, especially from patients. This approach should be industry-wide and provide specific guidance on how feedback from patients, and from the public should be gathered and become part of the regulatory process.

V. CONCLUSIONS

This paper presents some of the main benefits that the implementation of Healthcare IoT brings, where among the main ones are those in cost and time.

On the other hand as expressed by the literature and recent studies using different models and different frameworks that have made efforts to give the main points where a reliable HIoT should be supported. However as we discussed in the last section, the lack of standardization brings some obstacles to the evolution and rapid development of HIoT. Some aspects of security and privacy need to be improved such as: identity privacy, location privacy and compromising that can be done to the various component nodes. Traditional defenses such as pseudonymity, connection anonymization or data signature are not enough to adapt to new attacks and modes.

The safety of medical devices is seen in a broader perspective. Problems arise here in both hardware and regulatory policies. Regulatory policies in the EU continue to be rigid and not adapt to major developments. Secondly, a greater movement is needed in a macro framework to increase the trust of patients and users and also the cooperation between organizations to increase because these implementations have a large scope.

REFERENCES

Bandyopadhyay, D. & Sen, J.: *Internet of things: Applications and challenges in technology and standardization*. In: Wireless Personal Communications, 58(1), pp. 49—69;2011.

Catteddu D, Hogben G. ”*Cloud computing: benefits, risks and recommendations for information security.”* Heraklion: European Network and Information Security Agency; 2009.

Cook, A., Robinson, M., Ferrag, M.A., Maglaras, L.A., He, Y., Jones, K. DheJanicke, H.,(2018). *Internet of Cloud: Security and Privacy Issues. In Cloud Computing for Optimization: Foundations, Applications, and Challenges* ,fq. 271-281.

Cory, T. (2009), *“Building M2M services means overcoming new challenges”*, Telecom Engine, December 13, fq 385.

D. Metcalf, S. T. J. Milliard, M. Gomez, M. Schwartz (2016), "*Wearables and the Internet of Things for Health: Wearable, Interconnected Devices Promise More Efficient and Comprehensive Health Care,"* in IEEE Pulse, vol. 7, no. 5, fq. 35-39.

Dihn, H.T.; Lee, C.; Niyato, D.; Wang, P. (2013), ‘*A survey of mobile cloud computing: architecture, applications, and approaches’*, fq 13-15.

E. Agu et al., (2013) ,"*The smartphone as a medical device: Assessing enablers, benefits and challenges*" 2013 IEEE International Conference on Sensing, Communications and Networking (SECON), New Orleans, LA, fq. 76-80.

F. W., (2014) *Making Care Mobile: Introducing the apps pharmacy*

Finkle, J.,(2016). *U.S. Government Probes Medical Devices for Possible Cyber Flaws*.

FIPS PUB 140-2,(2001) ‘*Security Requirements for cryptygraphicmoduless,’*, Gaithersburg, Maryland,fq 13-20

Haller, S., Karnouskos, S. &Schroth, C.: *The internet of things in an enterprise context*. In: Springer Berlin Heidelberg. pp. 14—28; 2009.

Harries, P., (2014). '*The Prognosis for Healthcare Payers and Providers: Rising Cybersecurity Risks and Costs*' fq. 290-301.

Helal, A., Cook, D. J. & Schmalz, M.: *Smart home-based health platform for behavioral monitoring and alteration of diabetes patients. In: Journal of diabetes science and technology*, 3(1), fq. 141--148. (2009)

Hong, Y.J.; Kim, I.J.; ChulAhn, S. dhe Kim, H.-G (2010), ' *Mobile health monitoring system based on activity recognition using access parameters. Simululation Model, Practices and Theory*.'18, fq 446–455.

I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, M. V. Meyerstein,(2009), "*Trust in M2M communication*," Vehicular Technology Magazine, IEEE , vol.4, no.3, fq .69-75.

IEEE (2011), "*The potential of Internet of m-health Things m-IoT for non-invasive glucose level sensing*."In: Conf Proc IEEE Eng Med Biol Soc

Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M.dhe Kwak, K.S.,(2015). *The internet of things for health care:* a comprehensive survey. *IEEE Access*, *3*, fq.678-680.

J. Chambers, (2013) "*Internet of Everything",* Cisco, February 21, ,http://www.cisco.com/assets/sol/dc/internet_of_everything.pdf data e aksesit : 28/05/2018

J. S. Winter,(2012) "*Privacy and the Emerging Internet of Things: Using the Framework of Contextual Integrity to Inform Policy*", Pacific Telecommunications Council Conference Proceedings,

Jara, A. J. , Zamora-Izquierdo, M. A. dheSkarmeta, A. F.(2016) "*Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things,*" in IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, fq. 47-65.

K. Chang, A. Soong, M. Tseng, and Z. Xiang, (2011)"*Global Wireless Machine-to-Machine Standardization,"* IEEE Internet Computing, vol.15, no.2, fq .64-69.

Kwak, K.S.; Ullah, S.; Ullah, N. (2010), '*An overview of IEEE 802.15.6 standard. In Proceedings of the International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL)*', Roma, Italy.

Kwon, D. M. Hodkiewicz, R. J. Fan, T. Shibutani,Pecht, M. G. "*IoT- Based Prognostics and Systems Health Management for Industrial Applications,"* in IEEE Access, vol. 4, no. , fq. 3659-3670

L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, "*Mobile Cloud Computing Model and Big Data Analysis for Healthcare Applications,*" IEEE Access, vol. 4, pp. 6171–6180, 2016.

L. Atzori, A. Iera, G.M.: *"The Internet of Things: a survey, (2010*). " Computer Networks. vol. 54, fq. 2787–280

Lee, S. M., (2014). *Genentech CEO wonders if wearables craze is 'a bit trivial,*s.l.: San Francisco Chronicle fq. 12-15.

M. Balazinska, A. Deshpande, M.J. Franklin, P.B. Gibbons, J. Gray, S. Nath, M. Hansen, M. Liebhold, A. Szalay, V. Tao, (2007), "Data Management in the Worldwide Sensor Web," IEEE Pervasive Computing, vol.6, no.2, fq. 30-40.

Milovanovic, D. dheBojkovic, Z.(2017). Cloud based IoT healthcare applications: Requirements and recommendations. *International Journal of Internet of Things and Web Services*, *2*, fq.60-65.

N. Sultan, "*Making use of cloud computing for healthcare provision: Opportunities and challenges*," International Journal of Information Management, vol. 34, no. 2, pp. 177–184, 4 2014.

Niewolny, D. (2013),' *How the Internet of Things Is Revolutionizing Healthcare, Freescale Semiconductors*'.

Simonov,M., Zich,R., dheMazzitelli, F. (2012) '*Personalised healthcare communication in Internet of Things* 'vol.3, no.6, fq.241-246.

Ogunduyile, O.O.; Olugbara, O.O.; Lall, M. (2013), '*Development of Wearable Systems for Ubiquitous Healthcare Service Provisioning*. APCBEE Procedia', fq. 163–168.

P. Appavoo, M. C. Chan, A. Bhojan, E. C. Chang, (2016)"*Efficient and privacy-preserving* *access to sensor data for Internet of Things (IoT) based services*," 2016 8th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, fq . 1-3.

Perera, C., Zaslavsky, A., Christen, P. &Georgakopoulos, D. (2014) '*Context aware computing for the internet of things*: A survey. In: Communications Surveys & Tutorials, IEEE 16.1, fq: 414 -- 454.

R. Ram, et al. (2013) "*UniversAAL: provisioning platform for AAL services*." Ambient Intelligence-Software and Applications. Springer International Publishing, 2013. fq. 105-112.

R. T. Mercuri, (2004) "*The HIPAA-potamus in health care data security*."Communications of the ACM, vol. 47, no. 7 ,fq. 25-28.

Roman, R., Najera, P. & Lopez, J.: *Securing the internet of things*. In: Computer, 44(9), pp. 51—58;2011.

S. Bera, S. Misra, and J. J. P. C. Rodrigues, "*Cloud Computing Applications for Smart Grid: A Survey*," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 5, fp. 1477–1494, 2015.

S. Brave, C. Nass, dhe Hutchinson, K. (2005), "*Computers that care: investigating the effects of orientation of emotion exhibited by an embodied computer agent*", International journal of humancomputer studies 62.2 fq.161-178.

S. Kirk, (2014), "*The Wearables Revolution: Is Standardization a Help or a Hindrance?: Mainstream technology or just a passing phase?*", Consumer Electronics Magazine, IEEE 3.4 fq.45-50

S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, K. S. Kwak, (2009), "*The Internet of Things for Health Care: A Comprehensive Survey*," in IEEE Access vol. 3, no. , fq. 678-708.

Salama, U., Yao, L. dhe Paik, H.Y.(2018), *An Internet of Things Based Multi-Level Privacy-Preserving Access Control for Smart Living*. In *Informatics* (Vol. 5, No. 2, p. 23). Multidisciplinary Digital Publishing Institute fq. 1-10.

Smith, J. O.(2010), "*The Coming of Age of M2M Standards*," Connected World Conference, Keynote presentation.

Stephanie Baker, Wei Xiang, Senior Member, IEEE, and Ian Atkinson. "*Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities": * fq.14-15,2018.

Thierer, A. D. (2014)"*The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation*", Available at SSRN 2494382,.

Vermesan, O. &Friess, P. (2014) *Internet of Things-From Research and Innovation to Market Deployment*. In: River Publishers.

W. Zhao, C.W., Nakahira, Y. (2011)' *Medical Application On IoT. In: International Conference on Computer Theory and Applications* ' (ICCTA). fq. 660–665

Yang, Z., Zhou, Q. Lei, L.dheZheng, K., Xiang, W. (2016). *An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare.* Journal of medical systems, 40(12), 286.

Zhou, J., Cao, Z., Dong, X. DheVasilakos, A.V.,(2017). *Security and privacy for cloud-based IoT: Challenges. IEEE Communications Magazine*, *55*(1), fq.26-33.