IoT Ethics Challenges and Legal Issues

Ahmed AboBakr
Nisc research center.
Nile University
Cairo, Egypt
aaali@nu.edu.eg

Marianne A. Azer
National Telecommunication
. Institute, Nile University
Cairo, Egypt
mazer@nu.edu.eg

***Abstract*—** IoT systems have different technologies such as: RIFD, NFC, 3G, 4G, and Sensors. Their function is to transfer very large sensitive and private data. There are many ethical challenges that need to be taken into consideration by individuals and companies that use this technology. Amongst the challenges is the user awareness of attack risks. This paper discusses different ethical and legal challenges that need to be taken in account for IoT health care applications during the near future.

Index Terms: Big Data, Ethics, IoT, legal Issues, Morals, Policy

I. INTRODUCTION

The past ten years have encountered many changes in people's lifestyle and everyday habits. This is due to affordable low-cost, low-power communication technologies that made it possible for everyday objects to be part of the human-centric networks, thus creating the Internet of Things (IoT). Within the next fifteen years, most of the medical care services will be delivered virtually. It is expected to have 24/7 diagnostics monitoring from phones, wearables, handheld specific devices. This will result in a dramatic growth in sensing technologies from hospitals to the end users. The integration of these important and valuable devices owned by physicians, patients and related ones, into medical records is one of the most challenging and promising research topics within the next ten years. There will be millions of IoT devices that need new security policies associated with legal challenges and requirements. Researches have discussed new proposed healthcare systems and expected challenges including, privacy, authentication, node failure, and many different aspects [1-7]. This paper focuses on policy, security requirements and challenges for the companies that may provide the healthcare service virtually using IoT devices for real time monitoring the patients status.

The remainder of this paper is organized as follows. Section II presents related work. Section III introduce a brief description of a typical IoT system and its components, while section IV presents challenges, ethical and legal issues for IoT medical applications. Finally, section V concludes this paper.

II. RELATED WORK

In this section, we present the work that has been done in the literature in security and privacy of IoT. In [1], a discussion of how Australian privacy principles could protect the individual privacy in a new IoT environment that offers high stream collected data. A legal evolution was proposed to overcome specific challenges. This is done through setting dynamic modifiable policy rules by an international legal body to be specialized in control and accountability of IoT legal issues

In [2], the business that may be built upon the IoT technology to convert this huge amount of data to money was studied. Moreover, the challenge of protecting the users' privacy in these types of businesses was tackled. The paper introduced a different approach to the users regarding the interaction with IoT based on implementing a policy based framework.

Expected security and privacy challenges that will face IoT in the near future were introduced in [3]. The lack of international agreements related to data privacy and protection was addressed. According to [3], expected challenges will occur due to the huge number of devices connected and big data exchanged between devices in typical IoT network, any security or privacy breach will have a huge impact on the involved stakeholders. New measures have been suggested to ensure the system flexibility to attacks, client data privacy, access control, data encryption. It has been found in [4] that the best way to deal with security and privacy challenges is to implement a framework of key principles by legislators in an international level, with the aid of private sector to implement detailed regulations.

Table 1 IoT classification scheme

TECHNOLOGY	Hardware	*RFID*
		Near Field Communication
		3G/4G Wimax
		Sensors
	Software	*Middleware*
		Firmware
	Architecture	*Hardware Architectures*
		Software Architectures
		Network Architectures
APLICATIONS	Smart Infrastructure	
	Healthcare	
	Smart appliances Logistics	
	Social Applications	
CHALLENGES	Security Challenges	
	Privacy Challenges	
	Legal/Accountability Challenges	
	General Challenges	

978-1-5386-1191-3/17/$31.00 ©2017 IEEE

In [4], the authors investigated detailed interoperability and security issues related to healthcare IoT applications including benefits, difficulties and problems of employing and integrating different IoT devices in health care systems. Others in [6], [7], [8], and [9] discussed some questions related to the future of human being in a world with 70 billion cars and 7 billion of humans and thousands of billions of connected devices to internet infrastructure.

Until now, the market doesn't offer flexible products that can be used interchangeably [4], but only specific devices offered by manufacturers that allow access to pre-configured servers. This closed solution is not the optimum one when integration billions of IoT devices in a broader system, middleware using Service-Oriented Architectures (SOA) mechanisms as basis for middleware architecture in embedded networks is required.

Table.1 shows IoT classification scheme, including hardware, software, and challenges to simplify the process of locating the sub category in which the challenges occur, addressing the solution will be more efficient [1-9]

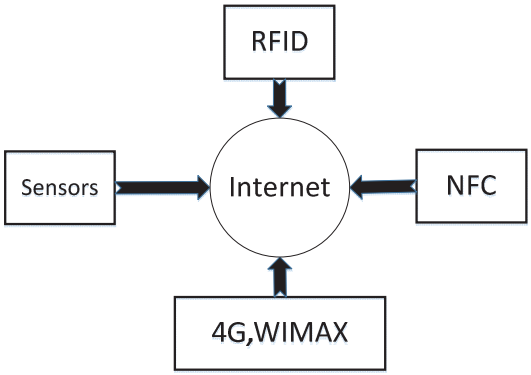

Fig. 1. Typical IoT block diagram [5]

III. TYPICAL IOT SYSTEM COMPONENTS

IoT depends on a worldwide infrastructure system, which interfaces physical and virtual objects in a unique system, by using the information gathered by the sensors, the hardware utilized for communication and positioning as shown in Fig.1 [5].

The idea of IoT has spread by consolidating innovations, for example, Near Field Communication, 2D bar code, remote sensors, localization and positioning, 3G or 4G networks and even 5G networks as stated in [6].

Radio Frequency Identification (RFID) is an innovation which utilizes electromagnetic fields to consequently distinguish objects, by marking them with a chip or receiving antenna, called "tag"[10]. The tag sends a unique electronic code which is collected by a receiver which can be set anyplace. The labels are all unique and RFID can be utilized to consequently track objects, including those connected to individuals (IDs, license, time labels, armlets for students) and those implanted or embedded inside human or under skin (for therapeutic purposes, additionally for the VIP access in specific zones). It has been widely used in hospitals to monitor patients and their medications and even locate them in case of any breaches. Additionally, labels can be connected to cell phones for different reasons.

The sensors used in typical IoT systems can have many types, according to the required application. For example medical application proximity, temperature, blood pressure, sugar level,… etc.. Just a little part of the electronic and family unit gadgets sold these days do not contain sensors.

These sensors are the key players for transforming the physical world to the virtual IoT world. Some of these sensors are Nano sensors, specifically sensors used in measuring very small dimensions. They can be utilized to analyze illness, for example, AIDS, to recognize the level of contamination in water.

IoT utilizes positioning technology. There are different technologies for long range positioning and localization. The most famous one is GPS. GPS uses satellites to monitor (vertically and horizontally) the position held by a client, his speed and current timing. It can be utilized anywhere in the world, including on planes, boats [11].

Near Field Communication (NFC) is a radio electronic device, on a frequency of 13.56 MHz, which can be used to communicate two devices when the range between these devices does not exceed 20 cms. The most valuable use of NFC are contactless installments, by just approaching a cell phone to specific device [12].

3G is the acronym utilized for the third era of cell phones. The innovation used to exchange voice and permits downloading applications, emails and short messages.

Continuous rapid development of current day use technology will push us to the edge, where integration is the most critical player beside minimizing the size and power consumption. A Nano size implantable device integrating positioning, identification, communication equipped, with a renewable source of energy is the most demandable product in the market.

IV. CHALLENGES AND ETHICAL ISSUES

In this section, we present the challenges, ethical and legal issues related to the use of IoT in sections A, B and C respectively.

*A. **Challenges***

There are several challenges associated with the use of IoT shown in Fig. 2. Amongst these challenges are the following ones.

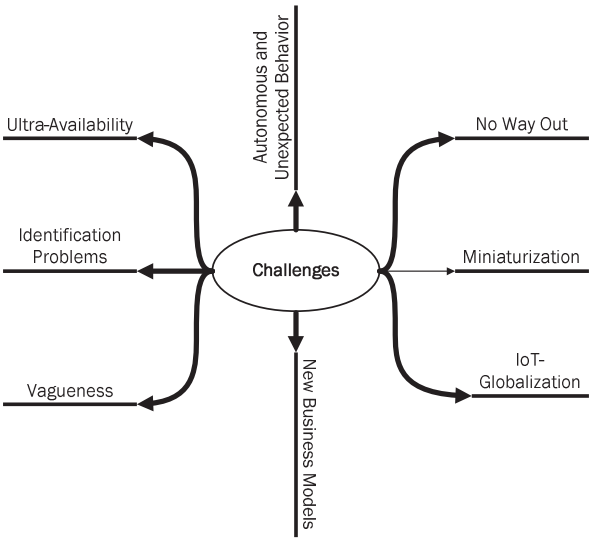

Fig. 2. IoT Challenges

• ***No Way Out***

The client is totally immersed in the IoT network. There is a high dependability from the user on the IoT network specially in healthcare applications.

• ***Miniaturization***

Nowadays, PC's are diminishing in size, and new IoT devices will be in the Nano size and transparent. Thus, it will be difficult to maintain any sort of audit, quality control or traffic control, due to the Nano size and huge number of devices.

•***IoT Globalization***

IoT cannot be localized, especially in medical applications where the service can be offered overseas. It is a challenge for nations to deal with this new concept, because may be almost every whisper in a country is collected and sent to the country that is providing the service.

•***New Business Models***

Using IoT will enforce companies that offer medical services to create new business models that take into consideration the available types of data and the high stream. Virtual hospitals will take place. Therefore, the service will be offered remotely.

• ***Vagueness***

The differentiation between physical and virtual devices and human being will be more difficult due to the ease of transformation from one category to another.

• ***Identification Problems***

There are billions of IoT devices, each needs a unique identification in order to log in the network. Identification problems will rise up with other identity proof problems.

• ***Ultra-Availability***

Billions of devices will be always on 24/7. This will result in massive amount of data (big data), which will be more exposed to malicious attacks.

• ***Autonomous and Unexpected Behavior***

Human beings will be part of IoT networks together with other devices and sensors, a hybrid network will be the result. Interconnected devices may interfere suddenly in human actions. The continuous development of IoT will lead to ambiguous behaviors not completely understandable by the users.

• ***Governance***

Due to the considerable number of routers, switches and information, IoT control and governance will be challenging. The data exchanges will be faster and less expensive, difficult to be controlled or monitored. The accountability is an additional challenge to tackle.

B. ***Ethical Issues***

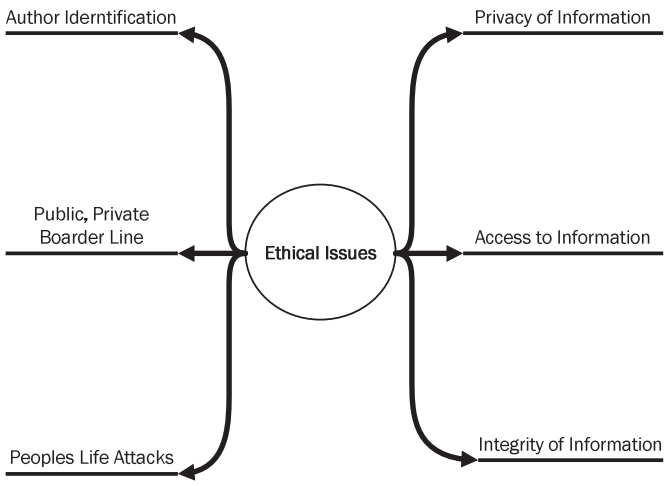

Fig. 3 Ethical Issues in IoT

Morals and ethics refer to social behavior standards in the IoT field. Most of the ethical debates are about, property rights, accessibility, private use of information shown in Fig. 3 According to [1], an ethical behavior requires enforcing the following:

• *Privacy* of information.

o *Access* to information.

o *Integrity* of the information.

It follows that ethical issues in IoT field have appeared, such as:

•***Author Identification***

The correct identification of the author of the data collected in typical IoT system will be hard to determine. There is also a concern about using the data without the patient's permission.

•***Public and Private Boarder Line***

IoT omnipresence will make the boarder lines between private and public life virtually transparent, in the absence of defined boundaries for users' information.

•***Peoples Life Attacks***

Hackers or virus attacks in typical computer systems may cause either data loss or physical loss of the computer system. In the IoT attacks the loss will not stop at this point, it will exceed to the point that will affect directly the people lives. For example, if an attacker can log in to a typical IoT medical application, a small change in a patient's information may result

in wrong medication, which will affect the patient's life.

C. *Legal Issues*

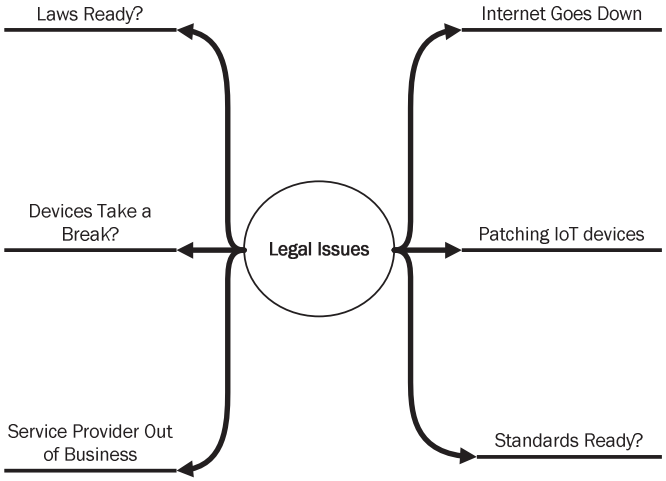

Fig. 4 Legal Issues in IoT

After having defined the challenges and ethical issues, a new legal question about the ability of the existence of laws ready to protect users in such an environment arises.. This is a major concern because the border between physical and virtual is almost transparent in IoT. The following questions are examples for issues needed to be discussed.

1- What will happen when internet goes down in medical applications, who is responsible, who will be sanctioned? Is it the medical service provider or the local or global internet service provider?
2- Who is responsible for patching new IoT devices to be sure its fully secured?
3- Are the standards and laws ready to deal with these situations?
4- What happens if a medical service provider is out of business? What is the fate of the patients, how the data will be used?
5- When these devices should take a break from collecting data?

According to the above mentioned challenges and ethical issues related to IoT generally and medical application specifically, IoT presents a threat from different perspectives, including privacy, property rights, life risk, in case of incorrect management is applied.

Effective technical solutions must be applied to encourage the users to enroll themselves inside the IoT network. Such solutions may be advanced encryption techniques, electronic signatures, legislations to limit the use of the collected data by third parties, and other. Fig. 5 summarizes the future challenges related to the IoT technology into three main items, ethical, legal, and technical, highlighting required action in order to minimize the risk.

New laws and standards should combine different existing laws like HIPPA, FIPPS, Electronic Communication Privacy Act and others should be considered to maintain complete security and privacy and cover all legal issues.

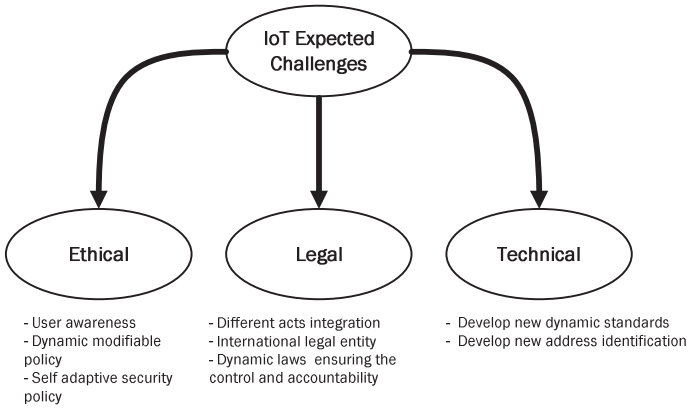

Fig. 5 IoT Issues proposed solutions

V. Conclusions and Future Work

The IoT is evolving rapidly. It connects people and devices and will cause dramatic shifts in different sectors. For instance, the health sector is one of the major areas that have improved but face a lot of challenges, In this paper, we explored some of the work done in the literature related to the privacy and security of IoT. We presented the different challenges, ethical and legal issues related to the IoT, as well as our vision for the main issues that need to be tackled promptly. In the future, we plan to work on developing customized standards for the health sector.

Further technical research must be applied in order to protect IoT from being the "All See Eye".

References

[1] Carron, X., Bosuo, R., Maynard, S. B., & Ahmad, A. (2016). The Internet of Things and Its Impact on Individual Privacy: An Australian Privacy Principle Perspective. Computer Law & Security Review, 21(1), 4-15.
[2] Baldini, G., Bottermon, M., Neisse, R., & Tallacchini, M. (2016). Ethical Design in the Internet of Things. Science and engineering ethics, 1-21.
[3] Weber, R.H., 2010. Internet of Things–New security and privacy challenges.Computer Law & Security Review, 26(1), pp.23-30.
[4] Tarouco, L.M.R., Bertholdo, L.M., Granville, L.Z., Arbiza, L.M.R., Carbone, F., Marotta, M. and de Santonna, J.J.C., 2012, June. Internet of Things in healthcare: Interoperatibility and security issues. In 2012 IEEE International Conference on Communications (ICC) (pp. 6121-6125). IEEE.

[5] Popescul, D., & Georgescu, M. (2013). Internet of Things–some ethical issues. The USV Annals of Economics and Public Administration, 13(2), 18.
[6] French, A. M., & Shim , J. P. (2016). The Digital Revolution: Internet of Things, 5G, and Beyond. Communications of the Association for Information Systems, 38(1), 40.
[7] Van den Hoven, J. (2013), Internet of Things Factsheet Ethics, http://ec.europa.eu/digitalagenda/en/news/conclusions-internet-things-public-consultation, 28.02.2013, accessed at 2.09.2013.
[8] Karimi, K. (2013), Why harp on Internet of Things security ,privacy issues?,The Embedded Beat, https://community.freescale.com/community/the-embedded beat/blog/2013/09/13/why-harp-on-internet-ofthings-security-and-privacy-issues, 13.09.2013, accessed at 14.09.2013.
[9] Sarma, S., Brock, D. L., Ashton, K. (2000), The Networked Physical World. Proposals for Engineering the Next Generation of Computing, Commerce & Automatic-Identification, White Paper of the Auto-ID Center at the MIT, Cambridge, MA.
[10] Frederix, Ines. "Internet of things and radio frequency identification in care taking, facts and privacy challenges." Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on. IEEE, 2009.
[11] Misra, P. and Enge, P., 2006. Global Positioning System: Signals, Measurements and Performance Second Edition. Massachusetts: Ganga-Jamuna Press.
[12] Want, R. (2011). Near field communication. IEEE Pervasive Computing, 10(3), 4-7.