12-2012

# Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey

Wassnaa AL-mawee

# PRIVACY AND SECURITY ISSUES IN IOT HEALTHCARE APPLICATIONS FOR THE DISABLED USERS. A SURVEY

by

Wassnaa AL-mawee

A Thesis submitted to the Graduate College
in partial fulfillment of the requirements
for the degree of Master of Computer Science,
Computer Science
Western Michigan University
December 2015

Thesis Committee:

Leszek Lilien, Ph.D., Chair
Ala Al-Fuqaha, Ph.D.
Ikhlas Abdel-Qader, Ph.D.

# PRIVACY AND SECURITY ISSUES IN IOT HEALTHCARE APPLICATIONS FOR THE DISABLED USERS. A SURVEY

Wassnaa AL-mawee, M.S.

Western Michigan University, 2015

Aging of the population resulted in new challenges for the society and healthcare systems. Ambient Assisted Living (AAL) that depends on Internet of Things (IoT) provides assistance to the disabled people and supports their vital daily life activities. Affordability of and accessibility to AAL and the usage of IoT starts revolutionizing healthcare services. This Thesis is a survey of the privacy and security issues in IoT healthcare applications for the disabled users. Introduction includes definitions of privacy and security terms, and discusses their relationship. Then, it presents an overview of the IoT, including its architecture and components. Next, the Thesis shows IoT-based solutions for healthcare for the disabled, which is preceded by a discussion of the types of disabilities. A range of IoT applications for the disabled users is identified, and their classification is proposed. Then, privacy and security issues in these IoT applications are discussed, along with IoT-based solutions known in the literature. Finally, the Thesis identifies privacy and security requirements for IoT applications for the disabled users.

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

# 1. INTRODUCTION

## 1.1. Definition of IoT and Its Role in the Healthcare Industry

As defined by Casagras [1], the Internet of Things is "*a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and involving Internet and network developments. It will offer specific object- identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.*"

Nowadays, Internet of Things (IoT) links the Internet with sensors and a multitude of devices, mostly using IP-based communications. In healthcare industry, IoT provides options to remote monitoring, early prevention, and medical treatment for institutionalized disabled. For IoT, people or objects can be equipped with sensors, actuators, Radio-Frequency Identification (RFID) tags, etc. Such devices and tags facilitate access by patients' caregivers. For example, RFIDs tags of patients or patients' personal devices (including medical devices) are readable, recognizable, locatable, and controllable via IoT applications [2].

IoT enables a wide range of smart applications and services to cope with challenges that individuals or healthcare sector faces [3]. For example, IoT has dynamic capabilities to connect D2M (Device-to-Machine), O2O (Object-to-Object), P2D (Patient-to-Doctor), P2M (Patient-to-Machine), D2M (Doctor-to-Machine), S2M (Sensor-to-Mobile), M2H (Mobile-to-Human), T2R (Tag-to-Reader). This intelligently connects humans, machines, smart devices, and dynamic systems in order to assure an effective healthcare system [16, 4].

Due to the increasing life expectancy, the group of people over the age of 60 is increasing faster than any other age group [5]. This can be considered a success of public health policies, health services and socioeconomic development. However, it also presents a challenge to the society, which must cope with many more disabled people. –According to the World Health Organization (WHO), the world's population of people over the age of 65 will reach 2 billion by 2050 [6]. To avoid overwhelming health services, there is a real need to prolong independent living of the disabled people (including the disabled elderly) at their own homes. This not only improves their quality of life, but also reduces costs for their families and the society at large.

Demographic changes require developing new functionalities and the integrating new technologies into home environments. Home automation technologies with the goal of improving quality of life for the disabled started to emerge decades ago. They began with simple features related to the automation of basic tasks, such as lighting control using motion detectors. In natural way of technological progress, smarter and smarter systems of a higher and higher complexity have and are being introduced. The integration of smart functionalities and Ambient Intelligence (AmI) at home results in Ambient Assisted Living (AAL) environments that support care and provide assistance to the disabled [7, 8]. Essentially, the same systems with some minor adjustment can also target a different population segment.

## 1.2. Thesis Contributions and Organization

The main contributions of this Thesis are: (i) identifying and classifying the range of IoT applications for the disabled; (ii) identifying the privacy and security *issues* for these IoT applications; (iii) presenting known privacy and security *solutions* for these IoT applications; and (iv) identifying privacy and security *requirements* for the IoT applications for the disabled.

Additionally, Section 1 presents relationship of privacy and security; Section 2 covers IoT architecture and its components; Section 3 discusses types of disabilities that the disabled face in their daily life activities; Section 4 presents privacy and security issues in IoT applications for the disabled users; Section 5 identifies privacy and security requirements for those applications and Section 6 concludes the Thesis.

## 1.3. Definitions of Privacy and Security

**Definition of Privacy.** Ensuring privacy requires making sure that individuals maintain the right to control what information is collected about them, who maintains it, who uses it, how it is used, and what purpose it is used for.

Figure 1 shows the main privacy services[1] and properties as defined by [53]:

1) *Untraceability*: Making it difficult for an adversary to identify that the same subject performed a given set of actions.

[1] We use the name "privacy services" as an analogy to security services defined by ISO [52].

2) *Unlinkability*: Hiding information about the relationship between any items, such as subjects, messages, actions, etc.
3) *Unobservability*: Hiding the fact that a message was sent (as opposed to hiding the identity of the sender of message).
4) *Anonymity*: Hiding information who performed a given action or who is described by a given dataset.
5) *Pseudonymity*: Using pseudonyms instead of using real identifiers.

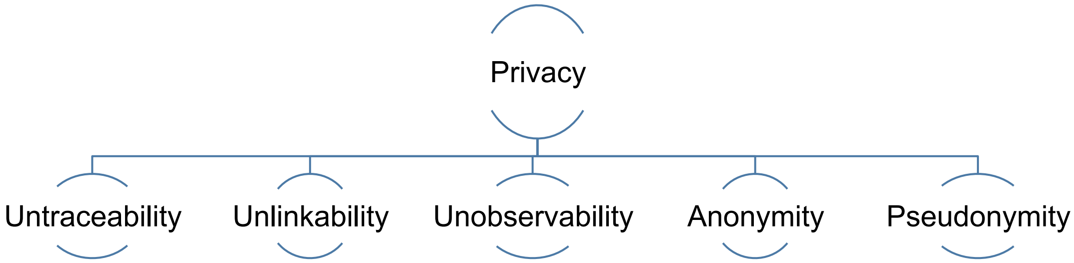

Figure 1. Privacy Services.

**Definition of Security**. Providing security requires preventing access to information or other objects by unauthorized users, as well as protecting against unauthorized alterations or destruction of users' information. The classic definition of security equals it with confidentiality, integrity, and availability, called (by its acronym) the *CIA triad*.

The ISO 7498-24 standard extends the security definition, as shown in Figure 2, to the following requirements that can use the abbreviation *CIA-AANN* (cf. [52]):

1) *Confidentiality*: Information is not made available or disclosed to unauthorized individuals, entities, or processes.
2) *Integrity*: Data has not been altered or destroyed in an unauthorized manner.
3) *Availability*: A system is operational and functional at a given moment (it is not down).
4) *Access control*: Users access only those resources and services that they are entitled to access, and qualified users are not denied access to services that they legitimately expect to receive.
5) *Authentication*: The corroboration that an entity is the one claimed, and the source of received data is as claimed.

6) *Nonrepudiation*: The senders/receivers of messages cannot deny that they in fact sent/received the messages.

7) *Notarization*: The registration of data with a trusted third party that assures the accuracy of data characteristics such as content, origin, and creation time.

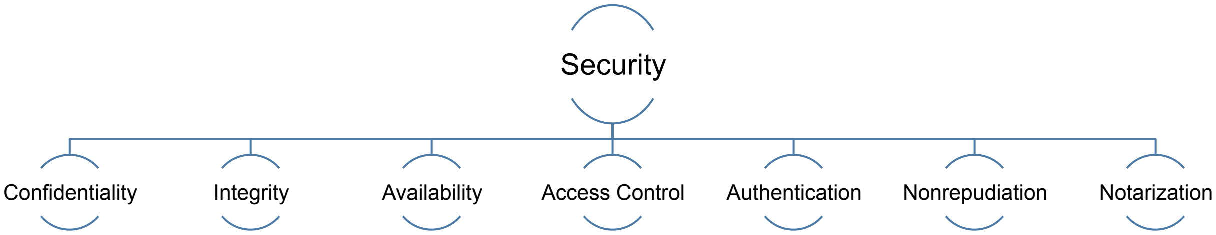

Figure 2. Security Services.

### 1.4. Mutual Relationship between Privacy and Security

Privacy and security are distinct. However, in healthcare field, the relationship between those two concepts is data protection.

We show the mutual relationship between security and privacy in Figure 3; that is, confidentiality is located in the intersection of privacy and security.

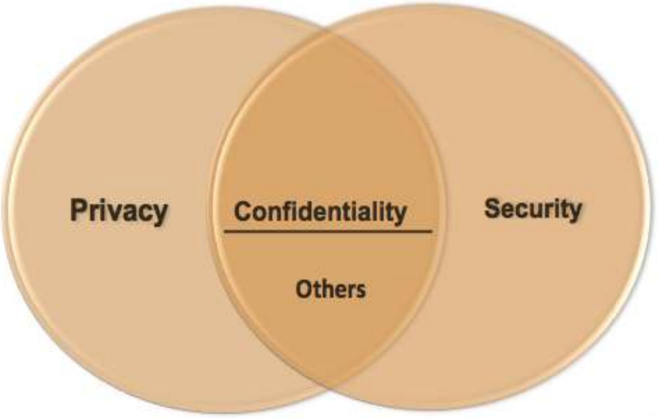

Figure 3. Mutual Relationship between Privacy and Security.

## 2. Overview of Internet of Things (IoT)

### 2.1. IoT Architecture

The architecture of IoT consists of several layers, starting from the edge technology layer at the bottom to the application layer at the top, as shown in Figure 4 [17, 18]. The two lower layers contribute to data capturing, while the two higher layers are responsible for data utilization in applications.

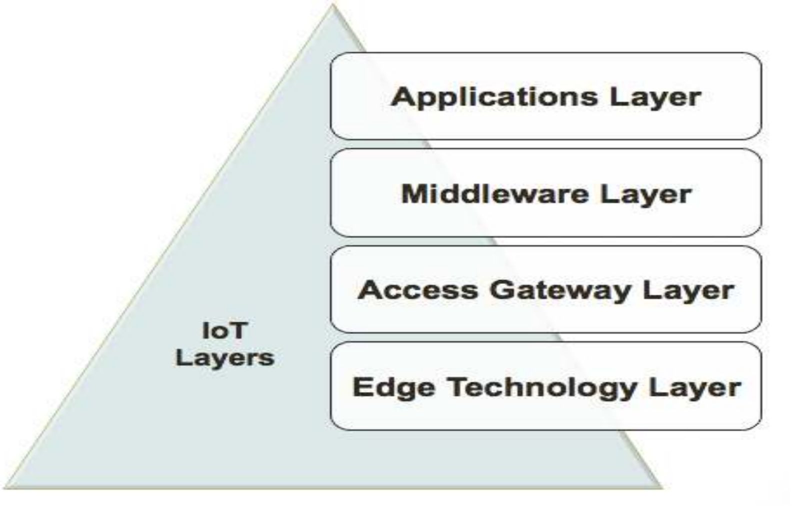

Figure 4. Layered Architecture of IoT [17].

The functions of the layers (from the bottom up) are as follows:

1) *Edge technology layer (a.k.a. perception layer):* This is a hardware layer which includes data collection components—such as wireless sensors networks (WSNs), RFID systems, cameras, intelligent terminals, electronic data interfaces (EDIs), global positioning systems (GPS). These hardware components provide identification and information storage (e.g., via RFID tags), information collection (e.g., via sensor networks), information processing (e.g., via embedded edge processors), communications, control and actuation (e.g., via robots).

   This Thesis focuses on RFID systems and WSNs since they are currently the most common IoT technologies [42].

   a) *RFID systems*: They are the most important components of IoT. They enable data transmission by a highly portable device called an *RFID tag*. An *RFID reader* reads the tag and processes the obtained data according to the needs of a specific application. RFID systems can be used to monitor healthcare objects in real-time, without the need of being in the line of sight. Data transmitted by the tag may provide disabled or device identification, disabled information (age, sex, blood pressure, glucose level, etc.), or location information [15].

   b) *Wireless sensor networks (WSNs):* A WSN may consist of a large numbers of sensing nodes, which report the sensing results to special nodes called *sinks* [18].

2) *Access gateway layer (a.k.a. network layer or transport layer):* This layer is responsible for data handling, including data transmission, message routing, and publishing and subscribing messages. It sends to the middleware layer information received from the edge layer, using communications technologies such as Wi-Fi, Li-Fi, Ethernet, GSM, WSN, and WiMax [17, 18].

3) *Middleware layer*: It is a software platform that provides abstraction to applications from things. Also, it offers many services such as device discovery and management, data filtering, data aggregation, semantic data analysis, access control, and information discovery (using Electronic Product Code (EPC), or Object Naming Service (ONS)).

4) *Applications layer*: This top layer. It is responsible for delivery of various applications to different IoT users. It consists of two sub-layers [73]:

   a) *Data management sub-layer:* It provides directory service, Quality of Service (QoS), cloud-computing technologies, data processing, machine-to-machine (M2M) services, etc.

   b) *Application service sub-layer:* It is responsible for interfacing to end users and enterprise applications running on top of the IoT applications layer.

**Table 1.** IoT Layers and Components.

| IoT Layers | IoT Components | Tasks | Used Technologies |
|---|---|---|---|
| Application Layer | Applications | Provide the disabled with care and assistance, and enable the disabled to read/view their health information | Smart home technology, robotics, Cloud computing, fog computing |
| Middleware Layer | Device Discovery, Access Control, Data Management | Enables communication between applications and things | CoAP, MQTT, REST, OMA Lightweight, OMA DM, EPC, ONS |
| Access Gateway Layer | Communication Technologies | Wireless WAN: Transmit information over Internet from devices or gateway | Wireless WAN: 2G, 3G,Long Term Evaluation (LTE), Long Term Evaluation- Advanced (LTE-A), 4G, Satellite networks, etc. |
|  |  | Wireless PAN/LAN: Enables devices to share or exchange information themselves | Wireless PAN/LAN: RFID, Bluetooth, Wi-Fi, Li-Fi, ZigBee, 6LoWPAN |
| Edge Technology Layer | Physical Objects | Collect, monitor, identify, and provide data about disabled users in their environments | RFID, sensors, actuators |

## 2.2. IoT Components

IoT involves different components that work together to realize the IoT concept. The major IoT components, described in Table 1, are discussed next.

### *2.2.1. The Physical Objects IoT Component*

*Physical objects (a.k.a physical devices)*: They collect, identify, and monitor information about disabled users in their environments. This includes devices monitoring disabled's vital signs (blood pressure, heart rate, glucose, daily life). The physical devices are connected to the Internet, and transform disabled-related information obtained in the physical world into data for the digital world.

### *2.2.2. The Communication Technologies IoT Component*

The most common types of networks for IoT healthcare applications for the disabled are Personal Area Networks (PANs), Local Area Networks (LANs), and Wide Area Networks (WANs) [45]. Each network type involves a number of wireless technologies, as shown in the row Access Gateway Layer of Table 1.

**Table 2.** Features of Selected of Wireless PAN/LAN/WAN Communications Technologies.

| Features | ZigBee | Bluetooth | Li-Fi | Wi-Fi | LTE/ LTE-A |
|---|---|---|---|---|---|
| **Standard** | IEEE 802.15.4 | IEEE 802.15.1 | IEEE 802.15.7 | IEEE 802.11 | LTE: 3GPP Rel. 9<br>LTE-A: 3GPP Rel. 10 |
| **Operating Frequency** | 2.4 GHz | 2.4 GHz | *N** 100 THz | 2.4 and 5 GHz | Depend on different # of bands[2] |
| **Range** | 10-300 m | 200 m BLE<br>100 m (class 1)<br>10 m (class 2)<br>1 m (class 3) | Direct line of sight or reflected light | 10-100 m<br>(cf. Footnote [3]) | Depend on different # of bands |
| **Power Consumption** | Low | Low | Low | High | High |
| **Cost Rank** | 1 (lowest) | 2 | 3 | 4 | 5 (Highest) |
| **Data Rate** | 20,40,and 250 Kbs | 1Mbs | >1Gbps | 11 and 54 Mbs | LTE: 300 Mbs (DL)<br>75 Mbs (UL)<br>LTE-A: 3 Gbs (DL)<br>1.5 Gbs(UL) |
| **Network Topology** | Ad hoc, mesh, peer-to-peer, or star | Ad hoc piconents | Point-to-multi point | Point-to-point | Cellular network |
| **Healthcare Applications** | Remote sensing and control: disease monitoring, personal wellness monitoring, home monitoring, personal fitness monitoring | Machine to machine (M2M): provide wireless connection between devices | Control medical equipment, automate procedures, and robotic surgeries | Networking, and Internet access | M2M services; monitoring, and tracking patients and devices |
| **Provided Security** | 128 AES encryption | 64/128 AES encryption, | 1s and 0s encryption, availability, light does not penetrate through walls | WEP, WPA, WPA2 encryption, access control, authentication, and confidentiality | Authentication, 128 AES encryption |
| **Security Issues** | Exploiting the key exchange process, and battery lifetime | Denial of service, secure pairing, scalability, power consumption, and turning on/off the discovery mode | Reliability and network coverage; data in light "stream" | Eavesdropping and malicious attackers | Man-in-the middle attack, user identity threats, and sequence number synchronization |

[2] Bands 1(2100 MHz), 2(1900 MHz), 3 (1800 MHz), etc. [185].

[3] An inexpensive Wi-Fi repeater can have a range of 10 km [182], a long-range Wi-Fi can cover up to 382 km [183].

The following communication technologies are most frequently used in the IoT healthcare applications [74] (in the order of cost rank):

a) *ZigBee:* It is the IEEE 802.15.4 standard for low power and short range, based on Low-Rate Wireless Personal Area Network (LR-WPAN). It is less expensive than Bluetooth, and operates in the 2.4 GHz ISM (The Industrial, Scientific, and Medical radio) band [76].

b) *Bluetooth:* It is the IEEE 802.15.1 standard for low-power short distance radio frequency that can facilitate point-to-point and point-multipoint configurations, based on Wireless Personal Area Network (WPAN), which operates in the 2.4 GHz ISM band [75]. Bluetooth devices are cheap, and Bluetooth Low Energy (BTLE, BLE, OR LE) (also called Bluetooth Smart or Version 4.0+) technology significantly reduces power consumption (operating for "months or years" on a button cell), and is aimed—among others—at novel healthcare applications [11].

c) *Light Fidelity (Li-Fi):* It is optical, Visible Light Communication (VLC) system using light instead of radio waves in a manner similar to Wi-Fi [178] (it uses the TCP/IP protocol). VLC uses rapid pulses of visible light between 400 THz (780nm) and 800 THz (375 nm) for data transmission. Li-Fi uses transceiver-fitted LED lamps (which provide room lighting) for transmitting and receiving information. Data (1 for on and 0 for off) are transmitted by the LED and received by photoreceptors, where the received signal is converted to the digital data [179].

   Li-Fi has security issues such as reliability and network coverage. In reliability, the path of transmission will cause disruption in the communication due to the interface from external light sources such as sunlight or normal bulbs. While, in network coverage, Li-Fi cannot provide data in an area where are trees, walls or obstacles.

   Li-Fi has many advantages such as low cost and no room for eavesdropping since the signal does not travel through walls. Also, Li-Fi avoids the problem of overlapping frequencies known when using Wi-Fi for medical devices since there is no electromagnetic interference in VLC. Therefore, for example, Li-Fi can be used in a room to monitor patients while simultaneously radio waves are used for an MRI scanner [180].

d) *Wi-Fi:* There are many Wi-Fi versions, such as IEEE 802.11x (Wireless LAN or WLAN). Wi-Fi operates on three different non-interoperable technologies, which are Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum (FHSS), and Infrared (IR). It can provide both point-to-point and point-multipoint configurations [77].

IEEE 802.11n provides a good performance with the maximum data rate 600 Mbps, and uses 2.4 GHz or 5 GHz RF bands. It can use Multiple Input Multiple Output (MIMO) in order to maximize the use of the available bandwidth.

Older Wi-Fi versions (802.11a,b, and g) are also used in the healthcare field.

WiFi security can be provided by the following protocols [46]:

- *Wired Equivalent Privacy (WEP)* is the first security protocol used for Wi-Fi. It is easy to break.
- *Wi-Fi Protected Access (WPA)* is a much stronger security protocol for Wi-Fi.
- *Wi-Fi Protected Access II (WPA2)* is the improvement of WPA, which includes the strong Advanced Encryption Standard (AES).

e) *Long Term Evolution (LTE*): It is a 4G wireless broadband standard developed by the Third Generation Partnership Project (3GPP), based on WWAN. LTE provides UpLink data rate up to 75 Mbps (UL), and DownLink (DL) up to 300 Mbps. LTE offers cost effective solution for M2M services [156, 184] for IoT for healthcare applications, including monitoring, and tracking patients and devices.

f) *Long Term Evolution-Advanced (LTE-A):* It is a “true” 4G mobile communication standard, which is a significant enhancement of the LTE; it provides up to three times higher data rates 3 Gbs (DL) 1.5 Gbs (UL) [185], and lower latency [159]. LTE-A should be backward compatible with LTE equipment [186], so upgraded M2M services can take advantage of existing LTE networks [184].

### *2.2.3. The Applications IoT Component*

The applications IoT component is responsible for data formatting and arranging data flow for specific applications [20]. It provides users with care and assistance through smart technologies like smart home technology. Smart health systems introducing new interconnections between the natural habitat of the disabled, their bodies, and the Internet at the purpose to produce and manage participatory medical knowledge. By replacing wireless sensors inside the home, on clothes and personal items, it becomes possible to monitor, in a way that preserves the privacy, the macroscopic behavior of the person as well as to compile statistics, to identify precursors of dangerous behavioral abnormalities, and finally to activate alarms or prompt for remote actions by appropriate assistance procedures.

Also, it enables users to read/ view their health information through smart applications, such as ECG monitoring applications, diabetes therapy management applications, etc.

Information processing is handled in applications layer. The information processing technologies for IoT healthcare applications include cloud and fog computing. Healthcare applications that depend on utilizing input from the physical world (e.g., via RFID or sensor networks, create a huge amount of data. These data can be sent to a cloud integrated with an IoT system for convenient and efficient storage, processing, and management [130]. For example, Cubo *et al.* [131] proposes three-component system for AAL applications, which consist of a sensor gateway at the sensor network level, network communication at the level of Internet-connected devices and applications, and a cloud platform at the topmost level for collecting data from the communication network (using a REST-based[4] API). The cloud-based approach enhances healthcare solutions by improving accessibility and quality of healthcare, and reducing costs [139].

Cloud computing can deliver three types of services [153, 154]:

a) *Infrastructure as a Service (IaaS)*: Infrastructure includes hardware and software, such as storage devices, networks, data, applications, and operating systems. Users can request for a certain infrastructure configuration, and then the cloud takes the administration and management duties off their shoulders.

b) *Platform as a Service (PaaS)*: The cloud can provide a set of services and tools that facilitate convenient creating and efficient running of users' applications. Users can fully control their applications in the cloud but they are limited by not being able to use the operating system[5], hardware, and network infrastructure of the cloud.

c) *Software as a Service (SaaS)*: SaaS provides applications available to the users over the web.

Fog computing extends cloud computing. It is a distributed computing infrastructure that provides the same application services to end-users as cloud computing such as data processing, storage, and execution of applications. However, the application services are handled at the network edge in a smart device instead of a remote data center in the cloud. The goal of fog computing is to improve the efficiency and reduce the amount of transported data to the cloud [181].

[4] REST stands for Representational State Transfer, which is the software architectural style of WWW [187].

[5] Users may run a virtual machine manager and control an OS run under the VMM's control.

## 3. IoT Solutions for Healthcare for the Disabled

Due to population growth and aging, expenditures for healthcare services are rapidly growing, limiting access to them by some disabled. The lack of specialized medical and caretaker professionals and facilities for the disables is especially acute in rural areas [3]. This forces the disabled to look for healthcare services in large hospitals or other high-cost healthcare institutes. IoT is an opportunity to extend proper healthcare services to the disabled conveniently and at a reduced cost.

### 3.1. Types of Disabilities

The disabled must perform many daily-life tasks to maintain their independence and health, including self-maintenance, instrumental, and enhanced activities of daily living. Self-maintenance *activities of daily living* (ADLs) include the ability to bathe, eat, dress and groom oneself [57]. *Instrumental activities of daily living* (IADLs) include using home devices such as computers, telephones, TVs, dishwashers, etc. *Enhanced activities of daily living* (EADLs) include social participation to learn new skills, to engage in or practice hobbies EADLs can be challenging or unsatisfying due to physical or technological disabilities [56, 58].

Our first classification of the disabled classifies them as follows, by the type of their disability or disabilities:

1) *Physical disabilities*: They are the most common ones among the elderly. According to Kaplan, most —if not all—elders cannot maintain physical activities such as strength, endurance or balance [9]. For instance, people 80 years or older have on average over three physical disabilities more than people 50-59 years old as shown in Figure 5.

2) *Intellectual disabilities*:

    a) *Perceptual disabilities:* These disabilities are often a result of physical disabilities; for example, hearing and vision loss result in perceptual challenges that most of elders experience [10].

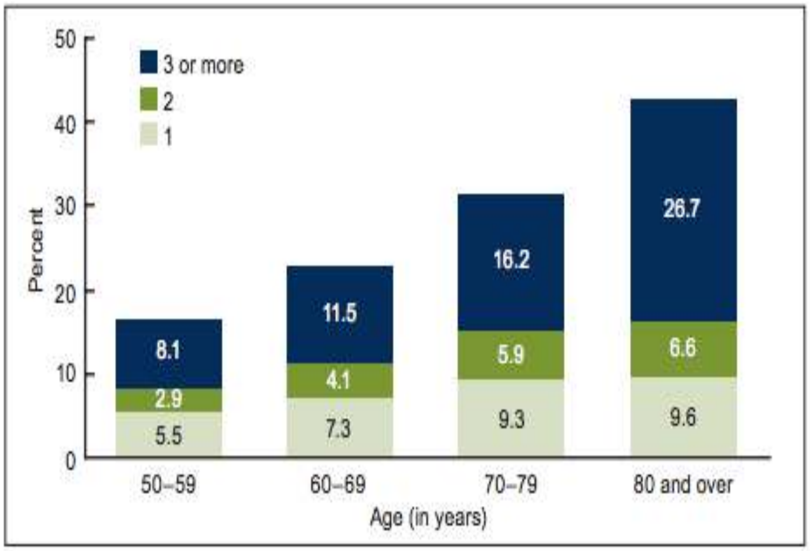

Figure 5. Percentage of adults over 50 years old, by age and the number of physical[6] disabilities [79].

b) *Cognitive disabilities:* These disabilities are mental malfunctions such as lack of or poor performance in the person receives, stores and uses the perceived information. Cognitive decline is one of the most difficult health problems in terms of both its relation to the overall functioning of the disabled and the cost of care [59].

Our second classification of the disabled classifies them depending on their capability for independent functioning:

1) *The independently-living disabled:* They can be further divided into mobile and immobile disabled individuals. Mobile disabled are people who can move, walk and travel independently. Immobile disabled are people who cannot walk or move on their on. The mobile disabled practicing sport activities can be tracked by GPS, monitored by a variety of smartphone sensors (accelerometer, video camera, proximity sensors, etc.), and connected by cellphone systems, Wi-Fi, Bluetooth, etc.
2) *Homebound disabled:* Those are people, who are restricted to staying at home, and require a special assistance to venture out. Deploying sensor systems in home environments and wearable sensors are among ways to assist the disabled and to make their lives easier. In this case, note that the goal is to make such solutions transparent to the user, which can be achieved by integrating them into common home objects, following the principles of

[6] The sum of the stacked sections in the bar for each group represents the total percentage of adults in the age group with 1-3 physical disabilities [79].

pervasive computing. IoT will be offered in smart homes, e.g., in the form of eHealth monitoring systems linked to healthcare providers [80]

3) *The institutionalized disabled:* These are people living in nursing homes or long-term care facilities because they require specialized care that cannot be provided even if they were homebound.

## 3.2. Range of IoT Applications for the Disabled Users

IoT plays a significant role in a broad range of IoT applications for the disabled users, from preventing diseases and disabilities at one end of the spectrum to managing chronic diseases and disabilities at the other. Here are some examples of how potential of IoT is already realized [13]:

1) *Remote monitoring:* A disabled person living alone (homebound or not) may prevent further diseases or disabilities by using a monitoring device that can detect—among others—a fall or problems with her vital signs (e.g., by using ECG in the latter case). Any person, in particular a disabled person or her caregiver, can keep track of their her condition continuously [81, 148]. Even healthy and active people can benefit in their daily activities from the IoT healthcare monitoring applications. Remote monitoring has another aspect in the countryside or developing nations, due to a restricted access to effective health monitoring [41]. Inexpensive remote monitoring solutions can capture a disabled's health data from a variety of sensors, apply complex algorithms to analyze the data, and then, when needed, alert a medical professionals [60].

2) *Early prevention*: Appropriate monitoring enables an early prevention, which is essential in avoiding future diseases or disabilities. For example, patients suffering from diabetes diseases who are being treated with digitalis could be monitored around the clock to prevent drug intoxication [12].

3) *Medical treatment of the institutionalized disabled:* The disabled living in nursing homes or long-term care facilities, or staying in hospitals benefit from continuous monitoring of their state and vital signs by IoT healthcare monitoring applications. Typically, solutions of this type employ sensors to collect physiological information, and can use the cloud to analyze and store a patient's data, and then send the analyzed data to appropriate caregivers for their further analysis and review. Such a continuous automated flow of information assures uninterrupted monitoring, improves the quality of care, and reduces the costs.

## 3.3. A Classification of IoT Applications for the Disabled Users

The increase in life expectancy and the consequent aging of the population, with increased frequency of chronic diseases, triggered a careful rethinking of the ways and means of providing care to the disabled people, including a disproportionate share of the elderly.

Extending independent life of the disabled people, including their stay in their own homes, contributes to their higher quality of life. It delays the need for traumatic changes of habits and their domestic environment [93]. The emerging model of IoT and using IoT for healthcare for the disabled promises a much more patient-friendly and highly personalized care.

### *3.3.1. An Overview of Ambient Assisted Living (AAL)*

AAL aims to extend the period of independent life for a disabled person, while giving her confidence that she will not be left alone if any health-related problem occurs. She can be assisted in her normal daily activities with IoT-based AAL solutions [14, 24, 47].

The AAL model consists of ubiquitous sensing and computing, ubiquitous communication, and intelligent user interfaces [60]. Ubiquitous sensing and computing integrates embedded systems with the common everyday objects. For example, a disabled's sensors can be implanted within her body (like a heart beat stimulator), attached to her body, or embedded in the furniture and other objects within home. All sensors can be networked, cooperating in capturing and sharing data obtained from sensors, analyzing these data, sending them to the cloud, as well as the caretaker or a medical professional.

Sets of biometric data (such as continuous ECG monitoring data) are accessible to healthcare professionals so that they can evaluate a disabled person's health status, and provide a remote diagnosis.

Many AAL solutions have been proposed in the literature. The disabled can be monitored by using an ECG monitoring and alarming system based on the Android smartphone [81]. There are wearable ECG signal monitoring solutions that rely on wireless body area networks (WBANs), low-power wireless sensors, and ZigBee communication technology [148]. Many applications for smart houses assist the disabled in leading an independent life [82]. The Home Automation System (HAS) [83] provides a remote access from a PC/laptop or a smartphone to a AAL system in the house. Another proposed IoT-based system provides diabetes therapy management in the AAL environment [12].

### *3.3.2. Categories of IoT Applications for the Disabled Users*

We show a classification of IoT applications for the disabled users in Figure 6, and describe the categories of these classifications in Table 3.

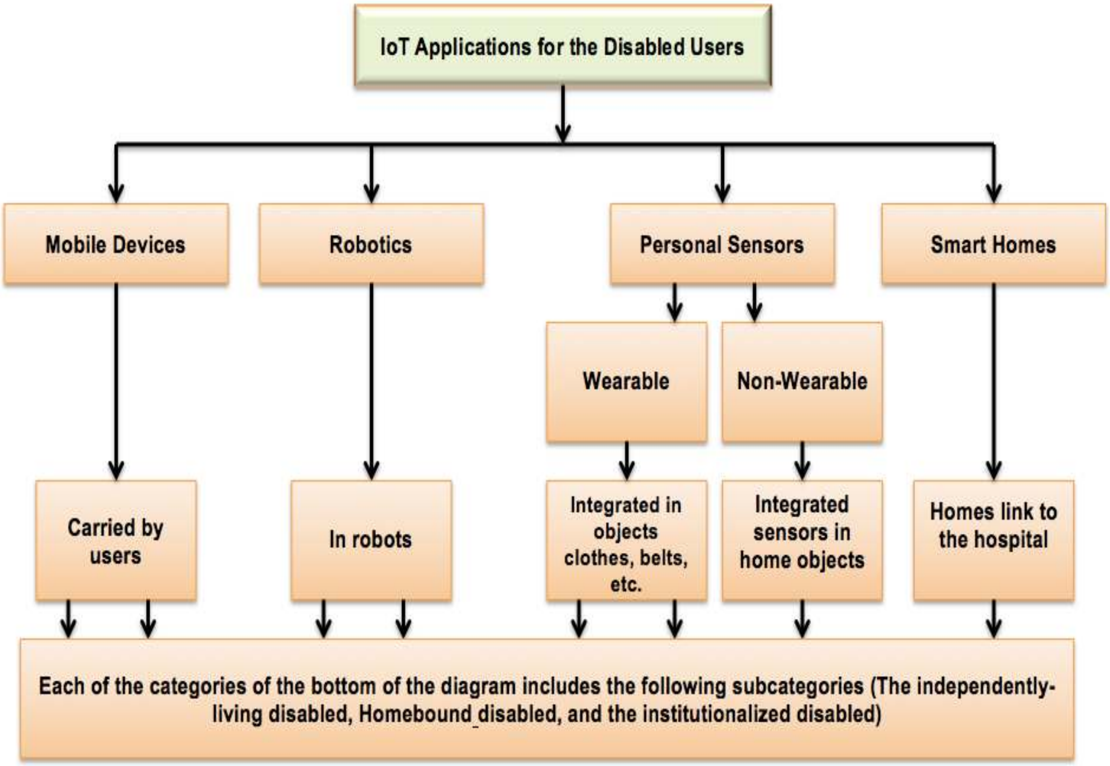
IoT Applications for the Disabled Users
Mobile Devices
Robotics
Personal Sensors
Smart Homes
Wearable
Non-Wearable
Carried by users
In robots
Integrated in objects clothes, belts, etc.
Integrated sensors in home objects
Homes link to the hospital
Each of the categories of the bottom of the diagram includes the following subcategories (The independently-living disabled, Homebound_disabled, and the institutionalized disabled)

Figure 6. A Taxonomy of IoT Applications for the Disabled Users.

**Table 3.** Classification of IoT Applications for the Disabled Users.

| IoT Application Category | | Tool Location | Disabled Category[7] | Task | Medical Devices and Applications |
|---|---|---|---|---|---|
| **Mobile Devices** | | Carried by users | 1,2,3 | Detecting user activity, mobility, and health monitoring | • Logbook app for diabetes patients [61]<br>• CardioMEMS Heart Sensor for patients with chronic pulmonary disease [25]<br>• HealthWear captures activity of the skin [187] |
| **Robotics** | | In robots | 1,2,3 | Helping and monitoring disabled in their daily life activities | • ADL: Grandma's robot buddy, assisting with dressing, feeding, and supporting mobility [28]<br>• ADL: a robot assisting with shopping, housekeeping, and managing medications [186]<br>• EADL : a robot assisting with social activities such as hobbies [44] |
| **Personal Sensors** | **Wearable** | Integrated in objects clothes, shoes, belts, etc. | 1,2,3 | Monitoring the disabled in their daily life activities | • Smart Shirt, monitoring heart rate, ECG or respiration, e.g., Nuubo Smart Shirt [27]<br>• Watches monitoring blood oxygen, glucose level [43] |
| | **Non-Wearable** | Integrated sensors in home objects | 1,2,3 | Obtaining information about users' behavior in their own home | • Checking body temperature, tracking sleep quality, and detecting movements in bed; examples are Smart Pillow [65], Alarm-Net [64], and a non-contact heart rate monitoring system [66] |
| **Smart Homes** | | Home healthcare system is linked to the hospital | 1,2,3 | Improving a users life by centralizing and automating home tasks | • Home-based health care system, providing monitoring, reminder services, and fall detection; examples are Beclose app. [63], and m-health for wheelchair users [62] |

[7] Disabled categories 1,2, and 3 represent the independently-living disabled, Homebound_disabled, and the institutionalized disabled respectively.

## 4. Privacy and Security Issues in IoT Applications for the Disabled Users

All of IoT applications and systems serving the disabled are prone to different kinds of security and privacy attacks.

### 4.1. Privacy Issues in IoT Applications for the Disabled Users

In IoT applications for the disabled users, massive amounts of health data need to be gathered and analyzed. Questions arise who owns the medical data for a disabled, who has the right to access it, and where the disabled's data are stored? [21, 67, 32].

In this section we addresses the most common privacy issues in IoT applications for the disabled users along with IoT-based solutions that are known in the literature.

#### *4.1.1. Risks of Patients' Privacy Exposure*

A *Personal Health Record (PHR)* is "an individual electronic record of health-related information that conforms to the nationally recognized interoperability standards. PHR can be drawn from multiple sources while being managed, shared and controlled by the individual" [145]. PHRs are reported to the e-health center directly, and the primary privacy and security issue is to keep the patients' PHRs confidential.

Li et al. [29] proposed a method to encrypt each PHR with one-to-many encryption methods, such as the ABE technique, before outsourcing it. Encryption algorithms such as AES and MD5, together with efficient key management, have been used to encrypt each PHR file [30, 31]. A health system can be divided into two security domains, namely *public domains (PUDs)* and *personal domains (PSDs)*, according to the different users' data access requirements. PUDs consist of users who need access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent economic sector, such as healthcare, government or insurance sectors. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner [29].

Ukil *et al*. [33] presents a privacy measurement scheme that detects and analyzes sensitive content of time-series sensor data. It measures the amount of privacy, to make a decision whether to release private data or not (as shown in Figure 7). The amount of the privacy can be defined as follows:

$$\gamma_{s,v} = \rho_{\mathrm{M}} = \frac{\sum_{i=1}^{|v|} pr(v_i)\log_2 \frac{1}{pr(v_i)}}{\sum_{i=1}^{|s|} pr(S_i)\log_2 \frac{1}{pr(S_i)}} \quad \ldots\ldots. (1)$$

where $v$ is the sensitive part of $S$ (sensor data set) and $\gamma$ is the non-sensitive - part: $S = v \cup \gamma$

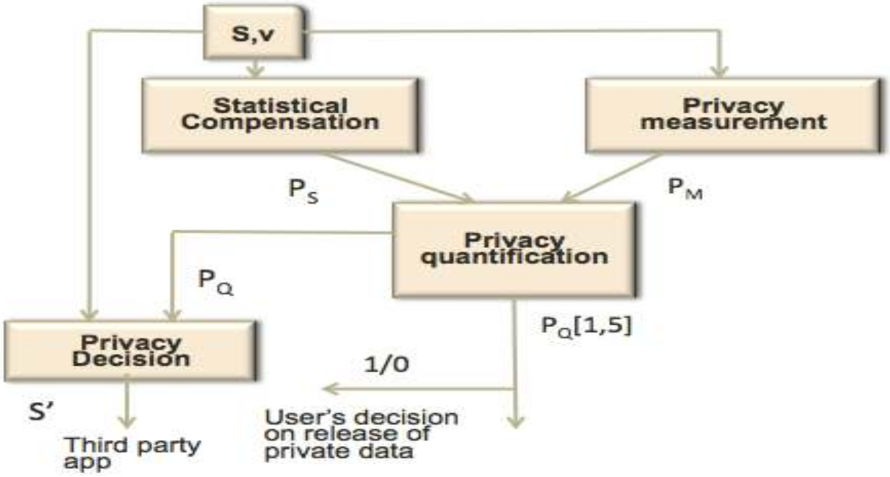

Figure 7. Privacy Measurement, Quantification, and a Data Privacy Decision [33].

### *4.1.2. Threats of Cyber-Attacks on Privacy*

Cyber attacks can inject false data into a system, causing critical damage in IoT applications. It is fundamental to provide the adequate level of protection against cyber-attacks in in smart home applications for the disabled. However, the resource-constrained nature of many of IoT devices present in a smart home environment do not allow to implement the standard security solutions.

Tajer *et al.* [71], proposed a framework that guarantees detection of the cyber attacks and recovering from them. Different controlling agents, distributed across the network, constitute the attack detection subsystem. System recovery involves iterative local processing and message passing. Nguyen *et al.* [88], proposed a new distributed cyber attack detection algorithm, based on the decision cost minimization strategy. It is shown that is a suitable solution for detection of both known and unknown cyber attacks.

### *4.1.3. Data Eavesdropping and Data Confidentiality*

Generally, the health data of patients, including the disabled, are held under the legal obligations of confidentiality, and made available only to the authorized caregivers. It is important to prevent stealing data from storage or eavesdropping on them while they flow over the wireless links. For example, a popular IoT-based disabled glucose monitoring and insulin delivery system utilizes wireless communication links, which are frequently used to launch privacy attacks.

Data eavesdropping may cause damage to the disabled by breaching the disabled's privacy. Li *et al.* [68] propose rolling-code cryptographic protocols and body-coupled communication to mitigate the eavesdropping on disabled's health data. Miaou *et al.* [69], propose a bi-polar multiple-base data hiding technique for images, where a pixel value difference between an original image and its default JPEG lossy decompressed image is taken as the number conversion base. The algorithm allows to hide, e.g., doctors' digital seals and PHR within a still image. (The doctors' digital seals are essential to the authentication of PHR.) The still image could be a logo of a hospital identifying where the PHR comes from. A diagnostic report and a biomedical signal, such as an electrocardiogram (ECG), can also be hidden in an image. The proposed approach allows hiding multiple data types in the same image. All these data can be separated and restored perfectly by the intended users [69].

Data confidentiality can be improved by using *Public Key Encryption (PKI)*. PKI creates an effective approach to data encryption as it can provide high level of confidence for exchanging information in an insecure environment. Atzori *et al.* [18] presents a conceptual design and a prototype implementation of a system based on IoT gateways that aggregate health sensor data and resolve privacy issues through digital certificates and PKI data encryption.

### *4.1.4. Identity Threats and Privacy of Stored Data*

Loss of a patient's privacy, especially her identity data may result in significant physical, financial, and emotional harm to the patient. Slamanig and Stingle [72] present mechanisms for preventing disclosure attacks:

1) *Unlinkability:* A system containing n users provides *unlinkability* if the relation of a document $D_i$ and a user $U_j$ exists with probability p = 1/n. Hence, an insider or attacker can not gain any information on links between users and documents by means of solely observing the system.
2) *Anonymity:* It is the state of being not identifiable within a set of subjects X. The degree of anonymity can be measured by the size of the anonymity set |X|. For example, anonymity is provided when anonymous user in a set $U' \subseteq U$ can access document $D_j$.
3) *Identity management:* A user's identity can be managed by dividing the identity of a person into sub-identities $I = \{I_{pub}, I_1, . . . , I_k\}$, where each the sub-identity is a user-chosen pseudonym. A user can assign any sub-identity for any subset of his PHR/EHR records. This allows her for hiding sensitive data via a sub-identity, thus protecting them from disclosure attacks.

Disclosing stored PHRs can cause losses of patients' privacy, especially her identity data. Anonymity and pseudonymity services can be used to hide the real identity that is tied to the stored data. Privacy services can guarantee protecting records by using differential privacy techniques that rely on adding noise to patients' records [84]. This may be used to assure that a database allows retrieving only statistical data, such as sum, average, count, etc.

### *4.1.5. Location privacy*

Location privacy is concerned with location privacy threats and eavesdropping on a user's location. Location privacy in WSNs, specifically hiding the message sender's location, can be achieved through routing to a randomly selected intermediate node (RRIN) [85]. Evesdropping and tracing of packets can be prevented by the Location Privacy Routing (LPR) protocol, which uniformly distributes the directions of incoming and outgoing traffic at sensor nodes [86].

Phantom single-path routing makes assures that packets reach the Base Station (BS) following different paths in such a way that every packet created by a source follows a different random path toward the BS [87].

This section has shown the privacy issues that directly influence disabled life. The privacy issues in IoT healthcare applications for the disabled users along with their IoT-based solutions are summarized in Table 4.

**Table 4.** Main Privacy Issues and the Corresponding IoT-based Solutions.

| **Privacy Issues** | **IoT-based Solutions** |
|---|---|
| PHRs exposure | Encryption before outsourcing, dividing health system into domains, analyzing sensitive data to be private or not |
| Cyber attacks | Detection methods and system recovery |
| Data eavesdropping and data confidentiality | Data hiding and cryptographic techniques |
| Identity threats and privacy of stored data | Pseudonymization of medical data, identity management, anonymity |
| Location privacy | Security protocols |

## 4.2. Security Issues in IoT Applications for the Disabled Users

The diversity of components of IoT makes the security issues in IoT applications for the disabled users more challenging. Thus, identifying and dealing with these security issues is a key issue for the development of these IoT applications. The minimum security requirements for the applications can be summarized as confidentiality, integrity, and availability (CIA).

Several research papers discuss security challenges for the IoT architecture [22, 23, 38, 49]. This Thesis investigates security issues for the following IoT components, described in Table 1: physical objects, communication technologies, and applications.

### *4.2.1. Security Issues for Physical Objects*

The security issues for physical objects include:

1) *Physical attacks*: Most of IoT devices are small and wirelessly connected such as constrained resource nodes. Therefore, it is important to protect the stored sensitive data in IoT devices and provide secure storage tools in the context of IoT. Moreover, since it is expected that more data would be in transit than in traditional architectures, there is an increased risk of realization of attacks and obtaining non-authorized access to data being transmitted [39]. Riahi *et al.* [40], define a systemic approach for IoT security. The system is made up of four

components: person, technological ecosystem, process and intelligent object. Those components interact through security factors namely identification, trust, privacy, safety, auto-immunity, reliability and responsibility. Moreover, an edge technology layer can be defined as sub-layers each one with their own security requirements. The sub-layers are multimedia, image and text or digital [106].

2) *Integrating RFID into IoT*: RFID technology has been used in IoT applications for the disabled users for identify, tracking, and tracing disabled. However, RFID systems are vulnerable to be attacked due to resource constrains. Nie *et al.* [96], IoT based RFID consists of three components including RFID system, middleware system, and Internet system. There are several security that correspond to those components such as eavesdropping, man in the middle attack, denegation of service, spoofing, cloning, tracking, abuse of tag, wireless communication risks, etc. [97, 98]. That is why we need to protect and restrict access to data from RFID tags. There are many RFID security defenses and techniques that are listed in literature such as two kinds of ciphers Symmetric and Asymmetric ciphers has been defined to avoid Eavesdropping peer-to-peer [35]. Since RFID technology does not need line of sight, unauthorized RFID readers can obtain the data if it is not encrypted. Rajan et al. [36], propose system-chaining method as a solution to avoid unauthorized RFID reader. Encryption is done using a chaining of AES algorithm and MD5 algorithm method. This encrypted data is send to the reader and then to the host computer. Authenticity is guaranteed by the use of MD5 algorithm. Therefore, the chaining method has improved the user authentication, integrity, security and privacy of the information being transferred from tag to reader. Moreover, authentication in IoT applications based on RFID is improved by using Elliptic Curve Cryptography [99]. While, protecting shares keys, encryption of the communication between the tag and reader, data encryption, data confidentiality and integrity are defined in [96, 99, 100].

3) *Integrating WSNs into IoT*: Those technologies have limited computational and energy resources. They are battery powered, and they are connected through lossy links. Therefore, they are vulnerable enough to be attacked by any adversary. An attacker can deploy malicious nodes that can work together to make damages to the network. For example, physical attack of the node can gain access to critical information such as security protocols, source code, and other data. Another issue is how to secure channel between a sensor node and Internet host [101]. WSNs have been used in many sensitive applications in the IoT for healthcare, so if the security of WSNs is attacked that may result in human harms and loss resources [78].

Therefore, there are some security requirements for WSNs must be considered such as encryption and calculation of Message Authentication Code (MAC) for data confidentiality and integrity, security protocols for secure location and availability. Li *et al.* [102], propose Signcryption that can improve securing of channel between a sensor node and Internet host, by achieving the *CIA* at lower cost.

4) *Denial of Service (DoS) attacks*: DoS and distribute DoS (DDoS) attacks makes the server resources/data unavailable to the disabled users. Once DoS attacks are presented from various compromised node is known as DDoS attack. We adopt RFID and WSNs technologies, and we describe the most common DoS attacks along with their solutions as shown in Figure 8 [94, 95]:

   a) *DoS on RFID*:

      - *Jamming*: Tags cannot communicate with readers; device broadcasts radio signals that block nearby RFID readers.
      - *Desynchronizing attacks*: Tags disabled; attacker aims to destroy the synchronization between RFID tag and reader.
      - *Kill command attacks*: Tags disabled; applying brute force method on it.

   b) *DoS on WSNs*:

      - *Node Destruction*: Destroying sensor nodes sensing and communications abilities.
      - *Jamming:* Disrupting a signal of nodes; sending/ receiving frequencies are jammed.
      - *SYN flood attack:* Server without resources; SYN sends thousands of SYN packets with spoofed source address.
      - *Denial of sleep attack:* High-energy consumption; transmitter remains awake for long time that bring down wireless networks.

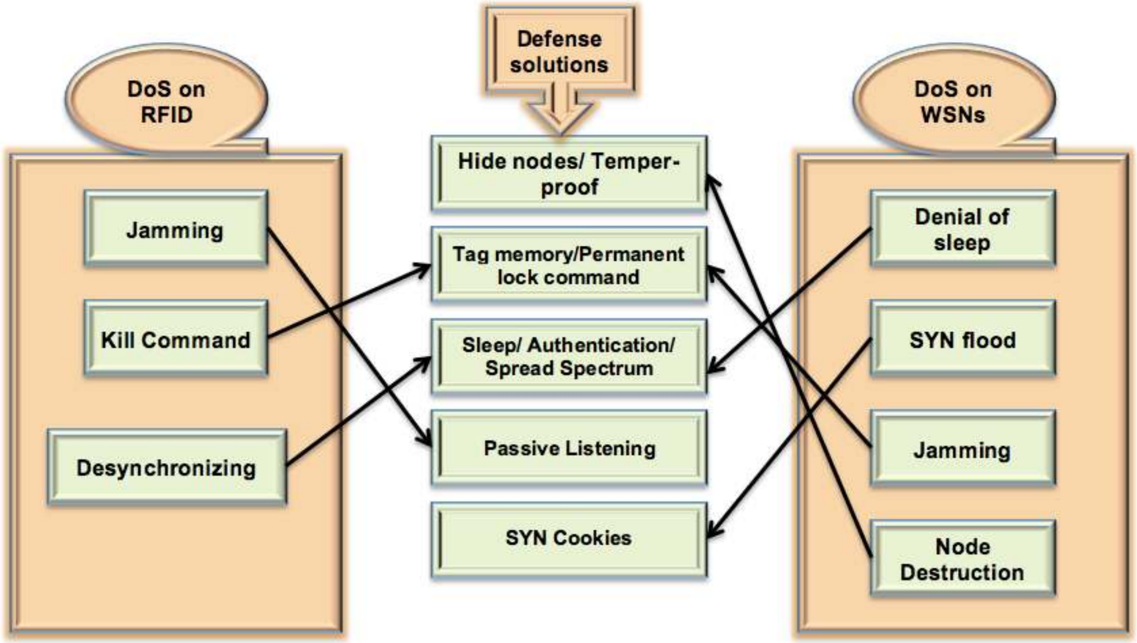

Figure 8. DoS on RFIDs and WSNs, and Known Defenses.

5) *Unauthorized data access/ access control*: Different users are assigned for different applications, and each application will have a big number of users. Therefore, effective authentication technology should take to prevent the illegal user involvement [55]. Moreover, access control is essential to prevent unauthorized entities from accessing to system's resources (data, services hardware, etc.) [34]. However, access threats without disabled's consent causes life-threatening risks. Therefore, access control mechanisms play a major role in preventing activities that lead to a breach of security in the IoT. Following are the security qualities of access control [90]:

   a) *Identification*: In IoT, things consist of several objects such as people, sensor nodes, laptops, medicines, etc [19]. Those things should be identified uniquely. There are different identification scheme that are proposed for IoT system such as RFID object identifier, IPv4, IPv6, EPCglobal, Near Field Communications Forum (NFC), etc. Therefore, identification is the attribute that identifies objects uniquely, and manages their identities while considering security and high scalability aspects of the IoT. Chun *et al.* [91], propose a scalable physical-object naming system (PONS) that reuses the existing ontologies and assigns URL-based semantic identifiers. The PONS constructs semantic (S-URLs) and assigns them to the IoT objects. Identification PONS is divided into four parts. The first part contains IoT objects registering and their properties. Second part includes S-URL that is generated according to the type of an object. Third part is the uniqueness checker that assures whether an object identifier is unique or not. The last component creates an encoded version of an S-URL. While another approach is an object identity management system (IdM). Current IdM systems are composed of two types of entities, which are identity providers (IdP) and service provider (SP), to manage authorization and to offer access and identity management services respectively [92].

b) *Authentication*: The corroboration that an entity is the one claimed, and the source of data received is as claimed. Authentication means identity verification. It plays a significant role before establishing a communication channel between two entities. Also, it confirms mutual trust between different objects or users by authenticating their identities [70]. Jing *et al.* [103], propose an authentication and access control method for IoT. The authentication is achieved by defining simple and efficient secure key establishment based on ECC. While access control is achieved by adopted Role Based Access control (RBAC)- base authorization method. Moreover, cluster based authentication is proposed in [104], and efficient authentication based on signal properties of the node is presented in [105]. Also, Huth *et al.* [112] present a system that provides the confidentiality and authenticity of devices for lightweight key distribution mechanism. The system is combined two technologies, which are Physical Unclonable Functions (PUF) and Physical Key Generation (PKG) over wireless communication. Those two technologies improve the physical properties of the communication channel.

### *4.2.2. Security Issues for Communication Technologies*

The security issues for communication technologies include:

1) *Secure Wireless PAN/LAN communication technologies:* In Table 2 we list and describe the main Wireless PAN/LAN communication technologies. There are security issues for these technologies, as shown in Table 2. For instance, launching DoS/ DDoS attacks that consist of reflection-based flooding attacks, flooding attacks, amplification-based flooding attacks, black hole attack, and homing attack [94]. Also, those technologies are prone to secure pairing, interface, scalability, power consumption, and turning on/ off discovery mode, exploiting the key exchange process, barites run out, Identity theft, tracking, spying, data theft, spam, man-in-the-middle attack, malicious attackers, and disrupting the network by interrupting [107]. The security techniques that should be applied in this group are intrusion

to detect malicious activates, identity based authentication, anti-jamming, firewalls to prevent unauthorized access to the networks. Also, encryption of all the wireless traffic provides the confidentiality of the transmitted data over wireless networks such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and EES (Escrowed Encryption Standard). In addition, strong authentication is required to prevent the alteration of the communications.

2) *Secure Wireless WAN communication technologies:* In this Thesis, we focus on LTE and LTE-A security issues. First, LTE supports people living in remote areas by facilitating services such as high speeds remote video stream due to its large bandwidths, next generation technology such as OFDM, and low- latency traffic [156]. LTE has several security issues such as man-in-the middle attack, user identity threats, and Sequence Number synchronization (SQN). Re-authentication protocol (Extensible Authentication Protocol-Authentication and Key Agreement) is proposed to provide mutual authentication, resistant any attacks, and strong security [157]. Huang *et al.* [161], show security transmission in LTE can enhanced by integration RSA and Diffie-Hellman, and intelligent protection key chain with data connection core. While LTE-A provides high data rate and low latency, but at the same time bandwidth issues is raisin here due to large number of IoT devices try to access the network in very short time. Scheduling algorithms can avoid the collision without affecting the QoS [159]. Another secure authentication scheme for LTE-A that combines Pseudo random number generator with Diffie-Hellman algorithms by using Data Connection Core (SPDiD) for a wireless environment [160].

**Table 5.** Standardized Security Solutions and Their Mapping into TCP/IP Layers.

| TCP/IP Layers | IoT Protocols | Security Protocols | Security Services |
|---|---|---|---|
| Application | CoAP, MQTT | DTLS, TLS/SSL | Confidentiality, integrity, availability, authentication, authorization |
| Transport | UDP | DTLS | Confidentiality, integrity, availability, authentication, protection against DoS attack |
| Network | RPL, IPv6 | RPL security, IPsec | Confidentiality, integrity, availability, authentication |
| Adaptation[8] | 6LoWPAN | IPsec | Confidentiality, integrity, availability, authentication |
| Data-Link | IEEE 802.15.4 | IEEE 802.15.4 security | Confidentiality, authentication |

[8] Adaptation layer has been added to the TCP/IP stack for IoT [173, 26].

3) *Secure IoT communication protocols for constrained-resource environment:* This Thesis highlights the main IoT communications protocols and shows their ability to provide security services. Communication protocols defined by the standards from the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF), enable the standardized stack [119].

   Table 5 summarizes the following standardized security solutions (and shows their mapping into TCP/IP Layers):

   a) *Secure communication in Data Link Layer:* Data-link layer includes wireless PAN/LAN/WAN communication technologies. Table 5 indicates that IEEE 802.15.4 is suitable for IoT due to several features, such as less complex modulation and better power management. IEEE 802.15.4 has two kinds of devices can participate: RFDs (Reduced functional devices) that are always in sleep mode and then it wakes up periodically to request data from the coordinator where data is stored, and FFDs (Full-Function Devices) is elected as Personal Area Network (PAN) coordinator and responsible for security and network management [175]. There are standards that are implemented in upper layer such as ZigBee and 6LoWPAN. 6LoWPAN has clear advantages over ZigBee. For example, 6LoWPAN works on enabling IPv6 over IEEE 802.15.4 standard. The security of IEEE 802.15.4 is provided through MAC layer that designed to secure communication. Security requirements for IEEE 802.15.4 MAC layer are access control that can achieve through maintain ACL of valid device, confidentiality through encryption, frame integrity provided by MAC, and sequential freshness through message counter to avoid old messages [176]. Furthermore, The standard includes a security suite AES (Advanced Encryption Standard 128 bits symmetric-key cryptography) [115]. IEEE 802.15.4 link-layer security is the current security solution for IoT. It secures the communication on a per-hop security that can detect the message modification on each hop in order to provide the trust for each node in the communication path [173]. Finally, number of security services that are provided by IEEE 802.15.4 such as confidentiality, data authenticity, and replay protection [177].

   b) *Secure communication in Adaptation Layer:* 6LoWPAN combines the latest version of the Internet Protocol (IPv6) and the Low Personal Area Networks (LoWPAN). 6LoWPAN enables devices (Constrained resources) to transmit information wirelessly using Internet protocols [48]. For example, the diabetes therapy management in AAL environments based on IoT that support patients' profile management architecture depending on RFID cards, and provide global connectivity based on 6LoWPAN [12]. It is large network size, low power consumption, mesh network topology, and use both 2.4 GHz and the 868 MHz/915 MHz ISM bands [155].

There are several issues are related to 6LoWPAN security such as low power, low processing, DoS attack, and small packet transmitting. Hussen *et al.* [158], show that 6LoWPAN attacks can be handled by proposing secure authentication and key established scheme. Moreover, Raza *et al.* [173], indicate communication in 6LoWPAN can be secured using IPsec protocol. The extension of 6LoWPAN with IPsec provides authentication, and the integrity of messages. Goswami *et al.* [174], show that the integration of Public Key Infrastructure (PKI) with 6LoWPAN provides Confidintiailty.

c) *Secure communication in Network Layer:* We outline Routing Protocol for Low power and Lossy network (RPL) and IPv6 as transport layer protocols. RPL allows developing of advanced monitoring applications; due to its ability to ensure building a very fast network setup and limited delay. RPL protocol supports various types of control messages, such as DIO (DODAG Information Object), DIS (DODAG Information Solicitation), DAO (Destination Advertisement Object), DAO-ACK (DAO acknowledgment) and CC (Consistency Check) messages [171].

RPL is light weight protocol, and it is suitable for IoT constrained devices [48]. Therefore, it is prone to a number of routing attacks that aim to disrupt the topology of the network. In topology attack, breaking the optimized network topology will change the node operation. Le *et al.* [172], show RPL is underlying protocol for 6LoWPAN devices that suffer from many security attacks such as internal and external attacks. Encryption solutions secure RPL control messages, while Intrusion detection system (IDS) can detect those malicious behavior. Moreover, RPL supports confidentiality (in cryptographic algorithms), integrity (AES/CCM with 128 bits keys for MAC), and authentication (RSA with SHA-256 for digital signature).

At the network layer, IPv6 needs to be used if data will be transmitted over the Internet. Security is supported by the IP Security (IPsec) protocol that provides confidentiality (using Encapsulated Security Payload (ESP)), integrity and authentication (IP header along with Authentication Header (AH) protocol) [173]. Transport protocols such as TCP, UDP, and HTTP can be used with IPsec. Several security schemes for IP protocols in IoT are proposed. Host Identity Protocol and Multimedia Internet Keying protocols provide securing network association and key management. HIP - based on asymmetric-key cryptography supports identification for unambiguous objects, mobility support, and secure network association. HIP with MIKEY capabilities provide enhanced key management using polynomials, which provide generating pair wise keys with any node depend on its identity. This combination of protocols and crypto-algorithms guarantees strong security [167]. While DoS threats can be prevented by using used Learning Automata (LA) concepts. LA concept is presented a Service Oriented Architecture (SOA), which is used as a system model for IoT.

d) *Secure communication in Transport Layer:* Under application protocols we describe the transmission control protocol, which is User Datagram Protocol (UDP). UDP sends packets as soon as are requested. Also, UDP is good for real-time data stream applications such as audio and video. The most common security protocols are Transport Layer Security (TLS) and Secure Sockets Layer (SSL). SSL provides encryption, authentication and integrity, and it comes below application layer protocol HTTP [164]. Combines Diffie-Hellman algorithm with SSL enhanced the performance of the network and improved the security of the communication [165]. Moreover, the combination of SSL and public key encryption can be used to enhance the transmitted data as presented in [166]. However, TLS is only used over TCP is suitable for human interaction with web such as e-mails and web browsing, but at the same time it is not suitable for smart objects communication because of its low-power networks [162]. Hence, Datagram Transport Layer Security (DTLS) is adopted by UDP that provides protection against DoS. Hummen *et al.* [113], presente delegation architecture based on DTLS protocol that secure and protect communication for constrained devices. Also, DTLS provides confidentiality, integrity and authentication [116, 170].

e) *Secure Communication on Application Layer:* There are several communications attacks in this layer such as end-to-end applications security issues, packet lost, recording, data access in compromised node, eavesdropping, and authentications. There are several communication protocols that secure the communications in application layer such as CoAP, MQTT, XMPP, REST, AMQP, and WEB socket [114]. The best known protocols for low cost, low power/constrained devices are CoAP, and MQTT [118]:

- *CoAP:* It is Constrained Application Protocol from CoRE (Constrained Resources Environment), designed by IETF group [50]. Also, it is one-to-one protocol for transferring data between client and server. For example, CoAP is the best choice for smart homes applications because smart homes network have low-cost and lightweight characters. Security is critical to protect the communication between devices. Thus, DTLS is introduced to provide security for transfer data over UDP [115]. DTLS includes three implements that provide strong security such as packet retransmission, reply detection, and assigning sequence number with the handshake. Therefore, DTLS protects end-to-end applications and provides confidentiality, integrity, and authentication [116, 170]. CoAP is tailored for M2M communication, constrained devices. Moreover, it supports sleepy devices better than MQTT, especially devices that have cycling duty (hourly, daily, etc.) [118].

- *MQTT:* It is Message Queue Telemetry Transport, designed by IBM, and providing efficient data transport under wireless environment with limited energy and bandwidth [51]. Also, it is many-to-many communication protocol for transferring information between multiple clients. Authentication in MQTT requires username and password from client to connect, and TCP connection encrypted with cryptographic protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS). SSL and TLS use handshake mechanism to create a secure communication between the client and server. Then, when the handshake is accomplished, the encrypted communication between client and server will be provided. Hence, an attacker cannot eavesdrop the communication [114]. Moreover, Gomes *et al.* [117], show MQTT can be integrated with ISO/IEEE 11073 standard to reduce the amount of the data traffic that comes from Personal Health Devices (PHD).

4) *Secure transmitted data*: The disabled's sensed data will be transmitted wirelessly to the caregivers (family members, doctors, nurses). The transmitted data could be attacked while it is in transmitting process in the wireless channel [54]. The adversary can alter the disabled's data by capturing the transmitted data from in wireless channels. Yang *et al.* [37], propose secure IoT transmission based on IBE and PKI/CA. Moreover, Dai *et al.* [108], propose chaotic synchronization system in order to solve security of data transmission in wireless networks. The proposed system contains two chaotic systems that are kept synchronized to realize the complete recovery of the encrypted signal. Li *et al.* [109], propose a DNS protocol to enhance the security of Object Naming Service (ONS) query process in the tag. The proposed system solves the security issues of the transmission of data in plain text. Moreover, Zhang *et al.* [163], propose peer to peer (P2P) or end to end security protocols to enhance protection of the transmitted data, and provide high security, high efficiency, and low cost. P2P secure communication includes three components, which are message handler

(message de/encapsulation/ routing), security configuration (security configuration), and security manager (operations for secure communication). Furthermore, there is a method to secure data transmission on wireless network by data encryption into text with dynamic inputs, which provides reliable and secure data transmission [111]. Then, using the existing protocols for wireless network like Kerberos data transmission uses ciphertext.

Secure data aggregation is another problem. For example, the data from disabled's monitoring environment is collected and send large amounts of them to the medical center through wireless channel. Liu *et al.* [110], proposed Trust–Based Secure Data Aggregation (TBSDA) for IoT. This data aggregation can be made secure by behavior-detecting trust evaluation and data assembling technique used inside of the sensor nodes.

### *4.2.3. Security Issues for Applications*

1) *Security issues for health cloud computing:* There are several cloud computing issues that are related to the security in the healthcare field:

   a) *Secure data access:* PHRs in cloud can be attacked and that lead to loss of personal data, failure of medical care, and shearing PHRs. Therefore, it is crucial to mange secure access to the stored data in the cloud. Another issue is a malicious insider attack that aims to modify the patients' data. Alshehri *et al.* [138] present encryption/decryption techniques to secure access of the data in the cloud. The security technique uses Ciphertext-Policy Attribute-Based Encryption (CPABE) that based on Elliptc Curve Cryptography (ECC), Bilinear Maps, and Attribute-Based Encryption (ABE). Encrypting PHRs depends on healthcare providers. While, decrypting PHRs needs sets of attributes for proper access. Moreover, Role-based access control (RBAC) cryptographic techniques have been developed to include cryptographic and access control techniques to secure and protect stored data in cloud. In this case, RBAC enables data owners to mange and share their data in cloud [135]. Also, data isolation has been proposed in order to ensure that the stored data in the cloud will be accessed only by one company [133]. Authors [139], proposed a secure data technique by using digital watermarking with encryption for detection of the modification by an insider attack. Disabled or caregivers' information can be used as a watermark. Then, the watermark will be embedded in the host data, combined with authorized users list names, encrypted with asymmetric secret key, and finally sent to the cloud.

b) *Data protection:* Data stored in the cloud in a shared environment. Those disabled's sensitive data are resided with other collected data from different costumers. Therefore, the big question has raisin here, which is how to secure stored data in the cloud. Data encryption is the security technique that has been used for secure data in cloud. Zardari *et al.* [132], classify data security into two groups: sensitive and non-sensitive (public data). Then, after classifying the sensitive data, data confidentiality will be achieved by applying RSA algorithm on sensitive data to keep it secure. A game-theoretic model is proposed [134] to enhance securing data from malicious cloud users. Moreover, losing PHRs in cloud is another issue, and it can be solved by keeping data encrypted and making backup plan of data loss [137].

c) *Big data:* It is a term not only means too large data can not be fitted into memory or standard database but also it is distributed into three dimensions: Volume, Velocity, and Variety [140]. In healthcare, Electrocardiogram (ECG) data are collected and proceed, and stored as a big data. For example, when such system collects ECG signals from one person at 240 Hz (240 data per second), it collects 864,000 data per hour. Therefore, data will be huge and called big data if collects form 10,000 persons [141].

One of the big data issues is moving big data to the cloud is still an open issue. Zhang *et al.* [136]**,** propose two algorithms, that are an online lazy migration (OLM) algorithm and a randomized fixed horizon control (RFHC) algorithm for optimizing of the data center, data aggregation, data processing, and transmitting data routers at any given time. Another issue is unstructured big data analysis. Big data can include both structured and unstructured data. Structured big data refers to type of data that has a defined length and format. For instance, structured data includes numbers, date, words, and strings that can be resided in database (row/column) [142]. While, unstructured big data refers to information that cannot be fitted in a traditional database such as videos, audio files, images, e-mail messages, and so on. Volume of the unstructured data is growing rapidly; experts estimate that 80 to 90 percent of the data is unstructured [143]. Islam *et al.* [144], show security of structured data can be handled by existing security technologies or standard SQL queries. While, the security scheme for unstructured data includes four security aspects that provides identification and authentication using signature and password verification scheme, confidentiality by using encryption an decryption algorithms, integrity by using hash function, and integrity and authentication by using MAC that is used for access control.

2) *Real-time information processing:* It is difficult to achieve real-time analysis of large amount of disabled's sensory data that are provided from different resources. Kolozali *et al.* [146], propose a stream annotation framework for real-time IoT stream by using Advanced Message Queuing Protocol (AMQP) that support delivering a huge amounts/volumes of data. While, time-based event is a scheme that is proposed for summarization of the stream data. Furthermore, PCA (Principal Component Analysis) algorithm is used to decrease the dimension of the multiple sensor dataset and project the dominating differences among measured water samples on a 2D scores plot [147]. Tsai [149], propose a real-time digital videos cameras can be enhanced using a Fast Dynamic Range Compression Format with a Local Contrast Preservation (FDRCLCP) algorithm that can improve real-time processing for videos efficiently. Moreover, real-time control decisions guarantee is another issue. Scheduling techniques that provide real-time decision control such as Hadoop, Grid-based scheduling, and Quincy scheduling techniques are presented in [150, 151, 152].

3) *DoS on application layer:* Application layer is the most top layer in IoT architecture that contains user interface. One of the most issues in this layer is DoS/DDoS. Sonar *et al*. [94], show there are two types DoS/DDoS in this application layer:

   a. *Reprogramming Attack:* An attacker/ hijacker can get access, modify, and control the source code such that the application request goes in infinite waiting for network resources. Therefore, an authentication stream is the defense mechanism against this attack [168].

   b. *Path based DoS Attack:* An attacker floods a multi-hop end-to-end communication path using replayed packets or injected spurious packets. In this case the sensor nodes will be overwhelmed, and network lifetime will be reduced. Therefore, anti reply protection and packet authentication are the defense mechanism against this attack [169].

*4) Web application attacks:* There are several attacks in application layer among them we explain the most common attacks related to the healthcare application such as XSS, CSRF, and SQL Injection attacks:

   a) *Cross-Site Scripting (XSS) Attack:* This attack works on compromising the trust relationship between the user and the web application site by injecting malicious code. Attackers can control the integrity of the application. Hence, the security and the privacy of the disabled users will be breached [120]. This kind of attack can be prevented using firewalls and cryptography mechanism. Also, XSS attack can be avoided by using secure coding/ programming techniques [121]. Moreover, machine learning based XSS detection system is presented in [122]. Finally, flirting method to prevent XSS attack is proposed [123].

b) *Cross-Site Request Forgery (CSRF) Attack:* also it known as a session riding or one click attack. This attack aims to transmit malicious user's requests that the target website trusts without user's consent [124]. Therefore, user clicks a URL link that contains an unauthorized requests against the website, so the website cannot distinguish whether those requests are authentic or not. Blatz [125], show CSRF attack can be prevented in two groups of solutions which are website protection such as conformation screens, using post, cryptography techniques. Another group solution personal protections mechanisms that includes logging out, changing default passwords, using different browsers, etc. Also, CSRF Guard is a tool that runs on Java EE platform that can be efficient to defend CSRF attack as presented in [126].

c) *SQL Injection Attack:* An attacker aims to inject a SQL query from the client to the application. Hence, attacker can read, modify, alter data from database management system (DBMS). Also, execution administration operations on the database can be accomplished via SQL injection attack such as recovering and shutdown the DBMS. The SQL injection attack consequences impact confidentiality, integrity, authorization, and authentication [127]. The defending mechanisms against SQL injection attacks consists of using web application firewall, intrusion detection, avoiding constructing SQL queries with user input, and data sanitization (filtering all user input) [128]. Moreover, tokenizing original query and a SQL injection query separately into two arrays. Then, comparing the length of the two arrays will be detected if there is an injection or not [129].

# 5. Privacy and Security Requirements for IoT Applications for the Disabled Users

This Section uses the issues identified in the preceding section to list the privacy and security requirements for the IoT applications for the disabled users.

## 5.1. Privacy Requirements for IoT Applications for the Disabled Users

We can summarize the privacy requirements for IoT healthcare applications for the disabled as shown in Figure 9:

1) Disabled should know who owns their health data.
2) Appropriate disabled's permission for using her health data (e.g., power of attorney for a caretaker).
3) Anonymity or pseudonymity to hide real identities of the disabled users by means of dividing the identity of a person into sub-identities.
4) Location privacy to keep locations of users, devices, etc., private.
5) Maximizing the locality of information.
6) Privacy for IoT devices.
7) Emphasizing privacy from the beginning of the application design.

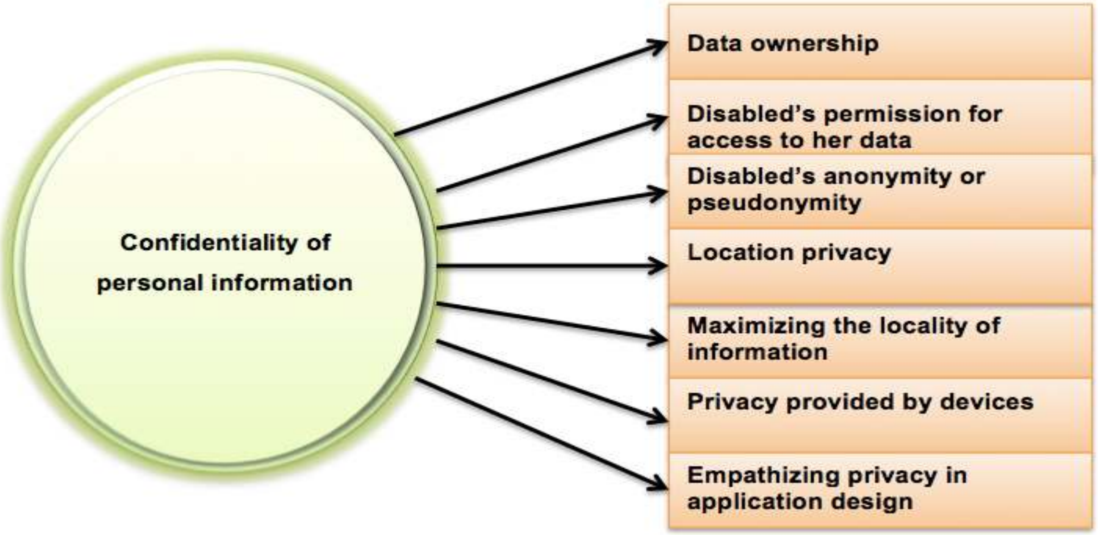
Confidentiality of personal information
Data ownership
Disabled's permission for access to her data
Disabled's anonymity or pseudonymity
Location privacy
Maximizing the locality of information
Privacy provided by devices
Empathizing privacy in application design

Figure 9. Confidentiality of Personal Information Requirements.

## 5.2. Security Requirements for IoT Applications for the Disabled Users

There are several different security requirements for each IoT applications for the disabled users. Table 6 presents security requirements for IoT components.

**Table 6.** Security Vulnerabilities, Threats/Attack Types, and Security Requirements/Solution Categories for IoT Components.

| IoT Components | Vulnerabilities | Threats/Attack Types | Security Requirements/ Solution Categories |
|---|---|---|---|
| **Physical Objects** | • Devices of this layer have limited calculation, communication and storage resources<br>• Nodes are distributed in distant location; adversary can easily accesses the devices and performs damages and illegal actions such as extract security information, keys, reprogram the device, etc. | • Physical attacks<br>• Integrating RFID<br>• Integrating WSNs<br>• DoS/DDoS<br>• Unauthorized data access and access control | • Evaluate suspicious nodes' behavior can reduce the influence of malicious nodes<br>• Encryption/ Cryptographic techniques<br>• Access control<br>• Authorization<br>• Identification<br>• Authentication |
| **Communication Technologies** | • IoT is a dynamic network infrastructure<br>• Low power<br>• Lossy network<br>• The challenges of selection security technique for each element<br>• Defense capability of the network varies in different networks | • Wireless PAN/LAN communications<br>• Wireless WAN communications<br>• Secure IoT communication protocols in constrained resources environment<br>• Secure transmitted data | • Communication security: the proposed security protocols ensure the smoothness transitions connections among different edge networks<br>• Confidentiality service can be ensured through encryption/ decryption<br>• Strong authentication<br>• Backup solution: the ability of providing fast backup solution when network fails<br>• Enhanced the security of IoT communication protocols<br>• Authorized access<br>• Availability[9] |

[9] Availability: It is provided by existing confidentiality, integrity, and authentication [173]

|  |  |  |  |
|---|---|---|---|
| **Applications** | • Cloud computing<br>• Data exposure<br>• Web application security issues<br>• Secure communication | • Data access<br>• Data protection<br>• PHRs Attacks<br>• Malicious insider attack<br>• Sharing data in multiple environments<br>• Real-time information processing<br>• Big data<br>• Sharing the same sensed data by several applications<br>• DoS<br>• XSS attack<br>• CSRF attack<br>• SQL Injection | • Implementing the separation between information content and information source/ data isolation<br>• Encryption/ decryption mechanisms<br>• Secure data access<br>• Confidintiailty of data<br>• Secure sensitive data<br>• Backup plan<br>• Scheduling techniques<br>• Assuring identification<br>• Proposing traditional distributed database technology<br>• Assuring authentication<br>• Firewall and antivirus<br>• Intrusion detection<br>• Enhanced communication protocols security |

## 6. CONCLUSIONS

The recent developments in the area of Internet of Things (IoT) show a great promise for providing solutions for healthcare, including healthcare for the disabled people. However, there are many privacy and security challenges in IoT healthcare applications for the disabled users.

This Thesis discusses IoT, its layered architecture, and its role in the healthcare industry. It describes privacy and security services, and proposes viewing confidentiality as the intersection of privacy and security. The Thesis presents IoT components in the context of the IoT architecture, and mainly from the security and privacy perspective. The Thesis identifies the types of disabilities and categorizes the with respect to their mobility. It describes the range of IoT healthcare applications for the disabled along with their classification. It investigates privacy and security issues in IoT healthcare applications for the disabled, and reviews IoT-based solutions known in the literature. The Thesis identifies privacy and security requirements for IoT healthcare applications for the disabled users.

# REFERENCES

[1] A.J. Jara, M.A. Zamora, and A.F.G. Skarmeta,"(HWSN6) Hospital Wireless Sensor Networks based on 6LoWPAN technology: mobility and fault tolerance management, *" 7th IEEE/IFIP Int. Conf. on Embedded and Ubiquitous Computing*, vol. 2, Vancouver, Canada, Aug. 2009, pp.879-848.

[2] R. Tesoriero, J.A. Guled, M.D. Lozano, and V.M.R., Penichet,"Tracking Autonomous Entities using RFID Technology ," *IEEE Trans. on Consumer Electronics*, vol. 55 (2), May 2009, pp. 650-655.

[3] D. Giusto, A. Iera, G. Morabito, and L. Atzori,"An Overview of Privacy and Security Issues in the Internet of Things, "*The Internet of Things*, 1st Ed., Springer, New York, 2010, pp. 389-395.

[4] P. Yang, W. Wu, M. Moniri, and C.C. Chibelushi,"Efficient Objects Localization Using Sparsely Distributed Passive RFID Tags," *IEEE Trans. on Industrial*, vol. 60(12), Dec. 2013, pp.1-11.

[5] U.S Department of Health and Human Services. Last access Oct. 12, 2014.

Available on: http://www.hhs.gov/ .

[6] World Health Organization. Last access Oct. 12, 2014. Available on: http://www.who.int/topics/aging/en/index.html,

[7] H. Steg, H. Strese, C. Loroff, J. Hull, and S. Schmidt,"Europe Is Facing a Demographic Challenge - Ambient Assisted Living Offers Solutions," *VDI/VDE/IT*, Berlin, Germany, 2006, pp. 26-33.

[8] A.J. Jara, M.A. Zamora, and A.F.G. Skarmeta,"An ambient assisted living system for telemedicine with detection of symptoms," *Bioinspired Applications in Artificial and Natural Computation 3rd Int. Work-Conf. on the Interplay Between Natural and Artificial Computation*, 2009, pp.75-84.

[9] G.A. Kaplan," Maintenance of functioning in the elderly," *Annals of Epidemiology* , vol. 2(6), 1992, pp. 823–834.

[10] Y.A. Chen, and M. Thomas, "Vision screening in the elderly: current literature and recommendations," *University of Toronto Medical J.*, val. 87(3), 2010, pp. 166–169.

[11] Bluetooth, Low Energy. Last access July 28, 2015. Available on: http://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy

[12] A.J. Jara, M.A. Zamora, and A. F.G. Skarmeta, " Diabetes Management and Insulin Therapy in the Hospital and AAL environments based on Mobile Health, " *II Int. Workshop on Ambient Assisted Living*, Valencia, Spain, 2010, pp.1-10.

[13] M.A. Cucciare, K.R. Weingardt, and K. Humphreys," How Internet Technology can improve the Quality of Care for Substance Use Disorders?," *Current Drug Abuse Reviews*, Bentham Science Publishers, 2009, pp.1-7.

[14] A.L. Bleda, R. Maestre, A.J. Jara, and A.G. Skarmeta, "Ambient Assisted Living Tools for a Sustanaible Aging Society, " *Resource Management in Mobile Computing Environments, Modeling and Optimization in Science and Technologies*, vol. 193(3), 2014, pp.193-220

[15] Kubo," The Reaserach of IoT Based on RFID Technology," *IEEE 7th Int. Conf. on Intelligent Computation Technology and Automation*, China, Changsha, Oct. 2014, pp. 832-835.

[16] An Internet of Things. Last access Mar. 14, 2015. Available on: http://postscapes.com/internet-of-things-examples/ .

[17] G. Santucci, "From Internet to Data to Internet of Things," *Proceedings of the Int. Conf. on Future Trends of the Internet, J. Wireless Personal Communications*, vol. 58(1), May 2011, pp. 49-69.

[18] L. Atzori, A. Lera, and G. Morabito,"The Internet of Things: A Survey," *Computer Networks*, vol. 54(15), Catania, Italy, 2010, pp.1-17

[19] Y. Zhen, "The development of the Internet of Things," *J. of Nanjing University of Posts and Telecommunications(Social Science)*, vol. 12(2), June 2010, pp. 8-9.

[20] D. Chen, G. Chang, L. Jin, X. Ren, J. Li, and F. Li,"A Novel Secure Architecture for the Internet of Things," *IEEE 5th Int. Conf. on Genetic and Evolutionary Computing*, Xiamen, China, Aug. 2011, pp.311-314.

[21] C. M. Medaglia and A. Serbanati,"An overview of privacy and security issues in the internet of things", *In Proc. of 20th Tyrrhenian Workshop on Digital Communications*, Italy, 2010, pp. 389-395.

[22] C. C. Aggarwal and P. S. Yu," An Introduction to Privacy- Preserving Data Mining," in *Privacy-preserving data mining models and algorithms,* 1st Ed., *Springer US*, New York, 2008, pp.1-9.

[23] R.H. Weber,"Internet of Things - New security and privacy challenges, "*Computer Law and Security Report*, vol. 26(1), Jan. 2010, pp. 23-30.

[24 ] A.J. Jara, M.A. Zamora, and A.F.G. Skarmeta,"An architecture for ambient assisted living and health environments," in *Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing, and Ambient Assisted Living*, Springer Berlin/Heidelberg, vol. 5518, Jan. 2009, pp. 882-889.

[25] CardioMEMS$^{TM}$ HF System. Last access Oct. 14, 2014.
Available on: http://www.cardiomems.com/content.asp?display=news&view=17.

[26] Z. Qian, Y. Wang, X. Wang, and S. Zhu," M/I Adaptation Layer Network Protocol for IoT Based on 6LoWPAN", *The Internet of Things*, Springer, Changsha, China, Aug. 19, pp. 208-215.

[27] Nuubo, wearable medical technology. Last access Oct. 20, 2014. Available on: http://nuubo.es/?q=en/node/162.

[28] Meet Mr. Robin, Grandma's robot buddy. Last access Oct. 20, 2014. Available on:http://www.cnn.com/2014/05/16/tech/innovation/meet-mr-robin-grandmas-robot/ .

[29] M. Li, S. Yu, Y. Zhen, K. Ren, and W. Lou," Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption" *IEEE Trans. on parallel and distributed system*, vol. 24(1), UT, Mar. 2012, pp.131-143.

[30] S.K. Manda, and B. Hanmanthu," Privacy Preserving Support for Mobile Health Care using Message Digest," *Int. J. of Advanced Research in Computer Science and Software Engineering*," vol. 3, Sept. 2013, pp. 197-102.

[31] Y. Ren, R.W.N. Pazzi, and A. Boukerche,"Monitoring Patients via a Secure and Mobile Healthcare System," *IEEE Wireless Communications*, vol. 17(1), Feb. 2010, pp. 59-65.

[32] K.D. Mandl, P. Szolovits and I.S. Kohane," Public Standards and Patients', Control: How to Keep Electronic Medical Records Accessible but Private, *BMJ,* vol. 322, Feb. 2001. pp. 283-287.

[33] A. Ukil, S. Bandyopadhyay, and A. Pal,"IoT-Privacy: To Be Private or Not To Be Private," *IEEE INFOCOM*, Toronto ON, Apr. 2014, pp.123-124.

[34] Basic security for the small healthcare practice. Last access Nov. 11, 2014. Available on:

http://healthit.hhs.gov/pdf/cybersecurity/Basic-Security-for-the-Small-Healthcare-Practice-Checklists.pdf,.

[35] K. Finkenzeller,"Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities," *5th European Workshop on RFID Systems and Technologies*, Nov. 2009, pp. 1-31.

[36] J.G. Rajan and A.K. Nair," Vlsi Implementation of Cryptographic Algorithms in Internet of Things," *IEEE 2nd Int. Conf. on Mechanical and Electrical Technology (ICMET)*, Apr. 2014, pp.521-525.

[37] L. Yang, P. Yu, W. Bailing, B. Xuefeng, Y. Xinling, and L. Geng," IOT Secure Transmission Based on Integration of IBE and PKI/CA," *Inter. J. of Control and Automation,* vol. 6(2), Apr. 2013, pp. 245-254.

[38] H. Sue, J. Wan, C. Zou, and J. Liu," Security in the Internet of Things: A Review", *IEEE Inter. conf. on computer science and electronics engineering*, vol. 3, Mar. 2012, pp. 648-651.

[39] Gambs et al. last access Nov. 19, 2014. Available on: http://licit.inrialpes.fr/apvp2010/slides/APVP_ADEPT_Gambs.pdf.

[40] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah," A Systemic Approach for IoT Security," *IEEE Int. Conf. on Distributed Computing in Sensor Systems (DCOSS)*, Boston, May 2013, pp.351-355.

[41] V.M. Rohokale, N.R. Prasad, and R. Prasad," A Cooperative Internet of Things (IoT) for Rural Healthcare Monitoring and Control," *IEEE 2nd Int. Conf. on Wireless Communication*, Chennai, Feb. 2011, pp.1-6.

[42] S. Hussain, S. Schaffner, D. Moseychuck," Applications of Wireless Sensor Networks and RFID in a Smart Home Environment," *IEEE 7th Annual Conf. on Communication Networks and Services Research*, Moncton, NB, May 2009, pp. 153-157.

[43] Apple Watch reportedly has onboard hardware for measuring blood oxygen saturation. Last access June 25, 2015. Available on: http://www.idownloadblog.com/2015/05/25/apple-watch-blood-oxygen-saturation-hardware/

[44] S. Brose, D. Weber, B. Salatin, G. Grindle, H. Wang, J. Vazquez, and R. Cooper, "The role of assistive robotics in the lives of persons with disability," *Amer. J. Phys. Med. Rehabil.*, vol. 89(6), 2010, pp. 509–521.

[45] Types of Networks. Last access Nov. 18, 2014. Available on: http://study.com/academy/lesson/types-of-networks-lan-wan-wlan-man-san-pan-epn-vpn.html.

[46] Wireless security protocols: WEP, WPA, and WPA2**.** Last access Nov. 18, 2014. Available on: http://www.dummies.com/how-to/content/wireless-security-protocols-wep-wpa-and-wpa2.html.

[47] IoT and people with disabilities. Last access Nov. 19, 2014. Available on: http://www.atlargeinc.com/insights/internet-things-iot-and-people-disabilities.

[48] P. Pongle and G. Chavan," A survey: Attacks on RPL and 6LoWPAN in IoT," *IEEE Int. Conf. On Pervasive Computing*, Pune, Jan. 2015, pp. 1-6.

[49] G.S. Matharu, P. Upadhyay, and L. Chaudhary," The Internet of Things: Challenges and Security Issues," *IEEE Int. Conf. on Emerging Technologies*, Islamabad, Dec. 2014, pp. 54-59.

[50] N.K. Giang, M. Ha, and D. Kim," SCoAP: An Integration of CoAP protocol with web-based application," *IEEE Global Communications Conf.* Atlanta, GA, Dec. 2013, pp. 2648-2653.

[51] K. Govindan and A.P. Azad," En-to-End Service Assurance in IoT MQTT-SN," *IEEE 12th*

*Annual Consumer Communications and Networking Conf.* Las Vegas, NV, Jan. 2015, pp. 290-296.

[52] B. Bhargava, , C. Farkas, , L. Lilien, , and F. Makedon. Trust, Privacy, and Security: Summary of a Workshop Breakout Session, the National Science Foundation Information and Data Management (IDM) Workshop held in Seattle, Washington. Sep. 14–16, 2003. Technical Report 2003-34. Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University. Last access Apr. 3, 2015. Available at: http://www.cerias.purdue.edu/tools_and_resources /bibtex_archive/archive/2003-34.pdf.

[53] L. Buttyan, and J. P. Hubaux,“ Privacy protection,” *in Security and cooperation in wireless networks: Thwarting malicious and selfish behavior in the age of ubiquitous computing*. New York: Cambridge University Press, 2008, pp. 237-254.

[54] J.L. H-Ramos, J.B. Bernabe´, A.F. Skarmeta,“Towards Privacy-preserving Data Sharing in Smart Environments”, *IEEE 8th Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing*, Birmingham, July 2014, pp. 334-339.

[55] M. Sain, P. Kumar, and H. J. Lee,“Secure Authentication and Communication in Ubiquitous Healthcare Middleware”, *IEEE 13th Int. Conf., Advanced Communication Technology (ICACT)*, Seoul , Feb. 2011, pp.173-178.

[56] M.P. Lawton, “Aging and performance of home tasks Human Factors,” 1990, pp. 527-536.

[57] Q. Zhang, M. Karunanithi, R. Rana, and J. Liu,” Determination of Activates of Daily Living of Independent Living Older People Using Environmentally Placed Sensors,” *IEEE 35TH Annual Int. Conf. on Engineering in Medicine and Biology Society*, Osaka, July 2013, pp. 7044-7047.

[58] D. Seidel , N. Crilly, F. E. Matthews, C. Jagger, C. Brayne, and P. J. Clarkson,“Patterns of functional loss among older people: A prospective analysis,” *Human Factors*, pp. 669-680.

[59] M. Morris, J. Lundell. E. Dishman, and B. Needham,“New Perspectives on Ubiquitous Computing from Ethnographic Study of Elders with Cognitive Decline” *Proc. Ubiquitous Computing5TH Int. Conf.* Seattle, WA, Oct. 2003, pp. 227-242.

[60] Ambient Assisted Living Communications. Last access Apr. 16, 2015. Available online: http://www.comsoc.org/files/Publications/Magazines/ci/cfp/cfpcommag0115a.html .

[61] Logbook app. Last access May 5, 2015. Available on: http://www.ihealthlabs.com/glucometer/wireless-smart-gluco-monitoring-system/.

[62] L. Yang, Y. Ge, W. Li, W. Rao, and W. Shen,” A Home Mobile Healthcare System for Wheelchair Users,” *IEEE 18th int. connf. on CSCWD*, Hsinchu, May 2104, pp. 609-614.

[63] Beclose app. Last access May 5, 2015. Available on: http//beclose.com/press-070912.aspx.

[64] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic,” ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring,” Department of Computer Science, University of Virginia; Charlottesville, VA, USA: 2006. Technical Report, 2006.

[65] SmartPillow. Last access May 5, 2015. Available on: https://itunes.apple.com/us/app/pillow-smart-sleep-cycle-alarm/id878691772?mt=8.

[66] M. Kagawa, Y. Yoshida, M. Kubota, A. Kurita, and T. Matsui,” Non-contact heart rate monitoring method for elderly people In bed with random body motions using 24 GHz dual radars located beneath the mattress in clinical settings,” *J Med Eng Technol*. 2012, pp.344-350.

[67] I. Brown and A.A. Adams,” The Ethical Challenges of Ubiquitous Healthcare,” *Int. Rev. of Information Ethics*, vol. 8, Dec. 2007, pp.53–60.

[68] C. Li, A. Raghunathan, and N. K. Jha,"Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System," *IEEE 13th Int. Conf. on e-health Networking, Applications and Services*, Columbia, MO, June 2011, pp. 150-156.

[69] S.G. Miaou, C.M. Hsu, Y.S. Tsai, and H. M. Chao," A Secure Data Hiding Technique with Heterogeneous Data-Combining Capability or Electronic Patient Records," *Proc. of the 22nd Annual EMBS Int. Conf.*, vol. 1, Chicago IL, July 2000, pp. 280-283.

[70] B. Copigneaux," Semi-Autonomous, Context-aware, agent using behavior modeling and reputation systems to authorize data operation in the Internet of things," *IEEE World forum on Internet of Things (WF-IoT)*, Seoul, Mar. 2014, pp.411-416.

[71] A. Tajer, S. Kar, H.V. Poor, and S. Cui," Distributed Joint Cyber Attack Detection and State Recovery in Smart Grids," *IEEE Int. Conf. on Smart Grid Communications,* Brussels, Belgium, Oct. 2011, pp.202-207.

[72] D. Slamanig, and C. Stingle," Privacy Aspects of eHealth," *IEEE* 3rd Int. Conf. on Availability, Reliability and Security, Barcelona, Mar. 2008, pp. 1226-1233.

[73] X. Jia, Q. Feng, T. Fan, Q. Lei," RFID Technology and Its Applications in Internet of Things (IoT)," *IEEE 2nd Int. Conf. on Consumer Electronics, Communications and Networks (CECNet),* Yichang, Apr. 2012, pp. 1282-1285.

[74] J. Newmarch and P. Tam," Issues in Ownership of Internet Objects," *5th Int. Conf. on Electronic Commerce Research*, Montral, Canada, 2002.

[75] Bluetooth. Last access May 25, 2015. Available on: http://www.radio-electronics.com/info/wireless/bluetooth/bluetooth_overview.php.

[76] ZigBee. Last access May 25, 2015. Available on: http://www.radio-electronics.com/info/wireless/ZigBee/ZigBee.php.

[77] Wi-Fi. Last access May 25, 2015. Available on: http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php.

[78] L. Mainetti, L. Patrono and A. Vilei," Evalution of Wireless Sensor Networks Towards the Internet of Things: A survey," *IEEE 19th Int. Conf. on Software, Telecommunications and Computer Networks (SoftCOM),* Split, Sept. 2011, pp.1-6.

[79] United States, 2001–2007. Reprinted from " by J. Holmes,E. Powell-Griner, M. Lethbridge-Cejku, and K. Heyman, 2009, NCHS Data Brief, 20, p. 1. © National Center for Health Statistics 2009.

[80] Smart House is More Than a Business. Lass access Feb. 2, 2015. Available on: http://thesmarthousesolution.com/smarthouse-is-more-than-a-business/.

[81] X. Gue, X. Duan, H. Gao, A. Huang, and B. Jiao," An ECG Monitoring and Alarming System Based on Android Smart Phone," *Communications and Networks*, vol. 5, Sept. 2013, pp.584-589.

[82] A. Rajabzadeh, A.R. Manashty, and Z.F. Jahromi," A mobile Application for Smart House Remote Control System," *World Academy of Science, Engineering and Technology*, 2010, pp. 80-86.

[83] R.A. Ramlee, M.A. Othman, M.H. Leong, M.M. Ismail, and S.S.S. Ranjit," Smart Home System Using Android Application," *IEEE Int. Conf. of Information and Communication Technology*, Bandung, Mar. 2013, pp. 277-280.

[84] R. Hall, A. Rinaldo, and L. Wasserman," Differential Privacy for Functions and Functional Data," *J. of Machine Learning Research*, 2013, pp.703-727.

[85] J. Ren, Y. Li, and T. Li ," Routing-Based Source-Location Privacy in Wireless Sensor Networks," *IEEE Int. Conf. on Communications*, Dresden, June 2009, pp.1-5.

[86] Y. Jian, S. Chen, Z. Zhang, and L. Zhang,“ Protecting Recevier-Location Privacy in Wireless Sensor Networks,” *IEEE 26th Int. Conf. on Computer Communications*, Anchorage, AK, May 2007, pp.1955-1963.

[87] K. Mehta, D. Liu, and M. Wright,“ Location Privacy in Sensor Networks Against a Global Eavesdropper,” *IEEE Int. Conf. on Network Protocols*, Beijing, Oct. 2007, pp. 314-323.

[88] H.D. Nguyen, S. Gutta, and Q. Cheng,“ An Active Distributed Approach for Cyber Attack Detection,” *IEEE Conf. on Signals, Systems and Computers*, Pacific Grove, CA, Nov. 2010, pp. 1540-1544.

[89] S. Misra, P.V. Krishna, H. Agarwal, A. Saxena, and M.S. Obaidat,” A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things,” *IEEE 4th Int. Conf. on Cyber, Physical and Social Computing*, Dalian, Oct. 2011, pp. 114-122.

[90] I. Alqassem, and D. Svetinovic,” A taxonomy of security and privacy requirements for the Internet of Things (IoT),” *IEEE Int. Conf. on Industrial Engineering and Engineering Management (IEEM)*, Bandar Sunway, Dec. 2014, pp. 1244-1248.

[91] S. Chun, J. Jung, X. Jin, G. Chi, and K. H. Lee,” Poster Abstract: Semantically Enriched Object Identification for Internet of Things,” *IEEE Int. Conf. on Distributed Computing in Sensor Systems*, Marina Del Rey, CA, May 2014, pp.141-142.

[92] A. B. Spantzel, A. Squicciarini, and E. Bertino,” Trust negotiation in identity management,” *IEEE Security and Privacy*, vol. 5(2), Mar. 2007, pp. 55–63.

[93] W. Zhao, C. Wang, and Y. Nakahira, “Medical Application On IoT,” *Int. Conf. on Computer Theory and Applications (ICCTA)*, 2011, pp. 660-665.

[94] K. Sonar and H. Upadhyay,“ A Survey: DDOS Attack on Internet of Things,” *Int. J. of Engineering Research and Development*, India, 2014, pp. 58-63.

[95] M.L. Messai,“ Classification of Attacks in Wireless Sensor Networks,” *Int. Congress on Telecommunication and Application*, Algeria, 2014, pp. 23-24.

[96] X. Nie and X. Zhong,“ Security the Internet of Things Based on RFID: Issues and Current Countermeasures,” *Proc. of the 2nd Int. Conf. on Computer Science and Electronics Engineering (ICCSEE),* Paris, 2013, pp. 1181-1184.

[97] B. Khoo, “ RFID as a Enabler of the Internet of Things: Issues of Security and Privacy”, *IEEE 4th Int. Conf. on Cyber, Physical and Social Computing*, Dalian, Oct. 2011, pp. 709-712.

[98] X. Jia, Q. Feng, T. Fan, and Q. Lei,“ RFID Technology and Its Applications in Internet of Things (IOT)”, *IEEE 2nd Int. Conf. on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, China, Apr. 2012, pp. 1282 – 1285.

[99] D. He and S. Zeadally,” An Analysis of RFID Authentication Schemes for Internet of Thing in Healthcare Environment Using Elliptic Curve Cryptography*,” IEEE, Internet of Things J.*, Sep. 2014, pp. 72-83.

[100] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi and G. Marrocco,” RFID technology for IoT-based personal healthcare in smart spaces,” *IEEE Internet Things J.*, vol. 1(2), Mar. 2014, pp.144 -152.

[101] M. Tharani,” Integrating Wireless Sensor Networks into Internet of Things for Security,” *Int. J. of Adv. Research in CS. and Management Studies*, vol. 1(2), Jan. 2014, pp. 485-490.

[102] F. Li and P. Xiong, ” Prctical Secure Communication for Integrating Wireless Sensor Networks into the Internet of Things,” *IEEE Sensors J.,* vol. 13(10), June 2013, pp. 3677-3684.

[103] L. jing, Y. Xiao, and C.L.P. Chen,” Authentication and Access Control in the Internet of Things,” *IEEE 32nd Int. Conf. on Distributed Computing Systems Workshops*, Macau,

China, June 2012; pp. 588–592.

[104] L. Venkatraman and D. P. Agrawal,"A novel authentication scheme for ad hoc networks," *IEEE Wireless Communications and Networking Conf.*, vol. 3, Chicago, IL, Sept. 2000, pp. 1268–1273.

[105] T. Suen and A. Yasinsac," Ad hoc network security: Peer identification and authentication using signal properties," *In Proceedings from the 6th Annual IEEE SMC Information Assurance Workshop*, June 2005, pp. 432–433.

[106] O. Said," Development of an Innovative Internet of Things Security System," *Int. J. of Computer Science issues*, vol. 10, Nov. 2013, pp. 155-161.

[107] M.K. Choi, R J. Robles, C. H. Hong, and T. H. Kim," Wireless Network Security: Vulnerabilities, Threats and Countermeasures," *Int. J. of Multimedia and Ubiquitous Engineering*, vol. 3, July 2008, pp.77-86.

[108] Z.C. Dai, B.W. Wang, and P. Li," Wireless secure Communication Systems Design Based on Chaotic Synchronization, " *IEEE Int. Conf. on Communication Technology*, Guilin, Nov. 2006, pp. 1-4.

[109] Z. Li, J. Fu, W. Fan, and R. Long, " A security Information Transmission Scheme for Internet of Things," *IEEE 4th Int. Conf. on Emerging Intelligent Data and Web Technologies*, Xi'an, Sept. 2013, pp. 459-465.

[110] Y. Liu, X. Gong, and C. Xing," A Novel trust-Based Secure Data Aggregation for Internet of Things," *IEEE 9th Int. Conf. on Computer Science and Education*, Vancouver, Aug. 2014, pp. 435-439.

[111] S. Kalyan, R. Vignesh, U.H. Thakkar, and T.A. Macriga," MISTIKOS-Secure Data Transmission in Wireless Networks," *IEEE Students' Conf. on Electrical, Electronics and Computer Science*, Bhopal, Mar. 2012, pp. 1-4.

[112] C. Huth, J. Zibusahka, P. Duplys, and T. Guneysu," Securing Systems on the Internet of Things via Physical Properties of Devices and Communications," *IEEE 9th Int. Systems Conf.*, Vancouver, BC, Apr. 2015, pp. 8-13.

[113] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle," Delegation-Based Authentication and Authorization for IP-Based Internet of Things," *IEEE 11th Annual Int. Conf. on Sensing, Communication, and Networking*, Singapore, July 2014, pp. 284-292.

[114] V. Karagiannis, P. Chatzimisios, F. V. Gallego, and J. A. Zarate," A Survey on Application Layer Protocols for the Internet of Things," *Trans. on IoT and Cloud Computing*, 2015, pp. 1-10.

[115] J. Granjal, E. Monteiro, and J. Silva," Security of the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE, Communications Surveys and Tutorials*, vol. PP, Jan. 2015, pp. 1.

[116] T. Kothmayr, C. Schimitt, W. Hu, and M. Bruning, "A DTLS Based End-To-End Security Architecture for the Internet of Things with Two-way Authentication, " 2012: Available on: http://kothmayr.net/wp-content/papercite-data/pdf/kothmayr2012dtls.pdf

[117] Y.F. Gomes, D.F.S. Santos, H.O. Almeida, and A. Perkusich, " Integrating MQTT and IS/IEEE 11073 for Health Information Sharing in the Internet of Things," *IEEE Int. Conf. on Consumer Electronics*, Las Vegas, NV, Jan. 2015, pp. 200-201.

[118] M. Collina, M. Bartolucci, A.V. Coralli, G.E. Corazza," Internet of Things Application Layer Protocol Analysis over Error and Delay Prone Links," *IEEE Advanced Satellite Multimedia System Conf. and the 13th Signal Processing for Space Communications Workshop*, Livorno, Sept. 2014, pp. 398-404.

[119] M. Palattella, N. Accettura, X. Vilajosana, et al.," Standardized Protocol Stack for the

Internet of (Important) Things," *IEEE Communications Surveys & Tutorials*, vol. 15, July 2013, pp.1389-1406.

[120] W. Alcorna," Cross-Site Scripting Viruses and Worms – a New Attack Vector," *J. of Network Security*, Elsevier, July 2006, pp. 7-8.

[121] M. Howard and D. LeBlanc," Writing secure code," Ed. 2nd, Microsoft Press: Redmond, Dec. 2003.

[122] R. Wang, X. Jia, Q. Li, and S. Zhang," Machine Learning Based Cross-Site Scripting Detection in Online Social Network," *IEEE 6th Int. Symp on Cyberspace Safety and Security*, Paris, Aug. 2014, pp. 823-826.

[123] I. Yusof and A.S.K Pathan," Prevent Persistent Cross-Site Scripting (XSS) attack by Applying Pattern Filtering approach," *IEEE 5th Int. Conf. on Information and Communication Technology for the Muslim World*, Kuching, Nov. 2014, pp. 1-6.

[124] M.S. Siddiqui and d. Verma," Cross Site Requst Forgery: A Common Web Application Weakness," *IEEE 3rd Int. Conf. on Commnication Software and Networks*, Xi'an, May 2011, pp. 538-543.

[125] J. Blatz," CSRF: Attack and Defense," Last access June 7, 2015. Available on: http://www.mcafee.com/us/resources/white-papers/wp-csrf-attack-defense.pdf,

[126] J. You and F. Guo," Improved CSRFGuard for CSRF Attacks Defense on Java EE Platform," *IEEE 9th Int. Conf. on Computer science and Education*, Vancouver, BC Aug. 2014, pp. 1115-1120.

[127] Y. Yan, S. Zhengyuan, and D. Zucheng," The Database Protection System Against SQL Attacks, " *IEEE 3rd Int. Conf. on Computer Research and Development*, vol. 3, Shanghai, Mar. 2011, pp.99-102.

[128] How to Prevent SQL Injection Attacks. Last access June 7, 2015. Available on: http://www.esecurityplanet.com/hackers/how-to-prevent-sql-injection-attacks.html,

[129] N. Lambert and K.S. Lin," Use of Query Tokenization to Detect and Prevent SQL Injection Attacks," *IEEE, 3rd Int. Conf. on Computer Science and Information Technology*, vol. 2, Chengdu, July 2010, pp. 438-440.

[130] C. Doukas, and I. Maglogiannis," Bringing IoT and Cloud Computing towards Pervasive Healthcare," IEEE, 6th Int. Conf. on Innovative Mobil and Internet Services in Ubiquitous Computing (IMIS), Palermo, July 2012, pp.922-926.

[131] J. Cubo, A. Nieto, and E. Pimentel," A Cloud-Based Internet of Things Platform for Ambient Assisted Living," *Sensors J.*, vol. 14 (8), Aug. 2014, pp. 14070-14105.

[132] M.A. Zardari, L.T. Jung, and N. Zakaria," K-NN Classifier for Data Confidentiality in cloud computing," *IEEE Int. Conf. on Computer and Information Sciences*, Kuala Lumpur, June 2014, pp. 1-6.

[133] Q. Shen, X. Yang, X.Yu, P. Sun, Y.Yang, and Z. Wu," Towards Data Isolation and Collaboration in Cloud Storage", *IEEE Asia-Pacific Services Computing Conf.*, Jeju Island, Dec. 2011, pp. 139-146.

[134] M. Jebalia, A.B. Letaifa, M. Hamdi, S. Tabbane," A Revocation Game Model for Secure Cloud Storage," *IEEE Int. Conf. on High Performance Computing and Simulation*, Bologna, July 2014, pp. 1016-1017.

[135] L. Zhou, V. Varadharajan, and M. Hitchens," Integrating Trust with Cryptographic Role-Based Access Control for Secure Data Storage," *IEEE 12th Int. Conf. on Trust, Security and Privacy in Computing and Communications*, Melbourne, VIC, July 2013, pp. 560-569.

[136] L. Zhang, C. We, Z. Li, C. Gue, M. Chen, and F.C.M Lau," Moving Big Data to The Cloud: An Online Cost-Minimizing Approach," *IEEE J. on Selected Areas in*

*Communications*, vol. 31, Dec. 2013, pp. 2710-2721.

[137] A. Mxoli, M. Gerber, and N. M. Phipps," Information security risk measures for Cloud-Based Personal Heath Records," *IEEE Int. Conf. on Information Society*, London, Nov. 2014, pp. 187-193.

[138] S. Alshehri, S.P. Radziszowski, R.K. Raj," Secure Access foe Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption," *IEEE 28th Int. Conf. on Data Engineering Workshops*, Arlington, VA, Apr. 2012, pp. 143-146.

[139] G. Garkoti, S.K. Peddoju, and R. Balasubramanian," Detection of Insider Attacks in Cloud Based e-Healthcare Environment," *IEEE Int. Conf. on Information Technology*, Bhubaneswar, Dec. 2014, pp. 195-200.

[140] J.A. Patal, and P. Sharma," Big Data for Better Health Planning," *IEEE Int. Conf. on Advances in Engineering and Technology Research*, Unnao, Aug. 2014, pp. 1-5.

[141] T. W. Kim, K.H. Park, S.H. Yi, and H.C. Kim," A Big Data Framework for u-Healthcare Systems Utilizing Vital Signs, " *IEEE Int. Symposium on Computer, Consumer, and Control*, Taichung, June 2014, pp. 494-497.

[142] Structured Data in a Big Data Environment. Last access June 11, 2015. Available on: http://www.dummies.com/how-to/content/structured-data-in-a-big-data-environment.html.

[143]Unstructured Data. Last access June 11, 2015. Available on: http://www.webopedia.com/TERM/U/unstructured_data.html,

[144] M.R. Islam and M.E Islam," An approach to Provide Security to Unstructured Big Data," *IEEE Int. Conf. on Software, Knowledge, Information Management and Applications*, Dhaka, Dec. 2014, pp. 1-5.

[145] J.S. Khan, V. Aulakh, and A. Bosworth," What It Takes: Characteristics of the Ideal Personal Health Record," *Health Aff (Millwood),* vol. 28(2), pp. 369-376.

[146] S. Kolozali, M.B. Edo, D. Puschmann, F. Gans, and P. Barnaghi," A knowledge-Based Approach for Real-Time IoT Data Stream Annotation and Processing," *IEEE Int. Conf. on Internet of Things*, Taipei, Sept. 2014, pp. 215-222.

[147] X. Qi, A.S. Ross, e. Crooke, and et al.," Real-time data processing and visualization of a hydrocarbon sensor network for hydrocarbon environmental monitoring," *IEEE OCEANS*, Taipei, Apr. 2014, pp.1-4.

[148] M. Rosu and S. Pasca," A WBAN-ECG Approach for Real-Time Long-Term Monitoring," *IEEE 8th Int. Symposium on Advanced Topics in Electrical Engineering*, Bucharest, May 2013, pp.1-6.

[149] C.Y. Tsai," A Fast Dynamic Range Compression Format with a Local Contrast Preservation and Its Application to Real-Time Video Enhancement," *IEEE Trans. on Multimedia*, vol. 14, Mar. 2012, pp. 1140-1152.

[150] P. Agrawal, D. Kifer, and C. Olston," Scheduling shared scans of large data files," *Proceedings of the VLDB*, vol. 1, Aug. 2008, pp. 958-969.

[151] I. Moschakis and H. Karatza," Evaluation of gang scheduling performance and cost in a cloud computing system," *The J. of Supercomputing*, vol. 59, Feb. 2012, pp. 975-992.

[152] M. Isard, V. Prabhakaran, J. Currey, U. Wieder, K. Talwar, and A. Gold- berg, "Quincy: fair scheduling for distributed computing clusters," *In Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles*, 2009, pp. 1-20.

[153] C.H. Liu, F.Q. Lin, and et al.," Secure PHR Access Contorl Scheme for Healthcare Application Cloud," *IEEE 42nd Int. Conf. on Parallel Processing*, Lyon, Oct. 2013, pp. 1067-1076.

[154] Understanding The Cloud Computing Stack SaaS, PaaS, IaaS. Last access June 16, 2015. Availableon:http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf.

[155] Wireless Communication for IoT. Last access June 16, 2015. Available on: http://www.ti.com.cn/cn/lit/wp/swry010/swry010.pdf.

[156]M2M Connectivity. Last access June 16, 2015. Available on: http://blog.m2mconnectivity.com.au/category/internet-of-things/,

[157] I.E Bouabidi, I.Daly, and F. Zarai, " Secure Handoff Protocol in 3GPP LTE Networks," *IEEE 3rd Int. Conf. on Communications and Networking*, Hammamet, Mar. 2012, pp.1-6.

[158] H.R. Hussen, G.A. Tizazu, M. Ting, Taekkyeun Lee," SAKES: Secure Authentication and key establishment Scheme for M2M Communication in the IP-Based Wireless Sensor Network (6LoWPAN)," *IEEE 5th Int. Conf. on Ubiquitous and Future Networks*, Da Nang, July 2013, pp. 246-251.

[159] P.K. Wali and D. Das," A Novel Access Scheme for IoT Communications in LTE-Advanced Network," *IEEE Int. Conf. on Advanced Networks and Telecommunications Systems*, New Delhi, India, Dec. 2014, pp.1-6.

[160] Y. L. Huang, F. Y. Leu, J. C. Liu, L.J. Lo, W.C.-C. Chu," A Secure Wireless Communication System Integration PRNG and Diffie-Hellman PKDS by Using a Data Connection Core, "*IEEE 8th Int. Conf. on Wireless Computing, Communication and Applications*, Compiegne, Oct. 2013, pp. 360-365.

[161] Y.L. Huang, F.Y. Leu, Y.K. Sun, C.C. Chu, and C.T. Yang," A Secure Wireless Communication System by Integration RSA and Diffie-Hellman PKDS in 4G Environment and an Intelligent Protection-Key Chain with a Data Connection Core," *IEEE Int. Conf. on Industrial Electronics*, Taipei, Taiwan, May 2013, pp. 1-6.

[162] Designing the Internet of Things. Last access June 16, 2015. Available on: http://micrium.com/iot/internet-protocols/.

[163] H. Zhang and T. Zhang," Short Paper: 'A Peer to Peer Security Protocol for the Internet of Things': Secure Communication for the Sensiblethings Platform," *IEEE 18th Int. Conf. on Intelligence in Next Generation Networks*, Paris, Feb. 2015, pp. 154-156.

[164] D. Berbecaru," On Measuring SSL-Based Secure Data Transfer with Handheld Devices, " *IEEE 2nd Int. Symposium on Wireless Communication Systems*, Siena, Sept. 2005, pp.409-413.

[165] R.K. Jha, and F. Khurshid," Performance Analysis of Enhanced Secure Socket Layer Protocol," *IEEE Int. Conf. on Communication and Network Technologies*, Sivakasi, Dec. 2014, pp. 319-323.

[166] R. Valia, and Y. Al-Salqan," Secure Workflow Environment," *IEEE 6th Workshop on Enabling Technologies Infrastructure for Collaborative Enterprises*, Cambridge, MA, June 1997, pp. 269-276.

[167] F.V. Meca, J.H. Ziegeladorf, and et al.," HIP Security Architecture for the IP-Based Internet of Things," *IEEE 27th Int. Conf. on Advanced Information Networking and Applications Workshops*, Barcelona, Spain, Mar. 2013, pp.1331-1336.

[168] Q. Li and W. Trappe," Reducing Delay and enhancing DoS Resistance in Multicast Authentication Through Multigame Security," *IEEE Trans. on Information Forensics and Security*, vol. 1, June 2006, pp. 190-204.

[169] C.M. Yu, Y.T. Tsou, C.S. Lu, and S.Y. Kuo," Constrained Function-Based Message Authentication for Sensor Networks," *IEEE Trans. on Information Forensics and Security*, vol. 6, Jan. 2011, pp.407-425.

[170] E. Rescorla and N. Modadugu," Datagram Transport Layer Security Version 1.2," RFC 6347, 2012. Last access June 1, 2015. Available on: http://www.ietf.org/rfc6347.txt ,

[171] N. Accettura, L.A. Grieco, G. Boggia, and P. Camarda," Peformance Analysis of the RPL Routing Protocol," *IEEE Int. Conf. on Mechatronics,* Istanbul, 2011, pp.767-772.

[172] A. Le, J. Loo, Y. Luo, and A. Lasebae," Specification-based IDS for securing RPL from toplogy attacks," *IEEE IFIP Wireless Days*, Niagara Falls, ON, Oct. 2011, pp. 1-3.

[173] S. Raza, S. Duquennoy, T. Chung et al," Securing Communication in 6LoWPAN with Compressed IPsec," *IEEE Int. Conf. on Distributed Computing in Sensor Systems and Workshops*, Barcelona, Spain, June 2011, pp.1-8.

[174] S. Goswami, S. Misra, G. Teneja, A. Mukherjee," Securing intra-connection in 6LoWPAN: A PKI integrated Scheme," IEEE Int. Conf. on Advanced Networks and Telecommunications Systems, New Delhi, India, Dec. 2014, pp.1-5.

[175] K. Devadiga, " IEEE 802.15.4 and The Internet of Things. Last access June 16, 2015. Available on: https://wiki.aalto.fi/download/attachments/59704179/devadiga-802-15-4-and-the-iot.pdf?version=1,

[176] Y. Xiao, S. Sethi, H.H. Chen, and B. Sun," Security Services and Enhancements in the IEEE 802.15.4 Wireless Sensor Networks", *Proc. IEEE Global Communication Conf.*, vol. 3, Dec. 2005, pp. 1796-1800.

[177] R. Daidone, G. Dini, and M. Tiloca," On Experimentally Evaluating the Impact of Security on IEEE 802.15.4 networks," *IEEE Int. Conf. on Distributed Computing in Sensor Systems and Workshops*, Barcelona, Spain, June 2011, pp. 1-6.

[178] Ekta and R. Kaur," Light Fidelity (Li-Fi)- A Comprehensive Study," *Int. J. of Computer Science ad Mobil Computing*, vol. 3 (4), Apr. 2014, pp. 475-481.

[179] B.R. Vatsala and V.R.C.," Internet of Things: Usage of Li-Fi and Need for Flow Control Protocol," *Int. J. on Recent and Innovation Trends in Computing and Communication*, vol. 2 (8), Aug. 2014, pp. 2510-2513.

[180] N.S. Poojashree, P. Haripriya, M.S. Muneshwara, G.N. Anil," Li-Fi Overview and Implementation in Medical Field," *Int. J. on Recent and Innovation Trends in Computing and Communication*, vol. 2(2), Feb. 2014, pp. 288-291.

[181] F. Bonomi, R. Militi, J. Zhu, and S. Addepalli," Fog Computing and Its Role in The Internet of Things," *In Processing of the First Edition of the MCC Workshop on Mobil Cloud Computing*, Helsinki, Finland, Aug. 2012, pp. 13-16.

[182] Wi-Fi repeater. Last access July 9, 2015. Available on: http://www.alibaba.com/product-detail/best-selling-products-10-km-hotspot_60237115644.html?spm=a2700.7724857.35.1.scVBLi.

[183] R. Flickenger, S. Okay, E. Pietrosemoli, and et al. ," Very Long Distance WiFi Networks," ACM, NSDR, Aug. 2008, Seattle, WA, pp. 1-5.

[184] LTE and The IoT-M2M Environment. Last access Aug. 4, 2015. Available on: http://www.telit.com/fileadmin/user_upload/media/telit_lte-m2m_wp.pdf.

[185] Frequency Bands Optimal for the Internet of Things. Last access Oct. 1, 2015. Available on: https://iotee.wordpress.com/2015/03/18/frequency-bands-optimal-for-the-internet-of-things/

[186] Older Adults' Preferences for and Acceptance of Robot Assistance for Everyday Living Tasks. Last access Feb. 2, 2015. Available on: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4182920/

[187] Leonhardt, S.," Personal Healthcare Devices," *Springer, Hardware Technology Drivers of Ambient Intelligence*, Dordrecht, Netherlands 2006, pp.349-370.