List of Tables

List of Figures

Chapter 1

Introduction

Internet of Things (IoT) does not have a unique definition. However, a broad interpretation of IoT is that it provides any service over the traditional Internet by enabling human-to-thing, thing-to-thing, or thing-to-things communications [3]. IoT represents the interconnection of heterogeneous entities, where the term entity refers to a human, sensor, or potentially anything that may request/provide a service [4].

The emergence of the IoT paradigm is one of the most spectacular phenomena of the last decade. The development of various communication protocols, along with the miniaturization of transceivers, provides the opportunity to transform an isolated device into a communicating thing. Moreover, computing power, energy capacity, and storage capabilities of small computing or sensing devices have significantly improved while their sizes have decreased drastically. Boosted by the rapid development of IoT-enabled systems in recent years, Internet-connected wearable medical sensors (WMSs) are garnering an ever-increasing attention in both academic and industrial research. Although WMSs were initially developed to enable low-cost solutions for continuous health monitoring, the applications of WMS-based systems now range far beyond health care. As discussed later in this chapter, several research efforts have

proposed the use of such systems in diverse application domains, e.g., education, human-computer interaction, and security.

As a side effect of rapid advances in the design and development of IoT-enabled systems, the number of potential threats and possible attacks against security of such systems, *in particular WMS-based systems that rely on resource-constrained sensors*, and privacy of their users has grown drastically. Thus, security threats and common privacy concerns need to be studied and addressed in depth. This would greatly simplify the development of secure smart devices that enable a plethora of services for human beings, ranging from building automation to health monitoring, in which very different things, e.g., temperature sensor, light sensor, and medical sensors, might interact with each other or with a human carrying a smart computing device, e.g., a smartphone, tablet, or laptop. This dissertation aims to explore and address different security/privacy issues associated with IoT-enabled systems with a special focus on WMS-based systems.

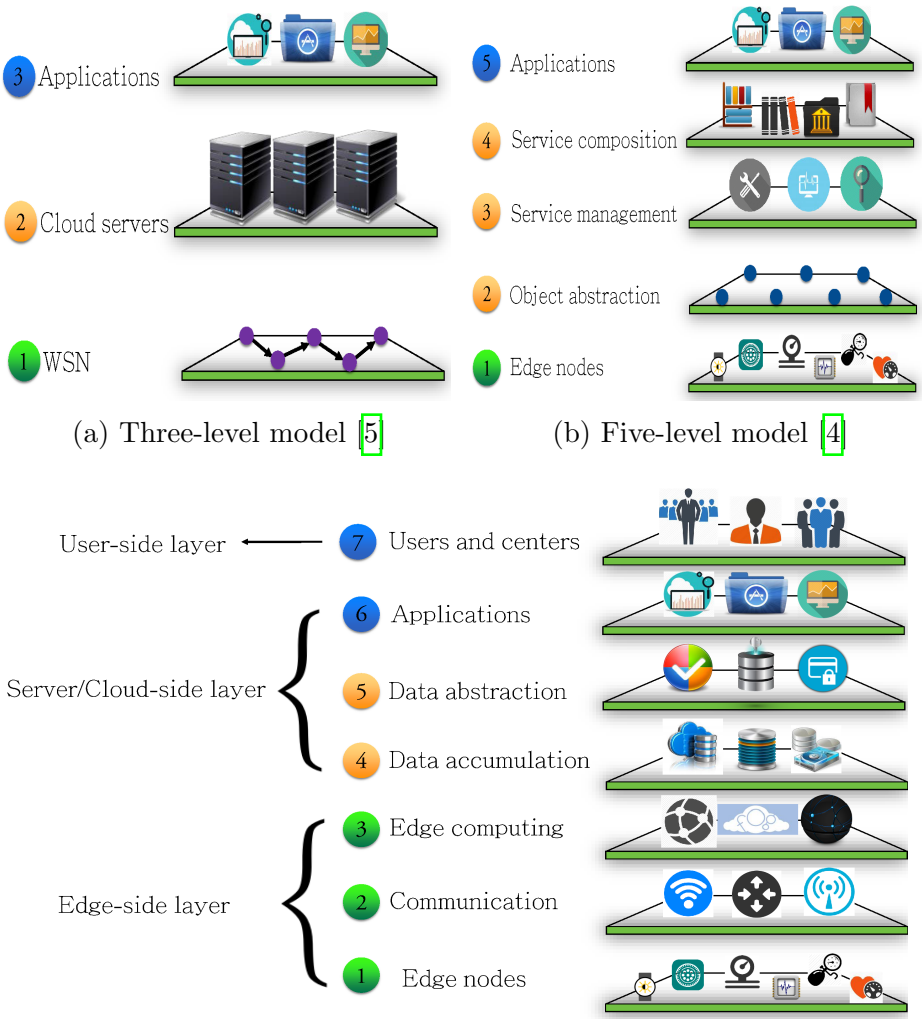
In the rest of this chapter, we first describe the IoT paradigm, and then discuss WMS-based systems.

1.1 The IoT paradigm

In this section, we first discuss different IoT reference models described in the literature. Then, we describe the scope of IoT applications. Thereafter, we explain what security means in the scope of IoT. Finally, we discuss who the attackers that target the IoT might be, and what motivations they might have.

1.1.1 IoT reference models

Three IoT reference models have been widely discussed in academic and industrial publications. Fig. 1.1 shows these models and their different levels. The three-level



(a) Three-level model [5] (b) Five-level model [4]

(c) CISCO's seven-level model [6]

Figure 1.1: Three IoT reference models

model [5] is among the first reference models proposed for IoT. It depicts IoT as an extended version of wireless sensor networks (WSNs). In fact, it models IoT as a combination of WSNs and cloud servers, which offer different services to the user. The five-level model [4] is an alternative that has been proposed to facilitate interactions among different sections of an enterprise by decomposing complex systems into simplified applications consisting of an ecosystem of simpler and well-defined components [4]. In 2014, CISCO suggested a comprehensive extension to the traditional three-level and five-level models. CISCO's seven-level model has the potential to be

standardized and thus create a widely-accepted reference model for IoT [6]. In this model, data flow is usually bidirectional. However, the dominant direction of data flow depends on the application. For example, in a control system, data and commands travel from the top of the model (applications level) to the bottom (edge node level), whereas, in a monitoring scenario, the flow is from bottom to top.

In order to summarize IoT security attacks and their countermeasures in a level-by-level fashion, we use the CISCO reference model in Chapter 2. Next, we briefly describe each level of this model.

Level 1-Edge devices: The first level of this reference model typically consists of computing nodes, e.g., smart controllers, sensors, RFID readers, etc., and different versions of RFID tags. Data confidentiality and integrity must be taken into account from this level upwards.

Level 2-Communication: The communication level consists of all the components that enable transmission of information or commands: (i) communication between devices in the first level, (ii) communication between the components in the second level, and (iii) transmission of information between the first and third levels (edge computing level).

Level 3-Edge computing: Edge computing, also called fog computing, is the third level of the model in which simple data processing is initiated. This is essential for reducing the computation load in the higher level as well as providing a fast response. Most real-time applications need to perform computations as close to the edge of the network as possible. The amount of processing in this level depends on the computing power of the service providers, servers, and computing nodes. Typically, simple signal processing and learning algorithms are utilized here.

Level 4-Data accumulation: Most of the applications may not need instant data processing. This level enables conversion of data in motion to data at rest, i.e., it allows us to store the data for future analysis or to share with high-level computing

servers. The main tasks of this level are converting the format from network packets to database tables, reducing data through filtering and selective storing, and determining whether the data are of interest to higher levels.

Level 5-Data abstraction: This level provides the opportunity to render and store data such that further processing becomes simpler or more efficient. The common tasks of entities at this level include normalization, de-normalization, indexing and consolidating data into one place, and providing access to multiple data stores.

Level 6-Applications: The application level provides information interpretation, where software cooperates with data accumulation and data abstraction levels. The applications of IoT are numerous and may vary significantly across markets and industrial needs.

Level 7-Users and centers: The highest level of the IoT is where the users are. Users make use of the applications and their analytical data.

1.1.2 Scope of applications

In this section, we first discuss the scope of IoT applications.

Smart homes and buildings, electronic health aids, and smarter vehicles are just some of the IoT instances [7–9]. Each smart device may provide several services to enable a more intuitive environment. However, we are not even close to exhausting the possible uses of IoT. IoT provides an opportunity to combine sensing, communication, networking, authentication, identification, and computing, and enables numerous services upon request such that access to the information of any smart thing is possible at any time. Fig. 1.2 demonstrates various applications of the IoT, which we describe next:

1. Smart vehicles: Smart vehicles have started to revolutionize traditional transportation. Small IoT-based systems can enable remote locking/unlocking of cars, download of roadmaps, and access to traffic information. Moreover, Internet-

Figure 1.2: Different applications of IoT [1]

connected cars provide significant protection against theft.

2. Smart buildings: Smart homes and buildings enable effective energy management. For example, smart thermostats, which have embedded sensors and data analysis algorithms, can control air conditioners based on user preferences and habits. Moreover, smart controllers can adjust lighting based on user's usage. Several household items, e.g., refrigerators, televisions, and security systems, could have their own processing units, and provide over-the-Internet services. These smart devices greatly enhance users' convenience. Remotely-controllable devices receive commands from users to perform actions that have an effect on the surrounding environment. Thus, attacks on these devices may lead to physical consequences [10].

3. Health monitoring: Recent advances in biomedical sensing and signal processing, low-power devices, and wireless communication have revolutionized health care. IoT-based long-term personal health monitoring and drug delivery systems, in which various physiological signals are captured, analyzed, and stored for future use,

provide a fundamentally new approach to health care [11]. Smart medical devices are already in use in fitness, diet, and health monitoring systems [12]. The future of IoT-based health care systems lies in designing personal health monitors that enable early detection of illnesses.

4. Energy management: Use of smart IoT-based systems, which integrate embedded sensors and actuation components, enables a proactive approach to optimizing energy consumption. In particular, power outlets, lamps, fridges, and smart televisions, which can be controlled remotely, are expected to share information with energy supply companies to optimize the energy consumption in smart homes. Moreover, such things allow the users to remotely control or manage them, and enable scheduling that can lead to a significant reduction in energy consumption.

5. Construction management: Monitoring and management of modern infrastructure, e.g., bridges, traffic lights, railway tracks, and buildings, are one of the key IoT applications [13]. IoT can be used for monitoring any sudden changes in structural conditions that can lead to safety and security risks. It can also enable construction and maintenance companies to share information about their plans. For example, a construction company can let GPS companies know its maintenance plans for the roads and, based on that, the smart GPS devices can choose an alternative route, which avoids the road under construction.

6. Environmental monitoring: The use of smart things with embedded sensors enables environmental monitoring as well as detection of emergency situations, e.g., a flood, which require a fast response. In addition, the quality of air and water can be examined by IoT-based devices. Moreover, humidity and temperature can be easily monitored [14].

7. Production and assembly line management: IoT-based smart systems allow rapid manufacturing of new products and an interactive response to demands by enabling communication between sensors and controlling/monitoring systems [15].

Moreover, intelligent management approaches that use real-time measurements can also enable energy optimization and safety management.

8. Food supply chain: The food supply chain model is fundamentally distributed and sophisticated. IoT can provide valuable information for managers of this chain. Although IoT is already in use within the supply management systems, its current benefits are limited. One of the most obvious and significant advantages of IoT in supply management is that it ensures security and safety of the products by utilizing IoT-based tracking [16]. These devices can raise a warning in case of a security breach at any unauthorized level of the supply management system.

1.1.3 Definition of security in the scope of IoT

Next, we define two of the most commonly-used terms in the scope of IoT: a secure thing and a security attack. When defining what a secure thing is, it is important to understand the characteristics that define security. Traditionally, security requirements are broken down into three main categories: (i) confidentiality, (ii) integrity, and (iii) availability, referred to as the CIA-triad. Confidentiality entails applying a set of rules to limit unauthorized access to certain information. It is crucial for IoT devices because they might handle critical personal information, e.g., medical records and prescription. For instance, an unauthorized access to personal health devices may reveal personal health information or even lead to life-threatening situations [17]. Integrity is also necessary for providing a reliable service. The device must ensure that the received commands and collected information are legitimate. An integrity compromise may lead to serious adverse consequences. For example, integrity attacks against medical devices, e.g., an insulin pump [18] or a pacemaker [19], may have life-threatening outcomes. IoT availability is essential for providing a fully-functioning Internet-connected environment. It ensures that devices are available for collecting data and prevents service interruptions.

Table 1.1: Security requirements

Requirement	Definition	Abbreviations
Confidentiality	Ensuring that only authorized users access the information	C
Integrity	Ensuring completeness, accuracy, and absence of unauthorized data manipulation	I
Availability	Ensuring that all system services are available, when requested by an authorized user	A
Accountability	An ability of a system to hold users responsible for their actions	AC
Auditability	An ability of a system to conduct persistent monitoring of all actions	AU
Trustworthiness	An ability of a system to verify identity and establish trust in a third party	TW
Non-repudiation	An ability of a system to confirm occurrence/ non-occurrence of an action	NR
Privacy	Ensuring that the system obeys privacy policies and enabling users to control their data	P

The insufficiency of the CIA-triad in the context of security has been addressed before [20–22]. Cherdantseva et al. [20] show that the CIA-triad does not address new threats that emerge in a collaborative security environment. They provide a comprehensive list of security requirements by analyzing and examining a variety of information, assurance, and security literature. This list is called the IAS-octave and is proposed as an extension to CIA-triad. Table 1.1 summarizes the security requirements in the IAS-octave, and provides their definitions and abbreviations. We define:

- *Secure thing*: A thing that meets all of the above-mentioned security requirements.
- *Security attack*: An attack that threatens at least one of the above-mentioned security requirements.

1.1.4 Potential attackers and their motivations

Next, we briefly discuss who the attackers that target the IoT might be, and what motivations they may have.

IoT-based systems may manage a huge amount of information and be used for services ranging from industrial management to health monitoring. This has made the IoT paradigm an interesting target for a multitude of attackers and adversaries, such as occasional hackers, cybercriminals, hacktivists, government, etc.

Potential attackers might be interested in stealing sensitive information, e.g., credit card numbers, location data, financial accounts' passwords, and health-related information, by hacking IoT devices. Moreover, they might try to compromise IoT components, e.g., edge nodes, to launch attacks against a third-party entity. Consider an intelligence agency that infects millions of IoT-based systems, e.g., remote monitoring systems, and smart devices, e.g., smart televisions. It can exploit the infected systems and devices to spy on a person of interest or to conduct an attack on a large scale. Also, hacktivists or those in opposition might be interested in attacking smart devices to launch protests against an organization.

1.2 WMS-based systems

Aging population and rapidly-rising costs of health care have triggered a lot of interest in WMSs. Traditionally, in-hospital monitoring devices, such as electrocardiogram (ECG) and electroencephalogram (EEG) monitors, have been used to sense and store raw medical data, with processing being performed later on another machine, e.g., an external computer [11, 23]. Several trends in communication, signal processing, machine learning, and biomedical sensing have converged to advance continuous health monitoring from a distant vision to the verge of reality. Foremost among these trends is the development of Internet-connected WMSs, which can non-invasively sense, col-

lect, and even process different types of body-related data, e.g., electrical, thermal, and optical signals generated by the human body.

WMSs enable proactive prevention and remote detection of health issues, thus with the potential to significantly reduce health care costs [24,25]. Since the introduction of the first wearable heart monitor in 1981 [26], numerous types of WMS-based systems have been proposed, ranging from simple accelerometer-based activity monitors [25,27] to complex sweat sensors [28]. WMS-based systems have also been developed for continuous long-term health monitoring [11,29].

In the last decade, with the pervasive use of Internet-connected WMSs, the scope of applications of WMS-based systems has extended far beyond health care. For example, such systems have targeted application domains as diverse as education, information security, and human-computer interaction (HCI). Park et al. [30] introduced a WMS-based teaching assistant system, called SmartKG. It collects, manages, and fuses data gathered by several wearable badges to prepare valuable feedback to the teacher. Barreto et al. [31] designed and implemented a human-computer interface, which uses EEG and electromyogram (EMG) signals gathered from the subject's head to control computer cursor movements.

Despite the emergence of numerous WMS-based systems in recent years, potential challenges associated with their design, development, and implementation are neither well-studied nor well-recognized. The rest of this section:

- provides a brief history of wearable computing devices and WMSs and discusses how their market is growing,
- explains in depth the scope of applications of WMS-based systems,
- describes the architecture of a typical WMS-based system and discusses constituent components, and the limitations of these components,

- suggests an inclusive list of desirable design goals and requirements that WMS-based systems should satisfy.

1.2.1 History and market growth

Wearable devices have a history that goes back longer than most people expect. The first truly wearable computer appeared in 1961, when Edward O. Thorpe and Claude Shannon created Roulette Predictor [32], a wearable computer that could be concealed in a shoe and accurately predict where the ball would land on a roulette circle. Integration of wearable sensors in wearable computing devices was done in 1981, when Polar Electro Company introduced the first wearable heart rate monitors for professional athletes [26]. After that, several companies were founded to offer various services based on WMSs. However, due to the immaturity of the sensing technology, implementation complexities, e.g., heat management, limitations of wearable sensors, e.g., small local storage, and security/privacy concerns, the majority of such companies experienced a difficult time commercializing their products, and as a result, went through bankruptcy [33].

Rapid advances in communication protocols and the miniaturization of transceivers in 1990s, along with the emergence of different WMSs in the early 2000s, transformed the market of wearable technologies. In the last decade, the rapidly-falling prices of WMSs and components used to implement WMS-based systems have changed the application landscape [34–36]. In addition, the rising market of personal smart devices, e.g., smartphones and tablets, that are powerful, ubiquitous, and less resource-limited relative to wearable sensors, has enabled a plethora of services, ranging from continuous health monitoring [11] to continuous user authentication [37]. The introduction of Apple's App Store for the iPhone and iPod Touch in July 2008, Google's Android Market (now called Google Play Store), and RIM's BlackBerry

App World in 2009, enabled easy distribution of third-party applications, further boosting the WMS industry [38, 39].

Global Wearable Sensors Market [40] recently published a report that includes information from 2011 to 2016. This report indicates that the introduction of smart watches from companies like Samsung, Sony, and Nike has given a significant boost to the wearable technology market. As of 2016, North America has the highest penetration of wearable sensors since Americans tend to be early adopters of new technologies. However, Asia is expected to show the highest growth rate in a few years due to the presence of developing countries like India and China [41]. A recently-published report provided by IHS Technology [42] forecasts that the number of WMSs will rise by 7× from 67 million units in 2013 to 466 million units in 2019. Another recent report by Business Insider [43] claims that 33 million wearable devices were sold in 2015 only for health monitoring. It forecasts that this number will reach 148 million by 2019. In the years after that, such usage is expected to explode further.

1.2.2 Scopes of applications

In this section, we describe various applications of WMS-based systems (a summary is shown in Fig. 1.3).

Health care

Rapid advances in WMS-based systems are transforming and revolutionizing health care. Medical WMS-based systems are of two main types: (i) health monitoring systems that monitor the patient to prevent the occurrence of a medical condition or detect a disease at an early stage, and (ii) medical automation systems, which offer continuous treatment or rehabilitation services. Next, we describe each type.

1. Health monitoring systems: Prevention and early detection of medical conditions are essential for promoting wellness. Unfortunately, conventional clinical di-

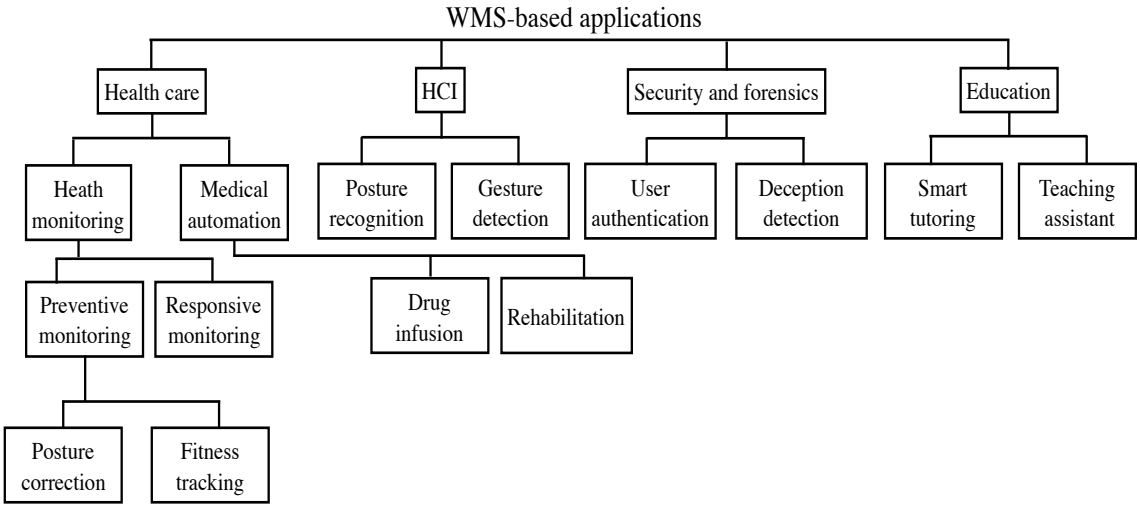


Figure 1.3: The scope of applications of WMS-based systems

agnostic practices commonly fail to detect health conditions in the early stages since diagnosis is typically performed after the emergence of major health symptoms, and previous medical data on the patient are often very sketchy. Furthermore, clinical practices are difficult to carry out in out-of-hospital environments.

In order to address the above-mentioned drawbacks of traditional clinical practices, several research studies have targeted WMS-based health monitoring systems. Such systems can be divided into two categories based on their main task: (i) preventive systems that aim to provide an approach to prevent diseases before the emergence of their symptoms, and (ii) responsive systems that attempt to detect health conditions at an early stage and provide health reports to the patient or the physician. Next, we describe each category.

Preventive systems: Preventive health monitoring systems provide real-time feedback to the user in an attempt to correct behaviors that might lead to adverse health conditions in the future. They promote healthy behaviors and lower the probability of serious illnesses by automatically detecting/predicting unhealthy activities and warning the user about them [44]. Posture correctors and fitness trackers are two of the most widely-known types of preventive health monitoring systems.

Posture corrector: A poor posture results in muscle tightening, shortening, or weakening, causing several health conditions, e.g., back pain and spinal deformity [45]. Posture correctors [46–48] monitor the user's movements and habits and offer real-time feedback upon the detection of any posture abnormality, e.g., slouching when sitting in front of a computer display. In fact, they help the user maintain a healthy posture while performing daily activities.

Fitness tracker: Such trackers are in widespread use and their market is rapidly growing. Although they may use different sensing technologies, they all have a common characteristic: they non-invasively measure some types of fitness-related parameters, e.g., calories burned, heart rate, number of steps taken [49], and even sleep patterns [50]. State-of-the-art fitness trackers play a significant role in the IoT paradigm by enabling object-to-object communication, transmission of user's data to the Cloud, and remote monitoring of user's activities [51]. For example, a fitness tracker, which can communicate with other objects, may be able to gather data from gymnasium equipment to support aspects of fitness progress awareness, such as shopping suggestions to support the user's fitness regime [52].

Responsive systems: Responsive health monitoring systems aim to detect medical conditions at an early stage by monitoring and analyzing various biomedical signals, e.g., heart rate, blood glucose, blood sugar, EEG, and ECG, over a long time period. For example, the CodeBlue project [53] examined the feasibility of using interconnected sensors for transmitting vital health signs to health care providers. Nia et al. [11] proposed an extremely energy-efficient personal health monitoring system based on eight biomedical sensors: (1) heart rate, (2) blood pressure, (3) oxygen saturation, (4) body temperature, (5) blood glucose, (6) accelerometer, (7) ECG, and (8) EEG. MobiHealth [54] offered an end-to-end mobile health platform for continuous health care monitoring.

2. Medical automation systems: Unlike health monitoring systems, medical automation systems enhance the user's quality of life after/during the emergence of health issues. They mitigate health issues or minimize disease symptoms by actively providing essential therapy. Based on their functionality, medical automation systems can be divided into two main categories: drug infusion and rehabilitating systems.

Drug infusion systems: Drug infusion systems enable safe injection of pharmaceutical compounds, e.g., nutrients and medications, into the body to achieve desired therapeutic effects. Automatic drug infusion systems control the drug release profile, absorption, and distribution to enhance the treatment efficacy and safety as well as patient convenience and compliance [55]. Insulin delivery systems are one of the most commonly-used types of drug infusion systems. They continuously monitor the patient's blood glucose level using wearable glucose sensing patches and inject a prescribed amount of insulin into the blood stream when necessary.

Rehabilitation systems: Such systems have attracted a lot of attention in the past two decades. They are currently used by patients after a major operation, sensory loss, stroke, severe accident, or brain injury [56]. They are also used to help patients who suffer from serious neurological conditions, e.g., Parkinson's disease or post-stroke condition [57]. Gait and/or motor abilities analysis is often used in rehabilitation in hospitals and health care centers [58].

An example of WMS-based rehabilitation system is Valedo [59], which is a medical back-training device developed by Hocoma AG to enhance patient compliance. It gathers trunk movements using two WMSs, transfers them to a game environment, and guides the patient through exercises targeted at low back pain therapy. Another example is Stroke Rehabilitation Exerciser [60] developed by Philips Research, which coaches the patient through a sequence of exercises for motor retraining. Salarian et al. [61] proposed a method for enhancing the gait of a patient with Parkinson's

disease. Hester et al. [62] proposed a WMS-based system to facilitate post-stroke rehabilitation.

HCI

In our daily conversations, the existence of common contexts, i.e., implicit information that characterizes the situation of a person or place that is relevant to the conversation, helps us convey ideas to each other and react appropriately. Unfortunately, the ability to share context-dependent ideas does not transfer well to humans interacting with machines. The design of WMS-based human-computer interfaces has notably improved the richness of communications in HCI [63]. In particular, various WMS-based gesture detection and emotion recognition systems have been proposed in the literature to enhance HCI.

1. Gesture detection systems: Several applications, such as sign-language recognition and remote control of electronic devices, need to respond to simple gestures made by humans. In the last decade, many WMS-based gesture recognition mechanisms have been developed to process sensory data collected by WMSs, e.g., magnetometer [64,65], accelerometer [25,27], and gyroscopes [66], to recognize user's gesture and enable gesture-aware HCI.

Although gestures from any part of the body can be used for interacting with a computing device, previous experimental research efforts [67] have demonstrated that finger-based gesture detection mechanisms are more successful in practice since their information entropy is much larger than that of interactions based on other human body parts. As a result, several research studies [66,68–70] have focused on developing algorithms to detect hand gestures in real-time. A promising example of WMS-based gesture detection systems is Pingu [66], a smart wearable ring that is capable of recognizing simple and tiny gestures from user's ring finger.

2. Emotion recognition systems: Wearable technology was first used to detect emotions/feelings by Picard et al. [71]. Since then, several researchers have used different sets of WMSs to detect different emotions/feelings, e.g., stress [72, 73], depression [74], and happiness [75]). However, we humans still cannot agree on how we define certain emotions, even though we are extremely good at expressing them. This fact has made emotion recognition a technically challenging field. However, it is becoming increasingly important in HCI studies as its advantages become more apparent.

Information Security and Forensics

Next, we discuss two well-known types of WMS-based systems developed in the domain of information security and forensics for deception detection and authentication.

1. Deception detection systems: The examination of the truthfulness of statements made by victims, suspects, and witnesses is of paramount importance in legal settings. Real-time WMS-based deception detection systems attempt to facilitate security screening and criminal investigation, and also augment human judgment [76]. They process sensory data collected by various types of WMSs (commonly heart rate, blood pressure, and accelerometers) to detect suspicious changes in the individual's mental state, e.g., a rapid increase in stress level, behavior, e.g., involuntary facial movements, and physiological signals, e.g., an increase in the heart rate. For example, PokerMetrics [77] is a lie detection system that processes heart rate, skin conductance, temperature, and body movements to find out when the user is bluffing during a poker tournament. FNIRS-based polygraph [78] is another fairly accurate lie detection system that processes data collected by a wearable near-infrared spectroscope.

2. Authentication systems: Authentication refers to the process of verifying a user's identity based on certain credentials [79]. A rapidly-growing body of literature on the usage of behaviometrics, i.e., measurable behavior such as frequency of

keystrokes, and biometrics, i.e., strongly-reliable biological traits such as EEG signals, for authentication has emerged in the last two decades [80–82].

Design of WMS-based authentication is an emerging research domain that is attracting increasing attention. Several research efforts have investigated the feasibility of using the data collected by WMSs as behaviometrics or biometrics. In particular, various research studies [83, 84] have demonstrated that the data collected by smart watches, e.g., acceleration, orientation, and magnetic field, can be used to distinguish users from each other. Furthermore, the use of EEG [85] and ECG [86] signals, as biomedical traits with high discriminatory power for authentication, has received widespread attention. Although EEG/ECG-based authentication systems have shown promising results, they have been unable to offer a convenient method for *continuous user authentication* for two reasons. First, the size/position requirements of the sensors that capture EEG/ECG signals significantly limit their applicability [86, 87]. Second, processing of EEG/ECG signals for authentication is resource-hungry [88]. A recently-proposed WMS-based authentication system, called CABA [37], has attempted to effectively address these drawbacks by using an ensemble of biomedical signals that can be continuously and non-invasively collected by WMSs.

Education

Next, we describe how technological advances in WMSs are transforming education by opening up new opportunities for employing smart tutoring and teaching assistant systems.

1. Smart tutoring: With the rapid development of online tutoring and exponential increase in the number of massive open online course websites, many research projects have been conducted on computer-based tutoring systems, which aim to select suitable instructional strategies based on the learner's reactions, mental conditions, emotional states, and feedback (see [89] for a survey). Moreover, there is a

strong motivation in the military community for designing adaptive computer-based tutoring systems to provide effective training in environments where human tutors are unavailable [90, 91]. WMS-based tutoring systems can recognize the user's emotional condition, level of understanding, physical state, and stress level by collecting and processing sensory data, e.g., user's heart rate and blood pressure. They can also predict learning outcomes, e.g., performance and skill acquisition, and continuously adapt their teaching/training approaches to optimize learning efficiency [89].

2. Teaching assistant: WMS-based teaching assistant systems can continuously collect and process various forms of biomedical signals from students, and analyze their voices, movements, and behaviors in order to reach a conclusion about the lecturer's quality of presentation and listeners' level of satisfaction. They can facilitate the teaching process by continuously assisting the lecturer in delivering and subsequently making the learning process shorter, more efficient, more pleasant, and even entertaining. For example, Grosshauser et al. [92] have designed a WMS-based teaching assistant system that monitors movements of dancers and provides feedback to their teacher. Park et al. [30] have designed SmartKG that relies on several wearable badges to provide valuable information about kindergarten students to their teacher.

1.2.3 Main components of WMS-based systems

In this section, we describe the components that constitute a typical WMS-based system, and their limitations. As shown in Fig. 1.4, a typical WMS-based system consists of three main components: WMSs, the base station, and Cloud servers. Next, we describe each.

WMSs

With continuing performance and efficiency improvements in computing and real-time signal processing, the number and variety of WMSs have increased significantly,

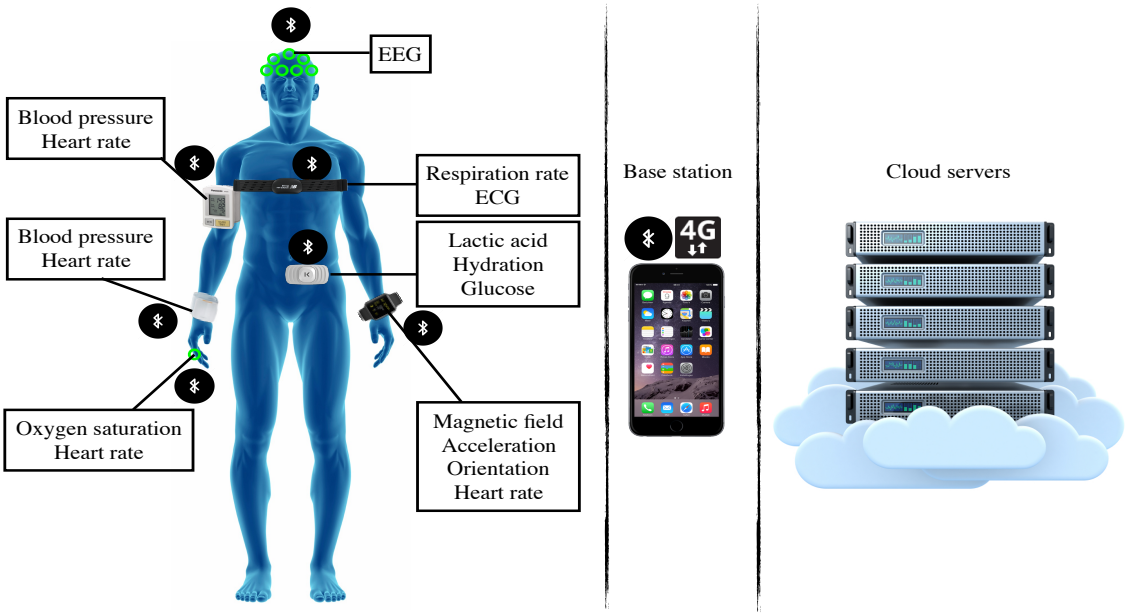


Figure 1.4: The three main components of WMS-based systems: WMSs, the base station, and Cloud servers [2].

ranging from simple pedometers to sophisticated heart-rate monitors. WMSs sense electrical, thermal, chemical, and other signals from the user's body. The majority of these sensors, e.g., EEG and ECG, directly sense and collect biomedical signals. However, a few sensors, e.g., accelerometers, gather raw data that can be used to extract health-related information. Table 1.2 lists various commonly-used WMSs in an alphabetical order, along with a short description for each sensor.

Despite the variety of WMSs available, they share two common limitations that must be considered while designing a WMS-based system: small storage capacity and limited energy.

1. Small storage: Storing a large amount of data in a WMS is not feasible for two reasons. First, adding a large storage to a WMS dramatically increases its energy consumption, and as a result, significantly decreases its battery lifetime [11]. Second, the size constraints of WMSs impose specific storage constraints. The WMS size needs to be kept small to ensure user convenience.

Table 1.2: Common WMSs

Sensor	Description
Accelerometer	measures changes in the acceleration of the device caused by user's movements
Blood pressure sensor	measures systolic and diastolic blood pressures
ECG sensor	measures the electrical activity of the heart
EEG sensor	measures the electrical activity of the brain
EMG sensor	records electrical activity produced by muscles
Glucometer	measures approximate blood glucose concentration
GSR sensor	measures continuous variation in the electrical characteristics of the skin
Gyroscope	measures changes in device orientation caused by user's movements
Heart rate sensor	counts the number of heart contractions per minute
Magnetometer	specifies user's direction by examining the changes in the earth's magnetic field around the user
Microphone	records acoustic sounds generated by the body (used for respiration analysis or emotion detection)
Near-infrared spectroscope	provides neuroimaging technology to examine an aspect of brain function
Oximeter	measures the ratio of oxygen-saturated hemoglobin to the total hemoglobin count in the blood
Pedometer	counts each step a person takes by detecting the motion of the person's hands or hips
Respiration rate sensor	counts how many times the chest rises in a minute
Strain sensor	measures strain on different body parts (used to detect when the user is slouching)
Thermometer	measures an individual's body temperature

2. Limited energy: The small on-sensor battery with limited energy capacity is one of the most significant factors that limits the volume of data sampled and transmitted by WMSs. It is still feasible to wirelessly transmit all raw data without performing any on-sensor processing if devices are charged regularly, e.g., on an hourly basis. However, forcing the user to frequently recharge the WMSs would impose severe inconvenience. As described later in Section 2.2.1, on-sensor processing may significantly preserve battery lifetime by extracting salient information from the data and transmitting it.

The above-mentioned limitations of WMS-based systems have three direct consequences. First, the data generated by WMSs cannot be stored on them for a long period of time and should be transmitted to other devices/servers. Second, only extremely resource-efficient algorithms can be implemented on WMSs. Third, WMSs cannot usually support traditional cryptographic mechanisms, e.g., encryption, and are vulnerable to several security attacks, e.g., eavesdropping.

Base station

Due to limited on-sensor resources (small storage and limited energy), the sensory data are frequently sent to an external device with more computation power. This device is referred to as the *base station*. It may range from smartphones to specialized computing devices, known as central hubs [11]. They commonly have large data storage, and powerful network connectivity through cellular, IEEE 802.11 wireless, and Bluetooth interfaces, and powerful processors [93]. Smartphones have become the dominant form of base stations since they are ubiquitous and powerful and provide all the technologies needed for numerous applications [94]. Moreover, smartphones support highly-secure encrypted transmission, which deters several potential attacks against the system [37].

The base station has its own resource constraints, though much less severe, in terms of storage and battery lifetime. Continuous processing along with wireless transmission to the Cloud may drain the base station's battery within a few hours, and as a result, cause user inconvenience. Base stations typically perform lightweight signal processing on the raw data and re-transmit a fraction or a compressed form of data to Cloud servers for further analysis and long-term storage.

Cloud servers

Since both WMSs and base stations are resource-constrained, sensory data are commonly sent to Cloud servers for resource-hungry processing and long-term storage. Depending on the wireless technology used, the data can be sent either directly or indirectly (through a base station, such as a smartphone) to the Cloud. In addition to the huge storage capacity and high computational power that Cloud servers can provide for WMS-based applications, they facilitate access to shared resources in a pervasive manner, offering an ever-increasing number of online on-demand services. Furthermore, Cloud-based systems support remote update of software, without requiring that the patient install any software on the personal devices, thus making system maintenance quick and cost-effective. This makes Cloud-based systems a promising vehicle for bringing health care services to rural areas [95].

Despite the promise of Cloud servers in this context, utilizing them in WMS-based systems has two drawbacks. First, Cloud-based systems are highly dependent on the reliability of the Internet connection. Outage of Internet service may have serious consequences. For example, unavailability of a seizure prediction system (that tries to detect the occurrence of a seizure a few seconds before the patient's body starts shaking) may lead to a life-threatening situation. Second, the use of Cloud servers increases the response time (the time required to collect sensory data, process them, and provide a response or decision). As a result, there may be a significant deterioration of the quality of service in real-time applications.

1.2.4 Design goals

Although the scope of applications of WMS-based systems is quite wide, they share several common design goals. We reviewed many recent research studies on the design and development of different types of WMS-based systems and realized that, unfortunately, there is no standard inclusive list of desirable goals in the literature.

In this section, we suggest such a list. Fig. 1.5 summarizes seven general design goals that should be considered in designing WMS-based systems. Next, we present the rationale behind each goal.

1. Accurate decisions: WMS-based systems process the input data, e.g., an EEG

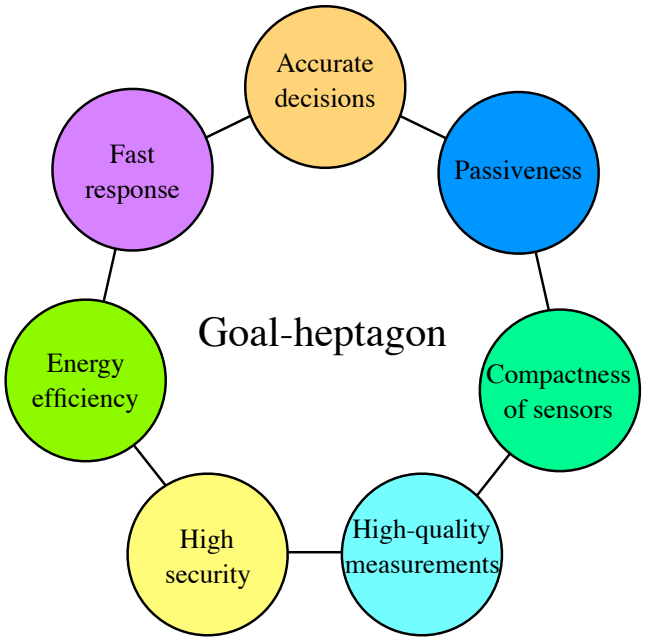


Figure 1.5: Goal-heptagon: Desiderata for WMS-based systems [2].

signal, and return decisions as output, e.g., whether a seizure is occurring or not. The quality of the service provided by a WMS-based system depends on the accuracy of decisions made by the system. For instance, a WMS-based authentication system must confidently determine if the user is authorized to use restricted resources, or a posture corrector must accurately decide whether the user's posture is healthy.

2. Fast response: A short response time is a desirable design goal for the majority of systems. In order to ensure user convenience, it is obviously desirable for the system to quickly respond to user requests. Moreover, a short response time is essential for an authentication system, in which the system must quickly authenticate a legitimate user and reject an impostor [37]. Furthermore, a long response time may endanger user safety in some scenarios. For example, if an insulin pump fails to immediately

detect an emergency, e.g., hyperglycemia or hypoglycemia, and provide a response when it is necessary, the patient might suffer from life-threatening conditions [96].

3. Energy efficiency: The battery used in a WMS is typically the greatest contributor to both size and weight. As a result, WMSs typically have very limited on-sensor energy [97]. Rapid depletion of battery charge, necessitating frequent, e.g., on a hourly basis, battery replacement/recharge would deter wide adoption of the device [98]. Thus, all components embedded in WMSs and the signal processing algorithms implemented on them must be energy-efficient.

4. High security: The emergence of the IoT paradigm has magnified the negative impact of security attacks on sensor-based systems. Furthermore, the demonstration of several attacks in recent research efforts (see [1] for a survey) has led to serious security concerns and highlighted the importance of considering security requirements. To ensure system security, different security requirements must be proactively addressed. As mentioned earlier, security requirements are often broken down into three main categories: (i) confidentiality, (ii) integrity, and (iii) availability, referred to as the CIA-triad [20].

5. High-quality measurements: Undoubtedly, the quality of the decisions offered by a WMS-based system depends on the quality of sensory measurements provided by WMSs. It has been shown that user's activities may negatively impact the quality of data obtained by the WMSs, e.g., running significantly deteriorates the quality of the signal collected by EEG sensors [99]. Hence, WMSs should be designed to provide accurate and noise-robust measurements during different daily activities, especially intensely physical ones.

6. Compactness of sensors: To ensure user convenience, WMSs must be kept lightweight and as small as possible. Moreover, in many scenarios, the presence of specific WMSs, e.g., blood glucose monitor, may reveal the presence of an illness along with the current level of the illness, leading to serious privacy concerns [100].

Thus, WMSs should be designed to be compact so that the user can easily hide them.

7. Passiveness: Passiveness, i.e., minimal user involvement, is a key consideration in designing a WMS-based system. It is very desirable that WMSs be calibrated transparently to the user and sensory data be measured independently of user activities [101]. Obviously, if a wearable device, e.g., a smart watch, asks the user to calibrate internal sensors, e.g., accelerometers and magnetometers, manually, it may be quite annoying to the user [102].

1.3 Contributions of the thesis

To mitigate the security/privacy issues in the IoT domain while considering domain-specific limitations (e.g., limited energy and small storage capacity) of various components utilized in IoT-based systems, this thesis provides low-energy solutions that make data encryption practical for resource-constrained sensors (e.g., WMSs). Furthermore, in order to shed light on new domain-specific security/privacy issues associated with IoT-based systems, two novel security attacks are introduced in this thesis. Moreover, a novel IoT-enabled continuous authentication system is presented, which aims to address the security issues and weaknesses of previously-proposed authentication systems. Our main contributions can be summarized as follows:

1. The thesis first targets health monitoring systems, one of the most widely-known types of IoT-based systems that are envisioned as key to enabling a holistic approach to health care. It describes different solutions for reducing the total energy consumption of different implantable and wearable medical devices (IWMDs) utilized in continuous health monitoring systems. The proposed solutions can significantly increase the battery lifetimes of different IWMDs while offering spare energy for encrypting medical data before transmitting them.

2. The thesis introduces OpSecure, an optical secure communication channel between an implantable medical device (IMD) and an external device, e.g., a smartphone. OpSecure enables an intrinsically user-perceptible unidirectional data transmission, suitable for physically-secure communication with minimal size and energy overheads. Based on OpSecure, we design and implement two protocols: (i) a low-power wakeup protocol that is resilient against remote battery draining attacks, and (ii) a secure key exchange protocol to share the encryption key between the IMD and the external device. The proposed protocols complement lightweight symmetric encryption mechanisms, so that common security attacks against insecure communication channels can be prevented.

3. The thesis shows how security/privacy attacks against health monitoring systems extend far beyond wireless communication to/from IWMDs, and explains why encryption cannot always provide a comprehensive solution for eliminating security/privacy attacks on IWMDs. In particular, it describes the possibility of privacy attacks that target physiological information leakage, i.e., signals that continuously emanate from the human body due to the normal functioning of its organs. Furthermore, it discusses several novel attacks on privacy by leveraging information leaked from them during their normal operation.

4. The thesis then introduces a generic security attack that is applicable to a variety of cyber-physical systems (CPSs), i.e., systems with integrated physical and processing capabilities that can interact with humans and the environment. These attacks are called dedicated intelligent security attacks against sensor-triggered emergency responses (DISASTER). DISASTER targets safety mechanisms deployed in automation/monitoring CPSs and exploits design flaws and security weaknesses of such mechanisms to trigger emergency responses even in the absence of a real emergency. In addition to introducing DISASTER, it

describes the serious consequences of such attacks, and demonstrates the feasibility of launching DISASTER against the two most widely-used sensor-based systems: residential and industrial automation/monitoring systems. Moreover, it provides several countermeasures that can potentially prevent DISASTER and discusses their advantages and drawbacks.

5. Finally, the thesis presents continuous authentication based on biological aura (CABA), a novel user-transparent system for continuous authentication based on information that is already gathered by WMSs for diagnostic and therapeutic purposes. The presented continuous authentication system can offer a promising alternative to one-time knowledge-based authentication systems (e.g., password-/pattern-based authentication systems) and potentially be used to protect personal computing devices and servers, software applications, and restricted physical spaces.

1.4 Thesis outline

The rest of this thesis is organized as follows. Chapter 2 discusses related work. Chapter 3 quantifies the energy and storage requirements of continuous personal health monitoring systems and presents several schemes to reduce the overheads of wirelessly transmitting, storing, and encrypting/authenticating the data. Chapter 4 discusses OpSecure and two protocols that can be used in conjunction with symmetric encryption to protect the wireless channel between the IMD and an external device from different security attacks. Chapter 5 describes the concept of physiological information leakage and how such leakage can be exploited by attackers even if the communication channels are encrypted. Chapter 6 introduces DISASTER and describes its consequences. Moreover, it suggests several countermeasures to mitigate such attacks. Chapter 7 presents CABA, describes its various applications, and

discusses how it can be extended to user identification and adaptive access control authorization. Chapter 8 concludes the thesis and presents ideas for future research.