Toward Uniform Smart Healthcare Ecosystems: A Survey on Prospects, Security, and Privacy Considerations

Hadi Habibzadeh and Tolga Soyata

Abstract A plethora of interwoven social enablers and technical advancements have elevated smart healthcare from once a supplemental feature to now an indispensable necessity crucial to addressing intractable problems our modern cities face, which range from gradual population aging to ever surging healthcare expenses. State-of-the-art smart healthcare implementations now span a wide array of smart city applications including smart homes, smart environments, and smart transportation to take full advantage of the existing synergies among these services. This engagement of exogenous sources in smart healthcare systems introduces a variety of challenges; chief among them, it expands and complicates the attack surface, hence raising security and privacy concerns. In this chapter, we study the emerging trends in smart healthcare applications as well as the key technological developments that give rise to these transitions. Particularly, we emphasize threats, vulnerabilities, and consequences of cyberattacks in modern smart healthcare systems and investigate their corresponding proposed countermeasures.

Keywords Privacy · Security · Wearable sensors · Access control · Authentication

1 Introduction

With the world slowly recovering from the last economic recession in 2007 [1, 2], which occurred in parallel with the gradual population aging and the prevalence of chronic diseases such as osteoarthritis and diabetes in epidemic proportions [3, 4], smart healthcare—often portrayed as a panacea for improving healthcare quality and reducing its ever-increasing expenses—has been recently gaining unprecedented momentum. Further driven by impressive breakthroughs in the Internet of Things

H. Habibzadeh (✉) · T. Soyata
University at Albany, SUNY, Albany, NY, USA
e-mail: hhabibzadeh@albany.edu; tsoyata@albany.edu

A. El Saddik et al. (eds.), *Connected Health in Smart Cities*,
https://doi.org/10.1007/978-3-030-27844-1_5

(IoT) and smart city technologies, smart healthcare (or alternatively electronic health or e-health) has shown massive potential to bring *continuous*, *real-time*, and *personalized* health services to masses, thereby substantially decreasing the burden of already under-staffed healthcare centers [5]. Indeed, the proliferation of a wide array of e-health services ranging from clinical-grade [6, 7] to fitness [8, 9] to logistical and infrastructure [10, 11] applications is a testament to the growth of this field.

The interplay of these social impetuses and technological advancements has now paved the way for the emergence of next-generation implementations, where healthcare services are not merely restricted to continuous monitoring of physiological parameters. Instead, they operate in tandem with non-healthcare aspects of a smart city—such as smart homes and smart environments [12]—to provide comprehensive care. This transition is transpiring in a broader context and outside the locus of smart healthcare. For example, in a future smart city, a wearable remote ECG monitoring system [13] can automatically contact emergency units at the onset of a heart attack. Then, an autonomous defibrillator ambulance [14] can be dispatched to help the patient. Traffic status can be manipulated to minimize ambulance travel time [15], thereby increasing the survival chance of the patient. Although this simple scenario falls under the smart healthcare umbrella (judging by its purpose), it involves other smart city services such as smart transportation. Additionally, considering the proliferation of smart electric vehicles, this scenario indirectly engages the smart grid [16]. Such a *unified single IoT infrastructure* is yet to be realized, however, recent developments in the IoT signal its beginnings.

This transition introduces numerous challenges and opportunities. It renders smart healthcare an even more interdisciplinary field, where the effectiveness of implementations hinges on a close cooperation among engineers, physicians, patients, city authorities, businesses, etc. Establishing such a communication among healthcare constituents, however, has become a major obstacle against its progression [17]. Furthermore, inflating the sphere of e-health substantially increases the breadth and complexity of the attack surface, which poses serious security and privacy concerns, particularly, considering the gravity of the task, which involves citizens' safety and well-being. The latter case has recently become more alarming in the aftermath of increasing attacks that target critical healthcare infrastructure such as hospitals [18]. The extent and intensity of these breaches, often conducted for extortion purposes, have created an aura of distrust and skepticism between smart healthcare and its users. Neglecting these apprehensions can indeed delay the widespread acceptance of smart healthcare.

We dedicate this study to security and privacy considerations of these emerging smart healthcare applications. To this end, we first investigate the latest trends in smart healthcare applications in Sect. 2 to see how the most recent research works in the literature take advantage of existing symbiotic relationship among e-health and various aspects of modern smart cities. We then analyze the overall structure of such services and discuss the underlying technical developments that have fueled this transition in Sect. 3. We study these enablers from the standpoint of sensing, communication, and data processing and elaborate on how emerging

technologies such as crowd-sensing, non-dedicated sensing, low-power short-range communication, machine learning, and deep learning solutions are driving smart healthcare toward its bright future. These nascent technologies, however, introduce security concerns. We review these vulnerabilities in Sect. 4 by discussing the latest attacks and threats against real-world implementations. Protecting smart healthcare applications from these ever-increasing threats and vulnerabilities requires a holistic approach. To this end, Sect. 5 provides a summary of some of the most prevalent attacks that target in-field individual components of smart healthcare along with their common countermeasures. Section 6 focuses on approaches that aim to protect the entirety of the system, particularly by providing services such as access control, authentication, and authorization. Sections 7 and 8 provide a discussion of existing unresolved challenges and concluding remarks, respectively.

2 Smart Healthcare Applications

Increasing public awareness about the importance of personalized, continuous, and efficient healthcare, coupled with recent breakthroughs in the IoT arena has made the scene ready for the emergence of a diverse range of smart healthcare applications. A substantial number of proposed services aim to provide a decision-support framework for physicians and specialists, thereby helping them with disease prevention, diagnosis, and therapy [19]. Such *clinical-grade* applications involve accurate data acquisition and processing that must comply with stringent procedures and standards enforced by specialized organizations such as American Diabetes Association (ADA) [20, 21] and American Heart Association (AHA) [22, 23]. Considering that these strict requirements can become prohibitive for many investors and researchers, a parallel branch of smart healthcare oriented toward *non-clinical* applications is gaining momentum. These services often include noninvasive monitoring devices such as smartwatches and wristbands to help users keep track of their activities, to promote healthier lifestyles. Alternatively, a wide variety of non-clinical applications are designed to provide continuous care for elderly and people with disabilities. Finally, instead of providing real-time and personalized healthcare, the third category of e-health aims to facilitate communication among healthcare's multiple constituents, including patients, physicians, specialists, hospitals' staff, and emergency units. In this section, we study smart healthcare applications under these three categories: (i) Clinical, (ii) Non-clinical, and (iii) Logistical applications.

As discussed in Sect. 1, the boundaries among these applications are narrowing. Investors and researchers must become cognizant of numerous challenges and complications this integration of a wide variety of smart city services poses. We discuss the significance of this in Sect. 3. This transition also introduces various security and privacy concerns. For example, a hardware-level attack to a smart healthcare device by an insider not only compromises health related private data but can also endanger the entire network, leaving the home network and other smart city services (such as smart home devices) vulnerable to cyberattacks [24]. We elaborate on major security and privacy concerns in Sections 5 and 6.

2.1 Clinical-Grade Healthcare Applications

Measuring major physiological parameters in clinical settings is traditionally conducted by trained staff and personnel via typically expensive and invasive monitoring systems. Although accurate—which is a fundamental requirement in these applications—traditional methods fail to provide continuous monitoring, which is becoming increasingly more relevant to the prevalence of chronic diseases [25]. Furthermore, measurements conducted in controlled environments of hospitals and laboratories do not sufficiently reflect patients' actual physical status in their day-to-day life. Numerous smart healthcare systems are proposed to address these requirements. The outputs of these services are directly used by physicians and specialists for prevention, diagnosis, and therapy purposes, which highlights the strict accuracy and reliability requirements of clinical smart healthcare. Unfortunately, however, noninvasive, inexpensive, and real-time monitoring does not yield high sensing accuracy. A part of these shortcomings can be offset by the utilization of advanced preprocessing and data processing techniques, which are now an integral component of every smart healthcare system. Nonetheless, as even occasional failures (false negatives) can lead to catastrophic outcomes, clinical-grade monitoring systems notoriously suffer from high false positive rates [26]. We provide more details on smart healthcare data processing in Sect. 3.3.

A large portion of clinical-grade smart healthcare applications uses continuous monitoring to detect specific events. Specifically, given the increasing share of heart failures, a wide range of applications targeting cardiovascular diseases (CVD) are proposed in the literature. For example, the authors in [27] propose a cloud-based ECG monitoring system that assists with diagnosing cardiovascular diseases by classifying heart activity into *normal*, *premature*, *ventricular contractions*, and *other*. The classification is carried out by a 30-neuron artificial neural networks (ANN) based on QRS complex features. In a telemonitoring scenario, processed information can be transmitted to a physician to assist them with decision making. This is, however, a non-trivial task as the sheer size of information collected in real-time continuous systems can readily inundate physicians and specialists. Effectively representing processing results has been subject to extensive research [28–30]. For example, a novel "QT-Clock" is presented in [31] that can summarize ECG data collected in a 24-h interval, facilitating prolonged QTc diagnoses considerably.

Although valuable, continuous sensing alone is insufficient in many cases, as a wide array of chronic diseases (such as diabetes) can only be contained through exhaustive adaptations in daily lifestyle. For such scenarios, comprehensive smart healthcare services have been developed to facilitate patient-physician collaboration, control their diet and medicine intake, and potentially recommend physical activities [32]. Aside from normal monitoring, such systems must analyze the environment and detect patients' activities, while meeting the requirements and recommendation of specialized groups. Data pertaining to patient progress and alerts indicating a critical event can be shared in real-time with a physician to provide telemonitoring [32]. Some IoT-based healthcare systems even involve

automatic medicine administration, thereby ensuring perfect scheduling and exact dosage without requiring patient's diligence. An implantable example of such devices is implemented in [33]. In spite of its invasive implantation, such methods can increase patients' comfort in long-run (particularly, as opposed to traditional glucose monitoring that involves taking blood samples by *finger sticking*). We further discuss advantages and disadvantages of such methods in Sect. 3.1.

2.2 Non-clinical Healthcare Applications

Clinical-grade applications inherently entail extreme accuracy and reliability, as even occasional errors can bring about grave consequences. Many researchers and investors prefer to explore new horizons of smart healthcare free of these stringent requirements and standards. Furthermore, developing applications for the entire population (healthy and non-healthy) provides further investment motivation by promising a larger market. These major enablers have stimulated the emergence of non-clinical applications, which mostly focus on improving users' lifestyles. Relatively looser regulations in non-clinical applications directly translate to cost reduction and improved noninvasiveness—both of which are integral requirements for these applications. This field has received substantial momentum with the advancement of smart portable devices such as smartphones, smartwatches, and smart glasses. Despite their rather casual implementations, the contribution of this branch of healthcare to prevention, diagnoses, and rehabilitation of diseases must not be underestimated. In this section, we review notable example developments in this field.

A typical non-clinical smart healthcare application involves wearable sensors that collect data on a variety of physiological and environmental parameters. Sensors can take different forms depending on target applications and their requirements. For instance, textile wearable sensors worn around feet and ankles transmit inertia measurements over Bluetooth Low Energy (BLE) to a smartphone; where Support Vector Machine (SVM) algorithm classifies user's gait as either normal or *foot drop* [34]. Achieving accuracies between 71% and 98%, such an application can expedite rehabilitation process [35]. Indeed, as discussed earlier, the new generation of the smart healthcare applications employ various aspects of smart city to improve their usability. An example of such an application is provided in [8], where a combination of participatory sensing and existing sensing infrastructure in environmental monitoring, air quality monitoring, and smart transportation is used to suggest a suitable exercise route. By considering pollution, traffic, the difficulty of the terrain, ultraviolet (UV) radiation index, and temperature, the proposed application uses collaborative filtering (CF) to classify routes into three categories (danger, caution, idle) based on the physical status and health condition of the user. An ambient assisted living (AAL) targeting outdoor activities of the elderly and people with disability is developed in [36]. The proposed system is based on crowed-sensing and assists users with navigation, finding urgent health attention, providing help

while afflicted with confusion, and routine tasks such as making calls and passing across streets. It can also classify user's status into various categories including *OK*, *Fallen*, *Wandering*, *Risk of Getting Lost*, etc. This example clearly shows how the implementation of an effective modern smart healthcare application can extend to not only multiple smart city infrastructures but also various social considerations.

Not all the non-clinical application focus on continuous personalized monitoring. Particularly, the prevalence of new technologies such as virtual reality (VR) and augmented reality (AR) has resulted in a variety of rehabilitation services. Particularly, VR-based video games proposed in [37] and [38] provide affordable home-based setups to accelerate rehabilitation of stroke patients with impaired arms. This directly translates to significant cost reduction by minimizing the involvement of trained personnel and special equipment.

2.3 Logistical and Infrastructure Healthcare Applications

Ubiquitous smart healthcare has created the "big data" problem, where transmission, storage, and processing of a large amount of data pose multiple challenges. Parallel to data acquisition research, many have redirected their focus to address these big data-related challenges, thereby completing the puzzle of the *uniform smart healthcare ecosystem*. For example, multi-agent systems (MAS) based on semantic comprehension can facilitate data sharing among various hospitals [39], even when the size of stored information and its distribution increases. However, in addition to its sheer size, the large number of stakeholders in smart city ecosystems also poses various challenges. An effective infrastructure is required to share data among patients, hospitals, insurance companies, pharmacies, and emergency units. Although cloud-based implementations are typically considered the natural choice in these scenarios, they raise genuine security and privacy concerns. Encryption and watermarking are proposed to protect data transfers to and from cloud servers [40]. We detail smart healthcare security considerations in Sections 5 and 6.

In addition to data sharing, some smart health applications aim to increase the efficiency of hospitals by introducing the *smart hospital* concept. An example of such system is developed in [41]. The system embodies a diverse range sensing nodes such as RFID tags, smartphones, and wireless sensor networks (WSNs) to collect information regarding the location and progress of each patient as well as their major biomarkers. The developed system allows patients with both registration and follow-up and helps them navigate within the building. Implementing such a smart environment in hospitals can reduce waiting time and costs while increasing the quality of provided services. Additionally, some applications can merely focus on facilitating face-to-face interaction between patients and physicians [17], which can be particularly of assistance to the elderly and people with disability, as they cannot make frequent visits to hospitals.

Some government agencies monitor social networks for early detection of outbreaks. This solution can effectively reduce the costs of expensive existing

methods (which mostly rely on a network of physicians and pharmacies) and help with detecting outbreaks in their early stages, thereby substantially increasing the chances of its containment. Particularly, detecting seasonal influenza outbreaks via social networks seems to be quite effective [42]. Multiple examples of similar works are provided in [43], which discusses the application of the artificial intelligence to the data collected from social networks for *computing* the health status of the society (e.g., via prediction of outbreaks, measuring the efficacy of countermeasures, etc.).

2.4 Summary

Smart healthcare applications can be categorized into (i) clinical, (ii) non-clinical, and (iii) logistical and infrastructure applications. Clinical-grade services aim to assist healthcare stakeholders with prevention, diagnoses, therapy, and rehabilitation of various diseases. Non-clinical applications target personal healthcare to promote a healthier lifestyle. Logistical applications mostly focus on hospital automation and facilitate patient-physician collaboration. The dissimilarities in scopes of these applications diversify their requirements and priorities. Table 1 summarizes the

Table 1 A comparison of smart healthcare major branches: (i) clinical, (ii) non-clinical, and (iii) logistical and infrastructure applications

Application	Priorities (high to low)	Example services
Clinical (Sect. 2.1)	High-accuracy Robust security Privacy protection Non-invasive Low-cost	Glucose monitoring [44] Respiration monitoring [45] Hypertension monitoring [46]
Non-clinical (Sect. 2.2)	Non-invasive Low-cost Privacy protection Robust security High-accuracy	Diet control [47] In-home rehabilitation [37] Stress monitoring [48]
Logistical (Sect. 2.3)	Robust security Privacy protection High-accuracy Non-invasive Low-cost	Smart hospital [49] Medical data sharing [50] Telemedicine [51]

This table contrasts the priorities and characteristics of each category. Priorities are listed based on decreasing importance for each category. For example, clinical-grade devices aim to provide high accuracy, even if that increases their costs and invasiveness. In contrast, non-clinical fitness services can decrease accuracy in favor of lower cost and lower invasiveness. *Example Services* lists some of the example implementations of each application

idiosyncrasies of each category. Particularly, the importance of five underlying characteristics of such systems is investigated: accuracy, security, privacy, non-invasiveness, and expense. For example, many clinical applications can trade off expense to increase accuracy. In contrary, the expense is the main criterion for many commercialized and non-clinical services (hence its priority is set to *high* in the table).

3 System Architecture

Despite its relatively short record, smart healthcare (as a subcategory of smart city and IoT) has been subject to profound changes. The early implementation of smart health was mostly centered around three components: Data acquisition and sensing, data concentration and aggregation, and data processing, storage, and visualization. Closest to the user, data acquisition involves a diverse range of sensing devices that collect raw data on user's multiple biomarkers. Due to stringent requirements on noninvasiveness, battery life, and ease-of-use (including weight and size), these sensing devices are incapable of providing intense computing. More importantly, these sensors oftentimes operate as stand-alone devices, implying that they do not have access to the entire acquired data. The most expedient solution is to outsource calculations to computationally-capable servers, where demanding data processing algorithms and long-term data storage can be provided free of the constraints sensing devices face. Direct cloud access, however, is typically far beyond the capabilities of sensing devices. This problem is typically circumvented through a hierarchal implementation, where an intermediary component bridges the gap between data acquisition and the cloud. This conduit provides transparent cloud connectivity via local wireless personal area networks (WPANs) and wireless body area networks (WBANs), thereby substantially removing communication burden from sensors. An abstract depiction of this architecture is shown in Fig. 1.

This classic architecture of smart healthcare sufficiently addresses application requirements. Particularly, hierarchal implementation is proven to be effective against system's large scale, rapid, and constant data generation, and extreme (and growing) heterogeneity. The cloud-based implementation also ensures *deep value*, where invaluable information can be revealed by combining data from multiple sources (data fusion). The backbone of this architecture, therefore, remains applicable to new-generation smart health applications as well; however, recent developments in the IoT field have resulted in significant modifications in implementation details. For example, the emergence of smart portable devices has introduced the mobile-health (m-health, as opposed to electronic-health or e-health) concept, where new sensing platforms such as the participating and non-dedicated sensing [52] have revolutionized the data acquisition component. Furthermore, as discussed in Sect. 2, smart healthcare is growing beyond its traditional definition. Similar evolution is transpiring in other smart city applications. These developments portend a uniform IoT ecosystem. Considering the functionality, this ecosystem

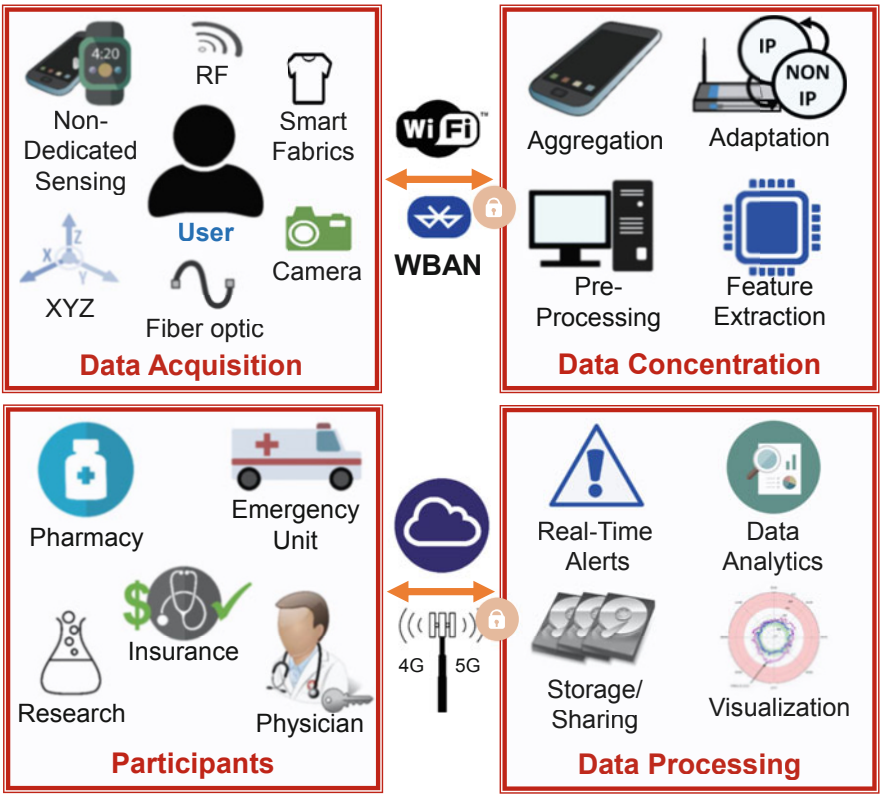

Fig. 1 Functionality of the smart healthcare infrastructure can be thought of as having three categories: (i) Data Acquisition involves dedicated and non-dedicated sensing to collect information about users and their surrendering environment, (ii) Data Concentration performs rudimentary data processing and bridges the local network with the cloud, and (iii) Data Processing stores, analyzes, and visualizes the data over an either distributed or non-distributed platform. The results are shared with various participants including physicians, insurance companies, pharmacies, etc

can be structured based on a four-component model. An *infrastructure* component gathers raw data and transfers them to the cloud for processing. *Utility* component provides application-specific services for parochial services such as smart health, smart transportation, AQ monitoring, etc. *Social development* component conflates individual applications to provide social services such as comprehensive healthcare, education, and entertainment [12]. Finally, *security and privacy* components must be spread over all building blocks of the system to ensure its robustness against cyber threats and security flaws. An abstract representation of this paradigm is depicted in Fig. 2. In the rest of this section, we study each component of smart healthcare in details and investigate how recent developments in smart city arena have affected its implementation. A thorough and complete review of the most recent advances in the smart city system architecture can be found in [53].

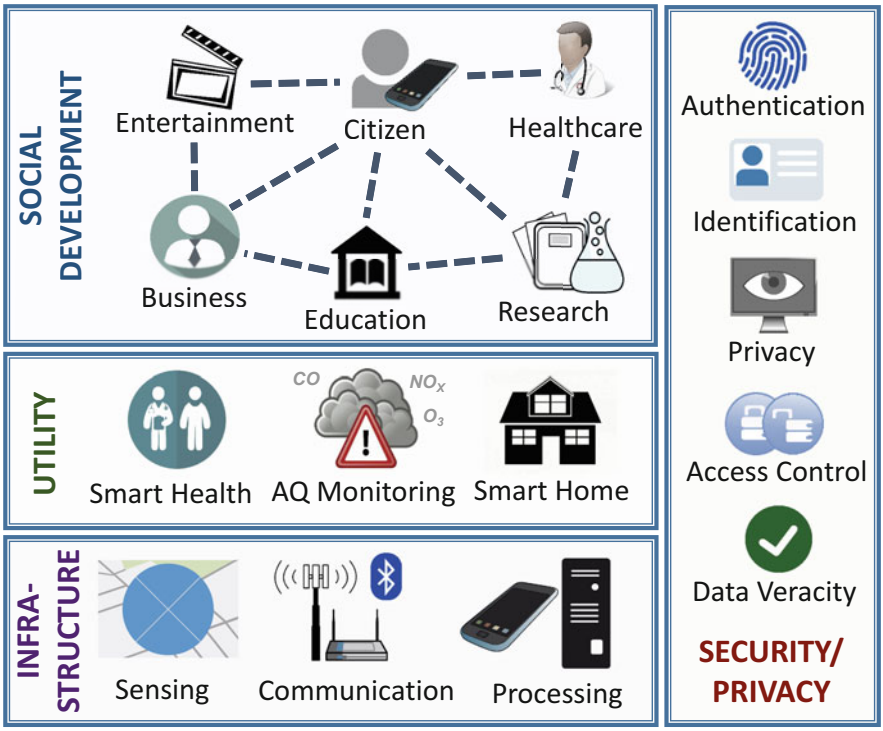

Fig. 2 A demonstration of state-of-the-art smart healthcare applications. Such systems encompass four components: (i) Infrastructure involves sensing, communication, and processing platforms, (ii) Utility employs the infrastructure toward parochial smart city applications, (iii) Social Development ensures interoperability among stand-alone applications, hence taking advantage of existing synergies, (iv) Security and Privacy protects the entire system from privacy leaks and cyber threats

3.1 Data Acquisition and Sensing

This component of the smart healthcare architecture embodies a variety of sensing devices, which aim to provide continuous, noninvasive, accurate, and inexpensive raw data acquisition of physiological and environmental parameters. These strict requirements coupled with a harsh deployment environment pose various restrictions on sensor weight, cost, size, and computational and communication capabilities. Hence, limited resource availability is the major consideration in data acquisition design and implementation. Similar to other aspects of smart healthcare, data acquisition component has been subject to gradual evolution. As explained in [3], the first generation of smart health sensing typically revolved around data acquisition from a limited number of sensors such as electrocardiogram (ECG) patches and pulse oximeters. It was soon discovered that *data fusion* in a multi-sensory setting can effectively reveal hidden information at the expense of increased

computational complexity (a trade-off worth making especially in the cloud-based architecture with abundant resources) [54, 55]. The recent generation of data acquisition implementations are centered around the same premise, however, they incorporate non-traditional sources of data such as patients' historical records, research results, and laboratories experiments [56]. Although this approach further complicates the challenges regarding the big data management, it adds substantial value to applications' performance, as systems tend to evince emergent characteristics.

Multiple enablers have fueled these developments in data acquisition. Advances in solid-state physics and VLSI design have increased the computational capability of smart sensors while reducing their power dissipation. In the meantime, recent breakthroughs in material sciences have resulted in the emergence of bio-compatible and flexible printed circuit boards (PCBs) [57]. Complementary to these, novel energy harvesting solutions have remarkably mitigated the limited power availability, thereby improving sensors' noninvasiveness and accelerating the emergence of perpetual data acquisition [58–60]. Finally, smart healthcare sensing has received significant momentum with the proliferation of smart portable devices and novel solutions such as crowd-sensing and non-dedicated data acquisition [52].

Being the backbone of data acquisition component, sensors are typically implemented in three forms: *ambient sensors*, *wearable sensors*, and *implantable sensors*. Ambient sensors can collect users' information from a distance, which minimizes their invasiveness. Cameras are the most common type of ambient sensors. When used with powerful image processing techniques, camera-based solutions can be applied to a wide spectrum of applications. For example, the system proposed in [61] uses smartphones' embedded cameras to capture changes in ambient light intensity caused by breathing-induced body movements. These changes can be processed to reveal information about tidal volume and respiration rate. Indeed, this approach is substantially less invasive and more cost-efficient than standard clinical methods such as trained personal observation, Doppler radars, and spirometry. However, cameras are susceptible to the noise induced by other light sources, suffer from a limited line of sight, and raise privacy concerns [62]. This has motivated some researchers to investigate RF-based sensors as a strong candidate for ambient sensing. Various studies show that users' movements caused by falling [63], respiration [64], and heartbeats [65] interfere with RF signals (particularly, Received Signal Strength (RSS) indicator). RF sensors address many limitations of cameras, however, the filed is still in its fledgling state and many proposed solutions are tested in highly controlled environments.

Wearable sensors must remain in close proximity of users' bodies. Some may require direct contact with the skin, while others may not. For example, the authors in [66] propose a cuffless wearable sensor for blood pressure monitoring based on photoplethysmograph (PPG) signals captured by pulse oximeters. Clearly, the proposed system excels clinical approaches, which involve trained physicians and sphygmomanometer—and require patients to wear a cuff around their arm—in terms of ease-of-use and continuous data acquisition. Pulse oximeters are typically worn at the fingertips, which can become cumbersome in the long-term use. A study conducted in [67] shows that when coupled with advanced image processing

techniques, built-in cameras of smartphones can also be employed to capture PPG signals. Furthermore, conducted studies in [68] and [69] prove the applicability of pulse oximeters to blood oxygen saturation monitoring applications. Other commonly used wearable sensors include dry and non-contact ECG patches [70] and Inertial Measurement Units (IMUs), which include multi-axis accelerometers, gyroscopes, and force sensors [71].

Once implanted within the body, in-vivo sensors can collect data and administer medicines accurately, without requiring any intervention from users. In spite of their invasive installation process, in-vivo sensors outperform their wearable alternatives in terms of ease-of-use in long-term operation. For example, an implantable device capable of glucose monitoring and injecting insulin is proposed in [33] for diabetic patients. The device can operate for 180 days after insertion when performing data measurements every 2 min. Limited power availability is the bane of in-vivo sensors. A study conducted in [72] proposes an implantable blood pressure monitoring system that is powered by RF backscattering; hence it can operate for an extended period. However, the sensor includes a wearable pair that continuously transmits wireless power to the device. Table 2 summarizes our discussion about most commonly used sensors in smart healthcare data acquisition.

Table 2 Sensors used in smart healthcare data acquisition component can be categorized into *ambient*, *wearable*, and *implantable* devices

Type	Advantages and disadvantages	Example applications
Ambient sensors	⇑ Minimal invasiveness ⇑ Cost-efficient ⇓ Limited accuracy ⇓ Privacy concerns ⇓ Interference susceptibility	Respiration monitoring (camera) [61] Blood oxygen monitoring (camera) [73] Fall detection (RF) [63] Heart beat monitoring (RF) [65] Respiration monitoring (WiFi) [64]
Wearable sensors	⇑ High flexibility ⇑ Cost-efficient ⇑ Non-invasive ⇓ Security concerns ⇓ Limited accuracy ⇓ Uncomfortable	BP monitoring (pulse oximeter) [74] Muscle activity monitoring (textile) [75] Seismocardiography (accelerometer) [76] Electrocardiography (ECG) [77] Fall detection (IMU) [71]
In-vivo sensors	⇑ High accuracy ⇑ Comfortable ⇓ Invasive ⇓ Limited battery life ⇓ Uncomfortable	Glucose monitoring (abdominal tissue) [33] BP monitoring (femoral artery) [72]

Ambient sensors are typically used for casual fitness-related applications. Wearable sensors can be used for both clinical and non-clinical purposes, while implantable (in-vivo) sensors are most suitable for clinical applications due to their unmatched accuracy

3.2 Data Concentration and Aggregation

Data concentration and aggregation component facilitates cloud access by creating a virtual conduit between in-field sensors and the cloud. Breaking the distance between these two components and placing the data concentrator close to sensing devices transfer the communication burden from sensors to the concentrator. Therefore, concentrators are typically provisioned to be relatively resourceful—sometimes grid-connected—computers that are not constrained with limitations of field devices. This approach is readily implementable, as a single concentrator can cater to many sensors. A concentrator establishes a short-range wireless with sensors, over which filed devices can upload their data and receive command and control messages from the cloud. Once a communication link is established, a concentrator provides three fundamental services to its associated sensor nodes: *preprocessing and aggregation*, *protocol adaptation*, and *cloudlet services*.

Radio Access Technologies (RATs) Establishing a connection between sensors and the concentrator faces the typical challenges of IoT and smart city communication. The power availability limitation is the main setback. Data is also highly heterogeneous; an application might involve multi-media, text-based, scalar, and real-time data, with each type demanding a specific quality of service management. Furthermore, as many smart healthcare applications are event-based (such as fall detection, heart attack prediction, etc.), the network traffic is highly bursty and unpredictable. Finally, security and privacy considerations are also of utmost importance. When combined with 3Vs (veracity, volume, and velocity) of the smart city communication [78], satisfying these requirements entails many challenges. A variety of WBAN and WPAN protocols are proposed in the literature. However, ZigBee, Bluetooth Low Energy, and WiFi have received the widest adoption. ZigBee (developed by ZigBee Alliance [79]) has for long been considered the de facto standard for WPAN implementations, due to its low complexity, acceptable reliability, low energy consumption, and decent data rate and range ($\leq$250 kbps and $\leq$100 m). This standard, however, suffers from multiple shortcomings. First, the performance of ZigBee deteriorates with the number of nodes [80]. More importantly, as ZigBee operates in the same frequency band as WiFi and due to its relatively lower transmission power, the standard is known to evince poor WiFi compatibility [81]. This can become a prohibitive limitation considering the ever-increasing popularity of WiFi. These limitations have inclined some researchers toward IEEE 802.11 (WiFi) standard, which provides remarkable throughput and unmatched ubiquity. Nonetheless, WiFi is not originally designed for smart city dense networks. Its performance decreases with the network density. Additionally, WiFi consumes orders of magnitude more energy than its low-power alternatives. BLE [82] is indeed the shining star of smart healthcare applications. It can provide relatively high data rates ($\leq$2 Mbps) and decent coverage ($\approx$ 70 m) [83]. In addition to its high energy efficiency (study conducted in [84] shows that a small coin battery can power a BLE-powered sensor for about a year in an activity recognition application), the popularity of BLE can be mostly attributed to its unparalleled

ubiquity, as many portable devices such as smartphones, laptops, and smartwatches shipped with embedded BLE compatibility. BLE, however, cannot be configured in the mesh topology, which limits its scalability and arises security and privacy concerns [85].

Expected to be available in 2020, the fifth generation of mobile communication (5G) promises a low-delay (less than 1 ms), long-range, low-energy (90% reduction in comparison to 4G), high-rate (up to 10 Gbps), and resilient connectivity for smart city applications [86]. The 5G's ability to provide diverse QoS and Quality of Experience (QoE) management coupled with its compatibility with both massive Machine Type Communication (mMTC) and Ultra-Reliable Low Latency Communication (URLLC) [87] promises great opportunities to dovetail smart healthcare and other smart city applications. To these, we should also add features such as impressive mobility support (500 kmph) [88], Device to Device communication [89, 90], and Licensed-Assisted Access (LAA) [91], all of which are critical to cross-application comprehensive healthcare services. Overall, taking into the account the close ties of cellular networks with smart cities [92], the share and importance of such RATs in the smart healthcare is expected to grow.

Data Preprocessing and Aggregation Two inherent characteristics of smart healthcare communication motivate data preprocessing and aggregation. First, the dense deployment of sensors often results in duplicates or values that are in the close vicinity of each other. For example, built-in accelerometers of a user's smartwatch and smartphone typically measure and report the same value, which implies some degrees of redundancy. The other contributing factor can be associated with event-based nature of many healthcare applications, where all the sensors deployed in an application generate a tide of data upon occurrence of an event. In these scenarios, having multiple sensors that report the same event represents redundancy. The data preprocessing and aggregation component aims to reduce long-range communication burden by detecting and reducing these redundancies. This, however, requires this component to perform basic calculations on raw data (such as max, min, mean, and average), which inexorably increases the energy consumption of the node. However, as communication is notably more demanding than computation—in terms of energy consumption—data aggregation can lead to a notable reduction in the overall power dissipation. Similarly, rudimentary data preprocessing can be applied to raw data to eliminate outliers and erroneous samples. Particularly, if the resource availability of the concentrator allows it, early event detection techniques and feature extraction methods can result in major reductions in network traffic. The data aggregation and preprocessing introduce multiple challenges. For example, whether the energy consumption reductions caused by aggregating are enough to offset computation power demand remains dependent on the application. Multiple models, however, are proposed in the literature to evaluate these trade-offs [93]. Furthermore, aggregating faulty samples with normal ones can vitiate veracity of measurements, as one corrupt recording can contaminate the entire sample [94].

Cloudlet A new approach to hierarchal smart healthcare involves deployment of relatively powerful machines in the close vicinity of field devices [95]. Often termed

as *cloudlet*, these machines can execute complicated data processing algorithms, offer extensive long-term data storage, and manage network operation [96], thereby minimizing the dependence of the application on the cloud [97]. This architecture improves various aspects of the application. For example, reducing the physical distance among sensors, users, and servers increases various aspects of QoS. Additionally, cloudlet-based applications can resume their operation in the absence of Internet connectivity, thereby providing offline services.

3.3 Data Processing: Structure and Algorithms

Sophisticated data analysis algorithms form the engine that drives smart healthcare toward once-unimaginable boundaries. These algorithms, nonetheless, are demanding and require access to a vast pool of data gathered from various sources—some of it is even not part of smart healthcare sphere, e.g., AQ data, traffic status, social networks, etc. This naturally calls for cloud-based implementations. We dedicate this section to major characteristics of this cloud-based architecture, studying not only the implementation but also various services it offers.

Structure and Framework Centralized cloud-based servers are the mainstream approach for data processing; they can well satisfy the ever-increasing demand of reliable computation by providing resourceful, always-on, flexible, scalable, and affordable (by benefiting from economy of scale) data processing and storage platforms. It is important to acknowledge that the term *centralized* is used loosely in this context, as almost all cloud-based servers are structured by an interconnection of a multitude resourceful machines (sometimes, physically distant from each other). However, as such services are typically offered by the same entity (Cloud Service Provider (CSP)) under the same policy, we consider them as centralized units (as opposed to massively distributed m-health services). CSP and the administration that controls a smart healthcare application can be the same entities, which yields to a *private* cloud implementation. In contrary, it is often more affordable to lease a *public* server form third-party CSPs, which share their resources with a multitude of subscribers. This, however, poses various security and privacy concerns [98]. The list of public CSPs, which customers can choose from is ever growing, as now the major tech companies provide their own processing services, including the Google Cloud IoT platform [99], Microsoft Azure IoT [100], Amazon AWS [101], and IBM Watson IoT [102] to name a few. These services not only provide a hardware platform for hosting data storage and processing but also offer off-the-shelf data analytics algorithms, visualization tools, and a spectrum of APIs for controlling end-devices; hence paving the way for the softwarization of the data plane [103]. Finally, for applications that require a middle-ground, hybrid implementations can be suggested, where sensitive data are stored and processed in private servers while demanding algorithms and long-term storage of the bulk of data are outsourced to public servers [104].

Alternatively, the diffusion of computationally capable smart portable devices, such as smartphones and smartwatches, gives rise to nascent m-health architecture, where computations are offloaded to a large number of distributed, heterogeneous devices. By putting volunteering individuals in charge of the communication and processing, the m-health substantially depresses operating costs while giving rise to flexibility and scalability of the system (epically when paralleled with non-dedicated sensing [52]). Multiple drawbacks, however, can be associated with this implementation. Aside from complications of incentivizing individuals, security and privacy considerations must also be addressed. Furthermore, the high entropy in device properties and stochastic nature of the network make it substantially difficult to guarantee the availability of the system [105]. Further curbing the applicability of distributed approaches, not all data processing algorithms are executable in a massively parallel fashion.

Machine Intelligence Software Core Whether distributed or centralized, public or private, the cloud must provide two fundamental services (aside from data storage): (i) data analytics and (ii) data visualization.

Data analytics refers to machine learning [106] and deep learning algorithms that extract valuable information from the pile of apparently unrelated raw data, thereby facilitating decision making by performing the descriptive, diagnostic, predictive, and prescriptive analysis. The data processing component must deliver these services while meeting the 5Vs (Veracity, Volume, Velocity, Variety, and Value) [78] requirements of IoT applications. Additionally, considering the gravity of the task—which directly affects the well-being of users—the machine intelligence must deliver exceptional accuracy (particularly in terms of low false-negatives) as well as immunity to noise [107]. Once such a platform is established, invaluable services can be provided to users. For example, the study conducted in [108] uses Support Vector Machine (SVM) to categorize voices recorded by numerous sensors such as smartphones and voice recorders with the objective of detecting Parkinson's Diseases (PD) in early stages (as PD causes speech impairments). Multiple features such as lowest and highest frequencies, jitter, perturbation, and amplitude are used for the classification. The SVM is executed by a centralized server, which shares the processing results with a physician. Being incorporated with other smart city services, the server can also collect traffic information to facilitate access and expedite emergency response when required. The system proposed in [109] uses cameras to capture head images, from which various features such as head movements, blinking rate, and facial expressions are extracted. These features are then combined with data obtained from user's usage of social networks to classify their mood into three separate states [109]. Using logistic regression, the authors achieve an accuracy of almost 90%. Aiming to improve the efficiency of emergency rooms, the authors of [110] propose an RFID-based patient localization technique based on k-means and Random Forest. Using this hybrid approach, they report an accuracy of 98%, showing the efficacy and robustness of hybrid and hierarchal implementations. These example data analytics applications clearly accentuate the

integral role of machine intelligence in the consolidation of smart healthcare with other smart city applications.

In response to the growth of the m-health, many research works in the literature have investigated the distributed implementation of data analytics [111–113]. Particularly, clustering solutions evince great potential for distributed implementations. Nonetheless, such approaches negatively affect various aspects of the system, with the communication plane typically receiving the brunt of the performance degradation, as distributed algorithms heavily rely on data exchange among nodes. Finally, once processed, the information must be output to participants in forms of recommendations, action control, and particularly, visualization. An effective approach to the latter is rife with myriad complications. First, the massive size of the extracted information calls for data abstraction and summarization. For example, the study conducted in [31] proposes a novel visualization solution for condensing 24-h heart rate data into a simple graph, helping physicians detect Long QT (LQT) syndrome. Second, various participants of the e-health system seek different information; therefore, data visualized for (say) patients differ substantially from those prepared for physicians. These two requirements necessitate a *hierarchal* and *personalized* presentation.

4 Smart Healthcare Vulnerabilities

Aside from its myriad advantages, the diffusion of smart healthcare (and IoT in general) in various dimensions of our healthcare system brings about multiple detrimental side effects. Particularly, by increasing the *attack surface*, this transition leaves security, safety, and privacy of the users vulnerable to cyberattacks. The extent of these vulnerabilities ranges from security flaws in individual smart devices to weaknesses in underlying infrastructures such as hospitals. For example, in 2017, Food and Drug Administration (FDA) issued a warning regarding the susceptibility of pacemakers and cardiac devices to intrusion and privacy breaches [114]. Fortunately, no specific attack exploiting these flaws was reported; nonetheless, considering the gravity of these devices to patients, such security threats cause genuine concerns and retard proliferation of smart healthcare devices.

Further adding to the security and privacy concerns, an increasing number of attacks are now targeting underlying health infrastructures. For example, in 2017, attackers used a ransomware to cut access to computers in a hospital in Los Angeles [115]. The hospital regained access only after paying $17,000 to the attackers. Although this incident did not directly threat hospitalized patients, it interfered with the admittance of new patients to the emergency center. Even more unsettling, in the same year, the so-called *WannaCry* ransomware affected UK's National Health Services (NHS), which led to "massive shutdowns and inconveniences to the country's health care infrastructure" [116]. Similar extortion-oriented attacks have been reported across the globe [117], including a $55,000 ransom attack to a hospital in Greenfield, Indiana in 2018 [114]. Indeed, the

interwoven structure of smart healthcare further exacerbates the situation, as the dispersion of even seemingly insignificant data can create security considerations. For example, it is known that fitness-related data can reveal sensitive information pertaining to military zones [118].

Considering the smart healthcare's inflating sphere of influence, it can be expected that the frequency and extent of such attacks continue to increase for the foreseeable future. This can depress the social acceptance of such applications and impede the prevalence of smart healthcare and its many advantages. Consequently, a massive amount of effort has been undertaken to strengthen the security and privacy aspects of this domain. These efforts can be subsumed under technical and non-technical (social) categories. The former involves applying security preserving techniques to different components of the architecture shown in Fig. 2, while the latter includes regulations passed by policymakers to legally oblige system developers to protect the privacy and security of their users. Health Insurance Portability and Accountability Act (HIPAA) and the European Data Protection Directive 95/46/EC [119] are the most eminent examples of such regulations. In this chapter, we focus on the former category.

The underlying contributing factor to security and privacy vulnerabilities of smart health can be ascribed to the service-oriented design approach of developers, who oftentimes neglect the security aspects of their systems to expedite the development and employment process. Still being its infancy, many smart healthcare products and services—whether commercial or not—are developed somehow as proof-of-concept prototypes to assess the feasibility of new ideas and evaluate their social acceptance. Furthermore, unlike performance metrics such as battery life, memory size, and physical dimensions, the security and privacy metrics are difficult to quantify and advertise [120]. This leaves some producers reluctant to heavily invest in these areas. It is, therefore, not surprising to see that many of these products regard security and privacy as *features* rather than an integral part of the system [121].

Although the maturity of IoT coupled with the rising awareness about security (fueled by recent attacks) has mitigated this problem to some extent, older vulnerable devices entail long-lasting repercussions by adding to the security *heterogeneity* of the system. The security heterogeneity is a multi-faceted problem that substantially complicates the fulfillment of a protective initiative. Following the preceding discussion, one aspect of this non-uniformity can be associated with the amalgamation of the older generation and insecure devices with newer (typically) secure ones. By creating weak links, this provides adversaries with the opportunity to exploit vulnerabilities of the former group to compromise the entire network. From another perspective, this heterogeneity evinces itself in data and user access requirements [122]; some data are inherently more sensitive than others. For example, video and audio-based information are more prone to attacks than air quality parameters. Nonetheless, when fused together, even unimportant data can disclose critical information about users [118]. User non-uniformity implies that a complex smart healthcare system involves numerous stakeholders from patients to their physicians to insurance companies to emergency units. These users

require various levels of data access, which often change dynamically based on the context [123]. Indeed, managing these heterogeneities is an onerous task.

Addressing these intricate security and privacy considerations in the smart city must be carried out in accordance with the limited resource availability of smart sensors, implying that many existing sophisticated techniques are not applicable to smart healthcare applications. This adds another dimension to the security and privacy problem, where these requirements must be met without adversely affecting the experience of the user. This dimension is sometimes referred to as *Quality of Protection* (*QoP*) [124]. Additionally, aside from intentional cyberattacks, smart health applications must also offer higher reliability, resilience, and self-healing features. Finally, even devices with robust security mechanisms may fail to protect users' data, unless both users and system administrators meticulously enforce security recommendations [120]. Increasing the awareness among various stakeholders is, therefore, critical to any holistic security framework.

The standardization of security and privacy protection mechanisms poses yet another challenge in securing smart healthcare services. Currently, the available solutions are highly fragmented, as a universal standard is yet to be adopted. This fragmentation occurs in each service of the smart city (including smart healthcare) but the problem will be more pronounced in entangled future ecosystems that involve a wide variety of smart city services. Indeed, the emergence of higher-level security services provided by CoAP, DTLS, IPSec, etc. can partially abate these concerns. Nonetheless, interoperable access control, identification, authentication, and trustworthiness assessment are yet to emerge. The major policymakers and standardization groups are aware of these shortcomings and have undertaken various efforts to standardize IoT security (e.g., ITU-T Y.2060, Y.2066, Y.2067, Y. 2075, etc. [125]). Particularly, ITU-T Y.2075 and ITU-T H860 target smart healthcare applications, the former defines the requirements for e-health monitoring, while the latter regulates multimedia data exchange [126].

Any effective protective solution must overcome the aforesaid challenges to satisfy various requirements that are subsumed under the general term, *security*, including [127, 128]:

- *Confidentiality* protects data against privacy leaks, eavesdropping, and unauthorized access.
- *Availability* implies that data must be made available to authorized users at their behest with least amount of delay possible.
- *Data integrity* detects and amends data manipulations, either intentional (caused by adversaries) or unintentional (caused by networking errors) ones.
- *Interoperability* facilitates authorized information sharing among various participants of the healthcare system.
- *Identification* limits the data access to the authorized users.
- *Authorization* verifies the legitimacy of data and users.
- *Data loss immunity* enables the system to recover to its original state after a partial loss of data.
- *Privacy* cuts access to the data for the irrelevant users.

Smart healthcare applications are particularly vulnerable to identity-based attacks. Unfortunately, traditional PIN-based authentication techniques are proven to be inadequate in many applications considering that (i) smart healthcare ecosystems involve a large number of stakeholders and (ii) many users are elderly, who might not easily remember their credentials. Various solutions are proposed to relax this requirement (e.g., using RFID tags [129]). In addition to identity-based threats, many smart healthcare systems are vulnerable to service attacks (Denial of Service), which can result in catastrophic consequences [130]. The following sections provide a more detailed study of some of the major threat models in smart healthcare applications.

5 Security and Privacy of Field Devices

As discussed in Sect. 4, regarding security and privacy protection mechanisms as supplementary *features* is the underlying cause of many existing vulnerabilities. Instead, security must be incorporated in the early phases of the design process as an integral component of the system. Furthermore, because it is the weakest link that determines the overall robustness of the system, any attempt to ensure security and protect privacy must include all components of the system. This latter consideration, however, is typically neglected, as developers often focus on the security of the communication and omit other components.

Cryptography is the backbone of the security and privacy protection in the sensing and communication planes. Particularly, taking advantage of its simplicity, many smart sensors are equipped with built-in Advanced Encryption Standard (AES) accelerators [131]. In case a more robust encryption is required, algorithms that use Elliptic Curve Cryptography (ECC), such as Elliptic Curve Digital Signature (ECDSA), can be employed. ECC security matches RSA, however, utilizing smaller keys renders it less resource demanding. ECDSA, however, involves complicated verification procedures, which shifts the computation burden to the cloud side [132]. These cryptography-based approaches can well improve device security against a wide variety of software-based attacks. However, they are oftentimes ineffective against hardware and side channel attacks. Additionally, many of these solutions are susceptible to attacks carried out by insiders [133].

5.1 Common Threats and Proposed Solutions

This section analyzes some of the major threats and the proposed solutions for ensuring security and privacy of field devices, by focusing on sensing and communication components. Instead of targeting the entirety of the system, most of the vulnerabilities studied in this section correspond with the system's individual components or at most aim at the underlying data collection network (as opposed

to enforcing access control, identification, and authentication that involve higher-level component of the system (e.g., cloud), which are discussed in Sect. 6). The relative parochial scope of these threats, however, does not translate to ineffectiveness. Although we have separated the solutions and threats into two sections, a comprehensive security package must be uniformly spread over all levels.

Node capture involves insider adversaries tampering a node in the network, oftentimes through hardware changes (including uploading code through debugging pins or soldering hardware pieces to the device). Therefore, it requires physical access to the device. Once compromised, the adversary can read the memory content of the captured node, make it generate false data, or gain full control over its operation, which allows them to perform insider attacks targeting the entire network. Firmware verification—particularly hardware-based solutions that rely on Trusted Platform Modules [134]—and limiting access to debugging pins can provide some degree of immunity to such attacks [135].

Node replication is based on secret key information gained from captured nodes, which allows the adversary to insert multiple compromised nodes into the network mimicking the identity and credentials of the captured device. Replicated nodes (imposters) can generate wrong data, perform selective packet forwarding, and conduct sinkhole attacks [128]. Typically, location-based solutions, where neighbors of a node attest its legitimacy are used for detecting imposters. Network mobility and colluding replicas, however, can render these solutions rather impotent. More robust approaches, such as token exchange based on Artificial Immune System (AIS) can mitigate these problems [136].

Injection attacks involve adversaries uploading malicious firmware to the device (code injection) or tampering with nodes to generate incorrect data (data injection). The former can be mitigated by checking the validity of the firmware, whereas the latter is typically detected by "estimators" [133]. An estimator contrasts the values generated by a senor with the expected values. A substantial and persistent deviation from expected values indicates an attack. The efficacy of such solutions, however, is limited when adversaries have some familiarity with the network and the expected values. More sophisticated estimators based on Kalman filter and machine learning solutions are proposed in the literature to address these limitations [137, 138]. Injection attacks are particularly common in smart healthcare applications. For example, the study conducted in [139] shows the susceptibility of BLE (arguably, the most prevalent communication in smart healthcare applications) to these attacks.

Side channel attacks are carried out by inspecting parameters such as execution time, power consumption, and cache access patterns to gain information about sensitive information (e.g., secret keys). Side channel attacks can then render software-based encryption techniques rather ineffective. Decreasing the correlation between the key size and computations (such as Montgomery's multiplication [140]) as well as randomizing calculations [141] can substantially improve the immunity of the system against side-channel attacks [131].

Jamming is a well-known type of Denial of Service (DoS) attacks, which targets system's availability. To achieve this, adversaries use jammer devices to generate random RF signals that intentionally cause interference with data transmission,

thereby decreasing the Signal-to-Noise Ratio (SNR). The complexity of jamming attacks increases with the knowledge of the adversaries about the network, which allows them to adjust their attack to the network's reaction. Countervailing jamming in such scenarios often involves game theory-based solutions that aim to detect an equilibrium between adversary's actions and network reactions [142]. Such solutions, however, typically take a toll on sensors' computational load and their energy consumption demands.

Denial of sleep (DoSL) is a link layer variant of DoS attacks. In DoSL, the adversary exploits security flaws to create packet collision, message overhearing, and idle listening to increase the energy consumption of smart sensors. Additionally, these attacks can be carried out simply by sending consecutive Request to Send (RTS) messages. DoSL accelerates battery drain. Knowing that battery replacement in many WSNs is cost prohibitive, this can lead to imminent shut down of such networks [143]. Securing the network against DoSL typically revolves around authentication and anti-replay mechanisms [144].

Vampire attacks reduce networks' expected lifetime by gradually draining sensors' batteries. Two aspects differentiate this attack from DoSL and resource exhaustion attacks; first, it typically targets long-term availability of the network and second, it exploits vulnerabilities of the network layer. Particularly, the malicious nodes generate and transmit packets that require higher-than-average routing and processing (e.g., by creating loops or establishing longer routes), hence increasing the power dissipation of the network. Vampire attacks can be mitigated by loop detection routing algorithms and optimal route re-computation as well as clean slate sensor routing protocols [145].

Black hole is a network layer DoS attack, where a malicious node exploits vulnerabilities in routing protocols such as Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) to broadcast a fake shortest path to a destination. Eventually, this results in all the packets generated by the network to be redirected to the compromised node. The malicious device can then drop these packets (black hole attack) or forward a select number of them (selective black hole attack). Various solutions are proposed in the literature to countermeasure black hole attacks including sending data through multiple paths and establishing trusted routes based on the packet delivery ratio. Such solutions, however, increase power demand of the system and add to its complexity [146].

Man-in-the-middle, or equivalently *manipulation* [147], describes (typically) network layer data manipulation attacks, where an adversary alters data traveling from its source to destination. Particularly, joining procedure of new devices to the network is known to be susceptible to such attacks [148]. This is indeed a major challenge for smart healthcare systems as their dynamism implies frequent inclusion and exclusion of devices, providing adversaries ample opportunities to compromise the data. Network robustness against man-in-the-middle attacks can be increased by employing data encryption techniques (either symmetric or asymmetric), network layer authentication, and digest algorithms [149].

5.2 Specificities of Smart Healthcare Applications

A majority of the vulnerabilities discussed in Sect. 5.1 are inherited from IoT-based nature of modern smart healthcare applications. In addition to these vulnerabilities, there still exists a wide range of security concerns that directly stem from immanent characteristics of smart healthcare. Particularly, extent and diversity of smart healthcare systems are proven to be the root cause of many such threats. A practical healthcare system likely relies on users conventional smart devices such as smartphones and smartwatches to collect and relay data. These devices forward information to the cloud using a heterogeneous communication network that involves home and public WiFi as well as cellular communication. This creates ample opportunity for adversaries to compromise the system. For example, many smart existing services revolve around Android-powered devices. The conducted studies in [150] show how adversaries can steal critical information from these devices using screen-shot attacks. Additionally, it is known that WiFi and ZigBee (two most commonly-used communication technologies in WBAN) can be compromised using man-in-the-middle, DDos, and replay attacks [151]. Therefore, due to this heterogeneity, providing end-to-end security is oftentimes augmented by employing higher-level encryption (e.g., Constraint Application Protocol (CoAP) [152] in the application layer and IPSec and Datagram Transport Layer Security (DTLS) [153] in the transport layer). Lower level security solutions are also available. For example, IPv6 over Low power Wireless Personal Area Network (6LoPAN) uses AES to provide authentication and confidentiality (by adjusting the Auxiliary Security Header). Although effective, many of these solutions substantially increase power demand of existing healthcare devices. There are some existing works in the literature that aim to address this limitation by outsourcing demanding computations of these algorithms to more resourceful devices such as gateways [154].

5.3 Summary

This discussion of a select number of cyberattacks clearly shows their diversity, which evinces itself in terms of exploited vulnerabilities (hardware and software), adversaries intentions (e.g., crippling the network or stealing data), targeted layers (e.g., physical, link, and network), scale and possible repercussions. Emerging sensing and processing paradigms such as crowd-sensing and edge-processing further complicate smart healthcare security equation by adding additional unknowns such as participant trustworthiness [155]. Table 3 summarizes our discussion about crypto-level security concerns in smart healthcare applications.

Table 3 Summary of some threats against sensing and communication components of smart healthcare, their repercussions, and common solutions

Attacks	Target		Repercussions	Proposed solutions
	HW	SW		
Node capture	✓	✗	False data generation Secret key leakage Basis for other attacks	Limiting access to debugging pins/firmware verification (SW or HW)
Node replication	✓	✗	False data generation Basis for sink hole attack Packet drop	Neighbor attestation/toke exchange
Injection	✓	✗	False data generation Basis for node capture attack	Data verification by estimators
Jamming	✓	✗	Degraded QoS Increased energy demand Packet drop	Game theoretic traffic analysis
Side channel	✓	✓	Secret key leakage	Montgomery's multiplication/randomizing computations
DoSL	✗	✓	Battery drain	Authentication/replay attack protection
Vampire	✗	✓	Gradual battery drain	Routing loop detection/clean slate sensor routing
Black hole	✗	✓	Gradual battery drain Packet loss Privacy leakage	Multi-path routing/establishing trusted routes
Man in the middle	✗	✓	False data injection Packet loss Privacy leakage	Data encryption/authentication/digest algorithms

6 Access Control, Identification, and Authentication

The diffusion of cloud-based computing in smart healthcare systems explicitly implies a separation between data's host (where data is processed and stored) and their generators (users). Considering that cloud-based servers are typically owned and controlled by third-party entities, such separation causes genuine security and privacy concerns. Furthermore, taking advantage of economies of scale, cloud resources are shared among various applications and services, which increases incidents of privacy leakage and provides more opportunities for adversaries to compromise the system's security. In addition to protecting data against the threats discussed in Sect. 5, an impervious security system cannot be established without overcoming cloud security challenges.

A comprehensive protecting solution must be spread over all functionality of the cloud [156]: data processing, data retrieval, and data storage. The first requirement can be satisfied by Fully Homomorphic Cryptography (FHC) techniques, which allow computation on encrypted data [157, 158]. FHC, however, is computationally complex even for powerful cloud-based servers. Ensuring security of data during retrieval and storage is typically addressed by identification, authorization, and access control mechanisms. Scale, dynamism, and complexity of healthcare systems render many traditional solutions impractical. Hence, this field calls for innovative solutions, which we investigate in detail in this section.

6.1 Access Control

Traditional access control mechanisms (based on RSA, AES, and IDEA) are developed to provide secure one-to-one data sharing, which makes them suitable for classic applications such as file transfer and email exchange. The requirements of modern smart healthcare platforms, however, differ significantly from these traditional services, which involve a large number of participants with highly dynamic access privileges, which change with roles, time, location, etc. [159]. Indeed, multiple copies of data can be created to implement more resilient data sharing paradigms based on the traditional techniques; nonetheless, the sheer scale of the smart healthcare renders such approaches impractical. Attribute-Based Access Control (ABAC) can satisfy this requirement. Based on Attribute-Based Encryption (ABE, also called Fuzzy Identity-Based Encryption) [160], ABAC utilizes users' attributes (e.g., location, profession, affiliation, etc.) to create private keys. Therefore, the combination of various attributes allows fine-grained access control management. For example, the authors in [161] develop a cloud-based framework for ABE-based personal health record sharing that manages access control among various owners and users (including patients, physicians, family members, pharmacies, etc.). The proposed solution also provides attribute revocation (a user's access to a record must be terminated as soon as their attributes change) and relies on honest but curious servers.

6.2 Identification and Authentication

A robust authentication mechanism must ensure protection against a multitude of attacks including eavesdropping, online and offline password guessing, spoofing, man-in-the-middle, replay, and dictionary attacks. Even a single vulnerability against one of these threats suffices to undermine the overall efficacy of the authentication mechanism. This comprehensiveness inexorably entails hybrid solutions, as developing a non-hybrid solution capable of satisfying all these requirements is proven to be cumbersome. Additionally, authentication techniques must comply with immanent characteristics of eHealth cloud, particularly its distributed and multi-server implementation [162], while offering simple and secure account recovery as well as system restoration after disasters and breaches [163].

Traditionally, the authentication is carried out using passwords, which can always be stolen and guessed (especially low-entropy ones). Alternatively, two-factor authentication can address some of these concerns, where in addition to passwords, users must insert a smart card to verify their identity. This prevents passwords guessing, stealing, and sharing, as there is only a single card per user. This remote-access identity-based verification mechanism, however, is still susceptible to eavesdropping, password guessing, and smart key stealing [164]. Addressing these limitations, emerging biometrics-based solutions use physiological parameters (e.g., fingerprints, facial features, etc.) to identify and authenticate users. Additionally, in response to nascent trends in the digital health domain, such as socialization of smart objects [165] and their interplay with social media [166], biometrics-based solutions can now authenticate users based on their behavioral patterns including their use of social networks [167] and handwriting [168]. These two approaches are also referred to as *hard* and *soft* biometrics-based authentication [169]. Strong protection can be maintained by a hybrid utilization of both the behavioral and biometrics-based authentication, as opposed to replacing one with the other.

Maximizing the security robustness of smart healthcare systems, various three-factor authentication mechanisms, based on passwords, smart cards, and biometrics have been proposed in the literature. Utilizing strong encryption mechanism such as RSA, ECC, and Hash function (ECC is typically preferred due to its strong protection and small key size) under the hood, the three-factor authentication can provide immunity against a variety of attacks including guessing, eavesdropping, intercept, replay to name a few [170]. Aside from its many advantages, three-factor authentication is rather a complicated system, which impedes its widespread proliferation among the elderly and disabled. Both groups are major participants in healthcare systems. This calls for alternative approaches that are user-friendly and independent from peripheral devices such as smartphones and card readers. To this end, various ambient sensors (e.g., cameras and RFID) can extract users' biometrics to authenticate them, thereby creating a naked environment, where interactions between users and the environment take place directly and continuously [171].

6.3 Data Trustworthiness

The system's heterogeneity coupled with a large number of stakeholders in a typical smart healthcare application introduces an extra dimension in data security and privacy: *data trustworthiness*. Intentional (by adversaries) and unintentional (e.g., by faulty devices) incidents can inject fallible data in smart healthcare applications. Due to the gravity of the task, it is necessary to evaluate and assess the *trustworthiness* of the collected data. This problem is particularly emphasized in crowd-sensing applications. Two key factors determine data trustworthiness. The first one is ascribed to the accuracy of the sensors (typically embedded into participants' smart devices), while the second is typically associated with their *reputation* [172]. Social Network-Aided Trustworthiness Assurance (SONATA) is a notable solution to evaluate data trustworthiness in a crowd-sensing application [173]. In this solution, a community of participants that perform the same sensing task is used to evaluate trustworthiness through a voting-based approach, dynamically. The study conducted in [174] uses a similar approach, however, the authors further increase the reliability of the voting process by increasing the *voting clout* of a group of selected trustworthy participants.

Aside from the preceding discussion, the recent incidents regarding the privacy violation of users by some of the major services providers have also added a new aspect to trustworthiness in IoT and smart healthcare systems. In fact, many users and system administrators now prefer to sever their reliance on third-party service providers. This has inexorably motivated the emergence of decentralized solutions. Particularly, block-chain services are expected to play a significant role for securely storing medical records on a distributed platform. Existing research has proven the efficacy of block-chain technology in protecting users' privacy and security [175].

7 Future Directions and Open Issues

Although the current smart healthcare services are fragmented and disjoint, the newest trends and developments in IoT and the smart city hint at an imminent fusion of services and applications into a unified ecosystem. Multiple trends fuel this unification including (but not limited to) the prevalence of smart wearables and crowd-sensing platforms, the emergence of electric vehicles and smart home services, the growth of machine learning and deep learning algorithms, the advancements of cloud and fog computing, etc. To these, one should also add societal developments such as the global aging population, increasing technology-awareness in eastern and southern Asia, as well ever increasing market dominance of some technology giants. Establishing such an ecosystem, however, is contingent upon guaranteeing interoperability among myriad components of smart cities, which for years has been the bane of IoT-based services.

There are multiple emerging technologies that can facilitate interoperability in the context of smart healthcare and the smart city. For example, 5G has the potential to overcome the fragmentation in communication technologies, particularly, considering its intrinsic compatibility with existing common Radio Access Technologies (such as WiFi) using the Licensed Assisted Technology (LAA) [176]. When coupled with the profusion of smart wearable devices, it is not unreasonable to imagine that BLE/5G will be the de facto approach for short and long range communication, respectively.

Equivalently impressive is the evolution of the blockchain technology, which simultaneously addresses the security concerns and the challenges regarding the data storage and sharing in smart healthcare services. Additionally, this technology can pave the way to further the adoption of fog computing, which is yet another major pillar for future smart healthcare ecosystem. Despite its increasing popularity, however, the adoption of blockchain technology faces various challenges including ensuring the interoperability among different blockchains, protecting the security of the data when at least 50% of the network is compromised, and evaluating the trustworthiness of information [177].

In addition to the aforementioned challenges, standardization and security remain the main deterrence against the growth of smart healthcare ecosystem. Although multiple efforts have been undertaken to standardize data communication, sensing, storage, and processing are often get neglected, which negatively impacts the integration of services in these levels. The unification of smart healthcare services with each other, as well as sundry smart city applications, also exacerbates security and privacy concerns as it complicates the existing attack surface. Unfortunately, many major stakeholders fail to properly incorporate a comprehensive security protection system in their designs (perhaps because in some cases companies short-term financial interests are in contrast with their customers or maybe privacy and security features are not as *advertisable* as performance metrics). Despite the remarkable advancements in communication component, preserving security and privacy for effectively sharing and processing information still remains the major hindrance against the proliferation of ubiquitous smart healthcare.

8 Summary and Concluding Remarks

Despite their relatively short life, fledgling smart healthcare systems have evolved from simple monitoring services with a limited number of sensors to now complicated multi-faceted and multi-dimensional systems, that are interwoven seamlessly with various aspects of our lives in the post-ICT era. This article is dedicated to unraveling major enablers that have contributed to this transition, spanning from technical breakthroughs to their security and privacy repercussions. Emphasizing the convergence of various smart city applications into a unified ecosystem and focusing on the security and privacy ramifications of such trends, we study modern smart healthcare systems from the standpoint of the following aspects:

(i) Application, where we investigate existing works to show how clinical grade, fitness-related, and infrastructure applications are evolving and merging to form a unified healthcare ecosystem.
(ii) Architecture, where we discuss underlying technical advances that have fueled the evolution of the smart healthcare. We explain how the maturity of sensing devices has made available to our disposal a wide spectrum of inexpensive, resourceful, noninvasive, and bio-compatible sensors. To this, we should add viable alternatives such as crowd-sensing, which substantially reduce the expenses of large-scale sensing platforms. Additionally, we detail the contribution of emerging low-power and high-rate communication such as BLE to a reduction in communication expenses. Furthermore, we provide an analysis of the critical role of machine learning and deep learning algorithms in the realization of the smart healthcare ecosystem.
(iii) Vulnerabilities, where we examine the most recent cyberattacks targeting actual implementations to identify major vulnerabilities and weaknesses of smart healthcare applications.
(iv) Crypto-level security, where we detail security flaws of the sensing and communication components of the smart healthcare, with an emphasis on less conventional hardware and software attacks carried out by insiders.
(v) System-level security, where we address the vulnerabilities of the cloud, myriad challenges it faces in quest of protecting users' security and privacy, as well as the proposed solutions and their associated advantages and disadvantages.

Our study concludes by arguing that nothing more than security and privacy considerations blocks the path toward the realization of the future healthcare ecosystem. This concern can only be mitigated by implementing security protection mechanisms as an integral part of the system, added to the design in early stages, and spread uniformly over every single component of the system.

References

1. C.J. Truffer, S. Keehan, S. Smith, J. Cylus, A. Sisko, J.A. Poisal, J. Lizonitz, M.K. Clemens, Health spending projections through 2019: the recession's impact continues. Health Aff. **29**(3), 522–529 (2010)
2. D. Stuckler, S. Basu, M. Suhrcke, A. Coutts, M. McKee, The public health effect of economic crises and alternative policy responses in Europe: an empirical analysis. Lancet **374**(9686), 315–323 (2009)
3. J. Andreu-Perez, D.R. Leff, H.M.D. Ip, G.Z. Yang, From wearable sensors to smart implants-toward pervasive and personalized healthcare. IEEE Trans. Biomed. Eng. **62**(12), 2750–2762 (2015)
4. L.E. Hebert, P.A. Scherr, J.L. Bienias, D.A. Bennett, D.A. Evans, Alzheimer disease in the us population: prevalence estimates using the 2000 census. Arch. Neurol. **60**(8), 1119–1122 (2003)
5. M. Estai, Y. Kanagasingam, M. Tennant, S. Bunt, A systematic review of the research evidence for the benefits of teledentistry. J. Telemed. Telecare **24**(3), 147–156 (2017). 1357633X16689433

6. K.A. Al Mamun, M. Alhussein, K. Sailunaz, M.S. Islam, Cloud based framework for Parkinson's disease diagnosis and monitoring system for remote healthcare applications. Futur. Gener. Comput. Syst. **66**, 36–47 (2017)
7. A. Page, M. Hassanalieragh, T. Soyata, M.K. Aktas, B. Kantarci, S. Andreescu, Conceptualizing a real-time remote cardiac health monitoring system, in *Enabling Real-Time Mobile Cloud Computing Through Emerging Technologies*, ed. by T. Soyata (IGI Global, Hershey, 2015), pp. 1–34
8. F. Casino, C. Patsakis, E. Batista, F. Borràs, A. Martínez-Ballesté, Healthy routes in the smart city: a context-aware mobile recommender. IEEE Softw. **34**(6), 42–47 (2017)
9. B. Reeder, A. David, Health at hand: a systematic review of smart watch uses for health and wellness. J. Biomed. Inform. **63**, 269–276 (2016)
10. J. Tavares, T. Oliveira, Electronic health record patient portal adoption by health care consumers: an acceptance model and survey. J. Med. Internet Res. **18**(3), e49 (2016)
11. G. Manogaran, R. Varatharajan, D. Lopez, P.M. Kumar, R. Sundarasekar, C. Thota, A new architecture of internet of things and big data ecosystem for secured smart healthcare monitoring and alerting system. Futur. Gener. Comput. Syst. **82**, 375–387 (2018)
12. G. Muhammad, M. Alsulaiman, S.U. Amin, A. Ghoneim, M.F. Alhamid, A facial-expression monitoring system for improved healthcare in smart cities. IEEE Access **5**, 10871–10881 (2017)
13. E. Spanò, S.D. Pascoli, G. Iannaccone, Low-power wearable ECG monitoring system for multiple-patient remote monitoring. IEEE Sens. J. **16**(13), 5452–5462 (2016)
14. H. Samani, R. Zhu, Robotic automated external defibrillator ambulance for emergency medical service in smart cities. IEEE Access **4**, 268–283 (2016)
15. R. Sundar, S. Hebbar, V. Golla, Implementing intelligent traffic control system for congestion control, ambulance clearance, and stolen vehicle detection. IEEE Sens. J. **15**(2), 1109–1113 (2015)
16. F. Mwasilu, J.J. Justo, E.K. Kim, T.D. Do, J.W. Jung, Electric vehicles and smart grid interaction: a review on vehicle to grid and renewable energy sources integration. Renew. Sustain. Energy Rev. **34**, 501–516 (2014)
17. A. Alaiad, L. Zhou, Patients' Adoption of WSN-Based Smart Home Healthcare Systems: An Integrated Model of Facilitators and Barriers. IEEE Transactions on Professional Communication **60**(1), 4–23 (2017)
18. A.L. Young, M. Yung, Cryptovirology: the birth, neglect, and explosion of ransomware. Commun. ACM **60**(7), 24–26 (2017)
19. A. Page, S. Hijazi, D. Askan, B. Kantarci, T. Soyata, Research directions in cloud-based decision support systems for health monitoring using Internet-of-Things driven data acquisition. Int. J. Serv. Comput. **4**(4), 18–34 (2016)
20. American Diabetes Association, About Us: American Diabetes Association. http://www.diabetes.org/ Accessed 02 August 2018
21. P. Kakria, N.K. Tripathi, P. Kitipawang, A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors. Int. J. Telemed. Appl. **2015**, 8:8–8:8 (2015)
22. American Heart Association, Building healthier lives free of cardiovascular diseases and strokes. http://www.heart.org/HEARTORG/ Accessed 02 August 2018
23. R. Pandey, N.C. Dingari, N. Spegazzini, R.R. Dasari, G.L. Horowitz, I. Barman, Emerging trends in optical sensing of glycemic markers for diabetes monitoring. Trends Anal. Chem. **64**, 100–108 (2015)
24. O. Arias, K. Ly, Y. Jin, *Security and Privacy in IoT Era* (Springer, Cham, 2018), pp. 351–378
25. U.E. Bauer, P.A. Briss, R.A. Goodman, B.A. Bowman, Prevention of chronic disease in the 21st century: elimination of the leading preventable causes of premature death and disability in the USA. Lancet **384**(9937), 45–52 (2014)
26. B. Veeravalli, C.J. Deepu, D. Ngo, *Real-Time, Personalized Anomaly Detection in Streaming Data for Wearable Healthcare Devices* (Springer, Cham, 2017), pp. 403–426

27. X. Wang, Q. Gui, B. Liu, Z. Jin, Y. Chen, Enabling smart personalized healthcare: a hybrid mobile-cloud approach for ECG telemonitoring. IEEE J. Biomed. Health Inform. **18**(3), 739–745 (2014)
28. M. Chen, Y. Ma, J. Song, C.F. Lai, B. Hu, Smart clothing: connecting human with clouds and big data for sustainable health monitoring. Mobile Netw. Appl. **21**(5), 825–845 (2016)
29. V.L. West, D. Borland, W.E. Hammond, Innovative information visualization of electronic health record data: a systematic review. J. Am. Med. Inform. Assoc. **22**(2), 330–339 (2014)
30. A. Page, T. Soyata, J. Couderc, M. Aktas, B. Kantarci, S. Andreescu, Visualization of health monitoring data acquired from distributed sensors for multiple patients, in *IEEE Global Telecommunications Conference*, San Diego (2015), pp. 1–7
31. A. Page, M.K. Aktas, T. Soyata, W. Zareba, J. Couderc, QT clock to improve detection of QT prolongation in long QT syndrome patients. Heart Rhythm **13**(1), 190–198 (2016)
32. G. Fico, A. Fioravanti, M.T. Arredondo, J. Gorman, C. Diazzi, G. Arcuri, C. Conti, G. Pirini, Integration of personalized healthcare pathways in an ICT platform for diabetes managements: a small-scale exploratory study. IEEE J. Biomed. Health Inform. **20**(1) (2016), pp. 29–38
33. J.Y. Lucisano, T.L. Routh, J.T. Lin, D.A. Gough, Glucose monitoring in individuals with diabetes using a long-term implanted sensor/telemetry system and model. IEEE Trans. Biomed. Eng. **64**(9), 1982–1993 (2017)
34. J.D. Stewart, Foot drop: where, why and what to do? Pract. Neurol. **8**(3), 158–169 (2008)
35. M. Abtahi, S. Barlow, M. Constant, N. Gomes, O. Tully, S. D'Andrea, K. Mankodiya, MagicSox: an E-textile IoT system to quantify gait abnormalities. Smart Health **5–6**, 4–14 (2017)
36. A.C.B. Garcia, A.S. Vivacqua, N. Sánchez-Pi, L. Martí, J.M. Molina, Crowd-based ambient assisted living to monitor the elderly's health outdoors. IEEE Softw. **34**(6), 53–57 (2017)
37. M. da Silva Cameirão, S. Bermúdez i Badia, E. Duarte, P.F. Verschure, Virtual reality based rehabilitation speeds up functional recovery of the upper extremities after stroke: a randomized controlled pilot study in the acute phase of stroke using the rehabilitation gaming system. Restor. Neurol. Neurosci. **29**(5), 287–298 (2011)
38. P. Standen, K. Threapleton, A. Richardson, L. Connell, D. Brown, S. Battersby, F. Platts, A. Burton, A low cost virtual reality system for home based rehabilitation of the arm following stroke: a randomised controlled feasibility trial. Clin. Rehabil. **31**(3), 340–350 (2017). PMID: 27029939
39. N.H. Alkahtani, S. Almohsen, N.M. Alkahtani, G. Abdullah Almalki, S.S.Meshref, H. Kurdi, A semantic multi-agent system to exchange information between hospitals. Procedia Comput. Sci. **109**, 704–709 (2017). 8th International Conference on Ambient Systems, Networks and Technologies, ANT-2017 and the 7th International Conference on Sustainable Energy Information Technology, SEIT 2017, 16–19 May 2017, Madeira, Portugal
40. M.S. Hossain, G. Muhammad, Cloud-assisted industrial Internet of Things (IIoT) – enabled framework for health monitoring. Comput. Netw. **101**, 192–202 (2016). Industrial Technologies and Applications for the Internet of Things
41. X. Chen, L. Wang, J. Ding, N. Thomas, Patient flow scheduling and capacity planning in a smart hospital environment. IEEE Access **4**, 135–148 (2016)
42. A. Alessa, M. Faezipour, A review of influenza detection and prediction through social networking sites. Theor. Biol. Med. Model. **15**(1), 2 (2018)
43. L. Fernandez-Luque, M. Imran, Humanitarian health computing using artificial intelligence and social media: a narrative literature review. Int. J. Med. Inform. **114**, 136–142 (2018)
44. M.A. Al-Taee, W. Al-Nuaimy, Z.J. Muhsin, A. Al-Ataby, Robot assistant in management of diabetes in children based on the internet of things. IEEE Internet Things J. **4**(2), 437–445 (2017)
45. A.G. Ferreira, D. Fernandes, S. Branco, J.L. Monteiro, J. Cabral, A.P. Catarino, A.M. Rocha, A smart wearable system for sudden infant death syndrome monitoring, in *2016 IEEE International Conference on Industrial Technology (ICIT)* (2016), pp. 1920–1925

46. G. Janjua, D. Guldenring, D. Finlay, J. McLaughlin, Wireless chest wearable vital sign monitoring platform for hypertension, in *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* (2017), pp. 821–824
47. K. Kaiya, A. Koyama, Design and implementation of meal information collection system using IoT wireless tags, in *2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)* (2016), pp. 503–508
48. S. Clarke, L.G. Jaimes, M.A. Labrador, mStress: a mobile recommender system for just-in-time interventions for stress, in *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)* (2017), pp. 1–5
49. A. Gomez-Sacristan, M.A. Rodriguez-Hernandez, V. Sempere, Evaluation of quality of service in smart-hospital communications. J. Med. Imaging Health Inform. **5**(8), 1864–1869 (2015)
50. B. Fabian, T. Ermakova, P. Junghanns, Collaborative and secure sharing of healthcare data in multi-clouds. Inf. Syst. **48**, 132–150 (2015)
51. P. Dayal, N.M. Hojman, J.L. Kissee, J. Evans, J.E. Natale, Y. Huang et al., Impact of telemedicine on severity of illness and outcomes among children transferred from referring emergency departments to a children's hospital PICU. Pediatr. Crit. Care Med. **17**(6), 516–521 (2016). https://doi.org/10.1097/PCC.0000000000000761
52. M. Habibzadeh, Z. Qin, T. Soyata, B. Kantarci, Large scale distributed dedicated- and non-dedicated smart city sensing systems. IEEE Sens. J. **17**(23), 7649–7658 (2017)
53. M. Habibzadeh, T. Soyata, B. Kantarci, A. Boukerche, C. Kaptan, Sensing, communication and security planes: a new challenge for a smart city system design. Comput. Netw. **144**, 163–200 (2018)
54. M. Liggins II, D. Hall, J. Llinas, *Handbook of Multisensor Data Fusion: Theory and Practice* (CRC Press, Boca Raton, 2017)
55. G. Fortino, S. Galzarano, R. Gravina, W. Li, A framework for collaborative computing and multi-sensor data fusion in body sensor networks. Inf. Fusion **22**, 50–70 (2015)
56. Y. Zhang, M. Qiu, C.W. Tsai, M.M. Hassan, A. Alamri, Health-CPS: healthcare cyber-physical system assisted by cloud and big data. IEEE Syst. J. **11**(1), 88–95 (2017)
57. H.L. Peng, J.Q. Liu, H.C. Tian, B. Xu, Y.Z. Dong, B. Yang, X. Chen, C.S. Yang, Flexible dry electrode based on carbon nanotube/polymer hybrid micropillars for biopotential recording. Sens. Actuators A Phys. **235**, 48–56 (2015)
58. M. Habibzadeh, M. Hassanalieragh, A. Ishikawa, T. Soyata, G. Sharma, Hybrid solar-wind energy harvesting for embedded applications: supercapacitor-based system architectures and design tradeoffs. IEEE Circuits Syst. Mag. **17**(4), 29–63 (2017)
59. M. Habibzadeh, M. Hassanalieragh, T. Soyata, G. Sharma, Solar/wind hybrid energy harvesting for supercapacitor-based embedded systems, in *IEEE Midwest Symposium on Circuits and Systems*, Boston (2017), pp. 329–332
60. M. Habibzadeh, M. Hassanalieragh, T. Soyata, G. Sharma, Supercapacitor-based embedded hybrid solar/wind harvesting system architectures, in *Proceedings of the 30th IEEE International System-on-Chip Conference*, Munich (2017)
61. B.A. Reyes, N. Reljin, Y. Kong, Y. Nam, K.H. Chon, Tidal volume and instantaneous respiration rate estimation using a volumetric surrogate signal acquired via a smartphone camera. IEEE J. Biomed. Health Inf. **21**(3), 764–777 (2017)
62. K. Arning, M. Ziefle, "get that camera out of my house!" conjoint measurement of preferences for video-based healthcare monitoring systems in private and public places, in *Inclusive Smart Cities and e-Health*, ed. by A. Geissbühler, J. Demongeot, M. Mokhtari, B. Abdulrazak, H. Aloulou (Springer, Cham, 2015), pp. 152–164
63. S. Kianoush, S. Savazzi, F. Vicentini, V. Rampa, M. Giussani, Device-free RF human body fall detection and localization in industrial workplaces. IEEE Internet Things J. **4**(2), 351–362 (2017)
64. X. Liu, J. Cao, S. Tang, J. Wen, P. Guo, Contactless respiration monitoring via off-the-shelf WiFi devices. IEEE Trans. Mob. Comput. **15**(10), 2466–2479 (2016)

65. F. Adib, H. Mao, Z. Kabelac, D. Katabi, R.C. Miller, Smart homes that monitor breathing and heart rate, in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. CHI '15* (ACM, New York, 2015), pp. 837–846
66. M. Kachuee, M.M. Kiani, H. Mohammadzade, M. Shabany, Cuffless blood pressure estimation algorithms for continuous health-care monitoring. IEEE Trans. Biomed. Eng. **64**(4), 859–869 (2017)
67. D.L. Carnì, D. Grimaldi, A. Nastro, V. Spagnuolo, F. Lamonaca, Blood oxygenation measurement by smartphone. IEEE Instrum. Meas. Mag. **20**(3), 43–49 (2017)
68. C.Y. Huang, M.C. Chan, C.Y. Chen, B.S. Lin, Novel wearable and wireless ring-type pulse oximeter with multi-detectors. Sensors **14**(9), 17586–17599 (2014)
69. S. Acharya, A. Rajasekar, B.S. Shender, L. Hrebien, M. Kam, Real-time hypoxia prediction using decision fusion. IEEE J. Biomed. Health Inform. **21**(3), 696–707 (2017)
70. V.P. Rachim, W.Y. Chung, Wearable noncontact armband for mobile ECG monitoring system. IEEE Trans. Biomed. Circuits Syst. **10**(6), 1112–1118 (2016)
71. P. Müller, M.A. Bégin, T. Schauer, T. Seel, Alignment-free, self-calibrating elbow angles measurement using inertial sensors. IEEE J. Biomed. Health Inform. **21**(2), 312–319 (2017)
72. N.J. Cleven, J.A. Müntjes, H. Fassbender, U. Urban, M. Görtz, H. Vogt, M. Gräfe, T. Göttsche, T. Penzkofer, T. Schmitz-Rode, W. Mokwa, A novel fully implantable wireless sensor system for monitoring hypertension patients. IEEE Trans. Biomed. Eng. **59**(11), 3124–3130 (2012)
73. D. Shao, C. Liu, F. Tsow, Y. Yang, Z. Du, R. Iriya, H. Yu, N. Tao, Noncontact monitoring of blood oxygen saturation using camera and dual-wavelength imaging system. IEEE Trans. Biomed. Eng. **63**(6), 1091–1098 (2016)
74. T.M. Seeberg, J.G. Orr, H. Opsahl, H.O. Austad, M.H. Røed, S.H. Dalgard, D. Houghton, D.E.J. Jones, F. Strisland, A novel method for continuous, noninvasive, cuff-less measurement of blood pressure: evaluation in patients with nonalcoholic fatty liver disease. IEEE Trans. Biomed. Eng. **64**(7), 1469–1478 (2017)
75. B. Zhou, M. Sundholm, J. Cheng, H. Cruz, P. Lukowicz, Measuring muscle activities during gym exercises with textile pressure mapping sensors. Pervasive Mob. Comput. **38**, 331–345 (2017). Special Issue IEEE International Conference on Pervasive Computing and Communications (PerCom) 2016
76. A.Q. Javaid, H. Ashouri, A. Dorier, M. Etemadi, J.A. Heller, S. Roy, O.T. Inan, Quantifying and reducing motion artifacts in wearable seismocardiogram measurements during walking to assess left ventricular health. IEEE Trans. Biomed. Eng. **64**(6), 1277–1286 (2017)
77. A. Page, O. Kocabas, T. Soyata, M.K. Aktas, J. Couderc, Cloud-based privacy-preserving remote ECG monitoring and surveillance. Ann. Noninvasive Electrocardiol. **20**(4), 328–337 (2014)
78. M. Habibzadeh, A. Boggio-Dandry, Z. Qin, T. Soyata, B. Kantarci, H. Mouftah, Soft sensing in smart cities: handling 3Vs using recommender systems, machine intelligence, and data analytics. IEEE Commun. Mag. **56**(2), 78–86 (2018)
79. ZigBee Alliance, ZigBee Alliance Web page (2017). http://www.zigbee.org/. Accessed 10 November 2017
80. T. de Almeida Oliveira, E.P. Godoy, Zigbee wireless dynamic sensor networks: feasibility analysis and implementation guide. IEEE Sens. J. **16**(11), 4614–4621 (2016)
81. Y. Kim, S. Lee, S. Lee, Coexistence of ZigBee-based WBAN and WiFi for health telemonitoring systems. IEEE J. Biomed. Health Inform. **20**(1), 222–230 (2016)
82. Bluetooth Special Interest Group (SIG), Core Specifications - Bluetooth Technology Website (2017). https://www.bluetooth.com/specifications/bluetooth-core-specification. Accessed 17 October 2017
83. M. Collotta, G. Pau, A novel energy management approach for smart homes using bluetooth low energy. IEEE J. Sel. Areas Commun. **33**(12), 2988–2996 (2015)
84. A. Basalamah, Sensing the crowds using bluetooth low energy tags. IEEE Access **4**, 4225–4233 (2016)
85. O. Bello, S. Zeadally, M. Badra, Network layer inter-operation of device-to-device communication technologies in Internet of Things (IoT). Ad Hoc Netw. **57**(C), 52–62 (2017)

86. M. Agiwal, A. Roy, N. Saxena, Next generation 5G wireless networks: a comprehensive survey. IEEE Commun. Surv. Tutorials **18**(3), 1617–1655 (2016)
87. N.A. Johansson, Y.P.E. Wang, E. Eriksson, M. Hessler, Radio access for ultra-reliable and low-latency 5G communications, in *2015 IEEE International Conference on Communication Workshop (ICCW)* (June 2015), pp. 1184–1189
88. O. Galinina, S. Andreev, M. Komarov, S. Maltseva, Leveraging heterogeneous device connectivity in a converged 5G-IoT ecosystem. Comput. Netw. **128**(Supplement C), 123–132 (2017). Survivability Strategies for Emerging Wireless Networks
89. M.N. Tehrani, M. Uysal, H. Yanikomeroglu, Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions. IEEE Commun. Mag. **52**(5), 86–92 (2014)
90. J. Qiao, X.S. Shen, J.W. Mark, Q. Shen, Y. He, L. Lei, Enabling device-to-device communications in millimeter-wave 5G cellular networks. IEEE Commun. Mag. **53**(1), 209–215 (2015)
91. A. Mukherjee, J.F. Cheng, S. Falahati, H. Koorapaty, D.H. Kang, R. Karaki, L. Falconetti, D. Larsson, Licensed-assisted access LTE: coexistence with IEEE 802.11 and the evolution toward 5G. IEEE Commun. Mag. **54**(6), 50–57 (2016)
92. M. Habibzadeh, W. Xiong, M. Zheleva, E.K. Stern, B.H. Nussbaum, T. Soyata, Smart city sensing and communication sub-infrastructure, in *IEEE Midwest Symposium on Circuits and Systems*, Boston (Aug 2017), pp. 1159–1162
93. Y. Lu, P. Kuonen, B. Hirsbrunner, M. Lin, Benefits of data aggregation on energy consumption in wireless sensor networks. IET Commun. **11**(8), 1216–1223 (2017)
94. P. Sridhar, A.M. Madni, M. Jamshidi, Hierarchical aggregation and intelligent monitoring and control in fault-tolerant wireless sensor networks. IEEE Syst. J. **1**(1), 38–54 (2007)
95. U. Shaukat, E. Ahmed, Z. Anwar, F. Xia, Cloudlet deployment in local wireless networks: motivation, architectures, applications, and open challenges. J. Netw. Comput. Appl. **62**(Supplement C), 18–40 (2016)
96. Y. Chen, Y. Chen, Q. Cao, X. Yang, Packetcloud: a cloudlet-based open platform for in-network services. IEEE Trans. Parallel Distrib. Syst. **27**(4), 1146–1159 (2016)
97. T. Soyata, H. Ba, W. Heinzelman, M. Kwon, J. Shi, Accelerating mobile cloud computing: a survey, in *Communication Infrastructures for Cloud Computing*, ed. by H.T. Mouftah, B. Kantarci (IGI Global, Hershey, 2013), pp. 175–197
98. M. Almorsy, J. Grundy, I. Müller, An analysis of the cloud computing security problem (2016). Preprint arXiv:1609.01107
99. Google LLC, Cloud IoT Core, Google Cloud Platform. https://cloud.google.com/iot-core/
100. Microsoft Corp., Microsoft Azure Cloud Computing Platform and Services. https://azure.microsoft.com/en-us/
101. Amazon Inc., Amazon Web Services (AES) - Cloud Computing Services. https://aws.amazon.com/
102. IBM Corp., IBM Watson Internet of Things (IoT). https://www.ibm.com/internet-of-things
103. L. Hu, M. Qiu, J. Song, M.S. Hossain, A. Ghoneim, Software defined healthcare networks. IEEE Wirel. Commun. **22**(6), 67–75 (2015)
104. J. Li, Y.K. Li, X. Chen, P.P. Lee, W. Lou, A hybrid cloud approach for secure authorized deduplication. IEEE Trans. Parallel Distrib. Syst. **26**(5), 1206–1216 (2015)
105. P.T. Endo, A.V. de Almeida Palhares, N.N. Pereira, G.E. Goncalves, D. Sadok, J. Kelner, B. Melander, J.E. Mangs, Resource allocation for distributed cloud: concepts and research challenges. IEEE Netw. **25**(4), 42–46 (2011)
106. S. Hijazi, A. Page, B. Kantarci, T. Soyata, Machine learning in cardiac health monitoring and decision support. IEEE Comput. Mag. **49**(11), 38–48 (2016)
107. S. Li, L. Da Xu, X. Wang, Compressed sensing signal and data acquisition in wireless sensor networks and internet of things. IEEE Trans. Ind. Inform. **9**(4), 2177–2186 (2013)
108. M. Alhussein, Monitoring Parkinson's disease in smart cities. IEEE Access **5**, 19835–19841 (2017)
109. D. Zhou, J. Luo, V.M. Silenzio, Y. Zhou, J. Hu, G. Currier, H.A. Kautz, Tackling mental health by integrating unobtrusive multimodal sensing, in *AAAI* (2015), pp. 1401–1409

110. L. Calderoni, M. Ferrara, A. Franco, D. Maio, Indoor localization in a hospital environment using random forest classifiers. Expert Syst. Appl. **42**(1), 125–134 (2015)
111. J. Qin, W. Fu, H. Gao, W.X. Zheng, Distributed k-means algorithm and fuzzy c-means algorithm for sensor networks based on multiagent consensus theory. IEEE Trans. Cybern. **47**(3), 772–783 (2017)
112. W. Kim, M.S. Stanković, K.H. Johansson, H.J. Kim, A distributed support vector machine learning over wireless sensor networks. IEEE Trans. Cybern. **45**(11), 2599–2611 (2015)
113. M.M.A. Patwary, D. Palsetia, A. Agrawal, W.k. Liao, F. Manne, A. Choudhary, A new scalable parallel DBSCAN algorithm using the disjoint-set data structure, in *2012 International Conference for High Performance Computing, Networking, Storage and Analysis (SC)* (Nov 2012), pp. 1–11
114. FDA Safety Communication, Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm. Accessed 03 December 2018
115. B. Barrett, Hack Brief: Hackers are Holding an LA Hospital's Computers Hostage. https://www.wired.com/2016/02/hack-brief-hackers-are-holding-an-la-hospitals-computers-hostage/. Accessed 12 March 2018
116. S. Balasubramanlan, The Global Cyberattack and the Need to Revisit Health Care Cybersecurity. https://www.huffingtonpost.com/entry/lessons-learned-the-global-cyberattack-the-need_us_591a1ac5e4b086d2d0d8d1ed. Accessed 12 March 2018
117. S. Larson, Why Hospitals are so Vulnerable to Ransomware Attacks. http://money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/index.html. Accessed 19 March 2018
118. J. Rogers, Fitness Tracking Data on Strava App Reveal US Military Bases Details, Sparking Security Concerns. http://www.foxnews.com/tech/2018/01/29/fitness-tracking-data-on-strava-app-reveal-us-military-bases-details-sparking-security-concerns.html. Accessed 19 March 2018
119. J.L. Fernández-Alemán, I.C. Señor, P. Ángel Oliver Lozoya, A. Toval, Security and privacy in electronic health records: a systematic literature review. J. Biomed. Inform. **46**(3), 541–562 (2013)
120. C. Cerrudo, An emerging us (and world) threat: cities wide open to cyber attacks. Securing Smart Cities (2015)
121. O. Arias, J. Wurm, K. Hoang, Y. Jin, Privacy and security in internet of things and wearable devices. IEEE Trans. Multi-Scale Comput. Syst. **1**(2), 99–109 (2015)
122. H. Takabi, J.B.D. Joshi, G.J. Ahn, Security and privacy challenges in cloud computing environments. IEEE Secur. Priv. **8**(6), 24–31 (2010)
123. A.B. Budurusubmi, S.S. Yau, An effective approach to continuous user authentication for touch screen smart devices, in *IEEE International Conference on Software Quality, Reliability and Security (QRS)* (Aug 2015), pp. 219–226
124. K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, H.H. Luo, Security and privacy for mobile healthcare networks: from a quality of protection perspective. IEEE Wirel. Commun. **22**(4), 104–112 (2015)
125. I. Hwang, Y. Kim, Analysis of security standardization for the internet of things, in *2017 International Conference on Platform Technology and Service (PlatCon)* (Feb 2017), pp. 1–6
126. P. Kumari, M. López-Benítez, G.M. Lee, T. Kim, A.S. Minhas, Wearable internet of things - from human activity tracking to clinical integration, in *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* (July 2017), pp. 2361–2364
127. J. Rajamäki, R. Pirinen, Towards the cyber security paradigm of ehealth: resilience and design aspects. AIP Conf. Proc. **1836**(1), 020029 (2017)
128. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. **4**(5), 1125–1142 (2017)

129. B. Ondiege, M. Clarke, G. Mapp, Exploring a new security framework for remote patient monitoring devices. Computers **6**(1), 11 (2017)
130. M.A. Ferrag, L. Maglaras, A. Derhab, A.V. Vasilakos, S. Rallis, H. Janicke, Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues (2018). Preprint arXiv:1803.10281
131. O. Kocabas, T. Soyata, M.K. Aktas, Emerging security mechanisms for medical cyber physical systems. IEEE/ACM Trans. Comput. Biol. Bioinform. **13**(3), 401–416 (2016)
132. Z. Liu, J. Großschädl, Z. Hu, K. Järvinen, H. Wang, I. Verbauwhede, Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the Internet of Things. IEEE Trans. Comput. **66**(5), 773–785 (2017)
133. K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, X.S. Shen, Security and privacy in smart city applications: challenges and solutions. IEEE Commun. Mag. **55**(1), 122–129 (2017)
134. X. Wang, C. Konstantinou, M. Maniatakos, R. Karri, Confirm: detecting firmware modifications in embedded systems using hardware performance counters, in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design. ICCAD '15* (IEEE, Piscataway, 2015), pp. 544–551
135. S. Agrawal, M.L. Das, A. Mathuria, S. Srivastava, Program integrity verification for detecting node capture attack in wireless sensor network, in *Information Systems Security*, ed. by S. Jajoda, C. Mazumdar (Springer, Cham, 2015), pp. 419–440
136. L.S. Sindhuja, G. Padmavathi, Replica node detection using enhanced single hop detection with clonal selection algorithm in mobile wireless sensor networks. J. Comput. Netw. Commun. **2016**, 1:1–1:1 (2016)
137. L. Hu, Z. Wang, Q.L. Han, X. Liu, State estimation under false data injection attacks: security analysis and system protection. Automatica **87**, 176–183 (2018)
138. A. Abbaspour, K.K. Yen, S. Noei, A. Sargolzaei, Detection of fault data injection attack on UAV using adaptive neural network. Procedia Comput. Sci. **95**, 193–200 (2016)
139. M. Ryan, et al., Bluetooth: with low energy comes low security. WOOT **13**, 4–4 (2013)
140. C. Mclvor, M. McLoone, J.V. McCanny, Fast Montgomery modular multiplication and RSA cryptographic processor architectures, in *Conference Record of the Thirty-Seventh Asilomar Conference on Signals, Systems and Computers, 2004*, vol. 1 (IEEE, Piscataway, 2003), pp. 379–384
141. A. Boscher, E.V. Trichina, H. Handschuh, Randomized RSA-based cryptographic exponentiation resistant to side channel and fault attacks (20 March 2012) US Patent 8139763
142. Y. Li, L. Shi, P. Cheng, J. Chen, D.E. Quevedo, Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach. IEEE Trans. Autom. Control **60**(10), 2831–2836 (2015)
143. M. Brownfield, Y. Gupta, N. Davis, Wireless sensor network denial of sleep attack, in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop* (June 2005), pp. 356–364
144. D.R. Raymond, R.C. Marchany, S.F. Midkiff, Scalable, cluster-based anti-replay protection for wireless sensor networks, in *Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC* (IEEE, Piscataway, 2007), pp. 127–134
145. E.Y. Vasserman, N. Hopper, Vampire attacks: draining life from wireless ad hoc sensor networks. IEEE Trans. Mob. Comput. **12**(2), 318–332 (2013)
146. Y. Liu, M. Dong, K. Ota, A. Liu, Activetrust: secure and trustable routing in wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **11**(9), 2013–2027 (2016)
147. H. Suo, J. Wan, C. Zou, J. Liu, Security in the Internet of Things: a review, in *2012 International Conference on Computer Science and Electronics Engineering (ICCSEE)*, vol. 3 (IEEE, Piscataway, 2012), pp. 648–651
148. M.J. Covington, R. Carskadden, Threat implications of the Internet of Things, in *2013 5th International Conference on Cyber Conflict (CyCon)* (IEEE, Piscataway, 2013), pp. 1–12
149. D. Puthal, S. Nepal, R. Ranjan, J. Chen, Threats to networking cloud and edge datacenters in the Internet of Things. IEEE Cloud Comput. **3**(3), 64–71 (2016)

150. S.M. Muzammal, M.A. Shah, H.A. Khattak, S. Jabbar, G. Ahmed, S. Khalid, S. Hussain, K. Han, Counter measuring conceivable security threats on smart healthcare devices. IEEE Access **6**, 20722–20733 (2018)
151. C. Kolias, A. Stavrou, J. Voas, I. Bojanova, R. Kuhn, Learning Internet-of-Things Security "Hands-On". IEEE Secur. Priv. **14**(1), 37–46 (2016)
152. C. Bormann, Z. Shelby, K. Hartke, Constrained application protocol (coap), draft-ietf-core-coap-18 (2013)
153. E. Rescorla, N. Modadugu, Datagram transport layer security version 1.2. Technical report (2012)
154. S.R. Moosavi, T.N. Gia, E. Nigussie, A.M. Rahmani, S. Virtanen, H. Tenhunen, J. Isoaho, End-to-end security scheme for mobility enabled healthcare internet of things. Futur. Gener. Comput. Syst. **64**, 108–124 (2016)
155. A. Zhang, L. Wang, X. Ye, X. Lin, Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems. IEEE Trans. Inf. Forensics Secur. **12**(3), 662–675 (2017)
156. J. Shen, D. Liu, J. Shen, Q. Liu, X. Sun, A secure cloud-assisted urban data sharing framework for ubiquitous-cities. Pervasive Mob. Comput. **41**, 219–230 (2017)
157. S. Tonyali, K, A., N. Saputro, A.S. Uluagac, M. Nojoumian, Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems. Futur. Gener. Comput. Syst. **78**(Part 2), 547–557 (2018)
158. O. Kocabas, T. Soyata, Towards privacy-preserving medical cloud computing using homomorphic encryption, in *Enabling Real-Time Mobile Cloud Computing through Emerging Technologies*, ed. by T. Soyata (IGI Global, Hershey, 2015), pp. 213–246
159. K. Yang, Z. Liu, X. Jia, X.S. Shen, Time-domain attribute-based access control for cloud-based video content sharing: a cryptographic approach. IEEE Trans. Multimedia **18**(5), 940–950 (2016)
160. T. Jung, X.Y. Li, Z. Wan, M. Wan, Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption. IEEE Trans. Inform. Forensics Secur. **10**(1), 190–199 (2015)
161. M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst. **24**(1), 131–143 (2013)
162. S.R. Moosavi, T.N. Gia, A.M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, H. Tenhunen, SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Comput. Sci. **52**, 452–459 (2015). The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015)
163. A. Sahi, D. Lai, Y. Li, Security and privacy preserving approaches in the ehealth clouds with disaster recovery plan. Comput. Biol. Med. **78**, 1–8 (2016)
164. D. Mishra, A. Chaturvedi, S. Mukhopadhyay, Design of a lightweight two-factor authentication scheme with smart card revocation. J. Inform. Secur. Appl. **23**, 44–53 (2015)
165. L.E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, H.W. Gellersen, Smart-its friends: a technique for users to easily establish connections between smart artefacts, in *International Conference on Ubiquitous Computing* (Springer, Berlin, 2001), pp. 116–122
166. L. Ding, P. Shi, B. Liu, The clustering of internet, internet of things and social network, in *2010 3rd International Symposium on Knowledge Acquisition and Modeling (KAM)* (IEEE, Piscataway, 2010), pp. 417–420
167. M.L. Gavrilova, F. Ahmed, S. Azam, P.P. Paul, W. Rahman, M. Sultana, F.T. Zohra, *Emerging Trends in Security System Design Using the Concept of Social Behavioural Biometrics* (Springer, Cham, 2017), pp. 229–251
168. J. Tian, Y. Cao, W. Xu, S. Wang, Challenge-response authentication using in-air handwriting style verification. IEEE Trans. Dependable Secure Comput. **PP**(99), 1–1 (2018)

169. M. Sultana, P.P. Paul, M. Gavrilova, A concept of social behavioral biometrics: motivation, current developments, and future trends, in *International Conference on Cyberworlds* (IEEE, Piscataway, 2014), pp. 271–278
170. L. Zhang, S. Zhu, S. Tang, Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. IEEE J. Biomed. Health Inform. **21**(2), 465–475 (2017)
171. T. Kumar, A. Braeken, M. Liyanage, M. Ylianttila, Identity privacy preserving biometric based authentication scheme for naked healthcare environment, in *2017 IEEE International Conference on Communications (ICC)* (May 2017), pp. 1–7
172. C. Prandi, S. Ferretti, S. Mirri, P. Salomoni, Trustworthiness in crowd-sensed and sourced georeferenced data, in *2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)* (IEEE, Piscataway, 2015), pp. 402–407
173. B. Kantarci, K.G. Carr, C.D. Pearsall, SONATA: social network assisted trustworthiness assurance in smart city crowdsensing. Int. J. Distrib. Syst. Technol. **7**(1), 59–78 (2016)
174. M. Pouryazdan, B. Kantarci, T. Soyata, H. Song, Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing. IEEE Access **4**, 529–541 (2016)
175. T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things. IEEE Access **6**, 32979–33001 (2018)
176. Y. Huo, X. Dong, W. Xu, M. Yuen, Cellular and WiFi co-design for 5G user equipment (2018). Preprint arXiv:1803.06943
177. M.N. Kamel Boulos, J.T. Wilson, K.A. Clauson, Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. Int. J. Health Geogr. **17**(1), 25 (2018)