Chapter 12
Security for Cyber-Physical Systems in Healthcare

Kashif Saleem, Zhiyuan Tan and William Buchanan

12.1 Introduction

Sensor and network technologies and ubiquitous healthcare have evolved and matured over recent years, and are now in the process of being implemented into healthcare scenarios worldwide. The European Commission estimates that the market volume of mHealth technologies will exceed the 17 Billion Euro mark globally by 2017 [1] (Fig. 12.1).

Pervasive healthcare systems with real-time monitoring will enable Personal Care strategies (Personalized Medicine) or "Precision Medicine" as it is called in the US [2]. This will involve the use of smart algorithms and cyber-physical systems in order to support real-time processes to respond to individual requirements anywhere, anyhow, and at any time. This will be inevitably be linked to a new breed of telecommunication services, some of them in preparation under current 5G network initiatives in the US, Europe, China, and elsewhere [3].

There is a general assumption based on some evidence that the use of wireless-based eHealthcare systems outside hospital may increase effectiveness and efficiency [4]. One of the prime examples is that reminders generated by messenger systems may enhance the adherence of patients with chronic conditions such as Diabetes, Asthma, and HIV thereby reducing the number of severe events such as

K. Saleem (✉)
Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia
e-mail: ksaleem@ksu.edu.sa

Z. Tan · W. Buchanan
School of Computing, Edinburgh Napier University, Edinburgh, UK
e-mail: Z.Tan@napier.ac.uk

W. Buchanan
e-mail: w.buchanan@napier.ac.uk

C. Thuemmler and C. Bai (eds.), *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*, DOI 10.1007/978-3-319-47617-9_12

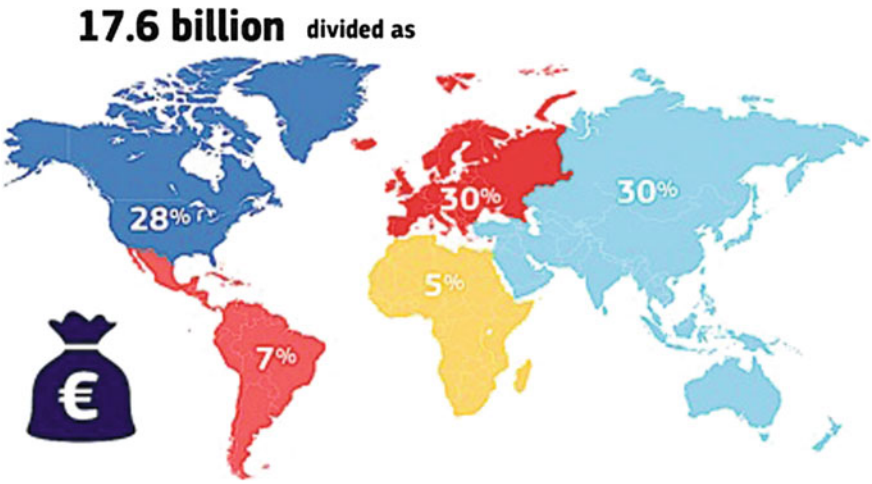

Fig. 12.1 Forecast: estimated global market value in 2017 [1]

hypoglycemic episodes, asthma attacks, or deterioration of blood counts [5]. This will result in fewer hospital admissions and increase of the overall quality of care. On the other hand, activities such as daily tasks, falls and movement detection, location tracking, medication intake, and medical status monitoring are very important features in Ambient Assisted Living (AAL) and tele monitoring [6].

Next generation eHealthcare systems will be based on cyber-physical systems and will be composed of multiple components that work on the basis of Industry 4.0 design principles in Health 4.0 setups integrating the physical world (e.g., patients, doctors, community nurses, and informal careers) and virtual components (e.g., algorithms, databases, and virtualized biosensors, etc.) [7].

Many different types of data will be gathered with the help of biosensors inside and outside the body, for example blood pressure, heartrate, blood glucose level, ECG, EEG; Cyber-physical systems will also process data from artificial organs such as Brain—or Cardiac Pacemakers, Insulin Pumps, and endoprothersis as knee and hip implants.

Especially those sensors deployed inside the body may be integrated into Wireless Body Area Network (WBAN) that integrate environment conditions and biometrics of the patient in order to present real-time analysis of biomedical processes. These networks typically communicate with network gateways following the IEEE 802.15.6 standard, which aims to provide an international standard for low power, short range and extremely reliable wireless communication with the surrounding of the human body [8].

12.2 WBAN Overview

WBAN and environment sensors use different protocols for communication. When the body sensors communicate with each other or with a node head, they are classified as Body Area Network (BAN). Communication between gateway devices/access points to the local management systems is normally wired. For indoor connectivity between sensors and PDA we have to use low range, reliable, and robust communication technologies like WiFi, Zigbee, 802.15.6, or 802.15. We can see from the literature [9] that Zigbee is the most widely used wireless protocol for BAN, while 802.15.6 is a specially crafted protocol, which focuses especially on WBAN medium access control mechanisms.

12.3 The Components in WBAN-Based eHealthcare System

A WBAN-based eHealthcare system generally consists of the following main components.

12.3.1 Wireless Sensor Node

A sensor or node is a tiny device measuring Physiological Values (PV) of a patient. As sensors are mostly attached to the body of the patient networks of body sensors are collectively called a Body Area Network or Body Sensor Network (BAN/BSN). These networks are normally wireless in nature due to the ease of use and mobility of the patient. They communicate to a relay or access point to transfer measured or sensed data. These sensors play a very important role in eHealthcare systems where secure, reliable, and ubiquitous patient monitoring are the key factors and data is generated at the sensor nodes. Therefore, reliable, secure and attack resistant acquisition, and transmission of data are of utmost importance for the efficiency and feasibility of eHealthcare systems. Rashidi and Mihailidis in [6] tabulated different types of sensor nodes that are used in eHealthcare. Sensors used can be of a versatile nature using different wireless technologies like Zigbee [10], Bluetooth [11], and UWB. The processing capability of a sensor is very low, as its main function is to sense and transmit data to the sink node or a smartphone. In the scenario where the data is required to transfer at long range the Long-Range Low-Power End Node Solution (LoRa) technology can be used [12]. LoRa is enabled with long range and with long life to perform environmental monitoring.

12.3.2 Gateway or Sink Node

An access point, a gateway, or a personal digital assistant function acquires data securely from sensors and transmits it securely to the required location [13]. This can be a personal device allocated for every patient in a hospital or a personal smartphone configured to handle data from sensors in a patient's home. It has more processing and storage capabilities as compared to measuring sensors. It is suggested to implement anonymity on such a device so that the patient's identity is ripped off when data is sent to the gateway and only a random patient ID is used onwards.

The access point is directly connected to a hospital information system in the case of local storage or to the Internet in the case of global data storage [14]. This part does not require data processing or computation capabilities as it just delivers data to the storage server. Usually WiFi compatible devices are used in this part. The patient should have the control to filter and allow which data to send to the network. The access point should support both communication technologies (e.g., sensor data aggregation) and transmission of data to relay node/gateway usually using Wi-Fi and a cellular technology present at the time. Other cases where the devices are communicated wirelessly to acquire critical data over long distances [15], the technology developed is narrow band radio for the IoT (NB-IOT), eMTC, and EC-GSM-IoT [16, 17] and is included in LTE [18, 19].

12.3.3 Authentication Server

A Public Key Infrastructure (PKI)-based authentication server is responsible for root level authentication of each and every actor in the whole infrastructure and also managing authentication across multiple domains and systems or multiple Electronic Health Record (HER) systems [14]. Every node, device, medical representative, emergency personnel, medical store personnel, and caretakers over the network are authenticated with the help of this server. The authentication server can be local to a hospital system or global system or can be based on a hierarchy. Recent architectures involve Cloud computing and Cloud servers for this purpose [20]. In Cloud-based architecture the encrypted data is directed toward the Cloud service provider authenticated and stored over multiple servers.

12.3.4 Storage Server

A storage server consists of all the databases and encrypted Protected Health Information (PHI) of patients. This can be a local storage server or a global connected one where a hospital stores the patients' data to access it globally [14].

This part requires a high performance and storage capabilities as well as high availability. In addition, access control mechanisms are also present on the server to make sure access is given to the authorized personnel only and also to run specific queries.

12.3.5 Policy/Delegation Server

A server for policy implementation check, creating and managing logs for accountability, and securely sharing information as controlled by a patient and delegated by a primary physician [14]. Policies are implemented and tested continuously so that no security breach occurs which can save an organization from a law suite of patient data privacy. This server can also handle delegation services like when a general physician refers a patient to another specialist and shares patient data and, after treatment, access to data is revoked [14]. This server requires global access to data for policy checking and verification. It is also required to have heavy computation capabilities.

12.4 Common Threats to Wireless Body Area Networks (WBANs)

Due to the heterogeneous and versatile nature of eHealthcare systems, it is essential to secure the health records from the monitoring side till the storage and/or retrieval. The violation of any aspect like patient confidentiality, privacy, integrity, patient approval, or data availability can have serious consequences to patient's life [20]. This is because the failure in generating and obtaining the authentic medical data by the WBAN can also prevent a patient from being treated effectively, or can lead to life-threatening situations.

An adversary can eavesdrop on the communication and/or temper with a patient's medical data if it is not encrypted, thus violating patient privacy. In the case of an emergency, if eHealthcare monitoring system is under Denial of Service (DoS)/Distributed Denial of Service (DDoS) attack can put the patient's life in danger due to the unavailability of patient's vital signs. An attacker can generate malicious activities in the network and can able to disrupt the normal operation of the patient's vital signs monitoring.

Furthermore, a number of attacks such as spoofing attacks, sybil attacks, wormhole attacks, session hijacking attacks, and resource consumption attacks against different communication layers, which are mentioned in [21, 22] can interrupt the overall system functionalities. Forward and backward secrecy are also important to ensure against attackers who read encrypted packets with an expired key. It has been shown that an eHealthcare system is prone to simple MAC and

network layer attacks like session hijacking, DoS/DDoS attacks, data corruption attacks, and multiple passive attacks [22]. Monitoring and eavesdropping have shown to be very easy to perform on protocols like Bluetooth and violate the privacy of patients [23].

12.4.1 Security Posture of Some Solutions

A complete eHealthcare history is discussed in [24]. A lot of work has been done, resulting in multiple types of solutions available, yet only few solutions propose complete system end-to end solutions addressing all the issues related to all the layers of the architecture. The following are some of the popular eHealthcare solutions along with their security standpoints and weaknesses.

A distributed eHealthcare system based on the Service Oriented Architecture (SOA) was proposed in [25]. It uses web services to provide support to nurses, pharmacists, physicians, and other healthcare professionals, as well as for patients and medical instruments used to monitor patients. Its main components include PDA, web Server, doctor PDA/computer, patient PDA, and Bluetooth for sensor communication. Its main security features include user authentication and session information logging. However, it lacks support for data storage on the local PDA for offline uses, and there is no support for emergency case scenarios as in HIPAA, no integrity checks, no availability issues handled, and no pseudonymization of the patient data.

CodeBlue is another important eHealthcare prototype defined over an architecture and a complete eHealthcare framework [26]. Its architecture allows for the integration of heterogeneous medical sensors. The framework provides protocols for device discovery, publish and subscribe routing layer, and query-based software to help caregivers in a hospital to request data from a group of patients. Its main components include PDA and mote sensors. Elliptic Curve Cryptography (ECC) was implemented on motes using integer arithmetic while Tinysec was proposed for symmetric encryption. It also lacks HIPAA compliance, no confidentiality on remaining architecture except sensors, no integrity check, and no privacy of data details.

Egbogah et al. [27] presented another project named MEDISN. It utilizes a wireless sensor network composed of a network gateway, Physiological Monitors (PMs), and Relay Points (RPs), to monitor the health, and transmit physiological data, of patients. Its main components were physiological monitors, relay points, a network gateway, and backend data-based server. No security feature was implemented other than client authentication which was done using an unknown authentication scheme.

Hamdi et al. presented another modular eHealthcare system called CAALYX in [4]. The system was composed of three subsystems: (1) A mobile monitoring system to collect and monitor PV of patients; (2) A home monitoring system to monitor patients at home and help them to keep in touch with their caregivers; and

(3) A monitoring system for caregivers to provide monitoring of elders by specialized personnel. Its main components were PDA and environmental sensors. It included privacy protection using local data processing but there was no encryption, authentication, or pseudonymization discussed in the paper.

Alarm-Net is another solution that consists of a body sensor network and an environmental sensor network [28]. Its main components include PDA, environmental sensors, body sensors, a network gateway, and a database. It used AES for encryption, a built-in cryptosystem for sensors and authentication using their own secure remote password protocol while HIPAA compliance, integrity check pseudonymization was absent from the solution. We can observe that most of the solutions use a PDA for end user connectivity and Bluetooth for the primary communication protocol for sensor interfacing which has multiple security limitations. Moreover, every solution has security shortcomings which include basic features like confidentiality, integrity, and pseudonymization.

12.4.2 WBAN Security Requirements in Healthcare Environment

Efficient communication in eHealthcare is defined as reliable, secure, fast, fault-tolerant, scalable, interference-immune, and low power. Attacks can be classified as active or passive [21]. Moreover, attacks can also be classified based on the layers they target, i.e., physical layer, MAC layer [22], network layer and application layer. We can mention the essential security and privacy requirements and issues in healthcare systems, by generally classifying them into four main categories based on the papers in the literature [6, 23, 26, 29–32].

(A) **Administrative level security**

This category of security includes nontechnical requirements. Privileges regarding policies and access control should be clearly defined and implemented. These policies should be context aware and adaptive to ensure data availability and access flexibility especially in the case of any emergency conditions. This category contains the following subcategories:

- Data access control: refers to the patient's data privacy. Multiple access control mechanisms can be implemented to enforce multiple levels of authorization to different categories of the patient's data [32].
- Accountability: includes the policies that bound users who are using the patient's data to be held accountable for their actions on data; nonrepudiation is one factor that can be achieved by enforcing those policies [32].
- Revocability: refers to revocability of any user from the patient's data when he/she seems malicious or performs a violation against the policies or set rules [32].

- Activity tracking threats: includes the privacy of the patient's data from any adversary that can measure or eavesdrop on the data and thus can monitor the patient's daily activities [31].
- Patient permission: is in accordance to international health laws and policies like HIPAA by which the patient has all the rights to his health record and he can allow or deny anyone to have access to his health records [14].
- Patient anonymity: includes sharing patient information to third parties without exposing the patient identity for research, surveys, or global health measures. This includes cases like when the government will likely take a precautionary measure of a disease if it sees its rapid increase in a specific area or a research student can analyze the health records of a disease without knowing the patient's real identity [14]
- Timeliness: is another important factor in eHealthcare systems as it may have an impact on the patient's health status. Even some minutes of delay can cost a patient's life [27].

(B) **Network level security**

Network layer security plays a crucial role in ensuring the security of an eHealthcare system. This layer provides secure transmission of patient data between body sensors and the gateway/relay point or the Internet. The protocols at this layer should also be attack resistant and reliable. Moreover, the adopted protocol should be energy-efficient, interference-immune, and reliable. In what follows we present the key security features that need to be ensured at this level.

- Secure routing: Secure routing is one important feature required in successfully transmitting data packets from wireless sensors to the head node or the gateway. Routing protocols should be attack resistant and reliable to transmit data packets [32, encryption].
- Intrusion Detection System: There should be an intrusion detection/mitigation mechanism built into the network layer protocols that identify malicious nodes/sensors and exclude them from the wireless network whether it is a single hop or a multiple hop wireless network [31].

Below are some of the famous routing attacks summarized from [21, 22, 28] that a network layer protocol should be resistant to:

- Selective forwarding attacks: An intermediate malicious node only forwards selective routing packets to the next node. This usually happens in multi hop routing protocols.
- Blackhole attack/Sinkhole attack: A malicious node sinks/ drops all packets that it receives.
- Sybil attack: A malicious node uses a valid node's identity to enter the network or disrupt it.

- Spoofing attack: A malicious node spoofs its identity in order to affect the normal operation of the network.
- Wormhole attack: It works by recording traffic from one part of the network and transmitting it to another part to poison the routing table, which may result in unreachable valid nodes.
- Rushing attack: A malicious node rushes to send its malicious packet to a destination node before a valid packet is received from a valid node.
- Cache Poisoning attack: A node's cache is poisoned by a fake node by sending wrong route updates to nodes in the network.
- Resource consumption/energy exhaustion attack: Valid packets are distributed in a network, which are not required to deplete the energy of nodes and thus reducing lifetime of the whole network.
- Session hijacking attack: An authentication session is hijacked just like a man in the middle attack in regular networks.
- Packet delay attack: A malicious node forwards packets but adding delay. This attack can be a critical one in case of an emergency.
- Jellyfish attack: A malicious node sends packets but in a disordered manner so that the destination node does not reorder them, if it can even reorder the packets it will at least cause latency in a network.

(C) **Physical/MAC level security**

Data generated by sensors are first converted to a specific format at the physical layer and they are transmitted through a wireless medium using a medium access control mechanism. The MAC layer defines the nodes' channel use, whether it is time division-based or CSMA-based. Following security features need to be considered at this layer:

- Fake node detection and mitigation: Protocols used at this layer should be resistant to fake nodes and identification of a fake node should be a part of these protocols. There should be an authentication mechanism as in [33, 34]. Moreover, mitigation at this level can stop many routing layer attacks.
- Secure and efficient MAC layer: Security is the best when it is implemented at the lower layers so a secure and efficient MAC layer protocol can save us from many upper layer attacks [6].
- Immune to DoS/Jamming attacks and other wireless technologies coexistence [30]: DoS and jamming attacks are the most common at this layer. A high gain noise transceiver can disrupt the communication of all the nodes and thus result in a total system failure.
- Monitoring and eavesdropping on patient vital signs: Monitoring is embedded in eHealthcare systems so solutions proposed at this layer should be aware of eavesdropping and mitigate those sources to avoid the privacy violations of patient data [14].

- Threats to information when in transit: security should be enforced in both modes, whether data is residing on the node and whether it is traveling in the network [32].

12.5 Securing Cyber-Physical Healthcare Networks

The current development of eHealthcare systems has gradually evolved from simple WBANs to Cyber-Physical Systems (CPS) owing to the recent advances in medical sensors, wireless sensor networks, and Cloud computing. CPS leverages sensing, processing and networking technologies to host computationaly expensive personalized healthcare applications, which make intelligent decision based on massive patient data. A typical cyber-physical healthcare system includes not only the components listed in Sect. 12.3 but also a high-capacity Cloud-based data center and analytical system.

As data storage and decision making are moved away from WBANs to Cloud, network security becomes vitally important. Securing only WBANs is far less than enough to prevent a cyber-physical healthcare from being compromised. The network segments formed with data sinks/gateways and Cloud are often the targets of attacks. Compared to hacking individual heterogonous sensing devices in WBANs, compromising the network segments between data sinks/gateways and Cloud is more lucrative, which results in higher information gain as patient data are aggregated and transmitted across the networks to Cloud.

Data and system security deserve top priority in this mission and time critical CPS. Confidentiality, integrity, freshness, and availability of patient data need to be guaranteed [35] as the reasons that (1) the privacy of patients should not be violated from legal and ethical perspectives, and (2) the correctness and timelessness of patient data are vital to promptly accurate decision making, especially in life-threatening cases.

Apart from the security and privacy of patient data, the confidentiality of patient identities and their clinic wearables is equally critical in the context of cyber-physical healthcare [36]. To prevent illegal/malicious devices gaining access to cyber-physical healthcare systems, entity authentication needs to be in place. Mutual authentication between wearables and networks has to be enforced.

Moreover, the availability of the network and decision making services should be under protection too. It will be life-threatening if they remain not accessible for just a few minutes in the case of an emergency. The impact will be more severe if the entire network comprised of multi-hypervisors is struck down by a massive attack. Hence, protecting systems from DoS/DDoS attacks is equally important [36]. Several common network attacks [37], which target the network layer of general-purpose computer networks rather than that of WBANs, are summarized as follows.

- Eavesdropping: An adversary, having access to data paths in a network, sniff or interpret the unsecured, or "cleartext" traffic.
- Data modification: An adversary modifies the data in his intercepted packets.
- IP address spoofing: An adversary constructs IP packets with forgery valid source IP addresses to hide the sender's real identity.
- Man-in-the-Middle attack: An adversary, having access to the data path of the communication between two network users, actively monitors, intercepts, and manipulates the communication without being known by the victims.
- Application-lLayer attack: The adversary exploits the vulnerabilities of applications to gain control of the applications and even the host machines or the connected networks.
- Denial-of-Service attack: The attacks attempt to force victims out of service by imposing intensive computation tasks or huge amount of useless packets.

12.6 Healthcare Cloud Security

Cloud Service Providers (CSP) are offering services that in large organizations and enterprises were previously delivered only on-premises. This introduced completely new challenges that potential CSP customers have to take care of. Major security organizations offer tough security standards that CSP have to comply with and standards that customers from governmental, financial, and public sectors have to implement [38]. Security standards compliance, however, is a regulatory form of information security practice not a safeguard that can actually protect the data.

To compete with new challenges many data protection services that were previously only delivered within strict security boundaries are offered as a cloud service. Some providers took additional security countermeasures, i.e., Microsoft enables on-premises Hardware Security Module (HSM) support [39] for its flag cloud-based Information Rights Management (IRM) product MS Rights Management Services (RMS) Online.

CSP or online data sharing services can protect data at rest using database encryption. Recently, Microsoft researchers published results around a new efficient homomorphic encryption that might be applicable for medical data [40] that should be processed in a secure manner without divulging underlying information. However, just a few months earlier Microsoft researchers demonstrated that database CryptDB encryption, previously acknowledged as a secure data protection technique can be broken with a single trick [41]. It has been shown that every cryptographic scheme currently believed to be secure could be broken with an emerging quantum technology [42], which has been hanging as sword of Damocles over the Cloud computing for a decade. Another threat can be directly related to Big data, which shows that machine learning and business intelligence as a service is a way to efficiently process large amounts of anonymized or encrypted personal data. Illegitimate data analysis applied on a large scale could have potentially a serious social impact [43].

With regards to frameworks for Cloud data sharing, data hosted by one cloud service provider cannot be securely transferred outside of a single CSP security boundary. Such a migration would require either data to be re-encrypted before migration or cloud providers would have to exchange cryptographic master keys. Cloud data hosting very often is based on storing data by homogeneous application in a public Internet space, what bends initial cloud service principals. Theoretically, cloud provider should offer a transparent service that could be dynamically transferred or seized by other cloud service provider without loss of actual service quality and data availability [44].

Furthermore, in [45], it is stated that "a single cloud is far more vulnerable to failure of service unavailability and malicious insiders and due to this reason it is less popular in healthcare, as medical healthcare systems are concerned about its security. From this notion of security concern an advanced model has emerged; multicloud also known to be Cloud-of-Clouds". Future research directions in securing IoT-Cloud-based SCADA systems are the managmenet, security, real-time data handling, cross-layer collaborations, application development migration of CPSs and the impact on existing approaches, sustainable management, engineering and development tools, sharing and management of data lifecycle, and data science that are illustrated [46].

12.7 Shaping the Future of Healthcare with 5G

The Fifth Generation (5G) networks are now at the heart of the development of future mobile telecommunication, and fully commercial ones are expected to be rolled out until 2020 [47]. 5G will be characterized by high broadband speeds, reliability, scalability, and intelligent networks [48]. Numerous wireless access technologies, including WiFi, LPWA, 4G, and millimeter wave, will be enclosed in 5G [49]. Rather than an upgrade of mobile network technologies in the sense of a Long Term Evolution (LTE), 5G represents a quantum leap from mobile networking to new networking/computing paradigm. It combines cloud infrastructure, Virtualized Network Functions (VNF), "intelligent edge services, and a distributed computing model that derives insights from the data generated by billions of devices" [50].

With its high-speed connectivity and mega data transmission capabilities, the 5G networks serve a new means to deliver healthcare including imaging, data analytics, diagnostics, and treatment at affordable prices. Patients can gain access to doctors worldwide through 5G networks for multimedia medical consultation which not only lowers medical cost but also increases accessibility to medical resources. Besides, instead of expensive in-patient hospital care, patients will be monitored remotely by smart algorithms through clinical wearables [51]. Medical data, such as body temperature, blood pressure, heart rate, respiratory rate, physical activity log

and medication adherence, will be transmitted to healthcare systems for analysis. These multisource medical data contribute more precise analytics and raise early warnings that help medical practitioners detect potential problems and provide proactive medical treatments to patients. However, there is absolute clarity amongst European governments and the European Commission that health care data are typically owned by the patients. Personal data may not even be stored outside the European Union against the wish of an individual according to European legislation as clearly demonstrated through the ruling of the Court of Justice of the European Union on "Safe Harboring" [52].

In spite of showing great potential to host Health 4.0 [53], 5G introduces challenges to the development of eHealthcare applications. In particular, one of its core technologies (i.e., network virtualization) poses new security requirements that cannot be effectively addressed with conventional security solutions. This requires network security personnel to have a thoughtful rethink of their strategy. To start up a discussion on the topic, several critical security issues with virtualization are introduced in the following section.

12.7.1 Security Challenges with Virtualization

5G is featured as smart networks that facilitate intelligent traffic routing and prioritize data traffic with automatic decision making. Network Function Virtualization (NFV) and Software Defined Networking (SDN) act as building blocks toward intelligent 5G networks. They enhance the capability of flexible computing resource allocation for real-time data aggregation and analytics. This, therefore, helps users gain a better insight into data and optimize healthcare applications accordingly.

NFV leverages virtualization technologies to decouple network functions from proprietary hardware [54]. To accelerate service provisioning and allow for new flexibilities in operating and managing mobile networks, network functions are implemented in software packages and deployed on high-capacity general-purpose computing platforms within the IT environments of service providers rather than dedicated proprietary hardware [55].

Based on the same technology with a different focus, SDN separates the control and forwarding plane of a network. SDN renders dynamic reconfiguration of network settings, including network function characteristics and behaviors, as well as real-time changes of a network topology [56]. Furthermore, SDN supplies a global view of an elastic decentralized network for efficient coordination of network services [57]. SDN allows businesses to tune their network bandwidth on the fly.

In CPS healthcare applications, both patients and healthcare providers can benefit from SDN. Patients, on the one hand, will be able to control access to their data even though these data will be stored in databases distributed across networks operated by different organizations [57]. Individual healthcare providing

organizations, on the other hand, will be allowed to perform allocation of "isolated" virtualized networks on a high level in order to prevent interference from third parties [57].

(D) **Security Issues**

However, new technologies always raise new challenges on security. NFV and SDN are not exceptions. The vulnerabilities of their underlying virtualization technologies result in undesirable security loopholes in CPS eHealthcare applications. There are five key security issues with NFV and SDN, which could lead to compromise of 5G CPS eHealthcare applications. They should be given proper consideration in design and carefully addressed during implementation.

- Hypervisor vulnerabilities: A system can hardly be secured with a vulnerable infrastructure. 39 critical vulnerabilities of hypervisors were recorded by the National Vulnerability Database (NVD) between January 2012 and June 2015 [58]. These vulnerabilities allow an adversary to directly compromise a hypervisor and to gain access to a less secure Virtual Machine (VM). Such that the attacker possibly takes advantage to manipulate SDN controllers that are not properly secured [59].
- SDN vulnerabilities: A conceptual SDN architecture consists of application, controllers, and networking devices. The vulnerabilities in these three SDN components could be exploited by adversaries to compromise the entire system. The adversaries might seize control of a SDN system, impersonate a host, cause network traffic congestion through diverting network flows to a heavy loaded network device, or intercept and manipulate traffic [59].
- Improper network isolation: Not all Cloud computing architectures properly isolate their data network from control network. An adversary could compromise the control plane of a shared SDN architecture through its fellow data network. Underlying data network traffic routes would be manipulated following a successful attempt, and then malicious traffic could escape from monitoring of NFV security devices [56].
- Security service insertion: Conventional security schemes are not originally designed to be deployed with NFV, where logical functions and physical hardware are separated to accelerate service provisioning. So, there is often no simple insertion point for a conventional security scheme to be deployed logically and physically inline in a hypervisor with NFV [56].
- Stateful inspection: NFV promises elastic networks. Asymmetric traffic flows created by on-demand alteration of virtual network functions may add complexity to stateful security control, in which every packet needs to be seen in order to provide access control [56].

(E) **Security Requirements**

The elastic nature of 5G networks poses new security requirements to CPS eHealthcare applications. Network function virtualization, a unique characteristic of 5G networks, enables flexible and cost-saving deployment of services and prompt

adjustment to networking. Virtualization, however, increases the complexity of implementation of security. Thus, the security of all parties should be given thoughtful consideration in this setting. Several requirements as follows are recommended to be addressed too.

- Dynamic security policies: Static security policies are not applicable in virtualized network environments, where virtualized services will be moved around to meet technical or business requirements on the fly. It is, therefore, critical to provide a solution to set up dynamic security policies self-adaptive to the relocation of virtual workloads [60].
- Impact on performance: The impact of a security scheme on the performance of an eHealthcare application is of importance. A feasible security scheme should protect an application from being compromised while ensuring that its performance remains meeting requirements [60].
- Comprehensive Protection: Standalone security schemes are incompatible to virtualized networks. It is impossible for them working alone to gain a clear vision on what are happening in the networks due to the dynamic nature of virtualized environments [53]. It would be wise to consider collaborative schemes with self-adaptive features.
- Fully virtualized network security solutions: Instead of deploying physical, hardware-based network security products on 5G networks, fully virtualized security solutions are viable and easier to cope with the changes of the virtualized networks.
- Elastic network boundaries: The network boundaries in NFV architecture are not as clear as those in physical one. These unclear boundaries complicate security matters [56]. VLANs are traditionally considered insecure so that there is no clear boundary in NFV architecture protecting services from being accessed by unauthorized third parties.
- Network segmentation: To be fault-tolerant, a large network is suggested to be divided into smaller segments. When one or more network segments start getting congested or becoming unavailable, the network administrator can use the SDN controller to route traffic to other healthy segments to maintain the vitality of the network.

12.7.2 Security Enhancement with Virtualization

Although NFV and SDN raise security challenges, they in the meanwhile offer numerous benefits in deployment of security services as well as potential enhancement to network security.

(A) **Benefits to deployment of security services**

- Reduced costs: Deploying virtualized security services on general-purpose computing platforms with NFV significantly reduces management costs.

SDN provides on-demand configuration for the data forwarding plane [56]. This saves service providers paying costly bills for changing physical network topology.

- On-demand deployment: NFV promises on-demand deployment of security services and scaling of their functional capabilities [61].

(B) **Enhancement to network security**

- Global and real-time view: The centralized management architecture of SDN renders a real-time global view of a distributed network, including topology, routes, and traffic statistics [53]. This capability is particularly useful for detecting and responding to cooperative attacks, such as DoS/DDoS attacks.
- Dynamic threat response: NFV together with SDN provide dynamic real-time response to threats [62]. SDN can be utilized to rearrange service chains or traffic route to optimize the performance of virtualized security services.

12.8 Conclusion

Health 4.0 will play a key role in future healthcare systems. These digitally connected healthcare systems will provide better quality personalized medical services. However, their security issues should be thoughtful addressed to ensure system reliability and user privacy. This is particularly important when 5G networks come into play its role as the network backbone to connect the different components of cyber-physical healthcare systems.

Therefore, proper security solutions are required to secure the entire systems, including the core components and their connected networks. The aforementioned security requirements are recommended to be taken into account when drawing security strategies and making choices of security schemes. Moreover, attention should be given to take advantages of NFV and SDN in deployment of these schemes.

References

1. Newsroom (ed) (2014) Mhealth, What is it?—Infographic. https://ec.europa.eu/digital-single-market/en/news/mhealth-what-it-infographic. Accessed 24 Sept 2016
2. Collins FS, Varmus H (2015) A new initiative on precision medicine. New England J Med 372(9):793–795
3. 5G-PPP (2014). https://5g-ppp.eu. Accessed 24 Sept 2016
4. Choi JS, Zhou M (2010) Recent advances in wireless sensor networks for health monitoring. Int J Intell Control Syst 14:49–58

5. Vervloet M, Linn AJ, van Weert JC, De Bakker DH, Bouvy M, Van Dijk L (2012) The effectiveness of interventions using electronic reminders to improve adherence to chronic medication: a systematic review of the literature. J Am Med Inform Assoc 19(5):696–704
6. Rashidi P, Mihailidis A (2013) A survey on ambient-assisted living tools for older adults. IEEE J Biomedical Health Inform 17:579–590. doi:10.1109/JBHI.2012.2234129
7. Zhang Y, Qiu M, Tsai CW, Hassan MM, Alamri A (2015) Health-CPS: healthcare cyber-physical system assisted by cloud and big data
8. IEEE Standards Association, 802.15. 6-2012 IEEE standards for local and metropolitan area networks–Part 15.6: Wireless Body Area Networks
9. Bangash J, Abdullah A, Anisi M, Khan AW (2014) A survey of routing protocols in wireless body sensor networks. Sensors 14:1322–1357. doi:10.3390/s140101322
10. Zigbee A (2012) ZigBee Security specification overview. http://www.zigbee.org/download/standards-zigbee-specification/. Accessed 24 Sept 2016
11. Bluetooth (2010) Bluetooth specifications. https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737. Accessed 24 Sept 2016
12. Augustin A, Yi J, Clausen T, Townsley WM (2016) A study of LoRa: long range and low power networks for the internet of things. Sensors 16(9):1466
13. Delmastro F (2012) Pervasive communications in healthcare. Comput Comm 35:1284–1295. doi:10.1016/j.comcom.2012.04.018
14. Sun J, Zhu X, Zhang C, Fang (2012) Security and privacy for mobile health-care (m-Health) systems. In: Elsevier BV (ed) Handbook on securing cyber-physical critical infrastructure, pp 677–704. doi:10.1016/B978-0-12-415815-3.00027-3
15. Dariz L, Selvatici M, Ruggeri M, Abrishambaf R (2016) Smart and wearable wireless sensors: scenario analysis and communication issues. In: Proceedings of the 2016 IEEE international conference on industrial technology (ICIT), IEEE, pp 1938–1943. doi:10.1109/ICIT.2016.7475063
16. News Standards (2016) IEEE Commun Mag 54(7):14–16. doi:10.1109/MCOM.2016.7514158
17. Gozalvez J (2016) New 3GPP standard for IoT [Mobile Radio]. IEEE Veh Technol Mag 11 (1):14–20. doi:10.1109/MVT.2015.2512358
18. Advanced Pro Heath Jr RW, Honig M, Nagata S, Parkvall S, Soong AC (2016) LTE-Advanced Pro: part 3 [guest editorial]. IEEE Commun Mag 54(7):52–53
19. Wu H, Cai J, Xiao H, Chen Y, Li YNR, Lu Z (2016) High-rank MIMO precoding for future LTE-Advanced Pro. In: Proceedings of the 2016 IEEE 83rd vehicular technology conference (VTC Spring), IEEE, pp 1–6
20. Riazul Islam SM, Daehan K, Humaun Kabir M, Hossain M, Kyung-Sup K (2015) The internet of things for health care: a comprehensive survey. IEEE Access 3:678–708. doi:10.1109/ACCESS.2015.2437951
21. Agrawal VM, Chauhan H (2015) An overview of security issues in mobile ad hoc networks. Int J Comput En Sci 1:9–17. ISSN: 0976-6367
22. Jo M, Han L, Tan ND, In HP (2015) A survey: Energy exhausting attacks in MAC protocols in WBANs. Telecommun Syst 58:153–164. doi:10.1007/s11235-014-9897-0
23. Kang J, Adibi S (2015) A review of security protocols in mHealth wireless body area networks (WBAN). In: Communications in computer and Information Science, ed: Springer, Berlin, pp 61–83. doi:10.1007/978-3-319-19210-9_5
24. Silva BMC, Rodrigues JJPC, de la Torre Díez I, López-Coronado M, Saleem K (2015) Mobile-health: a review of current state in 2015. J Biomed Inform 56:265–272. doi:10.1016/j.jbi.2015.06.003
25. Kart F, Miao G, Moser LE, Melliar-Smith P (2007) A distributed e-healthcare system based on the service oriented architecture. In: Proceedings of the IEEE International conference on services computing, SCC 2007, pp 652–659. doi:10.1109/SCC.2007.2
26. Egbogah EE, Fapojuwo AO (2011) A survey of system architecture requirements for health care-based wireless sensor setworks. Sensors 11:4875–4898. doi:10.3390/s110504875

27. Ullah S, Mohaisen M, Alnuem MA (2013) A review of IEEE 802.15.6 MAC, PHY, and security specifications. Int J Distrib Sens Netw 2013:1–12. doi:10.1155/2013/950704
28. Kumar P, Lee HJ (2011) Security issues in healthcare applications using wireless medical sensor networks: a survey. Sensors 12:55–91. doi:10.3390/s120100055
29. Latré B, Braem B, Moerman I, Blondia C, Demeester P (2010) A survey on wireless body area networks. Wireless Netw 17:1–18. doi:10.1007/s11276-010-0252-4
30. Hayajneh T, Almashaqbeh G, Ullah S, Vasilakos AV (2014) A survey of wireless technologies coexistence in WBAN: analysis and open research issues. Wireless Netw 20:2165–2199. doi:10.1007/s11276-014-0736-8
31. Butun I, Morgera SD, Sankar R (2014) A survey of intrusion detection systems in wireless sensor networks. IEEE Comm Survey Tuts 16:266–282. doi:10.1109/SURV.2013.050113.00191
32. Sawand A, Djahel S, Zhang Z, Nait-Abdesselam F (2015) Toward energy-efficient and trustworthy eHealth monitoring system. China Commun 12:46–65. doi:10.1109/CC.2015.7084383
33. Saleem K, Derhab A, Orgun MA, Al-Muhtadi J, Rodrigues JJ, Khalil MS, Ali Ahmed A (2016) Cost-effective encryption-based autonomous routing protocol for efficient and secure wireless sensor networks. Sensors 16(4):460
34. Group IT (2012, 2016). IEEE 802.15 WPAN Task Group 6 body area networks. Available via http://www.ieee802.org/15/pub/TG6.html. Accessed 24 Sept 2016
35. Suo H et al (2012) Security in the internet of things: a review. In: Proceedings of the 2012 international conference on computer science and electronics engineering (ICCSEE)
36. Schneider P, Horn G (2015) Towards 5G security. In: Trustcom/BigDataSE/ISPA, 2015 IEEE
37. Schneider D (2012) The state of network security. Netw Security 2012(2):14–20
38. Sergey S, Sieber M, Norden M (2015) Azure RMS security evaluation guide. Microsoft
39. Dowlin N, Gilad-Bachrach R, Laine K, Lauter K, MNaehrig M, Wernsing J (2015) Manual for using homomorphic encryption for bioinformatics. Microsoft Research
40. Naveed M, Kamara S, Wright CV (2015) Inference attacks on property-preserving encrypted databases. In: Proceedings of the 22nd ACM SIGSAC conference on computer and communications security—CCS'15, pp 644–655
41. Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Perlner R, Smith-Tone D (2016) NISTIR 8105 Draft—Report on post-quantum cryptography
42. Reimsbach-Kounatze C (2015) The proliferation of 'Big Data' and implications for official statistics and statistical agencies. Christian Reimsbach-Kounatze
43. Leimbach T, Hallinan D, Bachlechner D, Weber A, Jaglo M, Hennen L, Nielsen RØ, Nentwich M, Strauß S, Lynn T, Hunt G (2014) Potential and impacts of cloud computing services and social network websites
44. Khattak HAK, Abbass H, Naeem A, Saleem K, Iqbal W (2015) Security concerns of cloud-based healthcare systems: a perspective of moving from single-cloud to a multi-cloud infrastructure. In: Proceedings of the 2015 17th international conference on e-health networking, application and services (HealthCom), IEEE, pp 61–67
45. Sajid A, Abbas H, Saleem K (2016) Cloud-assisted IoT-based SCADA systems security: a review of the state of the art and future challenges. IEEE Access 4:1375–1384
46. Mitra RN, Agrawal DP (2015) 5G mobile technology: a survey. ICT Express 1(3):132–137
47. Gupta A, Jha RK (2015) A survey of 5G network: architecture and emerging technologies. IEEE Access 3:1206–1232
48. Bleicher A (2013) The 5G phone future [News]. IEEE Spectr 50(7):15–16
49. West DM (2016) How 5G technology enables the health internet of things
50. Zheng J et al (2013) Emerging wearable medical devices towards personalized healthcare. In: Proceedings of the 8th international conference on body area networks. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Boston, Massachusetts, pp 427–431

51. Ojanen T (2016) Making the essence of fundamental rights real: the court of justice of the European Union clarifies the structure of fundamental rights under the charter. Eur Const Law Rev 12(02):318–329
52. Ferrer-Roca O, Méndez DG (2012) Health 4.0 in the i2i Era. Int J Reliable Qual E-Healthc (IJRQEH) 1(1): 43–57
53. Abdelwahab S et al (2016) Network function virtualization in 5G. IEEE Comm Mag 54 (4):84–91
54. Hakiri A, Berthou P (2015) Leveraging SDN for the 5G networks, in software defined mobile networks (SDMN). Wiley, New York, pp 61–80
55. Milenkoski A et al (2016) Security position paper network function virtualization. https://downloads.cloudsecurityalliance.org/assets/research/virtualization/Security_Position_Paper-Network_Function_Virtualization.pdf. Accessed 25 Sept 2016
56. Agyapong PK et al (2014) Design considerations for a 5G network architecture. IEEE Comm Mag 52(11):65–75
57. Sgandurra D, Lupu E (2016) Evolution of attacks, threat models, and solutions for virtualized systems. ACM Comput Surv 48(3):1–38
58. Myerson J (2016) Addressing NFV security issues in the enterprise. http://searchsecurity.techtarget.com/feature/Addressing-NFV-security-issues-in-the-enterprise. Accessed 19 Sept 2016
59. Au D (2013) Network virtualization and what it means for security. http://www.securityweek.com/network-virtualization-and-what-it-means-security. Accessed 18 Sept 2016
60. Liyanage M et al (2015) Leveraging LTE security with SDN and NFV. In: Proceedings of the 2015 IEEE 10th international conference on industrial and information systems (ICIIS)
61. Yan Z, Zhang P, Vasilakos AV (2015) A security and trust framework for virtualized networks and software-defined networking. Security Comm Netw, Security and communication networks. doi:10.1002/sec.1243
62. Andress J, Winterfeld S (2014) Chapter 10—Computer network attack, in cyber warfare. Syngress, Boston, pp 181–192 (Second Edition)