CHAPTER 14

Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards

PIJUSH KANTI DUTTA PRAMANIK[a] • GAURAV PAREEK[b] • ANAND NAYYAR[c]
[a]National Institute of Technology, Durgapur, India; [b]National Institute of Technology, Goa, India; [c]Duy Tan University, Da Nang, Vietnam

1 INTRODUCTION

As a child, we remember, when we used to get sick, our family doctor was called upon at home. We rarely had to visit the doctor's place unless the family doctor was out of town or it was a critical case required consultation with other physicians. But the scenario is reversed today. It is a very rare case that doctors visit the patients' house. We have to go to the clinic whenever we need to visit a doctor. Besides other social and economic reasons, the major reason behind this, probably, the alarmingly decreasing ratio of physicians and the general population. For instance, as per National Health Profile's latest data, released by the Central Bureau of Health Intelligence, India, across the country, for approximately 11,082 people only one allopathic government doctor is available [1].

This changed health care scenario has affected patients from urban and rural areas differently. For urban patients, it is an economic problem. People have to take time off their work, drive or travel to the clinic, and spend a significant amount of time there. This causes productivity loss and a decrease in GDP and revenue. If the visit to the doctor is frequent and regular, as in the case of chronic patients, the loss will be more. But for rural people, the degree of suffering is much more mainly due to the absence of proper healthcare infrastructure in rural areas. If we consider the Indian scenario, out of 1.33 billion people, 70% are living in villages and a majority of which do not even have the basic and minimum healthcare facility. In many villages, even if there is some government medical center, they have no qualified physicians. Getting specialist doctors is out of a dream. In India, nearly 80% of doctors, 75% of pharmacies, and 60% of hospitals are in urban areas [2]. Of all the medical visits in India, nearly 86% are made by rural peoples, and the majority of them have to travel more than 100 km to avail healthcare facility [3], often spending a month's wage. Because of the inaccessibility of primary healthcare, these people sought for medical help at the later stage of the disease-cycle. This increases the medical expenses by nearly 1.5 times compared to those from urban areas. And approximately 80% of this cost is borne by themselves [4], most often by selling their assets, farmlands, and homes. This pushes them below the poverty line further.

Remote healthcare has come out as a promising way out of this challenge in the healthcare scenario. In this method of health care service, patients do not have to move to the clinics to visit a doctor in case of need of medical help. They can communicate with a remote city-based physician with the help of telecommunication and advanced features of ICT. Physicians diagnose the patients remotely and prescribe treatments and medicines accordingly. It is expected that with proper implementation of remote healthcare, 76% of rural patients need not have to go beyond their village for medical care [2]. Remote healthcare offers several benefits (see Section 2.2) and is capable of changing the healthcare crisis, especially for those people who are underserved and do not have easy access to urban healthcare facilities as well as for elderly peoples.

Remote health care is achieved through telemedicine and remote monitoring. Telemedicine refers to a system that allows patients from remote and rural areas to get a consultation from distance doctors. Whereas remote health monitoring allows doctors to continuously monitor patients remotely using health monitoring systems that are connected to the Internet. Though

Telemedicine Technologies. https://doi.org/10.1016/B978-0-12-816948-3.00014-3

telemedicine and remote monitoring seem to be different, in the waking of RFID [5], Internet of Things (IoT) [6], pervasive systems [7], healthcare data analytics [8], etc. and successful use of these technologies in healthcare, the differences between the two are getting blurred. The popularity and usability of nanosensors and IoT along with the advancement of high-bandwidth, energy-efficient wireless technologies, remote health monitoring has become more practical and affordable. More often, telemedicine is getting blended with remote monitoring for precision diagnosis and medication. In this text, we refer remote health care as both to remote health monitoring and telemedicine.

Though it has promising potentials, successful implementation of remote healthcare is not free of concerns. Several challenges need to be addressed to get the full utilization of remote healthcare (see Section 2.3). But, being a networked system and since healthcare data are sensitive to mishandling, maintaining security, privacy, and confidentiality are the primary concerns and of foremost priority. Doctors, in remote healthcare, heavily depends on the digital health record for diagnosis. Hence information integrity and reliability are essential for error-free diagnosis. These systems are vulnerable to a wide range of security threats. The threats can emerge at each level of a remote healthcare system, for instance, at data collection, data transmission, data storage, and data access levels [9]. In some cases, inadequate awareness and training lead to these threats. But, most of them have been surfaced because security threats are inherent in multi-attributed distributed networked systems and implementing end-to-end security in such a complex and the evolving system is really challenging [10]. The security threats can be mitigated by opting measures such as user authentication, access control, audit control, enforcing information integrity, confidentiality, and privacy, non-repudiation, secured data transmission, etc. Furthermore, considering the evolving nature and proliferating coverage of the threats, predictive and proactive measures are required [10].

Besides the aforementioned threats, another issue that holds back remote healthcare is that the users' trust in remote healthcare and its acceptability to the masses. It is necessary to infuse confidence to the patients in adopting the remote healthcare system. In this direction, patients' privacy and confidentiality need to be protected. In doing so, the obvious challenge faced is that having the balance between confidentiality and availability. Doctors will be able to provide better quality healthcare service if the patient's medical history and clinical records are accessible from other sources as well. More the patients' data are integrated and available across different medical service applications the patient can obtain more quality, time-saving, and economical healthcare services, and importantly, from anywhere because sharing medical data helps in realizing pervasive healthcare [7]. But again, all the data cannot be permitted to be accessed by all because of security and privacy reasons. It is to be determined wisely, which part of the patients' data should be confidential and which part should be pervasively accessible. The optimal balance between these two will result in delivering the best possible healthcare to the patients [9].

The rest of the chapter is organized as follows. Section 2 covers the basics of remote healthcare, mentioning its benefits and challenges. It differentiates between "health care" and "healthcare". Telemedicine and remote monitoring, the two approaches of remote health care, and their components and architecture are discussed briefly. Section 3 is devoted to security and privacy issues of remote healthcare. It presents the roles of various entities and their impact on the security of the health care system. It then highlights vital security and privacy issues in remote healthcare, formulates the concrete security requirements and describes a range of solutions to satisfy these requirements. The security standards for local and wide-range network transmission are described. The application-level security solutions like access control, privacy and reliability are also presented. It also presents important trade-offs and the challenges facing the implementation of security solutions in remote healthcare. Future of remote healthcare security is also discussed briefly. And finally, Section 4 concludes the chapter.

2 REMOTE HEALTHCARE

The traditional approaches of medical treatment models are not sufficient to address the challenge of the ever-growing demand for cost-effective health services either in a hospital or in other medical care units. Information and Communication Technology (ICT) being the key factor in the development of the latest medical models which has proposed advanced biosensors, efficient patient records management, and digital and computerized medical equipment. These advancements have facilitated bridging the gap between remote and underserved locations and infrastructurally equipped hospitals with the help of seamless information exchange. Such models are termed as *remote healthcare* or *e-health*. In simple words, remote healthcare is to take care of the patient's

health from a distant, i.e., remotely. The vision of remote healthcare is to provide healthcare services to patients outside of traditional healthcare establishments, usually at home.

Remote healthcare plays a crucial role in acquisition, management and exchange of personal as well as medical information of the patient, making it easier to follow treatment procedures without moving the patient, as well as the medical staff, here and there. Information exchange is the primary principle of remote healthcare. It should be done in a highly structured manner to support stakeholder interactions in the pathway, both in terms of self-management and lifestyle promotion and disease detection. The exchange of information should be such that, it assures efficient coordination and transition among the various phases to facilitate process continuation.

2.1 "Remote Health Care" Versus "Remote Healthcare"

Here, we would like to make clear the misunderstanding between the two terms used in the literature: "remote health care" and "remote healthcare".

Remote health care: The term "remote health care" can be defined as the use of existing and emerging ITeS and technologies to provide and support remote delivery of health care. It signifies the actions that are carried out to monitor and improve patients' health remotely. Remote health care is referred in the context of remote monitoring, remote diagnosis, e-imaging, remote medication, remote emergency support, remote consulting, etc.

Remote healthcare: The term "remote healthcare" (sometimes referred as telehealthcare) is used in a broader perspective. Remote healthcare refers to the system or industry that supports remote health care and may include other services related to health care, besides the clinical operations, such as logistics, e-commerce and e-marketing of health care, decision support, e-business intelligence in health care, remote home care applications, training and e-learning, online transactional transmissions, etc.

In summary, "remote health care" realizes "remote healthcare" whereas "remote healthcare" facilitates in providing "remote health care".

2.2 Benefits of Remote Healthcare

The key benefits of remote healthcare are as follows:

- Medical services are easily accessible to remote patients.
- Patients don't have to travel long to see doctors. This saves time and money.
- Patients feel less stressed being treated at home or near home, among the family and friends.
- If medical care is easily accessible people are less likely to delay care. Early diagnosis and treatment not only results in better and faster recovery and minimized chance of fatal health consequence but also reduces medical expenses.
- Emergency services and intensive care services, to some extent, can also be delivered remotely.
- Reduction in the need for and better utilization of emergency rooms and ICUs.
- Contagious diseases are managed better by isolating the affected patient and initiating early treatment.
- Shortage of medical professionals and nursing staffs can be addressed by remote healthcare.
- Specialist doctors can attend more patients.
- Remote healthcare curtails the traveling time for accessing medical services, waiting periods at the clinic, contact time with doctors, and duration of hospitalization. This saved time minimizes the productivity loss in organisations which in turn improves the national GDP.
- As an additional benefit, remote healthcare helps the environment by reducing carbon footprint due to less traveling.

2.3 Challenges in Remote Healthcare

Implementing remote healthcare systems are not straight forward. There are several challenges in terms of infrastructure, operations, management, policy, standards, legal, awareness, acceptability, etc. are needed to be addressed. Besides security and privacy which are elaborately discussed in Section 3, below some of the other factors that need to be focused on to achieve the real goal of remote healthcare are mentioned [11].

- Deficiency of adequate infrastructure.
- Lack of proper integration with the legacy and traditional healthcare systems.
- Shortage of specialized and skilled healthcare professionals.
- Lack of awareness and trust. People, by nature, are resistant to changes and reluctant to have faith in new services.
- Inadequate number of service centers for the medical equipment used in remote healthcare.
- Absence of global standards for different equipment and file formats for health data and storage. This complicates the interoperability.
- Absence of a legal framework precisely defining the responsibilities and liabilities of every stakeholder and course of legal actions in case of non-adherence.

- Absence of national e-healthcare policy and regulations.
- Nonexistence of comprehensive and national strategies regarding remote healthcare.

2.4 Remote Health Care Approaches

Remote health care generally has two main approaches: telemedicine (sometimes referred to as e-medicine) and remote health monitoring (sometimes referred to as telecare) [12].

2.4.1 Telemedicine

2.4.1.1 What is telemedicine and how it works?. Telemedicine is one of the first initiatives toward remote healthcare. It was proposed nearly 30 years back with the purpose of providing affordable medical services, especially for the unprivileged people, in terms of the medical facility, from the places where sufficient healthcare infrastructure is absent. In telemedicine, physicians interact with the patients located in remote and rural areas using information and telecommunication technologies. At the patient's end, at the local health center, the local health technicians act as mediators. They do the preliminary assessment of the patients, conduct basic diagnostic tests, note the information of vital parameters and enter all these relevant information into the electronic health record. These information are sent to the remote physician who assess the patient's health condition, diagnose and sends back the prescription or suggestions to the local health center. The doctors may use video and audio connections for real-time interaction with the patients in order to provide real-time consultations. Doctors may use other sophisticated remotely controlled medical examination equipment such as close-up cameras, microscopes, dermascopes, etc. for better assessment [13]. Modern telemedicine systems make use of IT technologies like high-resolution 4K monitors, high-performance communication networks, telecommunications, responsive websites and pervasive smart devices [7]. Today's telemedicine systems are highly integrated with the cloud and edge computing [14], IoT [15] and sophisticated communication systems.

To build an effective telemedicine system, the system should satisfy the following requirements:

- Efficient to handle emergency medical cases at remote sites and live consultant available with quick response.
- Enhanced intensive healthcare provision by providing telemedicine unit to ICU doctor and medical unit with the in-house telemetry system.
- Facilitates home monitoring by incorporating telemedicine unit at the home of the patient while the other units remain at the main hospital.

2.4.1.2 Infrastructural components of telemedicine. The following components form the backbone of any telemedicine system:

Local healthcare unit: In a telemedicine system, remote healthcare unit is regarded as a small health center, usually located in a rural or remote area. This is the primary point of contact between patients and healthcare givers. These health centers may comprise a computer with customized medical software connected to a few diagnostic instruments like ECG, EMG, X-ray, etc. for acquiring the health status of the patients. The major components found at a typical local healthcare center are mentioned below:

- Medical peripherals: These digital devices enable the local healthcare attendant to gather patient's vitals, monitor progress, view ultrasounds, check-up lung and heart, and capture images of skin, ears, eyes and other areas. The telemedicine medical kits comprise stethoscopes (interactive or telephonic-based), vital signs monitors, ECGs, spirometers and holters, retinal cameras, ultrasound probes, etc.
- HD Camera: To facilitate remote communication in a smooth manner via video conferencing, a high-quality HD camera is required. It is responsible for exchanging live feeds between patient and doctor from a distance.
- Computer: Health data processing, controlling and overall operations of records management, handling basic medical equipment's, performing communications are done with the help of a computer.

Data communication networks: The records acquired at the local healthcare unit are sent to the doctor remote at a remote hospital. For reliable and robust transmission, a strong data communication network is required to be integrated within the telemedicine system. The audio-visual communication is generally done using public telephone networks, and the recorded digital data are transmitted through IP-based networks using the standard network protocols, e.g., TCP/IP, HTTP, SMTP, etc. The specific network structure of any telemedicine system largely depends on the geographic factors of the area that will be served by the network and the type of local users there. The telemedicine units are equipped with standard network communication units like ADSL, Broadband, 3G/4G/LTE depending on the area to facilitate information exchange between the centers.

Medical database/EHR: The medical database, also called an electronic health record (EHR), is a centralized database that stores patients' data. The medical database in telemedicine is comprised of the following components:

- Subjective description: Refers to the details of patients, their health information with disease history. The information may contain attributes such as symptoms, duration, and description, along with other comments.
- Objective description: Comprise of all the results noted by the doctor in the previous description and comparison with regard to the current situation of the patient.
- Assessment: Details regarding the doctor's diagnosis as well as disease description based on the symptoms of the patient.
- Plan: A complete structure designed and implemented by the doctor regarding diagnosing the patient right from the start to completion of the treatment procedure.
- Application interface: To access the database, it is equipped with a proper web-based application interface which comprises the following modules:
  - Doctor registration: In order to become the part of the telemedicine program, every doctor has to properly register as a new doctor and after registration, the database provides information with regard to only those patients allocated to a specific doctor.
  - Patient registration: To become part of a telemedicine program to take live support from the medical practitioners, every patient has to register the portal with regard to details with valid information. This can be done by the medical staff at the local health center on behalf of the patient.
  - Portal interface: This interface is regarded as the middleware between the doctor at the frontend and database at backend. The doctor can make use of the portal to track all the progress, get notified updates of patients, access all types of images, alter information, interact with the patient live, update the information at the backend.

The database server is tightly integrated into the system to facilitate records storage of patients. The server may be hosted in the cloud for better access and management inexpensively.

Doctor unit/main hospital: The information acquired at the local health center is sent to the doctors at a remote hospital for examining the reports, diagnose, interact with patients and provide appropriate treatment support via tele or video conferencing. The hospital is responsible for collecting the data transmitted by the local healthcare unit. At this end, the doctors sit in the room with ICT-enabled equipment to provide live support to the patients and observe the data transmitted from remote centers. In order to facilitate communication, various audio/video devices (e.g., smartphones, laptops, PCs, etc.) are required. This unit is also connected to the central medical database server.

Online telemedicine portals/websites: To make the telemedicine system interactive, suitable websites and apps, both for PCs and mobiles, are required to be designed and developed. These portals are ideally user-friendly and simple to use with very fewer technicalities so that both patients and medical staffs will be prompted to use the system. With user-friendly online portals, telemedicine provides the following advantages:

- Easy and convenient access to healthcare services.
- Improved QoE (quality of experience) for all the stakeholders.
- Speedy medical follow up.
- Maximizing medical care efficiency.
- User satisfaction attracts new users which leads to market growth.
- Reduced liability because of the completely digital audit trail.

As the use of smart mobile devices (smartphone and tablets) is in continuous upsurge [16], mobile apps are getting more popular. These mobile apps enable users to use telemedicine systems pervasively. The apps are capable of triggering an alarm to alert the doctor in case of an emergency.

2.4.1.3 General architecture of telemedicine and its functionality.

Telemedicine systems, in general, follow a hierarchical tiered structure which includes the following:

- Level 1: Local/remote telemedicine center. These are the local or primary healthcare unit located in rural and remote areas.
- Level 2: City/district hospital. Local/rural health centers are connected to the city/district hospital. The district hospital, optionally, may further be connected to the state hospital.
- Level 3: Speciality center. The city hospital is connected to the speciality centers for disease-specific further assistance.

Fig. 14.1 presents a general architecture of a telemedicine system. A patient requiring medical attention

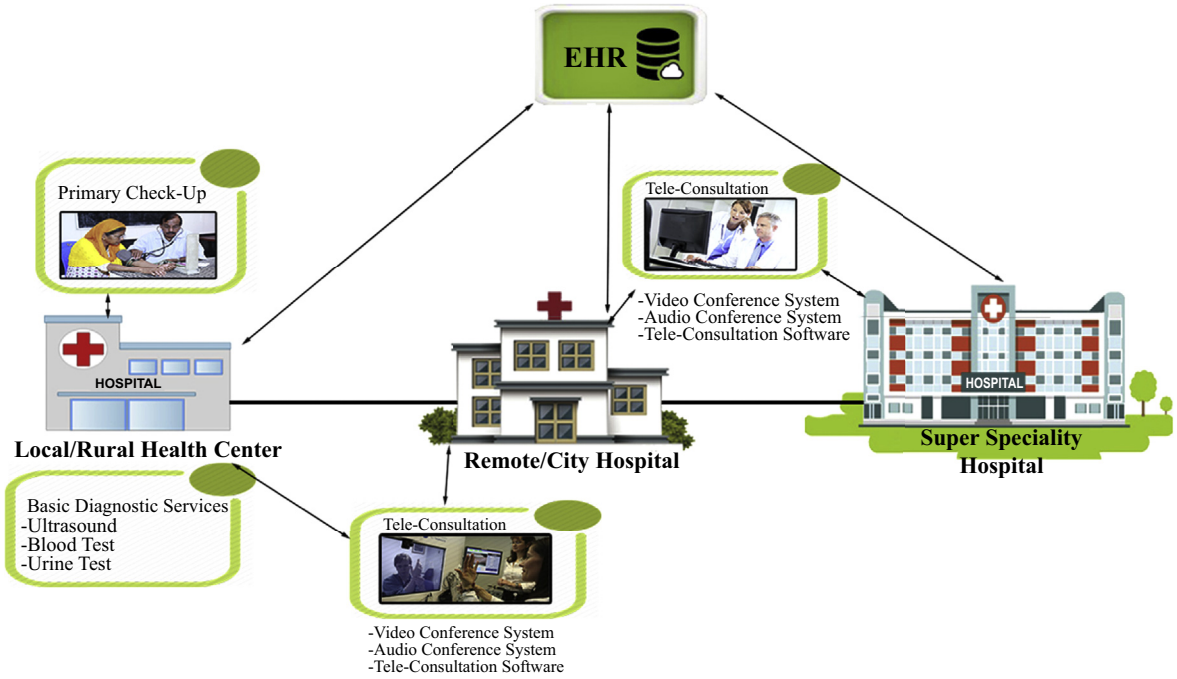

FIG. 14.1 A general telemedicine system.

approaches the nearby local health center where a local health professional (may not be a certified doctor) attends the patient and does the primary health check-up. This unit consists of basic diagnostic equipment and tele-consultation devices linked via PC and Internet to the city hospital. The primary responsibility of the local healthcare unit is to acquire all the vital statistics of the patient in terms of physiological data (e.g., blood, urine, etc.) and images (e.g., ultrasound) and transmits the data to the remote city hospital. After receiving the records, the remote medical practitioner goes through every detail, before proceedings with live Interaction with patients. After carefully examining the basic vital signs, the meeting is booked online between doctor and patient at remote healthcare unit. The doctor makes use of an audio or video conferencing system as well as automation live feeds to have live interaction with the patient. These remote hospitals are connected to a centralized database where all the data of the patient as well as other details and even the recorded audio/video interaction between doctor and patient are also stored. The stored information can be accessed using mobile apps or web-based interface. The main hospitals are also linked to specialist hospitals to provide specialized support to the patients in case of an emergency and these specialized hospitals have same teleconferencing units enabled to support remote patients.

2.4.1.4 Security vulnerability points in telemedicine.

A telemedicine system requires the data collected through equipment at the local hospitals to be transmitted to the remote super speciality hospital either through live sessions or through web-based applications. Privacy, integrity and authenticity of the collected data must be ensured in a telemedicine system to ensure timely and correct diagnosis and treatment without any abuse of privacy of patient's data. Following are the points of potential security and privacy vulnerabilities in telemedicine systems:

- **Local health center:** Incorrectly calibrated medical equipment is a source of potential failure of the telemedicine system. If the patient data collected by the equipment are incorrect, the diagnosis of the patient suffers serious integrity issues.
- **EHR:** If the doctors in the super-speciality hospital of a telemedicine system can be online, the data is transferred through live streaming or audio/video conferencing. Provided the data is collected using accurate and precise equipment, there is little chance of being modified by any outsider for creating the malicious effect. Assuming that no individual with

malicious intent has access to the personal, standalone storage of the doctors in hospitals, the patient data transmitted using standard security protocols over the Internet cannot be accessed by any adversary. However, live streaming is not always feasible because doctors may not be online. In such a case, data is transferred through a web-based application interface and is stored in a database (EHRs) accessible to the doctors. Security of data stored in EHRs is critical as they store data in digital format and Internet hackers do have the potential to access confidential medical information. Another consideration while storing data in EHRs is that the data may be modified by other applications that use the same database. The integrity of data stored on EHRs may be hampered if an unauthorized application modifies the stored data. Identity management of each individual patient is critical because indexing the patient data incorrectly may result in disastrous situations. Any unauthorized access to the EHR may potentially disclose sensitive medical data. Some of the existing popular attacks on databases include SQL injection, denial of service, privilege abuse, unauthorized privilege elevation etc.

- **Remote super-speciality hospital:** The web interface at the remote super speciality hospital is prone to platform attacks as well as privacy abuse by the local staff. If the local storage at the hospital does not have proper security mechanisms, there is a threat of loss of patients' data, breach of privacy, denial of service to the patients etc.
- **Tele-consultation interface:** If the application server used for Tele-consultation does not use secure system design practices and secure communication protocols, each Tele-consultation session is prone to be attacked by an external adversary. The adversary may be interested in aborting the session, learning sensitive medical information about the patients or disrupt the timely and correct diagnosis of the patients. Some of the known attacks on the web interface and include HTTP flood, distributed denial of service attacks (DDoS) etc.
- **The network:** Networking technology used in case of telemedicine is the wired/wireless telephone network or the Internet. The former is easier to eavesdrop than the latter. For Internet communications, complex attacks exist for traffic capture and analysis, external eavesdropping, denial of service, snooping, sniffing etc. Open source tools are available for carrying out these attacks and for analyzing the vulnerability of the network and the server to these attacks.

2.4.2 Remote health monitoring

2.4.2.1 What is remote health monitoring and how it works?.

Remote health monitoring is the latest advancement in remote healthcare which aims to perform automated patient health monitoring from anywhere. Unlike telemedicine, which is basically a reactive approach of healthcare, remote monitoring is generally proactive. Through periodical monitoring of the patient's health status, the health condition is predicted, and the required measures can be taken beforehand to prevent the full manifestation of the disease. The advancement in health sensors [7], wireless sensor network (WSN) [17], and wireless body area network (WBAN) [18] has enabled physicians to check a patient's health in a continuous manner, or whenever required. Patients need not to be hospitalized; rather they are free to be at a place of their choice, generally at home. Different health sensors planted within and on the body sense different physiological data like body temperature, heart and pulse readings, blood pressure, blood sugar, brainwave, the oxygen level in blood, etc. [7]. These data are sent to the concerned health professionals who interpret them to assess a patient's health status and the requirements and recommend suitable medication or treatment accordingly. Remote health monitoring offers real-time patient observations which result in a better diagnosis. This healthcare approach is good, especially for rehabilitating patients, patients suffering from chronic illness, patients who are under mental and physical therapy, and elderly people. The remote health monitoring enables to detect early symptoms of diseases which, in turn, reduces the emergency department visits, hospitalization expenses, duration of stay in hospitals. This increases the overall quality of the patient's life.

2.4.2.2 Infrastructural components of remote health monitoring.

The following components make up a remote health monitoring system in general:

Patient monitoring unit: This unit may be located at a local care unit or at the patient's home. This unit consists of high-end nano-scale bio-sensors for automated reading of a patient's physiological data and overall monitoring of the patient's health. Some of the most common health data collected are oxygen level, heart rate, non-invasive blood pressure, body temperature, respiration, etc. It also may comprise portable medical equipment's to ensure the patient's mobility and flexibility during treatment. Following

are the main parts of remote health monitoring that belong to a local care unit:

- WBAN: The primary and major component of a remote health monitoring system is the WBAN which incorporates various biosensors and wearables [7]. These sensors are embedded within or on the patient's body for collecting physiological data continuously. The collected data are assessed for diagnosis, treatment, and overall medical care. With technology enhancements, several medical sensors are proposed which are capable of performing simple as well as some sophisticated jobs such as a temperature reading, skin condition prediction cancer detection, heart attack prediction etc. Following are some examples of sensors used for remote monitoring [12]:
  - Wearable sensors
  - Ingestible sensors
  - Epidermal sensors
  - Blood sampling sensors
  - Tissue embedded sensors

  The sensor to be used depends on the type of disease and vital statistics of patients to be monitored. The sensors, in general, comprised of five subcomponents:
  - Sensor: An embedded chip to detect the physiological data from the patient's body.
  - Microcontroller: Performs very basic level data processing (e.g., data compressions) locally. It also coordinates the functionality of all other components comprising the sensor node.
  - Memory: Facilitates the temporary storage of data.
  - Wireless communication unit: Sends the sensed data to the coordinator to facilitate all communication between nodes to transmit the data wirelessly.
  - Battery Unit: To power on the batteries.
- Coordinator/collector: It is regarded as the central command station of a particular remote health monitoring system. The primary responsibility of a collector is to collect the sensed data from all the sensors, store them provisionally, pre-process (e.g., cleaning and filtering) and send to the remote server through a network gateway.
- WLAN: The communication between sensors and the coordinator is realized through a dedicated wireless LAN (WLAN) or WSN. The most popular WSN technologies used for this purpose are RFID, ZigBee, UWB, BLE, etc. Star topology is most commonly used as the network structure for this purpose.
- Network gateway: To transmit the information at remote locations, all the information is routed via a gateway. The gateway (usually, a dedicated router) acts as the bridge between remote centers as well as remote hospitals for information exchange.

WAN: The sensor data are transmitted to a remote server mainly via the Internet or cellular networks like 3G/4G/LTE. To make the remote health monitoring reliable, a secured and trusted high-performance network infrastructure is required.

Remote medical server/cloud server: The data collected by the coordinator from the sensors are stored in the cloud or in a dedicated medical server. These servers facilitate remote accessing of patient data to medical practitioners. The databases are updated continuously to facilitate precision monitoring of the patient's health.

Management/monitoring unit: Doctors access the patient's data from the server to assess health condition. The doctor sends feedback to the patient and, on a need basis, recommend treatment and medication. Modern remote health servers can trigger alarms in case of abnormality in physiological data to alert doctors, hospital and also the patient. Some of the imperative components of this unit are:

- Pervasive devices: These devices [19] which include laptops, PDAs, smartphones, etc. are used to assist real-time readability of patient health information.
- Application interface: This allows doctors to interact with the remote health monitoring system. The graphically rich interface helps doctors to apprehend and analyze the health statistics easily. Most of these interfaces also allow real-time interactions between patient and physicians.

2.4.2.3 General architecture of remote health monitoring and its functionality.

Fig. 14.2 represents the general architecture of a remote health monitoring system. As discussed in Section 2.4.2.2, the primary component of a remote healthcare unit is the WBAN which collects patient's health-related data which are sent through the network gateway to either a cloud or a dedicated medical server from where the doctor gets access of the patient's health record and recommend treatment.

The WBAN consists of different sensors used to read different physiological data. These sensors are connected to a coordinator via WSNs such as ZigBee, Bluetooth, WLAN, etc. The primary role of a coordinator is to maintain communication among the devices and server to facilitate reliable data exchange. Standards like IEEE 802.15.4a [20] and IEEE 802.15.6 [21] are

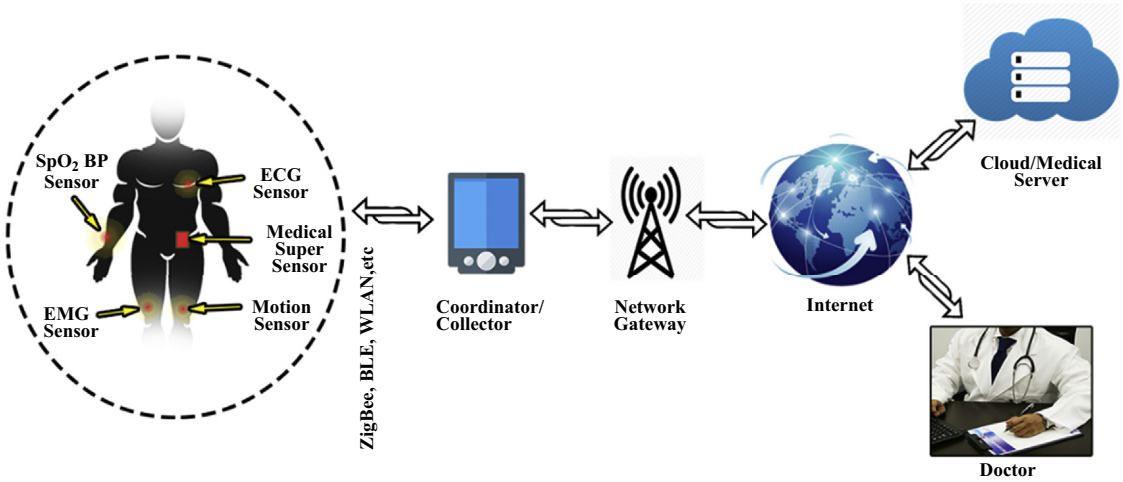

FIG. 14.2 A general remote health monitoring system.

proposed for effective WBAN communication. The coordinator is linked to the gateway whose role is to acquire data from the coordinator and transmit the data to the server over the Internet. The data is stored in a remote medical server database or cloud following the standard security measures. The data can be accessed by the patients and doctors in real time using web-based API or mobile apps to keep live track on the patient's vital signs and treatment progress. The server is also competent enough to provide suitable alerts to recognize serious health anomalies, alert medical staff in case of emergency to take immediate and required actions.

2.4.2.4 Security vulnerability points in remote health monitoring. Typically, remote health monitoring systems feature all the functionalities of a telemedicine-based remote healthcare system. Additionally, the remote health monitoring systems require the continuous and uninterrupted monitoring of health attributes of patients using a distributed network of sensors. These sensors and the personal gateway or coordinator are potential sources of security and privacy vulnerabilities. Also, with the growing size of patient information, and need to process it at a later point of time, there is a need for a fast and reliable third-party cloud storage. Here, we highlight the security vulnerabilities in these two components of remote healthcare monitoring.

- **Sensors and coordinator:** Sensors are prone to compromise attacks using which an attacker can potentially collect all the data passing through the sensor or the group it belongs to. Since all the collected data pass through the personal gateway or coordinator, compromising the coordinator can potentially reveal the values of all the health attributes corresponding to the patient. The coordinator directly interacts with the medical server through the network gateway and the Internet. The absence of proper security controls in communication may potentially lead to a privacy breach, obstruction in data delivery and denial of medical services to the patients.
- **Cloud/medical server:** In addition to being prone to failure, a medical server or Cloud can be potentially accessed by unauthorized entities through the web with the intention of producing malicious effects. In the absence of appropriate cryptographic mechanisms, the patient data stored on the medical server can be potentially accessed and/or modified by unauthorized entities including the Cloud service provider.
- **Networking:** The network over which the patient's data is transferred is always a potential source of vulnerability. This is because the nature of the Internet is public and it is exposed to all sorts of users, including the attackers motivated toward creating a malicious effect in the remote healthcare monitoring. Possible attacks on the network in remote healthcare and monitoring include Distributed Denial of Service (DDoS) attacks, session hijacking, spoofing attacks etc.

3 SECURITY & PRIVACY IN REMOTE HEALTHCARE

A great deal of functionality in WBANs for remote healthcare is achieved through the collection of data from the sensors attached to the patients' body. The data collected from various body parts is carried to the medical service provider who can be a human expert or an expert computer system. Data collection serves as a basis for not only the current advice but is also used for predicting possible future problems and can be used for medical research. It is usually the case that data collected by the sensors are transmitted to the healthcare service provider through the personal server called coordinator over a network such as the Internet [18]. Also, the data may have to be stored for a considerable period of time for processing and generating medical advice. For this, the medical service provider may use a dedicated third-party service for storing and processing the data. It is important to preserve privacy and ensure the security of patient's data. Security of patient's data ensures its availability, integrity and non-repudiation. Ideally, the patient who is the owner of the data has discretionary access over his/her health data. This means that the patient can choose to grant access to the collected data to anyone from the outside world. This section defines the security and privacy of data in remote healthcare systems, motivates the need of mechanisms for ensuring data security and privacy in remote healthcare and lists potential security and privacy risks along with their sources. This section also presents widely deployed solutions with security standards and software security protocols. As part of the future of security and privacy in remote and pervasive healthcare through WBANs, this section also briefly introduces patient-customizable security policies and their enforcement.

3.1 Entities in Remote Healthcare: Their Roles, Interests and Impact on Security

Before we highlight the security threats, security requirements, and the security solutions of remote healthcare, it is important to define its various external entities and their potential impacts on the security issues of the remote healthcare system. These entities include:

- **Patient:** Interested in the private, correct, and uninterrupted delivery of healthcare services. A patient provides his/her medical, health, and other related data to the third-party infrastructure/service provider.
- **Government agencies:** They regulate the security and privacy services incorporated in remote healthcare and monitoring by formulating policies. These policies cover the interests of the patients as well as the healthcare service provider. Additionally, these policies also define situations where the security and privacy of an individual patient's data can be overlooked for protecting the interests of a large number of people.
- **Service provider of infrastructural components:** Infrastructure required for remote healthcare is acquired from various vendors who may or may not provide all the hardware and software needed for data collection, its reliable and secure transfer over the local network and through the long-range network like the Internet to the healthcare server. Important infrastructure components include the following:
  - Sensors for data collection
  - Internal (local) short-range networking components
  - Network service provider for long-range (WAN) data communication

  These infrastructural components are usually provided by third-party vendors whose services are utilized by the hospital authorities under a contract. All these components deal with the collection and transfer of data between the patient and the remote healthcare server. In the rest of the chapter, we refer to the set of vendors supplying these components as a data collection agency. It is a mandatory requirement that these service providers are auditable under the contract and adhere to the security and privacy policy decided by the healthcare service provider.

  It must be ensured that these vendors do not learn or misuse the data collected by the devices provided by them. On the other hand, the interest of the data collection agency against any unwarranted prosecution should also be protected by having proper application-level accountability mechanisms in place.
- **Third-party storage/processing service provider:** Utilizing third-party services for maintaining and processing patient information relieves a hospital or a healthcare service provider of the operational expenditure and the cost of purchase and maintenance of expensive hardware for computing and storage. However, a third-party can be curious about the patients' data and may potentially use it for monetary benefits. If this is the case, the reputation of the hospital can be damaged, and the acceptability of remote healthcare will be limited.

3.2 Security and Privacy Threats in Remote Healthcare

Data security and data privacy are sometimes mistaken to be synonymous because the common goal of both is to protect sensitive data. Data security aims at confronting an adversary who tries to exploit loopholes in the system and steals and/or manipulates a user's sensitive personal data for which the adversary is not authorized. In many application contexts especially health-oriented services, unauthorized manipulation of patient data may potentially result in disastrous situations. This is because data collection without ensuring integrity may potentially lead to incorrect diagnosis and treatment. When a data owner provides the data to any organization, data privacy aims at deterring the organization's intentions, if any, of disclosing the data to anyone and/or misusing the data without data owner's consent. The misuse of data includes activities like unauthorized data publishing, archival for survey purposes without the patient's consent, selling the data to organisations for monetary benefits etc. Any patient who surrenders his/her health data to a hospital has no control afterward on who, apart from the hospital staff, can access the data. If indeed the hospital staff is indulged in selling patient's data, accountability mechanisms must be in place to hold the hospital staff responsible for the breach of security and privacy. This is because if personal details like health data are disclosed to any unauthorized party like the insurer of the data owner (patient), the data owner may suffer serious losses. Consider if the patient is suffering from some major ailment, it is highly likely that the patient may claim the medical insurance in the near future. Learning about the ailment of the patient, his/her insurer may sell the insurance policy to the patient at abruptly high premiums. Other problems with privacy abuse include leading to social prejudices, encouraging unethical business practices and many more. Apart from data disclosure to unauthorized entities, data misuse includes publishing it on public forums, its use for medical research without due consent from the patient etc. Broadly, the security requirements of remote healthcare include:

- Preservation of privacy of patient's data all through the storage duration.
- Prevention of unauthorized access of raw or processed data by any entity other than those authorized by the patient like hospital staff, close relatives, etc.

It is important to highlight the points of security vulnerabilities and activities that may potentially be attacked by an adversary to learn a patient's data. Also, since availability is another important factor that affects the quality of remote healthcare services, it is important to identify the potential points of failures in remote healthcare that may lead to denial of service to the patient. Sources of security and privacy threats in remote healthcare are classified based on the activities that potentially result in these threats [22]. These activities range from the collection of raw data from the patient's body through various sensors to the complex analyses of the collected data at a storage and computation server.

3.2.1 Distributed data collection and data transmission

Data of a patient can be collected from a patient's body using the sensors planted either inside the patient's body or on the body surface. Since these sensors have a limited lifetime, the sensors have to be replaced quite often over the service duration. Also, due to limited computation power, sensors are unable to perform computationally too expensive operations like asymmetric cryptographic algorithms to achieve both secrecy and access control. However, light-weight symmetric encryption algorithms and elliptic-curve cryptography algorithms are popular for encrypting data by the sensors. Usually, the network of sensors shares a symmetric encryption key under which data collected by the sensors is encrypted before transmission. The main reason for privacy and security breach in data collection phase is disclosure of the shared encryption key. This section discusses potential scenarios that may lead to the disclosure of data encryption key to any adversary. Also, data collection being an important phase demands the availability, integrity and consistency of collected data. The accuracy of the raw data collected from the patient's body determines the quality of diagnosis and treatment. The collected data must not be modified, must be consistent and delivered to the medical service provider in an uninterrupted manner. The participating entities in the data collection phase are the body-attached sensors and the personal coordinator which transmits data collected by sensors to the base station or medical service provider over a large range network like the Internet. What follows is the description of various sources of network and system security threats for the data collection phase of remote healthcare.

3.2.1.1 Sensor node or device compromise. Privacy of data communicated by the sensors nodes that reside in or around the patient's body is ensured through symmetric encryption using an encryption key stored on the local storage of each individual sensor. If any adversary

physically captures a sensor node, she can obtain the encryption key. Usually, since each sensor node has a common encryption key on their storage, the adversary not only potentially learns data collected by the compromised sensor, but also by the rest of the sensors in the network. To take control of the monitoring devices, an attacker needs to either attack the coordinator in the remote monitoring system at the patient end over the internet or go to the patient's location and physically get control of the sensors attached to the patient's body. All such methods of device compromise result in privacy breach of the raw data. There are health attributes whose value at first glance reveal no information to humans. However, since the attacker can potentially apply analysis algorithms to retrieve sensitive information, the device compromise problem can lead to the disclosure of the medical condition of the patient. On the other hand, there are health attributes whose values alone are critical, and health condition can be potentially revealed directly by learning the values of those attributes.

3.2.1.2 Dynamics of the network of sensors. The collection of sensors communicating data related to a particular patient forms a group. This group of sensors is dynamic because the sensors are short-lived and have to be replaced from time to time with the new ones. Also, the sensors may run out of battery power, and they need to be removed temporarily from the group and added again after replenishing the battery power. During the period a sensor is out of the group, any adversary may get physical access to the sensor and obtain the key material stored on it. Since this encryption key is the same for each sensor in the group, the data communication by the group of sensors to the personal coordinator and to the medical server may not be secure anymore. The adversary who has control of the encryption key can decrypt the data transmitted by the group of sensors and obtain values of health parameters of a patient in plaintext form. Adding a new sensor may be required for capturing values of any additional health parameters. If the monitoring of any health parameter required to be stopped, the corresponding sensor is removed from the group. By compromising the removed sensor and obtaining the encryption key stored on it, an adversary can obtain plaintext information communicated by the remaining sensors [23].

To understand this better, consider a group of sensors that share a common encryption key say K. Usually, an encryption key in sensor networks is used by sensors for encrypting the data before transmitting so that only those who share the same encryption key can access the transmitted data. This encryption key is a straightforward solution to the privacy problem in sensor networks. Consider that a sensor is removed from the group and is replaced with a new one. If the key material of the old sensor is not erased properly, any adversary getting possession of the old sensor may get access to the encryption key K stored on it. Now, given that K is not changed after sensor replacement, the adversary who has obtained K through compromise can sense and decrypt all the future transmissions meant for the group of sensors and transmitted to the medical service provider. Thus, keeping the encryption key constant during the course of network operation is a potential source of security issues due to the dynamics of the network of data collecting sensors.

3.2.1.3 External network eavesdropping. As discussed earlier, the patient's data is communicated to the distant processing or storage server or medical staffs in a hospital over a network like the Internet. An adversary may exploit the security loopholes in the networking technology for intra and inter-domain transmission and gain access to the transmitted data. Attacks on networking technologies are difficult but not rare, especially in the case of heterogeneous networks like in case of remote healthcare [24–27]. Typically, the goal of an external network eavesdropper is to obtain the data exchanged between communicating parties.

Eavesdropping attack can be active or passive depending on the adversary's motivation. For passive eavesdropping, an attacker can simply be sitting somewhere in the network path and capturing all the relevant network traffic for later analysis. The attacker does not need any active connection with the remote healthcare server. For active network eavesdropping, the adversary has to compromise one or more devices in the network path and install the eavesdropping software in the compromised device. This software analyses the traffic, reads the data being exchanged for the attacker, and also lets the attacker potentially modify the data being communicated. One of the popular network eavesdropping attacks is man-in-the-middle (MiTM) attack [28] where the adversary does not obtain the network session keys but establishes authenticated network connections with the communicating parties by masquerading as the authenticated communication party. This way, the adversary obtains all the secret network communications. MiTM attacks are particularly dangerous in remote healthcare systems if the attacker compromises one of the networking components. The

main motivation of network eavesdropping is to disrupt ongoing communication and create a malicious effect by reading the data being exchanged.

3.2.2 Data collection and processing

With the continuous collection of a large amount of patients' raw health-related data, arises the need to store, process and manage data. For highly responsive remote healthcare, it is required that the collected data is stored on high-speed storage networks for fast processing and reliable storage. It may be the case that the data collection agency (a hospital) utilizes the services of a third-party storage server for storing patient data. This way of utilizing third-party storage services for storing organisational data is often referred to as storage outsourcing or data outsourcing. Given a semi-trusted or untrusted third-party storage server, storage outsourcing may potentially lead to the disclosure of sensitive information of a patient. A third-party storage and processing server is best described as an honest-but-curious entity that follows the protocol decided upon by the data collection agency but may be interested in learning the data being stored. If data are stored in plaintext form, the third-party storage server can sell data to an unauthorized entity like the patient's insurer. An obvious first choice for dealing with this problem is encrypting the data before storing on a third-party storage server. Encrypting the data is not enough as most encryption algorithms limit the utility of data for processing. The encrypted data looks like a fully random string of bits. So, the results of processing on it do not yield desired results. Homomorphic encryption [29] algorithms exist that encrypt the data such that the results of computations over the original data can be recovered from the results of computations on the encrypted data. However, such encryption algorithms are computationally too expensive to be practical for a large-scale remote healthcare system that stores a huge amount of patient data. Here, we present potential security and privacy threats to data stored on distributed storage servers and processed by the third-party processing servers.

3.2.2.1 Honest-but-curious third-party storage services. The honest nature of an honest-but-curious storage server compels it to compulsorily store the data provided by its subscriber (healthcare service provider or hospital). However, due to curiosity, it may wish to learn the data stored on it or delegate access to stored data to any unauthorized entity. Consider a scenario where a healthcare service provider stores its patients' data in encrypted form on the server along with the encryption key. Since the server has been subscribed for storing data, it does so. However, the availability of encryption key means that the server can decrypt the data or potentially delegate access to data by transmitting encrypting keys to its users other than the authorized medical staff. This is a serious threat to the confidentiality and integrity of patient data.

3.2.2.2 Malicious (fully untrusted) third-party storage. For an honest-but-curious storage service provider, the only motivation is to learn stored data or delegate its access to any unauthorized entity. An even stronger adversary model applicable especially for public storage and computation service provider is that of a fully untrusted or malicious third-party. A malicious service provider not only features capabilities of a semi-trusted server but may also be motivated toward saving its storage cost by not storing the data at all. At a later point of time, when the subscriber wishes to access data, the server responds by sending bogus or modified data. One straightforward solution to this problem is storing a copy of the data locally by the subscriber. However, it is against the real motivation for storage outsourcing. Therefore, in a fully malicious setting, it is an important security challenge to assure the patients that the data being accessed from the server is indeed correct without subjecting the medical healthcare service provider to additional storage and computation overhead.

3.3 Security and Privacy Requirements in Remote Healthcare

This section defines the security requirements of a remote healthcare system using standard security terminology. It is important to identify the concrete security requirements of remote healthcare to address points of possible security vulnerabilities. These requirements encompass all the security services a remote healthcare system must provide in order to ensure the security and privacy protection of both raw and processed data by the data provider (patient and data collection agency).

3.3.1 Requirements for distributed data access security

The sensors in remote health care are distributed all over a patient's body. Accessing values of health attributes of patients should be both error-free and secure. The collection of data using a network of distributed sensors also poses scalability and accountability issues. In the below, data access security requirements of remote healthcare are formally listed with appropriate descriptions.

3.3.1.1 Data access control with revocability. As discussed earlier, selective access of patient data has to be granted to various parties. Patient data must be accessed by the medical staff. Anyone except the concerned medical staff must not be able to access the patient's data. This means that access to patient data must be given based on a policy decided by the patient. The access control policy must be defined such that it distinguishes between the authorized and unauthorized entities. Also, it must be possible to revoke access rights of any authorized entity for any piece of data.

3.3.1.2 Scalability. Ideally, computational and communication cost for accessing a scalable service does not grow linearly with the number of users of the service. In the context of data access security for remote healthcare, ensuring the security of patient data must not impose too much computation and storage cost on the users (hospital staff) or the data collection agency. Setting up and updating the access control policies of a data item should be computationally inexpensive. Security systems for ensuring private data collection and storage must also be scalable. As has been discussed earlier, the network of sensors collecting data from the patient's body and transmitting to the data collection agency is dynamic. In some specific attack scenarios, this addition of sensors to the existing group of sensors or removal of a sensor from the group may cause security problems. It must not be possible for any corrupting adversary to compromise an old removed sensor and obtain the current and/or future transmissions in plaintext form. This is called *forward secrecy*. Similarly, in the event of a new sensor joining the group of sensors, an adversary that corrupts a newly joining sensor node must not be able to access communications carried out by the sensors in the past. This is *backward secrecy*. In a group of sensors, forward and backward secrecy can be achieved by updating the encryption key following every dynamic update operation (sensor node joining or leaving) and securely availing the updated encryption key to only the current valid members of the group of sensors. Scalability of security services also concerns issues due to the growing size of the group of sensors. In case additional sensor nodes are to be added to capture data regarding more health attributes, the growing size of the group of sensors must not affect the time required for availing services to the patients.

3.3.1.3 Flexibility with non-repudiation. Having flexibility in access control mechanisms is practically motivated in remote healthcare systems. Consider a scenario where the patient's medical records have to be shared by a particular department or hospital with another hospital or department for a fixed period of time. Such cases are quite common as they may require to take expert advice from outside the hospital. A temporary access delegation of patient's data is both sufficient and necessary so that after the consultation with the outsider expert, the temporary access rights are revoked again. In such cases, the patient should reserve the rights of specifying access policies of his own and vary them according to various contexts like time, location or other events in a patient's life.

In many cases, the patient may not be in a position to provide the medical staff with his due consent for accessing and sharing data with other medical staff. In such cases, the access policy of patient data must allow someone else on behalf of the patient to delegate data access. In this case, someone is "authorized" on behalf of the patient to take policy decisions. Such temporary authorizations also form an important part of a flexible access control mechanisms for remote healthcare systems.

3.3.1.4 Accountability. An accountable security system has the capability of identifying the medical personnel who try to breach the security and privacy of the patient's data and hold him/her accountable for the same. This is important because it serves as evidence in the court of law in case of any abuse of privacy of patient's data by the hospital staff, data collection agency or the storage and processing server.

3.3.2 Requirements for distributed data storage security

3.3.2.1 Confidentiality. Confidentiality limits the use of data for only specific purposes and by only authorized entities. Data storage servers must keep patient data confidential and must be robust against compromise attacks. Since there may be many users of a storage service, confidentiality of data must be preserved even if one or more users collude with the storage service provider or unauthorized medical staff.

3.3.2.2 Dynamic integrity. Dynamic testing of the integrity of data against unauthorized modifications during storage periods of data on storage servers is very important. Any modifications may potentially lead to disastrous results as it is the degree of correctness of data that determines the correctness and effectiveness of treatment or advice. So, the remote healthcare system must not only detect malicious modifications to data but also generate alarms to the user following an

attempt of unauthorized modifications. All potential modifications during the data storage period must be detected and notified to the user.

Another way the storage server can disrupt the integrity of users' data is by not storing the data at all. Thus, ensuring dynamic integrity also includes ensuring that the data is possessed by the storage server in the first place. A method/scheme used to ensure this is called provable data possession. Similarly, a computation server may also cheat its users by not performing the desired computations at all. To ensure the integrity of the results of computations performed by the third-party computation server, a mechanism is used, known as a result verification mechanism. When result verification is combined with confidentiality of input and output data for computations, it becomes secure computation outsourcing.

3.3.2.3 Dependability. Unavailability of correct data at the time of requirement may disrupt medical services in emergency cases. This may cause life threats to the patient. All the components of a remote health monitoring system must be dependable and operable in real-time. The network of collecting sensors must be fault tolerant so that failure of a few sensors does not result in disruptions in data collection activity. The data collection server must also be available all the time for data access, data processing and communication of results to the patient. In addition to the availability requirement, dependability also concerns the correctness of the information being stored on servers of remote healthcare systems.

3.4 Privacy Policies and Regulations

Fulfilment of the security and privacy requirements discussed in the previous section depends entirely on the security and privacy policy in place. These security policies may be different for different service providers. Also, the healthcare service providers frame their policy based on the security and privacy policy of the region in which the healthcare service is provided. In remote healthcare, privacy aims at defining who is authorized for accessing a patient's data. A clear specification of the security mechanisms in place for providing quality remote healthcare to its patients enhances the acceptability of remote healthcare.

While there are rising concerns over privacy all over the world, no global definition of the right to privacy exists to date. Right to privacy of one's own body and body related aspects cannot be violated even by the state except in cases of superseding the *right to life* of a larger number of people. An efficient and durable structure of laws and policies regulates the protection of privacy in institutions that may not be government agents. An example of one such institution is remote healthcare monitoring systems. In general, systems for ensuring the security and privacy of data are a means of enforcing policies that serve the interests of the stakeholders of the system [30]. A privacy policy gives the users of service the power of self-determination through informed decision making. On the other hand, they also cater to the law of the land and pick and choose what can and what cannot be kept private about any user. In remote healthcare, the stakeholders include the patients, healthcare service provider and the government agencies [31]. The straightforward enforcement of these requirements forms a sound and robust security system for remote healthcare. Security and privacy solutions in remote healthcare systems must take into account all the policy regulations and its provisions in various scenarios. In the below, we discuss important considerations before providing security and privacy solutions in remote healthcare.

3.4.1 Identifying the data owner

In remote healthcare systems, the ownership of the patient's health data changes more frequently than other systems. Reasons that lead to dynamically changing ownership of data ranges from the consensual delegation of ownership by the patients for medical surveys, to government agencies for public interest campaigns etc. Another reason for changing ownership is the occurrence of an event(s) that invoke a clause of the privacy policy designating either the government agencies or the service provider into the owners of patient's health data. Transferring ownership of medical data is a critical activity and must be carried out in an informed manner. It is important before adopting an access policy for medical data to identify its owner. If an individual patient himself is the owner, due consent is required before any access policy comes into force. Upon transferring ownership of patient data, the access policy applicable to using patient data changes and the updated policy may or may not have to be intimated to the patient. In countries like Germany, the patient is the sole owner of his medical data and every time his data are used, a due consent is taken from the patient. This remains true even if the data is properly anonymized. In some other countries with not-so stringent privacy laws, the due consent is required to be taken only at the time of transfer of ownership of patient data.

3.4.2 Which data can be secreted and which cannot be?

A country's data access policies, especially for medical data, clearly specifies what can be hidden or kept in the private domain by the patients and what is meant to be public and what is meant to be produced when asked by competent authorities. These types of requirements concern mainly the security of the region. The outbreak of a contagious disease in a particular part of a region also requires the appropriate authorities other than the medical staff to keep track of the patient's health data. It is the duty of the data collection agency and the medical staff to comply with the access policies of the region and obtain due consent from the patients before data collection.

3.4.3 Who is in-charge in case of emergency situations?

The majority of the discussions presented above focuses the patient as the one who chooses "what and how his health data can be accessed and by whom". There may be cases where the patient himself is not in a position to take policy decisions. This results in a dilemma and may potentially obstruct the delivery of health services to the patient. In such cases, a designated person must be authorized to take such decisions. Now the question – "who authorizes a third person to have discretionary access to a patient's data" is answered in the access policy documents which again, vary from region to region and according to situations.

3.4.4 Policy reviews

There are scenarios where the access policies are reviewed and updated according to legislation from time to time. Recently, in India, the right to privacy has been codified as one of the fundamental human rights of its citizens. This has led to major policy shuffle in most of the organisations in the country. The security and privacy solutions must be durable and sustainable so that changes caused by any policy reviews can be included efficiently without much delay.

3.5 Security Solutions for Remote Healthcare

This section discusses some concrete solutions – cryptographic primitives, frameworks and security standards for all the security requirements highlighted in the previous sections. Table 14.1 summarizes the security and privacy threats in remote healthcare systems and WBAN and also their requirements and solutions.

TABLE 14.1
Summary of Security and Privacy Threats in Remote Healthcare and WBAN, and Their Requirements and Solutions.

Security Threats in WBANs	Security and Privacy Requirements	Security Solutions
Data collection and transmission	Data access control with revocability	Encryption Anonymous authentication Cryptographic access control
	Scalability	Dynamic access control and integrity assurance
	Flexibility with non-repudiation	Anonymous authentication Attribute-based encryption
	Accountability	Digital signature
Data storage and processing	Confidentiality	Encryption
	Dynamic integrity	Message digests and hashing
	Dependability	Provable data possession

3.5.1 Secure and dependable data storage and processing

As discussed earlier, data security requirements include privacy, authentication, non-repudiation and availability. A dependable data storage and processing concern dynamic integrity verification of data stored and computation results. It also involves protecting the secrecy of data and unauthorized modification. Here, we discuss a variety of solutions to suit the requirements discussed above of secure and dependable data storage and processing.

3.5.1.1 Symmetric and asymmetric encryption systems. Encryption is an important tool for preserving the privacy of data. In symmetric encryption, only one key is used for both encryption and decryption. Examples are Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest Ciphers (RC1 to RC6) etc. Whereas in asymmetric encryption systems, two keys, namely an encryption key and a decryption are used for encryption and decryption respectively. Examples include RSA (Rivest-Shamir-Adleman) cryptosystem [32], ElGamal cryptosystem

[33], Cramer-Shoup asymmetric encryption algorithm [34] etc. An asymmetric key cryptosystem is usually computationally costlier than the symmetric one. This is because the former involves computations over large primes in a finite field with a sufficiently large order. This makes it unsuitable for use in wireless sensor devices because of their low computing power and limited lifetime. The most important advantage of an asymmetric cryptosystem is that using these, cryptographic keys can be distributed without assuming fully secure communication channels or without having to deliver them physically. For secure delivery of symmetric encryption keys, the symmetric keys can be encrypted using asymmetric key cryptography algorithm under the recipient's public key and transmitted over an insecure channel. Assuming, only the intended recipient has the corresponding secret key, none other than the intended recipient can decrypt and obtain the underlying symmetric key. This technique is also called a digital envelope. Additionally, asymmetric key cryptography algorithms can also be used for digitally signing a document (the procedure is explained in Section 3.5.1.3). The purpose of digital signatures is not data privacy, but non-repudiation and integrity. Digital signatures are based on the principle of reverse encryption. That is, encrypting with the private key and decrypting with the public key. In an asymmetric key encryption setting, a sender encrypts the message using its secret key which can be decrypted by anyone using the corresponding public key which is already published on any centralized public storage. Assuming none other than the sender has its secret key, it can be ascertained that the message has indeed been sent by the sender and is not being repudiated.

To overcome the computational cost of asymmetric cryptosystems over large finite fields, asymmetric cryptosystems have been developed over elliptic curves. This requires comparatively very small numbers to be processed for encryption/decryption for security level equivalent to that achieved in classical asymmetric cryptosystems. Table 14.2 shows the key-sizes of traditional symmetric encryption, Elliptic curve cryptosystems and traditional asymmetric encryption algorithms like the RSA. The majority of the focus on elliptic curve cryptosystems research is about formalizing the security models and building security proofs of these lightweight cryptographic primitives. Though they lack formal proofs of security, there are no attacks known on elliptic curve cryptosystems. Therefore, elliptic curve cryptosystems are popular for asymmetric encryption in sensor networks. Some of the well-known elliptic-curve cryptosystems are Elliptic-curve Diffie-Hellman (ECDH) key agreement [35], Elliptic Curve Integrated Encryption Scheme (ECIES) [36], Elliptic Curve Digital Signature Algorithm (ECDSA) [37], etc.

TABLE 14.2
Key Sizes for Equivalent Security Levels (in bits) [38].

Symmetric	ECC	RSA
80	163	1024
128	283	3072
192	409	7680
256	571	15,360

Recently, hardware implementations of symmetric ciphers have gained widespread attention for securing data communication using sensor networks [39]. This is because a hardware encrypted device features a fast, portable, and tamper-proof encryption of data traffic through it. A symmetric encryption algorithm is hard-coded into a device's local fast access memory along with the encryption key. An important characteristic of hardware encryption is that it can use biometric features as encryption keys [40]. This makes it more suitable for encryption of data traffic in remote healthcare. Currently, a hardware implementation of AES is widely used as it is the most secure and practical symmetric encryption algorithm. While hardware encryption provides fast and reliable security in communication, this demands more local storage to be available on sensor devices.

3.5.1.2 Anonymous authentication. In security, authentication requires that an activity like read/write/update of data is performed by someone authorized for it. Also, the one performing the activity must be held accountable for the activity. For example, an email server grants access to someone's mail account only if the correct secret credentials are provided. Also, each user is held responsible for the e-mails sent and other activities like deleting the e-mails, saving the e-mails, etc. Anonymity requires that a user should not be uniquely identifiable. For example, the identity of a user visiting a webpage should not be disclosed to anyone, but every time any user visits the webpage, the hit count of the page should increment by one. While anonymity deals with not identifying a user, authentication grants someone access to services based on "who" the user is. The seemingly paradoxical term

Anonymous Authentication [41] is an important feature of remote healthcare for preserving the privacy of the identities of the patients who may store, modify or delete data on the storage server. Designing an anonymous authentication protocol requires building authorized sets of users and devising a method for the server to identify the user as nothing but someone who either belongs or does not belong to the authorized set. No information about the user is revealed that could potentially lead to the disclosure of a user's identity. Some of the important salient features of an anonymous authentication protocol are [42]:

- **Secure authentication:** It requires that no unauthorized user should be able to fool the server into granting it access to services. Anonymity requires that the server should not be able to know the identity of the user it is interacting with.
- **Verifiable anonymity:** It is concerned with providing methods using which the users interact with the server always detects the server's behavior that may potentially lead disclosure of user's identity. This requirement is very difficult to satisfy. Therefore, the relaxed version of it is that if in case there is a possibility of disclosure of the user's identity and the server does so, the user comes to know about it instantly. This is useful because the user, upon detection of the cheating behavior of the server, may disconnect from it without performing any operation. This leads to possible disclosure of the identity of the user who tried connecting to the server, but this information serves as limited motivation for cheating by the server and losing reputation.
- **Revocable anonymity:** It is important in cases where, for example, anonymous users are harassing others. For such behavior of the users, if some action has to be taken, the service provider must reserve the rights to revoke the anonymity of any of its users. Since there is no way of suspending the user's account and there is a risk of losing anonymity of the rest of the users, revocation is carried out using a secure protocol and under the order of the court of law.

3.5.1.3 Dynamic integrity assurance: signature, message digests.

The patient's data in a remote healthcare system should be checked dynamically for integrity. A verifying agency called verifier verifies the dynamic integrity of data. This verifier can be a public entity, the data collector or the data owner. The verifier, given some auxiliary public information and the copy of data being stored by the storage servers, tries to assure that the data stored is consistent and correct. This procedure is executed either periodically or when data is required for processing.

One of the effective ways of assuring the integrity of data is storing cryptographic hash [43] by the verifier. A cryptographic hash function is a one-way function that, given any fixed length input, generates a unique fixed length output. Concretely, a hash function H: $\{0, 1\}^n \rightarrow \{0, 1\}^m$ where n is the input size and m the output block size has the following properties [44]:

i. Deterministic: The same input always results in the same hash output.
ii. One-way: It is computationally infeasible to obtain the input, given the output.
iii. Collision-resistance: Two different inputs do not give the same hash output.

At any point of time, the verifier can verify the integrity of the stored data by computing the hash of the stored data value and compare it with the precomputed local hash value of the same data. If the data value is unchanged, the two hash values are the same. Otherwise, if even a single bit of data is modified, the two hashes differ on an average by at least half the total number of bits in the two hashes. The problem with this approach is that the storage overhead at the verifier is very large. Indeed, the verifier has to store as many hashes as the number of data items. Fig. 14.3A and B show the hashing and verification procedures, respectively.

To overcome this problem, instead of storing the hash locally, the verifier encrypts the hash under its secret key using an asymmetric key cryptography algorithm and stores it alongside the data item on the storage server. The two algorithms for hashing and encrypting the hash are collectively known as a signature algorithm. Note that the encryption is done using a secret key of the verifier, decryption can be done using its public key. This is the reverse of the conventional encryption process and is done so that no one except the verifier can sign the data. The hash encrypted under the secret key of the verifier is called a digital signature of the message [45]. For verification, the verifier applies a decryption algorithm on the digital signature to get a hash of the message. The verifier also computes the hash of the stored message. Now, the hash obtained by decrypting the signature is compared against the hash computed over the stored message. If the two hashes are equal, the message integrity is verified. Otherwise, the message is considered modified or inconsistent. The algorithms corresponding to decrypting the signature and computing the hash of the data are collectively

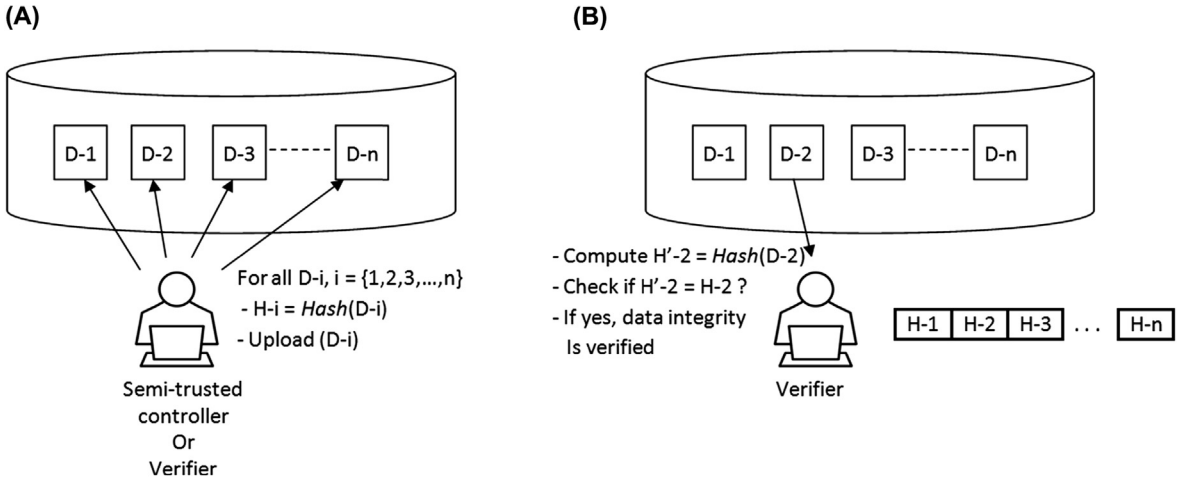

FIG. 14.3 Dynamic integrity verification using a cryptographic hash function. (A) Any semi-trusted entity can compute hash each data item before uploading. (B) Verifier who stores these hashes verifies the integrity of datum D-2.

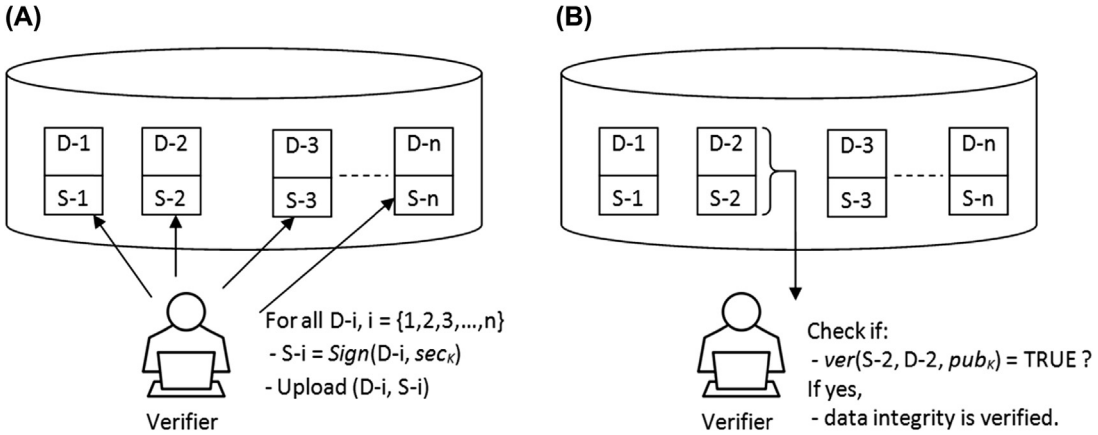

FIG. 14.4 Dynamic Integrity assurance using a digital signature. (A) Verifier signs all the data items using the signature algorithm sign and uploads the data (items, signature)-pair. (B) Verifier verifies the integrity of datum D-2 using the verification algorithm ver.

known as a signature verification algorithm. Since the digital signature is produced using a secret key of the verifier, no one else could have produced it. Therefore, no other value than a hash of the message could be obtained by decryption of the digital signature. Fig. 14.4A and B show how the signing and verification can be used for verifying the integrity of data stored on distributed storage. The advantage of this approach is that nothing has to be stored locally by the verifier. The decryption of the digital signature and computing the hash can be done on the go. However, a shortcoming of this approach is that the verifier cannot be a semi-trusted third party. The verifier must be the data owner or a data collection agency. Indeed, the encryption of the hash of the message requires secret keys, and it is not advisable to share a secret key with a semi-trusted third-party. The approach involving a digital signature is storage efficient, but it is computation and communication intensive.

3.5.2 Cryptographic access control

Access control is for the patients in remote healthcare to grant controlled access of their health data to various parties based on an access control policy. An access

control policy specifies access capabilities, according to a party's role. For example, a doctor can access all the health-related data but may not be allowed access to a patient's annual salary or annual premium of the insurance policy of the patient. Also, access to sensitive medical data should not be granted to anyone apart from the hospital staff. An efficient role-based access control mechanism is required for managing access to a patient's health data. Small granularity level and dynamic nature of access control policy make the system robust, efficient and flexible. Fine-grained access control means that access to different pieces of data should be granted to various actors based on the roles they have in the overall system operation. The policy specified by the data owner takes a predicate form which, if satisfied by the role or credentials of a potential user of data, the access is granted. Otherwise, access is denied to the user. Granularity plays an important part in making the access control system efficient and dynamic. A cryptographic primitive for fine-grained role-based access control has been proposed called attribute-based encryption [46–48]. Each data item is assigned a set of attributes which are selected from the set of attributes possessed by the users in the system. An attribute-based encryption grants access to a piece of data to a user only if the attributes possessed by the user are authorized subset of the attributes associated with the data. This set of attributes associated with the data item forms the access control policy of the data item.

As an example, consider a data item which has the attributes "XYZHospital and (CARDIOLOGY or DENTAL)" meaning that anyone from the XYZHospital's cardiology or dental department can access the data item. If anyone from the XYZHospital's orthopedic department tries to access the data, the access is not granted. This is because the set of attributes of the user trying to access the data does not form the authorized subset of the attributes associated with the data. It is possible to revoke or reinstate access rights of any user at any point in time. For example, the access policy of the patient data can be updated as "XYZHospital and (CARDIOLOGY or ORTHOPEDIC)". This means that now, the medical staff belonging to the DENTAL department of the XYZHospital cannot access the data anymore, but the one belonging to ORTHOPEDIC department of XYZHospital can access the data. This dynamic property of access control mechanisms is sometimes referred to as revocability. In the context of attribute-based encryption, it is called attribute revocation. Revoking an attribute from a data item's access control policy reflects in the access rights of multiple parties based on the attribute sets possessed by them.

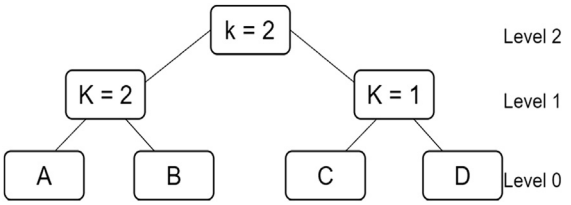

FIG. 14.5 A sample access structure in attribute based encryption.

A set of attributes are associated with a user's secret(s) cryptographically in a way that they cannot be repudiated by anyone else. An access control policy on attribute-based encryption contains several threshold gates connected to form a tree as shown in Fig. 14.5. A threshold gate with threshold K returns a value TRUE only if at least K of its child nodes evaluates to TRUE. For example, in Fig. 14.5, the threshold gates at Level 1 that has $K = 2$ indicates that it evaluates to TRUE only if both A and B attributes are possessed by a user in question. This gate can also be viewed as an AND gate. Similarly, the threshold gate with $K = 1$ can be viewed as OR gate. Gates with more general threshold values exist in attribute-based encryption to support expressive access control policies. Access structure of Fig. 14.5 is satisfied by a user having attribute set {A, B, C}. However, it cannot be satisfied by a user with attribute set {B, C, D} or {A, C, D} or {A, B} etc. While this type of access control policies seems to solve most of our problems, the access structures of attribute-based encryption systems are still far from supporting policies as expressive as an SQL statement [49]. The focus of current research if attribute-based encryption is in this direction.

There are two variants of attribute-based encryption, namely key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). The example discussed above is that of a CP-ABE where the policy is associated with the data/ciphertext, and each user has attributes associated with them. In KP-ABE, the policy is associated with the users' secret keys and ciphertext has associated with it the set of attributes. Arguably, CP-ABE is better suitable for scenarios where role-based access control is required.

3.5.3 Security standards

Various application-level solutions for remote healthcare security have been proposed. This section will look at the standardization of security measures in network communication part of the remote healthcare system which mainly consists of WBAN. Here, the

WBAN standard of IEEE 802.15.6 has been considered. For a detail discussion of the WBAN standards, readers are suggested to refer to the article of Pramanik et al. [12]. In this section, only the security aspect of IEEE 802.15.6 has been discussed. The standard defines three levels of WBAN communications:

- **Unsecured communication (level-0):** As the name suggests, in this communication mode, there is no protection against relay attacks, no authentication, and no integrity checks. In this level, data is transmitted in insecure frames.
- **Authentication only (level-1):** In this mode, the data is communicated in an authenticated way. Data privacy and confidentiality are not the concerns in this mode. The authentication only ensures nonrepudiation which means that if any changes are made to the data, these changes can be detected and the updating authority can be accounted for the changes such that the updating entity cannot deny that the changes were not done by her.
- **Authentication plus encryption (level-2):** This is the most secure level where both authentication and confidentiality are achieved for WBAN communication. Three keys come into play when a new sensor node joins the network of sensors namely masterkey (MK), pairwise temporal key (PTK) and group temporal key (GTK). An MK is either pre-shared between the sensors or is established between the sensors via authenticated association. Using this master key as input, a PTK is established to be used once per session. PTK is obtained by the sensors using a special public polynomial, called a pairwise key generation polynomial. This polynomial takes the secret key of one sensor and the public key of another to generate the session key between the two sensors. This session key can be used for encryption and decryption of data being exchanged between them. The main goal of sensor communication in WBAN is multicast. The overall collection of sensors is divided into activity driven multi-cast groups. For multicast, a GTK is computed based on PTKs of all the group members and the data intended for the whole group is encrypted and decrypted using the GTK.

3.5.4 Wireless, Bluetooth, Zigbee security protocols

The security protocols that are developed as part of wireless security are:

- WEP (wired equivalent privacy)
- WPA (Wi-Fi protected access)
- WPA-2 (Wi-Fi protected access version 2)

WEP was the first security protocol developed for security in wireless communication. WEP was ratified as part of the IEEE 802.11 in 1997. The security services provided by WEP include authentication and weak security. Authentication itself works in two modes:

- **Open system authentication:** In open system authentication, effectively there is no authentication. In fact, anyone can associate with the network. However, by some key distribution mechanism, the symmetric encryption keys are distributed to the intended participants. Messages are sent after encryption using encryption keys. The participant can decrypt only if she has the encryption key.
- **Shared key authentication:** In shared key authentication, the authentication service of WEP called four-step challenge-response handshake comes into play. Basically, the security service of the WEP protocol is provided by encryption using an RC4 stream cipher.

The problem with the RC4 stream cipher used in WEP is that the data encryption key must not be used twice. This means that the synchronization of devices to agree on the same key is required. Moreover, in 2001, the cryptanalysis of WEP was proposed by Scott Fluhrer et al. [50]. This attack broke the WEP protocol using a passive attack on the network. That is why the security service of the WEP protocol is also called Weak Security.

WPA and WPA-2 are developed to overcome the problems of weak security of WEP. Both use a pre-shared pairwise temporal key (PTK) and Group Temporal Key (GTK) for encrypting data for multicast. WPA and WPA-2 include message integrity checks as replacement of the Cyclic Redundancy Codes (CRC) that are designed to prevent an attacker from modifying and resending the data packets. WPA-2 has a major improvement over WPA in that it uses AES-based encryption mode with strong security. In January 2018, WPA-3 was announced as a replacement of WPA-2. WPA-3 uses a 192-bit key which is very strong, and it is expected to overcome security problems due to weak passwords and simplify the processing of joining the network by allowing very limited human intervention.

The highlights of the Bluetooth security protocol are the Link Manager Protocol (LMP) and Logical Link Control and Adaptation (L2CAP). LMP covers services like encryption, authentication, and exchanging the encryption keys. L2CAP supports a higher level of multiplexing and packet reassembly which can help in providing quality of service communication.

The Zigbee standard has a network layer that defines supplementary security services that include a process of authentication and key exchange. All this in addition to the IEEE 802.15.4. The Zigbee protocol also proposes to use the services of a trust center or coordinator, which allows sensor nodes to join the network and distributes encryption keys for encrypting network traffic.

3.6 Challenges and Trade-Offs

3.6.1 Interoperability

Remote healthcare systems are made realizable due to advances in low power communication standards, plug-and-play type device buses, handheld computer systems and internet technology. To increase acceptance of remote and pervasive healthcare, security with device interoperability is an important requirement [51,52]. Sensors attached to the patient's body may be bought by the patient from various vendors. Therefore. It is difficult to share the cryptographic material (e.g., encryption keys) between the sensors from different vendor sources.

As can be understood from the overall network architecture, a remote and pervasive healthcare system consists of several different types of devices with different capabilities. It starts with a sensor node which is least privileged in terms of resources like computing power and battery lifetime. A gateway device with the patient has little more computation and communication power than the sensors. Data transmitted over the internet is collected by the medical service provider which may be operating over a high computing machine to handle multiple concurrent requests. Based on their different computing powers, the devices in remote healthcare systems execute different protocols for achieving security of various aspects of data collection and processing. Devising security standards that address overall security while addressing this interoperability between devices of different computation and storage capabilities is a big concern in remote healthcare.

3.6.2 Security versus efficiency

Efficiency is a measure of the cost of any system. Security protocols for remote healthcare come with a cost associated with them. It is desirable that the security systems for remote healthcare are efficient in terms of storage requirement, communication bandwidth consumption, and computations for achieving the desired level of security. The cost of the security system is usually determined by the cost of assets it protects. If the cost of assets is greater than the cost of security measures, the security system is acceptable. Otherwise, the security system is considered inefficient. It is advisable that the security measures be deployed only after thorough feasibility and cost analysis.

3.6.3 Security versus usability

The operators of the devices in remote healthcare are either the patients or the medical staff that most probably do not possess any technical expertize. Therefore, it is required that the devices are easy to use and foolproof. Also, the devices should be plug-and-play like and with minimum human intervention required. While omitting human steps from operation is good for usability, it may potentially cause security issues in the remote healthcare system. This is because the minimum involvement also means a low level of understanding and knowledge about the system. There are high chances of a completely ignorant operator of a remote healthcare system falling in the trap of an attacker launching a social engineering attack to learn sensitive information and/or permanent and long-term credentials of the operator.

3.6.4 Security versus availability

Sometimes, security measures adopted to secure any system are too strict that the data cannot be made available in time for processing and generation of advice. Designing a balanced security protocol that does not restrict data flow and still provides the desired level of security is a challenge. This issue is sometimes referred to as "security versus safety".

3.7 Future of Remote Healthcare Security

Data security and privacy policies are dynamic and depend on many factors, including location, time and type of data and its usage. Some countries take the privacy of personal and sensitive data of their citizens very seriously. Whereas, privacy policies in some countries do not demand very stringent privacy protection mechanisms to be in place. Recently, as part of the 2016 General Data Protection Regulation (GDPR) passed by the European Union, new rules have been set up on how companies manage and share personal data. The regulation came into effect on May 25, 2018. In addition to the earlier privacy policy enforced by European Union countries, GDPR requires two more things. Firstly, it requires complete explicit informed consent from the users for accessing and using the personal data of a user. Secondly, there must be a transparent method of revoking that consent. A user can ask for all his data from the organization to verify the consent. Maximum fines per violation are set at 4% of a company's global turnover (or $20 million, whichever is

larger). GDPR has affected organizations not only in the EU but also outside the EU because of the global nature of the internet. This shift in privacy policy empowering the users is an indicator of the fact that the organizations are moving from large-scale unified security and privacy rules to more user-centric security services.

The future of remote healthcare security also lies in designing security mechanisms that suit an individual patient. Medical data, once collected, cannot be absolutely deleted from the memory of the data collection agency. However, revoking the consent of sharing the data by a patient would mean that in case of any breach of privacy, a patient can move to the court and get justice. While the users rightly keep getting privacy-aware, existing security mechanisms/frameworks may not be sufficient for proving the required level of flexibility and customization. The future of security of remote healthcare for remote and pervasive healthcare lies in innovative designs to cater to the application-specific and user-specific needs of remote healthcare systems.

4 CONCLUSION

ICT innovations play a key role to promote new medical assistance methodologies, especially in a remote way. Remote healthcare signifies a system that offers healthcare services remotely, which can be provided through telemedicine and remote health monitoring. In remote healthcare, patients and doctors do not get into face-to-face contact because of their geographical distance. Patient's health data are sent to the doctor for remote diagnosis and treatment. Being an internet connected system, any remote health monitoring system is vulnerable to a variety of passive and active security attacks. Breach of privacy, availability, and integrity of patient information can result in disastrous scenarios. The unlawful uses of health data used by an unauthorized person may be fatal. Hence, it is crucial to protect the privacy and integrity of data in remote healthcare. In this chapter, we have presented a wide variety of network and system attacks. Also, potential threats to the security of healthcare systems due to trust issues with various collaborators are also presented. To confront these security threats, standard secured communication protocols, application-level system security solutions and support of regulatory authorities for their enforcement is a must. This chapter has comprehensively described all these security solutions and provided a glimpse of where the security of remote healthcare is heading. Challenges in designing security protocols and application level solutions have also been highlighted. The future of security in remote healthcare systems, which demands more patient-centric and customizable security solutions, is faced with numerous challenges. The biggest of these challenges is the deletion of data and access revocability. Deletion of already shared data is practically very difficult, and so is the access revocability. Revocability mechanisms while maintaining flexibility of the overall healthcare system are the points of the current focus in the design of cryptographic solutions for remote healthcare. Further works are required to maintain the security and confidentiality of data by introducing advanced encryption-based techniques. Indeed, if remote healthcare is to flourish, along with other technical enhancement, security and privacy issues are needed to be handled with foolproof solutions.

ACKNOWLEDGMENTS

We would like to thank Mr. Shubham Botre, Linux System Administrator, CDAC, Pune, India for his contribution in drawing Figs. 14.1 and 14.2.

REFERENCES

[1] F. Online, Doctor-Population Ratio: In India, One Allopathic Doctor for 11,082 People, Official Data Shows; Bihar, UP Worst Hit, June 20, 2018 [Online]. Available: https://www.financialexpress.com/india-news/doctor-population-ratio-in-india-one-allopathic-doctor-for-11082-people-official-data-shows-bihar-up-worst-hit/1213243/.

[2] S.D. D'Cunha, India's Most Remote Villages Are Getting Better Healthcare with This Cloud-Based Solution, November 21, 2016 [Online]. Available: https://www.forbes.com/sites/suparnadutt/2016/11/21/indias-most-remote-villages-are-getting-better-healthcare-with-this-cloud-based-solution/#201d2d10593b.

[3] S. Singh, S. Badaya, Health care in rural India: a lack between need and feed, South Asian J. Cancer 3 (2) (2014) 143–144.

[4] R. Kumar, Academic institutionalization of community health services: way ahead in medical education reforms, J. Fam. Med. Prim. Care 1 (1) (2012) 10–19.

[5] L. Catarinucci, R. Colella, L. Tarricone, Integration of RFID and sensors for remote healthcare, in: 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010), Rome, Italy, 2010.

[6] P.K.D. Pramanik, P. Choudhury, IoT data processing: the different archetypes and their security & privacy assessments, in: S.K. Shandilya, S.A. Chun, S. Shandilya, E. Weippl (Eds.), Internet of Things (IoT) Security: Fundamentals, Techniques and Applications, River Publishers, 2018, pp. 37–54.

[7] P.K.D. Pramanik, B.K. Upadhyaya, S. Pal, T. Pal, Internet of things, smart sensors, and pervasive systems: enabling the connected and pervasive health care, in: N. Dey, A. Ashour, S.J. Fong, C. Bhatt (Eds.), Healthcare Data Analytics and Management, Elsevier, 2018, pp. 1–58.
[8] P.K.D. Pramanik, S. Pal, M. Mukhopadhyay, Healthcare big data: a comprehensive overview, in: N. Bouchemal (Ed.), Intelligent Systems for Healthcare Management and Delivery, IGI Global, 2018, pp. 72–100.
[9] I.A. Zriqat, A.M. Altamimi, Security and privacy issues in ehealthcare systems: towards trusted services, Int. J. Adv. Comput. Sci. Appl. 7 (9) (2016) 229–236.
[10] S. Sabnis, D. Charles, Opportunities and challenges: security in ehealth, Bell Labs Tech. J. 17 (3) (2012) 105–111.
[11] S.N. Khalifehsoltani, M.R. Gerami, E-health challenges, opportunities and experiences of developing countries, in: International Conference on e-Education, e-Business, e-Management and e-Learning, Sanya, China, 2010.
[12] P.K.D. Pramanik, A. Nayyar, G. Pareek, WBAN: driving E-healthcare beyond telemedicine to remote health monitoring - architecture and protocols, in: D.J. Hemanth, V.E. Balas (Eds.), Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare, Elsevier, 2019.
[13] J. Tan, Drivers of and barriers to E-health care, in: E-health Care Information Systems: An Introduction for Students and Professionals, Jossey-Bass, 2005, pp. 37–51.
[14] P.K.D. Pramanik, S. Pal, A. Brahmachari, P. Choudhury, Processing IoT data: from cloud to fog. It's time to be down-to-earth, in: Applications of Security, Mobile, Analytic and Cloud (SMAC) Technologies for Effective Information Processing and Management, IGI Global, 2018, pp. 124–148.
[15] P.K.D. Pramanik, S. Pal, P. Choudhury, Beyond automation: the cognitive IoT. Artificial intelligence brings sense to the internet of things, in: Cognitive Computing for Big Data Systems over IoT: Frameworks, Tools and Application, Springer, 2018, pp. 1–37.
[16] P.K.D. Pramanik, P. Choudhury, A. Saha, Economical supercomputing thru smartphone crowd computing: an assessment of opportunities, benefits, deterrents, and applications from India's perspective, in: 4th International Conference on Advanced Computing and Communication Systems (ICACCS – 2017), Coimbatore, India, January 2017.
[17] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Comput. Network. 38 (4) (2002) 393–422.
[18] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, V.C. Leung, Body area networks: a survey, Mobile Network. Appl. 16 (2) (2011) 171–193.
[19] M. Abo-Zahhad, S.M. Ahmed, O. Elnahas, A wireless emergency telemedicine system for patients monitoring and diagnosis, Int. J. Telemed. Appl. 2014 (2014).
[20] IEEE Standards, Part 15.4:Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANS): Amendment to Add Alternate Phy (Amendment of IEEE Std 802.15.4), IEEE, 2014.
[21] K.S. Kwak, S. Ullah, N. Ullah, An overview of IEEE 802.15.6 standard, in: 3rd International Symposium on in Applied Sciences in Biomedical and Communication Technologies, ISABEL), 2010.
[22] M. Li, W. Lou, K. Ren, Data security and privacy in wireless body area networks, IEEE Wirel. Commun. 17 (1) (2010) 51–58.
[23] J. Camenisch, I. Damgård, Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes, in: International Conference on the Theory and Application of Cryptology and Information Security, 2000.
[24] N. Zhao, F.R. Yu, Y. Chen, B. Chen, V.C. Leung, Internal collusive eavesdropping of interference alignment networks, in: 85th IEEE International Conference on Vehicular Technology Conference, 2017.
[25] M. Anand, Z. Ives, A.I. Lee, Quantifying eavesdropping vulnerability in sensor networks, in: 2nd International Workshop on Data Management for Sensor Networks, 2005.
[26] N. Zhao, F.R. Yu, M. Li, Q. Yan, V.C. Leung, Physical layer security issues in interference-alignment-based wireless networks, IEEE Commun. Mag. 54 (8) (2016) 162–168.
[27] G.S.S. Geraci, J.G. Andrews, J. Yuan, I.B. Collings, Secrecy rates in broadcast channels with confidential messages and external eavesdroppers, IEEE Trans. Wirel. Commun. 13 (5) (2014) 2931–2943.
[28] F. Callegati, W. Cerroni, M. Ramilli, Man-in-the-middle attack to the HTTPS protocol, IEEE Secur. Priv. 7 (1) (2009) 78–81.
[29] R.L. Rivest, L. Adleman, M.L. Dertouzos, On data banks and privacy homomorphisms, Found. Secure Comput. 4 (11) (1978) 169–180.
[30] M. Blount, V.M. Batra, A.N. Capella, M.R. Ebling, W.F. Jerome, S.M. Martin, M. Nidd, M.R. Niemi, S.P. Wright, Remote health-care monitoring using personal care connect, IBM Syst. J. 46 (1) (2007) 95–113.
[31] A. Cavoukian, A. Fisher, S. Killen, D.A. Hoffman, Remote home health care technologies: how to ensure privacy? Build it in: privacy by design, Ident. Inf. Soc. 3 (2) (2010) 363–378.
[32] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.
[33] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inf. Theory 31 (4) (1985) 469–472.
[34] R. Cramer, V. Shoup, A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, in: Annual International Cryptology Conference, 1998.
[35] N. Koblitz, Elliptic curve cryptosystems, Math. Comput. 48 (177) (1987) 203–209.
[36] V.S. Miller, Use of elliptic curves in cryptography, in: Conference on the Theory and Application of Cryptographic Techniques, 1985.

[37] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA), Int. J. Inf. Secur. 1 (1) (2001) 36–63.
[38] K. Lauter, The advantages of elliptic curve cryptography for wireless security, IEEE Wirel. Commun. 11 (1) (2004) 62–67.
[39] M. Healy, T. Newe, E. Lewis, Analysis of hardware encryption versus software encryption on wireless sensor network motes, in: Smart Sensors and Sensing Technology, 2008.
[40] S. Harper, P. Athanas, A security policy based upon hardware encryption, in: 37th Annual Hawaii International Conference on System Sciences, 2004.
[41] D. He, S. Zeadally, N. Kumar, J.-H. Lee, Anonymous authentication for wireless body area networks with provable security, IEEE Syst. J. 11 (4) (2017) 2590–2601.
[42] Y. Lindell, Anonymous authentication, J. Priv. Confidentiality 2 (2) (2011).
[43] P. Rogaway, T. Shrimpton, Cryptographic hash-function basics: definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance, in: International Workshop on Fast Software Encryption, 2004.
[44] M. Bellare, R. Canetti, H. Krawczyk, Keying hash functions for message authentication, in: Annual International Cryptology Conference, 1996.
[45] S. Goldwasser, S. Micali, R.L. Rivest, A digital signature scheme secure against adaptive chosen-message attacks, SIAM J. Comput. 17 (2) (1988) 281–308.
[46] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: 13th ACM Conference on Computer and Communications Security, 2006.
[47] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: IEEE Symposium on Security and Privacy (SP '07), 2007.
[48] N. Attrapadung, B. Libert, E.D. Panafieu, Expressive key-policy attribute-based encryption with constant-size ciphertexts, in: International Workshop on Public Key Cryptography, 2011.
[49] R. Bobba, H. Khurana, M. Prabhakaran, Attribute-sets: a practically motivated enhancement to attribute-based encryption, in: European Symposium on Research in Computer Security, 2009.
[50] S. Fluhrer, I. Mantin, A. Shamir, Weaknesses in the key scheduling algorithm of RC4, in: International Workshop on Selected Areas in Cryptography, 2001.
[51] A.-J. Samaher, I. Al-Shourbaji, M. Shojafar, S. Shamshirband, Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications, Egypt. Inf. J. 18 (2) (2017) 113–122.
[52] W. Steve, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, E. Jovanov, Interoperability and security in wireless body area network infrastructures, in: 27th Annual International Conference of the Engineering in Medicine and Biology Society, 2005.