1

Overview of e-Health Architectures

Omessaad HAMDI
IEEE, Rennes, France

1.1. Introduction

Digitization occupies a central place in all our daily activities, and the healthcare field is particularly affected by this digital evolution, which has considerably improved patient care (Hermes et al. 2020; Gupta et al. 2021). This improvement is based on two key factors: the increased involvement of patients in the management of their health, and easy access for healthcare professionals to digital tools and services.

Digitization is also improving people's quality of life, in terms of well-being and autonomy, and is helping respond to the growing number of elderly people worldwide. The phenomenon of aging is becoming a growing concern. To enable this population to age in a secure environment with a good quality of life, while reducing costs, several approaches have been developed.

In this chapter, we focus on e-health architectures. We begin by introducing the terms used in e-health. Next, we present the services offered by e-health systems and their requirements. The final sections will focus on security and the techniques used to guarantee the required security services. Finally, we look ahead to the future of e-health.

e-Health Security Management,
coordinated by Omessaad HAMDI. © ISTE Ltd 2024.

1.2. Definitions

1.2.1. *e-Health*

The term *e-health* refers to information and communication technologies (ICT) combined with the Internet in the service of health.

1.2.2. *Telehealth*

Telehealth is part of e-health. It refers to the use of tools for producing, transmitting, and managing digitized medical information. Telehealth encompasses telemedicine and mobile health (m-health).

1.2.3. *m-Health*

m-Health is part of telehealth. It refers to healthcare practices supported by mobile devices, such as cell phones, patient monitoring systems and other wireless devices. The term includes, among others, applications such as wellness apps. Bashshur et al. (2011) point out that m-health is the only ICT-based healthcare field that can be justified solely based on mobility.

1.2.4. *Telemedicine*

Telemedicine is part of telehealth. It refers to the digital transmission of medical information (images, recordings, etc.) for remote diagnosis, specialist advice and continuous monitoring of a patient.

There are four forms of telemedicine (2010 decree):

– Remote consultation is between a healthcare professional and a patient: It refers to the use of communication technologies to provide health consultations to patients in geographically different locations.

– Remote education is between healthcare professionals, in the absence of the patient: It consists of a remote request for advice from colleagues based on information provided by the patient.

– Remote monitoring involves remote monitoring of a patient's health parameters, providing assessments of the patient's state of health.

– Remote assistance occurs when a doctor remotely guides a medical act. This can take place between two healthcare professionals or between a healthcare professional and a third-party present with the patient, for example, in an emergency.

Figure 1.1 summarizes the components of telehealth.

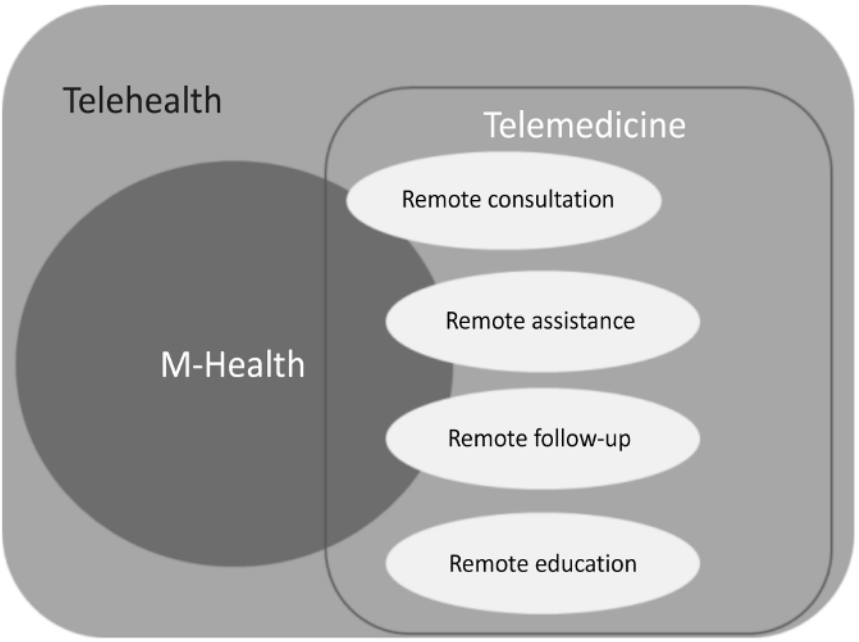

Figure 1.1. *Components of e-health*

1.3. e-Health services

e-Health offers a wide range of services designed to improve the quality of care and accessibility to medical services thanks to digital technologies:

– Cost reduction: e-health considerably reduces hospitalization and the need to keep elderly people in nursing homes. It also enables early detection of illness. Both services can significantly reduce healthcare costs (Atienza et al. 2007; Kostkova 2015).

– Social inclusion: the use of e-health technologies enables patients to remain active and independent as long as possible, enabling them to overcome their illness and/or disability without being excluded from society.

– Prevention: body and environmental data collected from sensors can be interpreted. By effectively managing these data, doctors can uncover facts and detect illness at an early stage.

– Support: e-health systems are designed to help people who are ill, elderly or disabled, and to promote their autonomy, safety and well-being. They make it possible to maintain and monitor patients at home, instead of hospitalizing them.

– Supervision: the acquisition and processing of patient data and the use of several devices enable the patient's condition to be monitored. This system is particularly interesting when it comes to high-risk patients, such as the elderly suffering from a wide range of chronic illnesses, for whom effective supervision is essential.

1.4. Requirements for e-health systems

e-Health systems must meet certain requirements if they are to be adapted by users.

In this section, we present some of these requirements:

– Acceptability: patients often wear sensors, and these are deployed in their environment to provide continuous monitoring. The sensors deployed must meet conditions of comfort and acceptability.

– Reliability: an e-health system must generate a very low false alarm rate.

– Energy autonomy: the energy autonomy of sensors plays an important role. Replacing sensor batteries is often complicated and/or costly.

– Ergonomics: it is essential that the devices and applications used are ergonomic and user-friendly to guarantee ease of use.

– Safety: devices and applications must comply with standards and regulatory requirements.

– Privacy protection: this is of paramount importance when dealing with media information, as this is sensitive data. To guarantee this protection,

appropriate mechanisms must be put in place, especially in an environment where several users are involved.

Figure 1.2 summarizes the services and requirements of e-health systems.

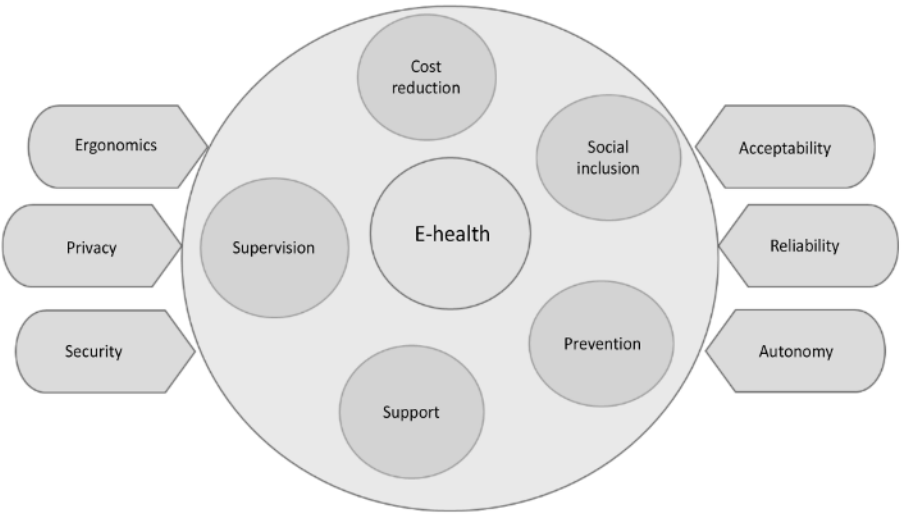

Figure 1.2. *Services and requirements for e-health systems*

1.5. e-Health system architecture

Different e-health system architectures have been developed to meet the specific needs of each project.

An architecture that summarizes most of the architectures proposed in the literature is shown in Figure 1.3.

In all e-health architectures, information flows from the patient to a medical server. Data are transferred from the sensors to a gateway that manages the sensors. Data transfer in the network can be continuous or ad hoc. Collected data are stored in a gateway, and then uploaded to a medical server.

1.5.1. *Components of an e-health architecture*

The main components of an e-health system are as follows (Hamdi et al. 2014):

– Sensors: these are devices that capture, store, process and transmit data.

– Wireless body area network (WBAN): it provides short-range wired or radio communication capability for sensors to exchange data with a gateway around an individual's body.

– Gateway: it collects vital and environmental data from sensors. It analyzes the data received from body and/or environmental measurements, compiles them and uploads them to a medical server via the network.

– Local area network (LAN): it provides wired or wireless communications for sensors to exchange data with a gateway.

– Wide area network (WAN): it provides wired or wireless (e.g. cellular) communications capability for gateways to download data to a medical server.

– e-Health systems platform: it includes servers for storing, processing and securing medical data.

Figure 1.3 gives an overview of the main components of e-health systems.

1.5.2. *Features of e-health systems*

– Data capture: this layer refers to the collection of patient data from vital signs and/or environmental sensors.

– Computation: this layer includes data analysis, management and personalization of care.

– Communication and storage: this layer covers vital signs communication, calculation and storage modules.

– Access: this layer refers to the way in which data are accessed. It often takes the form of a web portal or mobile application connected to a secure system hosted in the cloud, enabling continuous monitoring of patients' health status.

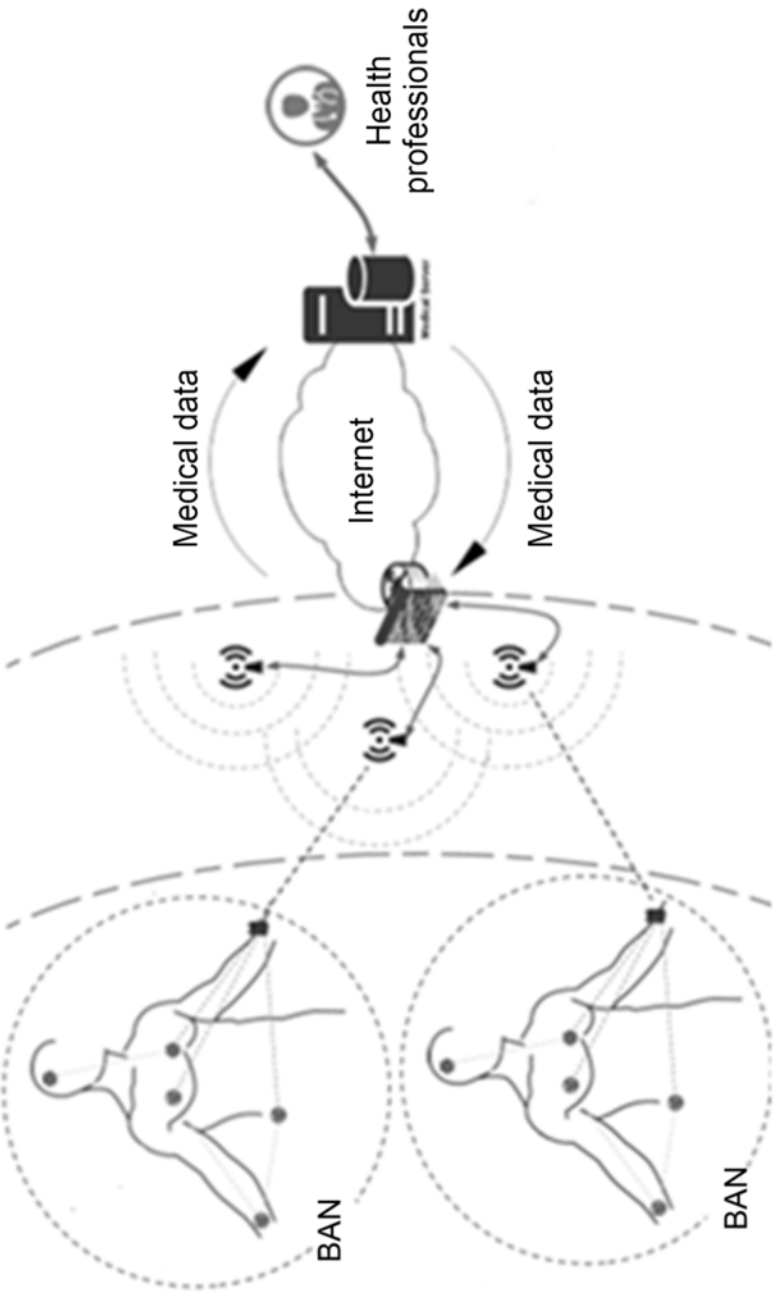

Figure 1.3. *Architecture of e-health systems (Hajar et al. 2021)*

1.6. e-Health system technologies

Connection technologies such as Bluetooth, WiFi, Internet and ZigBee play a key role in the growth of e-health applications and systems. When used in conjunction with other technologies, such as the Internet of Things (IoT), robotics, artificial intelligence (AI), cloud and Big Data, high-performance e-health systems can be created (Devedžić et al. 2021).

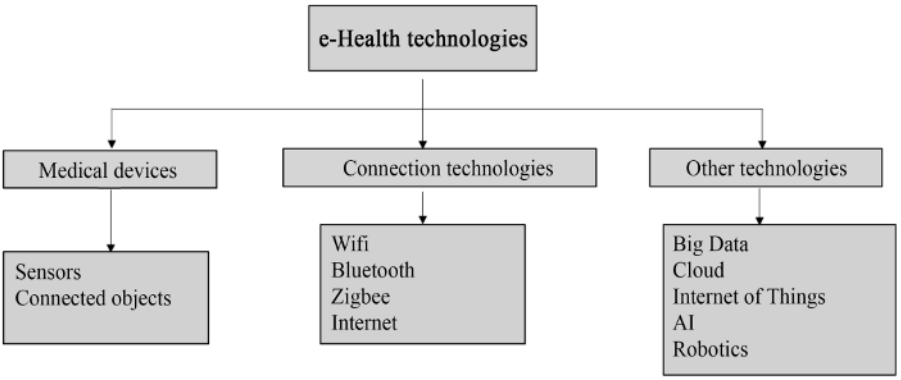

Figure 1.4. *e-Health technologies*

Figure 1.4 illustrates the main technologies used in e-health systems. These are grouped into medical devices, connection technologies and other technologies, and are detailed below.

1.6.1. *Devices*

Devices are mainly made up of sensors and connected objects, which play a key role in monitoring and ensuring the well-being of individuals, offering medical, safety and wellness services (Javaid et al. 2022).

– Sensors are devices that detect and measure specific information, such as body temperature, heart rate, blood pressure, physical activity, sleep quality and so on. These sensors collect valuable data on people's health and well-being.

– Connected objects, also known as IoT devices, are devices that can connect to the Internet and exchange data. These can include smartwatches, connected bracelets, connected scales, blood pressure monitors,

thermometers and many more. These connected objects work in tandem with sensors to collect, transmit and analyze data relating to users' health and well-being (Fagroud et al. 2019; Balakrishnan et al. 2021).

Using these sensors and connected objects, medical services can provide precise monitoring of an individual's health status, detecting signs of potential health problems and enabling early intervention. Security services can use these devices to ensure the safety of the elderly or people at risk by detecting falls or monitoring unusual movements.

Several approaches have focused on the uses of sensors or connected objects in the medical field. Table 1.1 illustrates a few examples.

References	Sensor	Proposition
(Rabbani et al. 2021)	Implant	A real-time immune response monitoring system used in cancer therapy to track disease progression and provide personalized care.
(Gourob et al. 2021)	Artificial hand	Human–robot interactions to control a patient's hand gesture recognition system.
(Basaklar et al. 2021)	Smart clothing	A portable, low-energy device for personalized care without manual intervention.
(Gupta et al. 2021)	WBAN	A system for monitoring psychological parameters such as temperature and heart rate to provide real-time diagnosis.
(Hodgkiss and Djahel 2022)	WBAN	The use of biometric data to ensure strong authentication as part of an e-health system.
(Behera 2022)	Patches	Using chip-less RFID sensors to measure data and monitor vital signs in real time.

Table 1.1. *Application of sensors and connected objects in e-health systems*

1.6.2. *Connecting technologies*

In this section, we present the connection technologies used in the various components of an e-health architecture.

1.6.2.1. *ZigBee*

ZigBee is a wireless technology offering long battery life, low data rate and a secure network (Chung et al. 2013; Minakshi 2016). In addition,

ZigBee is an easy network to install and configure, supports various network topologies and allows for a large number of nodes to be connected. ZigBee meets the specific requirements of WBANs.

1.6.2.2. *Bluetooth*

Bluetooth was designed for short-range wireless communications, where several Bluetooth devices form a short-range network (Negra et al. 2016). Bluetooth is widely used in WBANs.

1.6.2.3. *LPWAN*

LPWAN technology, proprietary to the LoRa (Long Range) Alliance, consists of two main elements, LoRa and the LoRaWAN protocol. This technology has been the focus of much research into e-health systems, due to its low cost, long coverage area and long sensor lifetime (Sundaram et al. 2019).

1.6.3. *Other technologies*

In recent years, e-health has become more efficient and smarter thanks to cloud technologies, Big Data, AI and robotics.

1.6.3.1. *Big Data*

The application of Big Data in the e-health sector has enabled the better exploitation of data to diagnose disease and improve quality of care.

Online e-health services and technologies generate huge volumes of data. The analysis of these data enables the transformation of conventional hypothesis-based information analysis into innovative data-driven analysis, capable of identifying links between heterogeneous information (Wang et al. 2016; Saranya et al. 2019).

1.6.3.2. *Artificial intelligence*

AI is attracting a great deal of interest due to its ability to process large quantities of data, produce accurate results and control processes to generate optimized outcomes. It is being used to aid decision-making and predict the effects of diseases, as well as longer term consequences (Kaur 2022). AI can perform processes such as logical reasoning, knowledge-based learning, drug discovery, guided surgery and advanced imagery (Sobhan et al. 2021).

1.6.3.3. *Robotics*

To ensure continuous, personalized care for patients in hospitals, or nursing homes, or homecare, solutions involving the use of robots are being proposed. These intelligent machines will help patients perform simple daily gestures, facilitate remote monitoring and communication with medical staff or relatives, administer simple therapies or be used for entertainment purposes (reading, storytelling, playing, etc.).

In addition to this type of robot, devices and control strategies for rehabilitation are being designed, such as the development of agents that can interact with the patient and provide real-time data to medical staff (Mashayekhi et al. 2020).

1.6.3.4. *Cloud*

It is known as a paradigm in which IT resources are made accessible to users. It offers many advantages, such as flexibility, cost and energy savings, resource sharing and rapid deployment. The rapid growth of e-health systems to deliver quality medical services has led to the use of cloud-based solutions. This choice makes it possible to take advantage of cloud resources to store and process large volumes of medical data.

1.6.3.5. *Internet of Things*

The IoT refers to a network of physical objects connected to the Internet and capable of communicating and exchanging data with each other and with other systems. These objects, also known as IoT devices, are equipped with sensors, software and communication technologies that enable them to collect, analyze and transmit information.

Currently, the approach used in most smart applications is to store all sensor data in the cloud and perform machine-learning processing on these data. The two worlds of IoT and cloud have seen rapid progress in the medical field. IoT can take advantage of the cloud's almost limitless resources to compensate for its insufficient capabilities. The main drivers of IoT integration in the cloud are as follows (Farahani et al. 2018; Yang et al. 2022):

– Communication: IoT is heterogeneous by nature and relies on a variety of communication protocols. The cloud offers an efficient solution for registering, discovering and managing any type of object, regardless of communication protocol.

– Resource pooling: physical IoT resources can be integrated into cloud resources, enabling us to allocate and share them on demand.

– Storage: IoT generates an enormous amount of data, characterized by its volume, variety and speed of data generation. In this context, IoT benefits from large-scale, long-term storage.

– Computing: data processing is generally a resource-intensive task. As a result, IoT can benefit from the cloud's unlimited processing resources to aggregate data and perform real-time analysis on the data collected.

1.7. Security in e-health systems

In this section, we present the required security services and legal requirements for e-health systems.

1.7.1. *Security services*

The main security services required for data in an e-health system are as follows:

– Confidentiality: medical data must be protected from disclosure to unauthorized parties during transmission, processing and/or storage (Siva Bharathi et al. 2019).

– Availability: having access to data and being able to dispose of it at any time is paramount in an e-health context. Given the critical applications of e-health, any disruption to the system can be life-threatening. Therefore, the ability to access the required data under any circumstances is essential.

– Integrity: integrity ensures that health data captured by a system or supplied to any entity is accurate and consistent with the information intended, without having been altered. Inappropriate treatment based on incorrect data can have serious consequences for patient health.

– Data authentication: unlike data integrity, which aims to prevent data being altered during transmission, data authentication aims to ensure that the message received comes from the originating node.

– Access control: it is a mechanism that limits access to legitimate entities. Access control policy is generally based on the privilege and right

of each authorized entity. Several solutions have been proposed to address access control issues, among which role-based access control (RBAC) and attribute-based access control (ABAC) are the most popular models for e-health (Sandhu 1996).

– Data freshness: an attacker may intend to capture transmitted messages and replay them later, leading to confusion and instability in the network. It is therefore essential to have a mechanism in place to verify that the message received is fresh.

– Non-repudiation: repudiation threats concern users who deny having had access to medical data after consulting it.

1.7.2. *Legal environment for e-health systems*

Devices and applications that manage medical data must comply with regulations. In Europe, a regulation on the protection of personal data processing was adopted in 2018 (Koren et al. 2022). This directive is called the general data protection regulation (GDPR). It aims to harmonize data protection standards at European level and defines the rights and responsibilities of entities in charge of data processing. In the medical field, this directive specifies that personal health data are considered regardless of the source, for example, from a medical device (Koren et al. 2022). This directive imposes the concept of security by design, which means that security requirements must be considered right at the start of the solution design process.

In the United States, personal health data are governed by the Health Insurance Portability and Accountability Act (HIPAA) (Koren et al. 2022). HIPAA establishes security rules for all healthcare providers who process health information in electronic format. The law protects all individually identifiable health-related information held or transmitted by healthcare providers and which is held or transmitted by an entity. Indeed, under the rules defined by HIPAA, an entity (healthcare provider, health service provider, etc.) is responsible for the security of patient data, which means that an application or service that collects, processes and stores patient data must ensure data confidentiality and integrity and impose access restrictions.

1.8. Medical data security

In this section, we present the security techniques most widely used in the medical field. These include cryptography, biometrics and blockchain. A comparative analysis is carried out to identify the contribution of the techniques examined.

Figure 1.5 illustrates the security services required in e-health systems, as well as the different security techniques most commonly used to mitigate attacks in medical environments.

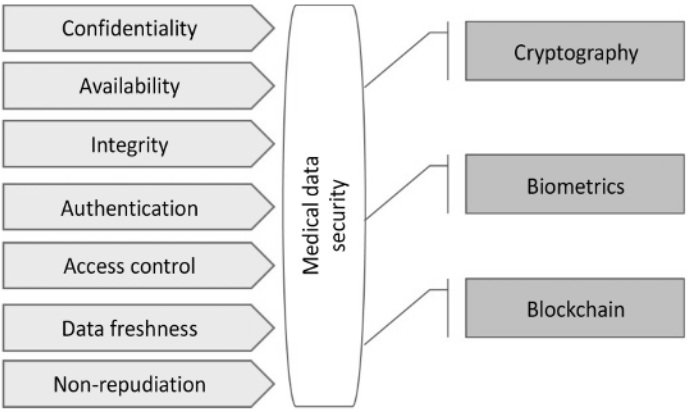

Figure 1.5. *Security in e-health systems*

1.8.1. *Cryptography*

Cryptography techniques offer important security services, such as confidentiality, integrity, non-repudiation and authentication of digital data (Anand et al. 2020; Singh et al. 2020).

Encryption is a technique used to encode information in order to guarantee the security of medical data (Thakur et al. 2018; Anand et al. 2020).

Some encryption techniques, such as public key cryptosystems or symmetric cryptosystems, have been developed to ensure confidentiality. In public-key cryptosystems, a public–private key pair is used to encrypt and

decrypt the message. In the symmetric method, a single key is used to encrypt and decrypt the data (Qadir et al. 2019; Gupta et al. 2020).

Vinoth et al. (2017) proposed a cryptographic approach to sharing and storing medical records in the cloud. The patient reserves the right to grant each party access to his or her record by sharing a key. Sujatha et al. (2013) proposed an approach for fast and secure transmission of electrocardiogram (ECG) data in a WBAN. They adapted an encryption technique (set partitioning in hierarchical trees [SPIHT]).

Sun et al. (2011) proposed an approach that ensures medical data security, including confidentiality, access control, integrity, accountability. This system ensures high security by encrypting medical records using searchable symmetric encryption (SSE) and public key encryption with keyword search (PEKS) algorithms and cryptographic algorithms using identity-based cryptography (IBC). This system is highly effective in emergency situations.

References	Type of Data	Algorithm	Proposition
(Sujatha et al. 2013)	ECG	SPIHT	Secure ECG transmission using encryption, compression and genetic algorithms.
(Vinoth et al. 2017)	Medical records	Blowfish	Storing and sharing medical records in unsecured environments.
(Sun et al. 2011)	Medical records	SSE, PEKS, IBC	Protecting patient privacy in emergency situations.
(Nagamani et al. 2018)	Medical data	MD5, password	Authentication and security of medical data in the cloud.
(Sammoud et al. 2020)	Session key	ECG	Session key exchange in a WBAN.
(Sharma et al. 2021)	Health data	Quantum	Securing IoT-based healthcare systems.
(Jegadeesan et al. 2020)	Health data	Authentication	Anonymous authentication preserves patient privacy while reducing communication and computing costs.

Table 1.2. *Cryptography for e-health*

Nagamani et al. (2018) proposed a secure e-health system to predict patient condition based on problems and symptoms described by the user. This approach uses a system to study symptoms and provide an appropriate solution. To guarantee the confidentiality of transmitted information, it is encrypted using password-based encryption (PBE). The system also generates an encryption key from the user's password. In addition, a checksum is generated using the MD5 hash algorithm, and this value is appended to the transmitted data for user authentication.

Sammoud et al. (2020) proposed a session key exchange protocol using ECG. Sharma and Bhatt (2021) used quantum mechanics to secure IoT-based healthcare systems. Jegadeesan et al. (2020) presented an anonymous authentication scheme that preserves patient privacy while reducing communication and computational costs. Table 1.2 presents some cryptography-based security proposals.

1.8.2. *Biometrics*

Biometrics is the science of establishing an individual's identity based on physical or behavioral characteristics. The most common examples of biometric characteristics are DNA, fingerprint, iris, face, keystroke, smell, signature, retina, voice and hand veins. Biometric systems normally operate in two modes: verification and identification. In verification mode, the system validates the person's identity by matching the captured biometric information with its own biometric template(s) stored in the database. In identification mode, the system identifies a person by looking for a match between the templates of all the users in the database. As a result, the verification system performs a one-to-many comparison to establish an individual's identity. Biometrics has been used to improve the security and confidentiality of patient data in e-health applications.

In Jahan et al. (2019), an efficient and robust biometric system is proposed to authenticate the user and preserve the confidentiality of medical records. An approach using ECG-based biometrics is proposed for verifying patient identity and maintaining confidentiality of medical records. The specificity and availability of the ECG make it a suitable biometric choice.

The signal is captured, processed and then compared with the sample model; the result obtained indicates whether the user is authentic or not.

Ali et al. (2018) used biometric authentication. It operates in several phases: initialization, registration, login and authentication. To provide multi-level authentication, both the patient's fingerprints and the smart card are verified for login. In addition, mutual authentication and session key exchange are performed between the user and the medical server.

After studying a variety of attacks when accessing electronic medical records in a cloud environment, Hathaliya et al. (2019) developed an authentication and key exchange system based on fingerprint biometrics. The system also encrypts biometric data and a 160-bit random number and performs mutual authentication using a message authentication code (MAC). Sammoud et al. (2020) have proposed a multifactor authentication protocol using ECG biometric data. Table 1.3 presents some biometric-based security proposals.

References	Type of Data	Algorithm	Proposition
(Ali et al. 2018)	Medical data	Digital fingerprint + hash function	Secure data transmission between patient and healthcare professional.
(Jahan et al. 2019)	Base of ECG	ECG	User authentication to safeguard the security of medical records.
(Hathaliya et al. 2019)	Medical record	Digital fingerprint	Fingerprint authentication for secure access to medical records.
(Sammoud et al. 2020)	Medical data	ECG	Multi-factor authentication using ECG.

Table 1.3. *Biometrics for e-health*

1.8.3. *Blockchain*

Blockchain is one of the technologies used in e-health systems. It consists of a list of blocks in a distributed connected structure (Casino et al. 2018). It stores transactions and groups them in a structure (Li et al. 2020). Each block is stored at all network nodes in chronological order. Blockchain has

solved the problem of centralization in a distributed system, bypassing single-point-of-failure issues and reducing transaction costs. Since no central authority is involved, transaction speed is also increased (Li et al. 2020).

Maintaining the integrity and confidentiality of medical records is paramount (Singh et al. 2017). The immutable property of blockchain ensures this (Agbo et al. 2019). In addition, it also guarantees data security and confidentiality. The decentralized structure of the blockchain can be implemented in healthcare systems, helping to preserve the confidentiality of sensitive data. Since blocks are replicated at each network node, the likelihood of data loss decreases and patients can also control access to their records (Agbo et al. 2019).

A system is proposed in Chen et al. (2018) for secure storage and communication using the blockchain of medical records between patients, medical institutes and third-party agencies. Patient details as well as medical records are encrypted using asymmetric encryption. What is more, the patient can authorize or withdraw access at any time.

An access control method is proposed in Fan et al. (2018), combining the concepts of blockchain and cryptography. It provides a solution for managing and sharing a large volume of medical data. Asymmetric encryption is used to secure medical records. The hash value of encrypted data is added to verify data integrity and authenticity.

Ichikawa et al. (2017) have designed an app for patients with insomnia, which allows timely scheduling of sessions based on patient-supplied data. JavaScript Object Notation (JSON) format is used to store the data. The proposed system also offers tamper-resistance using the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. Data can be successfully updated even in situations such as a network failure.

Garg et al. (2020) proposed a low-cost protocol with authentication in the IoT environment using blockchain. Islam and Young Shin proposed a blockchain-based healthcare system to help unmanned aerial vehicles (UAVs) secure health data collected from users and store it on the nearest server on the UAV's path (Islam et al. 2020). Miyachi et al. (2021) presented a blockchain-based system that preserves patient privacy.

Table 1.4 presents security proposals based on the blockchain.

References	Type of Data	Algorithm	Proposition
(Ichikawa et al. 2017)	Insomnia patient data	PBFT	Non-violation of medical data when updating.
(Chen et al. 2018)	Indexing information for medical data and transaction records	Encryption	Privacy protection, secure sharing and storage of medical data.
(Fan et al. 2018)	Medical information	Asymmetric encryption and hashing	Secure data sharing and controlled access to medical data.
(Garg et al. 2020)	Medical information	Hashing	Access control.
(Islam et al. 2020)	Patient data in UAVs	Hashing	Securing health data collected from users in the UAV and storing it on the server closest to the UAV.
(Miyachi et al. 2021)	Confidential patient data	Encryption and hashing	Protecting patient privacy.

Table 1.4. *Using the blockchain in e-health*

1.9. Perspectives

– Data sharing: data generated by different devices can pose a variety of security and confidentiality problems for e-health systems, as patient data are sensitive and should not be shared by all medical staff. It is therefore necessary to adapt security countermeasures to guarantee the security, confidentiality and access control of medical data and devices.

– Medical data: a considerable amount of data is collected from various devices. These data are constantly changing as a function of the patient's state of health. Managing this amount of information is a time-consuming task. What is more, different types of data need to be stored in different formats. It is therefore necessary to have an efficient data management system capable of converting the file according to the needs of each medical application.

– Lack of standardization: many devices are used in e-health systems to measure, collect and relay health data. Each device has its own set of protocols and configurations for sharing this information with medical staff. However, there is no centralized consensus or standardization available for the communication, implementation and deployment of these devices. It is

therefore necessary to research this aspect, so that devices using different standards and protocols can communicate.

1.10. Conclusion

In the digital age, e-health is playing an increasingly important role in the management of chronic diseases and in communication between healthcare professionals and patients. Thanks to technological advances, it is now possible to ensure continuous, real-time disease management, both inside and outside medical structures.

The aim of e-health is to improve healthcare services using digital technologies. This makes healthcare more accessible, efficient and personalized for a greater number of people, contributing to better health and well-being.

In this context, various e-health architectures have been developed to integrate digital technologies into healthcare systems. A simplified architecture has been presented, bringing together the different technologies used in this field. This architecture makes it possible to visualize the various components and interactions between healthcare system actors, connected medical devices, mobile applications, data platforms and so on.

The security of e-health systems is also an essential aspect examined in this chapter. Healthcare data are sensitive and confidential, and it is crucial to implement robust security measures to protect them against cyber-attacks and unauthorized access. Various security techniques are used, such as user authentication and authorization, data encryption, access management and suspicious activity monitoring.

In short, e-health uses technological advances to improve healthcare services and promote continuous, real-time management of chronic diseases. e-Health architectures provide a global vision of the various technologies used, while security techniques guarantee data protection and the confidentiality of medical information. These advances contribute to improved accessibility and more effective, personalized healthcare for patients.

1.11. References

Agbo, C.C., Mahmoud, Q.H., Eklund, J.M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare*, 7(2), 56.

Ali, R. and Pal, A.K. (2018). Cryptanalysis and biometric-based enhancement of a remote user authentication scheme for e-healthcare system. *Arabian Journal for Science and Engineering*, 43, 7837–7852.

Anand, A. and Singh, A.K. (2020). Joint watermarking-encryption-ECC for patient record security in wavelet domain. *IEEE MultiMedia*, 27(3), 66–75.

Atienza, A.A., Hesse, B.W., Baker, T.B., Abrams, D.B., Rimer, B.K., Croyle, R.T., Volckmann, L.N. (2007). Critical issues in e-health research. *American Journal of Preventive Medicine*, 32(5), S71–S74.

Balakrishnan, L. (2021). An Internet of Things (IoT) based intelligent framework for healthcare – A survey. In *2021 3rd International Conference on Signal Processing and Communication (ICPSC)*. IEEE.

Basaklar, T., Tuncel, Y., An, S., Ogras, U. (2021). Wearable devices and low-power design for smart health applications: Challenges and opportunities. In *2021 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*. IEEE.

Bashshur, R., Shannon, G., Krupinski, E., Grigsby, J. (2011). The taxonomy of telemedicine. *Telemedicine and e-Health*, 17(6), 484–494.

Behera, S.K. (2021). Chipless RFID sensors for wearable applications: A review. *IEEE Sensors Journal*, 22(2), 1105–1120.

Casino, F., Dasaklis, T.K., Patsakis, C. (2019). A systematic literature review of block-chain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81.

Chen, Y., Ding, S., Xu, Z., Zheng, H., Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. *Journal of Medical Systems*, 43, 1–9.

Chung, Y.F. and Liu, C.H. (2013). Design of a wireless sensor network platform for tele-homecare. *Sensors*, 13(12), 17156–17175.

Devedžić, G., Koceski, S., Savić, S.P. (2021). A brief overview of enabling technologies for digital medicine and smart healthcare. In *2021 10th Mediterranean Conference on Embedded Computing (MECO)*. IEEE.

Fagroud, F., Ben Lahmar, E., El Filali, S. (2019). Internet of things: Statistical study on research evolution. *International Journal of Advances in Electronics and Computer Science*, 6(5), 4–13.

Fan, K., Wang, S., Ren, Y., Li, H., Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of Medical Systems*, 42, 1–11.

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems*, 78, 659–676.

Garg, N., Wazid, M., Das, A.K., Singh, D.P., Rodrigues, J.J., Park, Y. (2020). BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment. *IEEE Access*, 8, 95956–95977.

Gourob, J.H., Raxit, S., Hasan, A. (2021). A robotic hand: Controlled with vision based hand gesture recognition system. In *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*. IEEE.

Gupta, B.B., Perez, G.M., Agrawal, D.P., Gupta, D. (2020). *Handbook of Computer Networks and Cyber Security*. Springer, Cham.

Gupta, M., Tanwar, S., Rana, A., Walia, H. (2021). Smart healthcare monitoring system using wireless body area network. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. IEEE.

Hajar, M.S., Al-Kadri, M.O., Kalutarage, H.K. (2021). A survey on wireless body area networks: Architecture, security challenges and research opportunities. *Computers & Security*, 104, 102211.

Hamdi, O., Chalouf, M.A., Ouattara, D., Krief, F. (2014). eHealth: Survey on research projects, comparative study of telemonitoring architectures and main issues. *Journal of Network and Computer Applications*, 46, 100–112.

Hathaliya, J.J., Tanwar, S., Tyagi, S., Kumar, N. (2019). Securing electronics healthcare records in healthcare 4.0: A biometric-based approach. *Computers & Electrical Engineering*, 76, 398–410.

Hermes, S., Riasanow, T., Clemons, E.K., Böhm, M., Krcmar, H. (2020). The digital transformation of the healthcare industry: Exploring the rise of emerging platform eco-systems and their influence on the role of patients. *Business Research*, 13, 1033–1069.

Hodgkiss, J. and Djahel, S. (2020). Securing fuzzy vault enabled authentication in body area networks-based smart healthcare. *IEEE Consumer Electronics Magazine*, 11(1), 6–16.

Ichikawa, D., Kashiyama, M., Ueno, T. (2017). Tamper-resistant mobile health using blockchain technology. *JMIR mHealth and uHealth*, 5(7), e7938.

Islam, A. and Shin, S.Y. (2020). A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. *Computers & Electrical Engineering*, 84, 106627.

Jahan, S., Chowdhury, M., Islam, R. (2019). Robust user authentication model for securing electronic healthcare system using fingerprint biometrics. *International Journal of Computers and Applications*, 41(3), 233–242.

Javaid, S., Zeadally, S., Fahim, H., He, B. (2022). Medical sensors and their integration in wireless body area networks for pervasive healthcare delivery: A review. *IEEE Sensors Journal*, 22(5), 3860–3877.

Jegadeesan, S., Azees, M., Babu, N.R., Subramaniam, U., Almakhles, J.D. (2020). EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). *IEEE Access*, 8, 48576–48586.

Kaur, D., Uslu, S., Rittichier, K.J., Durresi, A. (2022). Trustworthy artificial intelligence: A review. *ACM Computing Surveys (CSUR)*, 55(2), 1–38.

Koren, A. and Prasad, R. (2022). IoT health data in electronic health records (EHR): Security and privacy issues in era of 6G. *Journal of ICT Standardization*, 10(1), 63–84.

Kostkova, P. (2015). Grand challenges in digital health. *Frontiers in Public Health*, 3, 134.

Légifrance (2010). Décret No. 2010-1229 du 19 octobre 2010 relatif à la télémédecine [Online]. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000022932449/ [Accessed 22 February 2023].

Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107, 841–853.

Mashayekhi, A., Behbahani, S., Ficuciello, F., Siciliano, B. (2020). Influence of human operator on stability of haptic rendering: A closed-form equation. *International Journal of Intelligent Robotics and Applications*, 4, 403–415.

Minakshi, J.A.H. (2016). An overview of wireless body area network (WBAN) using Zigbee technology. *International Journal of Scientific Development and Research (IJSDR)*, 1, 2455–2631.

Miyachi, K. and Mackey, T.K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information Processing & Management*, 58(3), 102535.

Nagamani, S. and Nagaraju, D.R. (2018). A mobile cloud-based approach for secure m-health prediction application. *International Journal for Innovative Engineering & Management Research*, 7(12).

Negra, R., Jemili, I., Belghith, A. (2016). Wireless body area networks: Applications and technologies. *Procedia Computer Science*, 83, 1274–1281.

Qadir, A.M. and Varol, N. (2019). A review paper on cryptography. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE.

Rabbani, R., Najafiaghdam, H., Ghanbari, M.M., Papageorgiou, E.P., Zhao, B., Roschelle, M., Stojanovic, V., Muller, R., Anwar, M. (2021). Towards an implantable fluorescence image sensor for real-time monitoring of immune response in cancer therapy. In *2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*.

Sammoud, A., Chalouf, M.A., Hamdi, O., Montavont, N., Bouallegue, A. (2020). A new biometrics-based key establishment protocol in WBAN: Energy efficiency and security robustness analysis. *Computers & Security*, 96, 101838.

Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E. (1996). Role-based access control models. *Computer*, 29(2), 38–47.

Saranya, P. and Asha, P. (2019). Survey on big data analytics in health care. In *2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)*. IEEE.

Sharma, A. and Bhatt, A.P. (2021). Quantum cryptography for securing IoT-based healthcare systems. In *Limitations and Future Applications of Quantum Cryptography*, Kumar, N., Agrawal, A., Chaurasia, B.K. (ed.). IGI Global, Hershey, PA, 124–147.

Singh, A.K. and Kumar, C. (2020). Encryption-then-compression-based copyright protection scheme for E-governance. *IT Professional*, 22(2), 45–52.

Singh, A.K., Kumar, B., Singh, G., Mohan, A. (2017). *Medical Image Watermarking*. Springer Science Business Media, Berlin.

Siva Bharathi, K.R. and Venkateswari, R. (2019). Security challenges and solutions for wireless body area networks. In *Computing, Communication and Signal Processing: Proceedings of ICCASP 2018*. Springer, Berlin.

Sobhan, S., Islam, S., Valero, M., Shahriar, H., Ahamed, S.I. (2021). Data analysis methods for health monitoring sensors: a survey. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*.

Sujatha, S. and Govindaraju, R. (2013). A secure crypto based ECG data communication using modified SPHIT and modified quasigroup encryption. *International Journal of Computer Applications*, 78(6).

Sun, J., Zhu, X., Zhang, C., Fang, Y. (2011). HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare. In *2011 31st International Conference on Distributed Computing Systems*. IEEE.

Sundaram, J.P.S., Wan, D., Zhao, Z. (2019). A survey on LoRa networking: Research problems, current solutions and open issues. *IEEE Communications Surveys & Tutorials*, 22, 371–388.

Thakur, S., Singh, A.K., Ghrera, S.P., Dave, M. (2018). Watermarking techniques and its applications in tele-health: A technical survey. In *Cryptographic and Information Security: Approaches for Images and Videos*, Ramakrishnan, S. (ed.). CRC Press, New York.

Wang, K., Shao, Y., Shu, L., Zhu, C., Zhang, Y. (2016). Mobile big data fault-tolerant processing for e-health networks. *IEEE Network*, 30(1), 36–42.

Yang, Y., Wang, H., Jiang, R., Guo, X., Cheng, J., Chen, Y. (2022). A review of IoT-enabled mobile healthcare: Technologies, challenges, and future trends. *IEEE Internet of Things Journal*, 9(12), 9478–9502.