

SCIENCES

NETWORKS AND COMMUNICATIONS

Network Management and Control

e-Health Security Management

*Communications Security,
Data Processing Security
and Patient Privacy*

**Coordinated by
Omessaad Hamdi**

ISTE

WILEY

Table of Contents

[Cover](#)

[Table of Contents](#)

[Title Page](#)

[Copyright Page](#)

[1 Overview of e-Health Architectures](#)

[1.1. Introduction](#)

[1.2. Definitions](#)

[1.3. e-Health services](#)

[1.4. Requirements for e-health systems](#)

[1.5. e-Health system architecture](#)

[1.6. e-Health system technologies](#)

[1.7. Security in e-health systems](#)

[1.8. Medical data security](#)

[1.9. Perspectives](#)

[1.10. Conclusion](#)

[1.11. References](#)

[2 Vulnerabilities in e-Health and Countermeasures](#)

[2.1. Introduction](#)

[2.2. The importance of digitization in healthcare systems](#)

[2.3. The challenges of digitization in e-health systems](#)

[2.4. Cyber-attacks in the healthcare sector](#)

[2.5. Security incidents in the healthcare sector](#)

[2.6. Existing security measures for e-health systems](#)

[2.7. Recommendations for protecting e-health systems](#)

[2.8. Conclusion](#)

[2.9. References](#)

[3 Security Policies for e-Health Systems](#)

[3.1. Introduction](#)

[3.2. The concept of the security policy](#)

[3.3. Environment for specifying, validating and testing security policies](#)

[3.4. Security services for e-health systems](#)

[3.5. Security requirements for e-health platforms](#)

[3.6. Future security challenges for e-health](#)

[3.7. Conclusion](#)

[3.8. References](#)

[4 Adaptive, Dynamic, Decentralized Authorizations for e-Health](#)

[4.1. Introduction](#)

[4.2. Fundamental principles](#)

[4.3. Proposal for dynamic, decentralized adaptation of e-health authorizations](#)

[4.4. Conclusion](#)

[4.5. References](#)

[5 Applying Blockchain to e-Health](#)

[5.1. Introduction](#)

[5.2. Blockchain technology](#)

[5.3. Health sector](#)

[5.4. Issues and challenges for the healthcare sector](#)

[5.5. Application of blockchain technology in e-health systems](#)

[5.6. Implementing blockchain technology in healthcare](#)

[5.7. Contribution of the blockchain solution](#)

[5.8. Conclusion](#)

[5.9. References](#)

[6 Using Biometrics to Secure Intra-BAN Communications](#)

[6.1. Introduction](#)

[6.2. Security for WBAN](#)

[6.3. Security solutions for intra-WBAN communications](#)

[6.4. Biometric data-based security solutions for WBANs](#)

[6.5. Discussion](#)

[6.6. Conclusion](#)

[6.7. References](#)

[7 Using Biometrics for Authentication in e-Health Systems](#)

[7.1. Introduction](#)

[7.2. e-Health systems](#)

[7.3. Authentication techniques](#)

[7.4. Biometric authentication](#)

[7.5. Multimodal authentication](#)

[7.6. Multi-factor authentication approaches for e-health system security](#)

[7.7. Conclusion](#)

[7.8. References](#)

[8 Security of Medical Data Processing](#)

[8.1. Introduction](#)

[8.2. Homomorphic encryption](#)

[8.3. Attribute-based encryption](#)

[8.4. Conclusion](#)

[8.5. References](#)

[9 Artificial Intelligence for Security of e-Health Systems](#)

[9.1. Introduction](#)

[9.2. e-Health systems](#)

[9.3. e-Health system security](#)

[9.4. Artificial intelligence techniques](#)

[9.5. Intrusion detection based on artificial intelligence](#)

[9.6. AI-based IDS in WBANs](#)

[9.7. Conclusion](#)

[9.8. References](#)

[List of Authors](#)

[Index](#)

[End User License Agreement](#)

List of Tables

Chapter 1

[Table 1.1. Application of sensors and connected objects in e-health systems](#)

[Table 1.2. Cryptography for e-health](#)

[Table 1.3. Biometrics for e-health](#)

[Table 1.4. Using the blockchain in e-health](#)

Chapter 2

[Table 2.1. Overview of the measures described \(NCSC 2022\).](#)

Chapter 4

[Table 4.1. Comparison of the proposed solution with a conventional solution](#)

Chapter 5

[Table 5.1. Medical applications using blockchain](#)

[Table 5.2. Characteristics of blockchain projects in the medical field](#)

[Table 5.3. Comparison of data processing approaches in the medical field](#)

Chapter 6

[Table 6.1. Security solutions for intra-WBAN communications \(Narwal et al. 202...](#)

[Table 6.2. Notations used in the description of Sammoud et al.'s \(2020\) approa...](#)

[Table 6.3. Biometric-based approaches to securing intra-BAN communications](#)

Chapter 7

[Table 7.1. Authentication factors](#)

[Table 7.2. Biometric features](#)

[Table 7.3. Effectiveness of biometric features \(Fatima et al. 2019\)](#)

[Table 7.4. Multimodal authentication](#)

[Table 7.5. Comparison of resource consumption of multifactor authentication ap...](#)

[Table 7.6. Security comparison of multifactor authentication approaches betwee...](#)

[Table 7.7. Notations used in the description of Sammoud et al.'s \(2020\) approa...](#)

Chapter 8

[Table 8.1. Comparison of PHE schemes](#)

[Table 8.2. Comparison of SHE schemes](#)

[Table 8.3. Comparison of FHE schemes](#)

[Table 8.4. Main differences between KP-ABE and CP-ABE](#)

[Table 8.5. Comparison of ABE schemes](#)

[Table 8.6. Summary of ABE solutions for securing e-health](#)

Chapter 9

[Table 9.1. Possible solutions for WBAN security \(Chalouf 2020\).](#)

List of Illustrations

Chapter 1

[Figure 1.1. Components of e-health](#)

[Figure 1.2. Services and requirements for e-health systems](#)

[Figure 1.3. Architecture of e-health systems \(Hajar et al. 2021\)](#)

[Figure 1.4. e-Health technologies](#)

[Figure 1.5. Security in e-health systems](#)

Chapter 2

[Figure 2.1. Representation of data breach incidents by industry sector \(Seh et...](#)

[Figure 2.2. Attack statistics for e-health 2020, 2021 and 2022 \(WHO 2022\).](#)

[Figure 2.3. Safety mechanisms implemented \(HIMSS 2021\).](#)

Chapter 3

[Figure 3.1. Modeling an ESP](#)

[Figure 3.2. Security_policy test environment](#)

[Figure 3.3. Information accountability framework \(Gajanayake et al. 2012\).](#)

Chapter 4

[Figure 4.1. Context lifecycle](#)

[Figure 4.2. Example of a context-aware security system](#)

[Figure 4.3. ACE framework base protocol exchanges](#)

[Figure 4.4. ACE e-health security framework architecture](#)

[Figure 4.5. A simplified view of blockchain architecture](#)

[Figure 4.6. Architecture for dynamic and decentralized adaptation of e-health ...](#)

[Figure 4.7. Proposed new authorization flow for dynamic, decentralized adaptat...](#)

Chapter 5

[Figure 5.1. How blockchain technology works \(Dellys 2020\).](#)

[Figure 5.2. Blockchain types and applications](#)

Chapter 6

[Figure 6.1. Example of a BAN \(Hajar et al. 2021\).](#)

[Figure 6.2. An ECG sequence \(Yao et al. 2011\).](#)

[Figure 6.3. A PPG sequence \(Charlton et al. 2020\)](#)

[Figure 6.4. Establishing symmetrical keys between a parent node and its child ...](#)

[Figure 6.5. Establishing the symmetrical key between two child nodes](#)

[Figure 6.6. Primary key generation by nodes \$N_1\$ and \$N_2\$](#)

[Figure 6.7. Generating a biometric session key](#)

Chapter 7

[Figure 7.1. Authentication techniques](#)

[Figure 7.2. Protocol registration phase](#)

[Figure 7.3. Connection and protocol authentication phase](#)

Chapter 8

[Figure 8.1. Homomorphic encryption for e-health solutions in cloud computing](#)

[Figure 8.2. Stages of an asymmetric homomorphic encryption scheme](#)

[Figure 8.3. Gentry's model for building an FHE](#)

[Figure 8.4. KP-ABE schema](#)

[Figure 8.5. CP-ABE schema](#)

Chapter 9

[Figure 9.1. Confusion matrix for the "decision tree" model](#)

[Figure 9.2. Confusion matrix for the neural network model](#)

[Figure 9.3. Confusion matrix for the "naive Bayes" model](#)

[Figure 9.4. Confusion matrix for the “decision tree” model with 5% noise...](#)

[Figure 9.5. Confusion matrix for the “decision tree” model with 40% noise...](#)

[Figure 9.6. IDS performance as a function of noise level.](#)

SCIENCES

Networks and Communications,
Field Director - Guy Pujolle

Network Management and Control,
Subject Head - Francine Krief

e-Health Security Management

**Communications Security, Data
Processing Security and Patient
Privacy**

Coordinated by

Omessaad Hamdi

ISTE

WILEY

First published 2024 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licenses issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned address:

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

© ISTE Ltd 2024

The rights of Omessaad Hamdi to be identified as the author of this work have been asserted by her in accordance with the Copyright, Designs and Patents Act 1988.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s), contributor(s) or editor(s) and do not necessarily reflect the views of ISTE Group.

Library of Congress Control Number: 2024942248

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-78945-179-5

ERC code:
PE6 Computer Science and Informatics

PE6_5 Cryptology, security, privacy, quantum cryptography

PE6_7 Artificial intelligence, intelligent systems, multi agent systems

PE7 Systems and Communication Engineering

PE7_8 Networks (communication networks, sensor networks, networks of robots, etc.)

PE7_11 Components and systems for applications (in e.g. medicine, biology, environment)

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.

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.

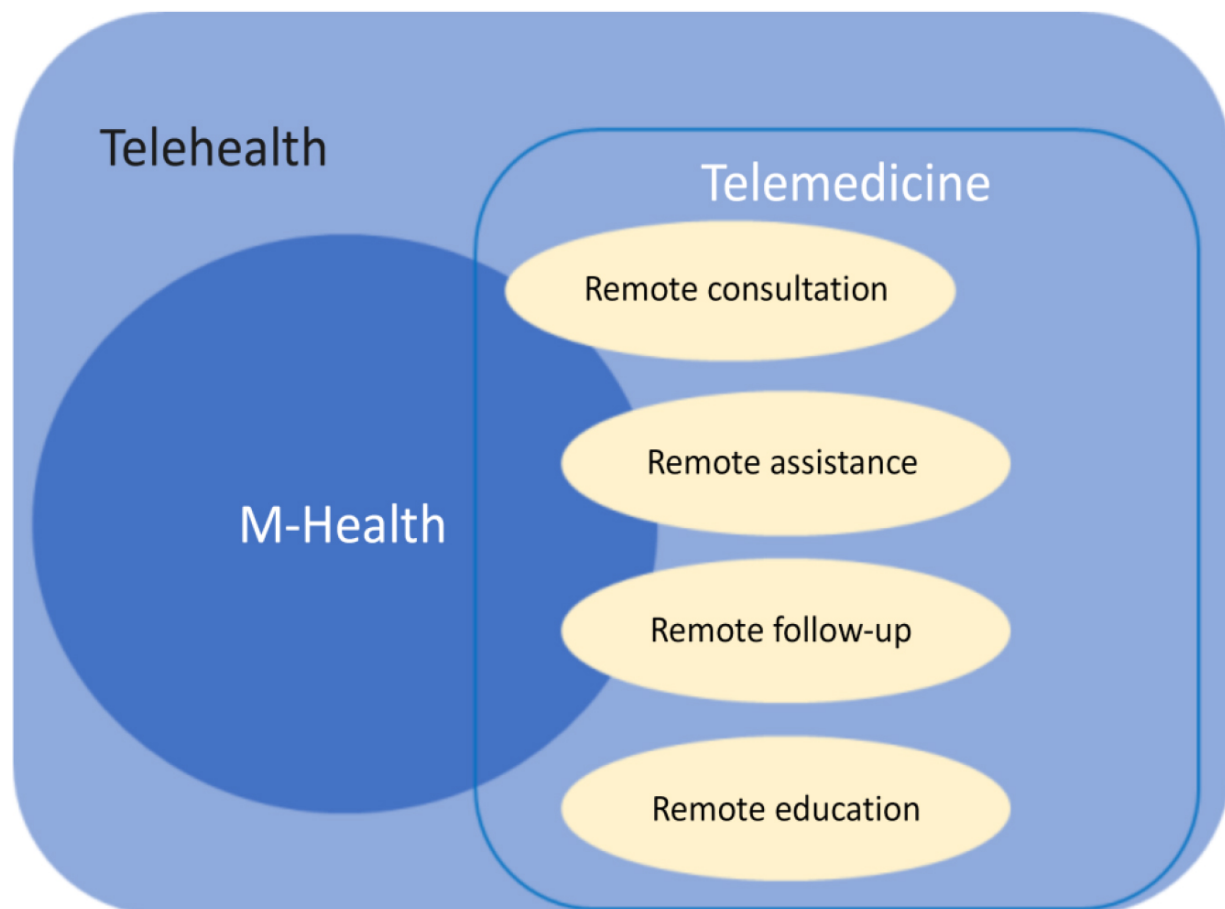


Figure 1.1. *Components of e-health*

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.

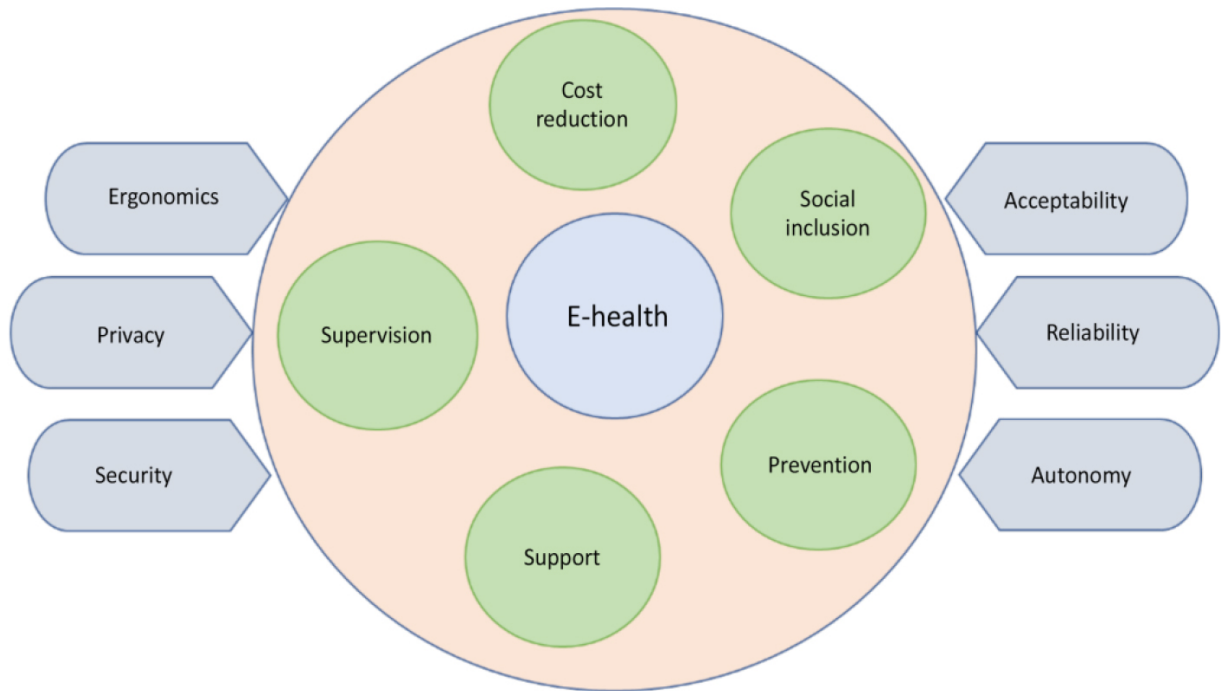


Figure 1.2. *Services and requirements for e-health systems*

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.

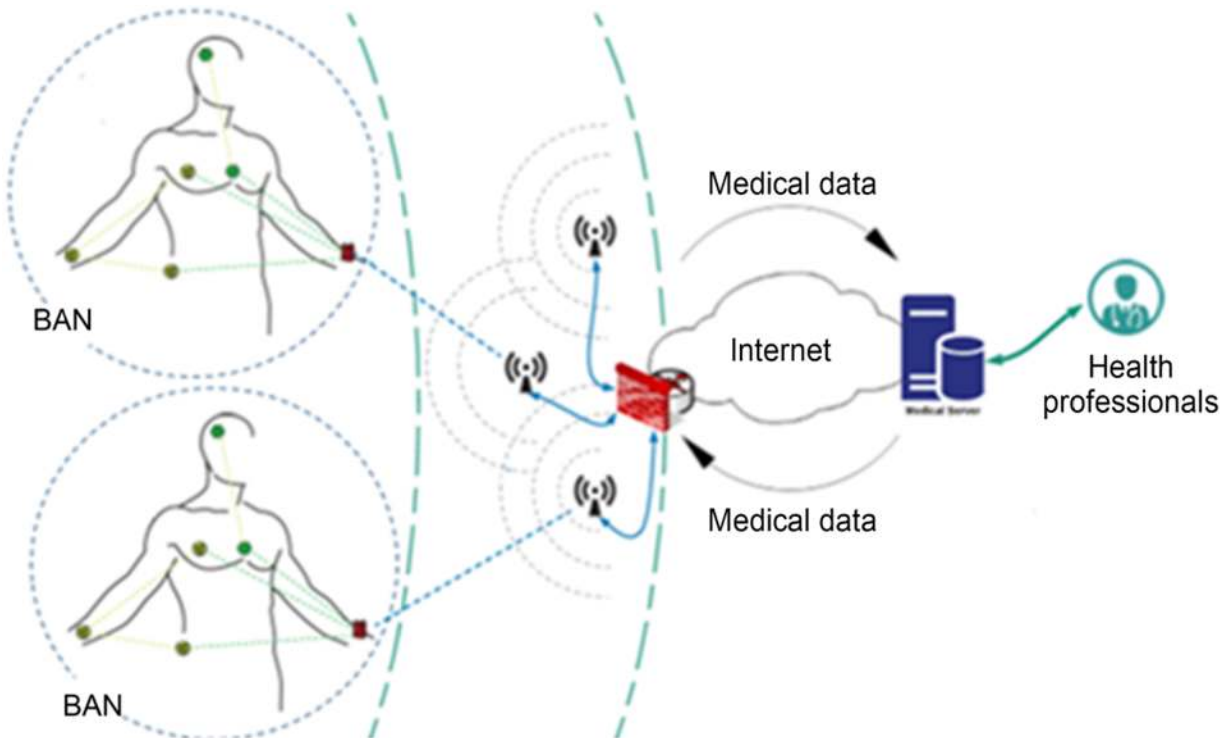


Figure 1.3. *Architecture of e-health systems (Hajar et al. 2021)*

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).

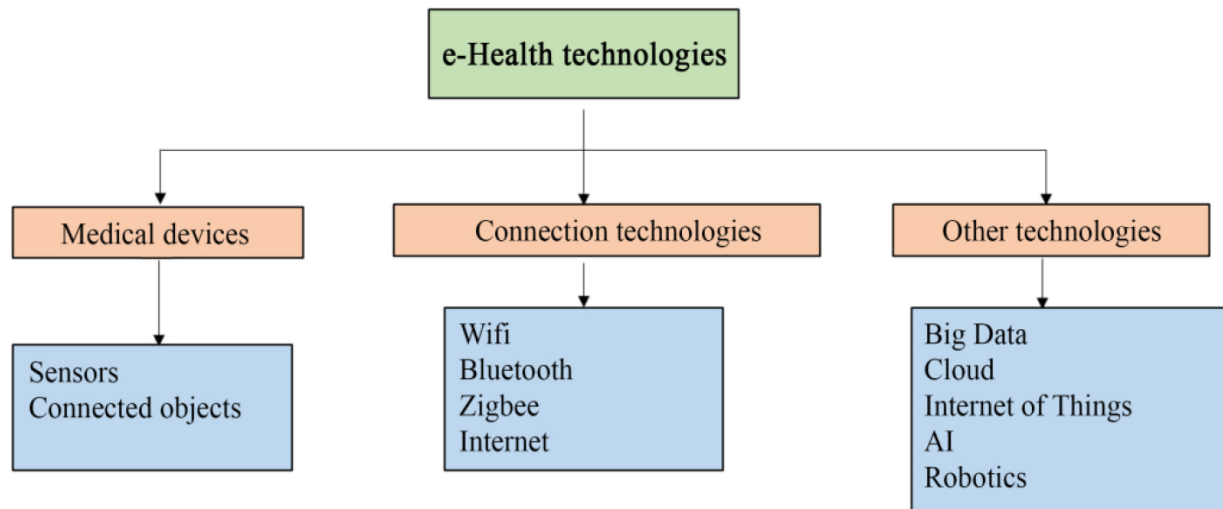


Figure 1.4. *e-Health technologies*

[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.

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

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.

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](#)).

List of Authors

Ryma ABASSI
Innov'COM
SUP'COM
Université de Carthage
Tunis
Tunisia

Manel ABDELHEDI
Noccs
ENISo
Université de Sousse
Tunisia

Mohamed AYMEN CHALOUF
IRISA
Université de Rennes
France

Aida BEN CHEHIDA DOUSS
Innov'COM
SUP'COM
Université de Carthage
Tunis
Tunisia

Faiza HAMDI
Jeddah University
Saudi Arabia

Omessaad HAMDI
IEEE
Rennes
France

Francine KRIEF
LaBRI
Bordeaux INP
France

Cyrine LAHSINI
Sys'Com-ENIT
Université de Tunis El Manar
Tunis
Tunisia

Hana MEJRI
Sys'Com-ENIT
Université de Tunis El Manar
Tunis
Tunisia

Léo MENDIBOURE
ERENA
COSYS
Université Gustave Eiffel
Marne-la-Vallée
France

Amal SAMMOUD
MIRA
Aflokkat
Ajaccio
France

Tidiane SYLLA
GEII
ISA
USTTB
Bamako
Mali