Securing advanced healthcare architectures

Mohamed Mohammedi

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Faculté des Sciences Exactes
Département d'Informatique
Laboratoire d'Informatique Médicale (LIMED)

THÈSE

EN VUE DE L'OBTENTION DU DIPLÔME DE DOCTORAT

Domaine : Mathématiques et Informatique **Filière :** Informatique
Spécialité : Réseaux et Systèmes Distribués

Présentée par
Mohamed MOHAMMEDI

Thème

Securing advanced healthcare architectures

Soutenue publiquement le 04/02/2018 devant le Jury composé de :

Nom et Prénom	**Grade**		
M. Abdellah BOUKERRAM	Professeur	Univ. de Bejaia, Algérie	Président
M. Abdelmadjid BOUABDALLAH	Professeur	UTC de Compiègne, France	Rapporteur
M. Mawloud OMAR	MCA	Univ. de Bejaia, Algérie	Co-rapporteur
M. Hachem SLIMANI	MCA	Univ. de Bejaia, Algérie	Examinateur
M. Mourad AMAD	MCA	Univ. de Bouira, Algérie	Examinateur

Année Universitaire : **2017/2018**

Acknowledgements

In opening, before any subjective consideration, I would like to express my great and special thanks to God, the Almighty, for his mercy upon us and to have endowed me with a great will and adequate knowledge to complete this research work successfully.

First, I would like to deeply thank Dr Mawloud Omar and Prof. Abdelmadjid Bouabdallah, my thesis supervisors for the assistance they gave me, for their encouragement, availability, sympathy, orientations, and advice, without them this work will not come to light. Also, thanks to their confidence I was able to fulfill myself completely in my missions. They were of precious help in the most delicate moments, that they find here the expression of my profound gratitude.

I am really grateful to Prof. Abdellah Boukerram for having agreed to chair the jury and review this thesis work. I would like also to express my very sincere thanks to Dr Hachem Slimani, and Dr Mourad Amad for the interest that they had kindly given to this thesis work, while accepting to be examiners about it.

All this without forgetting my family for their support during all my career studies: to my dearest parents who have always been there with me, for the sacrifices made towards me, for their support and all the efforts made for my education and training. To my sisters, Saida, Samira, Sonia, Katia, and my brother-in-law Hakim, for their moral support, their kindness, their availability, their trust and their precious advice, which helped me in difficult times, thank you for being with me. To my two lovely little nieces Malak and Celine. My thanks go also to all my uncles, aunts who pushed me to go all the way, and also to all my cousins for their support when I was sinking into a frightening pessimism.

My special thanks also go to the entire research team of Heudiasyc Laboratory, CNRS UMR 7253, for their welcome, team spirit and in particular my internship master, Prof. Abdelmadjid Bouabdallah, for his welcome, the time spent together, and sharing his expertise on a daily basis.

I would never forget to express all my gratitude to all the members of computer science department of University of Bejaia, whether they are teachers or administrators,

who closely or remotely saved no effort to ensure that our training and our work ends in good conditions.

Finally, I address my thanks to all my loyal friends who will recognize each other without my needing to name them ... for their multiple helps, their support or quite simply for their friendship.

I would like to dedicate this thesis
To my noble parents
To my dear sisters, my brother-in-law, and my nieces
To all those nice people that I love ...

The author publications

Journal papers

1. M. Mohammedi, M. Omar, and A. Bouabdallah. *Secure and lightweight remote patient authentication scheme with biometric inputs for mobile healthcare environments.* Journal of Ambient Intelligence and Humanized Computing (Springer Publisher), DOI: https://doi.org/10.1007/s12652-017-0574-5, 2017.

2. S. Zebboudj, F. Cherif, M. Mohammedi, and M. Omar. *Secure and efficient ECG-based authentication scheme for medical body area sensor networks.* Smart Health (Elsevier Publisher), DOI: https://doi.org/10.1016/j.smhl.2017.07.001, 2017.

3. M. Mohammedi, M. Omar, D. Zamouche, K. Louiba, S. Ouared, and K. Hocini. Energy-aware key management and access control for the internet of things. Submitted to journal: World Wide Web.

Conference papers

4. M. Mohammedi, M. Omar, W. Aitabdelmalek, A. Mansouri, and A. Bouabdallah. *Secure and lightweight biometric-based remote patient authentication scheme for home healthcare systems.* In proceedings of the 13^{th} International Symposium on Programming and Systems- ISPS'2018 (IEEE Publisher), DOI: 10.1109/ISPS.2018.8379017, 2018.

5. M. Mohammedi, M. Omar, and A. Bouabdallah. *Automatic removal of ocular artifacts in EEG signals for driver's drowsiness detection: A survey.* Submitted to SACONET '18: the 7^{th} IEEE International Conference on Smart Communications in Network Technologies (IEEE Publisher).

6. M. Mohammedi, M. Omar, Y. Challal, and A. Bouabdallah. *Cryptanalysis and improvement of identity-based multisignature scheme.* Submitted to ICFNDS '19: the 3^{rd} International Conference on Future Networks and Distributed Systems (ACM Publisher).

Seminars

7. M. Mohammedi. Biometric-based authentication scheme in mobile healthcare environments. LIMED laboratory, February 2015.

8. M. Mohammedi. Exploring EEG-based biometrics for user authentication on smart mobile devices. LIMED laboratory, May 2016.

Table of contents

List of figures

List of tables

Acronyms

BAN	Body Area Network
BEM	Bejaia Equipement Medical
CA	Certificate Authority
CDHP	Computational Diffie-Hellman Problem
CRC	Cyclic Redundancy Check
DNA	DeoxyriboNucleic Acid
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECG	ElectroCardioGram
ECG-AS	ElectroCardiGram-based Authentication Scheme
ECG-IJS	ElectroCardioGram-Improved Jules Sudan
EEG	ElectroEncephaloGram
EMG	ElectroMyoGram
EPR	Electronic Patient Record
FAR	False Acceptance Rate
FFT	Fast Fourier Transform
FRR	False Rejection Rate
GMM	Gaussian Mixing Model
GUI	Graphical User Interface
ID	IDentity
IPI	Inter Pulse Interval
MAC	Message Authentication Code
MBASN	Medical Body Area Sensor Network
MSB	Most Significant Bit

OPFKA	Ordered-Physiological-Feature-based Key Agreement
PDA	Personal Digital Assistant
PFKA	Physiological Feature based Key Agreement
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPG	PhotoPlethysmoGram
PSKA	Physiological Signal based Key Agreement
RAM	Random Access Memory
SIP	Session Initiation Protocol
WBAN	Wireless Body Area Network
WLAN	Wireless Local Area Network

General introduction

The recent progress in Microelectronics domain and the emergence of wireless communication technologies have given rise to new tools and communicating components, which improve the quality of life [95]. Thus, new lines of investigation were opened with the emergence of Body Area Sensor Networks (BASNs). This new monitoring and follow-up mechanism covers vast applications in several sectors, especially, in the field of military, healthcare, sports, entertainment and much else besides. However, the use of this type of network in the medical field is major, at a point that some authors present it as being dedicated only to health [13][116]. Today, the development of the BASNs becomes accessible at lower cost thanks to the availability of components with a reasonable cost, miniaturized, intelligent, and autonomous. In Medical Body Area Sensor Networks (MBASNs), these components could be deployed on or in the patient's body in close proximity. These medical sensors continuously monitor body functions, and collect different vital signs such as pulse oximeter, temperature, heart rate, oxygen saturation, blood pressure, blood glucose, etc., [81][119]. The need to measure these physiological parameters makes these components essential for the design of systems, which monitor and interact with the patient health to improve his recovery opportunities.

MBASNs conceal an enormous potential to revolutionize home healthcare area by providing real-time monitoring for people reached by serious and persistent disorders [40]. The need for medical and paramedical follow-up of this population is important to better monitor the evolution of their diseases and epidemics in order to hope to inhibit them, or even to prevent them before they are declared [66]. Likewise, the need for such monitoring is essential to ensure not only an early remote diagnosis, but also the possibility of drug treatment administration, and make pre-hospital emergency interventions in critical situations. In such monitoring technologies, each body sensor must transmit the vital signs, which has measured at a collection point (personal server/coordinator node) through a lower energy radio link. When the collection point

collects the medical data, it aggregates and sends it to a remote medical team via Internet or mobile telephone networks. This will facilitate the medical team to monitor the patient's health to ensure that the patient is within the expected health parameters [94].

Considering the social, ethical and legal aspects of medical systems, the collected data are very sensitive and must be managed correctly to ensure the patient privacy. An intruder can encrust himself in the system to impersonate a legitimate sensor and spy on, inject or reuse the patient-related data. Consequently, the communication parties must be able to exchange this data in a secure manner in order to avoid false processing due to malicious or erroneous modifications. Thus, in order to ensure reliable collection and transmission, it is essential to ensure the authentication service not only between the sensors, but also between the collection point and the remote server. However, providing an authentication system, which supports the protection of such critical data is a real challenge [90]. In this context, numerous of researches have been carried out to solve the security issue by using passwords and/or smart cards and establish a secure system based on authentication in a mobile healthcare environment [67]. However, these solutions foresee new challenges that require substantial revision or development of new solutions. By moving away from conventional authentication solutions, those based on physical or behavioral human features provide greater security and reliability for authentication between the communication parties [70][77][97]. Thus, this security mechanism allows these communication parties to agree on a cryptographic key enabling them to secure their future communications while ensuring their authenticity.

Considering all of the above, there is a need to find a security mechanism for the MBASNs so that the medical data will not be misused or involuntarily used by an intruder. Consequently, the main objective of this thesis is to design new authentication schemes adapted to the new medical management architectures, taking into account its constraints, meeting its specific needs in terms of security services and centered on the application requirements. So, the aim here is to come up with authentication solutions, which can be leveraged in different practical applications in healthcare environments. Besides, when proposing a new solution, the existence of some physical constraints of the MBASNs, especially, those of the sensors pose the problem of choosing the most appropriate cryptographic tools to use. As a result, our contributions put aside all these traditional cryptographic authentication tools, which

are expensive in resources.

This dissertation is structured into five chapters as follows. The current part represents the general introduction, which includes the context of our study, the challenges, as well as the thesis outline.

Chapter 1 will be devoted to the presentation of patient's health monitoring systems in healthcare environments. At the begining, we start with the definition of the various notions and concepts necessary revolving around this theme for understanding the remaining of the thesis. We present the medical monitoring mechanisms and technologies by describing their characteristics, their application areas, and their design constraints. In the rest of this chapter, we provide a general overview of the security requirements, as well as the biometrics, which exploit physical or behavioral human features for the identification and authentication of an individual in such a system.

Chapter 2 summarizes a critical review of biometric-based authentication schemes in the healthcare environments, which have been established over the past few years. In this study, we establish a detailed taxonomy of solutions, which we classify according to the orientation of the authentication service and the considered network architecture. Afterwards, we summarize the main operations of each solution followed by a discussion of the strengths and weaknesses of each one. Finally, we synthesize and compare the reviewed schemes based on a number of specific evaluation criteria, which we consider interesting.

In Chapter 3, we present our first contribution termed Secure and Lightweight Remote Patient Authentication Scheme with Biometric Inputs for Mobile Healthcare Environments. To address the issues of biometric-based authentication schemes, which introduce hard constraints, we propose an autonomous and secure approach to mend these shortcomings. This approach translates the patient's biometric data into cryptographic keys based on ECC (Elliptic Curve Cryptography). When a remote diagnosis is required or an unexpected incident has occurred on the patient's health, the latter can be effectively authenticated without the need to register or communicate the biometric data model. In order to validate the proposal, we analyze its security against some well known attacks. As well, we perform intensive simulations

by comparing it with recent schemes from the literature.

Chapter 4 will be devoted to the detailed description of our second contribution termed Secure and Efficient ECG-based Authentication Scheme for Medical Body Area Sensor Networks (MBASNs). In this chapter, we also propose an ECG-based authentication approach for medical body area networks, as well as a new method for biometric feature extraction. This method extracts with great accuracy the ECG features and makes the authentication between the sensors of the network more efficient. This scheme permits two sensors belonging to the same MBASN to agree on a shared secret key, which will be generated from the ECG signal features. To validate this proposal, we analyze its robustness against a panoply of attack scenarios. Moreover, we evaluate its performances through comparative simulations with concurrent schemes from the literature.

Chapter 5 is dedicated to the presentation of our third contribution termed Secure and Lightweight Biometric-based Remote Patient Authentication Scheme for Home Healthcare Systems. In this chapter, we propose a biometric-based remote patient authentication scheme through which two home healthcare system communication parties could authenticate each other in a public mobile healthcare environments. Through the security analysis, we demonstrate the robustness of this contribution against various malicious cryptographic attacks. Moreover, we develop plenty of intensive simulations to evaluate the performance of this proposal and consolidate the obtained results by comparing it against relevant criteria with concurrent schemes.

Finally, this thesis ends with a general conclusion synthesizing our different contributions, as well as possible research prospects, which we wish accomplish in the near future.

Chapter 1

Health monitoring systems

1.1 Introduction

The needs to observe and control patient's health remotely and in real-time, as well as the technological evolution in the field of microelectronics and wireless communication, have given birth to digital devices, which are wearable with low cost and power. These devices are equipped with a capacity of both computation and perception allowing them to ensure a continuous medical monitoring of the patients. This process can be realized in different places such as in ambulatory, at home, at hospital, or still in an open environment (e.g., monitoring of athlete's health) [61]. In this chapter, we take an interest in the basic concepts of medical monitoring mechanisms, which aim to monitor and measure vital signs inside/outside of a medical context for people suffering from chronic diseases or the elderly. For this purpose, we detail some of the main concepts necessary for understanding these mechanisms, as well as the different monitoring technologies, which are designed specifically for this type of system. Finally, we devote the rest of the chapter to the study of biometric system and security in mobile healthcare environments.

1.2 Medical monitoring for healthcare

1.2.1 Remote diagnostic systems

The remote diagnosis system can be used to remotely diagnose an evocative symptom of the disease or a given issue relating to the patient's health state [112]. As an alternative of the patient being next to a specialist or system which performs the diagnosis, this mechanism allows diagnoses to be established from a distance.

1.2.2 Patient telemonitoring systems

Medical telemonitoring is a branch of telemedicine, which aims to monitor the patient's vital signs at their own homes without visiting a hospital [91]. Subsequently, the physician interprets remotely the collected information, which is of a crucial nature for medical follow-up process [60]. Finally, the physician will make remote decisions regarding the patient care, and eventually delegate some actions to another health professional.

1.2.3 Wireless Body Area Networks

Wireless Body Area Network (WBAN) is one of the wireless medical monitoring mechanisms, which is based on radio frequency [2]. Obviously, the latter aim to interconnect a set of digital equipment, miniaturized placed on or in the immediate vicinity of the human body or possibly implanted in his body. These digital equipments sometimes are called sensors, and sometimes actuators. Sensors when it is a question of making measures, and actuators when acting in an active manner [13][101]. Considering all of the above, these sensors have the ability to interact with a remote service center to alert a detected event.

1.3 Applications of Wireless Body Area Networks

The WBAN consists of intelligent autonomous components, connected together through radio frequency links, capable of measuring parameters in numerous environments and coordinate to perform a specific application function. According to IEEE 802.15.6 standard this new monitoring technology can be divided into two different areas, including medical, and non-medical application [86].

1.3.1 Medical applications

- **Pateint medical monitoring applications:** in the field of medicine, WBANs are used to provide continuous monitoring of the vital signs of people suffering from chronic diseases through sensors, which are placed in or around the subject body in close proximity. The data from the different sensors are transmitted over the Internet to a remote medical team, which will monitor the patient's health status or alert the emergency services if necessary [87].

- **Animal medical monitoring applications:** the control of animal health parameters through WBANs can help to protect them from diseases, which could threaten their life. For example, the deployment of sensors in or around the animal body can help to detect a possible onset of a disease and thus facilitate the control of transmissible diseases before their propagation to avoid financial losses in this area [37][76].

- **Emergency services applications:** like all the above mentioned areas, that of emergency services have not excluded from this race to this technology. If a fire develops, the WBAN attached to the fire fighter suit collaborate with the emergency team to manage this emergency in a very efficient way. The sensors which constitute the WBAN measures environmental parameters such as carbon monoxide, oxygen, methane, air temperature and humidity. There are also those which measure the information about the fire fighter state such as blood oxygen saturation, heart rate, or the pressure in the air cylinder [98].

1.3.2 Non-medical applications

- **Sport applications:** the WBANs are deployed to measure in real-time the physiological parameters of the athletes such as respiratory rhythm, heart rate, distance traveled, locality, acceleration, etc., [111]. This will help in evaluating and improving the performance of athletes.

- **Military applications:** the military operation is one of the main applications of WBANs. In this context, the use of WBANs may be in the monitoring of some vital signs such as blood pressure, oxygen level, ECG, EEG, EMG, respiration, blood pressure, etc., in order to provide information about stress level and effectiveness of a fighter pilot [32]. WBANs can also be used to determine the influence of environmental parameters of military personnel such as intense cold, extreme heat, high altitudes, etc., or simply to monitor the physical training, health state, and performance of such personnel [49].

- **Video game and social network applications:** WBANs also have wide use in the video games and social networks sector. In this context, the avatar [1] is equipped with sensors to monitor the real positions of the players, so that the latter have a view on the contacts in proximity [29].

[1] A character representing the Internet surfer in the virtual world, whether in 2D form, (e.g., on forums and in messaging softwares) or in 3D form (e.g., in video games).

1.4 General architecture of healthcare environments

In health monitoring systems, each patient is equipped with a number of medical sensors, which are mounted on or around his body in close proximity. The main function of these sensors is to monitor body functions and acquire vital signs such as oxygen saturation, glucose level, pulse oximeter, blood pressure, heart rate, blood sugar, etc., [92]. Another type of sensor is added to medical sensors, these are environmental sensors. Unlike medical sensors, environmental sensors can be deployed in interior areas such as a patient's home, for example. These intelligent sensors monitor the environmental conditions like temperature, humidity, brightness, and noise level [91]. Because, these measurements are necessary for healthcare services. As medical and environmental sensors have a short communication range [51], they need to be connected to more powerful equipment to communicate the information collected by different sensors to healthcare providers. Consequently, this information is transmitted to patient personnel assistant (PDA) via wireless communication technologies such as Bluetooth, ZigBee, or WLAN, etc., [94]. The received medical information is analyzed and aggregated by the personal assistant. Finally, the latter transmits this information to the centralized processing center via Internet or by using mobile telephony networks.

As illustrated in figure 1.1, the general communication architecture of a healthcare monitoring system can be divided into three levels [35][86][116]:

- **Tier-1:** Intra-WBAN communication. This level refers to radio exchanges which take place in close proximity to the human body. These exchanges include those between medical sensors, as well as those of medical sensors and personal server (PDA) [94].
- **Tier-2:** Inter-WBAN communication. This level covers communications between the personal server and one or more access points [51][108]. Thus, the personal server transmits the medical information received at the first tier, to the central processing center via the Internet, after having made the necessary treatments.
- **Tier-3:** Beyond-WBAN communication. This level represents the communications between the access point and remote medical team. Tier-3 communications aim to improve the quality of medical monitoring of the patient. This is thanks to the interventions of the health personnel who monitor and have access to this information whenever and wherever.

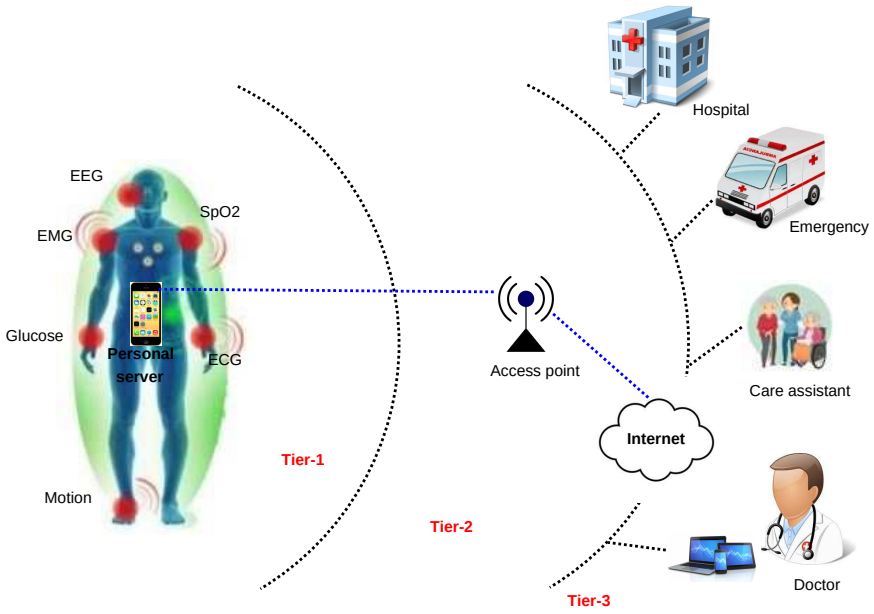


Fig. 1.1 Health monitoring system network architecture [86]

1.5 Design factors of healthcare environments

The design operation of a healthcare monitoring system is constrained by a set of specific requirements, so that an effective and secure communication can be ensured, among them we mention [96][128]:

- **Interference reduction capability:** health monitoring applications, can confront a high rate of errors and more jamming and interference between sensor communications resulting from different WBANs. In this case, the choice of the communication range must be chosen so that the WBAN devices can operate legally worldwide [96]. Furthermore, advanced digital processing techniques must also be applied to reduce the interference impact in the WBANs.

- **Deployment cost:** the cost of establishing a medical monitoring system must be controlled. This cost includes those of medical and environmental sensors, as well as the cost of the installation and maintenance, which are very important for assessing the overall cost of the network. Therefore, the total cost of implementing of this new technology should not exceed the cost of classical networks to justify its interest.

- **Fault tolerance:** failure or blocking of body medical sensors can be caused by several aspects, especially, energy depletion, physical damage, or interferences

related to the environment. Consequently, these problems must be essentially considered when designing a health monitoring system.

- **Limited resources:** in addition to energy, sensors deployed in WBANs also have limited processing, and storage capacity. Consequently, the proposed scheme for this type of system should be lightweight and does not use complex, resource-intensive computing [88][120].
- **Robustness and precision:** the robustness of the security method proposed for a health monitoring system should be studied by creating test cases with small variations in the internal sensor parameters, including radio ranges, initial energy, etc.
- **Reduced detection time:** the detection sensitivity of patient's vital signs through sensors belonging to WBAN must be increased to guarantee a very good monitoring of the monitored subject.
- **Data aggregation:** in order to save energy in the health monitoring systems and improve their lifetime, it is necessary to reduce the transmission of redundant information transmitted by the neighboring sensors using a data aggregation technique.
- **Data security:** the last important issue in a health monitoring system concerns the protection of patients' privacy, as well as the reliability of the transmitted medical data. In the absence of an authentication system, erroneous data could be injected, replicated, or even treated as legitimate. Therefore, the data security in such a system is a very important aspect, so exchanges between the WBAN devices must be secured.

1.6 Security requirements

The integration of security mechanisms into a healthcare monitoring system requires a good knowledge of the security requirements in such a system [86]. The development of an effective and strong security method to ensure the security against various malicious attacks depends on the understanding of the application nature to design [108]. Among the basic security requirements in the healthcare monitoring system, we mention [69]:

- **Confidentiality:** it is the property, which guarantees the protection of patient's data during transmission, as well as during storage against interception and reading by unauthorized persons.
- **Availability:** information required for monitoring and assessing a patient's health status must be accessible at all times, even in the case of denial of service attacks [69].
- **Integrity:** the integrity of patient-related data should be checked and detected to avoid false treatment due to malicious or erroneous changes during transmission and storage periods.
- **Authetication:** medical monitoring systems must not only verify that an entity corresponds to its declared identity, but also verify that the data originates from the advertised source and not from a malicious entity.
- **Accountability:** this property must be increased in each medical monitoring system, and this by facilitating access to patient's data even under data erasure or sensor failure.
- **Non-repudiation:** medical monitoring systems must imperatively prevent an entity from denying the origin, sending or reception of a piece of patient's data.
- **Access control:** access to the patient-related data should be restricted to the authorized users. Consequently, access to these sensitive data must be governed by complex policies to distinguish between each part of the data and each privileged user.
- **Data freshness:** patient's data intercepted by an intruder from previous communication periods should not be replayed to create confusion at the collection point. Consequently, the data freshness must be dynamically verified and guaranteed by the collection node.
- **Revocability:** if a WBAN user executes a suspicious task or behaves in a malicious manner, he/she will be isolated by depriving him to participate in WBAN activities.

1.7 Biometrics and security in healthcare

1.7.1 Definition

Biometrics refers to the mathematical analysis of one or more physical and/or behavioral features automatically measurable, permanent and distinctive. These features can be used to associate with an identity of a person who wants to perform an action, this thanks to the automatic recognition of biometric features relating to that person previously registered [19][24].

1.7.2 Classification

Biometrics is an effective technique more often used for the identification and authentication of an individual using his biometric features. We distinguish four main families of biometric modalities, among which we mention [1][19][31]:

- **Biological modalities:** this type of modality is done using a person's biological analysis like tests on odor, saliva, blood, urine, DeoxyriboNucleic Acid (DNA), etc.
- **Behavioral modalities:** this type of modality is based on the analysis of some behaviours expressed by a person, such as voice, signature dynamics, gait, keystroke dynamics, etc.
- **Morphological modalities:** this type of modality is based on the identification of particular physical features, which are unique and permanent to any person. Among these physical features we mention the tests on facial features, hand geometry, palmar and digital fingerprints, retina, iris, etc.
- **Physiological modalities:** this type of modality is based on the identification of the individual's physiological features like tests on EEG, ECG, EMG, PPG, voice, etc.

1.7.3 Desired properties for a biometric system

A biometric features are a data containing sufficient information to identify and distinguish any two individuals [25]. So that the physiological and/or behavioral biometric features of each individual, can be qualified as biometric modality, they must meet the following criteria [20][30][117]:

- **Universality:** means that each person should possess these biometric features.
- **Uniqueness:** indicates that the biometric features must be unique and representative of a single person.
- **Permanence:** permanence, or stability, means that the biometric features should be constant in a person over the time. In the case where the biometric features are invariant, they must be only for a reasonable period of time.
- **Easy measurability:** represents the facility level during acquisition and digitalization of an individual's biometric data using a relevant device.
- **Performance:** refers the recognition accuracy, execution speed and robustness taking into account the limited biometric system resources to reach the expected accuracy.
- **Acceptability:** acceptance of users to present their biometric data to the system for using them as an identifier.
- **Non-reproducibility:** reflects the impossibility of duplication of an individual's character by an impostor to avoid fraud acts.

1.7.4 Cancellable biometrics

Cancellable biometrics refer to the transformation of raw biometric data before their uses, using well-chosen functions [23][103]. The data resulting from this transformation should be imperatively reliable and respects the private life of the person [18]. A good cancellable biometric system must essentially ensure the following properties [75]:

- **Non-inversibility:** this property means that the chosen function to transform the raw biometric data must be one-way. In other words, from the transformed biometric data the intruder must not be able to deduce the original biometric data.
- **Revocation:** this property reflects the facility of the revocation process of the biometric data during their compromising.
- **Diversity:** means the ability to use a single raw biometric data to generate different transformed biometric data for different type of applications.
- **Performance:** refers mainly to the efficiency of the recognition system, which should not be deteriorated due to biometric data transformation process.

Considering all of the above proprieties, the combination of biometrics and cryptography in healthcare systems seems to be a good mechanism to ensure the security of transactions between the communication parties of this type of system. Indeed, this technique consists in replacing the conventional authentication of an individual by another technique by means of its morphology or behavior. The biometric features of the individual can be used not only in the generation of symmetric encryption keys, but also in the authentication of the communication parties in mobile healthcare environments.

1.8 Conclusion

Health monitoring systems are a new technology, which has emerged after the great technological advances in the fields of microelectronics and wireless communication technologies. However, these systems bring a very large number of challenges, particularly those related to security. In this chapter, we have presented the medical monitoring systems in general, and their basic concepts in particular, which are necessary for the understanding of healthcare environments. Thus, we have described the general architecture of this type of system. Afterwards, we have represented the constraints and the main security requirements in patients' medical monitoring applications. Finally, we have enumerated the main security requirements in the healthcare environment using biometric systems, which have become very popular in the development of security schemes.

In the next chapter, we present the state of the art regarding the authentication in mobile healthcare environments.

Chapter 2

Authentication schemes in healthcare environments: a state of the art

2.1 Introduction

The real-time medical monitoring and transmission of the collected data provide quickly the necessary information to remote physicians to ensure that the patient is in the planned health measures or to ensure only that he/she is responding to a given treatment. However, this process may expose the collected data pertaining to the patient's health status to malicious intruders or eavesdroppers. The most serious threats are generally related to the possible disclosure of confidential information. All patient information, which is legally confidential must be properly managed to ensure its privacy. Therefore, it is essential to ensure the security of this information during transmission, as well as during storage. To achieve this goal, several schemes have been proposed, such as secure remote patient authentication schemes for healthcare environments. In this chapter, we focus on the presentation and critical study of the main recently proposed schemes to assure the authentication service for medical monitoring architectures. For this purpose, we determine our evaluation criteria, followed by a biometric authentication taxonomy, which classifies the reviewed schemes. Afterwards, we present the critical study of the reviewed schemes. Finally, we conclude this chapter by presenting a synthesis and comparison.

2.2 Evaluation criteria

Issues related to the security and confidentiality of patient's data are essential requirements for any communication environment. These issues, which have been widely studied in several communication environments, are not an exception for mobile healthcare systems. Therefore, in order to understand the diversity of the reviewed authentication schemes, we propose an evaluation of these schemes based on the following criteria:

- **Security:** as the patient-related data exchanged in the healthcare systems are very sensitive, these systems must be secured against malicious attacks, which might threaten the patient's privacy. This characteristic is essential to ensure the proper conduct of medical diagnosis and treatment processes. Indeed, failure to obtain correct medical data will put the patient's life in danger.
- **Communication cost:** this criterion represents the amount of transmitted data traffic between two or more communication parties. Thus, the communication load depends on the capacity of the transmission channel and the total data size transported over this channel.
- **Processing time:** the processing time represents the required time involved in the execution of a protocol during the authentication process. An authentication scheme is considered to be more efficient by ensuring less complicated computations to avoid causing slowness in its execution, especially, when it is an unexpected incident that will underwent on the patient's health.
- **Storage cost:** storage capacity represents the memory space required for the system parameters, which are required to be stored. Therefore, it is necessary to limit the number and size of cryptographic parameters to be stored.
- **Biometrics extraction:** this analysis criterion is specific to authentication schemes with biometric inputs. The key pair of the communication parties can be calculated based on biometric features. The decision to authenticate, or reject a communication party in a healthcare environments depends on its biometric template. Thereby, the accuracy of biometric features play a very important role as it attempts to minimize False Rejection Rate (FRR) and False Acceptance Rate (FAR).

2.3 Classification of the reviewed schemes

We illustrate in Figure 2.1 our taxonomy of the most relevant and recent biometric-based authentication schemes in healthcare environments. We have classified the reviewed schemes into two main categories depending on the orientation of the authentication service and the considered network architecture. Thus, these two main categories can be defined as follows:

1. **Mobile device based architectures:** in this category, the types of transported data in the home healthcare system is very sensitive. Indeed, these systems provide real-time medical monitoring of several patient types, while preserving their autonomy and comfort everywhere and anywhere. To do this, the two home healthcare communication parties (patient's mobile device and hospital server) have to authenticate each other in such open network environment to ensure the security of this type of data. This category is divided into two principal sub-categories, namely: authentication scheme based on ECC (Elliptic Curve Cryptography), and authentication scheme based on hash functions.

2. **Medical Body Area Sensor Network based architectures:** in this category, the biometric authentication issue between the sensors of the same MBASN (Medical Body Area Sensor Network) is approached in two different ways. Depending on the type of biometric authentication provided, we organize this category in authentication without key generation using biometric features, and authentication with key management whether it is generated or not from biometric features, while authenticating between sensors.

   (a) **Without key management:** in this subcategory, the biometric authentication service is provided without taking into consideration the generation and exchange of keys between sensors of MBASN. This sub-category is based on biometric features to check whether the sensors belong to the same MBASN or not.

   (b) **With key management:** in this subcategory, certain authentication schemes generate a secret key in an authenticated manner between the sensors of the same MBASN using the biometric features, while other schemes rely on these features to solely facilitate the key exchange.

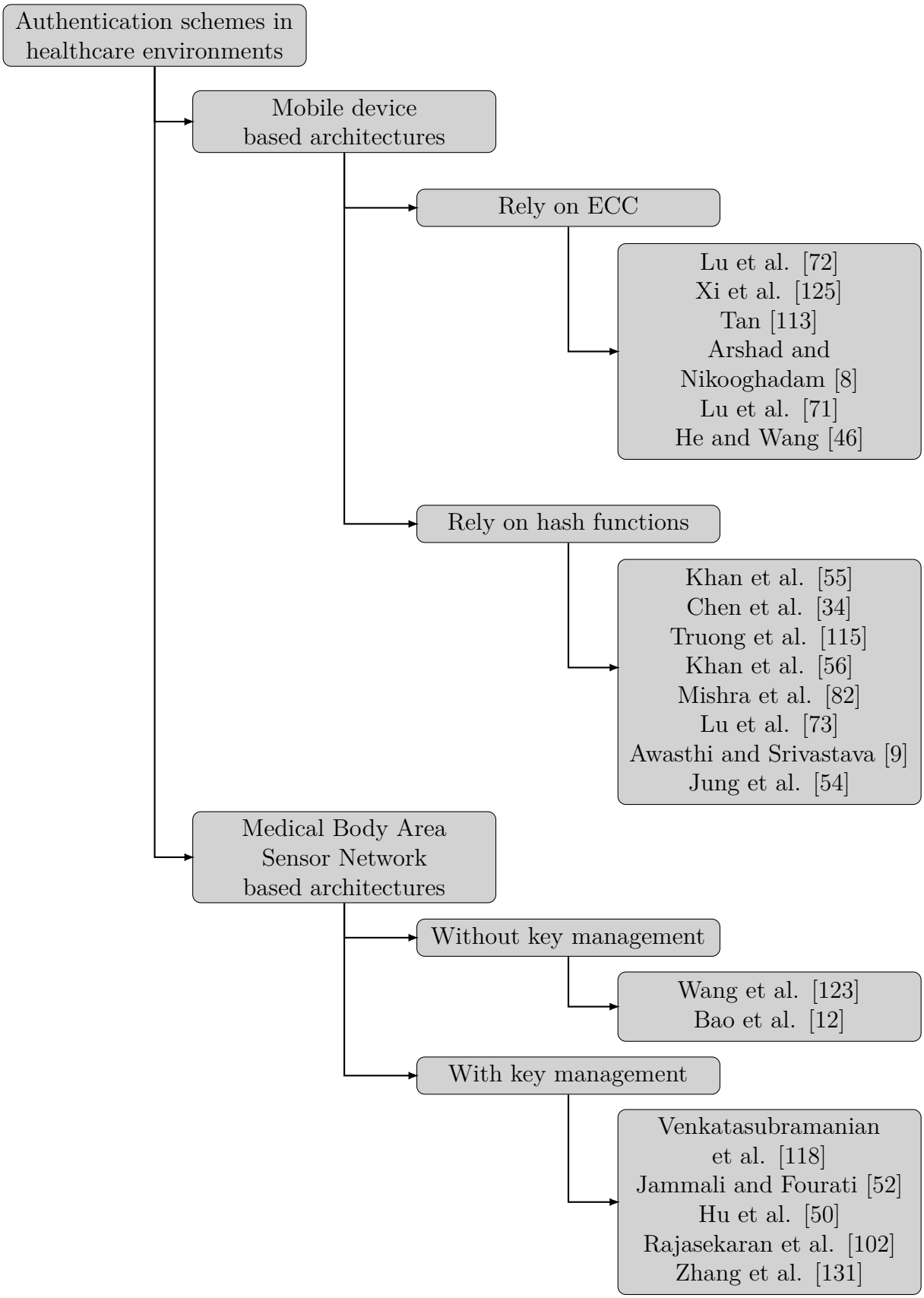


Fig. 2.1 Taxonomy of authentication schemes in healthcare environments

2.4 Critical study

Several research has been carried out to address the security issue of patient's data, which are of a major importance in the healthcare environments. In this context, this research was crowned by the suggestion of numerous biometric-based remote user authentication schemes to overcome the aforementioned pitfall. In what follows, we review from the literature some relevant and recent schemes.

2.4.1 Mobile device based architectures

This first category is subdivided into two subcategories, namely authentication schemes, which rely on hash functions, and those which rely on ECC.

2.4.1.1 Rely on hash functions

Chaotic Hash-based Fingerprint Biometric Remote User Authentication Scheme on Mobile Devices

Overview: In [55], Khan et al. have proposed a chaotic hash-based biometric remote user authentication scheme using mobile devices (e.g., cell phones, personal digital assistants, smartphones, etc.) in order to access his resources remotely with an authentic and secure manner. Khan et al.'s scheme is a two-factor authentication scheme, using passwords, and fingerprints. This means that during the authentication process the user have to use both something he knows, like password and something he is, like biometric template. Contrary to modular exponentiation-based authentication schemes, Khan et al.'s scheme is entirely focused on the one-way collision free chaotic hash functions.

The main objective of this proposal lies in the fact that it allows commercial companies to provide for the mobile users the ability to remotely access to their resources such as e-banking, e-commerce, e-health, etc., in full security. Once a user needs to access a commercial company service, he firstly must execute the authentication system using his own mobile device to access the desired service. Khan et al.'s scheme is divided into four phases namely: registration, login, authentication, and password change. The registration phase of user U_i consists of selecting some personal secret information (e.g., ID, password, etc.) and submitting them to the registration center. The second and third phases are executed when a user U_i wants to authenticate himself and pretends to be the user U_i. The last phase, whenever the user U_i wants to change or update his old password PW_i to the new one.

Advantages and drawbacks: the main advantage of Khan et al.'s scheme lies in the fact that it never keeps password tables and the biometric template on the remote server. However, it has been proved by Chen et al. [34] that this scheme is vulnerable to the impersonation attack by using information leaked from the mobile device.

Mobile Device Integration of a Fingerprint Biometric Remote Authentication Scheme

Overview: In [34], Chen et al. have demonstrated that the scheme [55] is vulnerable to the impersonation attack by using information leaked from the mobile device. Besides, the intruder can analyze this information and forge, form it secret parameters. In remedy of these drawbacks, Chen et al. have proposed an improved scheme, which is a combination of a fingerprint biometric and passwords. In order to improve the security of Khan et al.'s scheme [55], they have used hash functions instead of the chaotic functions. The authors have claimed that their scheme is more secure and efficient while providing a low computation requirement.

Advantages and drawbacks: in the improved scheme, contrary to the original version of Khan et al. [55], Chen et al.'s scheme uses only the simple hash functions instead of the chaotic ones in order to implement a secure and efficient authentication scheme with a low computational cost. However, the improved scheme does not significantly reduce the storage, computation, and communication costs. Chen et al.'s scheme does not overcome the existing security issues in the original version.

Robust Mobile Device Integration of a Fingerprint Biometric Remote Authentication Scheme

Overview: In [115], Truong et al. have demonstrated that the scheme [34] fails to replay attack, server and user spoofing attacks and lacks the user's anonymity, and they have proposed enhancements. The latter is due to the mitigation and isolation of theft risk of the user's identity, which could be used by an intruder to re-register him to the service provider. This is done so that the intruder could obtain a secret key to impersonate either the legitimate user or the server. The improved scheme differs from the two previous versions in the integration of a random value during the registration phase of each user to avoid registering with the same secret key for all users. The authors have claimed that their scheme provides greater security and is practical for wireless communication systems.

Advantages and drawbacks: the main benefit of Truong et al.'s scheme is that is more secure than the two original versions, as it retains the advantages of the

previous ones, while trying to eradicate the loopholes of the previous versions. On top of that, although the improved scheme meets the primary security requirements for communications in the wireless environments, the security level of this scheme depends directly on cryptographic properties of the hash function employed. However, the security level of the latter is no longer guaranteed due to its exposure to collision attacks.

More Efficient Key-Hash based Fingerprint Remote Authentication Scheme using Mobile Device

Overview: In [56], Khan et al. have shown that the scheme [115] is vulnerable to other attacks, such as password guessing, user and server impersonation attacks by using the information extracted from the user's mobile device and the intercepted login request. They have proposed an improved scheme, which overcomes not only the attacks, but also inherits the original merits of the two previous schemes [34][55]. The only difference between the improved scheme and that of Chen et al. and Truong et al. lies solely in the technical details of the four phases constituting this improved scheme.

Advantages and drawbacks: the main merits of this improved scheme is successfully eradicates the deficiencies of the two initial schemes and resists to various malicious attacks. However, the improved scheme presents some performance limits regarding the storage, computation and communication overhead. Another disadvantage associated to Khan et al.'s scheme [56], is that it does not respond to revocation condition due to the non-transformation of the raw biometric template, using a chosen function, so that the resulting template will be revocable and respect user's privacy. On top of that, the solution is unable to achieve user's anonymity and still vulnerable to user impersonation, and desynchronization attacks [124].

A Secure User Anonymity-Preserving Biometric-based Multi-Server Authenticated Key Agreement Scheme using Smart Cards

Overview: In [82], Mishra et al. have proposed a biometric-based authenticated key agreement scheme using smart cards. The solution is an improvement of the Chuang and Chen's scheme [38], which has been elaborated the expert systems for network management to achieve the user's anonymity in the multi-server environments. The main concern of Mishra et al. in their scheme is to get rid of security pitfalls found in the basic scheme, while maintaining both the anonymity and low computation overhead of the latter.

Advantages and drawbacks: Mishra et al. have claimed that their improved scheme eradicates the loopholes originate from the basic scheme. In addition, their improved scheme uses only light arithmetic operations such as one-way hash functions, which makes this solution effective in terms of computational cost. However, later, Wang et al. [121] have stated that the scheme [82], is susceptible to some malicious attacks, such as replay, user and server masquerade, denial of service attacks, and does not provide both user's anonymity and perfect forward secrecy.

Robust Biometrics based Authentication and Key Agreement Scheme for Multi-Server Environments using Smart Cards

Overview: In [73], Lu et al. have introduced a more secure three-factor authentication scheme for enabling to conquer the drawbacks of the scheme [82]. This solution is an extension of Mishra et al.'s scheme in order to improve and strengthen the security aspect of the latter. Indeed, there are also three parties involved in this improved scheme: the user U_i, the server S_j, and the registration center RC. The latter shares its secret key PSK and a secret number x with the server S_j through secure channels to use them for securing the exchanged messages relating to phases which constitute the improved scheme. On the whole, this solution focuses mainly on the security weaknesses of the original version while addressing the issue of password change phase.

Advantages and drawbacks: the proposed solution is interesting in the sense that it provides convenient network services for the distributed systems. Besides, Lu et al.'s scheme [73] offers better performance results in terms of computation cost compared to the original version. However, Reddy et al. [104], have pointed out that Lu et al.'s scheme suffers from some malicious attacks including, clock synchronization problem, man-in-the-middle attack, impersonation attack, attack against anonymity, and it does not provide perfect forward secrecy.

A Biometric Authentication Scheme for Telecare Medicine Information Systems with Nonce

Overview: Telecare medicine information systems, which provide home healthcare services for patients, suffer from some security issues. Among them, privacy and confidentiality of patient's information are the most important either for patients or physicians, especially, during transmission and storage process. To address these subjected flaws, several security schemes have been suggested, but none of them are neither effective nor user-friendly. In [9], Awasthi and Srivastava have proposed a biometric based remote patient authentication scheme for this system type using

nonce. Indeed, initially, each user registers himself at the registration center by interactively sending some information about his identity including his biometric template. However, the feature extraction process is not applied on the biometric template. Upon receiving the registration request message sent out from the user U_i, the registration system performs some operations on the received parameters in order to complete this registration phase. Subsequently, the user U_i who wants to login to the remote system, introduce his identity, password and biometric template in his mobile device. If the user U_i is successfully verified by its biometric template, the mobile device will perform some operations to complete the mutual authentication process between the mobile device and remote server.

Advantages and drawbacks: Awasthi and Srivastava's scheme present's a low computational overhead due to the use of light operation functions during the authentication process and key agreement. However, the main drawback of this scheme is that the user's identity and its biometric template are stored in plaintext in the user's mobile device. If an intruder acquires the lost or stolen the user's mobile device, he/she can guess the user's password in an online manner [82]. On top of that, this scheme does not resist against the reflection attacks, does not achieve three-factor security, and is incapable to protect the user's anonymity [113].

An Improved and Secure Anonymous Biometric-Based user Authentication with Key Agreement Scheme for the Integrated EPR Information System

Overview: In [54], Jung et al. have proposed an anonymous user authentication scheme with a session key agreement for the integrated EPRs (Electronic Patient Records) information system. This solution is an extended of three-factor user authentication scheme, which has been proposed to remedy the flaws of Li et al.'s scheme [68] in order to protect the user information.

Advantages and drawbacks: the extended authentication scheme proposed by Jung et al. is very unavoidable to secure electronic transactions in the healthcare systems. However, the solution is vulnerable to denial of service and impersonation attacks, and fails to preserve the user's anonymity.

2.4.1.2 Rely on ECC (Elliptic Curve Cryptography)

A Secure and Efficient Mutual Authentication Scheme for Session Initiation Protocol

Overview: In [72], Lu et al. have proposed an improved scheme to solve issues encountered in Zhang et al.'s scheme [130]. Their scheme is another three-factor authentication scheme for the Session Initiation Protocol (SIP), which is largely needed in the multimedia services. Lu et al.'s scheme is performed when a user needs to access the SIP services such as creating, maintaining, and terminating sessions, including phone calls and multimedia conferences via the Internet [109]. So, Lu et al. have proposed an improved ECC based authentication scheme for the client/server protocol (SIP) to ensure the optimal security of multimedia services.

Advantages and drawbacks: compared to the original version, this one is more efficient, where the improved scheme uses biometric features to work with elliptic curve cryptography which is more appropriate for low-resource devices. However, Kumari et al. [62] have shown that Lu et al.'s scheme [72] cannot withstand the impersonation attack, it does not provide the user's anonymity, and still failed to achieve mutual authentication between the communicating parties.

A Fingerprint based Bio-cryptographic Security Protocol Designed for Client/Server Authentication in Mobile Computing Environment

Overview: In [125], Xi et al. have proposed a scheme to provide a local protection of users related sensitive information and mutual authentication between these users over an insecure network. Xi et al.'s scheme combines the advantages of two security techniques, namely conventional cryptography and biometric security for a more efficient solution, which overcomes the disadvantages of both of them. Xi et al.'s scheme is divided as usual in biometrics, in two phases, namely: registration, and authentication. In the first phase, a new user is required to present at the server side to provide it with some personal information and also present his biometric template, which will be used not only for biometric verification but also for bio-cryptographic key generation. As the raw biometric data is a commonly non-revocable as is the case with a password. So, this data is transformed and hidden using the fuzzy vault technique such that the genuine minutiae of biometric data be scrambled by a number of chaff points greater than 200. Finally, the second phase is executed so that both the client and server authenticate each other and then initiate the step of generating the shared secret key. In order to accomplish this phase, the two communication parties exchange few

requests, which are encrypted by the key pair of each delivered part by the certificate authority.

Advantages and drawbacks: Xi et al.'s scheme is based on a public key infrastructure (PKI), where the key pair generation center facilitates to the client and server not only to authenticate each other, but also to agree on a symmetric bio-cryptographic key. It ensures the security of the data during processing because it does not store raw biometric templates. In addition, it provides security against some malicious attacks, including brute force and replay attacks, and ensures a reduced False Acceptation Rate. One of the main weaknesses of this scheme is that it has a certain performance limits regarding the computation and communication overhead. Moreover, it suffers from a high False Rejection Rate and is also vulnerable to mobile device lost attack, which stores in plaintext almost all the information necessary for the authentication process.

A User Anonymity Preserving Three-Factor Authentication Scheme for Telecare Medicine Information Systems

Overview: In [113], Tan has proposed a new three factor authentication scheme based on ECC for telecare medicine information systems. This scheme is an improvement of Awasthi and Srivastava's scheme version. The author aims to improve both the security and efficiency of the original version to protect patient transactions benefiting from medical monitoring in his own home when he access health services on supposedly unsecure networks.

Advantages and drawbacks: Tan has claimed that the performance of its scheme is better than the previous ones in both efficiency and security. However, Tan's scheme is not secure against denial-of-service and replay attacks [8]. Moreover, the freshness of the sent login message from the patient to the server is not verified by the server.

Three-factor Anonymous Authentication and Key Agreement Scheme for Telecare Medicine Information Systems

Overview: In [8], Arshad and Nikooghadam have proposed a three-factor authenticated key exchange scheme to remedy the weaknesses of Tan's scheme [113] and to provide various security aspects. The authors have proved that the original version does not use techniques to verify the freshness of the exchanged data to ensure the integrity and confidentiality of this sensitive data. For that reason, in this improved scheme the authors integrate a timestamp and two fresh random numbers to guarantee this property. As well, to prevent intruders from intercepting the login and authentication messages and replay them later to create confusion at the collection point. Besides,

in order to compare two biometric inputs to determine the differences between them, Arshad and Nikooghadam use a symmetric parametric function instead of a hash function like it has done in the original version.

Advantages and drawbacks: the authors have claimed that their scheme not only withstands various attacks, but also is more efficient than Tan's scheme and is more suitable for telecare medicine information systems. However, Arshad and Nikooghadam's scheme still fails to protect against the impersonation and on-line password guessing attacks [71].

An Enhanced Biometric-Based Authentication Scheme for Telecare Medicine Information Systems using Elliptic Curve Cryptosystem

Overview: In [71], Lu et al. have proposed an enhancement based on Arshad and Nikooghadam's scheme. Lu et al.'s technique employs lower computational operations such as ECC and hash function as the primitives to improve the security and efficiency of Arshad and Nikooghadam's scheme. Furthermore, they adopt BAN logic [28] to demonstrate the completeness of the enhanced scheme.

Advantages and drawbacks: the main merit of Lu et al.'s scheme is its reliance on ECC, which is very appropriate for devices, which suffers from various resource constraints such as energy, memory space, computing capacity, etc. In addition, ECC offers the same level of security with a reduced key storage space and faster arithmetic operations. Consequently, Lu et al.'s scheme provides sufficient security against cryptographic attacks. However, their scheme relies on complex cryptographic algorithms, resulting in computation, communication, and storage loads, which are still important.

Robust Biometrics-based Authentication Scheme for Multiserver Environment

Overview: In [46], He and Wang have proposed an authentication scheme based on biometric data for multiserver environment using ECC in order to provide convenient and efficient network services. Likewise, they have proposed this solution to particularly overcome the shortcomings of the conventional schemes designed for client/server authentication, which are not appropriate for multiserver environment. This is due to the difficulties of remembering the access passwords related to each service provider. Despite the many efforts made by some authors to solve this problem, security flaws still persist in their proposed schemes. To address these security issues, He and Wang have concentrated mainly on both Yoon and Yoo's [126] scheme and Kim et al.'s scheme [57],

to inherit their benefits and mend the security loopholes found in them. Unlike the two original versions, the authors have tried to improve the security of their authentication scheme by using fuzzy extractor technique to avoid the storage of the user's biometric data and limit the risk of stealing them.

Advantages and drawbacks: the main advantage of He and Wang's scheme is that is able to revoke the secret data, whether this one was compromised, without the biometric data being compromised. Although this solution is the first truly three-factor authenticated scheme, the integration of the registration center provides high computation requirements [105]. Additionally, Odelu et al. [93] have pointed out that He and Wang's scheme [46] suffers from some security weaknesses, including user's anonymity, impersonation, and known session-specific temporary information attacks.

2.4.2 Medical Body Area Sensor Network based architectures

This second category, as for it, decomposes the MBASN-based architecutres according to authentication scheme with or without the session key computation.

2.4.2.1 Authentication without key management

A Stochastic Biometric Authentication Scheme Using Uniformed GMM in Wireless Body Area Sensor Networks

Overview: In [123], Wang et al. have proposed an authentication system based on uniform Gaussian Mixing Model (GMM) to secure the inter-communications among sensors in the MBASN to resolve the key exchange challenges. Indeed, Wang et al.'s scheme use the heartbeat timing information (IPI signals) [99] of the sender as a biometric key for the authentication process. As well, to check if the medical data comes from the sensor attached to the same MBASN, the sender IPI signals are also used to generate a signature using uniformed EM algorithm [106]. The sender extracts the statistical characteristics and the log-likelihood from the biometric authentication information (IPI and medical data) to be attached to the medical data as a signature. The latter will be attached to the request sent out from the sender to authenticate him near the receiver sensor. As well, this signature will serves to ensure the integrity of both the IPI signals and the patient's data.

The receiver sensor follows the same uniformed EM algorithm and uses the received medical data and its own IPI' signals to obtain its own likelihood. Afterwards, the transmitter checks whether its IPI' signals and the received one have a strong resemblance. If it is true and the difference between the sender and the receiver

log-likelihoods, is fewer than the predetermined threshold. Thus, the receiver sensor authenticates the transmitter and considers that the received medical data is valid.

Advantages and drawbacks: the proposed scheme is based essentially on physiological signals to ensure two important services for a security system. The first is the authentication between sensors belonging to the same MBASN, and the second is the integrity of the critical patient's data. In addition, Wang et al.'s scheme generates a lower False Rejection Rate. That is because it considers that the IPI signals measured on the same subject may not be totally identical. Another merit of this scheme is that it solves the challenges of synchronization time through the signing process based upon statistical. The major disadvantage of this scheme is the computation cost which is high. Because the use of IPI signals to generate a signature engender additional costs.

Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems

Overview: In [12], Bao et al. have proposed an authentication scheme between two sensors belonging to the same MBASN using the physiological signal features PPG. The authentication phase of this scheme takes place in two sessions: the first is used to authenticate the prover sensor near the verifier sensor and the second session as for it is used to authenticate the verifier sensor near the prover one. So that the two sensors can be authenticated using signal physiological, the two sensors are synchronized in order to measure the same signal physiological at the same time. The different processes and exchanges between the two sensors are described as follows: initially the server (prover sensor) wanting to communicate with the client (verifier sensor), sends a message composed of its encrypted physiological signal features I_0 and a random number R_s generated using the Bao et al.'s scheme [10]. The client (verifier sensor) decrypts the features received using the schemes presented in [10][11]. Subsequently, it computes the hamming distance between its own features and that already received in order to compare the physiological signal features to deduce whether the two sensors are of the same MBASN or not. If the hamming distance is unacceptable regarding a predetermined threshold, then the authentication process fails, otherwise the server is authenticated. During the second session, the server becomes a verifier, and the client becomes a prover, and the same procedure will be followed so that the client will authenticate near the server during the second session using the same physiological signal features.

Advantages and drawbacks: the disadvantage that we can cite for the Boa et al.'s scheme is that it involves two independent schemes during the phases of encryp-

tion/decryption and the generation of random number, which gives an increasingly higher complexity by generating additional computation costs and energy consumption. In addition, the security against the attack of the man in the middle is no longer guaranteed in this scheme. Because there is a possibility that an attacker intercepts the message $(Rs, E(I_0))$ sent by the server and send it back to him directly to authenticate with him.

2.4.2.2 Authentication with key management

Usable and Secure Key Agreement Scheme for Body Area Networks

Overview: In [118], Venkatasubramanian et al. have proposed a scheme termed PSKA (Physiological Signal-based Key Agreement), allowing two sensors belonging to the same MBASN to exchange a symmetric encryption key while authenticating each other based on the physiological signal. The basic principle of PSKA is that these two sensors measure the physiological signal at the same instant and each of them extract a feature vector obtained from that signal. These two sensors which belong to the same subject exchange some messages to compute their shared symmetric secret. So, the transmitter sensor constructs a secret polynomial $p(x)$ using the randomly generated coefficients. After the concatenation of the latter, the transmitter sensor forms the symmetric key. The constructed polynomial is used with the feature vector of the transmitter sensor to form the set of the genuine points. These points are added to random points called chaff points in order to get the fuzzy vault. Before the fuzzy vault be transmitted to the receiver sensor, it must be first scrambled by changing the points positions which forming it. This, is necessary to ensure that both the random and genuine points are indistinguishable. In the receiver side: at the reception of the fuzzy vault, the receiver sensor performs the reverse process to unlock the vault by using its local version of physiological signal features. Thus, the receiver sensor eliminates the random points to reconstruct the polynomial $p(x)$ by using the Lagrangian interpolation. Finally, the receiver sensor reconstructs the symmetric key already computed by the transmitter sensor.

Advantages and drawbacks: this scheme ensures the authentication service while ensuring that only sensors belonging to the same MBASN can share a random symmetric key to avoid the brute force attack. Subsequently, this shared secret is used to provide other security services such as privacy and data integrity during the transmission process. The use of the fuzzy vault technique ensure that the sensors of the same MBASN which do not obtain the identical biometric features can generate and exchange

a symmetric key. These two important processes are carried out while guaranteeing a lower FRR. Besides, the security of Venkatasubramanian et al.'s scheme depends on the fuzzy vault size. Because every time the fuzzy vault size is large, the adversary finds difficulties to recover the genuine points in the intercepted fuzzy vault. The drawback of this scheme is the storage and computation costs, which are increasingly higher, especially, during the reconstruction of the polynomial departure $p(x)$, which results in high energy consumption.

A Physiological Feature based Key Agreement for Wireless Body Area Network

Overview: In [52], Jammali and Fourati have proposed a key agreement scheme based on biometric features termed PFKA (A Physiological Feature based Key Agreement for wireless body area network). The aim of this scheme is to ensure the generation and exchange of a symmetric cryptographic key between the sensors belonging to the same MBASN. This symmetric cryptographic key is generated using the physiological signal features extracted from the ECG signal of the same subject. The key agreement scheme proposed by Jammali and Fourati is summarized as follows. Both the sender and receiver sensors collect ECG physiological signals from the same subject at the same instant. Afterwards, each of them extract separately its feature vectors from the physiological signal using either the Enhanced FFT [44] or IPI Method [99].

After the step of physiological feature extraction, the sender sensor generates a vector of random numbers. Afterwards, it divides the latter into two parts, the right and the left one. The feature vector is also divided in the same way in two parts, at the end of this step the feature vector is modified using the vector of random numbers. Finally, before the obtained vector be sent to the receiver sensor, the sender sensor encodes the obtained vector with a Reed-Solomon coding [21]. Upon receiving the message sent from the sender sensor, the receiver decodes the encoded vector to have the modified vector. Afterwards, it tries to find the vector of the random numbers using its own feature vector by following the inverse process of features vector modification. Finally, each sensor calculates separately its shared secret symmetric key.

Advantages and drawbacks: the main advantage of PFKA lies in the use of the ECG physiological features to authenticate two sensors belonging to the same human body. Indeed, an attacker can not find the vector of random numbers, without having in his possession the correct physiological features. This, implies the impossibility of deducting the shared secret symmetric key. The greatest drawback of this scheme is that the two feature vectors resulting from the same subject, cannot always be identical

to one hundred percent. Consequently, the two feature vectors may be practicable for the authentication process, but not for the symmetric key computation, especially when there is not a predetermined threshold for the biometric verification.

Secure and Efficient Ordered-Physiological-Feature-based Key Agreement for Wireless Body Area Networks

Overview: In [50], Hu et al. have proposed a biometric based security system termed OPFKA (Ordered-Physiological-Feature-based Key Agreement for wireless body area networks). The biometric features are extracted from the physiological ECG signal measured by two sensors belonging to the same MBASN after they have been synchronized. In order to generate the shared symmetric key, these two sensors follow a certain strategy to order the two biometric feature sets collected on both sides. This, is necessary to have an order that only these two sensors know.

Once the two sensors computed their biometric feature vectors, the sender sensor uses a larger set of random chaff points to scramble its biometric feature vector. Thereafter, it uses a random permutation function to mix the genuine points and the random chaff points. The purpose of that is to avoid all attempts, which can be used to separate the genuine and random chaff points. Finally, the resulting fuzzy vault and some parameters are sent to the receiver sensor. Upon receiving the request, the receiver sensor uses its biometric feature vector to identify the biometric features in common with the fuzzy vault calculated by the sender. At the end of this step, the receiver sensor, calculates the shared secret key based on the biometric features in common. So that the sender sensor calculates the same key, the receiver sensor sends him the index set of the biometric features, which are retained and some parameters. Finally, an acknowledgment message is sent out from the sender to the receiver to complete the shared key establishment process and also confirm the success of this process.

Advantages and drawbacks: the use of the fuzzy vault technique allows to reduce the theft risk of biometric features. Consequently, it improves the security of the biometric authentication process between the sensors belonging to the same MBASN. As well, the use of this technique allows the generation of a shared secret even if the two feature vectors are not completely identical. However, we have detected a fault in the key establishment process such as the unencrypted sending of fuzzy vault and the index set, can make the biometric features compromised. An intruder who intercepts these two parameters can easily deduce the symmetric key, which allow him to impersonate the

two communicating sensors. Consequently, the intruder bypasses the authentication system.

An Efficient and Secure Key Agreement Scheme Using Physiological Signals in Body Area Network

Overview: In [102], Rajasekaran et al. have proposed a biometric based security system, enabling secure inter sensor communication. Indeed, this scheme allows the sensors belonging to the same MBASN to agree on a symmetric cryptographic key in an authentic manner. The sensors concerned, namely the sender and the receiver sensors measure from the same subject the physiological signal at the same instant. Subsequently, the sender sensor selects $N+1$ data of specific dimensions from its feature vector extracted from the physiological signal as x-coordinates. In addition, it also chooses random numbers after Cyclic Redundancy Check (CRC) [100] coding as y-coordinates. These two coordinates (x, y) are used to form the set R, which is transformed in its turn into a cubic spline curve [58], which is defined in pieces using a set of cubic polynomials. The coefficients of these polynomials are concatenated to form the symmetric cryptographic key. Before the set R be sent to the receiver sensor, the sender sensor must firstly shuffle the information coming from R using the fuzzy vault technique. Upon receiving the request, the receiver sensor selects in the received fuzzy vault the set of points of the form (i, j), where i is close to a x-coordinate value of the biometric feature vector. After the step of Y-coordinates CRC Error Detection, the receiver sensor reconstructs the cubic polynomials of the spline. Finally, the receiver sensor finds the symmetric cryptographic key.

Advantages and drawbacks: this scheme is based on a simple principle, which takes into account the problems relating to the physiological features collection on the same subject to agree on a symmetric key. The combination between the fuzzy vault technique and the cubic spline interpolation [58] reduced the computation complexity related to the polynomial interpolation. As well, this combination not only allow to obtain the desired results, but also it kept a lower FRR and FAR. However, Rajasekaran et al.'s scheme generates a large size of the fuzzy vault set, which can cause high communication, and computation costs.

ECG-Cryptography and Authentication in Body Area Networks

Overview: In [131], Zhang et al. have proposed an improved scheme termed ECG-IJS (ElectroCardioGram-Improved Jules Sudan) for key agreement between sensors belonging to the same MBASN, using the overlapping physiological signal features.

To do this, both sensors belonging to the same MBASN have the same ability to measure the ECG signal at the same time and also use the same method for extracting biometric features. Thus, each sensor, namely sender and receiver, extracts its feature vector. Subsequently, the sender uses its vector to generate the symmetric key, then it also uses the same feature vector to construct a unique ECG monic polynomial of degree s. At the end of this step, the sender sensor calculates the coefficients of the ECG monic polynomial already constructed. Then it sends to the receiver sensor the ECG vault coefficients from the degree (s-1) to (s-t), where t represents the coefficient number. Upon receiving, the receiver sensor uses the coefficients, which he has received from the sender to construct a new ECG feature polynomial of degree s. Afterwards, it evaluates the latter on all points in its feature vector to get a set of pairs. After this, it search for a polynomial with degree (s-t-1) to meet most of the pairs using the Reed-Solomon decoding [110] process. Finally, the secret cryptographic key is reconstructed by computing the roots of the polynomial p.

Advantages and drawbacks: the main advantage of Zhang et al.'s scheme is that it requires more moderate use of memory space and a reduced communication cost. The reason for that it does not resort to store only the coefficients of the generated polynomial, and only one subset of coefficients must be forwarded to the receiver sensor. Another merit of this scheme is that it does not use chaff points to hide the symmetric key, which reduces the computational cost. However, Zhang et al.'s scheme is vulnerable to polynomial attack, which can easily recognize Reed-Solomon decoding [110].

2.5 Overall discussion

The security and privacy of patient-related data in healthcare environments during their transmission, as well as during their storage is a very attractive research area. Numerous biometric-based schemes have been proposed in the literature to ensure the authentication process either between sensors or between mobile device and remote server. On top of that, some of them allow to agree on a symmetric bio-cryptographic key, which is generated from the biometric features of the subject. The shared secret symmetric key calculated from the same biometric features at different parts of the same subject will be used not only to encrypt the messages exchanged between the two communication parties, but also to authenticate each other. Each scheme has strengths in some aspects either in security or performance, but also some gaps. In healthcare environments, biometric-based key agreement schemes must transform the

raw biometric data employed in the authentication process, using a chosen function such as, fuzzy vault, fuzzy commitment, shielding functions, etc., so that the resulting data will be revocable and respect patient's privacy. Because, the direct use of the inputted biometric of the same subject can cause some issues during the authentication process and even during the generation of the shared secret key. This prevents the two sensors belonging to the same MBASN from having the same symmetric bio-cryptographic key due to variability differences each time between the two biometric templates of the same subject. In the reviewed schemes [12][50][52][102][118][123][125][131], the transformation of the raw biometric data has been taken into account. Contrary to the schemes [8][9][34][54][55][56][71][72][73][82][113][115], where the transformation and the determination of the differences between the biometric templates have not been fully considered. The performance, robustness and security levels of the reviewed schemes differs from one to another. The reviewed approaches suffer from the security flaws where attacks, which delay and disturb the delivery of packets in the healthcare system can lead to the loss of sensitive data, while putting the patient's health in danger. Moreover, most of these approaches rely on complex cryptographic algorithms, resulting in performance limitations concerning computation, storage, as well as communication, in particular by sending as many packets as possible.

At the end of this comparative study, we have been able to better address the major issues surrounding the security of patient's health in healthcare environments. The bio-cryptography, which combines both benefits of classical cryptography and biometric security could be a very interesting solution to address security issues in such system. Table 2.1 illustrates an overall comparison of the different reviewed schemes based on the criteria defined previously in Section 2.2.

Schemes	**Evaluation Criteria**				
	Security	Communication cost	Processing time	Storage cost	Biometrics extraction
Khan et al. [55]	✗	low	medium	medium	✗
Chen et al. [34]	✗	medium	low	medium	✗
Truong et al. [115]	✗	high	high	high	✗
Khan et al. [56]	✗	high	high	high	✗
Mishra et al. [82]	✗	medium	medium	high	✗
Lu et al. [73]	✗	low	low	low	✗
Lu et al. [72]	✗	low	medium	medium	✗
Jung et al. [54]	✗	low	low	low	✗
Xi et al. [125]	✗	medium	medium	medium	✓
Awasthi and Srivastava [9]	✗	low	low	medium	✗
Tan [113]	✗	low	low	medium	✗
Arshad and Nikooghadam [8]	✗	hight	hight	hight	✗
Lu et al. [71]	✗	medium	medium	hight	✗
Wang et al. [123]	✓	low	medium	low	✓
Bao et al. [12]	✓	medium	high	high	✓
Venkatasubramanian et al. [118]	✓	medium	hight	medium	✓
Jammali and Fourati [52]	✗	medium	high	low	✗
Hu et al. [50]	✗	high	medium	medium	✓
Rajasekaran et al. [102]	✓	low	medium	medium	✓
Zhang et al. [131]	✗	medium	high	medium	✓

Table 2.1 Overall comparison of the reviewed schemes (✓: conscientiously addressed, ✗: totally or partially addressed)

2.6 Conclusion

Although the protection of patient's data in healthcare environments is a very attractive domain, there are still considerable challenges to be overcome to ensure the patient's privacy. Consequently, in this chapter we have presented a state of the art of authentication schemes proposed in the last few years to solve the issue of patient's data security in mobile healthcare environments. Besides, we have established a detailed taxonomy of these solutions according to the orientation of the authentication service, and network architecture. Afterwards, we have described all these solutions followed by a discussion of the strengths and shortcomings of each one. Finally, we have concluded this chapter by the presentation of a synthesis and comparison between the whole of the reviewed schemes. Based on this critical study, we describe in detail in the next chapter our first contribution, which is an authentication scheme based on biometric inputs for mobile healthcare environments to solve the issues which we have already raised.

Chapter 3

Secure and lightweight remote patient authentication scheme with biometric inputs for mobile healthcare environments

3.1 Introduction

Biometrics is an emerging technology for patient authentication due to its advantages over other methods, as passwords and smart cards. However, in mobile environments, it introduces hard constraints on computation, storage and communication, respectively, when analyzing, saving and transmitting the patient biometric data. This chapter will be dedicated, primarily, on the presentation of our proposed authentication scheme (Secure and Lightweight Remote Patient Authentication Scheme with Biometric Inputs for Mobile Healthcare Environments) [85] through a detailed description of its different phases. The proposed scheme is based on ECC (Elliptic Curve Cryptography), in which a correspondence is established between the biometric template of a patient and its cryptographic keys. After extracting the patient's biometric template, its key pair is computationally derived from that template. The key pair is used to produce a session key with the remote server for mutual authentication. In the second part of this chapter, we provide the results obtained by the security analysis of our scheme against various malicious attacks compared to concurrent schemes. We also emphasize in this part on the validation of our proposal through simulations and performance analysis, and this by comparing it with concurrent schemes from the literature.

3.2 Motivations

In distributed healthcare applications, the mobile devices such as cell phones, personal digital assistants and smartphones are now able to collect individual health-related data and report them to healthcare professionals situated anywhere. These data allow for distributed care, enabling remote diagnoses, alerting doctors for an emergency intervention or to change conditions as they occur and providing the total picture of the patient's health so that necessary care can be administered. When an unexpected incident underwent on the health of a patient, the latter may be not able to authenticate itself using something he/she knows as passwords. In such critical situation, the authentication process should be done automatically without the patient intervention. A biometric-based authentication scheme responds well to this important requirement. In classical biometric-based authentication methods, the identification of a user is performed through a specific analytical comparison between the introduced user's biometric data and the prior stored one [114]. In mobile environments, this process introduces hard constraints on computation, storage and communication, respectively, when analyzing, saving and transmitting this type of complex data. An extensive analysis of the literature has shown that various biometric-based remote patient authentication schemes have been proposed. However, the previously proposed schemes are much more complex, present performance limits and do not show a sufficient security level against attacks. In this paper, we address these limits and we propose a secure and lightweight remote authentication scheme for mobile healthcare environments. The proposed scheme is based on ECC (Elliptic Curve Cryptography) [59][80], in which a correspondence is established between the biometric template of a patient and its cryptographic keys. After extracting the patient's biometric template, its key pair is computationally derived from that template. The key pair is used to produce a Diffie-Hellman-based session key [42] with the remote server for mutual authentication. Through the security analysis and simulations, we conduct an overall comparison to concurrent schemes, where the proposed scheme demonstrates promising results. The contributions of this work are quintuple: (1) the proposed scheme translates the patient biometric data to ECC-based key pair and it does not require to save or to communicate the patient's biometric template; (2) it transforms the biometric inputs before their use, so that the transformed template be revocable, non-invertible, reliable, and respects the patient privacy; (3) it performs in four rounds of communication in both phases: registration and authentication; (4) it provides an effective robustness against replay, impersonation, server spoofing, anonymity, insider, man-in-the-middle,

physical, parallel session, reflection and denial of service attacks; and (5) it operates with a lightweight load of storage, communication and computation.

3.3 The proposed scheme

In this section, we give the overview and assumptions followed by the detailed description of the proposed scheme.

3.3.1 System model

There are three parties involved in the proposed scheme: the remote server S, the patient P_i and its own mobile device. The latter could be a personal digital assistant or a smartphone, which acts as a sink and collects information regarding the patient's medical information. The supervision process could be realized through a wireless body area network [7][27], where sensors are deployed on or around the patient's body. The mobile device communicates the patient's data to the remote server via the Internet. The remote server keeps electronic medical data of the registered patients. These data are shared among authorized users, such as the healthcare staff, researchers, government agencies and/or insurance companies [33][43][69]. The remote server is a trusted party, which is responsible for initializing the system, publishing the system parameter and outputting the authentication credentials for the system patients.

We do not focus on a particular biometric feature. Furthermore, we assume that each patient is equipped with a biometric data reader specific to the targeted type of application. The proposed scheme is executed in three phases: (1) the system initialization, (2) the patient registration; and (3) the mutual authentication with session key agreement. The overall framework of the proposed scheme is illustrated in Figure 3.1. Table 3.1 summarizes the main used notations and the following subsections describe the operations of each phase.

3.3.2 System initialization phase

In this phase, two distinct operations are involved, namely the cancellable biometric template extraction and the system parameter generation.

3.3.2.1 Cancellable biometric template extraction

The generation of a cryptographic key using biometric inputs has emerged as one of the most effective process used to overcome the security weakness in classical methods

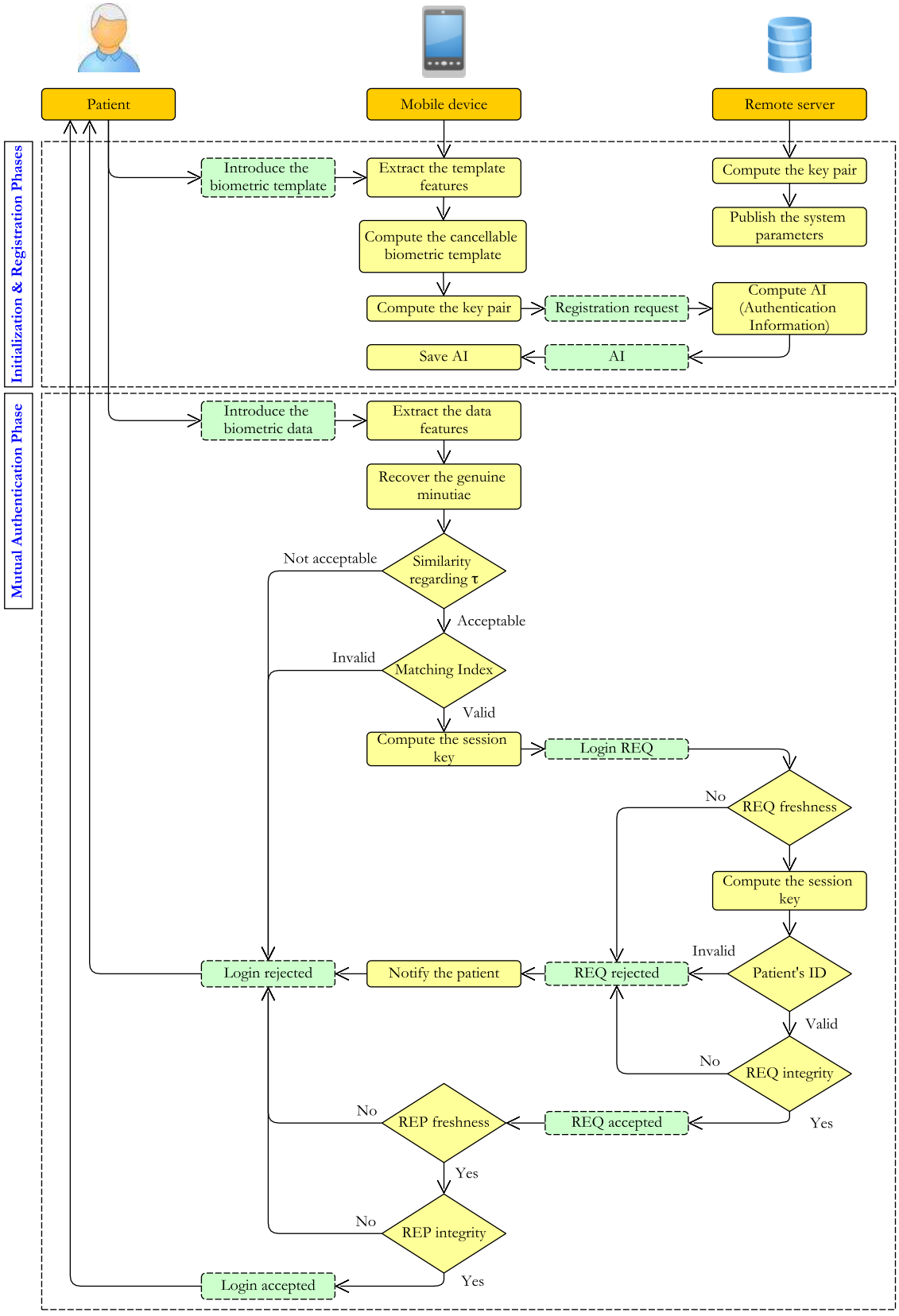


Fig. 3.1 Overall operations of the proposed scheme

Notation	**Description**
S	The remote server
P_i	The patient i
ID_i	The patient P_i's identity
DI_i	The patient P_i's dynamic identity
B_i	The patient P_i's biometric template
M_i	The B_i's minutiae points set
C_i	The B_i's chaff points set regarding M_i
m_k	A minutiae point
(x_k, y_k)	The m_k's Cartesian-coordinates
θ_k	The m_k's orientation
d_{kl}	The Cartesian-distance between m_k and m_l
$\langle \widehat{K_S}, K_S \rangle$	The remote server S's private and public keys
$\langle \widehat{K_i}, K_i \rangle$	The patient P_i's private and public keys
r_i / r_S	A random numbers chosen by a patient i/server S
$E_q(a, b)$	An elliptic curve equation with order n
n	A large number
V_i	The patient P_i's matching index
γ_i	The patient P_i's cancellable biometric template
AI_i	The patient P_i's authentication information
SAI_i	The patient P_i's secret authentication information
ℓ	Session key
H	A collision free one-way secure hash function
F	The private key generation function
$\langle +, -, \cdot \rangle$	Elliptic curve point addition, subtraction and multiplication
$\|\|$	Concatenation operation
$\oplus$	Bit-wise exclusive-or (XOR) operation

Table 3.1 Main notations

based on passwords, tokens, etc. However, the biometric data cannot be used directly in the cryptographic operations because:

1. The biometric data are not uniformly distributed [22][26].
2. Two different biometric impressions of the same person are infrequently identical, and hence, this type of data is not accurately reproducible [22][26].

Furthermore, the biometric data is a personal feature usually non-cancellable, because when there is theft or forgery, it is not possible to change it as in case of PIN-codes (Personal Identification Number) or passwords [14][18]. In this study, we address

these limitations by the computation of the patient's key pair from its cancellable biometric template.

In order to obtain the cancellable biometric template, the patient imprints his biometric data B_i using the mobile device, which extracts the minutiae points as features. The extraction process of these features involves four major steps [5][63]: (1) normalization; (2) orientation and frequency estimation; (3) phase estimation; and (4) minutiae points detection. Actually, several embedded biometric recognition devices are used to retrieve the minutiae points from the acquired fingerprint image (e.g., Lumidigm M301 [15], Suprema BioMini [16], Verifi P5100 [17], etc.).

The acquired biometric data are subject to significant variations. Thus, the minutiae points can disappear from an extraction to another. According to the literature, the number of minutiae points collected from a good quality of biometric readers contain usually between 40 and 100 minutea [48]. Nevertheless, this number is reduced to between 20 and 30 minutiae [127], when are collected from a latent or a partial template. The minutiae points set of the acquired patient P_i's biometric data B_i is denoted by M_i such as

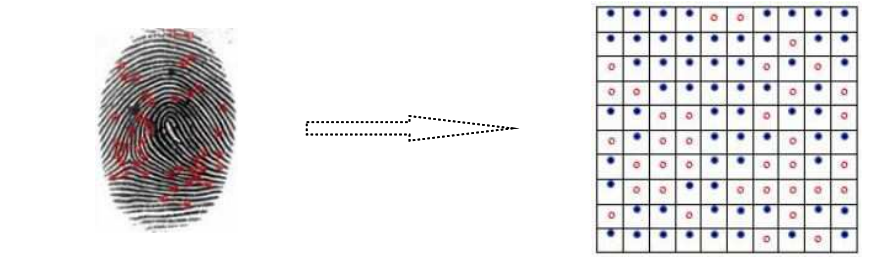
$$M_i = \Big\{ m_k = (x_k, y_k, \theta_k) \Big\}_{1 \leq k \leq u} \tag{3.1}$$

where u is the total number of minutiae points extracted from the patient's biometric template, (x_k, y_k) are the point m_k's Cartesian-coordinates, and θ_k is the point m_k's orientation. The distance between any pair of minutiae points m_k and m_l, with coordinates (x_k, y_k) and (x_l, y_l), respectively, is computed by the Cartesian-distance.

To generate the cancellable biometric template from the acquired minutiae points, first, we compute the distance between each pair of minutiae points. Then, the obtained values are structured and sorted in a matrix, denoted by A_i such as

$$A_i = \begin{array}{c} \\ m_1 \\ m_2 \\ \vdots \\ m_u \end{array} \begin{array}{c} \begin{array}{ccccc} m_1 & m_2 & m_3 & \cdots & m_u \end{array} \\ \begin{bmatrix} d_{11} & d_{12} & d_{13} & \cdots & d_{1u} \\ d_{21} & d_{22} & d_{23} & \cdots & d_{2u} \\ \vdots & \vdots & \vdots & & \vdots \\ d_{u1} & d_{u2} & d_{u3} & \cdots & d_{uu} \end{bmatrix} \end{array} \tag{3.2}$$

Note that $\forall k, l \in \{1, u\}^2, d_{kl} = d_{lk}$, where the set of d_{kl} represent the coefficients. We consider either the upper or lower triangular part of A_i. For instance, in case of the upper part, the patient P_i's cancellable biometric template γ_i is computed such as



(a) Original fingerprint image with genuine minutiae points location

(b) Matrix image with genuine minutiae and chaff points

Fig. 3.2 Shuffling of a fingerprint-based minutiae points set with chaff points insertion

$$\gamma_i = \sqrt{\sum d_{kl}}, d_{kl} \in A, k \leq l. \tag{3.3}$$

To protect the extracted minutiae points $M_i = \{m_k\}$, the latter set is completed by a set of chaff points C_i such as $C_i = \{c_l\}$ with $m_k \neq m_l$. The aim of the shuffling is to avoid all the attempts, which can be used to distinct between genuine and chaff points. On the mobile device is kept C_i secretly, which can be used to recover the genuine minutiae from $M_i \cup C_i$. In figure 3.2, we illustrated an example of shuffling in case of fingerprint template.

3.3.2.2 System parameter generation

In the server side, S chooses an elliptic curve $E_q(a,b)$ with an order n, where n is a large number for security considerations. Then, it selects a base point G with an order n over $E_q(a,b)$, chooses its private key $\widehat{K_S} \in [1, n-1]$, and computes the corresponding public key $K_S = \langle Q_S, G \rangle$ such as

$$Q_S = \widehat{K_S} \cdot G. \tag{3.4}$$

Afterwards, it chooses a secure one-way hash function $H : \{0,1\}^* \rightarrow Z_p^*$, where Z_p^* is a cyclic group of an order $p-1$. Finally, it keeps secretly $\widehat{K_S}$ and publishes $\langle K_S, n, G, H \rangle$ as system parameters.

In the patient side, the key pair is computationally derived from its biometric template. First, by using the biometric reader, the mobile device extracts the patient P_i's biometric template B_i and computes its corresponding cancellable biometric template γ_i using the genuine minutiae points (cf. Section 3.3.2.1). Then, the mobile device computes its private key $\widehat{K_i}$ such as

$$\widehat{K_i} = H\Big(\gamma_i \cdot G\Big). \tag{3.5}$$

Finally, it computes its public key $K_i = \langle Q_i, G \rangle$ such as

$$Q_i = \widehat{K_i} \cdot G. \tag{3.6}$$

Note that it is hard to forge $\widehat{K_i}$ from Q_i and G because of the Elliptic Curve Discrete Logarithm Problem (ECDLP)[1].

3.3.3 Patient registration phase

This process is executed at the first interaction of a patient P_i with the remote server S. All the operations performed by the patient P_i are executed by its mobile device. First, by using the biometric reader, the mobile device extracts the patient P_i's biometric template B_i and computes his/her cancellable biometric template γ_i. Then, it computes the matching index V_i such as

$$V_i = H\Big(ID_i \| \widehat{K_i}\Big), \tag{3.7}$$

and sends the registration request $\langle V_i, ID_i, K_i \rangle_{K_S}$ to the remote sever S, where ID_i represents the patient's identity (the mobile's serial number is recommended). The parameter V_i matches the patient's identity to its private key that is already linked to its biometric template. Upon receiving the request, the remote server S generates a random number $r_S \in [1, n-1]$ and computes the patient's authentication information AI_i such as

$$AI_i = H\Big(ID_i \| r_S \cdot \widehat{K_S} \| T\Big) \oplus V_i, \tag{3.8}$$

where T is the current timestamp of the remote server S. Finally, it saves $\langle ID_i, AI_i \rangle$ in its locally and sends $\langle ID_i, V_i, AI_i \rangle_{K_i}$ to the patient's mobile device.

[1] Given two points Q and G over an elliptic curve, it is computationally hard to find an integer $k \in [1, n-1]$ such as $Q = k \cdot G$. This means that, for a big integer n, there is no polynomial-time bounded algorithm allowing to compute k in a reasonable time due to the high number of possible combinations. This problem is known, in the literature, as ECDLP (Elliptic Curve Discrete Logarithm Problem). For more detail about the ECDLP, kindly refer to [39][45].

3.3.4 Mutual authentication with session key agreement phase

The parameter B_i represents the patient P_i biometric template from which is already generated the key pair during the system initialization. Later, when a given user pretends to be the patient P_i, the mobile device extracts its biometric data, denoted by B_i', and checks its correspondence to the generated keys. In this context, the patient P_i's mobile device extracts the minutiae set M' by using the embedded biometric module and recovers the genuine minutiae points from $M_i \cup C_i$. If the similarity degree between the sets M' and M is unacceptable regarding a predetermined threshold τ, the mobile device rejects the login request. Otherwise, the mobile device computes the patient's cancellable biometric template γ_i from which it computes the key pair $\langle \widehat{K}_i, K_i \rangle$. Then, it computes V_i' such as

$$V_i' = H\Big(ID_i \| \widehat{K}_i\Big). \tag{3.9}$$

If the matching index is invalid, i.e., $V_i' \neq V_i$, then the mobile device rejects the login request. This process authenticates the patient P_i by its own mobile device, restricting the usage of the latter only by its proper owner. If the patient P_i is authenticated, the mobile device selects a secret random number $r_i \in [1, n-1]$, computes

$$W_i = r_i \cdot Q_i, \tag{3.10}$$

$$D_i = r_i \cdot \Big(V_i + Q_S\Big), \tag{3.11}$$

$$R_i = r_i \cdot G, \tag{3.12}$$

and finally the secret authentication information by

$$SAI_i = AI_i \oplus V_i. \tag{3.13}$$

The mobile device computes the session key ℓ such as

$$\ell = \widehat{K}_i \cdot Q_S, \tag{3.14}$$

and the patient P_i's dynamic identity DI_i such as

$$DI_i = ID_i \oplus H\Big(T_i \| r_i \cdot V_i \| \ell\Big), \tag{3.15}$$

where T_i denotes the current timestamp of the mobile device. Finally, the mobile device sends $\langle Q_i, DI_i, D_i, T_i, R_i, \langle W_i, H\Big(R_i \| SAI_i \| T_i\Big)\rangle_\ell\rangle$ to the remote server S. Upon receiving, the remote server S extracts T_i. Then, it checks the timestamp validity, such as $T_S - T_i \leq \Delta T$, where T_S and ΔT denote, respectively, the current timestamp of the remote server and the expected valid time interval of the transmission delay. If $T_S - T_i > \Delta T$, a replay attack is suspected and then, the remote server S rejects the login request. Otherwise, the remote server S computes in its side the session key such as

$$\ell = \widehat{K}_S \cdot Q_i. \tag{3.16}$$

Note that the session key ℓ is shared between the patient P_i and the remote server S and both of them computes it without any anterior interaction. In the patient side, the mobile device by holding the remote server S's public key $K_S = \langle Q_S, G\rangle$, it has already computed

$$\ell = \widehat{K}_i \cdot Q_S = \widehat{K}_i \cdot \widehat{K}_S \cdot G = \widehat{K}_S \cdot \widehat{K}_i \cdot G = \widehat{K}_S \cdot Q_i, \tag{3.17}$$

which represents the same session key computed in the remote server side. Next, it computes $\langle r_i \cdot V_i\rangle$ such as

$$r_i \cdot V_i = D_i - \widehat{K}_S \cdot R_i. \tag{3.18}$$

The remote server S can check the patient identity by verifying the following equality

$$ID_i = DI_i \oplus H\Big(T_i \| r_i \cdot V_i \| \ell\Big). \tag{3.19}$$

Otherwise, it rejects the login request. In the other case, it decrypts $\langle W_i, H\Big(R_i \| SAI_i \| T_i\Big)\rangle_\ell$, computes $H\Big(R_i \| SAI_i \| T_i\Big)$ and compares the result to the already stored value. If it holds, the remote server S authenticates the patient P_i, or else, the login request is rejected.

In order to authenticate the remote server S, the latter selects a secret random number $r_S \in [1, n-1]$, computes

$$W_S = r_S \cdot Q_S, \tag{3.20}$$

and responds to the patient P_i with $\langle W_i \oplus W_S, T_S, \langle H\Big(W_S \| SAI_i \| T_S\Big)\rangle_\ell\rangle$. Upon receiving, the mobile device checks the validity of the timestamp, such as $T_i - T_S \leq \Delta T$.

If it not holds, the mobile device rejects the request. Otherwise, it decrypts the message by computing

$$h = \langle H\Big(W_S \| SAI_i \| T_S\Big)\rangle_\ell, \tag{3.21}$$

extracts W_S from $\langle W_i \oplus W_S\rangle$, computes

$$h' = H\Big(W_S \| SAI_i \| T_S\Big), \tag{3.22}$$

and finally verifies if $h = h'$. If it holds, the patient P_i authenticates the remote server S.

3.4 Security analysis

In this section, we analyze the security of the proposed scheme against well known threats. Its robustness is effective against the following attacks:

- *Replay attack:* an adversary may try replaying the exchanged messages between a patient P_i and the remote server S. Suppose that he/she has already intercepted a valid login request previously sent-out by the patient P_i. If he/she replays the login request, the remote server S detects the attack by verifying the timestamp T_i of the received request, which will be rejected if $T_S - T_i > \Delta T$. In the other hand, the adversary cannot succeed replaying the remote server S's login request. The patient P_i detects such attack by verifying the inequality $T_i - T_S > \Delta T$.

- *Impersonation attack:* an adversary may try impersonating a legitimate patient through the intercepted messages from the previous sessions. Assume that the adversary has already intercepted a valid login request previously sent-out by the patient P_i or by the remote server S. The adversary cannot succeed the patient impersonation attack because he/she cannot create a forged login request for the fresh timestamps without holding the private keys $\widehat{K_i}$ and $\widehat{K_S}$.

- *Server spoofing attack:* an adversary may try masquerading as a remote server to discover the patient's long-term secret by intercepting the request message $\langle Q_i, DI_i, D_i, T_i, R_i, \langle W_i, H\Big(R_i \| SAI_i \| T_i\Big)\rangle_\ell\rangle$ of a previous session. It is impossible for the adversary to figure-out W_i or $H\Big(R_i \| SAI_i \| T_i\Big)$ from the message without holding the session key ℓ. Moreover, it is not possible to forge a valid login request $\langle W_i \oplus W_S, T_S, \langle H\Big(W_S \| SAI_i \| T_S\Big)\rangle_\ell\rangle$ without holding the private keys $\widehat{K_i}$ and $\widehat{K_S}$, and he/she cannot compute $\langle r_i \cdot V_i\rangle$ or W_S from D_i and $\langle W_i \oplus W_S\rangle$.

- *Attack against anonymity:* from the login request, an adversary has no way to guess or to compute the patient's original identity ID_i from its dynamic identity DI_i without holding the session key ℓ. Also, the biometric template is used only when generating the key pair. Hence, the proposed scheme preserves the patient's anonymity.

- *Insider attack:* from the registration request $\langle V_i, ID_i, K_i \rangle_{K_S}$ sent-out by the patient to the remote server, the privileged insider cannot obtain from this request any secret information without holding the server private key $\widehat{K_S}$. Moreover, the proposed scheme does not require any password. Hence, the privileged-insider cannot impersonate any legitimate patient.

- *Man-in-the-middle attack:* the first authentication step is accomplished directly between the patient and its mobile device without any intermediate entity. Therefore, the man-in-the-middle attack cannot succeed. In the second authentication step, an adversary may attempt to stand between the mobile device and the remote server S. However, since the exchanged messages are authenticated, the adversary has no possibility to impersonate anyone of them.

- *Physical attack:* assume that an adversary finds or steals the patient's mobile device and attempts to obtain the confidential parameters $\langle ID_i, AI_i \rangle$. In that situation, it is impossible for him/her to figure-out any secret information from these parameters without holding the server's private key $\widehat{K_S}$ and the corresponding timestamp.

- *Parallel session attack:* assume that an adversary intercepts the exchanged messages between a patient P_i and the remote server S, and then try to open a parallel session with the remote server S (respectively to the patient P_i). The remote server S (respectively the patient P_i) detects such attack by verifying the freshness of the timestamp T_i (respectively T_S) of the received request.

- *Reflection and denial of service attacks:* it is impossible for an adversary to forge a valid login request out of those intercepted between the two communication parties without holding the secret parameters: ℓ, $\widehat{K_i}$, $\widehat{K_S}$, r_i, and r_S. The denial of service attack is countered by the inability of the adversary to introduce both a valid biometric template B_i and a correct identity ID_i.

In Table 3.2, we summarize the overall security analysis of the proposed scheme with comparison to the related works.

Security requirements	**Schemes**									
	Jung et al. [54]	Lu et al. [72]	He and Wang [46]	Lu et al. [73]	Khan et al. [55]	Chen et al. [34]	Truong et al. [115]	Khan et al. [56]	Mishra et al. [82]	Our scheme
Replay attack	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓
Impersonation attack	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Server spoofing attack	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Attack against anonymity	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓
Insider attack	✓	✓	✗	✓	✗	✗	✓	✓	✓	✓
Man-in-the-middle attack	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓
Physical attack	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓
Parallel session attack	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
Reflection attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Denial of service attack	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓

Table 3.2 Security analysis (✓: prevent the attack, ✗: do not prevent the attack)

3.5 Performance evaluation

In this section, we provide the simulation results comparing the proposed scheme to some relevant schemes presented in Chapter 2. The simulations are developed on a Samsung Galaxy S6 smartphone characterized by a processing rate of 2.1GHz, a memory of 3Go, and a wireless transmission rate of 5.76Mbps. The smartphone interacts with a server machine characterized by a processing rate of 2.3GHz, a memory of 4Go, and a wireless transmission rate of 54Mbps. The authentication process is performed through the fingerprint-based biometric feature.

The performance evaluation is performed for both mobile and server sides, covering three major metrics: (1) the communication cost, which represents the amount of transmitted data traffic per session of authentication, (2) the processing time, which represents the time spent in computation per session of authentication, and (3) the storage cost, which represents the memory space spent for the system parameters per session of authentication. These metrics are evaluated according to three hash function families: MD5 (128bits), SHA-1 (160bits) and SHA-256 (256bits).

Figure 3.3 and 3.4, illustrate the obtained results in terms of communication cost, respectively, in the mobile device and the remote server side. We note that the communication overhead increases for all the compared schemes when increasing the hash function output size. The results denote out performance of the proposed scheme compared to the other solutions. In fact, the proposed scheme performs the mutual authentication process in two rounds of communication. Both mobile device and remote server compute, independently, an identical session key without extra communication. The schemes of Khan et al. [55] and Chen et al. [34] perform the mutual authentication process in four rounds of communication, achieving better results in the mobile device side compared to the schemes of Jung et al. [54], Lu et al. [73], Truong et al. [115], and Khan et al. [56] operating in five rounds.

Figure 3.5 and 3.6, illustrate the obtained results in terms of processing time, respectively, in the mobile device and the remote server side. We note that the processing time increases for all the compared schemes when increasing the hash function output size. The results denote out performance of the proposed scheme compared to the other solutions. Indeed, the proposed scheme uses a symmetrical session key in the mutual authentication process. In the two rounds of communication, both the mobile device and the remote server perform one operation of encryption in their side, and hence, reducing significantly the computational overhead.

Figure 3.7 and 3.8, illustrate the obtained results in terms of storage cost, respectively, in the mobile device and the remote server side. We note that the storage cost

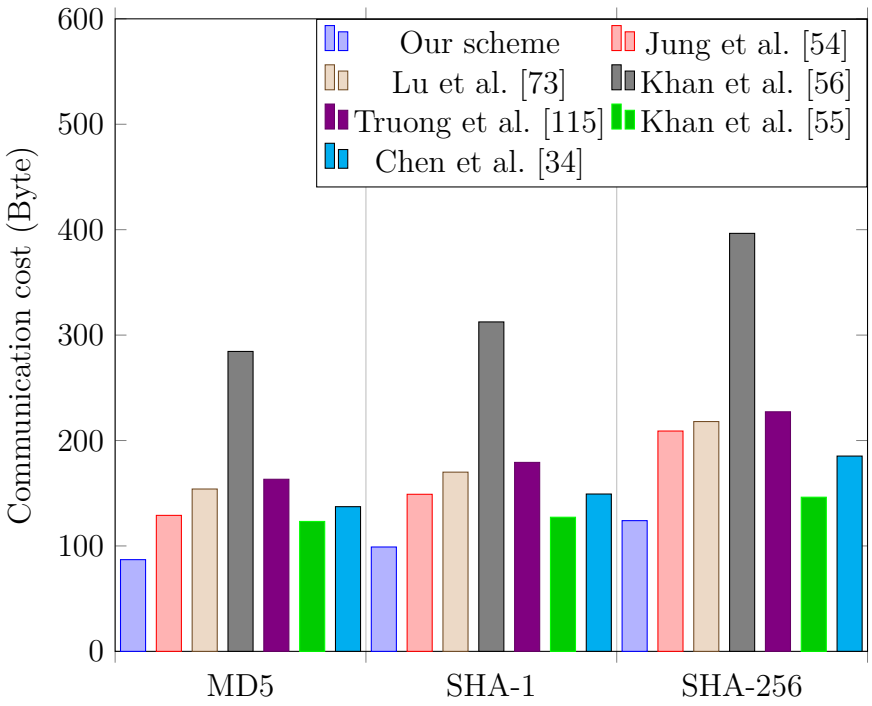


Fig. 3.3 Communication cost evaluation in the mobile device side per session of authentication

increases for all the compared schemes when increasing the hash function output size. The results denote out performance of the proposed scheme compared to the other solutions. Following the other schemes, an important number of cryptographic parameters are stored in both mobile device and remote server side. These parameters are necessarily required to achieve the authentication process. In the proposed scheme, two cryptographic information are maintained per one mobile and all the other parameters and keys are dynamically computed.

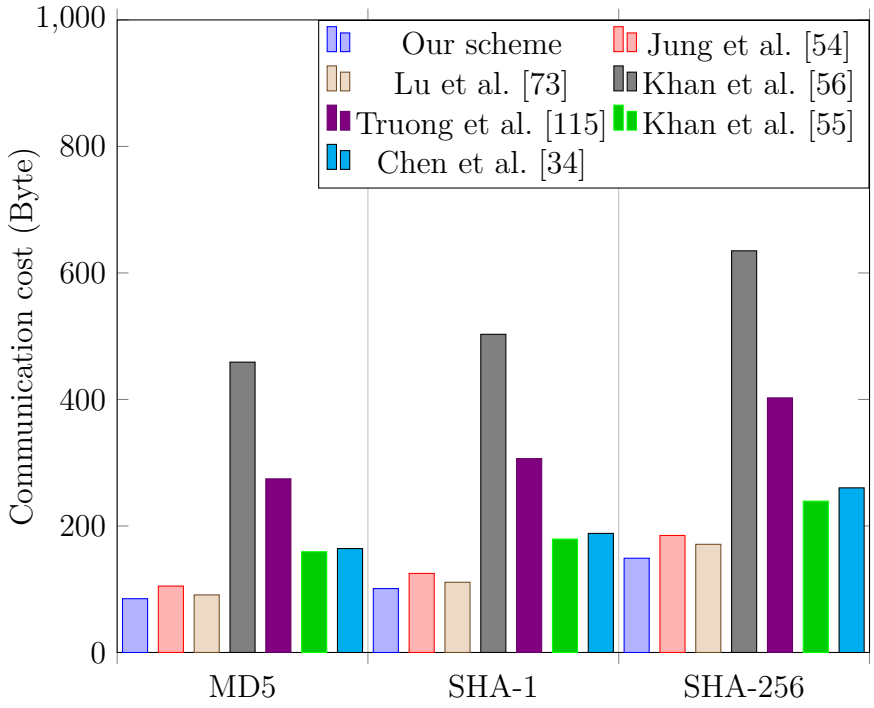


Fig. 3.4 Communication cost evaluation in the remote server side per session of authentication

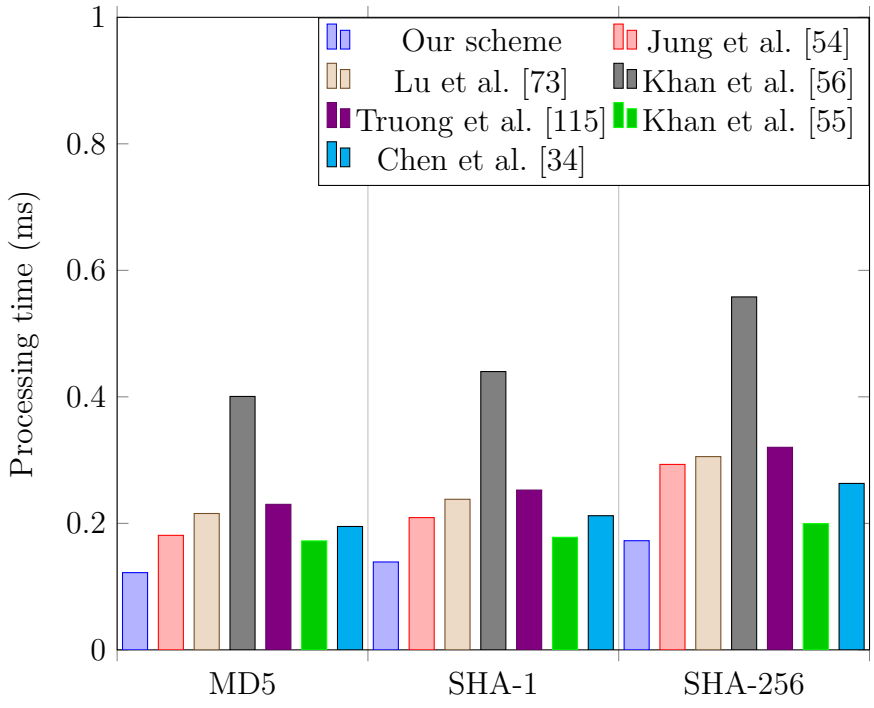


Fig. 3.5 Processing time evaluation in the mobile device side per session of authentication

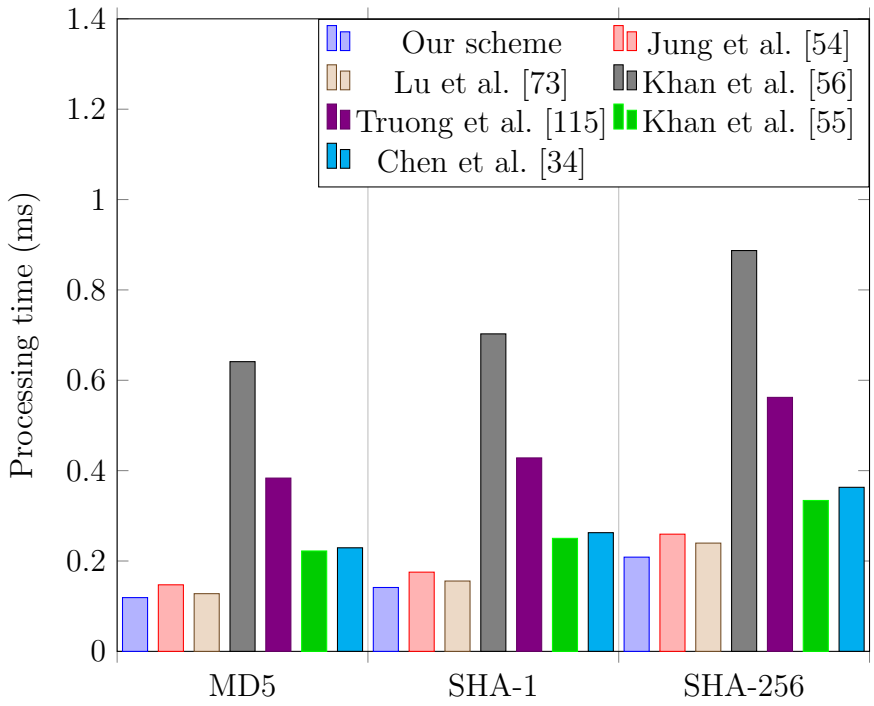


Fig. 3.6 Processing time evaluation in the remote server side per session of authentication

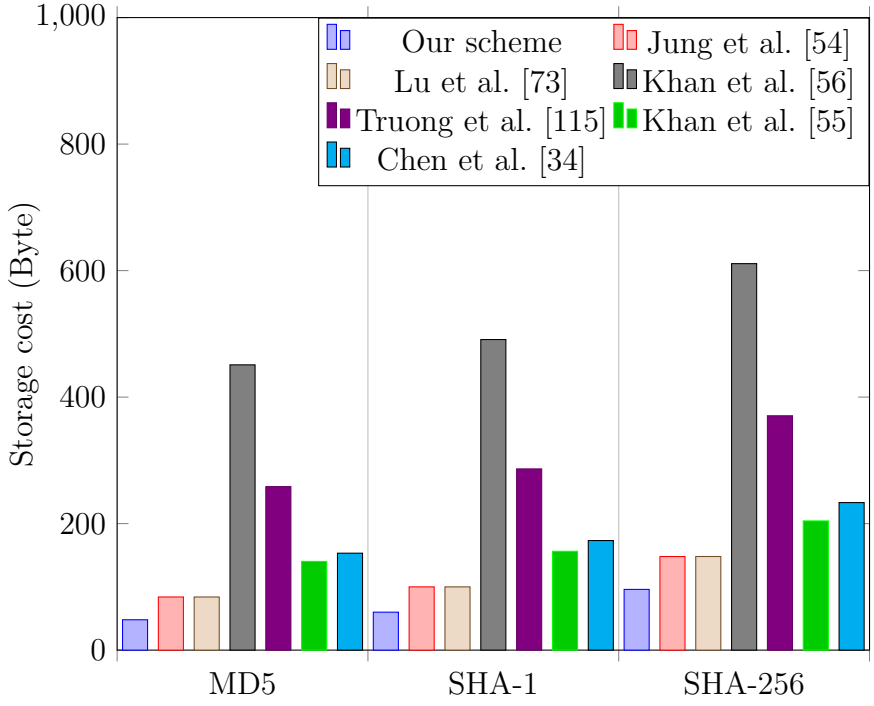


Fig. 3.7 Storage cost evaluation in the mobile device side per session of authentication

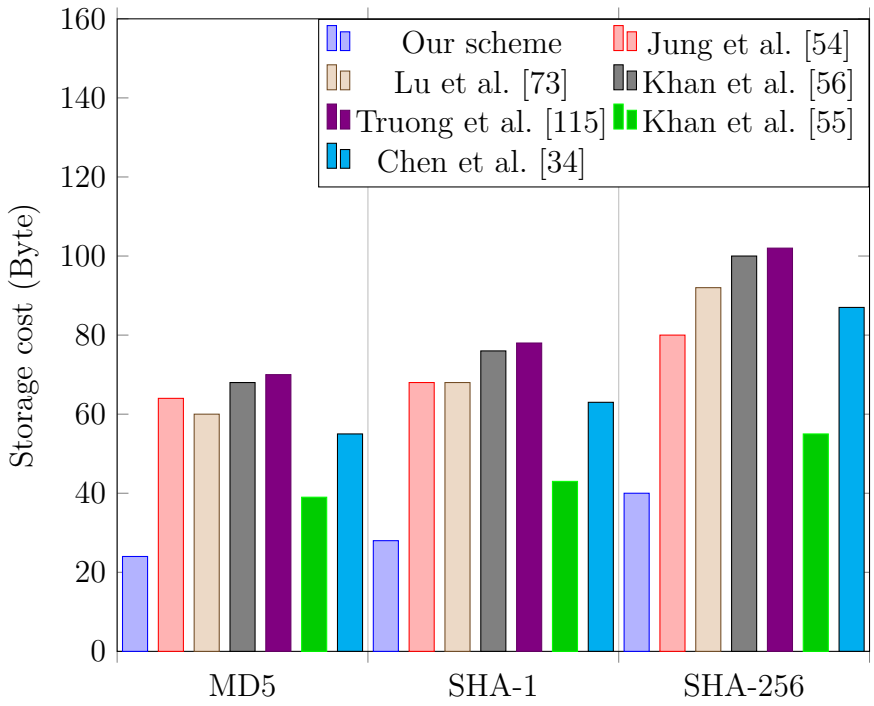


Fig. 3.8 Storage cost evaluation in the remote server side per session of authentication

3.6 Conclusion

In this chapter, we have proposed a secure and lightweight remote patient authentication scheme with biometric inputs for mobile healthcare environments. The purpose of this scheme is to translate the biometric input of a patient to ECC-based keys. The latter ones are used instead of the patient's biometric template in the authentication process. To validate this proposed scheme, simulations are carried out, and this with the aim of showing the contribution of the proposed scheme compared to the already existing ones. According to the tests, the obtained results show the advantages and performances of our scheme while providing effective security. Indeed, our proposal offers several benefits: (1) it provides mutual authentication with session key agreement, (2) it does not require remote transmission of the patients biometric data, (3) it does not hold a database of correspondence, binding patients to their biometric templates, (4) it does not need to analyze biometric data and the computational cost is thoroughly minimized, and (5) it resists against various attacks such as replay, impersonation, server spoofing and anonymity attacks. We have performed an overall evaluation of our scheme through simulations. In the next chapter, we present our second contribution, which exploits the biometric physiological (ECG) features for the authentication process among sensors belonging to the same MBASN in mobile healthcare systems.

Chapter 4

Secure and efficient ECG-based authentication scheme for MBASNs

4.1 Introduction

A Medical Body Area Sensor Network (MBASN) is a health monitoring system, consisting of autonomous sensors communicating through wireless links. These sensors are placed in or around the patient's body in close proximity. They cooperate to transmit the collected information to the remote processing center. However, intruders can easily get into the network to listen the traffic and inject or replicate old messages which can put the patient's health in danger. For that reason, these sensors must be able to exchange information in a secure manner to ensure that intruders will not be able to inject erroneous information. In this chapter, we present our second contribution which provides authentication in MBASNs, termed ECG-AS (Secure and Efficient ECG-based Authentication Scheme for Medical Body Area Sensor Networks) [129]. The main idea of this scheme is to allow two sensors belonging to the same MBASN to agree on a symmetric key, generated using physiological signal features of the same subject. This is to allow these sensors to authenticate each other and exchange information securely in such a network. In this scheme we develop a new mechanism of biometric feature extraction. This mechanism extracts with a high precision the electrocardiogram-based features and achieves higher efficiency of authentication among the sensors. We firstly present the attack and system models; then, we give the detailed description of the ECG-AS operations. Afterwards, we provide the security analysis of our proposal against well known cryptographic threats. Finally, we devote the rest of this chapter to the presentation of the obtained simulation results of our scheme, and this by comparing it with some relevant and recent concurrent schemes.

4.2 Motivations

Medical Body Area Sensor Networks has emerged as one of the most useful technologies for real-time patient healthcare monitoring to ensure a good support for caregivers and healthcare providers. The sensors of a MBASN are often confronted with inter-sensor communications type in order to achieve a common goal. Due to the sensitive nature of the collected and exchanged information between the sensors of the same MBASN, such a network requires taking measurements in order to ensure the confidentiality and integrity of this information, not only to protect the patient's health, but also to guarantee the privacy of the latter. Adding to this, the issue of interferences between sensors of two different MBASNs that can cause another threat to this type of environment. Indeed, failure to obtain genuine and correct medical information can directly influence the diagnoses and appropriate treatments of the patient. To remedy these complications, the security solutions are strongly solicited in order to correctly manage the collected medical information to guarantee the patient's privacy. The principle of such a scheme consists in protecting communications between all the sensors belonging to the same MBASN, while guaranteeing authentication to establish communities of sensors, helping each other to achieve the common objectives in a secure manner. For that reason, we want to secure the inter-sensor communications in a MBASN so that authentication be guaranteed at the time of symmetric cryptographic key generation. Indeed, the latter is generated in an authenticated and transparent manner by using the physiological signals of the same patient by two sensors of the same MBASNs. Consequently, the accuracy of the physiological features of the ECG signal used for the computation of the shared secret remains a very important point in our scheme. Obviously, the combination of biometrics and cryptography emerges as a very powerful solution for the authentication and generation of a random key in this environment. This is due to the unstable and random nature of the ECG signals which vary with time, which leads to guaranteeing the freshness of the generated keys from these signals. Clearly, a malicious sensor will never be able to guess or reproduce the ECG signal features to authenticate itself near the legitimate sensors or computed the shared secret. It is on these principles that we have based to develop our proposal to take into account the inconveniences that we have already raised in this environment.

4.3 System and attack models

In MBASNs, the sensor nodes have the ability to measure health parameters (ECG, PPG, EEG, etc.) on the patient's body. These data can be transmitted either directly or via a sensor-head responsible for sending the information to the data hub. The data hub then transmits the patient's data to the central processing center or to the information server of a hospital, where the healthcare professionals can establish a diagnosis. We assume that all the sensor nodes are within range and are deployed on or in the patient's body. Only the sensor nodes installed by the physician or the surgeon are considered as legitimate. They are the only sensors which are able to measure the patient's physiological signals. An intruder can be in form of an attacker within range of the legitimate sensor nodes seeking access to the exchanged patient's medical information in the MBASN. It could be also a sensor worn by another patient which is within range of the legitimate sensor nodes. We assume that the network is exposed to several attacks, namely [41][74][89]:

(1) *Replay attack:* an attacker may reutilize past exchanged messages between the sensors in their encrypted form in order to be authenticated as a legitimate sensor member.

(2) *Impersonation attack:* an attacker may steal the identity of a legitimate sensor in order to do what only the sensor members are authorized to do.

(3) *Insider attack:* an attacker may steal the client's password verifier from the verification table of the server, and try to access other servers with the stolen password.

(4) *Man-in-the-middle attack:* an attacker may secretly mediate between two communicating sensors, and hence, try to perform the role of both of them.

(5) *Physical attack:* an attacker may find or steal a sensor from a patient's body and attempt to obtain confidential parameters.

(6) *Session hijacking attack:* an attacker may expect from two sensors to initiate a communication session before it takes the place of one of them.

(7) *Reflection and denial of service attacks:* an attacker may clutter the communication between the sensors using all the network bandwidth or submerge a sensor by acknowledgment messages to prevent it from taking any action.

(8) *Sybil attack:* an attacker may usurp the identity of several sensors in order to collect privileges and/or to compromise the network.

(9) *Brute force attack:* an attacker may cryptanalyze the exchanged messages in order to get information about the secret-keys and/or the private patient's data.

4.4 The proposed scheme

The purpose of our work is to develop a secure and efficient ECG-based authentication scheme that enables each pair of sensor nodes to exchange an encryption-key. With the latter, the sensor nodes will be able to authenticate each other and protect the exchanged medical data. The key exchange is processed using the ECDH protocol [6]. However, this protocol does not guarantee the authentication during the key exchange process. Hence, we propose to enhance the process by integrating an authentication phase to ensure that only the sensor nodes of the same MBASN can access to patient's data.

The authentication between the sensor nodes is performed using a biometric technique based on the measurement of the ECG signal. According to Poon et al. [99], time information about heart beats can be an excellent biometric feature for securing MBASNs due to the chaotic nature of heart rate variability. Indeed, the time interval between two successive heart beats at a given instant, is the same for all the sensor nodes measuring the same ECG signal, but is different for each individual [99]. Therefore, the ECG signal can be efficiently used to authenticate the sensor nodes of the same MBASN, as well as to obtain sufficiently random encryption-keys [99]. As illustrated in Figure 4.1, the key exchange and authentication process of our scheme requires four main phases, namely:

(1) Initialization phase, where both the sensor nodes agree upon the parameters to consider in the key exchange and authentication process.

(2) Feature extraction phase, where the ECG signal is measured and used to generate biometric features.

(3) Key exchange phase, where the key is computed and shared according to the ECDH protocol.

(4) Authentication phase, where the biometric features of the two sensors are checked.

In Table 4.1, we present the important notations used in this chapter, and in the following subsections, we give the description of each phase.

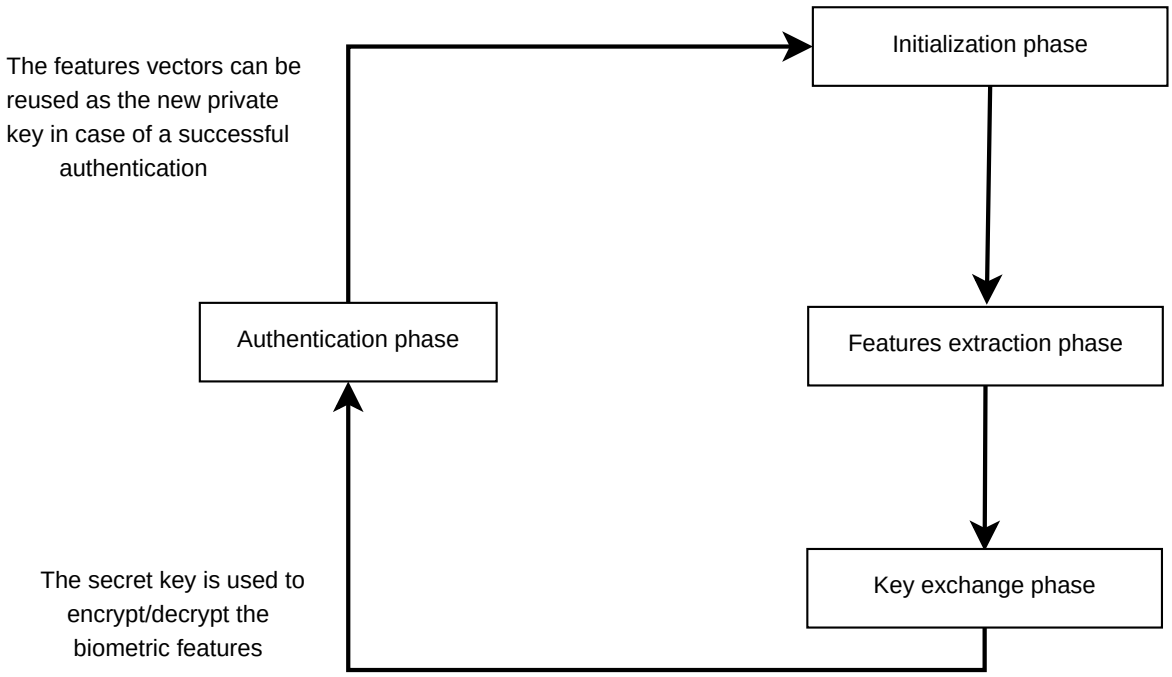


Fig. 4.1 The phases of our authentication scheme

Notation	Description
ID_i	Identity of the sensor node i
T_i	Period chosen by the sensor node i
F_p	Prime field
E	Elliptic curve
G	Generator point of E
$\langle d_i, Q_i \rangle$	Private/public-key of the sensor node i
I_i	Biometric features vector of the sensor node i
I_i^r	Right side of I_i
I_i^l	Left side of I_i
H	Hamming distance
SK_{ab}	Shared-key between A and B

Table 4.1 Notations

4.4.1 Initialization phase

Initially, two sensor nodes agree, in a public manner, on an elliptic curve $E(a,b,p)$ defined over a finite field F_p. The equation of the elliptic curve E is defined as [6]:

$$y^2 \bmod p = x^3 + ax + b \bmod p. \tag{4.1}$$

Where, the integers a and b verify the condition:

$$4a^3 + 27b^2 \bmod p \neq 0. \tag{4.2}$$

The two sensor nodes also agree on a point generator $G(x_g, y_g)$ of the elliptic curve, which is used for the key computation. The ECDH requires from each sensor node i to randomly choose a number d_i from $\mathbb{N}^*$ as a private-key. Then, each sensor node i, computes its public-key Q_i where:

$$Q_i = d_i \cdot G. \tag{4.3}$$

The computation of the private-key d_i requires a random number generator algorithm. This generates additional costs regarding the time complexity and energy, especially in the case of frequent key updates. Therefore, we propose to use the extracted biometric features from the ECG signal as a private-key. The features used previously for the authentication can be subsequently reused as the new private-key. Indeed, if the authentication is successful, then the biometric features form the new private-key d_i. Otherwise, the sensor node measures the ECG signal at a random time and extracts a new private-key.

4.4.2 Feature extraction phase

Each sensor node measures the ECG signal in a synchronized manner and divides it into severals windows, which are first submitted to a Fast Fourier Transformer (FFT) then to an integral computation. The results of the integral computation are converted into binary strings and concatenated to form a vector of biometric features I. The purpose of using the integral computation is to consider all the points of the curve forming the signal and thus, take full advantage of the chaotic nature of heart rate variability, compared to the Enhanced FFT method [118], which uses a limited number of points. The feature extraction phase of our scheme is illustrated in Figure 4.2.

In order to obtain usable biometric features for authentication, it is necessary for both sensor nodes to be synchronized. The sensor node A sends to B a request containing ID_a, ID_b and a period T_a, chosen randomly. Then, the sensor node B responds with T_b, chosen randomly. Afterwards, both A and B compute $s = |T_a - T_b|$. Finally, the sensor nodes A and B wait for a period of time equivalent to s before starting to measuring the ECG signal and computing the biometric features vectors I_a and I_b. The synchronization process of our scheme is illustrated in Figure 4.3

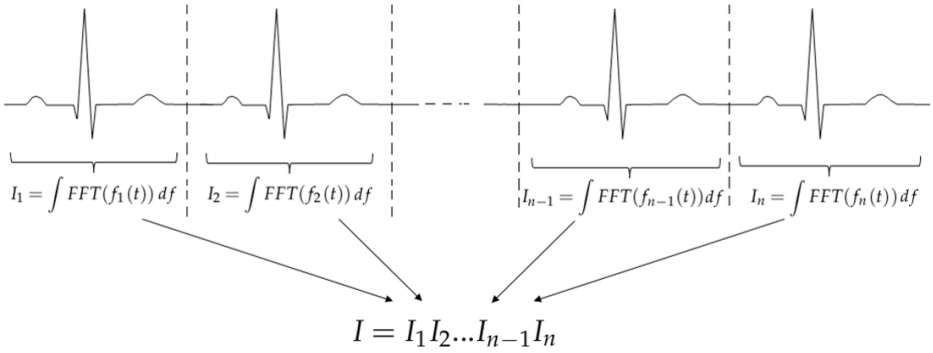


Fig. 4.2 Feature extraction phase

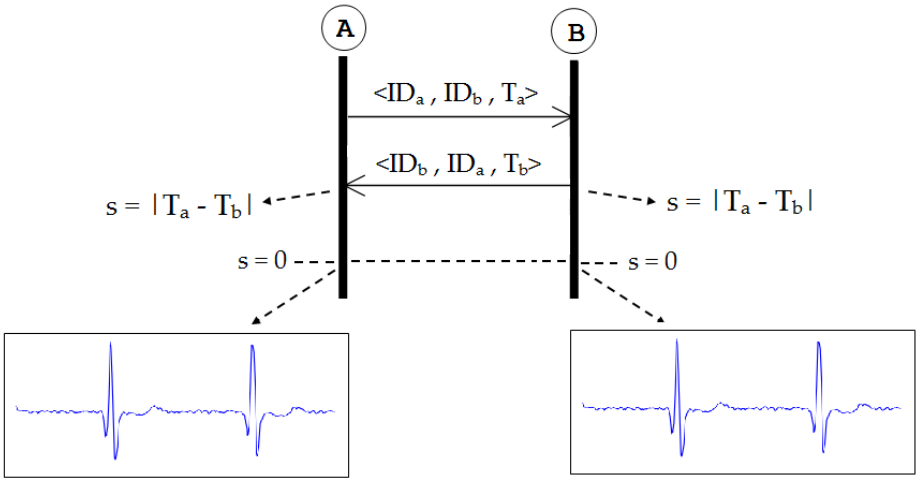


Fig. 4.3 Synchronization process

4.4.3 Key exchange phase

During the key exchange phase, the sensor nodes A and B compute a shared key SK_{ab} using the ECDH algorithm. All the sensor nodes can communicate directly between them. Hence A and B can follow the process without needing any intermediate sensor node. The key exchange process is executed as follows. The sensor nodes A and B exchange their respective public-keys Q_a and Q_b. Then, A computes $d_a \cdot Q_b$ and B computes $d_b \cdot Q_a$. Since

$$d_a \cdot Q_b = d_a \cdot d_b \cdot G = d_b \cdot d_a \cdot G = d_b \cdot Q_a. \tag{4.4}$$

then the secret-key is:

$$SK_{ab} = d_a \cdot Q_b = d_b \cdot Q_a. \tag{4.5}$$

The key exchange phase is illustrated in Figure 4.4.

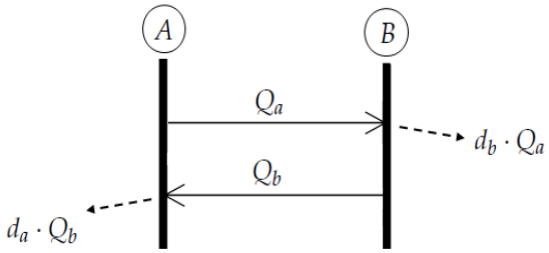


Fig. 4.4 Key exchange phase

4.4.4 Authentication phase

This phase, which is illustrated in Figure 4.5, identifies whether the generated key will be used or not to secure the communication. This phase is executed as follows. The sensor nodes A and B divide their biometric features vectors into two parts, a left side I_i^l and a right side I_i^r, where $i \in \{a, b\}$. The sensor node A sends $\langle I_a^l \rangle_{SK_{ab}}$, the left side of its features vector encrypted with the shared key SK_{ab} to the sensor node B. Upon receiving, B decrypts the block using SK_{ab}. Although I_a^l and I_b^l may seem slightly different, if the sensor nodes are synchronized and use an efficient feature extraction method, the difference between the two vectors does not exceed a threshold. Thus, we use a threshold h to authenticate the two sensors. Let h be the Hamming distance between I_b^l and I_a^l. If $H(I_a^l, I_b^l) > h$, then the sensor node B rejects the authentication request. Otherwise, B responds with the right part of its features vector encrypted with SK_{ab} to A. Upon receiving, the sensor node A proceeds in the same way. In the case of $H(I_a^r\ ,\ I_b^r) \leqslant h$, A sends a positive acknowledgment to B. Otherwise, the authentication process fails.

The constant variation of the ECG signal is advantageous since it is very difficult for an attacker to generate it. As for the legitimate nodes, since they are on the same body, they have to be synchronized in order to measure the ECG signal at the same time and obtain similar features, which will be used for the authentication process of our method. Once the session expires, the ECG signal cannot be reused for future authentication sessions since they are no longer valid. Thus, a replay attack using these features would be detected.

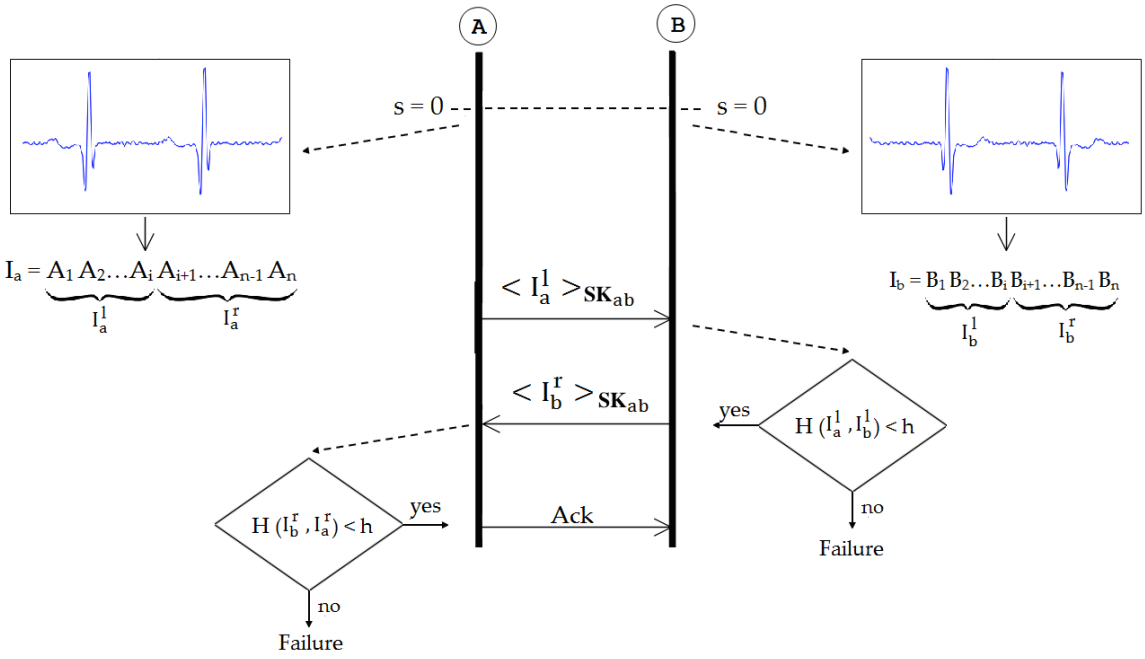


Fig. 4.5 Authentication phase

4.5 Security analysis

In this section, we analyze the security of our proposed scheme by showing its resistance against the attacks described in Section 4.3.

- *Replay attack:* an attacker cannot reuse messages from a session in another one since the key is frequently updated and the biometric features are time variant. Suppose that an attacker happen to intercept $\langle I_a^l \rangle_{SK_{ab}}$ from A and wishes to be authenticated to B. The attacker will be tempted to use Q_a as a public-key and reuse $\langle I_a^l \rangle_{SK_{ab}}$. However, SK_{ab} and the biometric features I_a^l are no longer valid since the private-key of B, which is used to compute SK_{ab}, has already been updated and the Hamming distance between the reused biometric features and the recent ones would not be within the threshold, since they have not been extracted from two ECG signals measured at the same time.

- *Impersonation attack:* biometric authentication is a solution to counter this attack. If an attacker wants to be authenticated as a sensor node belonging to the MBASN, it must obtain the biometric features from the ECG signal. However, only the legitimate sensor nodes are able to measure the ECG signal which are difficult to fake or reproduce given the chaotic nature of heart rate variability.

Suppose that an attacker manage to exchange a key with a sensor node A of the MBASN. In the authentication phase, A must receive the left side of the features of the attacker node before sending its right side.

- *Insider attack:* in this scheme, there is no registration phase, so the sensors send no registration request to the remote server. Also, the privileged insider cannot obtain from the requests exchanged between the sensor A and B any secret information without holding the session key SK_{ab}. Moreover, this scheme does not require any password.

- *Man-in-the-middle attack:* all the sensor nodes of the MBASN are within range. The authentication process will then be performed directly between any pair of sensor nodes without intermediate nodes. An attacker, trying to stand between the two sensor nodes A and B will have no way to impersonate neither A nor B. It is hard to launch a man in the middle attack in such case, because both A and B receive the messages transmitted by the attacker.

- *Physical attack:* in this type of attack, an attacker will have no way to alter the data exchanged between the two sensors A and B. Indeed, when B checkes the biometric features I_a^l after having decrypted them, it will obtain a Hamming distance greater than the value tolerated since the biometric features I_a^l, not extracted from an ECG signal measured at the instant s of the current session, are very different from those of B. Likewise, it is difficult to lead such attack because the key SK_{ab} is known only by A and B and the computation of d_a knowing G, and $d_a \cdot G$, amounts to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP).

- *Session hijacking attack:* once the two sensor nodes A and B are mutually authenticated, each exchanged message is encrypted with the shared key SK_{ab}. If an attacker wishes to impersonate A after, the latter has been authenticated, it must have either the private-key of A or SK_{ab}. However, neither the private-key is communicated, nor is the key SK_{ab} which is only known by A and B. Even if the attacker makes A unavailable with a denial of service attack and then impersonates the sensor node, it cannot retrieve the patient's data from the messages sent from B to A.

- *Reflection and denial of service attacks:* this type of attack is not taken into account in this scheme in the sense that it cannot prevent it from occurring. However, it provides authentication and data privacy services when this attack

occurs or is combined with another attack. Suppose that an attacker overwhelms a sensor with useless requests in order to conduct an identity theft or a session robbery attack, the attacker will not be able to authenticate or obtain confidential patient's data.

- *Sybil attack:* suppose that an attacker wishes to impersonate two different sensor nodes A and B. To do that, it must first exchange a key with A and another key with B. It can then attempt to obtain the biometric features of B to be successfully authenticated to A and those of A to be authenticated to B. However, neither A nor B would send their biometric features before receiving the other part of the features vector and checking it using the Hamming distance. This also is valid for an attacker who can steal more than two identities, the Sybil attack cannot be successfully achieved.
- *Brute force attack:* this attack is countered by our scheme thanks to the randomness of the biometric features used in the key exchange and the authentication. Indeed, the chaotic nature of the heart rate does not allow to quickly find the biometric features that can be extracted from the ECG signal, or even infer the next ones. For a sequence of 64 bits, there are about 1.8×10^{19} possible keys and biometric features to be tested.

4.6 Performance evaluation

In this section, we evaluate first the efficiency of our feature extraction method and then we test the performances of our authentication solution with comparison to the concurrent schemes.

4.6.1 Our feature extraction method efficiency

We have used clean ECG data provided by the BEM company ("Bejaia Equipement Médical", Algeria). These data were collected from 11 different patients using Holter monitors. They were basically collected for medical purpose during a period of 24 hours at a sampling rate of 200Hz. We have used about 2s of the ECG data for each subject with a window size of 30 points for $h = 22$. Figure 4.6 shows the obtained variation of our scheme in terms of FRR and FAR in function of the number of MSBs (Most Significant Bits) taken from each result of the integral computation. FRR= 0.16 and FAR= 0.17 are the lowest rates and are obtained when we consider MSB = 10bits. In this case, only 60ms of the ECG data are used to obtain a features vector of 128bits

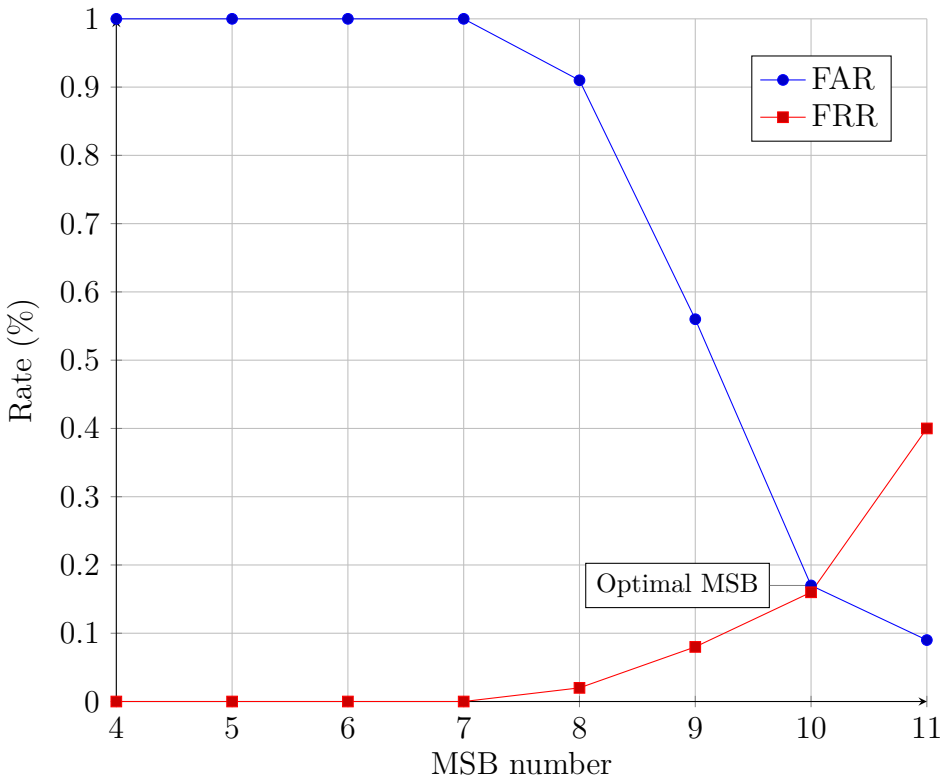


Fig. 4.6 FRR and FAR comparison for the optimal value of MSB

Regarding the Enhanced FTT method, the optimal FRR and FAR rates are obtained when the order of used polynomial is 14 [118]. In Table 4.2, we give the obtained results with comparison to our solution. Indeed, our method ensures lower FRR and FAR than the Enhanced FFT method and also shorter ECG signal to compute longer ECG features vector. This is due to the fact that in our feature extraction method, we do not use only peaks to compute the vector, but every single point obtained from the sampling. Thus, the information between two peaks will not be wasted. The biometric features obtained using our method are perfectly usable for both authenticating the sensor nodes and computing random keys. However, those features should not be used directly as a shared key since the Hamming distance is not always null. Otherwise, the keys would not be the same and the symmetric encryption and encryption functions would be erroneous.

4.6.2 Our authentication scheme efficiency

The implementation of our solution and some concurrent schemes presented in Chapter 2 are performed using Java programming language. To evaluate the performances of

Metrics	Enhanced FFT	Our method
Number of iterations	180	100
Features vector length (bit)	$\backsim 1105$	128
Duration (s)	$\backsim 4$	60×10^{-3}
FAR (%)	0.18	0.17
FRR (%)	0.23	0.16

Table 4.2 Our method compared to the Enhanced FFT

each scheme, we simulate two sensor nodes which are deployed on a patient's body to monitor his physiological signal. The authentication process operates over biometric features extracted from two physiological signals measured on the patient's body, at the same time, by the sensors. The performance metrics are: (1) the communication cost, which represents the total size of data sent out per sensor node in the mutual authentication session, and (2) the processing time, which represents the required time involved in the execution per sensor node in the mutual authentication session. To estimate the performances. These metrics are evaluated in function of different key sizes regarding the Elliptic Curve Cryptography standards, namely P-128, P-160, P-192, and P-224 bits.

Figure 4.7, shows the obtained results of communication cost. As we can see, the communication cost increases for our proposed scheme and the other schemes when the key size increases. This is expected because more update establishments in the transmitted data traffic are done in the sensor node side with the increase of the key size. We note that the performance results of our proposed scheme are clearly higher than those obtained for the others. This is explained by the less update in the packet sent out from the sender sensor, which leads to achieving better results. Indeed, in the schemes based on the fuzzy vault [102] [118] and the "coffer" [50], chaff points are used to hide the biometric features, which increases the size of the transmitted messages. Moreover, Message Authentication Codes (MAC) used in the other schemes also increases the message size. In our scheme, neither chaff points nor MAC are needed since the biometric features are encrypted and authenticated with a private-key.

Figure 4.8, shows the obtained results in terms of processing time. We note that the processing time increases by increasing the key size. We can see also that the performances of our scheme is higher than other schemes. In fact, during the synchronization stage and authentication phase of our scheme, the sender sensor performs less relationship establishments and updates with the receiver sensor with

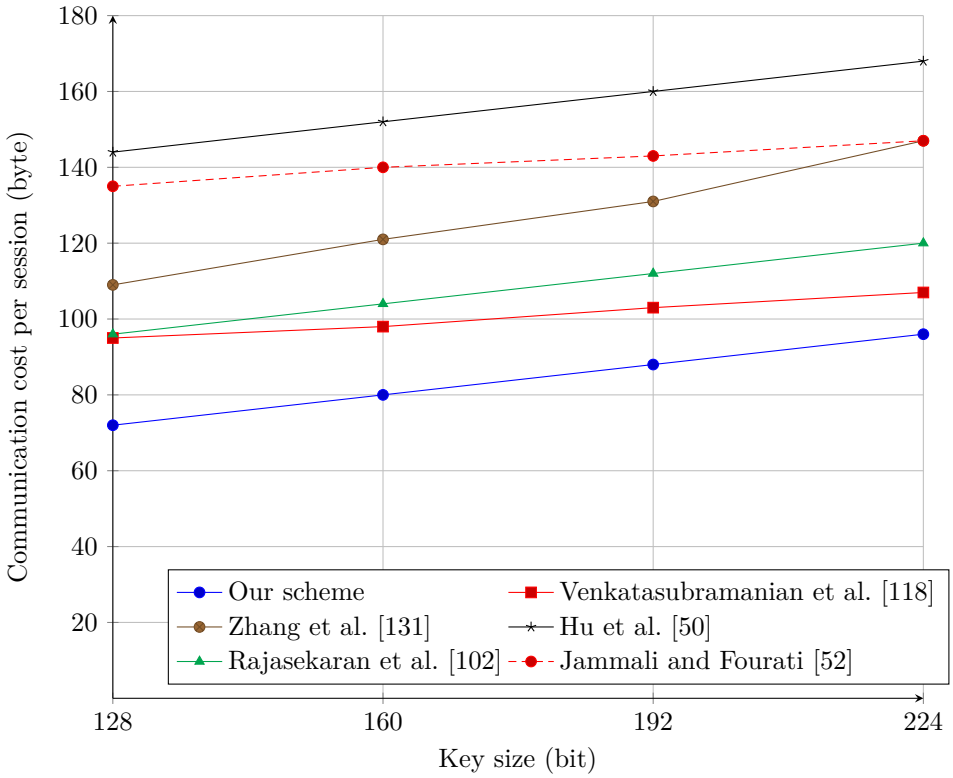


Fig. 4.7 Communication cost in the sender sensor side

less computation, which are necessary to accomplish the mutual authentication process between the two communication nodes.

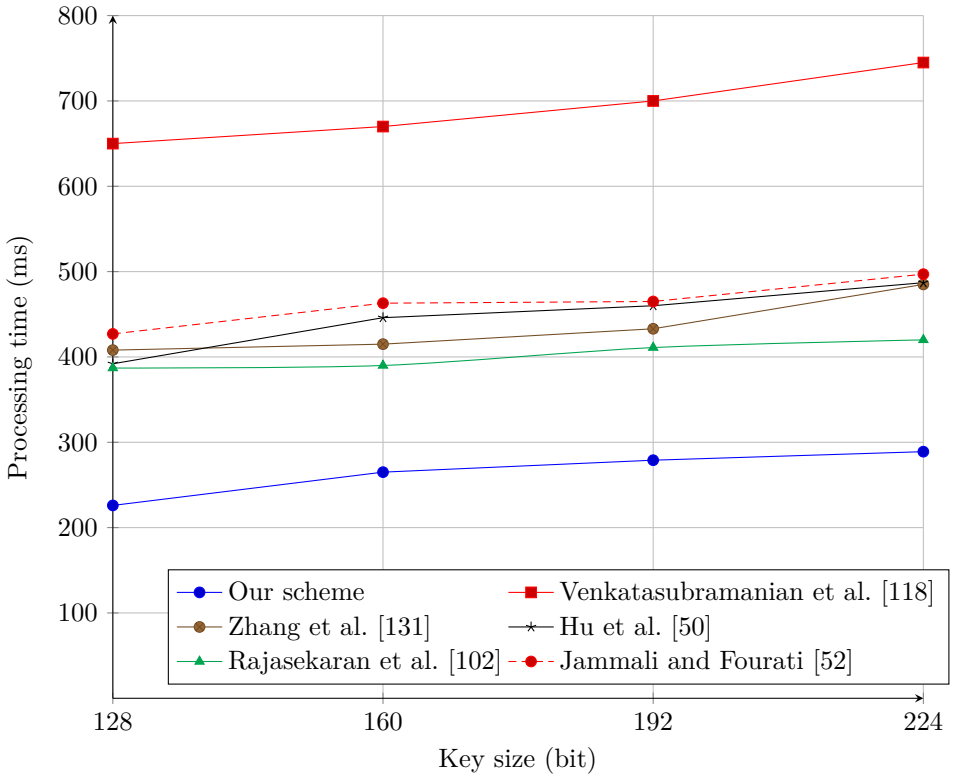


Fig. 4.8 Processing time in the sender sensor side

4.7 Conclusion

In this chapter, we have proposed an electrocardiogram-based authentication scheme to ensure the security of inter-sensor communications in MBASNs. Our proposal operates in a healthcare environment, in which sensors of the same MBASNs agree on a symmetric bio-cryptographic key which is generated in an authenticated and transparent manner. This symmetric key is generated from the physiological signal features which are recorded at the same instant by sensors belonging to the same subject. As these features are not usually completely identical, so we have developed in our scheme a new extraction method, based on the integral computation, which offers better FRR and FAR rates than those based upon the Enhanced FFT method. Through the security analysis, we have proved that our scheme ensures higher security against various malicious attacks. Finally, the performance of our scheme was evaluated by simulations, in which the obtained results indicate that our scheme ensures a lower processing time and communication cost than concurrent schemes. In the next chapter, we present our third contribution, which is an authentication scheme based upon biometric fingerprints for solving the security issues in home healthcare systems.

Chapter 5

Biometric-based remote patient authentication scheme for home healthcare systems

5.1 Introduction

Home healthcare systems are designed to assist patients remotely without visiting medical centers. These systems provide patient with prevention, rehabilitation, therapeutic and educational services. Furthermore, they reduce patient visits at hospitals for emergency services, and present comprehensive healthcare for less economic cost. Thereby, these mechanisms alleviating the burden on the home healthcare system and patient. Unlike classical methods, these new systems allow both patients and healthcare professionals to access sensitive data or receive remote medical treatment using wireless interfaces whenever and wherever. Despite the multitude of advantages offered by this kind of system, an intruder can encrust himself in the network and spy on, inject or reuse the exchanged medical data putting patient's health and life in danger. In this chapter, we propose a secure and lightweight biometric-based remote patient authentication scheme using elliptic curve encryption through which two mobile healthcare system communication parties could authenticate each other in public mobile healthcare environments [84]. This chapter will be devoted, initially, to the presentation of an overview on the home healthcare system, then, we describe our authentication scheme for such systems through a detailed description of the different phases which constitute it. Afterwards, we will define the attack model and security analysis. Finally, we provide the obtained experimental results of our scheme. To

evaluate its performance, we have compared it with concurrent schemes from the literature.

5.2 Motivations

Nowadays, home healthcare system has emerged as one of the most useful inventions for e-healthcare. From this system, patients can receive medical service they usually need in their homes without going physically to be treated face-to-face in the hospital [53]. Through Medical Body Area Sensor Networks (MBASNs) [7], patient's vital signs, such as blood sugar, pulse oximeter, heart rate, and blood pressure, etc., are constantly measured. These vital signs must be monitored remotely in real-time by a doctor via a Graphical User Interface (GUI), then processed and forwarded to medical databases on hospital server [3][4][69]. Afterwards, this sensitive and private data can be accessed by different authorized users, including healthcare staff, researchers, government agencies, and insurance companies; to provide immediate medical assistance in case of emergency or in situations representing a danger to the patient's life [33][43][69]. Nevertheless, the accessibility to this medical data of a particular registered patient must not be allowed for all the users. For instance, clinicians are only permitted to access the medical data related to their patients but, they do not have the right to access other patients' medical data [33][69]. The communication of these sensitive data through wireless networks between the patient's mobile device and remote server plays a censorious role in remote medical diagnosis. Indeed, wrong or unauthenticated medical data may put the patient's life in danger. Therefore, a secure authentication may help to ensure the security of the exchanged medical data between patient's mobile device and remote server to protect patient's privacy. In order to provide a greater security of the system and overcome security flaws, some user authentication schemes use passwords and smart cards have been proposed [36][46][69][122]. However, passwords are not only difficult to remember in case of emergencies, but also ineffective in deterring guessing attacks [53], and smart cards might be shared, lost, stolen [46][79], misplaced, or willingly given to an unauthorized user [9]. Contrary to classical authentication methods, biometrics-based authentication schemes have not such drawbacks [46], and can offer higher security and reliability for user authentication [78][107]. The reason for that, is biometric systems frees the user to remember something or keep a physical object in their possession [47]. In addition, biometric features do not change over the time [107], are hard to share or forge, and might not be lost or forgotten [75][83]. In mobile healthcare systems, numerous remote user authentication schemes using biometric data have been

proposed in the literature. However, in terms of security the majority of them are vulnerable to different malicious cryptographic attacks, which influence on the privacy of patient's medical data. In addition, these schemes result in high computational, communication, and storage costs, which cannot promote the real-time criteria. To overcome these pitfalls and those of the conventional authentication schemes cited above, a combination of both biometrics and cryptography techniques is needed. Because of the fact that biometrics and cryptography are mutually complementary and seems to be a good solution for the authentication and key generation process in mobile healthcare environments. In this chapter, we propose a new biometric-based authentication scheme for home healthcare system using mobile devices, biometric inputs and Elliptic Curve Cryptography (ECC). Our proposal combines the patient's biometric template with ECC technique to generate the key pair, which is computationally derived from that template. When a remote diagnostic is required or an unexpected incident underwent on the health of a given patient, the latter can be authenticated by the remote server without requiring to save or communicate the patient's biometric template. The security analysis and simulation results demonstrate that our proposal is appropriated for use in practical healthcare applications.

5.3 Home healthcare system model

We consider a typical architecture of home healthcare system illustrated in Figure 5.1, composed of two communication parties involved in remote patient authentication scheme. Each patient is equipped with different types of body medical sensors, which are deployed on or in his body to permanently monitor his vital signs. Owing to the short communication range of body medical sensors, patient's vital signs are periodically forwarded to a sink (e.g., personal digital assistant, smartphone, laptop computer, etc.) using short-range wireless communication techniques such as, Bluetooth, ZigBee or WLAN. Afterwards, the patient's vital signs collected by the sink are forwarded to the remote medical server at the hospital via the Internet or mobile telephone networks for further analysis. Finally, these sensitive medical data are shared among authorized users, such as clinicians, chemists, nurses, insurance companies, etc., to monitor and diagnose the registered patient.

Generally, a home healthcare system consists of five basic components [4][33][64][65][83]:

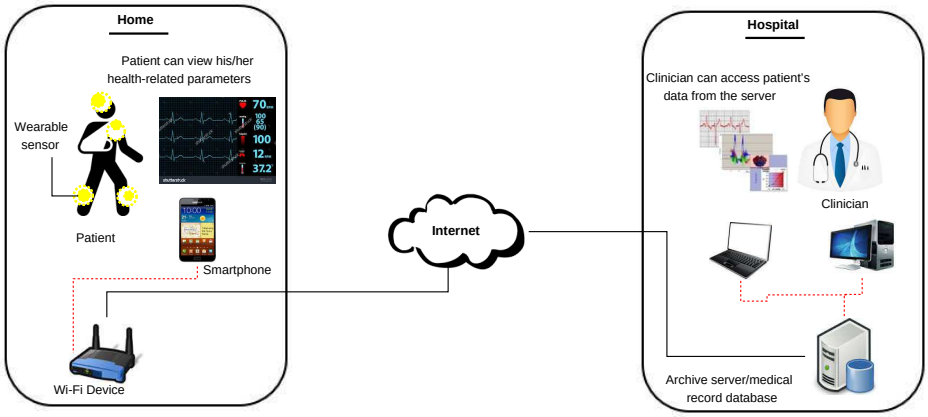


Fig. 5.1 Typical architecture of home healthcare system

1. Body medical sensors, permanently monitor the patient's vital signs, such as oxygen saturation, pulse oximeter, blood pressure, heart rate, and blood sugar, etc. Afterwards, these vital signs are forwarded to the patient's mobile device.

2. Wireless communication channel between the body medical sensors and patient's mobile device. This channel is used for secure communication of patient's vital signs captured by the different body medical sensors.

3. Patient's mobile device, which could be a personal digital assistant or a smartphone, establishes a secure communication of patient's vital signs to the remote server through wireless networks.

4. Wireless communication channel between patient's mobile device and remote server. This channel is used for secure communication of patient's vital signs collected by the patient's mobile device to the remote server using mobile telephone networks or Internet.

5. Remote server, analyses vital signs forwarded from the patient mobile device. Afterwards, this sensitive medical data is securely stored in the database of the remote server. After the storage of these medical data, various users, such as clinicians, nurses, chemists, researchers and insurance companies, can access to this data with limited permissions to monitor and diagnose patients.

5.4 The proposed scheme

In this section, we give the detailed description of our biometric-based remote patient authentication scheme between two communication parties, namely (1) the patient P_i's mobile device, which executes all the operations performed by the corresponding patient; and (2) the remote server S of home healthcare system in the hospital for collecting and managing the patient's medical information. The proposed scheme consists of three phases, namely the system initialization, the patient registration, and the mutual authentication with a session key agreement, which are described in the following subsections. Before presenting the operations of each phase, some important notations used through this paper are recapitulated in Table 5.1.

Notation	Description
P_i	The patient i
S	The remote server
ID_i	The patient P_i's identity
$\langle \widehat{K_S}, K_S \rangle$	The remote server S's private and public keys
$\langle \widehat{K_i}, K_i \rangle$	The patient P_i's private and public keys
$\langle \rangle_{K_j}$	Encryption operation using public key K_j
$E_q(a,b)$	An elliptic curve equation with order n
n	A large number
G	The base point with the order n over $E_q(a,b)$
B_i	The patient P_i's biometric template
M_i	The patient P_i's alert message
SN_i	The patient P_i's mobile device serial number
SK	Session key
H	A collision free one-way secure hash function
$\langle +, -, \cdot \rangle$	Elliptic curve point addition, subtraction and multiplication
$\|\|$	Concatenation operation
$\oplus$	Bit-wise exclusive-or (XOR) operation

Table 5.1 Notations

5.4.1 System initialization phase

This process is executed between two communication parties once at the system initialization time, to initialize and select some parameters of the system, and compute ECC key pair, which will be used by both the remote server S and patient P_i's mobile device during the registration and authentication phases. In the server side, S chooses

an elliptic curve equation $E_q(a,b)$ with order n, where n is a large number for the security considerations and selects a base point G with order n over $E_q(a,b)$. Afterwards, the remote server S chooses a number $\widehat{K_S}$ as a private key, where $\widehat{K_S} \in [1, n-1]$ and computes its corresponding public key $K_S = \langle Q_S, G \rangle$, where $Q_S = \widehat{K_S}.G$. In the patient side, the patient P_i's mobile device also computes its key pair $\langle \widehat{K_i}, K_i \rangle$ by using the biometric reader. The mobile device extracts the patient P_i's biometric template B_i from which the patient P_i's mobile device computes its own private key $\widehat{K_i} = H(B_i||r_i||SN_i)$, where r_i (such as $r_i \in [1, n-1]$) and SN_i represent a random number and the serial number of the patient P_i's mobile device, respectively. Finally, after generating the private key, the patient's mobile device derives its public key $K_i = \langle Q_i, G \rangle$, where $Q_i = \widehat{K_i}.G$. Note that it is hard to forge the patient P_i's private key $\widehat{K_i}$ from Q_i and G due to the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP).

5.4.2 Patient registration phase

This process is operated when a patient P_i attempts to register himself/herself in the system. Initially, the patient P_i freely chooses his/her identity ID_i. Then, he/she introduces his/her biometrics by using the biometric reader of the mobile device to obtain the template B_i. Afterwards, the patient's mobile device computes $A_i = H(\widehat{K_i}||ID_i)$ and sends the registration request $\langle ID_i, K_i, A_i \rangle_{K_S}$ to the remote server. Upon receiving the P_i's registration request, the remote server S decrypts the registration request message using its own private key $\widehat{K_S}$, and checks the unicity of patient's identity ID_i. If patient's identity ID_i already exists in its database, the remote server S requests the patient P_i for another identity ID_i. Otherwise, the remote server S computes some security parameters: $E_i = H(ID_i||T||\widehat{K_S})$, and $W_i = E_i \bigoplus A_i = H(ID_i||T||\widehat{K_S}) \bigoplus H(\widehat{K_i}||ID_i)$, where T denotes the current timestamp of the remote server S. Finally, the remote server S saves $\langle ID_i, W_i \rangle$ in its locally for the future authentication and sends $\langle ID_i, A_i, W_i \rangle_{K_i}$ to the patient's mobile device.

5.4.3 Mutual authentication

This process is operated when a body medical sensor of a monitored patient detects an abnormal situation in the captured vital signs. Further to an abnormal situation on patient's health, the body medical sensor triggers an alert message M_i. This alert message is automatically communicated to the patient P_i's mobile device. Following

this release of alert message, the authentication phase starts. The detailed steps of this phase are presented as follows:

- **Step-1:** Initially, the patient P_i inputs his/her identity ID_i. Then using an appropriate biometric reader, the patient P_i's introduces his/her biometrics allowing the extraction of the biometric template B_i, from which the patient P_i's mobile device computes its key pair $\langle \widehat{K}_i, K_i \rangle$. Afterwards, the patient's mobile device P_i computes $A_i' = H(\widehat{K}_i || ID_i)$, and verifies whether A_i' is equal to the already stored $A_i = H(\widehat{K}_i || ID_i)$ or not. If the two are not equal, the patient authentication process terminates immediately. Otherwise, the patient's mobile device selects a random number $r_i \in [1, n-1]$ and computes $R_i = r_i.G$, $R_i' = r_i.K_S = r_i.\widehat{K}_S.G$, $E_i = W_i \bigoplus H(\widehat{K}_i || ID_i)$, $PID_i = ID_i \bigoplus H(R_i')$, $PAM_i = M_i \bigoplus H(R_i')$, and $\theta = H(ID_i || E_i || R_i || R_i' || M_i || T_i)$, where T_i denotes the current timestamp of the mobile device. Furthermore, the patient's mobile device sends the login request message $\langle PID_i, R_i, \theta, PAM_i, T_i \rangle$ to the remote server S over an insecure channel. Finally, the patient's mobile device waits for a period of time, which depends on the type of alert message. If it does not receive any acknowledgement from the remote server S, the patient's mobile device sends back the same alert message.

- **Step-2:** After receiving $\langle PID_i, R_i, \theta, PAM_i, T_i \rangle$, the remote server S checks the timestamp validity, such as $T_S - T_i \leq \Delta T$, where T_s and ΔT denote, respectively, the current timestamp of the remote server and the expected valid time interval for a transmission delay. If it is incorrect, S rejects the login request, otherwise, the remote server S computes $R_i' = \widehat{K}_S.R_i$, and then extracts $ID_i = PID_i \bigoplus H(R_i')$, checks the validity of ID_i. If it is not valid, the remote server S rejects the login request; otherwise, the remote server S extracts the alert message $M_i = PAM_i \bigoplus H(R_i')$ then checks whether θ and $H(ID_i || E_i || R_i || R_i' || M_i || T_i)$ are equal. If they are not equal, S rejects the login request; otherwise, the remote server S authenticates the patient P_i, and then generates a random number $r_s \in [1, n-1]$, computes $R_s = r_s.G$, $R_s' = r_s.K_i = r_s.\widehat{K}_i.G$, $C_i = M_i \bigoplus H(R_s')$, and $\gamma = H(ID_i || E_i || R_s || R_s' || M_i || T_s)$, where T_s is the current timestamp of the remote server S. Afterwards, it computes the session key SK to be shared with the patient's mobile device, such as $SK = r_s.R_i = r_s.r_i.G$. Finally, the remote server S computes the response, which is an acknowledgement such as $\langle R_s, R_i, \gamma, C_i, T_s \rangle$, and sends it to the patient's mobile device.

- **Step-3:** After receiving $\langle R_s, R_i, \gamma, C_i, T_s \rangle$, the patient P_i's mobile device checks the validity of the timestamp by $T_i - T_S \leq \Delta T$. If it is incorrect, a replay attack could be suspected and then, the patient P_i's mobile device rejects the login request. Otherwise, the patient's mobile device computes $R'_s = \widehat{K_i}.R_s$, extracts $M_i = C_i \bigoplus H(R'_s)$, and then verifies the validity of alert message M_i. If the alert message verification fails, the patient's mobile device considers the remote server S as illegitimate and the authentication process terminates immediately. Otherwise, the patient P_i's mobile device checks whether γ and $H(ID_i||E_i||R_s||R'_s||M_i||T_s)$ are equal. If they are not equal, the patient P_i's mobile device rejects the login request. Otherwise, the patient P_i authenticates the remote server S and computes the common secret session key SK shared with the remote server S, such as $SK = r_i.R_s = r_i.r_s.G$. Finally, the patient P_i's mobile device computes $\delta = H(ID_i||R_i||R_s||SK)$ and sends $\langle \delta \rangle$ to the remote server S.

- **Step-4:** After receiving $\langle \delta \rangle$ from the patient P_i's mobile device, the remote server S computes $\delta' = H(ID_i||R_i||R_s||SK)$ and verifies whether the computed δ' is equal to the received δ. If the two are not equal, the remote server S rejects the login request; otherwise, the remote server S believes that the patient P_i is an authentic remote party. Finally, mutual authentication process between patient P_i's mobile device and remote server S is completed successfully. Therefore, the computed secret session key SK can be used by the two communication parties for their confidential future communication.

5.5 Security analysis

In this section, we analyse the security of our proposed scheme by showing its resistance to various malicious attacks as described below. Table 5.2 summarizes the overall security analysis of our proposed scheme compared with the existing solutions.

- *Replay attack:* assume that an adversary intercepts the login request $\langle PID_i, R_i, \theta, PAM_i, T_i \rangle$ sent out from the patient P_i's mobile device to the remote server S and tries to impersonate the legitimate patient P_i. If the adversary replays the same intercepted request, the remote server S could obviously detect the attack by checking the validity of $T_S - T_i \leq \Delta T$. If it is incorrect, the adversary will not be considered as legitimate patient, therefore, the remote server S will reject the login request. Inversely, the adversary cannot impersonate the legitimate remote server S just by replaying the intercepted login request

$\langle R_s, R_i, \gamma, C_i, T_s \rangle$ to the patient P_i's mobile device, because the later can easily detect the attack by checking the validity of $T_i - T_S \leq \Delta T$. In addition, the remote server S can easily detect the forged request by checking the correctness of $\delta = H(ID_i||R_i||R_s||SK)$ in the fourth step of the authentication phase since both R_i and R_s will be frequently changed in each session. Therefore, we conclude that our proposed scheme can provide the security against replay attack.

- *Impersonation attack:* assume that an adversary intercepts a valid login request message sent out from the patient P_i's mobile device $\langle PID_i, R_i, \theta, PAM_i, T_i \rangle$ or from the remote server $\langle R_s, R_i, \gamma, C_i, T_s \rangle$ of previous sessions of the protocol. However, the adversary has no way to create a forged request message for the fresh timestamps T_i and T_S without knowing the patient and server private keys ($\widehat{K_i}$, $\widehat{K_S}$). Conversely, the adversary cannot impersonate both the patient P_i's mobile device and the remote server S without knowing $\widehat{K_i}$ and $\widehat{K_S}$. Therefore, we conclude that our proposed scheme can resist against impersonation attack.

- *Server spoofing attack:* assume that an adversary intercepts the request message $\langle PID_i, R_i, \theta, PAM_i, T_i \rangle$ of a previous sessions of the protocol and attempt to masquerade as the remote server S to discover the patient's long-term secret. However, it is impossible for an adversary to extract the original identity ID_i from PID_i, and the patient P_i's alert message M_i from PAM_i without holding server S's private key $\widehat{K_S}$. In addition, it is also not possible to forge a valid login request message $\langle R_s, R_i, \gamma, C_i, T_s \rangle$ without server S's private key $\widehat{K_S}$ and E_i. Consequently, the adversary cannot get success in Step-2 of the authentication phase. Therefore, we conclude that our proposed scheme has the ability to successfully prevent the server spoofing attack.

- *Attack against anonymity:* assume that an adversary intercepts the login request message $\langle PID_i, R_i, \theta, PAM_i, T_i \rangle$ sent out from the patient P_i to the remote server S. However, the adversary is unable to figure out the original patient's identity ID_i from $PID_i = ID_i \bigoplus H(R_i')$. For the reason that to extract the original patient's identity ID_i, the adversary has to compute R_i' using R_i and K_S. However, it computationally impossible due to difficulties of the computational Diffie-Hellman problem (CDHP). Therefore, we conclude that our proposed scheme preserves thoroughly the patient anonymity and the original patient's identity ID_i cannot be known anymore.

- *Insider attack:* in our scheme, the patient P_i's registers himself to the remote server S by sending $\langle ID_i, K_i, A_i \rangle_{K_S}$. Since $\langle ID_i, K_i, A_i \rangle$ is encrypted by the server S's private key $\widehat{K_S}$, the privileged-insider is unable to figure out A_i from the bloc $\langle ID_i, K_i, A_i \rangle_{K_S}$ without server S's private key. In addition, he cannot obtain $\widehat{K_i}$ from $A_i = H(\widehat{K_i}||ID_i)$ due to the one-way property of the hash function. Hence, the privileged-insider who is unable to authenticate himself to the remote server S, cannot impersonate the legal patient to access the remote server S without holding patient P_i's private key $\widehat{K_i}$. Therefore, we conclude that our proposed scheme can resist the privileged-insider attack.

- *Man-in-the-middle attack:* assume that an adversary who is in the middle of patient P_i's mobile device and remote server S attempts to masquerade both mobile device and remote server by creating a fake login request message for authentication. However, the adversary cannot successed this type of attack because he/she cannot create a valid login request message without knowing some secret parameters. As a result, we conclude that our proposed scheme can resist the man-in-the-middle attack.

- *Physical attack:* assume that an adversary intercepts the login request message $\langle PID_i, R_i, \theta, PAM_i, T_i \rangle$ sent out from the patient P_i's mobile device. Then, the adversary modifies the intercepted message and sends it to the remote server S. However, this attack cannot successed because the remote server S can easily detect the attack by verifying the correctness of θ. Inversely, the patient P_i's mobile device can detect the attack just by verifying the validity of the communicated messages. Therefore, we conclude that our proposed scheme provides security against physical attack.

- *Parallel session attack:* assume that an adversary intercepts the login message $\langle PID_i, R_i, \theta, PAM_i, T_i \rangle$ sent out from the patient's mobile device. Then, it tries to put the mobile device offside and initiate one or more sessions simultaneously with the remote server, by sending it the intercepted message. The adversary passes the server verification test in step 2, so the server responds with $\langle R_s, R_i, \gamma, C_i, T_s \rangle$ to the adversary. However, in step 3 the latter cannot compute the same session key $SK = r_i.R_s = r_i.r_s.G$ already computed in the server side because it does not know r_i. As a result, we conclude that our proposed scheme resists against this type of attack.

- *Reflection and denial of service attack:* assume that an adversary steals or finds a patient P_i's mobile device. Then, he/she attempts to modify wrong verification information of a valid patient inside the lost or stolen mobile device. However, the adversary cannot access the lost or stolen mobile device without being able to introduce a valid biometric template B_i and without a real identity ID_i. Consequently, the adversary is unable to replace or modify patient's security parameters inside a lost or stolen mobile device. Moreover, in our proposed scheme, the patient P_i's mobile device will be locked if the login attempts number with wrong identity ID_i and/or wrong patient's biometric template B_i reaches the predefined value. Therefore, we conclude that our proposed scheme has the capability to withstand the reflection and denial of service attack.

Security requirements	**Schemes**			
	Lu et al. [71]	Arshad and Nikooghadam [8]	Tan [113]	Our scheme
Replay attack	✓	✓	✗	✓
Impersonation attack	✓	✗	✓	✓
Server spoofing attack	✓	✗	✓	✓
Attack against anonymity	✓	✓	✓	✓
Insider attack	✓	✓	✓	✓
Man-in-the-middle attack	✓	✓	✓	✓
Physical attack	✓	✓	✓	✓
Parallel session attack	✓	✓	✓	✓
Reflection attack	✗	✓	✗	✓
Denial of service attack	✗	✓	✗	✓

Table 5.2 Security analysis (✓: prevent the attack, ✗: do not prevent the attack)

5.6 Performance evaluation

In this section, we provide the simulation results comparing our proposed scheme, with three latest biometrics-based authentication schemes for tele-care medicine information systems, that is, Tan's scheme [113], Arshad and Nikooghadam's scheme [8], and Lu et al.'s scheme [71]. The simulations of our proposed scheme and other concurrent schemes [113], [8] and [71] are developed on a Samsung Galaxy $S6$ smartphone with the following system configuration of processor speed of 2.1 GHz, RAM rate of 3 Go, capacity of memory card of 32 Go, and a wireless transmission rate of 5.76 Mbps. The smartphone interacts with a remote server machine characterized by a processing rate of 2.3 GHz, a memory of 4 Go, hard-disk capacity of 260 Go, and a wireless transmission rate of 54 Mbps. Before given the simulation results, we firstly start, by specifying the three major metrics that we have considered to be interesting to study: (1) the communication cost, which represents total number of packet sent out from patient's mobile device or remote server machine S per session of authentication, (2) the processing time, which represents the required time involved in the execution of a scheme per session of authentication, and (3) the storage cost, which represents the memory space required for the system parameters which are required to be stored per session of authentication. We evaluated these metrics following different elliptic curve cryptography key size: P-160, P-192, P-224, and P-256.

Figure 5.2 and 5.3, show the obtained results for the communication cost, respectively, in mobile device and remote server side. As expected, the communication overhead increases for both our proposal and for all the compared schemes when the ECC key size increases. From the Figure 5.2 and 5.3, it is clear that the performance of our proposal is very higher than the other schemes. Indeed, our proposal require 5 message exchanges, while Tan's scheme [113] require 4 exchanges, achieving better results compared to the schemes of Lu et al. [71], and Arshad and Nikooghadam [8] which require 5 exchanges.

Figure 5.4 and 5.5, show the obtained results for the processing time, respectively, in mobile device and remote server side. As expected, the processing time increases for both our proposal and for all the compared schemes when the ECC key size increases. From the Figure 5.4 and 5.5, it is clear that the performance of our proposal is very higher than the other schemes. In fact, our scheme performs the mutual authentication process in three rounds of communication. During the registration and authentication phases, both mobile device and remote server perform less number of hash and ECC operations, while the other schemes perform an important number of hash and ECC operations, which are necessarily required to achieve the authentication process.

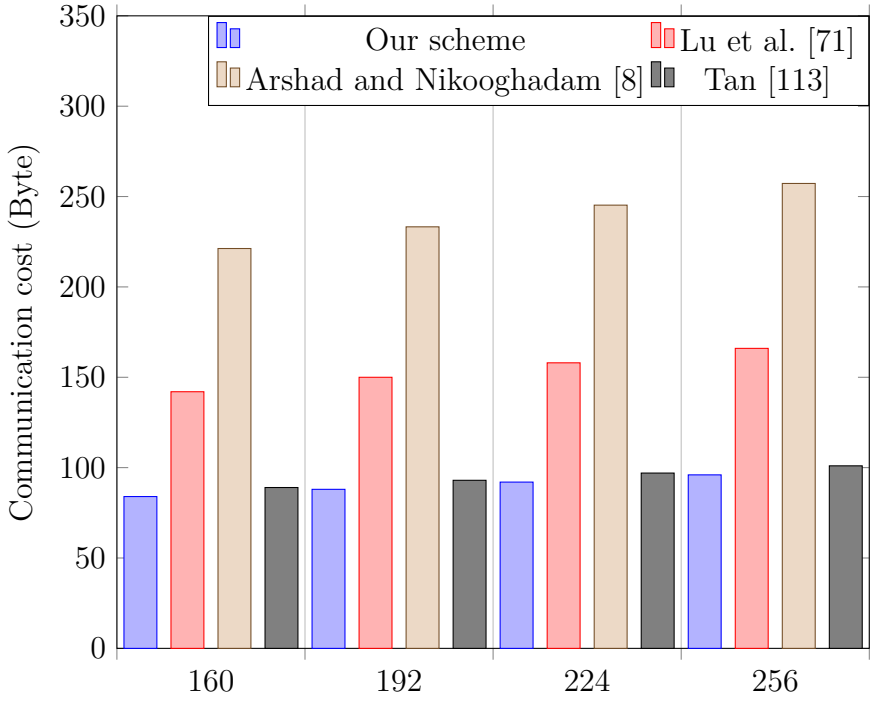


Fig. 5.2 Communication cost evaluation in the mobile device side per session of authentication

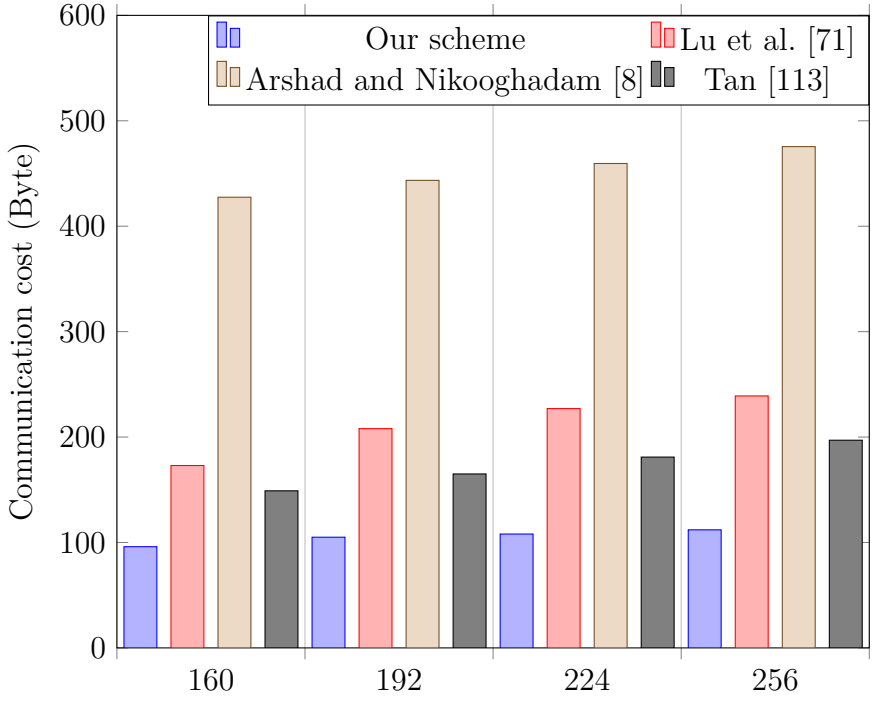


Fig. 5.3 Communication cost evaluation in the remote server side per session of authentication

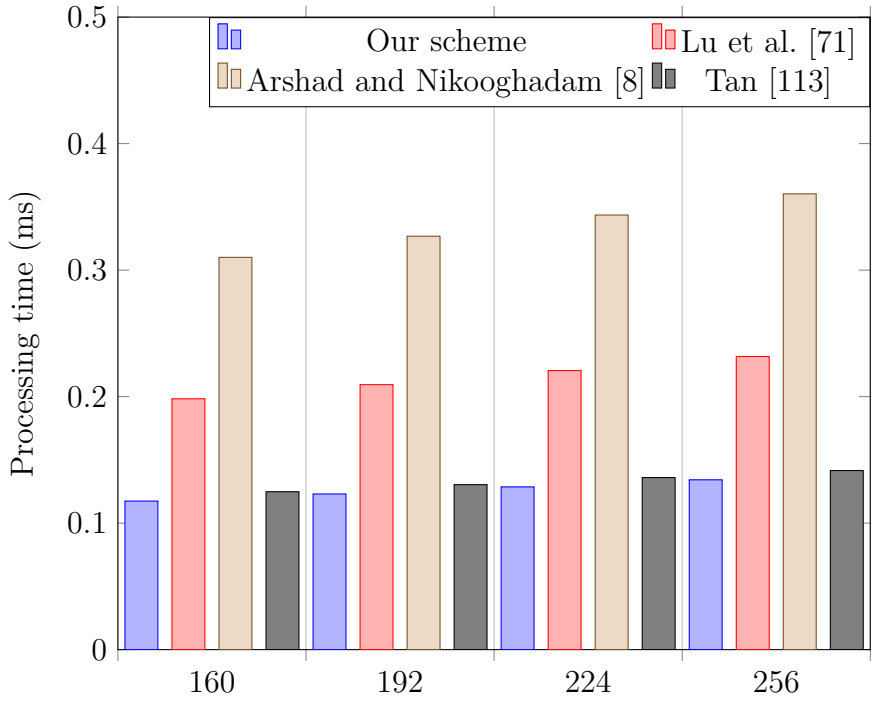
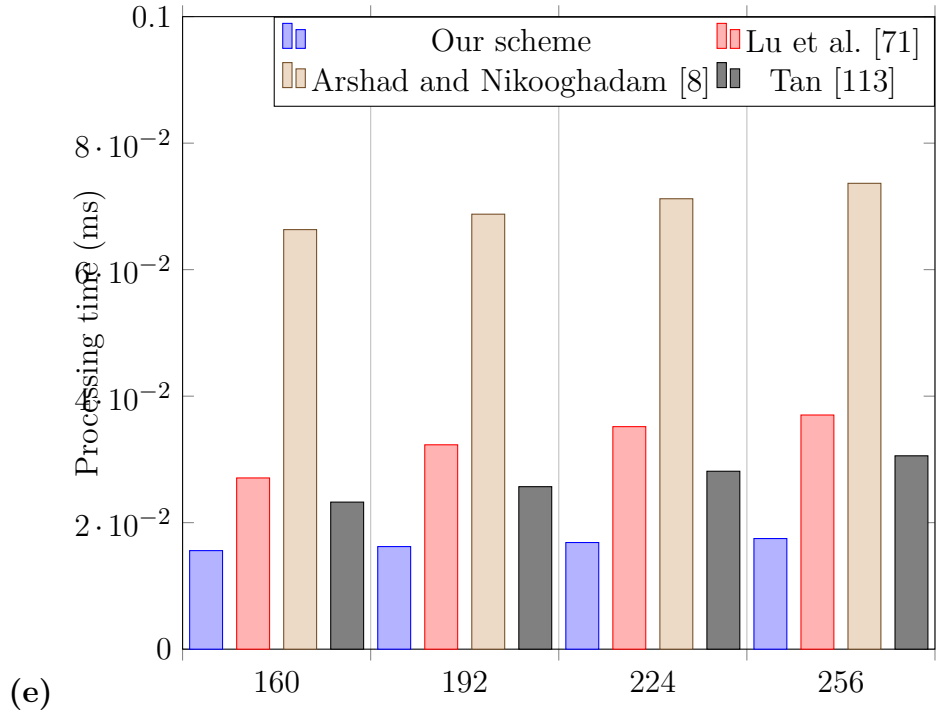


Fig. 5.4 Processing time evaluation in the mobile device side per session of authentication



(e)

Fig. 5.5 Processing time evaluation in the remote server side per session of authentication

Figure 5.6 and 5.7, show the obtained results for the storage cost, respectively, in mobile device and remote server side. Obviously, when the ECC key size increases, it is expected that the storage cost respectively, in mobile device and remote server side increases for our proposal and for all the compared schemes. The results indicate that the performance of our proposal is very higher than the other schemes. In the case of our scheme, there is one and two cryptographic parameters stored per one patient, respectively, in patient's mobile device and remote server side, and all the other parameters and keys are dynamically computed. In the case of the other schemes, there are many cryptographic parameters, which are required to be stored in both mobile device and remote server side for the future authentication process.

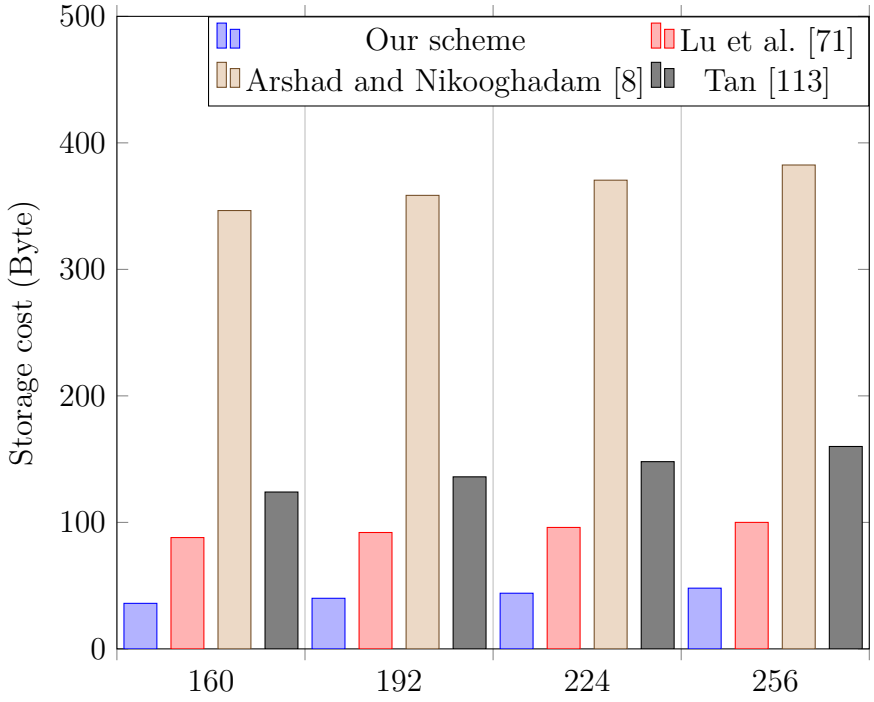


Fig. 5.6 Storage cost evaluation in the mobile device side per session of authentication

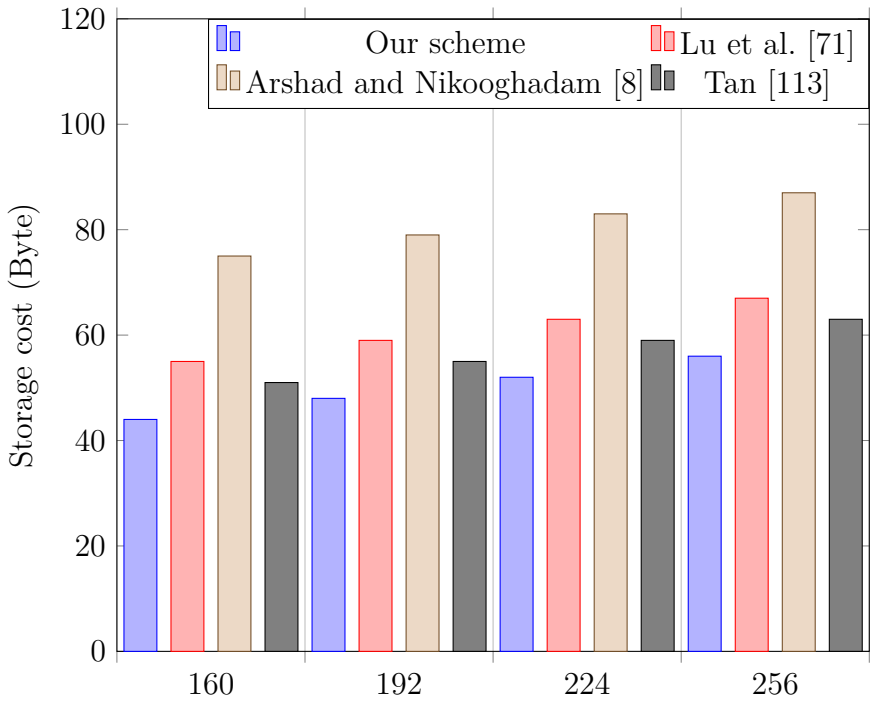


Fig. 5.7 Storage cost evaluation in the remote server side per session of authentication

5.7 Conclusion

The home healthcare system provides medical service to patients in their own homes without visiting the hospital. This type of system offers great rapidness for clinicians, chemists, nurses, and patient in medical service. However, access to patient's vital signs or receive remote medical treatment using wireless interfaces, can directly put patient's life in danger. Therefore, it is more important to secure these critical data exchanged among the two communication parties. In this chapter, we have proposed a biometric-based remote patient authentication scheme, allowing the secure exchange of critical data between communication parties in home healthcare systems. This proposal properly combines the patient's biometric template with elliptic curve cryptography techniques to produce an ECC key pair, which is computationally derived from that template. Indeed, the two communication parties, namely the patient, and remote server authenticate each other and perform mutual authentication without requiring to save or communicate patient's biometric template, which allows to guarantee the respect for the patient's privacy. We have evaluated the performance of our scheme by comparing it with concurrent ones by varying the elliptic curve cryptography key size. This comparison done is based on three performance criteria such as communication

cost, processing time, and storage cost. The security and performance analysis indicate that our scheme achieves better security than other concurrent ones, with lower storage, communication and calculation costs. This allows it to be extremely appropriate, especially for practical applications in mobile healthcare environments.

Conclusion and future works

The recent advances in microelectronics and wireless communications have resulted in the emergence of electronic components, which currently acquire an increasingly important place in daily lives of patients attained by chronic diseases. These electronic components have become an essential elements of these patients as tools of assistance, monitoring, communication, information, etc. This technological advance is one factor among others which has also allowed the design and implementation of a mobile healthcare system. This has greatly facilitated the provision of both patients and medical workers with a multitude of accessible medical services whenever and wherever. The most important characteristics of mobile healthcare environments lies in their capability to remotely, continuously, and automatically monitor the patient's health. However, these systems are still at the early stage of their development, and many research challenges must be overcome so that they can be widely accepted by the main actors of this environment. Consequently, one of the main challenges to be raised in these systems consists in contributing to enhance the security of the exchanges data between the communication parties, while proposing an authentication system between them. The transactions of authenticated medical data are the paramount requirements for this type of system. Because the failure to obtain correct medical data can deprive the patient to be diagnosed and treated in a correct and effective manner. Obviously, transactions between the communication parties must be encrypted to protect not only the patient's private life, but also to not put his/her health in danger. For this reason, the medical staff who gather the patient's data must be sure of the integrity of the latter, as well as from where they originate. In the framework of the work described in this thesis, the purpose was the proposal of new biometric-based authentication schemes in mobile healthcare environments. The main motivation, which is governed this thesis work was the proposal of security solutions adapted to the new medical management architectures, taking into account of its constraints, meeting their specific needs in terms of security services and centered on the application requirements.

In the first part of this thesis, we gave a general overview of health monitoring systems, describing their characteristics, application fields, architectures, as well as their design factors. Thereafter, we have devoted the rest of the chapter to the study of biometrics and security in healthcare.

In the second part of this thesis, we have provided a state of the art on the authentication schemes in healthcare environments, where we have classified, surveyed and compared them. In this context, we have proposed a new taxonomy of schemes depending on orientation of the authentication service and the considered network architecture. Afterwards, we have described the main operations of each reviewed scheme, while discussing their perks and flaws. Through the latter, we have drawn up a comparative table according to different relevant criteria such as security level, processing time, computation cost, storage cost, etc.

In the third part of this thesis, we have presented our first contribution, which is a biometric-based remote patient authentication scheme for mobile healthcare environments. The proposed scheme translates the patient's biometric data into ECC key pairs. When a remote diagnosis is required or an unexpected incident underwent on the patient's health, the patient can be authenticated in a secure and cost-effective manner without the need to register or communicate his biometric template. In order to validate this proposal, we have implemented this scheme under JAVA programming language to measure its reliability in terms of communication cost, processing time, and storage cost. In all the simulation tests, the obtained results are not only encouraging, but also favorable in the side of our scheme compared to the concurrent ones. Through the security analysis, we have also demonstrated the robustness and resistance of our scheme against various types of malicious cryptographic attacks.

In the fourth part of this thesis, we have presented our second contribution, which is an authentication scheme based on electrocardiogram (ECG) signals for Medical Body Area Sensor Networks. This approach allows to address the issue of extracting biometric features. Indeed, we have proposed a new method which ensures the extraction, with great precision, the features based on the ECG signals and makes the authentication between the sensors more suitable. The proposed approach has been validated experimentally. On the one hand, in view of the performances obtained by simulations, showing the considerable reduction in processing time, energy consumed and memory space thanks to the efficiency of our method of extracting biometric features. Besides, our second contribution is characterized by lower False Rejection Rate and False Acceptance Rate than Enhanced FFT, while guaranteeing a shorter measurement time of the ECG signal. On the other hand, the security analysis of this

scheme allowed us to demonstrate its robustness and high security level against various types of known cryptographic attacks.

In the fifth part of this thesis, we have presented our third contribution, which is an authentication scheme for the remote patient in the home healthcare system. This scheme is a combination of both the biometrics and ECC (Elliptic Curve Cryptography), which is a good mechanism for ensuring the security of patient-related data. Through this proposal two communication parties, namely the mobile device and remote server could be mutually authenticated in public mobile healthcare environments. The simulation scenarios carried out and the comparative results of this scheme with other concurrent ones have indicated the adaptability of this scheme for use in practical healthcare applications, while providing a compromise between security and efficiency.

Our future work will focus on solving the problem of fingerprint variability, which reduces the accuracy of the authentication process. Indeed, sometimes the acquisition of the fingerprint can generate false identification values. This is due to external factors of the system, which mainly depend on how the finger is placed on the biometric reader or simply due to its humidity degree. The generation of a false biometric template generates a wrong cryptographic key, which implies a rejection of this user by the processing server despite its legitimacy. We have thought about a beginning of a method, which can solve this issue, but this method needs to be studied more. The basic principle of this method is to study the degree of variability for a user and link the entire range of possible values to his fingerprint. This will be very beneficial when comparing two fingerprints because the identification will focus on more than a hundred feature points. Considering all of the above, this idea can solve the false rejection issue with the proviso that the value range does not overlap with a variation range of another user. Another area of research will be centered on the improvement of the extraction method of ECG physiological signal features. We believe that a method using different physiological signals (e.g., PPG, EMG, EEG, etc.) or a combination of them and more efficient key exchange algorithms would be interesting to study. Finally, we also plan to extend our work as part of the implementation of our authentication schemes on experimental platforms.

References

[1] Akrouf, S. (2011). *Une approche multimodale pour l'identification du locuteur*. PhD thesis, Ferhat Abbas university-Setif, Department of Computer Science.

[2] Al-Ghamdi, B. (2015). *Etude des méthodes d'ordonnancement sur les réseaux de capteurs sans fil*. PhD thesis, Champagne-Ardenne university-Reims.

[3] Alemdar, H. and Ersoy, C. (2010). Wireless sensor networks for healthcare: A survey. *Computer Networks*, 54(15):2688–2710.

[4] Ameen, M., Liu, J., and Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, 36(1):93–101.

[5] Andalib, A. and Abdulla-Al-Shami, M. (2013). A novel key generation scheme for biometric cryptosystems using fingerprint minutiae. *In: Proceedings of the International Conference on Informatics, Electronics and Vision*, pages 1–6.

[6] Anoop, M. (2007). Elliptic curve cryptography – an implementation tutorial. Technical report, Tata Elxsi Ltd, Thiruvananthapuram, India.

[7] Aqsa, M., Junaid, Q., Basharat, A., Kok-Lim, A., and Ubaid, U. (2015). Qos in ieee 802.11-based wireless networks: a contemporary review. *Journal of Network and Computer Applications*, 55:24–46.

[8] Arshad, H. and Nikooghadam, M. (2014). Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems. *Journal of Medical Systems*, 38(12):1–12.

[9] Awasthi, A. and Srivastava, K. (2013). A biometric authentication scheme for telecare medicine information systems with nonce. *Journal of Medical Systems*, 37(5):1–4.

[10] Bao, S., Shen, L., and Zhang, Y. (2004). A novel key distribution of body area networks for telemedicine. *In: Proceedings of the International Workshop on Biomedical Circuits and Systems*, pages 1– 17–20a.

[11] Bao, S., Zhang, Y., and Shen, L. (2005a). A new symmetric cryptosystem of body area sensor networks for telemedicine. *In: Proceedings of the* 6^{th} *Asian-Pacific Conference on Medical and Biological Engineering.*

[12] Bao, S., Zhang, Y., and Shen, L. (2005b). Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. *In: Proceedings of the* 27^{th} *Annual International Conference of the Engineering in Medicine and Biology Society*, pages 2455–2458.

[13] Barakah, D. and Ammad-uddin, M. (2012). Survey of challenges and applications of wireless body area network (wban) and role of a virtual doctor server in existing architecture. *In: Proceedings of the* 3^{rd} *International Conference on Intelligent Systems Modelling and Simulation*, pages 214–219.

[14] Barman, S., Samanta, D., and Chattopadhyay, S. (2015). Revocable key generation from irrevocable biometric data for symmetric cryptography. *In: Proceedings of the* 3^{th} *IEEE International Conference on Computer, Communication, Control and Information Technology*, pages 1–4.

[15] Bayometric. Lumidigm m301 multispectral fingerprint scanner. https://www.bayometric.com/fingerprint-scanner-lumidigm-mercury-m301-m30x-sensor/. Accessed 26 Aug 2017.

[16] Bayometric. Suprema biomini usb fingerprint reader/scanner. https://www.bayometric.com/suprema-biomini-biometric-usb-fingerprint-reader-scanner/. Accessed 26 Aug 2017.

[17] Bayometric. Zvetco verifi p5100. http://www.neurotechnology.com/fingerprint-scanner-zvetco-verifi-p5100.html. Accessed 26 Aug 2017.

[18] Belguechi, R., Le-goff, T., Cherrier, E., and Rosenberger, C. (2011). Study of the robustness of a cancelable biometric system. *In: Proceedings of the Conference on Network and Information Systems Security*, pages 1–7.

[19] Benchennane, I. (2016). *Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus*. PhD thesis, Mohamed Boudiaf university-Oran, Department of Electronics.

[20] Benkhaira, S. (2010). Systèmes multimodaux pour l'identification et l'authentification biométrique. Magister thesis, 20 August 1955 university-Skikda, Department of Computer Science.

[21] Blahut, R. (1983). *Theory and practice of error control codes*. Massachusetts: Addison – Wesley Publishing Company, Inc.

[22] Bo, Y., Aidong, S., and Wenzheng, Z. (2009). A fully robust fuzzy extractor. *In: Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pages 392–395.

[23] Bolle, R., Connel, J., and Ratha, N. (2002). Biometric perils and patches. *Pattern Recognition*, 35(12):2727–2738.

[24] Boudjellal, S. (2006). Détection et identification de personne par méthode biométrique. Magister thesis, Mouloud Mammeri university-Tizi-Ouzou, Department of Electronics.

[25] Boukraa, F. (2016). Caractéristiques biométrique pour l'identification. Magister thesis, Ahmed Ben Bella university-Oran, Department of Computer Science.

[26] Boyen, X., Dodis, Y., Katz, J., Ostrovsky, R., and Smith, A. (2005). Secure remote authentication using biometric data. *In: Proceedings of the* 24^{th} *Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT: Advances in Cryptology, Part of the Lecture Notes in Computer Science book series*, 3494:147–163.

[27] Bradai, N., Chaari, L., and Kamoun, L. (2011). A comprehensive overview of wireless body area networks (wban). *International Journal of E-Health and Medical Communications*, 2(3):1–30.

[28] Burrows, M., Abadi, M., and Needham, R. (1990). A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36.

[29] Campbell, A., Eisenman, S., Lane, N., Miluzzo, E., Peterson, R., Lu, H., Zheng, X., Musolesi, M., Fodor, K., and Ahn, G. (2008). The rise of people-centric sensing. *IEEE Internet Computing*, 12(4):12–21.

[30] Chaari, A. (2009). *Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée*. PhD thesis, Evry Val d'Essonne university, UFR Science and Technology.

[31] Chantaf, S. (2011). *Biométrie par signaux physiologiques*. PhD thesis, Paris-Est Creteil university, Science and Technology UFR.

[32] Chatterjee, G. and Somkuwar, A. (2008). Design analysis of wireless sensors in ban for stress monitoring of fighter pilots. *In: Proceedings of the* 16^{th} *IEEE International Conference on Networks*, pages 1–6.

[33] Chatterjee, S., Das, A., and Sing, J. (2013). A novel and efficient user access control scheme for wireless body area sensor networks. *Journal of King Saud University Computer and Information Sciences*, 26(2):181–201.

[34] Chen, C., Lee, C., and Hsu, C. (2012). Mobile device integration of a fingerprint biometric remote authentication scheme. *International Journal of Communication Systems*, 25(5):585–597.

[35] Chen, M. and Gonzalez-Valenzuela, S. (2010). Body area networks: A survey. *Mobile Networks and Applications*, 16(2):171–193.

[36] Chien, H., Jan, J., and Tseng, Y. (2002). An efficient and practical solution to remote authentication: smart card. *Computer & Security*, 21(4):372–375.

[37] Chu, M., Iguchi, S., Takahashi, D., Arakawa, T., Kudo, H., and Mitsubayash, K. (2009). Wearable biosensor for monitoring tear glucose on rabbit eye as novel device of body sensor network. *In: Proceedings of the* 5^{th} *International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pages 191–194.

[38] Chuang, M. and Chen, M. (2014). An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. *Expert Systems with Applications*, 41(4):1411–1418.

[39] Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., and Vercauteren, F. (2005). *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman and Hall/CRC Boca Raton, FL.

[40] Darwish, A. and Hassanien, A. (2011). Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors*, 11(6):5561–5595.

[41] Dave, K. (2013). Brute-force attack seeking but distressing. *International Journal of Innovations in Engineering and Technology*, 2(3):75–78.

[42] Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE Transactions in Information Theory*, 22(6):644–654.

[43] Elgazzar, K., Aboelfotoh, M., Martin, P., and Hassanein, H. (2012). Ubiquitous health monitoring using mobile web services. *Procedia Computer Science*, 10:332–339.

[44] Guoan, B. and Yonghong, Z. (2004). *Transforms and fast algorithms for signal analysis and representations*. Birkhäuser Basel.

[45] Hankerson, D., Menezes, A., and Vanstone, S. (2004). *Guide to elliptic curve cryptography*. Series Title: Springer Professional Computing. Springer-Verlag.

[46] He, D. and Wang, D. (2015). Robust biometrics-based authentication scheme for multiserver environment. *IEEE Systems Journal*, 9(3):816–823.

[47] Hidano, S., Ohki, T., Komatsu, N., and Kasahara, M. (2008). On biometric encryption using fingerprint and it's security evaluation. *In: Proceedings of the* 10^{th} *International Conference on Control, Automation, Robotics and Vision*, pages 950–956.

[48] Hong, L., Wan, Y., and Jain, A. (1998). Fingerprint image enhancement: algorithms and performance evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(8):777–789.

[49] Hoyt, R. (2008). Sparnet– spartan data network for real-time physiological status monitoring. *U.S. Army Telemedicine Partnership Series 2008: "Personal Health Monitoring"*, pages 1–27.

[50] Hu, C., Cheng, X., Zhang, F., Wu, D., Liao, X., and Chen, D. (2013). Opfka: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. *In: Proceedings of the* 32^{nd} *IEEE International Conference on Computer Communications*, pages 2275–2282.

[51] Hung, X., Khalid, M., and Sankar, R. (2011). An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare. *Journal of Networks*, 6(3):355–364.

[52] Jammali, N. and Fourati, L. (2015). Pfka : A physiological feature based key agreement for wireless body area network. *In: Proceedings of IEEE International Conference on Wireless Networks and Mobile Communications*, pages 1–8.

[53] Jin, Q., Jeon, W., Lee, C., Choi, Y., and Won, D. (2013). Fingerprint-based user authentication scheme for home healthcare system. *In: Proceedings of the* 5^{th} *International Conference on Ubiquitous and Future Networks*, pages 178–183.

[54] Jung, J., Kang, D., Lee, D., and Won, D. (2017). An improved and secure anonymous biometric-based user authentication with key agreement scheme for the integrated epr information system. *PLoS One*, 12(1):e0169414.

[55] Khan, M., Jiashu, Z., and Wang, X. (2008). Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. *Chaos, Solitons and Fractals*, 35(3):519–524.

[56] Khan, M., Kumari, S., and Gupta, M. (2014). More efficient key-hash based fingerprint remote authentication scheme using mobile device. *Computing*, 96(9):793–816.

[57] Kim, H., Jeon, W., Lee, K., Lee, Y., and Won, D. (2012). Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme. *In: Proceedings of the International Conference on Computer Science, Applied Mathematics and Applications*, pages 391–406.

[58] Knott, G. (2000). *Interpolating cubic splines. Series title Progress in Computer Science and Applied Logic*. Birkhäuser Basel.

[59] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48:203–209.

[60] Kocsis, O., Vasilopoulou, M., Tsopanoglou, A., Papaioannou, A., and Vogiatzis, I. (2015). Telemonitoring system for home rehabilitation of patients with copd. *In: Proceedings of the* 5^{th} *IEEE International Conference on E-Health and Bioengineering*, pages 1–4.

[61] Kumar, P. and Lee, H. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors*, 12(1):55–91.

[62] Kumari, S., Karuppiah, M., Das, A., Li, X., Wu, F., and Gupta, V. (2017). Design of a secure anonymity preserving authentication scheme for session initiation protocol using elliptic curve cryptography. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–11.

[63] Lalithamani, N. and Soman, K. (2009). An effective scheme for generating irrevocable cryptographic key from cancelable fingerprint templates. *International Journal of Computer Science and Network Security*, 9(3):183–193.

[64] Lee, C., Lee, K., Kim, S., and Won, D. (2011a). Analysis on vulnerability of home healthcare medical devices and development of protection profile based on common criteria version 3.1. *In: Proceedings of the* 1^{st} *ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering*, pages 240–247.

[65] Lee, C., Won, D., and Park, N. (2011b). A study on the secure home healthcare wireless service. *Future Generation Information Technology*, pages 277–248.

[66] Leu, F., Ko, C., You, I., Choo, K., and Ho, C. (2017). A smartphone-based wearable sensors for monitoring real-time physiological data. *Computers and Electrical Engineering*, pages 1–17.

[67] Li, C., Lee, C., and Weng, C. (2014). A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. *Journal of Medical Systems*, 38(9):1–11.

[68] Li, C., Weng, C., Lee, C., and Wang, C. (2015). A hash based remote user authentication and authenticated key agreement scheme for the integrated epr information system. *Journal of medical systems*, 39(144):1–11.

[69] Li, M., Lou, W., and Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, 17(1):51–58.

[70] Limbasiya, T. and Doshi, N. (2017). An analytical study of biometric based remote user authentication schemes using smart cards. *Computers and Electrical Engineering*, 59:305–321.

[71] Lu, Y., Li, L., Peng, H., and Yang, Y. (2015a). An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. *Journal of Medical Systems*, 39(3):1–8.

[72] Lu, Y., Li, L., Peng, H., and Yang, Y. (2016). A secure and efficient mutual authentication scheme for session initiation protocol. *Peer-to-Peer Networking and Applications*, 9(2):449–459.

[73] Lu, Y., Li, L., Yang, X., and Yang, Y. (2015b). Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. *PLoS One*, 10(5):e0126323.

[74] Lupu, T. (2009). Main types of attacks in wireless sensor networks. *In: Proceedings of the* 9^{th} *WSEAS International Conference on Signal, Speech and Image Processing and* 9^{th} *WSEAS International Conference on Multimedia, Internet & Video Technologies*, pages 180–185.

[75] Maltoni, D., Maio, D., Jain, A., and Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer-Verlag London.

[76] Martinez, A., Schoenig, S., Andresen, D., and Warren, S. (2006). Ingestible pill for heart rate and core temperature measurement in cattle. *In: Proceedings of the* 28^{th} *International Conference of the IEEE on Engineering in Medicine and Biology Society*, pages 3190–3193.

[77] Mastali, N. and Agbinya, J. (2010). Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile computing: A survey paper. *In: Proceedings of the* 5^{th} *International Conference on Broadband and Biomedical Communications*, pages 1–6.

[78] Matyas, V. and Riha, Z. (2003). Toward reliable user authentication through biometrics. *IEEE Security and Privacy*, 1(3):45–49.

[79] Messerges, T., Dabbish, E., and Sloan, R. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, 51(5):541–552.

[80] Miller, V. (1986). Uses of elliptic curves in cryptography. *In: proceedings of the Conference on the Theory and Application of Cryptographic Techniques CRYPTO 1985: Advances in Cryptology — CRYPTO '85, Springer Verlag LNCS 218*, pages 417–426.

[81] Minutolo, A., Esposito, M., and Pietro, G. D. (2016). An hybrid reasoning system for mobile and intelligent health services. *In: Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*.

[82] Mishra, D., Das, A., and Mukhopadhyay, S. (2014). A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. *Expert Systems with Applications*, 41(18):8129–8143.

[83] Moganeshwaran, R., Hani, M., and Suhaini, M. (2012). Fingerprint-fingervein multimodal biometric authentication system in field programmable gate array. *IEEE, International Conference on Circuits and Systems*, pages 237–242.

[84] Mohammedi, M., Omar, M., Aitabdelmalek, W., Mansouri, A., and Bouabdallah, A. (2018). Secure and lightweight biometric-based remote patient authentication scheme for home healthcare systems. *In: Proceedings of the* 13^{th} *International Symposium on Programming and Systems- ISPS'2018*, pages 81–86.

[85] Mohammedi, M., Omar, M., and Bouabdallah, A. (2017). Secure and lightweight remote patient authentication scheme with biometric inputs for mobile healthcare environments. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–13.

[86] Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., and Jamalipour, A. (2014). Wireless body area networks: A survey. *IEEE Communications Surveys & Tutorials*, 16(3):1658–1686.

[87] Nadeem, A., Hussain, M., Owais, O., Salam, A., Iqbal, S., and Ahsan, K. (2015). Application specific study, analysis and classification of body area wireless sensor network applications. *Computer Networks*, 83(4):363–380.

[88] Neves, P., Stachyra, M., and Rodrigues, J. (2008). Application of wireless sensor networks to healthcare promotion. *Journal of communications software and systems*, 4(3):181–190.

[89] Newsome, J., Shi, E., Song, D., and Perring, A. (2004). The sybil attack in sensor networks: analysis and defenses. *In: Proceedings of the* 3^{rd} *International Symposium on Information Processing in Sensor Networks*, pages 259–268.

[90] Ng, H., Sim, M., and Tan, C. (2006). Security issues of wireless sensor networks in healthcare applications. *BT Technology Journal*, 24(2):138–144.

[91] Noury, N., Fleury, A., Nocuaa, R., Poujaud, J., Gehin, C., Dittmar, A., Delhommea, G., Demongeot, J., and McAdama, E. (2009). e-health sensors. biomedical sensors, algorithms and sensors networks. *IRBM*, 30(3):93–103.

[92] Ntouni, G., Lioumpas, A., and Nikita, K. (2014). Reliable and energy efficient communications for wireless biomedical implant systems. *IEEE journal of biomedical and health informatics*, 18(6):1848–1856.

[93] Odelu, V., Das, A., and Goswami, A. (2015). A secure biometrics-based multiserver authentication protocol using smart cards. *IEEE Transactions on Information Forensics and Security*, 10(9):1953–1966.

[94] Otto, C., Milenkovic, A., and C. Sanders, E. J. (2006). System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia*, 1(4):307–326.

[95] Pakzad, S. and Fenves, G. (2004). Structural health monitoring applications using mems sensor networks. *In: Proceedings of the* 4^{th} *International Workshop on Structural Control*, pages 47–56.

[96] Patel, M. and Wang, J. (2010). Applications, challenges, and prospective in emerging body area networking technologies. *IEEE Wireless Communications*, 17(1):80–88.

[97] Peralta, D., Galar, M., Triguero, I., Paternain, D., García, S., Barrenechea, E., Benítez, J., Bustince, H., and Herrera, F. (2015). A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation. *Information Sciences*, 315:67–87.

[98] Piotrowski, K., Sojka, A., and Langendoerfer, P. (2010). Body area network for first responders - a case study. *In: Proceedings of the* 5^{th} *International Conference on Body Area Networks*, pages 37–40.

[99] Poon, C., Zhang, Y., and Bao, S. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Journals & Magazines*, 44(4):73–81.

[100] Pujolle, G. and Salvatori, O. (2011). *Les réseaux*. Eyrolles, Paris, 7^{e} édition.

[101] Ragesh, G. and Baskaran, K. (2012). An overview of applications, standards and challenges in futuristic wireless body area networks. *International Journal of Computer Science Issues*, 9(2):180–186.

[102] Rajasekaran, R., Manjula, V., Kishore, V., Sridhar, T., and Jayakumar, C. (2012). An efficient and secure key agreement scheme using physiological signals in body area network. *In: Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, pages 1143–1147.

[103] Ratha, N., Connelle, J., and Bolle, R. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634.

[104] Reddy, A., Das, A., Odelu, V., and Yoo, K. (2016). An enhanced biometric based authentication with key-agreement protocol for multi-server architecture based on elliptic curve cryptography. *PLoS One*, 11(5):e0154308.

[105] Reddy, A., Yoon, E., Das, A., Odelu, V., and Yoo, K. (2017). Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment. *IEEE Access*, 5:3622–3639.

[106] Redner, R. and H.Walker (1984). Mixture densities, maximum likelihood and the em algorithm. *Society for Industrial and Applied Mathematics*, 26(2):195–239.

[107] Sagayee, G., Arumugam, S., and Mala, G. (2013). Biometric encryption using enhanced fingerprint image and elliptic curve. *International Journal of Computer Science and Network Security*, 13(7):106–112.

[108] Saleem, S., Ullah, S., and Yoo, H.-S. (2009). On the security issues in wireless body area networks. *International Journal of Digital Content Technology and its Applications*, 3(3):178–184.

[109] Salsano, Y., Veltri, L., and Papalilo, D. (2002). Sip security issues: the sip authentication procedure and its processing load. *IEEE Network*, 16(6):38–44.

[110] Sidelnikov, V. and Shestakov, S. (1992). On insecurity of cryptosystems based on generalized reed-solomon codes. *Discrete Mathematics and Applications*, 2(4):439–444.

[111] Smeaton, A., Diamond, D., Kelly, P., Moran, K., Lau, K., Morris, D., Moyna, N., O'Connor, N., and Zhang, K. (2008). Aggregating multiple body sensors for analysis in sports. *International workshop on wearable micro and nanosystems for personalised health (pHealth)*, 30(3):1–5.

[112] Stevens, I. and Rasmussen, W. (1982). Remote medical diagnosis system (rmds) concept. *Journal of Medical Systems*, 6(5):519–529.

[113] Tan, Z. (2014). A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. *Journal of Medical Systems*, 38(3):1–9.

[114] Tong, V. V. T., Sibert, H., Lecour, J., and Girault, M. (2007). Fingerkey, un cryptosystème biométrique pour l'authentification. *In: Proceedings of the Conference on Network and Information Systems Security <hal-00156447>*, pages 1–10.

[115] Truong, T., Tran, M., and Duong, A. (2012). Robust mobile device integration of a fingerprint biometric remote authentication scheme. *In: Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications*, pages 678–685.

[116] Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., and Kwak, K. (2012). A comprehensive survey of wireless body area networks. *Journal of Medical Systems*, 36(3):1065–1094.

[117] Uludag, U., Pankanti, S., Prabhakar, S., and Jain, A. (2004). Biometric cryptosystems: issues and challenges. *In: Proceedings of the IEEE (Special Issue on Multimedia Security for Digital Rights Management)*, 92(6):948–960.

[118] Venkatasubramanian, K., Banerjee, A., and Gupta, S. (2010). Pska : Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine*, 14(1):60–68.

[119] Vijayakumar, P., Pandiaraja, P., Karuppiah, M., and Deborah, L. (2017). An efficient secure communication for healthcare system using wearable devices. *Computers and Electrical Engineering*, pages 1–14.

[120] Walters, J., Liang, Z., Shi, W., and Chaudhary, V. (2007). *Wireless sensor network security: A survey.* CRC Press: Boca Raton, FL, USA, New York.

[121] Wang, C., Zhang, X., and Zheng, Z. (2016). Cryptanalysis and improvement of a biometric-based multi-server authentication and key agreement scheme. *PLoS One*, 11(2):e0149173.

[122] Wang, H., Zhang, Y., Xiong, H., and Qin, B. (2012). Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme. *IET Information Security*, 6(1):20–27.

[123] Wang, W., Hua, K., Hempel, M., Peng, D., Sharif, H., and Chen, H. (2010). A stochastic biometric authentication scheme using uniformed gmm in wireless body area sensor networks. *In: Proceedings of the* 21^{st} *Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1620–1624.

[124] Wu, F., Xu, L., Kumari, S., and Li, X. (2015). A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client-server networks. *Computers and Electrical Engineering*, 45:274–285.

[125] Xi, K., Ahmad, T., Han, F., and Hu, J. (2010). A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment. *Security and Communication Networks*, 4(5):487–499.

[126] Yoon, E. and Yoo, K. (2013). Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. *Journal of Supercomputing*, 63(1):235–255.

[127] Zaeri, N. (2011). *Minutiae-based fingerprint extraction and recognition.* Biometrics, Edited by Jucheng Yang, ISBN: 978-953-307-618-8, InTech.

[128] Zatout, Y. (2011). *Conception et évaluation de performances d'un réseau de capteurs sans hétérogène pour une application domotique.* PhD thesis, University of Toulouse le Mirail - Toulouse II, Networks and Telecommunications.

[129] Zebboudj, S., Cherif, F., Mohammedi, M., and Omar, M. (2017). Secure and efficient ecg-based authentication scheme for medical body area sensor networks. *Smart Health*, pages 1–20.

[130] Zhang, Z., Qi, Q., Kumar, N., Chilamkurti, N., and Jeong, H. (2014). A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography. *Multimedia Tools and Applications*, 74(10):3477–3488.

[131] Zhang, Z., Wang, H., Vasilakos, A., and Fang, H. (2012). Ecg-cryptography and authentication in body area networks. *IEEE Transactions on Information Technology in Biomedicine*, 16(6):1070–1078.

Abstract: The progress achieved in the areas of microelectronics and wireless communication technologies have given birth to the development of miniaturized, autonomous and intelligent sensors. These latter have become essential elements in every healthcare monitoring system. The primary role of these equipments, which are placed on or in close proximity to the human body, is to participate in collecting the patient's vital signs and then communicate them to a remote analysis center using wireless interfaces for process them in real-time. However, one of the major issues of these systems is the security of the collected data, which is considered as a major unresolved concern. Consequently, it is essential to ensure the security of these sensitive data during their transmission, as well as during their storage. Another issue comes to be added to the risk of altering the collected data, this concerns the requirements of medical applications and the constraint relating to the limited resources of the sensors which leave this problematic in search of an optimal resolution. The work carried out in this thesis focuses on authentication mechanisms based on morphological or physiological human features in mobile healthcare environments. Subsequently, the communications parties will be able to agree on a shared secret symmetric key to authenticate each other to ensure reliable collection and transmission of such critical data. The proposed schemes were evaluated through simulations, the obtained results indicate out performance and efficiency of our schemes with comparison to other concurrent ones, while providing effective security.
Key-words: Security, Authentication, Sensor, Healthcare Monitoring, Healthcare Environments.

Résumé : Les progrès réalisés dans les domaines de la micro-électronique et des technologies de communication sans fil, ont fait naître des capteurs miniaturisés, autonomes, et intelligents. Ces derniers sont devenus des éléments incontournables dans chaque système de supervision médicale. Le rôle principal de ces équipements qui sont placés sur ou à proximité immédiate du corps humain, est de participer à la collecte des signes vitaux du patient, puis les communiquer à un centre d'analyses distant à l'aide d'interfaces sans fil pour les traiter en temps réel. Cependant, l'un des problèmes majeurs de ces systèmes est la sécurité de données recueillies qui est considéré comme un sujet de préoccupation majeure non encore résolu. Par conséquent, il est indispensable d'assurer la sécurité de ces données sensibles lors de leur transmission ainsi que pendant leur stockage. Un autre problème s'ajoute au risque de modification de données recueillies, il s'agit des exigences des applications médicales et la contrainte relative aux ressources limitées des capteurs qui laissent cette problématique à la recherche d'une résolution optimale. Les travaux réalisés dans le cadre de cette thèse portent sur les mécanismes d'authentification basés sur les caractéristiques humaines morphologiques ou physiologiques dans les environnements de soin et de santé mobile. Subséquemment, les parties de communications pourront se mettre d'accord sur une clé symétrique secrète partagée pour s'authentifier afin de garantir une collecte et une transmission fiables de ces données critiques. Les protocoles proposés ont été évalués à travers des simulations, les résultats obtenus ont prouvé la performance et l'efficacité de nos solutions par rapport à divers protocoles concurrents, tout en fournissant une sécurité efficace.
Mots clés: Sécurité, Authentification, Capteur, Supervision médicale, environnements de soin et de santé.

ملخص: أدى التقدم في مجال الالكترونيات الدقيقة وتكنولوجيات الاتصالات اللاسلكية إلى أجهزة استشعار مصغرة، مكتفية ذاتيا، وذكية. وأصبحت هذه العناصر الأخيرة عناصر أساسية في كل نظام من نظم الإشراف الطبي. الدور الرئيسي لهذه الأجهزة، التي توضع على أو بالقرب من جسم الإنسان، هو المشاركة في جمع علامات المريض الحيوية ومن ثم توصيلها إلى مركز تحليلي عن بعد باستخدام واجهات لاسلكية لمعالجتها في الوقت الحقيقي. ومع ذلك، فإن إحدى المشاكل الرئيسية لهذه النظم هي سلامة البيانات التي تم جمعها والتي تعتبر مصدر قلق كبير لم يتم حله. ولذلك، من الضروري ضمان أمن هذه البيانات الحساسة أثناء نقلها وكذلك أثناء تخزينها. وهناك مشكلة أخرى تضاف إلى خطر تغيير البيانات التي تم جمعها، فمن مطالب التطبيقات الطبية والقيود على الموارد المحدودة من أجهزة الاستشعار التي تترك هذه المشكلة بحثا عن قرار الأمثل. ويركز العمل المنجز في هذه الأطروحة على آليات المصادقة القائمة على الخصائص البشرية المورفولوجية أو الفسيولوجية في بيئات الرعاية الصحية والرعاية الصحية المتنقلة. واستنادا إلى هذه الآليات، سوف تكون أطراف الاتصالات قادرة على الاتفاق على مفتاح متماثل السري المشترك للمصادقة لضمان جمع موثوق بها ونقل هذه البيانات الهامة. وقد تم تقييم البروتوكولات المقترحة من خلال المحاكاة، وقد أثبتت النتائج التي تم الحصول عليها أداء وكفاءة حلولنا مقارنة مع مختلف البروتوكولات المتنافسة، مع توفير الأمن الفعال.
كلمات البحث: الأمن، المصادقة، الاستشعار، الإشراف الطبي، بيئات الرعاية الصحية.