Implementing a Secure Remote Patient Monitoring System

Othmane Nait Hamoud, Tayeb Kenaza, Yacine Challal, Lina Ben-Abdelatif, Maroua Ouaked

Implementing a Secure Remote Patient Monitoring System

Othmane Nait Hamoud[a,b], Tayeb Kenaza[b], Yacine Challal[a], Lina Ben-Abdelatif[c] and Maroua Ouaked[c]

[a]Ecole nationale Supérieure d'Informatique, BP 68M, 16309, Oued-Smar, Algiers, Algeria.
[b]Ecole Militaire Polytechnique, BP 17, 16111, Bordj El-Bahri, Algiers, Algeria.
[c]Université M'Hamed Bougara, Boumerdès, Algeria.

ARTICLE HISTORY
Compiled April 30, 2021

ABSTRACT
Remote patient monitoring (RPM) system is an important technology to reduce contamination risk for the elderly population in COVID19 pandemic. However, security and data privacy are the major challenges that hinder the development of such technology. A secure RPM platform should satisfy several security requirements such as authentication, confidentiality, and access control. Public Key Infrastructure (PKI) is one of the main widely-used key management schemes.Unfortunately, in an e-Health system supporting constrained devices, PKI suffers from some issues related to the burden of certificate management (e.g. revocation, storage, and distribution) and the computational cost of certification verification. In this paper, we present our contribution to the development of a secure RPM system. Our security solution is based on Certificate-less Public Key Cryptography (CL-PKC) which ensures a dynamic solution for securing communications between patient devices and the e-Health services core. The proposed solution provides secure authentication and key agreement protocol to establish secret session keys. These keys are used for secure exchanging real-time electronic health records (EHR). To evaluate our approach, we conducted both simulation and real experiments. The security and performance analysis show that our approach is secure and effective while being easy to implement on resource-constrained devices with a low computational cost.

KEYWORDS
e-Health; Remote patient monitoring; Certificate-less public key cryptography; Confidentiality; Privacy

1. Introduction

After World War II, global life expectancy increased dramatically, leading to increased demand for health services. Life expectancy is now around 72 years worldwide and around 82 years in some countries like Japan (World Health Organization). Thus, the resulting healthcare deficiency creates a need for innovative information and communication technologies (ICT) solutions.

Indeed, over the past few decades, we have witnessed a significant transformation in the quality of health services provided by organizations and health professionals. Recent progress has led to the emergence of electronic health (e-Health) **(Della Mea**

CONTACT Tayeb Kenaza. Email: ken.tayeb@gmail.com

(2001)), made possible in large part by the massive deployment and adoption of ICT. e-Health, through its many applications, offers new opportunities to help the elderly and suffering population to maintain their independence and mobility.

One of the revolutionary e-Health technologies is the Remote Patient Monitoring (RPM) system **(Malasinghe, Ramzan, & Dahal (2019))**, which aims to remotely monitor the health status of patients using sensors installed on and around the patient's body **(Rasyid, Sukaridhoto, Sudarsono, & Kaffah (2020))**. Thanks to the quality of its services, it helps meet the healthcare needs of the growing number of elderly people, patients with chronic diseases and people living in isolated rural areas **(Yaacoub, Abualsaud, Khattab, & Chehab (2020))**. It also ensures better medical follow-up for patients and rapid intervention by health staff in emergency cases. However, the deployment of new technologies such as RPM systems in e-Health care applications may leave patients' privacy exposed to attacks exploiting vulnerabilities that are mainly related to ICT **(Qiu, Qiu, Memmi, & Liu (2020))**. Therefore, security is a primary requirement of e-Health applications.

Key management schemes (KMS) are the foundation of any security solution based on cryptography. Indeed, they are important to find efficient cryptographic solutions to satisfy security requirements such as authentication and key agreement, confidentiality, and integrity. KMS refers to procedures related to the management of cryptographic keys especially in terms of keys generation, distribution, and revocation. The design of an efficient key management scheme mainly relies on the security of these procedures.

Public Key Infrastructure (PKI) is one of the main widely-used key management schemes which, from a cryptography point of view, bind users' public keys with their respective identities through a process of registration and issuance of certificates at and by Certificate Authority (CA). Unfortunately, PKI suffers from issues related to burden due to certificate management (revocation, storage, and distribution), and computational cost of certification verification. Several issues related to PKI are discussed by Gutmann (2002). These issues need to be considered more carefully when PKI is deployed in resource-constrained environments in terms of computing power and storage, such as IoT-based RPM systems.

Identity-Based Public Key Cryptography (ID-PKC) (Shamir (1984a)) was seen as a solution to the main PKI problem, which is the dependency on CA, to authenticate an entity public key. ID-PKC cancels this dependency so that an entity's public key is derived directly from its identity. The private key, on the other hand, is generated by a Private Key Generator (PKG) based on a system-wide master key. Unfortunately, the dependency on PKG introduces the key escrow problem, since PKG may gain access to all entities' private keys and thus, decrypt their ciphertexts and forge their signatures.

Certificateless Public Key Cryptography (CL-PKC) was introduced in Al-Riyami & Paterson (2003) as the intermediate between PKI and ID-PKC. That is, CL-PKC dispenses with the use of certificates and does not suffer from the key escrow problem while enjoying both PKI's and ID-PKC's properties. The user's private key generation in a CL-PKC system is a combination of two partial private keys, one from the user and the other from the Key Generation Center (KGC) which, by way of contrast to the PKG in ID-PKC, does not have access to users' private keys.

In the context of RPM systems, most of the existing solutions in the literature (Monshizadeh, Khatri, Koskimies, & Honkanen (2020), Yew, Ng, Ping, Chung, Chekima, & Dargham (2020), Ondiege, Clarke, & Mapp (2017)), that we will discuss in the next section, are based on the use of (PKI) or RSA based authentication schemes which are complicated to set up and to maintain, especially with resource-constrained IoT devices in real-time applications. Furthermore, if the CA is compromised, this exposes all the system security to risks of a single point of failure. Moreover, most of these solutions are not implemented and are merely simulated, which does not lead to concrete results. Our contributions in this paper are summarized as follows:

(1) Explore and analyze the state-of-the-art of e-Health systems' security.
(2) Develop an RPM system.
(3) Propose an efficient and dynamic security solution guaranteeing the confidentiality and protection of patient's medical data.
(4) Implement concretely the architecture proposed by the National Institute of Standards and Technology (NIST) (Jennifer, Nakia, Bronwyn, Jason, Kevin, Julie, Sue, Ryan, & Kangmin (2020)).

Our security solution relies on Certificate-less Public Key Cryptography (CL-PKC) which gives a dynamic solution by avoiding the use of PKI servers. CL-PKC ensures a secure cryptographic keys establishment between all RPM actors (such as sensors and health staff) and the e-Health services core. Also, our solution can be extended to ensure user consent as required by the GDPR, by applying the CL-PKC aggregation mechanism proposed by Hamoud, Kenaza, & Challal (2019).

The remainder of this paper is organized as follows. Section 2 presents a brief overview of related works. Section 3 presents an overview of the CL-PKC. An overview of RPM systems is presented in Section 4. Section 5 presents in detail the threat models and security requirements of an RPM system. Section 6 presents the design of our proposal. Section 7 presents the simulation and implementation of our proposed solution. We discuss security and performance analysis in Section 8. Section 9 concludes this paper.

2. Related Works

In this section, we present a synthesis of research efforts related to RPM system security issues that have been the subject of much academic research. Most of them mainly focus on Body Area Networks (BAN) or hospital networks. A thorough and comprehensive analysis of the entire RPM systems is not discussed in the literature.

The role-based and time-bound access control approach has been introduced by Zhang, Liu, & Xue (2014). The approach is effective for storing Electronic Health Records (EHRs) encrypted in unreliable clouds and resolves cryptographic keys management issues. This approach applies time-limited hierarchical key management that allows legitimate users to access EHRs for a given period, depending on their access roles. EHRs are encrypted using symmetric key encryption. However, the approach is complicated in implementation because it requires that a user must have multiple roles. As a result, users must manage several keys.

Shin, Jeon, Ju, Lee, & Jeong (2015) have assessed various privacy-related security

requirements in e-Health care services. They proposed an improved model of role-based access control to design a platform integrating healthcare services. The proposed model is unfortunately unusable in a collaborative environment. The model does not give the user the exclusive privilege to dictate who should access their medical information, as required by the GDPR.

Benzschawel & Da Silveira (2011) have introduced a multi-level security architecture to improve the security and privacy of medical information during storage and sharing against external and internal attacks by combining pseudonymization, digital signature, and encryption techniques. The proposal relies on a PKI to encrypt pseudonymized data. However, the approach focuses only on secure access to medical data which is not even encrypted. **Although the identity of patients is protected, an attacker could link a patient's identity to his/her medical data based on the access time to the system. Furthermore, authors have adopted the traditional PKI which is involved to deliver key pairs (private/public) and digital certificates to authenticate users. Thus, CA is considered as a single point of failure.**

Fan, Buchanan, Lo, Thümmler, Lawson, Uthmani, Ekonomou, Khedim, & Sharif (2012) have implemented a design of the e-Health platform DACAR integrating the Single Point of Contact (SPoC) mechanism. The latter guarantees a claim-based authorization and facilitates the integration and deployment of reliable e-Health services that can be hosted in a cloud environment. The result of the model is quite reliable. However, the platform can only work with a limited number of users and is not flexible and dynamic enough for a large number of users.

An approach called "Patient Centered Secure Access Control Scheme (ESPAC)" has been presented by Barua, Liang, Lu, & Shen (2011). The scheme allows access to health data based on access privileges. ESPAC uses identity-based encryption (IBE) for secure data transmission between the remote patient and the healthcare service, while access control is achieved using an Attribute-based encryption approach (CP-ABE). The system ensures that user privacy and data integrity are properly supported. However, the lack of dynamism and flexibility in the patients' data collection and their transmission to care core services, makes this approach inefficient in practice (Abbas & Khan (2014)).

Hupperich, Löhr, Sadeghi, & Winandy (2012) have developed a privacy and access control architecture for EHR where patients can authorize remote access to their medical information via a mobile device. The architecture is more flexible since the access is both time and place independent, and the architecture relies solely on a modern cryptographic security approach (ABE). **However, since the Private Key Generator (PKG) creates users' private keys, this leads to key escrow problem.** Also, the main disadvantage of this architecture is in the time required in exchanging keys from one end to the other for both encryption and decryption. The complexity of key management is a serious challenge of this approach. **It should be noted that the proposed architecture was neither implemented nor simulated.**

Srinivas, Mishra, & Mukhopadhyay (2017) proposed a symmetric key-based authentication scheme for healthcare applications with wireless medical sensor networks. To access the patient's medical information sensed by medical sensors remotely, the medical staff receive a smart card during the registration process to the hospital's registration centre via a gateway node (GWN). During the authentication step, the smart card receives the medical staff's login credentials then sends a login request to the sensor via the GWN. This work could be integrated into an RPM system, however, it

lacks the servers' security study where patients' EHRs may be saved. Besides, solutions that rely on password-based authentication through smart cards are prone to the DOS and smart card stolen attack. For example, an ineffective password change can result in a DOS attack if the password is entered incorrectly during the password change phase.

Ondiege et al. (2017) have proposed a new and enhanced security framework of a capability-based RPM system in a multi-user environment and a new NFC-based identification technique. The capability-based RPM system only authenticates registered devices and prevent rogue ones from sending their readings. The system relies on PKI to establish session encryption and to authenticate managers and telemonitoring servers. Here also, the proposed framework was neither implemented nor simulated.

Recently, Alzahrani, Irshad, Alsubhi, & Albeshri (2020) designed a new efficient and secure authentication protocol where a BAN logic-based formal security analysis was used to formally prove its security, and ProVerif automated security tool was used to validate their results. The authors used asymmetric cryptography for authentication between the different actors in the RPM system. However, nowhere does their paper make any reference how to ensure public keys' authenticity. In addition, the protocol does not elaborate on the security of a compromised Registration Centre (RC).

Yaacoub et al. (2020) proposed an end-to-end secure approach for Delay Tolerant Networks (DTN) communication of mobile health (m-Health) monitoring data. A DTN relies on "data mules" (vehicles) and is used in rural areas where there is no connectivity to carry the data from rural areas to urban centres. However, their approach is not suitable for real-time m-Health monitoring. In addition, to authenticate patients, the authors' approach relies on a three-way handshake process carried out by data mules for secure key exchange, which wastes a lot of time, while pre-shared keys are more suitable for this kind of applications.

We notice that the existing works do not address the security of the entire RPM system, while our proposal ensures security at each part of the NIST's RPM system architecture. Also, almost all of the discussed works apply public key cryptography through a PKI. However, if the CA is compromised, the cybercriminal could issue false certificates and mislead users to send data to illegitimate recipients. Thus, this exposes all the system security to risks of a single point of failure. For example, attackers may, by disguising themselves as a trustworthy CA, carry out several attacks such as impersonation attack, man-in-the-middle attack, fishing attack, etc. Besides, PKI is not suitable for resource-constrained devices in an RPM system, especially when real-time monitoring is required. Furthermore, all the discussed works are merely simulated and not implemented.

3. Overview of the Certificate-less Public Key Cryptography

The paradigm of certificate-less public key cryptography CL-PKC was introduced for the first time by Al-Riyami & Paterson (2003). Authors proposal was an intermediary cryptosystem between (PKI) and (ID-PKC) (Shamir (1984b)), to avoid problems related to certificates management on the one hand and eliminate the "key escrow

problem" on the other hand. A CL-PKC cryptosystem, similarly to ID-PKC system, relies on a trusted third party called the key generation center (KGC). However, unlike PKG in ID-PKC, the KGC does not have access to the private keys of the entities.

The KGC provides an entity A with a partial private key D_A which it calculates from an identifier ID_A and a master key. The process of providing partial private keys should be confidential and authentic. Entity A generates its private key S_A by combining its partial private key D_A with a secret value x_A. Consequently, A's private key is not known by the KGC unlike for the PKG in the ID-PKC. Entity A then calculates its public key P_A by also combining the same secret value x_A with the public parameters of KGC. The public key of user A, P_A, could be made available to other users either by transmitting it within messages, or by publishing it in a public directory. It should be noticed that no security mechanism is applied to protect public keys in CL-PKC. In particular, there is no certificates for A's public key. To encrypt a message sent to an entity A, or verify its signature, an entity B uses only P_A and ID_A.

To make concrete their new paradigm, CL-PKC's authors introduced four schemes which are as follows:

(1) Certificate-less Public Key Encryption (CL-PKE),
(2) Certificate-less Public Key Signature (CL-PKS),
(3) Certificate-less Authenticated Key Agreement Protocol (CL-AKA),
(4) Hierarchical Certificate-less Public Key Encryption (HCL-PKE).

All these schemes are specified by five common algorithms: $(1)Setup, (2)Partial-Private-Key-Extract, (3)Set-Secret-Value, (4)Set-Private-Key, (5)Set-Public-Key$, and additional algorithms: $Encrypt, Decrypt$ in CL-PKE scheme, $Sign, Verify$ in CL-PKS scheme. Note that Biswas, Anisuzzaman, Akhter, Kaiser, & Mamun (2014) focus on Certificate-less Public Key Encryption (CL-PKE) showing that a concrete pairing-based CL-PKE scheme is secure provided that an underlying problem closely related to the Bilinear Diffie-Hellman Problem is hard.

In the following, we describe briefly the basic scheme of CL-PKE which is based on seven randomized algorithms as shown in Figure 1:

(1) *Setup*: performed by the KGC. It takes as input a security parameter k and returns the system public parameters *param*, the system's master public key P_0 and the system's master private key s.
(2) *Partial private key extract*: for a user A with its identity ID_A, the KGC takes $params$, s and ID_A as inputs and returns to A, over a confidential and authentic channel, a partial private key D_A.
(3) *Set secret value*: a user A takes $params$, ID_A and a random x_A and outputs its secret value x_A.
(4) *Set private key*: a user A takes as inputs its partial private key D_A, its secret value x_A and $params$ and outputs its full private key S_A.
(5) *Set public key*: a user A takes as inputs its secret value x_A and $params$ and outputs its public key P_A.
(6) *Encrypt*: a user B, intending to transmit an encrypted message to a user A, takes as inputs $params$, a message M, A's public key P_A and identity ID_A and outputs a cipher text C.
(7) *Decrypt*: a user A, receiving an encrypted message C, takes as inputs $params$, C and its private key S_A and outputs the message M.

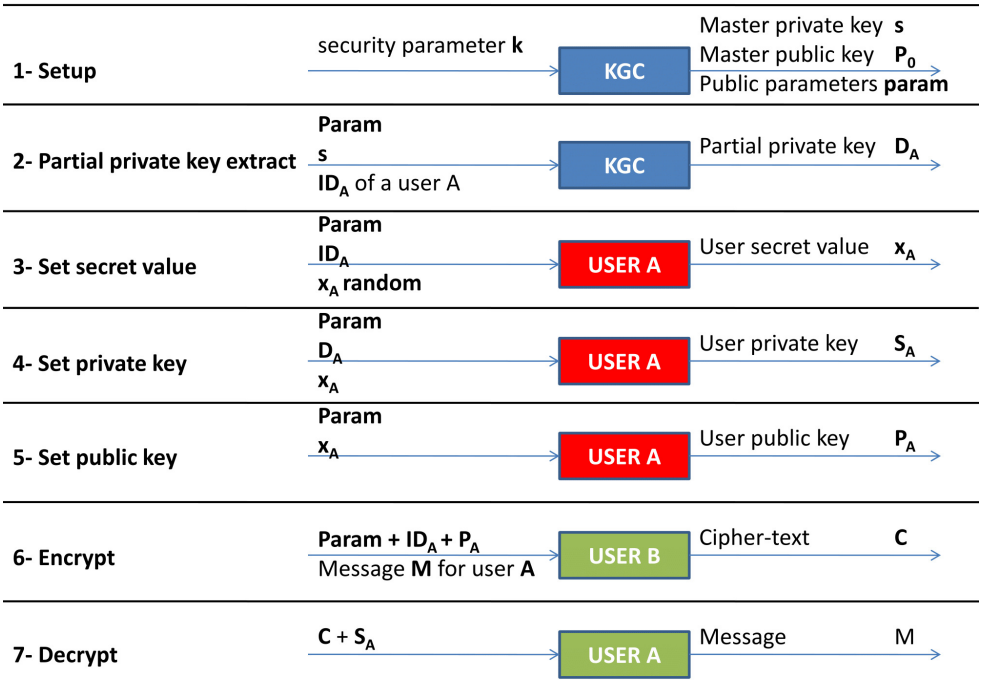


Figure 1.: Basic scheme of CL-PKE.

4. Remote Patient Monitoring (RPM) Systems

The World Health Organization defines e-Health as "the use of information and communication technologies (ICTs) for health[1]". To enhance this broad definition, the French research and documentation institute in health economics distinguishes two major domains[2]:

- Health information systems (HIS) or hospital information systems (HIS) are the basis for e-Health. They organize the exchange of information at the ICT level between private doctors and hospitals, or between departments within a hospital.
- Tele-health includes mobile health (m-Health) and tele-medicine. m-Health is the most familiar to the general public, i.e. health via smartphones. Tele-medicine is a professional activity that uses digital telecommunication means to enable doctors and other medical personnel to perform medical procedures at a distance, such as:
  (1) Tele-consultation: it involves the use of technology so that the medical professionals and patients can interact with each other.
  (2) Tele-expertise: a doctor remotely requests the opinion of one or more of her/his colleagues.
  (3) Remote patient monitoring : a doctor remotely interprets the data necessary for the medical follow-up of a patient and, if necessary, takes decisions relating to his/her healthcare.

[1]National e-Health Strategy Toolkit. World Health Assembly Resolution and ITU World Telecom Development Conference Resolution. https://doi.org/978 92 4 154846 5

[2]`http://www.irdes.fr/documentation/syntheses/e-sante.pdf`

(4) Medical tele-assistance: a doctor remotely assists another health professional during performing a medical act.

In recent decades, the medical community is more and more integrating e-Health in their care services. However, the development of this domain meets several challenges. Biswas et al. (2014) have mentioned the following challenges:

- Security: Multiple cloud providers and healthcare organizations will take part in the e-Health Cloud, and interact with the different resource pool. Therefore, a proper security mechanism is a challenge to maintain data persistence, integrity, confidentiality and availability.
- Flexibility and interoperability: Organizations and individuals will expect different functions, operations and services. Quality of service (QoS) requirements will therefore have to be maintained. Adding new services to the system must be flexible and require a minimum of effort and cost, without compromising security and privacy.
- Maintainability: Perfect test models must be developed to reduce maintenance time, and to provide error-free services to people and organizations,

In this work, we address the security challenges related to the use of an RPM system, mainly by ensuring the confidentiality of sensitive patient data against several threats, as will be explained in the next section. To this end, we propose a concrete implementation of the architecture proposed by the National Institute of Standards and Technology (NIST) (Jennifer et al. (2020)), by proposing a technical solution of several of its security requirements such as authentication, confidentiality and access control.

5. Threats and Security Requirements

In this section, we give a brief overview of the NIST architecture, the threat model and security requirements.

The NIST architecture includes three parts (Figure 2): (1) the patient's home environment, (2) the platform provider, and (3) the healthcare delivery organizations (HDOs)(e.g. healthcare provider). The patient home is the environment in which the patient lives and uses RPM components such as sensors and communication devices. The telehealth platform provider maintains and receives data communications from either the patient home or the HDO. The HDO maintains its environment including clinical systems to receive, interpret and record patient data in EHR (Jennifer et al. (2020)).

Unfortunately, e-Health systems are subject to attacks that are intentionally or unintentionally executed to capture confidential information or control the entire system. This affects the efficiency and performance of health services and facilitates the compromise and breach of the integrity, confidentiality and availability of patient health data. **In the following we discuss threat modal and security requirements to develop a secure RPM.**

5.1. Threats targeting an RPM system

Several threats are emerging at each part of an RPM system with respect to the NIST architecture. In the following we review some of attacks identified in each part as mentioned by Altamimi et al. (2016).

(1) Attacks on data collection: these attacks can lead to several data collection threats, such as changing information, deleting important data, or replaying data messages.
   - Scramble attack: this is a kind of intentional interference attack on the radio frequency of the sensor nodes to isolate them and prevent them from sending or receiving messages.
   - Flood attack: the attacker repeatedly broadcasts many victim with connection requests until all resources reach a maximum limit, causing a flood attack.

(2) Attacks on data transmission: these attacks can lead to several transmission threats, such as spying, changing information, and interrupting communication.
   - Eavesdropping: This is the most common attack on the patient's privacy. By monitoring the vital signs of the patient, an adversary can easily discover the patient information from the communication channels. Besides, an adversary can also detect the content of the message, including its identifier, timestamp, source address, a destination address, and other relevant information. Monitoring and sniffing can therefore pose a serious threat to the privacy of patients (Kumar & Lee (2012)).
   - Man in the middle: This is one of the most common attacks in which the attacker intercepts a communication between the patient and the remote server and exchanges messages between them. The communication is completely controlled by the attacker allowing him to read, insert and modify the data in the intercepted communication.
   - Modification of the messages: in this attack, the attacker captures the wireless channels of the patient and extract his medical data; later, it can alter them, which can mislead the medical staff.

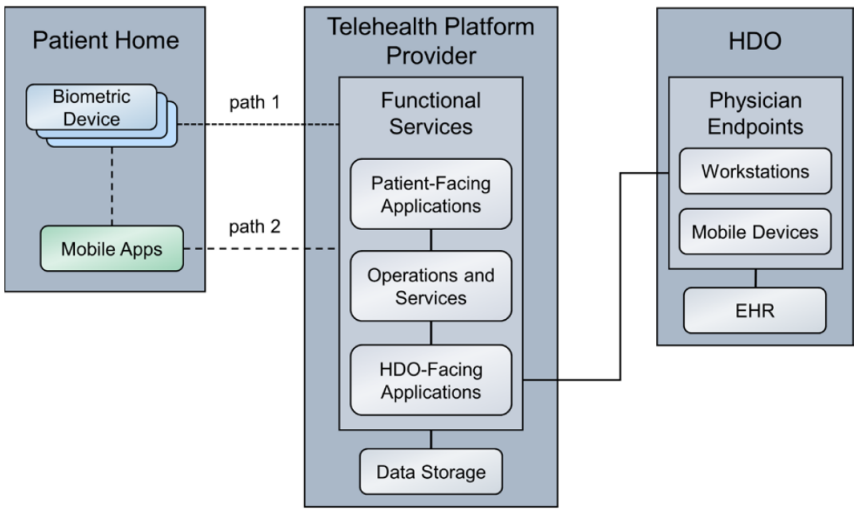


Figure 2.: The NIST Architecture for Remote Patient Monitoring

(3) Attacks on Data Storage : these attacks can lead to multiple storage threats, such as changing the patient's medical information or configuring the system's monitoring servers.
   - Inference of patient information: Attackers attempt to combine the allowed information with other available data, which leads them to identify sensitive patient data such as diseases.
   - Unauthorized Access to Patient's EHRs: This type of attack can be committed by an unauthorized individual without valid authentication.
   - Malware attack: Malware is designed to perform malicious actions. This type of attack is capable of infecting and spreading throughout the system, which can lead to system malfunction, downtime and disruption of services and communication.

5.2. Security Requirements

The successful deployment of an RPM system relies on the secure transfer of vital signs from the patient to the hospital. Secure transfer requires that the RPM system meets the main objectives and requirements of security. In the process of evaluating the security, it is essential to address these requirements at each level (Niksaz & Branch (2015)).

(1) Body Area Network (BAN): Communication links within the BAN are built using wireless technologies. The requirements and security objectives in such a network require more attention than structured networks.
   - Confidentiality of the data is necessary to prevent the disclosure of data during its storage or transmission in the BAN.
   - Data privacy should be maintained even if network nodes are compromised. The disclosed data may reveal information relating to the patient's disease.
   - Data integrity is needed to protect the data against changes not only during transit but also during storage. Modified data can induce health staff to misdiagnose the patient.
   - Availability of data is necessary to ensure that health personnel have timely access to patient data. Late or non-existent access to information may prevent the patient's treatment procedures.
   - Data authentication is necessary to detect and identify falsified data sent by an opponent. It is also important to build trust in the data received and throughout the system.

(2) Communication Network: Once the patient's health status is monitored, processed in the BAN and stored in the smartphone, the data is transferred over the communication network.
   - Data confidentiality is necessary to prevent disclosure of information in case of interception of a communication session.
   - Data integrity is necessary to ensure that data transferred from the BAN to the hospital is not changed.
   - Data reliability can ensure that data transferred from the BAN to the hospital is available even if a link or sensor node fails.
   - The accuracy of the data is necessary to ensure that the data is fresh and not reorganized by an opponent.

(3) Hospital: Patient data is collected at the hospital for medical diagnosis, treatment and storage.

- Security requires limited physical access to the hospital's medical servers containing the patient's medical records. Poor physical security procedures may allow unauthorized persons to modify data and compromise the system.
- Data privacy primarily concerns patient health data, which is generally subject to legal and ethical confidentiality requirements. It should be confidential and accessible only to authorized health personnel.
- Data integrity is necessary to ensure data security against unauthorized changes.
- Availability of data is necessary to ensure data availability for medical staff, even in the event of system failure.
- An authentication mechanism is needed not only to authenticate hospital users, but also to ensure that data is received from the legitimate patient.

To mitigate the security risks of RPM systems, we propose to follow the security policy defined by the NIST National Center for Cybersecurity (NCCoE) project (Jennifer et al. (2020)). The objective of this policy is to improve the security of the overall RPM system. It should be made clear that our solution doesn't deal with all of the above-discussed threats, it mainly deals with attacks related to storage and transmission by providing solutions for authentication, access control and data protection/privacy, and this, by the use of the `CL-PKC`. Security requirements that our solution ensures are underlined above.

6. The Proposed Solution

This section exposes our security solution based on (`CL-PKC`) to protect patient's data confidentiality and privacy. It is organized into two main parts; the first is devoted to the presentation of the developed RPM system; the second is dedicated to the development of the proposed security solution.

6.1. Presentation of the Developed RPM system

The developed RPM platform (Figure 3), inspired by the NIST architecture, contains two main parts: the body area network and the hospital network.

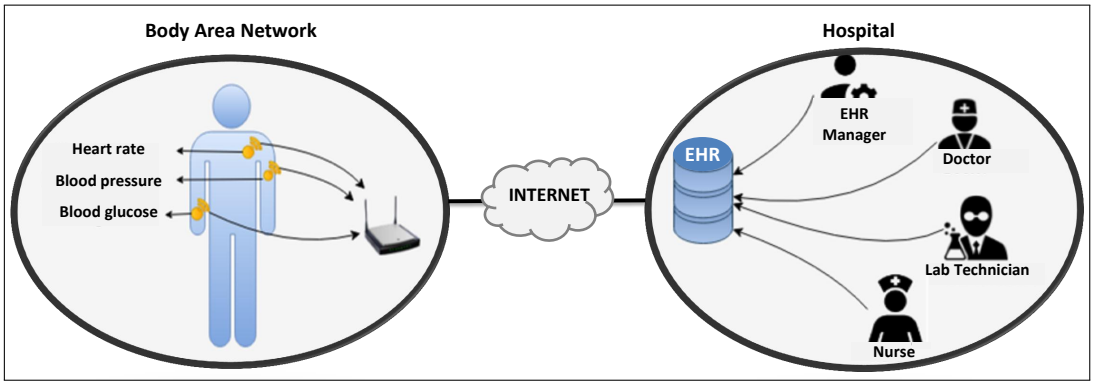


Figure 3.: Architecture of the proposed remote monitoring system.

6.1.1. Body Area Network

In our RPM system, the patient's BAN is intended for the medical monitoring of the patient at home. The physiological sensors implanted on his body, are first acquired by the patient from a pharmacy or hospital, then are configured in the hospital to activate remote medical monitoring. Periodically, the sensors collect vital signs and send them through a gateway to the hospital to analyze and examine the patient's health state. We consider the implantation of three body medical sensors, one for measuring blood glucose, the other for blood pressure and the last for heart rate. These sensors need configuration and communication protocol as described below.

- **Configuration phase:** During this phase, the sensors acquired by the patient are manually configured at the hospital by the attending physician to activate remote monitoring. Thus, each sensor is configured with the following parameters: Sensor's ID, Patient's ID, Sensor's name, and Sensor's function. In addition, and for security reasons, which will be discussed in section 6.2, the sensors are equipped with a private and public key pair issued by a `CL-PKC` system.
- **Communication protocol:** To send the data collected from the patient's body, the sensors must use a specific communication protocol. First of all, they must go through an initialization phase. During this phase, the sensors send a boot message to the gateway to initiate the sending of the data packets. Once received, the gateway responds with an acknowledgement message, triggering the authentication phase. The latter will be carefully elaborated in section 6.2.1. Once authenticated, the sensors send the data packets.

The sensors are programmed to collect and send the vital signs of the patient's body three times a day (8 a.m., 2 p.m. and 9 p.m. as an illustrative example). The data packet produced and sent is shown in Figure 4.

Patient ID	Sensor ID	Sensor Function	Vital Sign	Date	Time	Observation

Figure 4.: Structure of the data packet.

6.1.2. Hospital

At the hospital, a web application (Figure 5) is developed for the health staff for the management of patient's EHRs. The EHRs are organized in a database managed by the EHR manager. An EHR is created during the patient's first visit to the hospital by the attending physician and is accessed and modified only by authorized health staff. EHRs ensure improved patient's health tracking through the accuracy, up-to-date and completeness of the patient's medical information they provide. Additionally, they provide quick access to patient's records for effective healthcare and more coordination between the health staff.

To implement an EHR database within our RPM system, we used existing open source software, namely OpenEMR[3], FreeMED[4] and OpenMRS[5].

The developed electronic medical record includes the following information:

[3]OpenEMR: `https://www.open-emr.org`
[4]FreeMED : `https://freemedsoftware.org`
[5]OpenMRS:`https://openmrs.org`

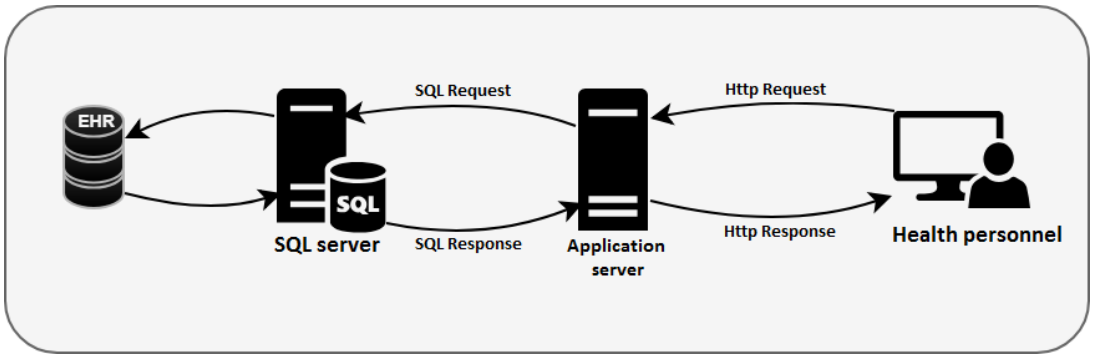


Figure 5.: Architecture of the web application.

- Patient's personal information
- Family history
- Medical history
- Surgical history
- Allergies
- Pathologies
- Diagnoses
- Medical Examinations
- Laboratory results
- Results of remote monitoring
- Tests

6.2. The proposed Security Solution

In this section, we present the security solution adopted in this work. Our contribution concerns the protection phase with respect to the NIST security policy. As a result, the adopted solution deals with the following points: Authentication, Access Control, and Data protection/privacy.

6.2.1. Authentication

Authentication in our RPM system involves both the medical sensors implanted in the patient's home and the health staff. The mutual authentication is based on the formally proofed `CL-PKE` scheme (Al-Riyami & Paterson (2003)). That is, the actors should possess their respective private and public key pairs, issued after the registration step to the Key Generator Center (`KGC`). Keys are calculated during the sensor setup phase, and at the registration to the health staff. Once the system actors acquire their key pairs, they authenticate to the EHR manager, as follows:

Let a sensor A and the EHR manager B with their respective public/private key pairs $< P_A, S_A >$ and $< P_B, S_B >$, be the intended participants in the authentication and key agreement step. First, each of them chooses random values a, b and calculates $T_A = aP$ and $T_B = bP$ respectively, where P is the generator within our `CL-PKC` system parameters. After exchanging their triplets $< ID_A, P_A, T_A >$ and $< ID_B, P_B, T_B >$, both participants verify the validity of each others' public key. In case of verification failure, the authentication is canceled. Otherwise, they may calculate an `AES` symmetric key.

6.2.2. Access Control

EHRs are sensitive data and are exposed to possible misuse and security risks because of their transmission over the internet. Thus, imposing an access control on EHRs

is mandatory to ensure the confidentiality and privacy of such sensitive data. Several works are done in the context of the protection of patient privacy in e-Health (Abbas & Khan (2014); Azeez & Van der Vyver (2019); Shin et al. (2015); T.Jayasankar (2021); Zhang et al. (2014); Zhou, Liu, Liu, & Wu (2016)) showing that role-based access control (`RBAC`) ensures an efficient and flexible access control. Therefore, it is adopted in our solution and, depending on their roles, the appropriate operations are assigned to different entities (staff, sensor, etc.) to handle different tasks.

6.2.3. Data Protection/Privacy

The patient's medical data is of major sensitivity, whether in the hospital, at the patient's home or in transit; it must be protected at all times and secured against all malicious attacks.

(1) Data security at rest: At the hospital, the implementation of EHRs is an essential part of an e-Health system. Despite the potential gains, EHRs are exposed to security threats. For this purpose, when creating the patient's EHR, it is encrypted by the EHR manager using a symmetric key. The symmetric algorithm adopted in our solution is the `AES`. To manage the various keys relating to the different EHRs, the EHR manager creates a table to save patient's IDs and respective symmetric keys dedicated to the encryption of their EHRs. To enhance the security and confidentiality of symmetric keys, the table is encrypted using the private key of the EHR manager.

(2) Data security at transit: After actors' authentication (sensors, health staff), each of them negotiates with the EHR manager a session key for the symmetric encryption and decryption of the data exchanged between them. The entire data packet (containing collected vital signs and other information, see Figure 4) is encrypted using the previously negotiated session key and is safely sent to the hospital through the Internet. Once arrived, the data is stored in the patient's EHR by the EHR manager, as follows:
   - The received data packet is decrypted by the EHR manager using the session key shared between it and the actor,
   - Using its private key, the EHR manager decrypts the symmetric key table,
   - Using the patient's ID recovered from the received data packet, the EHR manager retrieves the corresponding symmetric key,
   - Using the retrieved symmetric key, the EHR manager encrypts the data, locates the patient's EHR and saves data.

7. Implementation and simulation

To implement our RPM system, we firstly simulated the patient home part under the OMNeT++ simulation tool. Then, to ensure the medical follow-up of patients, we have developed a real EMR-Manager with a real EHR database and web application for the hospital's health staff using the J2EE development environment. We present in the following some details of the simulation part.

Figure 6 illustrates the network architecture of the remote monitoring platform simulated using the OMNet++. The network includes the following elements: 03 sensors (blood glucose, blood pressure and heart rate sensor), 02 access points (gateway), 02 routers, the EHR manager, and the e-Health core services.

As discussed in section 6.2, the developed communication protocol involves the

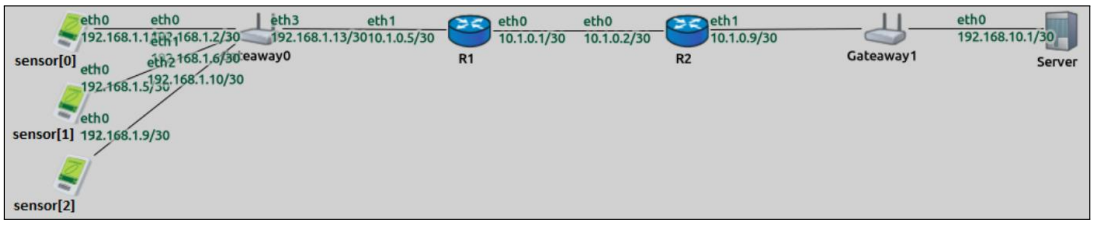


Figure 6.: Network architecture of the RPM system.

execution of the three phases: Initialization, Authentication phase, and Session key generation and data sending.

(1) Initialization phase : During this phase (Figure 7), the sensors send to the gateway an initialization message (Figure 7-A) to inform it that they are ready to send data packets. After receiving the message, the gateway returns an acquittal message (figure 7-B). In Figures 7-A and 7-B, exchanged packets during this initialization phase are illustrated in red.

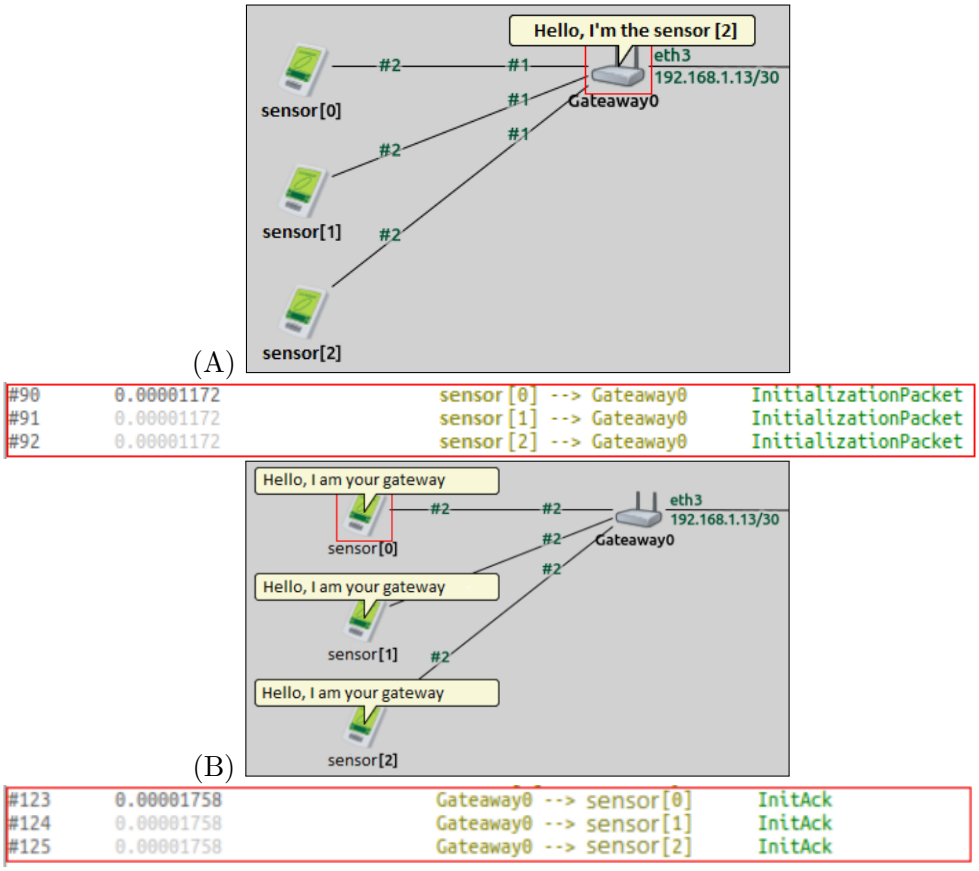


Figure 7.: Initialization messages sending (A). Acquittal messages sending (B).

(2) Authentication phase : Authentication is the most important phase in our solution. To achieve it, we implemented the Certificate-less public key encryption system of Dent, Libert, & Paterson (2008). Figure 8 illustrates the successful authentication of a sensor. Here the gateway just transmits messages from sensors

to the hospital server and vice versa. This is to run the authentication protocol explained in 6.2.1.

It should be noted that the gateway in our system can be used for other purposes such as providing to patients some user-friendly interfaces with several functionalities. For example, the gateway saves locally some vital sign that patients can, in addition to some local processing to alarm patients in case of connection loss with central services care or in case of detecting some abnormal measure of vital signs.

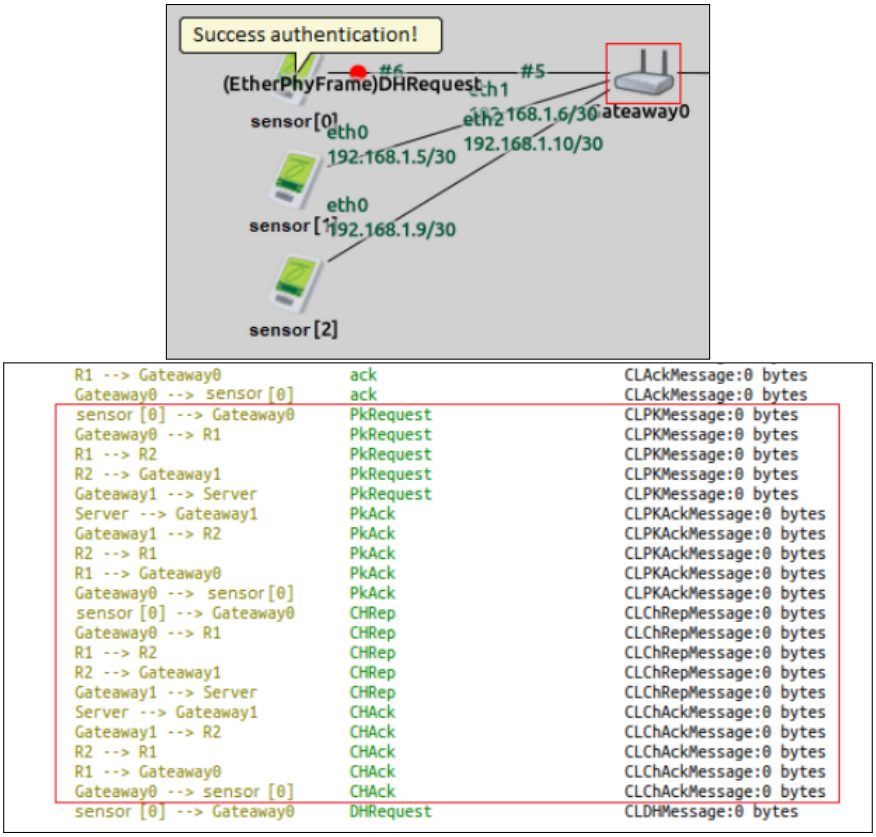
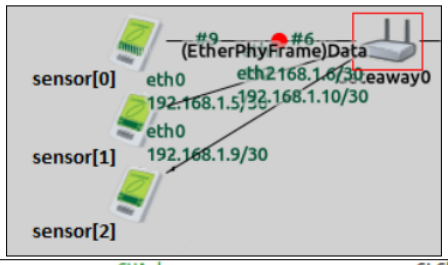


Figure 8.: Authentication of a sensor.

(3) Session key generation and data sending : As soon as the EHR manager authenticates the sensors, the two parties negotiate a session key to establish a secure communication channel for the transfer of the data packets. Once the secure channel is established, the sensors encapsulate vital signs in a data packet, encrypt the data packet using the session key, and send it to the hospital. Figure 9 shows messages exchanged during the generation of the session key and sending of the data packets.

Furthermore, we set up a real patient home environment with a real sensor and a multi-function gateway. Figure 10 show the gateway with a snapshot of real-time sensing of the ECG sensor. Results of both simulation and real experiment are very satisfactory and show that our approach is effective while being easy to use with a low computational cost for constraint devices.



R1 --> Gateaway0	CHAck	CLChAckMessage:0 bytes
Gateaway0 --> sensor[0]	CHAck	CLChAckMessage:0 bytes
sensor[0] --> Gateaway0	DHRequest	CLDHMessage:0 bytes
Gateaway0 --> R1	DHRequest	CLDHMessage:0 bytes
R1 --> R2	DHRequest	CLDHMessage:0 bytes
R2 --> Gateaway1	DHRequest	CLDHMessage:0 bytes
Gateaway1 --> Server	DHRequest	CLDHMessage:0 bytes
Server --> Gateaway1	DHAck	CLDHMessage:0 bytes
Gateaway1 --> R2	DHAck	CLDHMessage:0 bytes
R2 --> R1	DHAck	CLDHMessage:0 bytes
R1 --> Gateaway0	DHAck	CLDHMessage:0 bytes
Gateaway0 --> sensor[0]	DHAck	CLDHMessage:0 bytes
sensor[0] --> Gateaway0	Data	CLDataMessage:64 bytes
Gateaway0 --> R1	Data	CLDataMessage:64 bytes
R1 --> R2	Data	CLDataMessage:64 bytes
R2 --> Gateaway1	Data	CLDataMessage:64 bytes
Gateaway1 --> Server	Data	CLDataMessage:64 bytes
sensor[0] --> Gateaway0	Data	CLDataMessage:64 bytes
Gateaway0 --> R1	Data	CLDataMessage:64 bytes
R1 --> R2	Data	CLDataMessage:64 bytes
R2 --> Gateaway1	Data	CLDataMessage:64 bytes
Gateaway1 --> Server	Data	CLDataMessage:64 bytes
sensor[0] --> Gateaway0	Data	CLDataMessage:64 bytes

Figure 9.: Session key generation and data packets sending.

8. Security and Performance Analysis

In this section, we analyze firstly our proposal's security in terms of security requirements mentioned above (subsection 5.2) and compare it with existing solutions in the literature. Recall that our solution only meets the underlined security requirements, since the aim of our proposal in this paper is to carry out real experiments and simulations, bearing in mind the development of the proposal to meet further requirements in future work. Secondly, we move to the performance analysis of our proposal in comparison with existing ones.

8.1. Security Analysis

The proposed solution achieves data confidentiality at the BAN level through symmetric encryption of the patient's vital signs with the negotiated session key. Since this key is only known by the sensor and the EHR manager, an eavesdropper gains nothing useful from an intercepted data. In addition, the session key is negotiated between the participants only after they have been mutually authenticated. This prevents an attacker to impersonate either the sensor or the EHR manager. In other words, an attacker who replaces a participant's public key with a fake one, will not be able to decrypt ciphertexts encrypted with this key. This is because the corresponding private key's generation depends on the KGC's collaboration through the partial private key generation.

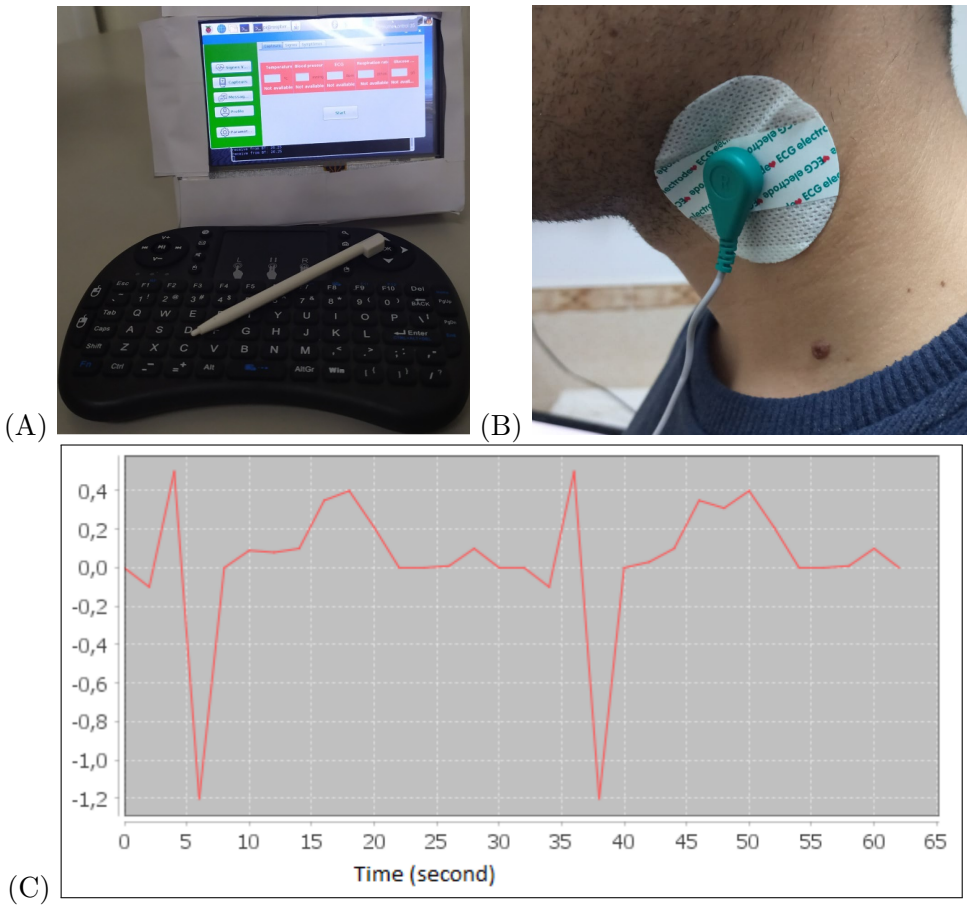


Figure 10.: The gateway (A). The ECG sensor (B). A real-time sensing from the ECG sensor (B).

Elsewhere, our proposal achieves a lightweight mutual authentication and key agreement scheme. That is, the participants authenticate each other only by verifying the public key's validity based on pairings on elliptic curves (Joux (2002)). Also, our proposal is resistant to the man-in-the-middle attack that could be carried out even by a compromised KGC and this, by applying the same bind technique proposed by Al-Riyami & Paterson (2003). The replay attack is prevented by the freshness of session keys by sending only new random values (i.e. T_A, T_B).

At the hospital level, access control is provided through the application of a role-based access control according to the role of each medical staff member. This prevents even authenticated medical staff members to gain access to patient's sensitive data to which they are not entitled. Data confidentiality is therefore ensured and further enhanced as EHRs are encrypted by the EHR manager using the patient's symmetric keys which are also encrypted by the EHR manager's private key.

Table 1 presents a comparison of the security requirements ensured by our proposal and existing related solutions in the literature. We note that the existing works do not address security of the entire RPM system, while our proposal ensure security at each part of the NIST's RPM system archi-

tecture. Besides, our solution security resists various type of attacks such eavesdropping attack, man-in-the-middle attack, replay attack, and impersonation attack. Confidentiality and Data authentication are ensured by the use of the AES symmetric encryption algorithm and our authentication and key agreement protocol, respectively.

Table 1.: Security attributes comparison.

RPM system's parts	Security attributes	w1	w2	w3	w4	w5	w6	Ours
BAN	Confidentiality	-	✓	✓	-	✓	✓	✓
	Authentication	-	✓	✓	-	✓	✓	✓
	Privacy	-	✓	✓	-	✓	✓	✓
Network	Confidentiality	-	✓	-	✓	✓	✓	✓
Hospital	Access Control	-	-	✓	✓	-	-	✓
	Privacy	✓	-	-	✓	✓	-	✓

w1: Zhang et al. (2014) w2: Srinivas et al. (2017)
w3: Ondiege et al. (2017) w4: Hupperich et al. (2012)
w5: Alzahrani et al. (2020) w6: Yaacoub et al. (2020)

8.2. Performance Analysis

The findings in the Related Works section show that existing works rely on PKI to ensure an RPM system's participants authentication and there is little real implementation of secure RPM systems. Also, almost of these works are simulated which does not give a clear view on real-time and empirical evidence on proper implementation of such systems.

The RPM system we developed is based on CL-PKC which provides more flexibility, as it avoids the management and verification of certificates. Since the infrastructure needed to support CL-PKC is lightweight when compared to a traditional PKI (Al-Riyami & Paterson (2003)), and small ECC keys have the equivalent strength of larger RSA keys (Mallouli, Hellal, Saeed, & Alzahrani (2019)), our Secure RPM system is lightweight and more efficient.

Table 2 summarizes the performance comparison in terms of the computation cost and number of exchanged messages of our authentication and key agreement protocol among other existing protocols. The performance parameters and hardware platform we have considered were taken from (Dharminder, Mishra, & Li (2020)). That is, we considered for the security level a 1024-bit cyclic group and a 160-bit point in the prime field $\mathbb{F}_p$, and AES and SHA1 algorithms for symmetric encryption and hash function, respectively. Let $T_s = 0.0064\ s$ and $T_s = 0.00032\ s$ be the execution time of AES and SHA1 algorithms, respectively. Let $T_c = 0.0.0171\ s$, $T_e = 0.01922\ s$ and $T_p = 0.0513\ s$ be the time execution of elliptic curve point multiplication, exponentiation modulo and bilinear pairing operations, respectively.

From Table 2, although our protocol is more efficient in terms of communication cost (only two exchanged messages), however, it costs $0.0516\ s$ which is higher than those of Dharminder et al. (2020), Srinivas et al.

(2017), and Alzahrani et al. (2020) schemes, but less than Wu, Xu, Kumari, & Li (2017) scheme. This is due to the so-known computational cost of the pairing operations (Baek, Safavi-Naini, & Susilo (2005)). Notice that there are several pairing-free CL-PKC cryptosystems (Yang, Wang, & Mu (2021) and Du, Wen, & Zhang (2019)) which we can adopt to our protocol in future work. This would render our scheme more efficient.

Overall, our authentication and key agreement protocol uses only two passes and thus, is efficient in terms of communication cost. Additionally, it is efficient in terms of computation cost since no encryption/decryption operation is required in the authentication step, whereas in traditional PKI, authentication requires certificate verification which is expensive in terms of resource and computation time, especially by resource-constrained devices in an RPM system. To ensure the freshness of session keys and thus prevent the replay attack, the involved participants need the only transmission of new random values (i.e. T_A, T_B).

Also, solutions that rely on password-based authentication using smart cards are both prone to DOS and smart card theft on one hand, and are not flexible on another hand, especially in an emergency situation where a healthcare staff may forget their smart card.

Table 2.: Performance comparison.

Schemes	w1	w2	w3	w4	Ours
Computation cost (s)	$2T_e + 9T_h$ ≈ 0.0412	$3T_s + 8T_h$ ≈ 0.0217	$2T_s + 23T_h$ ≈ 0.0201	$4T_c + 4T_s + 26T_h$ ≈ 0.1023	$T_p + T_h$ ≈ 0.0516
Messages	2	3	4	4	2

w1: Dharminder et al. (2020) w2: Srinivas et al. (2017)

w3: Alzahrani et al. (2020) w4:Wu et al. (2017)

9. Conclusion

This paper presents a security solution for a remote patient monitoring system. For this purpose, we have developed a secure RPM system dedicated to the home monitoring of elderly people with chronic diseases. As mentioned above, the major problem for such a solution is security which is provided generally with a solution based on conventional PKI or RSA based authentication schemes. To address the drawbacks of the existing security proposals in a resource-constrained environment, we introduced in our work, Certificate-less public key cryptography (CL-PKC), which is a lightweight, efficient and secure solution compared to traditional PKI.

Our approach ensures secure authentication, access control to EHRs, and medical data protection using CL-PKC, RBAC, and AES algorithm, respectively. The solution has been successfully implemented in both simulated and real environment. The obtained results are satisfactory in terms of security requirements, and computation and communications costs.

References

Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE Journal of Biomedical and Health Informatics*, *18*(4), 1431–1441.

Al-Riyami, S. S., & Paterson, K. G. (2003). Certificateless public key cryptography. In *International conference on the theory and application of cryptology and information security*, (pp. 452–473). Springer.

Altamimi, A. M., et al. (2016). Security and privacy issues in ehealthcare systems: towards trusted services. *International Journal of Advanced Computer Science and Applications*, *7*(9), 229–236.

Alzahrani, B. A., Irshad, A., Alsubhi, K., & Albeshri, A. (2020). A secure and efficient remote patient-monitoring authentication protocol for cloud-iot. *Int. J. Commun. Syst.*, *33*(11). URL `https://doi.org/10.1002/dac.4423`

Azeez, N. A., & Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. *Egyptian Informatics Journal*, *20*(2), 97–108.

Baek, J., Safavi-Naini, R., & Susilo, W. (2005). Certificateless public key encryption without pairing. In J. Zhou, J. López, R. H. Deng, & F. Bao (Eds.) *Information Security, 8th International Conference, ISC 2005, Singapore, September 20-23, 2005, Proceedings*, vol. 3650 of *Lecture Notes in Computer Science*, (pp. 134–148). Springer. URL `https://doi.org/10.1007/11556992_10`

Barua, M., Liang, X., Lu, R., & Shen, X. (2011). Espac: Enabling security and patient-centric access control for ehealth in cloud computing. *International Journal of Security and Networks*, *6*(2-3), 67–76.

Benzschawel, S., & Da Silveira, M. (2011). Protecting patient privacy when sharing medical data. In *Proceedings of the 3rd International Conference on eHealth, Telemedicine, and Social Medicine (eTelemed), France*. Citeseer.

Biswas, S., Anisuzzaman, Akhter, T., Kaiser, M. S., & Mamun, S. A. (2014). Cloud based healthcare application architecture and electronic medical record mining: An integrated approach to improve healthcare system. In *2014 17th International Conference on Computer and Information Technology (ICCIT)*, (pp. 286–291).

Della Mea, V. (2001). What is e-health (2): The death of telemedicine? *J Med Internet Res*, *3*(2), e22. URL `http://www.jmir.org/2001/2/e22/`

Dent, A. W., Libert, B., & Paterson, K. G. (2008). Certificateless encryption schemes strongly secure in the standard model. In *International workshop on public key cryptography*, (pp. 344–359). Springer.

Dharminder, D., Mishra, D., & Li, X. (2020). Construction of rsa-based authentication scheme in authorized access to healthcare services - authorized access to healthcare services. *J. Medical Syst.*, *44*(1), 6:1–6:9. URL `https://doi.org/10.1007/s10916-019-1471-6`

Du, H., Wen, Q., & Zhang, S. (2019). An efficient certificateless aggregate signature scheme without pairings for healthcare wireless sensor network. *IEEE Access*, *7*, 42683–42693. URL `https://doi.org/10.1109/ACCESS.2019.2907298`

Fan, L., Buchanan, W., Lo, O., Thümmler, C., Lawson, A., Uthmani, O., Ekonomou, E., Khedim, A. S., & Sharif, T. (2012). Spoc: protecting patient privacy for e-health services in the cloud. *eTELEMED*, *2012*, 99–104.

Gutmann, P. (2002). Pki: it's not dead, just resting. *Computer*, *35*(8), 41–49.

Hamoud, O. N., Kenaza, T., & Challal, Y. (2019). A new certificateless system construction for multiple key generator centers to secure device-to-device communications. In *ICETE (2)*, (pp. 84–95).

Hupperich, T., Löhr, H., Sadeghi, A.-R., & Winandy, M. (2012). Flexible patient-controlled security for electronic health records. In *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*, (pp. 727–732).

Jennifer, C., Nakia, G., Bronwyn, H., Jason, K., Kevin, L., Julie, S., Sue, W., Ryan, W., & Kangmin, Z. (2020). Nist special publication 1800-30 : Securing telehealth remote patient monitoring ecosystem. Tech. rep., National Institute of Standards and Technology.
URL https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth

Joux, A. (2002). The weil and tate pairings as building blocks for public key cryptosystems. In C. Fieker, & D. R. Kohel (Eds.) *Algorithmic Number Theory, 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002, Proceedings*, vol. 2369 of *Lecture Notes in Computer Science*, (pp. 20–32). Springer.
URL https://doi.org/10.1007/3-540-45455-1_3

Kumar, P., & Lee, H.-J. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey. *sensors*, *12*(1), 55–91.

Malasinghe, L. P., Ramzan, N., & Dahal, K. P. (2019). Remote patient monitoring: a comprehensive study. *J. Ambient Intell. Humaniz. Comput.*, *10*(1), 57–76.
URL https://doi.org/10.1007/s12652-017-0598-x

Mallouli, F., Hellal, A., Saeed, N. S., & Alzahrani, F. A. (2019). A survey on cryptography: Comparative study between RSA vs ECC algorithms, and RSA vs el-gamal algorithms. In M. Qiu (Ed.) *6th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2019 / 5th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom 2019, Paris, France, June 21-23, 2019*, (pp. 173–176). IEEE.
URL https://doi.org/10.1109/CSCloud/EdgeCom.2019.00022

Monshizadeh, M., Khatri, V., Koskimies, O., & Honkanen, M. (2020). *IoT Use Cases and Implementations*, chap. 12, (pp. 225–245). John Wiley Sons, Ltd.
URL https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119527978.ch12

Niksaz, P., & Branch, M. (2015). Wireless body area networks: attacks and countermeasures. *Int. J. Sci. Eng. Res*, *6*(9), 556–568.

Ondiege, B., Clarke, M., & Mapp, G. (2017). Exploring a new security framework for remote patient monitoring devices. *Computers*, *6*(1).
URL https://www.mdpi.com/2073-431X/6/1/11

Qiu, H., Qiu, M., Memmi, G., & Liu, M. (2020). Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. *IEEE Journal of Biomedical and Health Informatics*, (pp. 1–1).

Rasyid, M. U. H. A., Sukaridhoto, S., Sudarsono, A., & Kaffah, A. N. (2020). Design and implementation of hypothermia symptoms early detection with smart jacket based on wireless body area network. *IEEE Access*, *8*, 155260–155274.

Shamir, A. (1984a). Identity-based cryptosystems and signature schemes. In *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, (pp. 47–53).
URL https://doi.org/10.1007/3-540-39568-7_5

Shamir, A. (1984b). Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques*, (pp. 47–53). Springer.

Shin, M. S., Jeon, H. S., Ju, Y. W., Lee, B. J., & Jeong, S.-P. (2015). Constructing rbac based security model in u-healthcare service platform. *The Scientific World Journal*, *2015*.

Srinivas, J., Mishra, D., & Mukhopadhyay, S. (2017). A mutual authentication framework for wireless medical sensor networks. *J. Medical Syst.*, *41*(5), 80:1–80:19.
URL https://doi.org/10.1007/s10916-017-0720-9

T.Jayasankar, N. G. S. R., R.M.Bhavadharini (2021). Securing medical data using extended role based access control model and twofish algorithms on cloud platform. *European Journal of Molecular amp; Clinical Medicine*, *8*(1), 1075–1089.
URL https://ejmcm.com/article_6677.html

Wu, F., Xu, L., Kumari, S., & Li, X. (2017). A new and secure authentication scheme for wireless sensor networks with formal proof. *Peer Peer Netw. Appl.*, *10*(1), 16–30.
URL https://doi.org/10.1007/s12083-015-0404-5

Yaacoub, E., Abualsaud, K., Khattab, T., & Chehab, A. (2020). Secure transmission of iot mhealth patient monitoring data from remote areas using dtn. *IEEE Network*, *34*(5), 226–

231.

Yang, W., Wang, S., & Mu, Y. (2021). An enhanced certificateless aggregate signature without pairings for e-healthcare system. *IEEE Internet Things J.*, *8*(6), 5000–5008.
URL https://doi.org/10.1109/JIOT.2020.3034307

Yew, H. T., Ng, M. F., Ping, S. Z., Chung, S. K., Chekima, A., & Dargham, J. A. (2020). Iot based real-time remote patient monitoring system. In *2020 16th IEEE International Colloquium on Signal Processing Its Applications (CSPA)*, (pp. 176–179).

Zhang, R., Liu, L., & Xue, R. (2014). Role-based and time-bound access and management of ehr data. *Security and communication Networks*, *7*(6), 994–1015.

Zhou, X., Liu, J., Liu, W., & Wu, Q. (2016). Anonymous role-based access control on e-health records. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16, (p. 559–570). New York, NY, USA: Association for Computing Machinery.
URL https://doi.org/10.1145/2897845.2897871