A Three-Tier Approach for Lightweight Data Security of Body Area Networks in E-Health Applications

MIGUEL MORALES-SANDOVAL, RICARDO DE-LA-PARRA-AGUIRRE, HIRAM GALEANA-ZAPIÉN, AND ALEJANDRO GALAVIZ-MOSQUEDA

ABSTRACT Wireless body area networks (WBANs) can enable e-health applications under Internet of Things (IoT) scenarios. However, to use WBAN technologies in practical applications, sensitive data collected by wireless sensors must be protected when transmitted across a network and until accessed by authorized applications or end-users. Specifically, it is necessary to provide confidentiality, integrity, authentication, and access control in WBANs. This paper presents a security approach to provide these security services in a layered WBAN system using lightweight cryptography. Layer 1 consists of the communication between the sensor nodes and the base station (data acquisition); Layer 2 involves the communication between the base station and a data repository (data storage); and Layer 3 deals with the communication of end-users to the repository (data access). In the past, security has focused only on Layer 1 and for limited security levels. In this paper, security concerns in the three layers of a WBAN system are studied and addressed. As primary contributions, the design details of a secure WBAN system prototype and the impact of lightweight cryptographic engines on the performance of the primary use cases in the WBAN system are highlighted from data acquisition until data use. We present a novel WBAN system prototype that ensures most of the required security services for standard security levels.

INDEX TERMS The IoT, e-health, secure WBAN, security services, lightweight cryptography, attribute-based encryption.

I. INTRODUCTION

The demand for advanced healthcare applications is expected to grow with the progressive deployment of the Internet of Things (IoT), including remote patient monitoring, which has become a reality to continuously track vital sign data (e.g., blood pressure, blood oxygen levels, heart rate, etc.) from individuals. Then, collected information could be accessed by an authorized healthcare provider to enable, for example, the timely detection of clinical deterioration.

In this context, a prominent enabling technology in the IoT ecosystem to monitor patients’ vital sign data is the wireless body area network (WBAN). A WBAN is composed of small smart devices that play an important role as both data collectors and data gateways in WBAN applications. Such sensors can be either situated in a fixed position in the body or even carried at different positions in clothing if wearable-like sensors are used. In e-health applications, a WBAN aims to provide an efficient and reliable communication infrastructure to all implanted, nonimplanted and wearable sensor devices for the human body [1]. In this regard, because health data transmitted through a WBAN could be exposed to unauthorized parties, or even malicious adversaries, it is critical to ensure security services through the entire data stream (data life cycle), which involves data acquisition, data transmission to a storage system, and the data accessed by
authorized users. From an architectural viewpoint, the data cycle can be decomposed into a three-layer network architecture in terms of data collection (sensory stage), transmission (communication network) and storage (application).

The provision of security services over the entire data life cycle in a WBAN is of paramount importance to prevent attacks such as tampering, falsification, or data capture by a third party. The development of security and privacy services for IoT healthcare architectures is an important research area [2]. Two core challenging issues related to the design and development of secure WBANs have been addressed thus far. On the one hand, since a standardized system architecture is not well defined, data restriction and preservation of its integrity and the robustness of the WBAN system, in general, are not achieved [3]. On the other hand, the design of computational and energy efficient security mechanisms is essential because WBAN sensors are resource-constrained devices.

As in other systems, WBANs require security services at three architectural layers that provide confidentiality (C), integrity (I), authentication (A) and access control (AC) [4], [5]. Each of these services can be guaranteed when using cryptography algorithms and, in this particular case, by lightweight cryptography algorithms [6], [7]. Unfortunately, few studies have investigated these security services (C, I, A, and AC) at a time when e-health services are relying on a WBAN. Specifically, most existing research regarding secure WBANs primarily investigated the design of lightweight security services for data collection (e.g., those produced in the sensor nodes and delivered to a base station) [8]–[10]. Other studies reported custom security protocols that address some but not all of the required security services [11]–[14], or practical deployments with experimental evaluation of security mechanisms are missing [15]–[17]. It is worth noting that custom protocols usually only address one single security service, and only for two actors in the WBAN (sensor node and base station, or sensor node and cloud server). However, an integrated approach that can provide security services to protect the entire data life cycle in a WBAN has not yet been proposed for all recommended security services, since data is produced in the sensor nodes, when data is transmitted to the base station then to the cloud server, and until data is finally accessed by end users (nurse, pharmacy, doctors, etc).

This study aims to fill this void. The primary contributions of this study are enumerated below.

1) We propose a novel abstraction model in which each security service (C, I, A, or AC) is characterized by a set of generic operations, which are provided by algorithms that have been carefully selected from the state-of-the-art on lightweight cryptography.

2) A holistic security model for e-health in WBANs is developed and validated to provide four security services within the three layers of a WBAN system.

3) As a proof-of-concept, a prototype was designed and validated with real-world wearable devices. This prototype was used as the experimental platform to evaluate the impact of lightweight cryptography on three primary figures of merit in WBAN systems, execution time, memory usage and energy consumption.

The proposed prototype allows us to evaluate the costs of providing security services over the entire data life cycle in WBAN deployments with resource-constrained devices. Results show that this cost is tolerable for end-users when sensitive data are protected with recommended security levels against the most common threats to confidentiality, integrity, authentication and access control.

In this study, we take advantage of available lightweight cryptographic algorithms and provide a security approach under a WBAN model that is commonly found in practice, where the data life cycle requires specific security services (not only confidentiality and authentication), including access control mechanisms, at different stages in the WBAN model. Relying on standard cryptographic engines improves interoperability and practical deployment of the proposed security approach. To our knowledge, this study represents the first attempt to evaluate lightweight cryptography on a three-layered WBAN prototype. The analysis and results presented in this study can be used as a reference for the evaluation of specific e-health applications, such as remote patient monitoring and teleconsultation.

The remainder of this article is organized as follows. Section II presents preliminaries and the system model of the WBAN. In Section III, a review of the literature is presented and highlights related studies that used security services in some layers of a WBAN, as well as the algorithms used to guarantee these services. An abstraction-based security scheme used as the basis for designing the secure WBAN is presented in Section IV. This section also presents the design of secure WBANs, including security services and the cryptographic algorithms used for secure WBAN realization. Section V provides the implementation details of the proposed abstraction-based security scheme. We propose a prototype in which a ciphersuite of lightweight cryptographic algorithms for encryption, hash, message authentication, and access control is validated. In Section VI, we describe the experimental evaluation and analyze the results of this study, primarily focusing on the impact of the security scheme on the WBAN performance. Finally, Section VII provides concluding remarks.

II. PRELIMINARIES

We now present background information regarding the context of this study. Specifically, we describe the primary components of a generic WBAN architecture according to the well-known three-layer model. Then, we discuss the typical security services that are expected to be supported in a WBAN environment for collecting and transmitting healthcare data. Finally, we briefly summarize the primary lightweight security approaches for WBANs.
A. WIRELESS BODY AREA NETWORKS

A WBAN is a wireless communication network between low-power sensing devices that is used around the body of a patient. Thus, WBANs are considered wireless sensor networks (WSNs) that have a special purpose and are used to provide communication solutions for medical applications [18], [19]. Specifically, a WBAN is defined in the IEEE 802.15.6 standard as a communication standard designed for low-energy-consumption devices and used for the benefit of patients [20]. In addition to the IEEE 802.15.6 standard, other wireless technologies, such as IEEE 802.15.4 and Bluetooth, have been widely used to enable WBANs in the literature [21], [22].

As with WSNs, WBANs are vulnerable to security attacks because they continuously collect physiological data to monitor people’s physical condition. Considering the security challenges of WBANs and the importance of the data that is transmitted in them, it is necessary to guarantee security services to keep the data protected [5].

The network security issues in WBANs are commonly addressed in the sensor-base station (BS) layer [23]. However, in different e-health applications, collected data are sent to the cloud for storage and processing purposes. Then, users request access to healthcare data, for example, for knowledge extraction [3]. Therefore, security concerns should be addressed throughout the data flow. Thus, we propose that WBAN security in e-health applications should be constructed as a three-layer security model, as shown in Fig. 1. As previously mentioned, the communication that occurs between WBAN components is divided into three separate layers [24]:

- **Layer 1. Data collection**: Sensor interaction is limited to the patient body. Data transmission is between sensors and BS, which works as a data source in layer 2.
- **Layer 2. Communication**: Communication connects the BS with layer 3 to send the sensors’ data via the Internet to a repository.
- **Layer 3. Application**: Tasks are executed to retrieve sensed data and to analyze those data. Both tasks are performed by authorized entities.

B. SECURITY SERVICES IN WBANs

Security services are considered security mechanisms to mitigate the risks that exist in a networked environment, such as WBANs [25]. Data obtained from WBAN sensors are particularly sensitive, which is how WBANs can be subject of attacks [24]. Attacks can be passive (e.g., eavesdropping on traffic between WBAN components: sensors, BS, and the remote repository) or active (e.g., injecting, modifying or replaying messages). Cryptography has traditionally addressed security and privacy issues in networked environments on the premise that security is centered on data. Thus, if data are encrypted, attackers are unable to access the data in plaintext form (e.g., compromise health information in transit or at rest). With cryptography, it is also possible to ensure integrity and authentication over the data generated and transmitted; thus, the entities involved in communications can perform verification checks to validate the source and destination of data and discard possible fake messages coming from unauthenticated sources. Security then relies on the strength of underlying cryptographic algorithms. Other attacks related to perimeter security (e.g., intrusion detection) or physical security (e.g., compromise device functionality) are out of the scope of cryptographic algorithms.

In a WBAN, the following security requirements are required:

- **Confidentiality.** To prevent confidential information from being revealed to unauthorized persons, this service ensures that data are transmitted securely and confidentially between origin and destination.
- **Integrity.** This service allows the detection of intentional or unintentional alterations of the data from its origin to its destination, which may include insertion,
deletion or substitution of data, and allows the user to verify if the information has been altered.

- **Authenticity.** This service ensures that the data must be sent from legitimate entities, and that senders and receivers must confirm their identity.

- **Access control.** Apart from ensuring that only authorized users can access the data, this service validates the tasks they can perform within a system.

### C. Lightweight Cryptography

In the IoT, many interconnected devices with limited resources are not designed to perform continuous data-intensive computing that severely impacts their energy consumption, as is the case when using cryptographic algorithms, which are widely known to be computationally intensive. Therefore, most conventional cryptographic algorithms are difficult to implement in IoT devices (e.g., sensor nodes) with reduced computing capabilities and insufficient to run classical cryptography techniques. This issue leads to a branch of cryptography called lightweight cryptography [7], which is focused on the design and implementation of cryptographic algorithms by considering the limitations of the devices on which they will run.

In a WBAN environment, security services can be guaranteed by a lightweight cryptographic algorithm:

- **Lightweight block encryption** [26]. Symmetric key cryptography can be used to provide confidentiality, which is based on a shared key that is used to encrypt plaintext or to decrypt ciphertext. A block cipher is a type of symmetric cipher that processes information blocks (often 64- or 128-bit blocks) through several rounds.

- **Lightweight hash function.** Integrity is generally guaranteed by a cryptographic hash function $H$, which is also called the checksum function. This algorithm uses a fixed-length hash value calculated from a piece of data (a bit string) of arbitrary size. The function uses every bit of the input data to generate a unique unrepeatable code of fixed length through a series of processing rounds.

- **Message Authentication Code (MAC).** MAC values are used to authenticate a message. The MAC generation takes two arguments: a fixed size $k$ key and an arbitrary length $M$ message. MAC values are calculated using a cryptographic hash function $H$ to $M$ mixed with $k$, which is known only to the sender and receiver.

- **Attribute-based encryption.** Attribute-based encryption is an effective method to achieve fine-grained access control, where encrypted data must be readable only by a group of users who satisfy a certain access policy [27]. This type of encryption is based on identity-based encryption (IBE) and replaces the use of an identity with a set of attributes that validate if the entity is certified and with access permissions. ABE systems use an access structure $\mathcal{A}$ that is defined by a logical expression on a set of attributes belonging to a universe $U$. $\mathcal{A}$ specifies a nonvoid subset of the power set $\mathcal{P}(U)$. Each set in $\mathcal{A}$ is an authorized set of attributes that is allowed to decrypt ABE-encrypted data, while the sets in $\mathcal{P}(U)$ but not in $\mathcal{A}$ are non-sets authorized [28].

Even though lightweight cryptography is intended to provide security services in constrained computing environments (e.g., WBANs), there are still several problems to solve, most importantly, the compromise between WBAN efficiency and the level of security achieved by the block cipher, a hash function or an MAC algorithm. The greater the security level is, the lower the performance and lifetime of a WBAN. Additionally, the greater the security level is, the more energy and memory consumed in the devices. With ABE-based access control, more elaborate policies (e.g., more attributes or more complex policies to restrict data access at the application level) lead to lower performance, increased memory and energy consumption and a penalty in the performance of underlying computing devices.

### III. RELATED WORK

Efforts have been made to provide security services in WBANs based on cryptographic algorithms. In the literature, there is a consensus that the security services that should be guaranteed in WBANs include the CIA triad (confidentiality, integrity, and authentication). AC services are also considered because several users (doctors, nurses, patients, etc.) interact with the WBAN to access the data.

Based on the three-layered model of a WBAN system for e-health applications, Table 1 shows the most important studies of WBAN security considerations, and Table 2 summarizes the cryptographic algorithms used in related studies to highlight the different security services in a WBAN.

![Table 1](image-url)

**TABLE 1.** Existing approaches used to provide security services in each layer of WBANs.
Table 1 shows that the four security services of interest have not been considered concurrently in the complete data life cycle, covering the three layers of a WBAN deployment. Conversely, Table 2 shows that security services in previous WBAN studies have been provided primarily through cryptographic algorithms. However, most related studies have limited the validation of security solutions in simulations, and few have reported implementation results from a prototype. The security level provided, if less than 128 bits, is also obsolete [41]. The community and standards coincide that cryptographic security solutions must provide a security level of at least 128 bits [42].

The most common security services being implemented are confidentiality and authentication, followed by access control and then integrity. All related studies primarily focused on Layer 1 of the WBAN model because patient data is generated in this layer. However, for the entire data life cycle, data must be protected from origin (sensor nodes) to final delivery point (access by end-users), which is not covered in existing research.

Lightweight symmetric ciphers have been used to ensure confidentiality, with the exception of AES and Twofish, which are general-purpose symmetric ciphers. For authentication, most related studies used an asymmetric approach (e.g., digital signatures). Integrity is ensured in only three studies; two of them using an asymmetric approach via digital signatures. To ensure access control, all related studies use ABE.

The authors in [11] proposed a three-tier security architecture that is different from that presented in this study. Security is addressed by a custom method that is based on key management (one for each tier, comprised of sensor nodes, base stations, and network connection nodes) and hash functions. Instead of custom methods, other studies used cryptographic algorithms to achieve confidentiality, authentication or access control. Refs. [30], [31] use lightweight ciphers at Layer 1 but do not provide authentication or access control. In [8], the authors use signcryption to provide confidentiality, authentication and integrity within the three layers of the WBAN model. However, access control is not implemented. Also, signcryption is a public-key cryptography that uses cryptographic pairings, which imposes a penalty in processing for the sensor nodes in Layer 1.

Authentication is one of the most studied security services in WBANs. Some studies focus only on this service under the assumption that confidentiality or access control is ensured by other means. Authentication has typically been approached either using known cryptographic algorithms (e.g., public key cryptography, identity-based encryption) or by custom solutions that are generally based on key management and hashing. Elliptic curve-based signatures are used in [15], [32], [33], and [37] to authenticate data in Layer 1, and authentication relying on identity-based encryption (IBE) signatures is studied in [13] and [40] to authenticate the sensor nodes and a cloud server. Both of these studies present results from simulations only and for an outdated security level (80 bits) in the first study. IBE is achieved with cryptographic pairings, which are heavy algorithms for sensor nodes. The complexity of pairings increases considerably when the security level also increases. Thus, IBE solutions for WBANs can be difficult to implement in practice for recommended security levels. Examples of custom solutions for authentication in WBANs are proposed in [38] and [39]. In [38], a custom authentication algorithm between the sensor node and a base station (personal server) that is based on the use of a hash function and key management is presented.
TABLE 3. Abstractions for the security services required in a WBAN.

| Abstraction | Description                  | Operation                                  | Security service |
|-------------|------------------------------|--------------------------------------------|------------------|
| E           | Symmetric block cipher       | $C_D = E(ENC(k_i, D))$                      | Confidentiality  |
|             |                              | $D = E(DEC(k_i, C_D))$                      |                  |
| H           | Data hash                    | $h_i = H(GEN(C_P))$                         | Integrity        |
| MAC         | Message Authentication Code  | $\sigma = MAC\cdot GEN(k_i, h_i)$          | Authentication   |
|             |                              | $\{0, 1\} = MAC\cdot VER(\sigma, k_i, h_i)$ |                  |
| ABE         | Attribute-based encryption   | $C_P = ABE\cdot ENC(P, k_i)$               | Access control   |
|             |                              | $k_i = ABE\cdot DEC(SK_U, C_P)$             |                  |

Security at Layers 2 and 3 nor the security services of confidentiality, integrity and access control are considered. No details are given on the implementation or simulation, nor is the security level used. In [39], a similar approach is presented to authenticate the sensor node and the cloud server directly based on the use of hash functions and key management to cover Layers 1 and 2 in the proposed model, assuming that there is not a base station or personal server as in [38]. Experiments are reported using a single sensor node and a desktop computer as the server.

Thus, the literature review shows that although some studies have developed secure WBANs, not all the required security services have been supported, not all the layers of the WBAN have been considered to be secured, and in some studies, the security level used is obsolete (Tables 1 and 2). To our knowledge, a holistic security model for WBANs in e-health applications that considers the three layers discussed in the previous sections has not been previously reported in the literature. In this paper, a three-layer security model is proposed to design a secure WBAN for e-health applications. In addition, an experimental testbed was implemented to evaluate the proposed model under a real WBAN prototype.

IV. DESIGN OF A SECURE WBAN FOR E-HEALTH APPLICATIONS

To design a secure WBAN, we defined a security scheme that is based on abstractions associated with the security services required in a WBAN, as previously discussed in Section III. Each security service is guaranteed by a cryptographic defense mechanism: lightweight cryptographic algorithms.

A. ABSTRACTION MODEL

Abstractions are defined according to the notation shown in Table 3. To ensure confidentiality, a data encryptor is required to use a secret key shared between the involved entities. We refer to this process with the notation $E$. The integrity service is obtained by generating a hash of the data, which is denoted as $H$. Authentication is guaranteed by generating message authentication codes from the input data, which are denoted as MACs. Finally, data access control is achieved by encrypting the data using attribute-based encryption (ABE).

Each abstraction in Table 3 defines a set of operations (e.g., data encryption or decryption using a symmetric key, MAC generation/verification using an authentication key, or encryption/decryption using an access control policy).

In $E$, $ENC$, $k$ is a symmetric key, and $D$ is the data to be encrypted. In $E$, $DEC$, the same symmetric key $k$ is used, and $C_D$ is the ciphertext, which is the result of the $E$. $ENC$ operation. $H \cdot GEN(D)$ produces the hash of the data $D$. $MAC \cdot GEN(k, D)$ uses a key $k$ and data $D$ to generate the authentication code of $D$. For verification, $MAC \cdot VER(\sigma, k, D)$ verifies if $\sigma$ (the result of $MAC \cdot GEN(k, D)$) is the valid authentication code of $D$. Finally, $ABE \cdot ENC(P, K_a)$ uses the access control policy $P$ to encrypt the symmetric $k_a$. This key is that used by $E$. In $ABE$, $DEC(SK_U, C_P)$, $SK_U$ is an access key generated based on the attributes of user $U$, and $C_P$ is the ciphertext resulting from $ABE \cdot ENC$.

B. DESIGN OF A SECURE WBAN

Based on the abstractions summarized in Table 3, we define the model of a secure WBAN for e-health applications based on three layers. Security services are provided at each layer of the secure WBAN based on the abstractions and their operations defined in the security model. In Table 3, $k_i$ is a shared secret key, $SK_U$ is a secret access key assigned to user $U$, $P$ is an access control policy and $D$ is the data from the sensors. In this section, we present the details of the approach to provide security services through cryptography to a WBAN based on the three-layer model. We also make the following assumptions:

1) The BS stores a symmetric key $k_i$, which is shared uniquely with the sensor node $S_i$.
2) Each access control policy $P$ is defined by the system administrator (e.g., hospital administrator) by considering the available attributes under the format required by the ABE algorithm.
3) The generation of user private keys $SK_U$ ensures that data access can only be granted by the system administrator.

In the following, the process involving the provision of security services at each layer of the WBAN model is described.

- Layer 1 (data collection). In this layer, CIA-triad security services are guaranteed for data collection and transmission from each sensor $S_i$ to the BS in the WBAN. In Fig. 2, the operation and interactions between nodes in Layer 1 are shown. After collecting vital sign data, which are denoted as $D$, an encryption and authentication process is applied before transmission to the BS.
When the BS receives the data, integrity and authentication checks are performed using the \texttt{MAC.VER} operation. Data access control is performed by encrypting the symmetric key \(k_i\) shared with \(S_i\) using \texttt{ABE.ENC} with the access control policy \(P\). Generation and access to \(k_i\) is performed directly in code so that it is not possible to isolate the key and obtain it via a third unauthorized party or by the same user \(U_j\) for later distribution.

• **Layer 2 (communication).** This layer of the secure WBAN model encompasses communication and data transfer from the BS to a repository. The collected data are administered by a trusted authority (TA), which is the same authority in the ABE system in this case. The BS sends \(C_D\) and \(C_P\), which was already authenticated previously, to the repository. These encrypted data are received and verified by the BS using the \texttt{MAC.VER} operation. Data are rejected if the verification process does not succeed. Fig. 3 shows the interaction on layer 2 of the secure WBAN model.

• **Layer 3 (application).** Access to the collected data is managed by the system administrator TA. Each user \(U_j\) should request an access key to the TA, which in turn assigns the attributes that correspond to \(U_j\) and generates the user key \(SK_{U_j}\). With \(SK_{U_j}\), \(U_j\) can retrieve and decrypt the WBAN data in the repository managed by the system. The decryption process is achieved whenever the user attributes embedded in \(SK_{U_j}\) satisfy the policy \(P\) used to encrypt the private key in the BS. Fig. 4 shows the interaction in Layer 3 in the secure WBAN model.

### C. LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS

Based on the security services required in a secure WBAN for e-health applications, lightweight cryptographic algorithms are ideal for deploying the security scheme described in the previous sections. There are several lightweight cryptographic algorithms in the literature, and NIST’s selection process of an algorithm as the standard in lightweight cryptography has considered several proposals. However, there are standards that already consider lightweight cryptography, including ISO/IEC 29192-2:2019 [43], which features three lightweight algorithms for block encryption: PRESENT [44], CLEFIA [45], and LEA [46]. The first two algorithms were postulated as standards since 2012, while LEA was recently added to the list. The primary difference among the three algorithms is the number of rounds and the type of operation employed. Particularly, PRESENT uses 31 rounds and a network of permutations, while LEA uses 24, 28 or 32 rounds depending on the security level and is based on an ARX (Add, Rotation, XOR) architecture. Finally, CLEFIA uses 18, 22 or 26 rounds depending on the selected security level and based on a Feistel network.

Based on their recommendation on standards, acceptance and use in the community, we selected PRESENT and LEA for data confidentiality. PRESENT provides 80-bit and 128-bit security levels, but the 80-bit level is known to be obsolete today, as it can be violated via brute-force attacks. LEA provides security levels of 128 bits, 192 bits, and 256 bits, which makes it a better choice.
The cryptographic algorithms that can ensure data integrity were selected by considering the ISO/IEC 29192-5:2016 [47] which provides the standard algorithms for hash functions, including SPONGENT [48], a lightweight hash function with permutation sizes of 88, 136, 176, 240, and 272 bits that computes hash codes of length 88, 128, 160, 224, and 256 bits, respectively. SPONGENT uses sponge construction and the PRESENT permutations network. The second algorithm selected to provide integrity is QUARK [49], which is a lightweight hash function based on sponge construction and inspired by lightweight Grain and KATAN ciphers. The QUARK family of hash functions is composed of the three instances U-QUARK of 128 bits, D-QUARK of 160 bits and S-QUARK of 224 bits. QUARK can be used for
authentication messages, stream encryption or authenticated encryption.

Finally, we selected LIGHTMAC, one of the cryptographic algorithms that is part of the ISO/IEC 29192-6:2019 [50], to provide data authentication. LIGHTMAC [51] is an algorithm that generates MACs based on block encryption, where the length of the message has no effect on the security limit. What makes LIGHTMAC lightweight is the inclusion of PRESENT as the primary component for MAC generation.

In this study, we also considered using HMAC [52], a general purpose algorithm with the particularity of being lightweight by including a lightweight hash function (SPONGENT in this study).

D. SECURITY ANALYSIS

The security analysis for the three-tier model of a secure WBAN is based on the threat model that considers attacks initiated by unauthorized entities that can compromise the data in transit or at rest in the storage servers, and intentionally access the content generated at Layer 1.

The proposed method prevents these attacks by ensuring confidentiality, integrity, authentication and access control over data.

1) CONFIDENTIALITY

An adversary that has access to the content in the repository without a valid set of attributes and the corresponding decryption key cannot learn anything from the ciphertext. The repository stores and processes ABE encrypted content. The decryption key cannot learn anything from the ciphertext.

The decryption key cannot be retrieved from unauthorized users.

服务器 is honest and securely implemented, CP-ABE construction is assumed to be secure in Layer 2 based on a set of attributes retrieved from the trusted authority, which also creates and securely delivers the symmetric key \( SK_u \) associated with an authorized set of attributes will be able to recover the encryption key \( k \) and then to decrypt the content.

The base station constructs the encryption access policy in Layer 2 based on a set of attributes retrieved from the trusted authority, which also creates and securely delivers the encryption keys \( SK \) to authorized end-users. Thus, if the trusted server is honest and securely implemented, CP-ABE ensures that only entities with valid attributes satisfying the access policy used during encryption in Layer 2 will be able to decrypt and gain access to the content in plain form.

V. WBAN PROTOTYPE FOR E-HEALTH APPLICATIONS

In the deployment of the WBAN prototype and security scheme in each layer, we consider the implementation of cryptographic algorithms for security levels recommended in international standards [41]. The secure WBAN prototype...
FIGURE 5. WBAN deployment based on the 3-layer model.

consists of sensors and microprocessors embedded in programmable cards that are used to measure a person’s vital signs. A smartphone with an Android operating system was used as the BS, and a desktop computer was used as a server to host the system to store data and provide access to that data for authorized entities. In Table 4, we show the sensor devices used in the implemented secure WBAN prototype.

As described in Section 4, the proposed secure WBAN is based on a three-layer model: data collection, communication, and application. The WBAN prototype for e-health applications is shown in Figure 5 and described below.

- **Data acquisition.** Each layer of the WBAN has a data source. In Layer 1, three different devices are used as sensor nodes: a Galaxy Watch measures the person’s heart rate, a Raspberry Pi 3 senses the person’s blood oxygen saturation, and a TI LaunchPad CC3220SF measures the person’s body temperature. In Layer 2, upon receiving the data sent from the sensor nodes, the BS becomes the data source. Finally, in Layer 3, the repository where the data and encrypted symmetric key are stored is the data source.

- **Security services.** As in data acquisition, in each layer of the WBAN, we provide all data security services. In Layer 1, we guarantee the CIA triad by implementing lightweight cryptography algorithms: data encryption, hashing functions, and MACs. We use different symmetric keys for each sensor node. In Layer 2, we guarantee access control by implementing digital envelopes through DET-ABE [58], a scheme that encrypts the symmetric key of the sensor node with an access control policy. By controlling access to this key, access control is implemented for the data. Authentication is also provided at this layer using MACs, which are verified and generated with the data received in Layer 2. In Layer 3, a user with the proper attributes can access the data by decrypting the symmetric key and then decrypting the vital sign data collected from the sensor nodes.

- **Communication.** The devices used in the WBAN prototype for e-health applications have Wi-Fi or Bluetooth communication technologies. In Layer 1, the communication between the sensor nodes and BS occurs via Bluetooth. In Layers 2 and 3, communication between the BS and the system occurs via Wi-Fi over the Internet via a RESTFUL web service.

To understand the data flow in the WBAN prototype for e-health applications, the process of sending a data packet on the secure WBAN from a sensor node to the system is discussed in detail, using the Galaxy Watch node as an example.

1) The value obtained from the heart rate sensor node is a 16-bit number. Because cryptographic algorithms process blocks of data, these reads are stored in a buffer until completing a valid block for the cipher (e.g., 128 bits).

2) The data block is passed to the encryption process. Using the shared symmetric key, the process of encrypting the data block is performed, resulting in an encrypted data block of the same size (128 bits). The security level used in cryptographic algorithms is 128 bits.

3) The encrypted data block is sent to the algorithms for authentication. This cryptographic algorithm also uses a symmetric key to perform the processing. The result of this algorithm is a 128-bit authentication block.

4) The ID that is assigned to each sensor is a simple unique 8-bit integer.
TABLE 4. Components of the developed WBAN prototype platform.

| Device          | Description                        | Security services | Security level (bits) | Programming language | Communication technology |
|-----------------|------------------------------------|-------------------|-----------------------|-----------------------|--------------------------|
| Galaxy Watch    | Heart rate sensor                  | C, I, A           | 128, 192 and 256      | JavaScript            | Bluetooth                |
| TI LaunchPad CC3220SF | Body temperature sensor           | C, I, A           | 128                   | C/C++                 | Bluetooth                |
| Raspberry Pi 3  | Blood oxygen sensor saturation     | C, I, A           | 128, 192 and 256      | Python                | Bluetooth                |
| Galaxy A6+      | Base station                       | C, I, A, AC       | 128, 192 and 256      | Java                  | Bluetooth and Wi-Fi      |
| HP Pavilion     | Healthcare server                  | C, I, A, AC       | 128, 192 and 256      | Java                  | Wi-Fi or Ethernet        |

5) The data blocks are sent via Bluetooth from the sensor node to the BS.

6) At this point, the BS has already obtained the access control policy with which the symmetric key will be encrypted. The BS receives the data block, looks for the symmetric key assigned to the sensor node ID, and verifies that the data are authentic.

7) After validating the received data, BS uses the DET-ABE algorithm to encrypt the symmetric key assigned to the sensor node ID using the previously obtained access control policy.

8) A data block that includes the encrypted heart rate data, the MAC for that data, the encrypted symmetric key, and the sensor node ID is created. This data block is sent to the system via a RESTFUL web service hosted on the same system.

9) The system validates that the data received are authentic via the MAC and the verification process.

10) After verification, the encrypted heart rhythm and the encrypted symmetric key are extracted from the data block to store them in a specific data repository.

A. EVALUATION STAGES

The metrics of interest are execution time, memory and energy consumption. We used these metrics to primarily evaluate data security operations in Layer 1, where the devices have reduced computational resources compared to general purpose desktop computers. Note that these metrics are commonly used in the related literature, but not all are typically considered concurrently. Experiments are performed for evaluation and comparison purposes.

1) Execution time. The time elapsed from the beginning of a cryptographic operation (encryption, hashing, MAC gen/ver, ABE enc/dec/keygen) until its end.

2) Memory consumption. The amount of memory consumed by all security services related to the operations as summarized in Table 3.

3) Energy consumption. The energy consumed by calculating the theoretical ampere-hours [59]. The electrical consumption (EC) of a sensor device $i$ is given by the expression:

$$EC_i = \frac{CB_i}{DB_i}$$

where $CB_i$ and $DB_i$ are the electrical charge battery, in (mA), and DB is the discharge time (in h), respectively, of sensor $i$. With the previous metrics, we evaluate the performance and impact of the lightweight cryptographic algorithms in the proposed secure WBAN model. We defined three evaluation stages (ES) for the experimental evaluation. We use the notations ES1, ES2, and ES3 to refer to the evaluation stage occurring in Layers 1, 2, and 3, respectively. Next is the description of each use case that guides the experimental evaluation. For better presentation, we describe the experiments involving each of the layers in the proposed security model.

- **ES1. Sending data from sensor nodes to BS.** The goal of this experiment is to measure the impact of lightweight cryptographic algorithms on each sensor node and compare the performance of the algorithms on each security service. Therefore, the process is performed independently on each sensor. Table 5 summarizes the details of ES1.

- **ES2. Sending data from BS to the system.** The goal of this experiment is to measure the impact of lightweight cryptographic algorithms on the BS within the secure WBAN when transmitting the encrypted and authenticated data to the repository. In this experiment, the BS executes ABE, and ENC ensures access control over data by encrypting the $k_i$ key. The BS also uses policies

| Sensor nodes   | Security services | Security levels (bits) | Metrics of interest          |
|----------------|-------------------|------------------------|------------------------------|
| Galaxy Watch   | C, I, A           | 128, 192, 256         | Execution time, memory and energy consumption |
| Raspberry Pi 3 | C, I, A           | 128, 192, 256         | Execution time and memory consumption |
| TI LaunchPad CC3220SF | C, I, A | 128 | Execution time, memory and energy consumption |
TABLE 6. Details of ES2 experiment.

| Device            | Security de services | Security levels (bits) | Metrics of interest            |
|-------------------|----------------------|------------------------|--------------------------------|
| Samsung Galaxy A6+ | C, I, A, AC          | 128, 192, 256          | Execution time and memory consumption |
| HP Pavilion       | AC, A                | 128, 192, 256          | Execution time                  |

of different sizes (4, 8 and 16 attributes). We summarize the details of this experiment in Table 6.

- **ES3. Access to data by authorized users.** The goal of this experiment is to validate the correct operation of the secure WBAN. This experiment tests the performance of security services on a different data flow, from data generated on sensors to the access of data in plaintext by authorized users. In this experiment, we used an HP Pavilion computer as a server where both the system and user keys were generated. The security levels were 128, 192 and 256 bits, measuring the execution time for key generation and for accessing the data.

VI. RESULTS

In this section, we present the results and analysis of the data obtained from the experimental evaluation based on the three experiments described in the previous section involving the security concerns at each layer in the proposed WBAN security model. The minimum security level used in each lightweight cryptographic algorithm is 128 bits.

A. ES1. SENDING DATA FROM SENSOR NODES TO BS

In ES1, we performed an experiment between two sets of lightweight cryptographic algorithms selected in Section IV-C. The first ciphersuite (Suite 1) includes the LEA, SPONGENT and HMAC algorithms. The second ciphersuite (Suite 2) is confirmed by PRESENT, QUARK for integrity and LightMAC for authentication. The experiment was run for the 128-bit security level because PRESENT only has 80- and 128-bit security levels.

Table 7 summarizes the results when executing both ciphersuites on the sensor nodes. Time results obtained from the temperature sensor were kept below one second in both ciphersuites. With the blood oxygen saturation sensor, the integrity security service was the most time consuming in this comparison. Suite 1 achieved the best performance.

The ciphersuite with better performance in ES1 was used to evaluate ES2 and ES3 in the WBAN prototype. The ES1 results are summarized in Table 8 for execution time, Table 9 for memory usage, and Table 10 for energy consumption.

Table 8 shows the ES1 results in terms of execution time from the sensors during the experimentation. All values are expressed in milliseconds. As shown in this table, the execution time of the CIA triad increases with the security level (in bits) for the three sensor nodes. Additionally, in all cases, the implementation of the CIA triad implies a significant increase in the execution time, as high as nearly 1500 times the execution time when no service is implemented for the 256-bit security level in the Galaxy Watch sensor node.

Table 9 summarizes ES1 memory consumption. For this metric, the impact of the CIA triad implementation is marginal regardless of the security level (in bits). Note that the TI Launchpad consumes the lowest amount of memory, which can be explained by considering how the different implementation platforms (JavaScript, Python and C/C++) manage memory usage.

Table 10 summarizes ES1 energy consumption. The Raspberry Pi sensor node incorporates an operating system that begins when executing a process. Because this issue affects energy consumption, the Raspberry Pi sensor node was excluded from this experiment. As in the execution time metric case, the energy consumption increases with the security level (in bits).

From the results of the ES1 use case, the performance of ensuring the three services at the same is not a simple sum of individual performance. Thus, in experimental settings, isolating the effect of a single component is not feasible, as several factors, such as programming language, compiled code and scenario features, are involved. However, based on
TABLE 10. Battery energy consumed in sensors during experimentation.

| Sensor nodes | Security level (bits) | Energy consumption (mA) |
|--------------|-----------------------|-------------------------|
|              | None                  | C                       | I              | A              | C, I, A       |
| Galaxy Watch | 128                   | 86.34                   | 69.41          | 54.66          | 60.64         |
|              | 192                   | 86.34                   | 69.41          | 48.66          | 83.91         |
|              | 256                   | 85.3                    | 40.57          | 115.44         |               |
| TI LaunchPad CX3020SF | 128 | 25.27 | 53.1 | 34.5 | 61.42 | 59.94 |

FIGURE 6. ABE’s runtime for encrypting the symmetric key used to encrypt the sensors’ data. Encryption is done for different numbers of attributes in the access policy.

FIGURE 7. Memory consumption during encryption of the symmetric key in the BS as the number of attributes in the access policy increases.

FIGURE 8. Access key generation time at different curve types and security levels.

FIGURE 9. Time of access to data by a user for ES3 and as the number of attributes in access policy increases.

In an Android device, the Java virtual machine (JVM) administers memory by allocating what is necessary to each process and freeing up memory when it is no longer used; this causes the behavior observed in Fig. 7. Therefore, the memory consumed by the BS in this scenario is dynamic. In addition to Java management, we can observe that the ABE algorithm demands a greater amount of memory compared to the implemented algorithms in sensors (see Table 9). The highest memory consumption in sensors is approximately 3 times lower than the lowest memory consumption in BS.

In an Android device, the Java virtual machine (JVM)

administers memory by allocating what is necessary to each process and freeing up memory when it is no longer used; this causes the behavior observed in Fig. 7. Therefore, the memory consumed by the BS in this scenario is dynamic. In addition to Java management, we can observe that the ABE algorithm demands a greater amount of memory compared to the implemented algorithms in sensors (see Table 9). The highest memory consumption in sensors is approximately 3 times lower than the lowest memory consumption in BS.

experiment, we used the DET-ABE algorithm, which uses digital envelopes for the secure transport of the symmetric key $k$ used in sensor encryption. That key is encrypted with an access control policy $P$ using CP-ABE. As shown in Fig. 6, the execution time increases with the security level, and the number of attributes in the access policy has a minimum impact on the execution time. Conversely, as shown in Fig. 7, memory usage increases with the number of attributes in the access policy.

In an Android device, the Java virtual machine (JVM)

administers memory by allocating what is necessary to each process and freeing up memory when it is no longer used; this causes the behavior observed in Fig. 7. Therefore, the memory consumed by the BS in this scenario is dynamic. In addition to Java management, we can observe that the ABE algorithm demands a greater amount of memory compared to the implemented algorithms in sensors (see Table 9). The highest memory consumption in sensors is approximately 3 times lower than the lowest memory consumption in BS.
C. ES3. ACCESS TO DATA BY AUTHORIZED ENTITIES

As part of the experimentation in this scenario, we measured the time it takes for the DET-ABE algorithm to generate keys with security levels of 128- and 192-bit when using symmetric pairings, and 128-, 192-, and 256-bit when using asymmetric pairings. These algorithm configurations apply 4, 8 and 16 attributes of a user in the access key. In this experiment, we named the symmetric pairings approach with the prefix $A$ and the asymmetric one with the prefix $F$, followed by the level of security that was measured. The letter refers to the elliptic curve type used for each case [60]. In Fig. 8, we show the behavior of both approaches when generating access keys with 4, 8 and 16 attributes. We observed that in general, both pairing approaches demand generating time as the security level and number of attributes increase. The symmetric approach also requires more time resources than the asymmetric approach. This is due to the nature of the cryptographic constructions of pairing, being more efficient the constructions in the symmetric setting for the higher embedding degree in the elliptic curves used.

The ES3 scenario is primarily affected by sensor data decryption. In Fig. 9, we show the time it takes a user to access the data at different security levels and with an access control policy with different numbers of attributes.

The proposed secure WBAN model performance in the ES3 scenario is primarily characterized by the time required by a user for sensor data decryption. This time is presented in Fig. 9, where we show the time it takes a user to access sensor data with different security levels and numbers of attributes in the access policy. In Fig. 9, the behavior is similar to that shown in Fig. 6, where the required time increases with the security level. However, the time it takes to decrypt the data is less than the time it takes to encrypt it. This result is corroborated by observing that the maximum time with a 256-bit security level in data decryption is half the lower time with a 128-bit security level in the data encryption. The behavior we observed in both Fig. 6 and Fig. 9 is as expected, considering that as the security level increases, algorithms employ more processing rounds, and thus the latency increases with the size of the operands. This fact translates into a higher running time. These results highlight the relevance of lightweight data encryption algorithms, which must be deployed in sensor nodes, where processing and energy resources are limited.

VII. CONCLUSION

In this study, we proposed a three-tier security model for WBAN systems suitable for e-health applications that relies on the use of lightweight cryptography to provide security services in the entire data cycle. As a proof of concept, a prototype was deployed based on the three-layer model to determine the performance of the proposed method in terms of execution time, memory and energy consumption. We first provided extensive experimental evaluations to determine the most appropriate cyphersuites to ensure specific security services in a real WBAN deployment. Conversely, we observed that the cost of crypto-algorithms in terms of computational resources is acceptable. Specifically, the penalty in performance due to the computational processing of cryptographic layers can be tolerated by end-users while still meeting the expected data rate of sensed data.

Also, the design of the proposed secure WBAN deployment offers some degrees of freedom to provide different security levels (128, 192, and 256 bits) as desired. This flexibility could help to adjust the security level depending on the requirements and the available computing resources in the WBAN. Similarly, the lightweight cryptography algorithms in the experimental setup can be updated to a new version or newer crypto-algorithms due to the modular design of the proposed solution. Last, a fair and complete comparison with other methods is difficult due to the heterogeneous implementations of existing methods in terms of offered security services, device types, and security level. In any case, the proposed security solution exhibits competitive performance in terms of execution time, memory and energy consumption.

REFERENCES

[1] A. Tewari and P. Verma, “Security and privacy in E-healthcare monitoring with WBAN: A critical review,” Int. J. Comput. Appl., vol. 136, no. 11, pp. 37–42, Feb. 2016.
[2] M. Roy, C. Chowdhury, and N. Aslam, “Security and privacy issues in wireless sensor and body area networks,” in Handbook of Computer Networks and Cyber Security: Principles and Paradigms. Cham, Switzerland: Springer, 2019, pp. 173–200.
[3] M. M. Dhanvijay and S. C. Patil, “Internet of Things: A survey on enabling technologies in healthcare and its applications,” Comput. Netw., vol. 153, pp. 113–131, Apr. 2019.
[4] H. D. Jude and V. E. Balas, Eds., “Security and privacy in remote healthcare: Issues, solutions, and standards,” in Telemedicine Technologies. London, U.K.: Academic, 2019, pp. 201–225.
[5] K. R. Siva and R. Venkateswari, “Security challenges and solutions for wireless body area networks,” in Computing, Communication and Signal Processing. Singapore: Springer, 2019, pp. 275–283.
[6] A. Shah and M. Engineer, “A survey of lightweight cryptographic algorithms for iot-based applications,” in Proc. ICCS, 2019, pp. 283–293.
[7] S. B. Sadkhan and A. O. Salman, “A survey on lightweight-cryptography algorithms for iot-based applications,” in Proc. Int. Conf. Advance Sustain. Eng. Appl. (ICASEA), Mar. 2018, pp. 105–108.
[8] J. Shen, Z. Gui, X. Chen, J. Zhang, and Y. Xiang, “Lightweight and certificateless multi-receiver secure data transmission protocol for wireless body area networks,” IEEE Trans. Dependable Secure Comput., vol. 21, no. 2, pp. 12606–12633, 2012.
[9] M. Ali, M.-R. Sadeghi, and X. Liu, “Lightweight fine-grained access control for wireless body area networks,” Sensors, vol. 20, no. 4, p. 1088, Feb. 2020.
[10] C. Meshram, C.-C. Lee, S. G. Meshram, R. J. Ramteke, and A. Meshram, “An efficient mobile-healthcare emergency framework,” J. Med. Syst., vol. 44, no. 3, pp. 1–14, Mar. 2020.
[11] P. K. Sahoo, “Efficient security mechanisms for mHealth applications using wireless body sensor networks,” Sensors, vol. 12, no. 9, pp. 12606–12633, 2012.
[12] A. M. Almuhaideb and K. S. Alqudaihi, “A lightweight three-factor authentication scheme for WHSN architecture,” Sensors, vol. 20, no. 23, p. 6860, Nov. 2020.
[13] M. Kumar and S. Chand, “A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network,” IEEE Syst. J., vol. 15, no. 2, pp. 2779–2786, Jun. 2021.
[14] S. .. M. U. H. Al Rasyid, and I. G. P. Astawa, “Implementation of energy efficiency based on time scheduling to improve network lifetime in wireless body area network (WBAN),” EMITTER Int. J. Eng. Technol., vol. 3, no. 2, pp. 28–42, Apr. 2016.
A secure broadcast access control system for wearable devices,” in Proc. IEEE Int. Conf. W Biomed. Technol. Security, 2020, pp. 1–5.

K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, “Report on lightweight cryptography,” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 8114, 2017.

F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, “Internet of Things security: A survey,” J. Netw. Comput. Appl., vol. 88, pp. 10–28, Jun. 2017.

M. Morales-Sandoval, J. L. Gonzalez-Compean, A. Diaz-Perez, and V. S. Sosa-Sosa, “A pairing-based cryptographic approach for data security in the cloud,” Int. J. Inf. Secur., vol. 17, no. 4, pp. 441–461, Aug. 2018.

P. Picazo-Sanchez, J. E. Tapiador, P. Peris-Lopez, and G. Suarez-Tangil, “Secure publish-subscribe protocols for heterogeneous medical wireless body area networks,” Sensors, vol. 14, no. 12, pp. 22619–22624, 2014.

T. Narmadh, M. Kalaiarasi, and M. Meenakshi, “Lightweight secure ECC transmission in wireless body area networks—PRESENT cipher based implementation,” in Proc. Int. Conf. Commun. Signal Process. (ICCSSP), Apr. 2017, pp. 1066–1070.

A. Z. Alshamsi and E. S. Barka, “Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks,” in Proc. Int. Conf. Inform. Technol. (ICHIT), Feb. 2017, pp. 1–7.

A. Arfaoui, O. R. M. Boudia, A. Kibiche, S.-M. Senouci, and M. Hamidi, “Context-aware access control and anonymous authentication in WBAN,” Comput. Secur., vol. 88, Jan. 2020, Art. no. 101406.

M. Polai, S. Mohanty, and S. S. Sahoo, “A lightweight mutual authentication protocol for wireless body area network,” in Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN), Mar. 2019, pp. 760–765.

B. Chandrasekaran, R. Balakrishnan, and Y. Nogami, “TP-CPABE: An efficient and secure data communication policy with updating in wireless body area networks,” Persian J., vol. 41, no. 4, pp. 465–472, 2019.

F. P. Diez, D. S. Touceda, J. M. S. Camara, and S. Zeadally, “Lightweight access control system for wearable devices,” IT Prof., vol. 21, no. 1, pp. 50–58, Jan. 2019.

A. Bander Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, “A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks,” Wireless Pers. Commun., vol. 117, pp. 47–69, Mar. 2020.

M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, “A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data,” IEEE Access, vol. 8, pp. 52018–52027, 2020.

T. Wan, L. Wang, W. Liao, and S. Yue, “A lightweight continuous authentication scheme for medical wireless body area networks,” Peer–Peer Netw. Appl., vol. 14, no. 6, pp. 3473–3487, Nov. 2021.
MIGUEL MORALES-SANDOVAL received the B.Sc. degree from the University of Puebla, in 2002, and the M.Sc. and Ph.D. degrees from the National Institute for Astrophysics, Optics, and Electronics, Mexico, in 2004 and 2008, respectively.

He is currently a Computer Science Researcher with special interest in information systems, data security, cryptography, and embedded systems. He is currently focused on the development of software engineering, encrypted data retrieval mechanisms, and security in the Internet of Things domain and in the Cloud. He actively participates in graduate programs in computer science and information technology and in the development of research projects. He has served as a reviewer for several journals and conferences and as an associate editor.

RICARDO DE-LA-PARRA-AGUIRRE received the B.S. degree, as a Computer Systems Engineer, from the Technological Institute of Tapachula, Chiapas, Mexico, and the M.Sc. degree in engineering and computer technologies from the Center for Research and Advanced Studies (Cinvestav), Mexico. His research interests include information security, applied cryptography, software engineering, and network security.

HIRAM GALEANA-ZAPIÉN (Member, IEEE) received the Electronics and Telecommunications Engineering degree from the Autonomous University of Nuevo Leon, Mexico, in 2001, and the Ph.D. degree in telecommunications engineering from the Technical University of Catalonia (UPC), Barcelona, in February 2011. Since June 2011, he has been a Researcher with Cinvestav Tamaulipas, Mexico. His research interests include resource allocation in 5G cellular networks, the Internet of Things, smartphone-based location sensing, and mHealth.

ALEJANDRO GALAVIZ-MOSQUEDA received the M.Sc. degree in computer science from the University of Colima, Mexico, in 2006, and the Ph.D. degree from the CICESE Research Center, Mexico, in 2013. He is currently a Researcher with CONACYT-CICESE, Unidad Monterrey, Mexico. His main research interests include mobile and wireless networks for intelligent transport systems and mHealth.