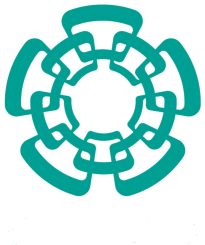

Centro de Investigación y de Estudios Avanzados del IPN

Unidad Tamaulipas

Seguridad en redes inalámbricas de área corporal mediante criptografía ligera

Tesis que presenta:

Ricardo Enrique de la Parra Aguirre

Para obtener el grado de:

Maestro en Ciencias en Ingeniería y Tecnologías Computacionales

Director de la Tesis:
Dr. Miguel Morales Sandoval

Cd. Victoria, Tamaulipas, México. Septiembre, 2020

"Este trabajo de investigación se realiza en el marco del proyecto 281565 del Fondo de Investigación para la Educación SEP-CONACYT, bajo la dirección del Dr. Miguel Morales Sandoval."

La tesis presentada por Ricardo Enrique de la Parra Aguirre fue aprobada por:

Dr. Hiram Galeana Zapién

Dr. Gabriel Alejandro Galaviz Mosqueda

Dr. Miguel Morales Sandoval, Director

Cd. Victoria, Tamaulipas, México., 14 de Septiembre de 2020

A mis padres Isael e Inés y a mi hermana Fernanda

Agradecimientos

- Antes de todo agradezco a Dios por darme vida, llenarme de bendiciones, darme fortaleza durante toda esta aventura y poner en este camino a todos los amigos que conocí durante mi estancia.
- Agradezco a mis padres y hermana por el apoyo incondicional durante esta experiencia a pesar de la distancia, por mantenerse al pendiente de mí y por darme motivación todos los días para seguir alcanzando mis metas.
- Agradezco a mi familia que ha estado pendiente de mí y me han dado su apoyo durante toda mi estancia realizando la maestría.
- Agradezco infinitamente a mis amigos y compañeros de la generación, Melissa, Shanel, Diana, Elías, Lalo, Armando, Moguel, Fernando, Yeyo, Tipa e Iván por hacer de esta estancia una experiencia agradable compartiendo festividades, trabajos y juegos. También por brindar su amistad durante toda la maestría y por el apoyo en los momentos difíciles de la misma.
- Un agradecimiento especial para Lalo y sus padres por el apoyo y atención brindado no sólo a mí, si no a los demás amigos foráneos y a Armando por estar pendiente de nosotros y apoyarnos en lo necesario. Ambos por apoyarnos cuando recién llegamos a la ciudad y aconsejarnos. De igual manera, agradezco especialmente a Elías, Moguel y Fernando por la confianza, amistad y apoyo durante el tiempo que compartimos casa.
- Un agradecimiento especial a mi asesor y director de tesis, Dr. Miguel Morales Sandoval, por la confianza y paciencia que me tuvo y por compartir sus conocimientos durante el desarrollo de la tesis, con una dirección excelente y acertada.
- Quiero agradecer a mis revisores, el Dr. Hiram Galeana Zapién y el Dr. Alejandro Galaviz Mosqueda, por su valiosa retroalimentación para mejorar mi documento de tesis y por sus disposición para atender las dudas.
- Agradezco a los profesores e investigadores del Cinvestav unidad Tamaulipas por el conocimiento impartido y por el apoyo brindado durante esta etapa de formación.
- También agradezco al personal administrativo, técnico y de limpieza de la unidad por todas las facilidades brindadas durante mi estancia.
- Finalmente, agradezco al CONACyT por la beca de manutención otorgada que me permitió concentrarme en los estudios a lo largo de la maestría.

Índice General

Índice de Figuras

Índice de Tablas

Índice de Algoritmos

Resumen

Seguridad en redes inalámbricas de área corporal mediante criptografía ligera

por

Ricardo Enrique de la Parra Aguirre
Unidad Tamaulipas
Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, 2020
Dr. Miguel Morales Sandoval, Director

El sector médico ha sido un área de oportunidad para el uso de tecnologías de información, las cuales coadyuvan a eficientizar sus procesos tradicionales. Uno de estos procesos es el cuidado de la salud de un paciente, la cual se realiza generalmente de manera presencial. Un enfoque, aprovechando la disponibilidad de las tecnologías de información y de comunicaciones, es monitorizar a los pacientes remotamente, esto es, recolectar los datos de los signos vitales de los pacientes y transferirlos hasta un repositorio, donde más adelante dichos datos serán accedidos y usados por aplicaciones o usuarios autorizados. Esto se logra con el uso de tecnologías como las redes inalámbricas de área corporal (WBAN). Sin embargo, los datos de signos vitales de pacientes son sensibles y es recomendable que dichos datos se protejan y mantengan privados durante su recolección, transporte, almacenamiento y uso. En este proyecto de investigación se plantea el desarrollo de un prototipo de WBAN segura que permita cuantificar el impacto en el sobrecosto de los recursos computacionales de los sensores al usar algoritmos criptográficos ligeros para garantizar servicios de confidencialidad, integridad, autenticación y control de acceso sobre los datos recabados por los sensores, transmitidos por la red WBAN, almacenados en un repositorio y accedidos por usuarios autorizados. Al determinar casos de usos representativos en el entorno de WBAN para evaluar el prototipo y el impacto de los algoritmos de criptografía se obtuvo como resultado que la confidencialidad es el servicio de seguridad con mejor desempeño de todos los servicios de seguridad requeridos en una WBAN y el costo es asumible debido a que la tasa en la transmisión de datos está por arriba de lo reportado en la literatura para el sensor de ritmo cardíaco.

Abstract

Security in Wireless Body Area Networks through lightweight cryptography

by

Ricardo Enrique de la Parra Aguirre
Cinvestav Tamaulipas
Research Center for Advanced Study from the National Polytechnic Institute, 2020
Dr. Miguel Morales Sandoval, Advisor

The medical sector has been an area of opportunity for the inclusion of information technologies that allow the efficient implementation of the underlying processes. One of these processes is the supervision and monitoring of vital signs of a patient, generally done by a specialist and person. One alternative approach, taking advantage of the impact of the IoT, is to monitor patients remotely, that is, to collect the patient's vital signs and transfer those data to a server. This can be achieved by using technologies such as wireless body area networks (WBAN). However, a very important issue that encompasses this whole process is data security; since the biomedical data being collected is highly sensitive. That data must be kept private and protected. This research proposes the development of a secure WBAN prototype by means of lightweight cryptography. Such a prototype allows measuring and evaluating the impact of lightweight cryptographic algorithms on other prototype's components to guarantee the confidentiality, integrity, authentication and access control security services. Under representative use cases in the WBAN environment to evaluate the prototype and the impact of the cryptography algorithms, resulted that confidentiality was the security service with the best performance of all the other security services required in a WBAN, and the cost is affordable because the data transmission rate is higher than the one reported in the literature for the heart rate sensor.

1

Introducción

En este capítulo se presenta una descripción de esta tesis detallando aspectos como antecedentes, motivación, planteamiento del problema, hipótesis, objetivos general y particulares, metodología y la organización del documento.

1.1 Antecedentes y motivación

La tecnología ha tenido un gran impacto en la sociedad a tal grado que ya es parte de la cotidianidad de las personas, favoreciendo la comodidad y practicidad en el ámbito laboral y personal de las personas.

Con esa visión nace el paradigma del Internet de las Cosas (IoT, por sus siglas en inglés). El IoT provee una integración de varios sensores, objetos o "cosas" que pueden comunicarse directamente unos a otros, mediante una red, sin la necesidad de la intervención humana. El término fue introducido por Kevin Ashton en 1999. Años después, en 2009, Ashton escribió el artículo *"That 'Internet of Things' Thing"*, donde explica el panorama del IoT [9].

El objetivo principal del IoT es proveer una infraestructura de red con protocolos de comunicación interoperables y software que permita la conexión e incorporación de sensores físicos/virtuales, computadoras, dispositivos inteligentes, automóviles, y objetos como refrigeradores, lavadoras, horno de microondas, comida y medicinas en cualquier momento en cualquier red [4].

Se ha encontrado en el IoT un área de oportunidad dentro del sector médico; que permita el despliegue de plataformas para el monitoreo de pacientes, recolección de datos y comunicación entre los pacientes y los diferentes usuarios en el entorno médico. Uno de los campos recientes y relevantes son las redes inalámbricas de área corporal (WBANs, por sus siglas en inglés) [2] donde se combinan diversos elementos del IoT para que a través de una red de sensores inalámbricos se realice el monitoreo de los signos vitales de los pacientes de manera que se puedan detectar posibles anomalías en los valores esperados y actuar en consecuencia de manera oportuna.

Rango	Total	Hombres	Mujeres
1	Enfermedades del corazón (149,368)	Enfermedades del corazón (79,997)	Enfermedades del corazón (69,357)
2	Diabetes mellitus (101,257)	Diabetes mellitus (49,679)	Diabetes mellitus (51,576)
3	Tumores malignos (85,754)	Tumores malignos (41,590)	Tumores malignos (44,416)
4	Enfermedades del hígado (39,287)	Homicidios (32,765)	Enfermedades cerebrovasculares (17,841)
5	Homicidios (36,685)	Enfermedades del hígado (28,750)	Influenza y neumonía (12,826)
6	Enfermedades cerebrovasculares (35,300)	Accidentes (26,540)	Enfermedades pulmonares obstructivas crónicas (11,220)
7	Accidentes (34,589)	Enfermedades cerebrovasculares (17,459)	Enfermedades del hígado (10,533)
8	Influenza y neumonía (28,332)	Influenza y neumonía (15,504)	Accidentes (8,030)
9	Enfermedades pulmonares obstructivas crónicas (23,414)	Enfermedades pulmonares obstructivas crónicas (12,193)	Insuficiencia renal (6,018)
10	Insuficiencia renal (13,845)	Insuficiencia renal (7,825)	Ciertas afecciones originadas en el periodo perinatal (5,230)

Enfermedades del corazón · Diabetes Mellitus · Tumor maligno · Otras enfermedades no transmisibles · Accidentes · Agresiones · Enfermedades transmisibles

Figura 1.1: Principales causas de muerte en México durante 2018.

En México durante 2018, el 88.4 % (638,862) de las defunciones se debieron a enfermedades y

problemas relacionados con la salud. En la Figura 1.1 se muestran las 10 principales causas de muerte en México durante 2018. La principal causa de muerte en México son enfermedades del corazón. Dado que una WBAN monitorea signos vitales, los referentes al corazón son una opción viable debido al índice de mortalidad según lo reportado por el INEGI en México.

Los signos vitales que más se recomienda monitorear de un usuario [18], están los referentes al corazón como el ritmo cardíaco, la saturación de oxígeno en la sangre y la presión arterial. El Instituto Nacional de Cardiología realiza cada año un censo de las causas de morbilidad en México[1]. En el periodo de enero a diciembre del 2018 se registraron las siguientes causas principales:

- Enfermedades isquémicas del corazón (32.15 %).
- Anomalías congénitas del sistema circulatorio (21.54 %).
- Enfermedades de arterias, venas y vasos capilares (5.79 %).
- Enfermedades hipertensivas (4.18 %).

La incorporación y uso de tecnología WBAN en e-salud puede tener un impacto significativo en el seguimiento y tratamiento de enfermedades, como las descritas en la Figura 1.1. La e-salud se define como el uso rentable y seguro de las Tecnologías de Información y Comunicación (TICs) modernas en apoyos de los campos relacionados con la salud para la satisfacer las necesidades de los usuarios [22]. El entorno de WBANs es un área en desarrollo con distintos retos, particularmente los que se refieren a la seguridad de información [67]:

- **Seguridad de datos:** Los datos que se transmiten en una WBAN son sumamente sensibles y cruciales, dado que contienen los signos vitales de los pacientes. Todos los datos recolectados juega un rol importante en el proceso del cuidado de la salud, debido a que los procesos posteriores hacen uso de ellos.

[0] https://www.inegi.org.mx/app/saladeprensa/noticia.html?id=5277

[1] `https://www.cardiologia.org.mx/transparencia/transparencia_focalizada/estadisticas/`

- **Gestión de datos:** Los sensores de las WBANs pueden generar una enorme cantidad de datos, lo que implica que deben existir mecanismos de gestión eficientes para distribuir y almacenar dichos datos.

- **Consistencia de datos:** En toda la WBAN se involucran diferentes usuarios como médicos, pacientes, etc., desde diferentes ubicaciones y todos ellos utilizan los datos recolectados. La consistencia de datos se refleja al proporcionar solamente los datos que cada usuario necesita para realizar sus actividades.

- **Validación de sensor:** Para asegurarse de la autenticación de cada nodo sensor, es necesario validar su identidad en cada proceso que se realice. Esto evita los ataques de suplantación de identidad y la manipulación de nodos. Esto también implica enfrentar otros retos como los recursos limitados y la eficiencia energética.

- **Consumo de energía:** Los nodos sensores que se utilizan en una WBAN son pequeños, lo que limita sus recursos. En este contexto, las aplicaciones y procesos que se ejecutan deberían ser "ligeros", es decir, de bajo consumo tanto en recursos computacionales como en energía.

- **Seguridad:** Se debe garantizar un nivel de seguridad aceptable, al menos de 128 bits [21, 43]. Sin embargo, los algoritmos criptográficos convencionales que pueden hacerlo son costosos computacionalmente y difícilmente se pueden implementar de manera directa en nodos sensores.

Por la sensibilidad de los datos médicos que se manejan y que pueden afectar directamente al usuario en la toma de decisión respecto a su condición, una solución WBAN debe considerar desde su diseño el aspecto de la seguridad de los datos, en las diferentes capas de comunicación y procesamiento, esto es, incorporar mecanismos que garanticen los servicios de ***confidencialidad***, ***integridad***, ***autenticación*** y ***control de acceso***.

Las principales amenazas en una red, que también compete a las WBANs, se presentan en la

Tabla 1.1, mostrando las capas del modelo OSI donde ocurren las posibles amenazas y algunos mecanismos de defensa [68].

Tabla 1.1: Posibles amenazas en una red.

Capa del modelo OSI	Ataque	Mecanismos de defensa
Física	Interferencia	Espectro expandido, mensaje de prioridad
	Manipulación	Ocultamiento
Enlace	Colisión	Código de corrección de errores
	Manipulación	Ocultamiento
	Agotamiento	Limitación de velocidad
Red	Negligencia	Redundancia, sondeo
	Falsificación	**Autenticación de datos**
	Homing	**Cifrado de datos**
	Desvío	Filtrado de egreso, monitoreo de autorizaciones
	Black holes	Autorización, seguimiento, redundancia
Transporte	Desincronozación	**Autenticación de datos**

En la Tabla 1.1 se puede observar que existen diferentes mecanismos de seguridad para prevenir ataques en redes de comunicación, como las WBANs, lo cual resulta ser una importante herramienta para proteger los datos cuando son sensibles como los signos vitales. Entre esos mecanismos de defensa resalta el cifrado y autenticación de datos; éstos garantizan servicios de confidencialidad, integridad y autenticación sobre los datos que se generan desde los sensores hasta el acceso por usuarios autorizados como médicos, enfermeras, especialistas, etc. Particularmente, estos servicios se pueden proveer mediante algoritmos criptográficos.

En marzo de 2017, el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) publicó un reporte [45] donde compara los algoritmos que han sido diseñados como ligeros y los algoritmos con enfoque general, dividiéndolos según sus construcciones. En ese reporte se aborda los algoritmos para cifrado de datos, funciones hash y código de autenticación de mensaje. Actualmente, el NIST mantiene un proceso de estandarización para determinar un algoritmo estándar en criptografía ligera para cada uno de los rubros. Este proceso comenzó en febrero de 2019 y en

octubre del mismo año, se publicó un reporte [71] donde se resume lo ocurrido durante la primer ronda del concurso. Actualmente se encuentran 32 candidatos en la segunda ronda y el proceso de estandarización está en pausa.

1.2 Planteamiento del problema

Actualmente, existe poco uso de tecnologías IoT para el monitoreo de signos vitales de pacientes en hospitales, tales como ritmo cardiaco, saturación de oxígeno en la sangre, temperatura corporal, entre otros, con un enfoque de WBAN. Sin embargo, la recopilación y monitoreo de estos signos pueden ayudar significativamente en las tareas de prevención de problemas de salud en la población. Tecnologías IoT como las WBANs son una herramienta eficiente para las tareas de monitoreo de signos vitales.

Aunque la tecnología de WBAN es relativamente incipiente, existe un área de oportunidad en México para la asimilación de esta tecnología y su despliegue en escenarios reales, que coadyuven a combatir los altos niveles de morbilidad en el país, como se ha señalado en la Sección 1.1.

Dado que los datos biomédicos de signos vitales tratados en WBANs son sensibles, es esencial contar con mecanismos de seguridad eficientes, que sean conscientes de las limitaciones en el poder de cómputo de los nodos sensores de una WBAN. Para garantizar los mecanismos de seguridad [20] como confidencialidad, integridad, autenticación y control de acceso, que son requeridos, sobre la información que se genera, almacena, transmite o procesa [42] en los nodos de una WBAN, es necesario implementar algoritmos criptográficos ligeros [62] de forma eficiente y segura.

La inclusión de algoritmos de criptografía incrementa la fiabilidad del sistema en una WBAN al proveer servicios de seguridad requeridos, pero esto tiene un alto costo en los recursos computacionales disponibles en una WBAN. Proveer los servicios de seguridad mediante la implementación de algoritmos criptográficos convencionales, que generalmente se han usado en

[1] `https://csrc.nist.gov/projects/lightweight-cryptography`

sistemas y redes de computadoras y que no tienen restricciones de recursos de cómputo como las WBAN, puede agotar los recursos de energía rápidamente y por otro lado, el incremento en la carga computacional de un nodo en una WBAN por operaciones asociadas a la seguridad afecta la latencia.

Bajo este contexto, existe una línea de investigación de criptografía ligera, la cual estudia los algoritmos criptográficos más adecuados para entornos donde existe limitaciones computacionales, como en WBANs. Con los algoritmos conscientes de los recursos computacionales disponibles, se pueden garantizar los servicios de seguridad requeridos [68] para una WBAN, y tratándose de un modelo de capas, los servicios de seguridad se pueden ajustar a cada una de las capas según las necesidades de la misma WBAN.

Proveer servicios de seguridad en WBANs mediante algoritmos criptográficos de forma eficiente es un problema actualmente abordado en la comunidad [32, 58, 63], los principales retos [8, 57] son debido a los siguientes factores:

1. Existen diversos tipos de algoritmos criptográficos, algunos más adecuados para contextos con recursos de cómputo limitados. Actualmente se realiza un proceso de estandarización de criptografía ligera[2] a cargo del NIST, y existe un área de oportunidad para evaluar algoritmos de criptografía ligera que mejor se adapten a las necesidades de la aplicación, como el caso de las WBAN.

2. Los algoritmos criptográficos son costosos computacionalmente. Por otro, los nodos sensores tienen pocas capacidades de cómputo (memoria, poder de procesamiento y energía), lo que implica que los algoritmos criptográfico implementados en los sensores sean ligeros y conscientes de las limitaciones. El sobrecosto por requerimientos de seguridad de datos debe ser el menor posible, por lo que el diseño e implementación de esquemas criptográficos debe realizarse cuidadosamente.

3. Aunque en la literatura existen propuestas algorítmicas para proveer algunos servicios de

[2] https://csrc.nist.gov/Projects/lightweight-cryptography

seguridad en WBANs las soluciones existentes, generalmente, solo se enfocan en un servicio de seguridad (confidencialidad, integridad, autenticación, control de acceso, etc.), lo cual no es suficiente para mitigar los riesgos en un contexto práctico.

4. En la mayoría de los trabajos relacionados, generalmente, no se reporta la validación ni evaluación de los algoritmos criptográficos utilizados en escenarios reales para determinar su viabilidad.

El problema abordado en esta tesis es el diseño de una WBAN segura basado en el modelo de 3 capas, garantizando servicios de seguridad en cada una de las capas mediante la implementación de algoritmos de criptografía ligera y un estudio de factibilidad para evaluar el desempeño de la WBAN segura con los algoritmos criptográficos ligeros en casos de uso relacionados con la WBAN.

1.3 Preguntas de investigación

Debido a los factores mencionados en la sección 1.2, en esta tesis se aborda el problema de provisión de servicios de seguridad en WBAN de extremo a extremo, esto es, garantizar la seguridad de datos en una WBAN desde su generación en los sensores y hasta su uso por las entidades autorizadas. De esta forma se puede garantizar la seguridad a lo largo del ciclo de vida de los datos recabados en una WBAN. Un aspecto relevante es la evaluación del impacto de los servicios de seguridad requeridos por una WBAN a través de un prototipo, que permite determinar la idoneidad de usar algoritmos criptográficos ligeros específicos. En esta tesis se abordan las siguiente preguntas de investigación:

1. *¿Cuáles son los algoritmos de criptografía ligera más recomendables para garantizar servicios de confidencialidad, integridad, autenticación y control de acceso bajo el modelo de operación de una WBANs?*

2. *¿Qué costo computacional e impacto asociado tienen los algoritmos de criptografía ligera cuando se evalúan en un prototipo de WBAN en las métricas de mayor interés?*

Para responder a las preguntas anteriores, en esta tesis se realizó el estudio, diseño, implementación y evaluación de mecanismos criptográficos ligeros como parte del proceso de diseño de un prototipo de WBAN segura, que pueda ser viable de implementarse en aplicaciones de e-salud en el contexto de IoT.

1.4 Hipótesis

Un prototipo WBAN para monitoreo de signos vitales en aplicaciones de e-salud permite estudiar algoritmos de criptografía ligera y evaluar su viabilidad para proveer servicios de seguridad sobre los datos que se adquieren, transmiten, almacenan y acceder bajo el modelo de referencia WBAN de tres capas. La viabilidad de los algoritmos está determinada por su impacto, medido por el tiempo de servicio, memoria y energía consumida, para los casos de uso más representativos de operación de una WBAN.

1.5 Objetivo general

Crear un prototipo de WBAN segura que permita el estudio y evaluación del impacto del uso de algoritmos de criptografía ligera para la provisión de servicios de seguridad en casos de uso representativos de una WBAN.

1.6 Objetivos particulares

1. Determinar el modelo de una WBAN segura que permita garantizar los servicios de confidencialidad, integridad, autenticación y control de acceso en los casos de uso más

representativos de una WBAN.

2. Diseñar y desarrollar un prototipo de WBAN que permita monitorear al menos tres signos vitales y realizar el despliegue del modelo de WBAN segura mediante algoritmos de criptografía ligera.

3. Cuantificar el impacto de la provisión de servicios de seguridad mediante algoritmos de criptografía ligera de acuerdo a casos de uso representativos de WBAN.

1.7 Metodología

Este proyecto de investigación se desarrolló con una metodología dividida en tres etapas, las cuales se describen a continuación:

- **Etapa 1. Estado del arte.** Esta etapa se divide en actividades que se realizaron para cumplir el primer objetivo particular.

  1.1. Revisar el estado del arte para identificar los servicios de seguridad requeridos en WBANs, de acuerdo con un modelo de 3 capas.

  1.2. Para los servicios de seguridad seleccionados, revisar la literatura para determinar los algoritmos criptográficos más adecuados para el contexto WBAN. La idoneidad de un algoritmo estará en función de su complejidad computacional, sus requerimientos de área, su desempeño, entre otros. La revisión se enfocará en criptografía ligera.

  1.3. Estudiar los algoritmos del estado de arte del punto 1.2, identificando sus características como latencia, complejidad, ventajas/desventajas desde el punto de vista de implementación en WBANs. Complementar el estudio mediante su implementación en software usando APIs disponibles.

  1.4. Determinar el modelo de WBAN segura, incluyendo los servicios de seguridad que deben garantizarse en cada una de las capas del modelo.

El modelo de WBAN segura propuesto en esta etapa es la primera aportación de esta tesis.

- **Etapa 2. Diseño e implementación del prototipo WBAN.** En esta etapa se realizan una serie de actividades para cumplir el segundo objetivo particular.

  2.1. Revisar la literatura sobre prototipo existentes de WBAN, alcances y limitaciones.

  2.2. Con base en el modelo WBAN de la Etapa 1 y con el análisis de trabajos relacionados sobre prototipos WBAN, proponer un prototipo de WBAN y formalizar su definición.

  2.3. Revisión de dispositivos y tecnologías más adecuadas para el despliegue del prototipo WBAN definido.

  2.4. Implementación del prototipo de WBAN segura, incluye: implementación de algoritmos criptográficos ligeros, integración de componentes, despliegue del modelo de WBAN segura de 3 capas.

La construcción del prototipo de WBAN segura es la segunda aportación de esta tesis.

- **Etapa 3. Evaluación y resultados.** En esta etapa se cumplió el tercer objetivo particular, mediante las siguientes actividades:

  3.1. Definir métricas de interés recabadas en cada experimento realizado para la evaluación del prototipo de WBAN segura.

  3.2. Evaluar el impacto del CU1: envío de datos desde cada nodo sensor hasta la estación base en el prototipo de WBAN segura, cuando se garantizan los servicios de seguridad requeridos y cuando se prescinde de ellos.

  3.3. Evaluar el impacto del CU2: envío de datos desde la estación base hasta el servidor en el prototipo de WBAN segura, cuando se garantizan servicios de seguridad requeridos y cuando se prescinde de ellos.

3.4. Evaluar el impacto del CU3: generación de llaves acceso de usuarios en el prototipo de WBAN segura.

3.5. Documentación y publicación de resultados.

La evaluación de los algoritmos criptográficos ligeros en cada uno de los experimentos y resultados obtenidos es la tercera aportación de esta tesis.

1.8 Organización del trabajo de tesis

El resto de la tesis se divide en 5 capítulos. El Capítulo 2 presenta el marco teórico que proporciona definiciones de los conceptos utilizados a lo largo del desarrollo de la tesis. En el Capítulo 3 se describen y discuten los trabajos relacionados con el tema de investigación y se realiza una comparación entre ellos y con la propuesta de esta investigación. En el Capítulo 4 se propone un esquema de seguridad para una WBAN y se detalla el diseño de una WBAN segura, abarcando las tres capas que la conforman: recolección de datos, comunicación y aplicación. En el Capítulo 5 se definen las métricas de interés y los experimentos en tres casos de uso, después se detallan los resultados obtenidos en la experimentación realizada. Finalmente, en el Capítulo 6 se presentan las conclusiones obtenidas del trabajo realizado, además, se describen las áreas de oportunidad de esta tesis para una trabajo futuro.

2

Marco teórico

En este capítulo se presentan los fundamentos, conceptos y elementos necesarios para comprender el desarrollo de la tesis, lo que le permite al lector familiarizarse y tener una mejor perspectiva del trabajo de investigación de esta tesis.

2.1 Internet de las Cosas y Redes de Área Corporal

El IoT supone una conectividad a través de Internet entre objetos inteligentes. El IoT esta identificada como la siguiente era en las TICs donde la computación ocurre en cualquier momento, lugar, y se realiza prácticamente por cualquier çosa inteligente"[61], con capacidades de sensado, comunicación y cómputo que la hacen autosuficientes para realizar procesos por sí mismas.

Salud, domótica y el sector militar, industrial y agropecuario son áreas de oportunidad relevantes para IoT, donde se requieren actividades de monitoreo continuo y controlado. El inconveniente para estas áreas de aplicación del IoT es la seguridad de los datos que se generan, almacenan, procesan o transmiten [42]. Por consiguiente, se necesita garantizar que los datos, así como el acceso a los

dispositivos del IoT que los producen deben ser seguros y brindar total integridad de los datos. Diferentes factores hacen que un sistema sea vulnerable, hablando de IoT, desde la arquitectura con la que se desarrolla hasta la forma en la que se utiliza. Las principales amenazas a las que se enfrenta el IoT [4], tanto a nivel hardware, software y aplicación son: *manipulación de la información*, *espionaje* y *falsificación*.

2.1.1 Redes de sensores

El término sensor se refiere a un elemento de medición que detecta la magnitud de un parámetro físico y lo cambia por una señal que puede procesar el sistema. Al elemento activo de un sensor se le conoce comúnmente como transductor. El diseño de sensores y transductores siempre involucra alguna ley o principio físico o químico que relaciona la cantidad de interés con algún evento medible.

El estándar IEEE 1451 [36] define un conjunto de interfaces de comunicación para conectar transductores inteligentes a sistemas basados en microprocesadores, instrumentos y redes; y proporciona un conjunto de protocolos para sistemas tanto cableados como inalámbricos.

Los sensores que son de interés para esta tesis son los mencionados en el estándar IEEE 1451.5 [69], sensores con comunicación inalámbrica, dado que la red en la que actuarán es inalámbrica.

2.1.2 Redes inalámbricas de sensores

Una red inalámbrica de sensores (WSN, por sus siglas en inglés) se basa en dispositivos de bajo consumo (nodos) que son capaces de obtener información de su entorno, procesarla localmente, y comunicarla a través de enlaces inalámbricos hasta un nodo central de coordinación, normalmente llamado estación base. Los nodos actúan como elementos de la infraestructura de comunicaciones al reenviar los mensajes transmitidos por nodos más lejanos hacia al centro de coordinación. Los sensores son alimentados por baterías. La estructura de una WSN se puede observar en la Figura 2.1. Debido a las limitaciones del tiempo de vida de la batería, los nodos se construyen teniendo

presente la conservación de la energía, y generalmente pasan mucho tiempo en modo *sleep* de bajo consumo. Éstos pueden ser fijos o móviles [14].

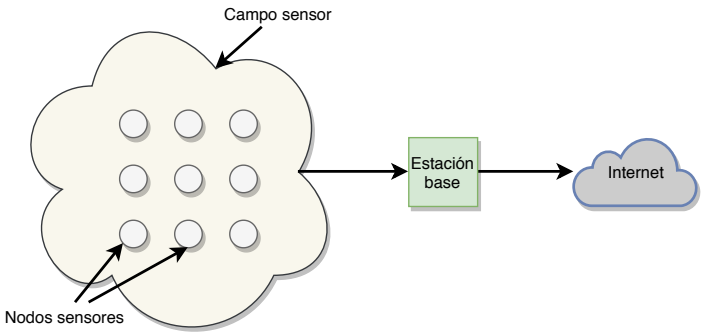

Figura 2.1: Estructura general de una WSN.

Una WSN tienen capacidad de auto-restauración, es decir, si se avería un nodo, la red encontrará nuevas vías para encaminar los paquetes de datos. De esta forma, la red sobrevivirá en su conjunto, aunque haya nodos individuales que pierdan potencia o se destruyan. Las capacidades de auto-diagnóstico, auto-configuración, auto-organización, auto-restauración y reparación, son propiedades que se han desarrollado para este tipo de redes para solventar problemas que no eran posibles con otras tecnologías. Las redes de sensores se caracterizan por ser redes desatendidas (sin intervención humana), con alta probabilidad de fallo (en los nodos, en la topología), habitualmente construidas ad-hoc para resolver un problema muy concreto (es decir, para ejecutar una única aplicación) [44].

Protocolos de comunicación

En el IoT, los objetos se reconocen a sí mismos y obtienen un comportamiento de inteligencia al tomar o habilitar decisiones relacionadas, ya que pueden comunicar información sobre sí mismos [4].

Normalmente, los protocolos de comunicación para IoT se organiza dentro de dos categorías: Red de área amplia de bajo consumo (LPWAN, por sus siglas en inglés) y redes de corto alcance. LPWAN se caracteriza por usar tecnología de baja potencia para proveer la comunicación inalámbrica, permitiendo el transporte de datos hasta una distancia de 50 Km [3]. Mientras que las redes de corto

alcance se caracterizan por proveer protocolos de comunicación estándares como: *6LowPAN*, *ZigBee*, ***Bluetooth Low Energy***, *RFID*, *NFC* y *Z-Wave*. Todos esos protocolos están enfocados a entornos de IoT, garantizan un bajo consumo de los recursos computacionales y conectividad de alto nivel [60].

Topologías

No puede existir IoT sin una topología de red que defina física o lógicamente la estructura de las comunicaciones entre los actores de la red. Los estándares de red [33] para IoT clasifican tres topologías de red básicas: *punto a punto*, *estrella* y *malla*. La topología punto a punto establece una conexión directa entre dos nodos de red.

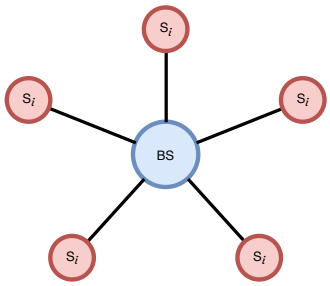

Figura 2.2: Estructura de una red con topología estrella. S_i representa un sensor y BS representa a la estación base.

En la topología de malla todos los nodos de red están conectados entre sí, proporciona una gran cantidad de redundancia cuando se trata de enlaces de red y un costo elevado de implementación. La topología estrella es la más utilizada debido a su baja complejidad de implementación y por la estructura cliente-servidor que proporciona. La estructura de la topología estrella se puede observar en la Figura 2.2.

2.1.3 Introducción a e-salud

Dentro del área médica, se encuentra un concepto reciente, que está teniendo una interesante relevancia, llamado e-salud [24]. El objetivo de e-salud es proveer herramientas que faciliten la recolección de datos, además de mantener la confidencialidad e integridad de los mismos [64] y permitan el monitoreo de la salud de los pacientes aún si éstos no están en un centro médico [72].

En un sentido más amplio, e-salud es la aplicación de TICs en un entorno médico o sanitario en prácticamente todos sus niveles: gestión, prevención, diagnóstico, tratamiento y seguimiento [74]. El término engloba tres áreas principales:

1. La entrega de información sanitaria, por profesionales sanitarios y consumidores, a través de Internet y telecomunicaciones.

2. La utilización del poder de las tecnologías de la información y el comercio electrónico para mejorar los servicios de salud pública, por ejemplo a través de la formación de los profesionales sanitarios.

3. El uso de prácticas relacionadas con el comercio electrónico en la gestión de servicios sanitarios.

Signos vitales del cuerpo humano

Uno de los objetivos de e-salud es monitorear la condición física de los pacientes tanto presencial como remotamente. Esto permite que tecnologías emergentes, como las redes inalámbricas de sensores, puedan tener lugar y crear un entorno de monitoreo remoto utilizando sensores que permitan obtener datos de los signos vitales de un paciente.

Los signos vitales son mediciones de las funciones más básicas del cuerpo. Los médicos indican que la presión arterial, la temperatura corporal, la frecuencia cardíaca y la saturación de oxígeno en la sangre son cruciales para reflejar el estado médico actual del paciente, y deben evaluarse de manera consistente y ser documentadas con precisión [48].

Presión arterial

La presión arterial resulta de la fuerza ejercida por la columna de sangre impulsada por el corazón hacia los vasos sanguíneos. La fuerza de la sangre contra la pared arterial es la presión sanguínea y la resistencia opuesta por las paredes de las mismas es la tensión arterial. Estas dos fuerzas son contrarias y equivalentes. La presión sistólica es la presión de la sangre debida a la contracción de los ventrículos y la presión diastólica es la presión que queda cuando los ventrículos se relajan [73].

Las pautas del Instituto Nacional del Corazón, Pulmones y Sangre (NHLBI, por sus siglas en inglés) ahora definen a la presión sanguínea normal de la siguiente manera:

- Presión sistólica de menos de 120 mm Hg.
- Presión diastólica de menos de 80 mm Hg.

Se cuantifica por medio de un manómetro de columna de mercurio o aneroide (tensiómetro), sus valores se registran en milímetros de mercurio (mm/Hg) [11].

Temperatura corporal

La temperatura corporal (TC) se define como el grado de calor conservado por el equilibrio entre el calor generado (termogénesis) y el calor perdido (termólisis) por el organismo. Cuando la TC sobrepasa el nivel normal se activan mecanismos como la vasodilatación, hiperventilación y sudoración que promueven la pérdida de calor. Si por el contrario, la TC cae por debajo del nivel normal se activan otros procesos como aumento del metabolismo y contracciones espasmódicas que producen los escalofríos y generan calor. La TC normal, de acuerdo a la Asociación Médica Americana, oscila entre 36.5º y 37.2º C [11].

Cuando la TC es anormal puede producirse por la fiebre (temperatura alta) o por la hipotermia (baja temperatura).

Frecuencia cardíaca

La frecuencia cardíaca (FC) es la cantidad de veces que el corazón late por minuto. A medida que el corazón impulsa la sangre a través de las arterias, las arterias se expanden y se contraen con el flujo sanguíneo [73].

La FC promedio de adultos en reposo es de 70 latidos por minuto, y oscila entre 60 y 100 latidos por minuto. En adultos, la taquicardia es una FC que excede los 100 latidos por minuto, y la bradicardia es una FC inferior a 60 latidos por minuto [11].

Saturación de oxígeno en la sangre

La saturación de oxígeno es la medida de la cantidad de oxígeno disponible en la sangre. Cuando el corazón bombea sangre, el oxígeno se une a los glóbulos rojos y se reparten por todo el cuerpo. Los niveles de saturación óptimos garantizan que las células del cuerpo reciban la cantidad adecuada de oxígeno.

Se considera que el porcentaje adecuado y saludable de oxígeno en sangre es de entre el 95 % y el 100 %. Por eso, cuando la saturación se encuentra por debajo del 90 % se produce hipoxemia, es decir, el nivel por debajo de los normal de oxígeno en sangre. Cuando esto ocurre, uno de sus síntomas característicos es la dificultad para respirar. Además, cuando se da un porcentaje inferior a 80 % se considera hipoxemia severa [73].

2.1.4 Redes Inalámbricas de Área Corporal

El creciente costo del mantenimiento de la salud y la frecuencia de enfermedades prolongadas en todo el mundo exigen fervientemente la reconstrucción de los servicios de salud con atención en el control de las enfermedades y el estado de salud de los pacientes. La atención que se requiere a los pacientes hospitalizados cuyo estado fisiológico debe ser monitoreado continuamente puede hacerse mediante el uso de tecnologías de monitoreo de IoT. Los sensores de salud inteligente se utilizan

para recopilar información fisiológica integral y utilizan puertas de enlace y la nube para almacenar los datos, analizarlos y luego enviar los datos analizados de forma inalámbrica a los cuidadores para su posterior análisis y revisión. De esta manera, al mismo tiempo mejora la calidad de la atención a través de una atención constante y reduce el costo de la atención al reducir el costo de las formas tradicionales de atención además de la recopilación y el análisis de datos [61].

Una WBAN es una red de comunicación inalámbrica entre dispositivos sensores de baja potencia utilizados en el cuerpo, consiste en un conjunto móvil y compacto de comunicación entre dispositivos móviles en un entorno de IoT. Éstas se consideran WSN de propósito especial, que se utilizan para proporcionar soluciones de comunicación a las aplicaciones médicas y de atención médica, en la Figura 2.3 se observa la relación entre ellas. Las WBANs suelen ser redes más pequeñas en comparación con las WSN, sin embargo, son vulnerables a ataques de seguridad [68]. Debido a la nula seguridad en la red y a la importancia de los datos que se transmiten en ella, es necesario garantizar seguridad para mantener protegidos los datos.

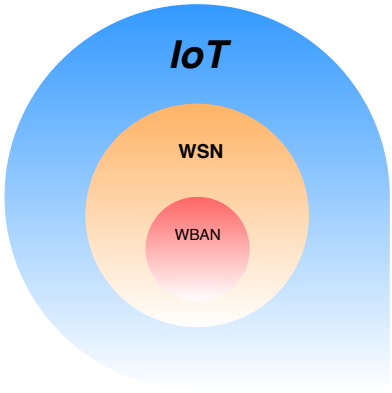

Figura 2.3: Relación en un entorno IoT de WSN con WBAN.

Los requisitos clave, tecnologías y consideración de diseño de las tecnologías de comunicación inalámbrica, que tienen el potencial de aplicarse en sistemas de salud IoT basadas en WBAN, se pueden caracterizar en seis temas principales: seguridad, consumo de energía, cuidado de la salud ubicuo, gestión de recursos, calidad de servicios y monitoreo en tiempo real [23], mismos que se

pueden observar en la Figura 2.4. En esta tesis, el área de estudio de WBAN se centra en seguridad de la información y en el diseño de soluciones eficientes para proveer los servicios de seguridad requeridos en una WBAN.

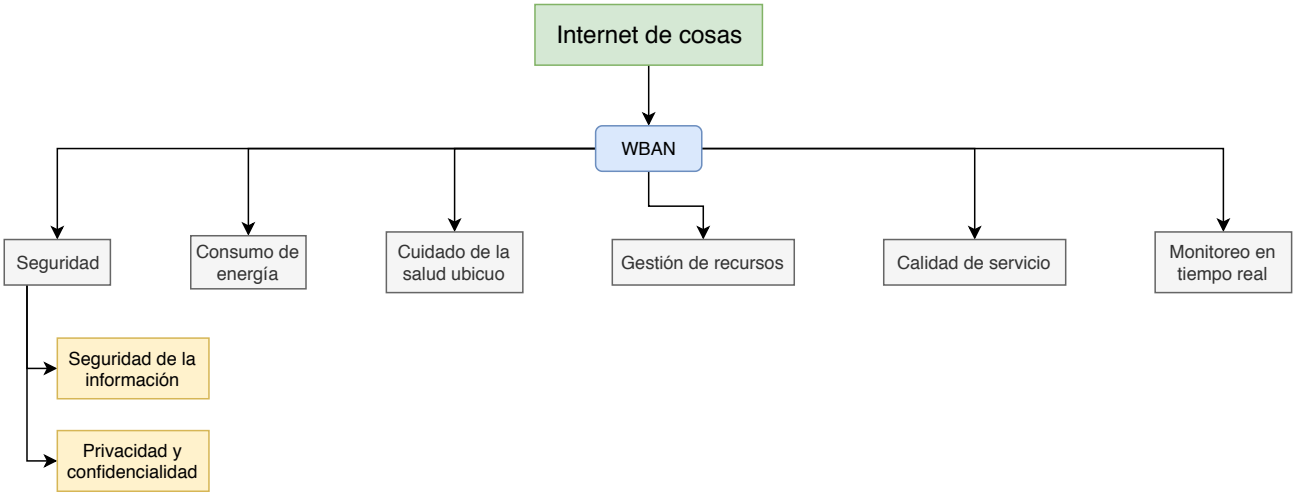

Figura 2.4: Tecnologías para el sistema de salud de IoT basado en WBAN.

2.1.5 Protocolos de comunicación de WBAN

El Instituto de Ingeniería Eléctrica y Electrónica (IEEE, por sus siglas en inglés) estableció un grupo de tareas llamadas IEEE 802.15.6 [38] para la estandarización de WBAN. La propuesta del IEEE 802.15.6 fue para definir nuevas capas física (PHY): Narrowband (NB), Ultra wideband (UWB), Human Body Communications (HBC) [59]; y Control de acceso al medio (MAC, por sus siglas en inglés), responsable del control de acceso al canal, proveer la flexibilidad para hacer posible el acceso múltiple por división de tiempo (TDMA, por sus siglas en inglés), acceso múltiple por detección de portadora y prevención de colisiones (CSMA/CA, por sus siglas en inglés) y la combinación de TDMA y CSMA/CA para reunir la demanda de las aplicaciones en las WBANs [38].

Para garantizar un alto nivel de seguridad, el estándar define tres niveles:

- Nivel 0 - Comunicación no segura. Los datos son transmitidos sin mecanismos de seguridad alguno. Los mensajes no son incluidos con autenticación e integridad de datos, o respuesta de

defensa, protección de la privacidad y confidencialidad.

- Nivel 1 - Sólo autenticación. Los mensajes son transmitidos de una manera segura pero sin mecanismo de cifrado. Este nivel no incluye protección de la privacidad ni confidencialidad. La respuesta de defensa, integridad y autenticación de mensaje son soportados.
- Nivel 2 - Autenticación y cifrado. La comunicación es segura usando cifrado y autenticación segura. Este nivel incluye una solución para resolver todos los problemas mencionados en los niveles anteriores.

Además del estándar IEEE 802.15.6, existen dos estándares que se utilizan para la comunicación en WBAN y en WSN. Estos estándares son el IEEE 802.15.1, mejor conocido como Bluetooth que es una tecnología utilizada para la conectividad inalámbrica de corto alcance entre diferentes dispositivos. Es una tecnología de radiofrecuencia que trabaja en la banda de 2.4 GHz y utiliza salto de frecuencia para expansión del espectro [27]. Y el estándar IEEE 802.15.4, conocido como ZigBee, cuyo propósito es ofrecer una solución completa para el tipo de redes de WPAN construyendo los niveles superiores de la pila de protocolos. ZigBee utiliza la banda ISM para usos industriales, científicos y médicos; siendo la banda de 2.4 GHz libre para todo el mundo [34].

2.1.6 Modelo de una red inalámbricas de área corporal

Una WBAN se define en IEEE 802.15.6 [38] como un estándar de comunicación diseñado para dispositivos de bajo consumo energético y funcionamiento alrededor del cuerpo (humano) y empleado en beneficio de los usuarios. Las WBANs están continuamente recopilando datos fisiológicos para monitorear la condición física de las personas [68].

Para comprender el tipo de mecanismo de seguridad que implementa una WBAN, primero se necesita conocer la estructura de la comunicación dentro de cada una de estas redes, así como su comunicación con el mundo exterior y con otras WBAN coexistentes. En la Figura 2.5 se muestra una visión general de la estructura de comunicación en WBANs, mostrando que los dispositivos están

distribuidos en una red, con la ubicación del dispositivo que actúa como estación base vinculado a una determinada aplicación. Debido a que el cuerpo cambia continuamente la posición, la topología de red no es fija. Por lo tanto, las WBAN no pueden clasificarse como una red fija. En la mayoría de los sistemas WBAN, la comunicación que se realiza entre sus componentes se divide en tres capas separadas de la siguiente manera [63]:

- **Capa 1. Recolección de datos:** en esta capa, la interacción de los sensores se limita al cuerpo de un usuario. Las señales de comunicación dentro de la región utilizan una estación base (BS, por sus siglas en inglés). Estos pueden ser dispositivos móviles como teléfono inteligente o tabletas, que actúan como BS, la cual funciona como fuente de datos en la capa 2.

- **Capa 2. Comunicación:** la comunicación en este nivel procura conectar la WBAN con otros sistemas o redes para que la información se pueda recuperar fácilmente a través de varios medios, como Internet.

- **Capa 3. Aplicación:** en esta capa se realiza el análisis de los datos recolectados y recibidos por parte de WBAN. En un entorno médico la base de datos es una parte especialmente importante de la comunicación de esta capa, debido a que contiene el historial médico y el perfil específico del usuario. Esta capa también permite la restauración de información importante para el usuario que puede ser crucial para planificar el tratamiento adecuado.

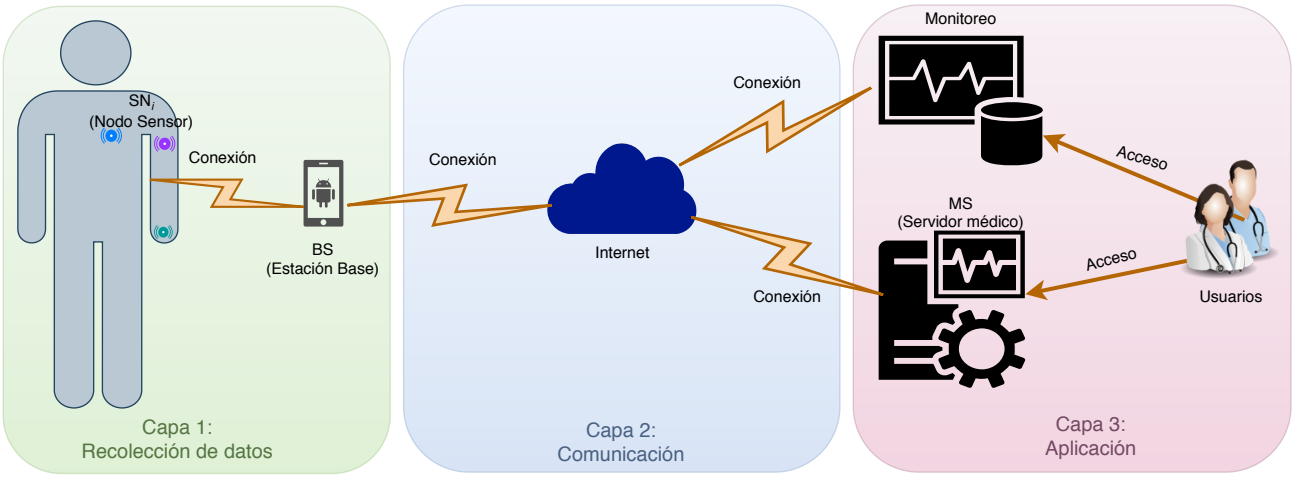

Figura 2.5: Estructura de un sistema de WBAN.

2.2 Criptografía ligera

En IoT, muchos dispositivos interconectados de recursos limitados no están diseñados para llevar a cabo costosos cálculos los cuales demandan un consumo de energía alto. Este es el caso de la ejecución de algoritmos criptográficos los cuales han sido considerados altamente demandantes en las redes convencionales. Por tanto, la mayoría de los algoritmos criptográficos convencionales son difíciles de implementar en dispositivos de IoT, dado que muchos dispositivos no cuentan con la energía suficiente o no cuentan la memoria necesaria para ejecutar un proceso de criptografía convencional. Garantizar la seguridad y la protección de la privacidad en el IoT, mediante algoritmos criptográficos convencionales, se convierte en una seria preocupación al integrar dispositivos con recursos limitados en el IoT de forma segura.

Actualmente existe una amplia gama de algoritmos criptográficos que se han usado de manera eficiente en redes convencionales, con dispositivos de cómputo de altas prestaciones como computadoras de escritorio o servidores. Sin embargo, la mayor parte de estos algoritmos criptográficos no tiene un rendimiento adecuado en el contexto de cómputo restringido como son las WBANs. Esto lleva a otra rama de la criptografía llamada *Criptografía ligera*, cuyo enfoque es que el

diseño e implementación de algoritmos los algoritmos criptográficos sea consciente de las limitaciones de los dispositivos sobre los que se ejecutará. La criptografía ligera es una técnica empleada tanto a nivel de hardware como software. Implementar un algoritmo criptográfico ligero que permita realizar un proceso con menor consumo de energía, memoria, tiempo de procesamiento, garantiza que el dispositivo mantendrá una autonomía suficiente para realizar otros procesos que se requieran.

2.2.1 Servicios de seguridad

Las WBANs son redes cuya función es monitorear la condición física de un usuario remotamente. Esta característica hace que las WBANs convencionales tengan riesgos de seguridad en cuanto a la transferencia de datos recolectados. Dado que los datos son sensibles, es un atractivo para cualquiera que desee obtener una ventaja al capturarlos y utilizarlos [68].

Los servicios de seguridad se consideran para mitigar los riesgos que existen en un entorno con comunicación inalámbrica como las WBANs. Estos servicios son garantizados por medio de mecanismos criptográficos [2].

- **Confidencialidad.** Con el fin de evitar que la información confidencial se revele a personas no autorizadas, este servicio garantiza que los datos se transmiten de manera segura y confidencial entre el origen y el destino.
- **Integridad.** Este servicio permite detectar alteraciones intencionales o no intencionales de lo datos desde su origen hasta el destino. Esto incluyen cualquier inserción, eliminación o sustitución de datos, lo que permite al usuario verificar si la información ha sido alterada.
- **Autenticación.** Este servicio es utilizado para garantizar que los datos deben ser enviados desde entidades legítimas y que los involucrados deben confirmar su identidad.
- **Control de acceso.** El control de acceso a parte de garantizar que solamente usuarios autorizados pueden acceder a los datos, asigna a los usuarios qué funciones pueden realizar

dentro de un sistema.

2.2.2 Criptografía de llave simétrica ligera

La criptografía de llave simétrica se basa en una llave compartida que se utiliza para cifrar texto o descifrar texto cifrado, como se puede observar en la Figura 2.6, al contrario con la criptografía de llave asimétrica, donde las llaves de cifrado y descifrado son diferentes. El cifrado simétrico es, generalmente, más eficiente que el cifrado asimétrico y, por lo tanto, se prefiere cuando es necesario garantizar confidencialidad sobre más de un bloque de datos [37]. Establecer la llave compartida es difícil utilizando solo algoritmos de cifrado simétrico, por lo que en muchos casos, se utiliza un cifrado asimétrico como mecanismo para establecer un secreto compartido entre dos partes, que sirva después como la llave compartida entre ellas para el intercambio seguro de datos mediantes criptografía simétrica.

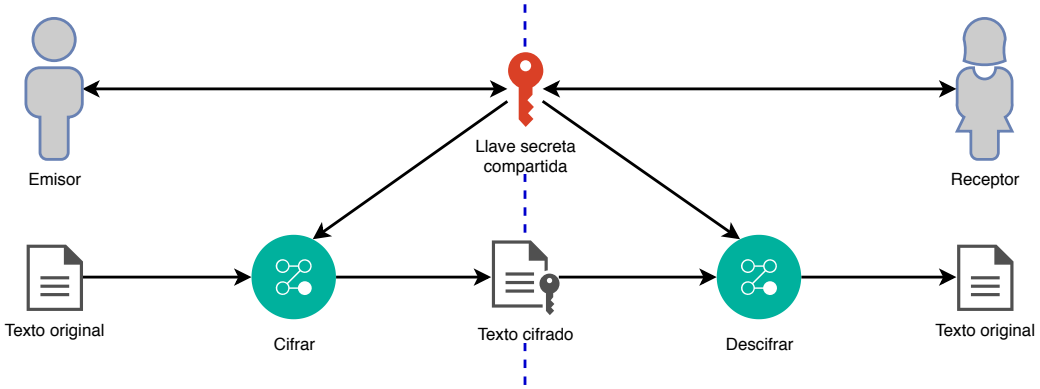

Figura 2.6: Diagrama de cifrado y descifrado de un texto.

Este campo, la criptografía ligera provee algoritmos adecuados para entornos con recursos limitados para cifrado de datos. Estos algoritmos son cifradores ligeros, específicamente, cifradores ligeros por bloques [45].

2.2.3 Funciones hash ligeras

Las funciones hash, también llamadas funciones resumen, son algoritmos que, en esencia, no usan clave. En cambio, se calcula un valor de hash de longitud fija a partir de una pieza de datos (cadena de bits), como se observa en la Figura 2.7. La función usa cada bit de los datos de entrada y mediante una serie de rondas de procesamiento genera un código de longitud fija, único e irrepetible. Dado los datos D y la función hash H, el código obtenido de D mediante H es $H(D)$. Las funciones hash deben tener propiedades especiales, siendo la más importante la de unidireccionalidad y resistencia a colisiones. La primera propiedad indica que dado $H(D)$ es imposible obtener D. La segunda propiedad indica que si $H(D_1) = H(D_2)$, entonces $D_1 = D_2$. El cambio de un solo bit en D producirá un valor $H(D)$ diferente en al menos la mitad de sus bits. Por ello, las funciones hash proporcionan un mecanismo para garantizar la integridad de datos.

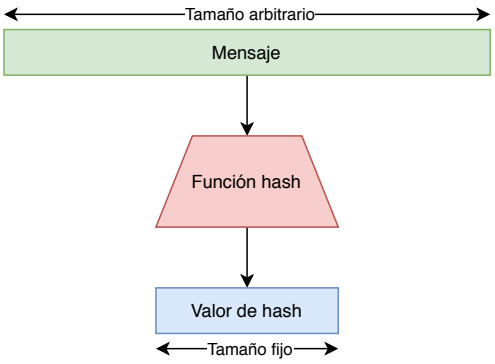

Figura 2.7: Diagrama de bloques de una función hash.

Los ataques más comunes a los que se enfrenta una función hash son ataques de preimagen cuyo objetivo es intentar encontrar un mensaje que tiene un valor hash específico, es decir, a partir del resultado de una función hash, encontrar el mensaje de entrada. Y colisiones que es una situación que se produce cuando dos entradas distintas a una función de hash producen la misma salida.

Las funciones hash convencionales no pueden ser adecuadas para entornos limitados computacionalmente, debido a sus grandes tamaños de estado y a los altos consumos de energía.

Esto ha llevado al desarrollo de funciones hash ligeras. El uso de las funciones hash convencionales y ligeras difiere en dos aspectos [45]:

1. Estado interno y tamaños de salida más pequeños: los tamaños de salida grandes son importantes para aplicaciones que requieren resistencia a colisiones de funciones hash. Para aplicaciones que no requieren resistencia a la colisión, podrían usarse estados internos y tamaños de salida más pequeños. Cuando se requiere una función de hash resistente a colisiones, puede ser aceptable que una función de hash tenga la misma seguridad contra ataques de preimagen. Una función hash tiene resistencia a la primera preimagen si dado un valor hash y, es computacionalmente imposible encontrar x tal que $H(x) = y$. Tiene resistencia a la segunda preimagen si dado un mensaje x, es computacionalmente imposible encontrar un x', $x \neq x'$, tal que $H(x) = H(x')$. Finalmente tiene resistencia a colisiones si encontrar un par (x, y) con $y \neq x$ tal que $H(x) = H(y)$ es computacionalmente imposible. Es decir, es difícil encontrar dos entradas que tengan el mismo valor resumen.

2. Tamaño de mensaje más pequeño: se espera que las funciones hash convencionales admitan entradas con tamaños muy grandes (alrededor de 264 bits). En la mayoría de los protocolos de destino para funciones hash ligeras, los tamaños de entrada típicos son mucho más pequeños (por ejemplo, como máximo 256 bits). Por lo tanto, las funciones de hash optimizadas para mensajes cortos pueden ser más adecuadas para aplicaciones ligeras.

2.2.4 Código de autenticación de mensajes

Un Código de Autenticación de Mensaje (MAC, por sus siglas en inglés), es un código de longitud fija utilizado para autenticar un mensaje. Los valores MAC se calculan mediante la aplicación de una función hash criptográfica con llave secreta k, que sólo conocen el remitente y destinatario, pero no los atacantes. La función hash tiene que cumplir ciertas propiedades de seguridad que las hacen resistentes frente ataques de adversarios. Matemáticamente la función hash toma dos argumentos:

una llave k de tamaño fijo y un mensaje M de longitud arbitrario. El resultado es un código MAC de longitud fija, este proceso se puede observar en la Figura 2.8.

$$\sigma = \text{MAC}(k, M) \tag{2.1}$$

Donde:

1. M es un mensaje de longitud arbitraria.
2. MAC es la función que transforma el mensaje en un valor MAC y que utiliza una llave secreta k como parámetro.
3. σ es el valor MAC calculado de longitud fija.

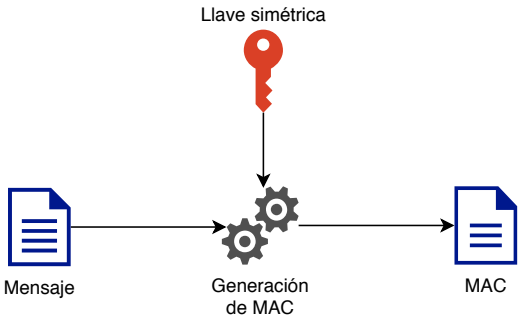

Figura 2.8: Diagrama general de la generación de MAC de un mensaje.

Si el valor MAC enviado coincide con el valor que el destinatario calcula, éste puede garantizar que:

- El mensaje no fue alterado.
- El mensaje proviene del remitente indicado en el mensaje.
- Si el mensaje incluye un número de secuencia, que el mensaje sigue la secuencia correcta.

HMAC es una especificación de MAC publicada en [13, 35]. Es el algoritmo más utilizado para cálculos de códigos de autenticación de mensajes.

2.2.5 Cifrado autenticado

Un esquema de cifrado autenticado es un esquema de criptografía que provee confidencialidad y autenticación a los datos, usando una llave secreta. Este esquema realiza un proceso similar al cifrado convencional, la compartición de datos se hace entre dos entidades. Ambas deben compartir una llave secreta que se utiliza tanto para cifrar como para descifrar los datos. Lo adicional es que se autentican los datos, antes de cifrarlo o después, dependiendo del enfoque que se utilice [15], como se puede observar en la Figura 2.9.

El cifrado autenticado puede ser mapeado a una ecuación que representa el cifrado de los datos, tal que:

$$C, \sigma = \varepsilon_k^{N,A}(M) \tag{2.2}$$

Donde ε es el proceso de cifrado, C es el texto cifrado, σ es la MAC generada, N es un número aleatorio, A son los datos asociados (opcionales), k una llave secreta compartida entre ambas entidades y M es el mensaje.

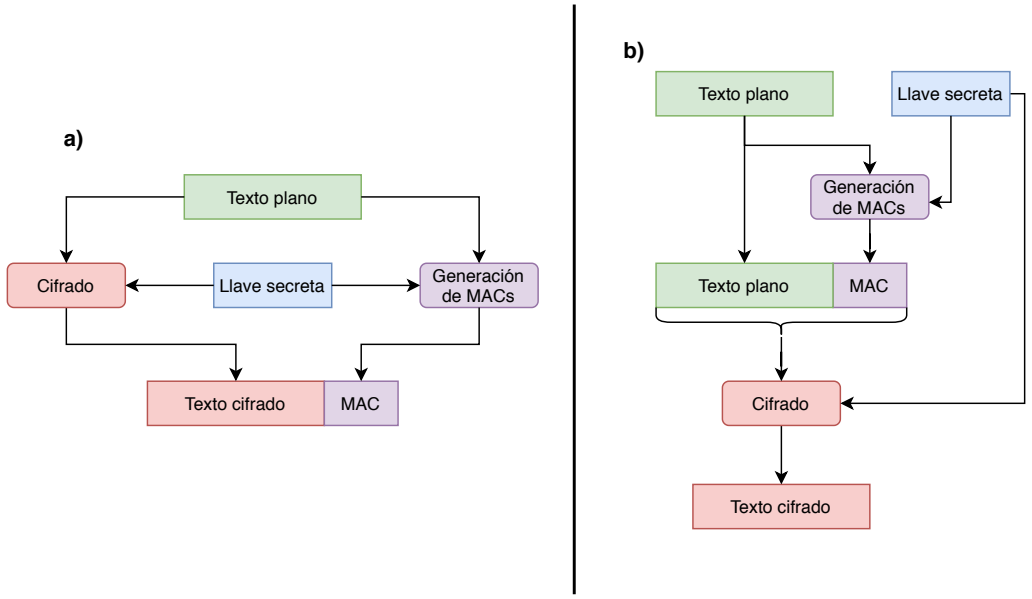

Figura 2.9: Diagrama de bloques del cifrado autenticado. a) Primero se cifra, después se autentica. b) Primero se autentica, después se cifra.

La implementación de este esquema proporciona las siguientes funciones:

1. **Cifrado**

   - Entada: texto plano (M), llave secreta (k), y opcionalmente un encabezado en texto plano que no será cifrada, pero serán cubiertos por la protección de la autenticidad.
   - Salida: texto cifrado (C) y la etiqueta de autenticación o MAC (σ).

2. **Descifrado**

   - Entrada: texto cifrado (C), llave secreta (k), etiqueta de autenticación (σ), y opcionalmente un encabezado (A).
   - Salida: texto plano (M), o un error si la etiqueta de autenticación no coincide con el texto cifrado o cabecera .

2.2.6 Criptografía de curva elíptica

La criptografía de curva elíptica (ECC, por sus siglas en inglés) [39] es un caso de Criptografía de llave pública (PKC, por sus siglas en inglés), basado en un conjunto de puntos en una curva elíptica. ECC provee la misma funcionalidad que otros esquemas PKC, realiza cifrado de datos, firmas digitales o intercambio de llaves. La multiplicación escalar denotada como nP, donde n es un entero positivo y P es un punto en la curva elíptica, es la operación esencial y más costosa (computacionalmente) que se realiza. A pesar de ello, provee los mismos niveles de seguridad que un esquema PKC pero utiliza un tamaño de llaves más pequeño.

En ECC se usa una curva elíptica definida sobre un campo finito $\mathbb{F}_q$, que se denota como $E(\mathbb{F}_q)$ y contiene puntos $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ que satisface la ecuación Weierstrass 2.3. Un ejemplo de una curva elíptica se puede observar en la Figura 2.10.

$$y^2 a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \qquad \text{dónde} \quad a_i \in \mathbb{F}_q \tag{2.3}$$

La curva $E(\mathbb{F}_q)$ junto con un elemento llamado punto en el infinito $\mathcal{O}$, forman un grupo abeliano. $\mathcal{O}$ actúa como el elemento neutro dentro de la operación de grupo. La seguridad en ECC se basa en la dificultad de resolver el problema de logaritmo discreto de curva elíptica (ECDLP, por sus siglas en inglés). ECDLP es un problema que se considera difícil de resolver para un tamaño de grupo (número de puntos en la curva elíptica) relativamente grande: dados dos puntos, P y Q, en una curva elíptica, encuentre el número entero n, si existe, tal que $Q = nP$ [54].

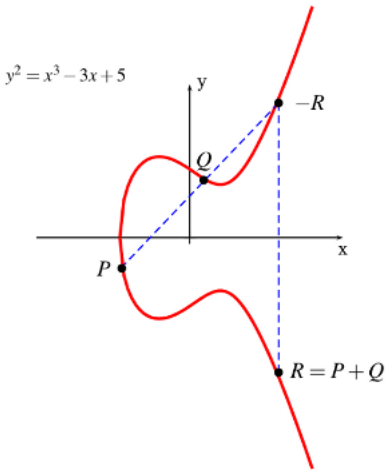

Figura 2.10: Curva elíptica con $a = -3$ y $b = 5$

La forma generalizada de una curva elíptica puede reducirse o simplificarse para identificar los conjuntos particulares de curvas de una forma más simple, son llamadas familias.

- **Curvas primas.** Las curvas elípticas definidas sobre un campo $\mathbb{F}_q$ con $q = p^m$ y $m = 1$, la ecuación de Weierstrass es simplificada como:

$$E_p : y^2 = x^3 + ax + b, \qquad \text{con } a, b \in \mathbb{F}_q \text{ y } 4a^3 + 27b^2 \neq 0 \tag{2.4}$$

- **Curvas elípticas binarias.** Las curvas elípticas sobre un campo finito $\mathbb{F}_q$ con $q = p^m$ y $p = 2$ son definidas por la ecuación:

$$E_b : y^2 + xy = x^3 + ax^2 + b, \qquad \text{con } a, b \in \mathbb{F}_{2^m} \tag{2.5}$$

- **Curvas Montgomery.** Es una forma de curva elíptica definida sobre $\mathbb{F}_q$ por:

$$E_M : By^2 = x^3 + Ax^2 + x, \qquad \text{con } A \in \mathbb{F}_q \setminus \{-2, 2\}, B \in \mathbb{F}_q \setminus \{0\} \text{ y } B(A^2 - 4) \neq 0 \tag{2.6}$$

- **Curvas de Koblitz.** También conocidas como curvas binarias anómalas. Esta familia de curvas satisface una ecuación de la forma:

$$E_K : y^2 + xy = x^3 + ax^2 + 1, \qquad \text{con } a \in \mathbb{F}_2 \tag{2.7}$$

Protocolos criptográficos basados en curva elíptica

- **Protocolo de Diffie-Helman**. Este protocolo cuenta con dos versiones, la clásica y la de curvas elípticas [56].

  - *Versión clásica*. Sea p un número primo, $\alpha \in \mathbb{Z}_p$, un elemento primitivo. Cada usuario U elige aleatoriamente un número secreto $n_U \in \mathbb{Z}_p^*$ y hace público el valor α^{n_U}. Los usuarios A y B desean compartir una llave secreta:

$$\begin{aligned} A \quad & \xrightarrow{\alpha^{n_A}} \quad B \\ A \quad & \xleftarrow{\alpha^{n_B}} \quad B \end{aligned} \tag{2.8}$$

    La llave secreta será $K = \alpha^{n_A \cdot n_B}$, que solo es conocida por A y B.

  - *Versión con curvas elípticas*. Sea E una curva elíptica sobre $\mathbb{F}_q$ y $P \in E$ punto públicamente conocido. Cada usuario U elige aleatoriamente un número secreto $n_U \in \mathbb{F}_q$ y hace público el valor $n_U \cdot P$. Para compartir una llave secreta, A y B deben hacer:

$$\begin{aligned} A \quad & \xrightarrow{n_A \cdot P} \quad B \\ A \quad & \xleftarrow{n_B \cdot P} \quad B \end{aligned} \tag{2.9}$$

    La llave secreta será $K = (n_A \cdot n_B) \cdot P$ que solo es conocida por A y B.

- **Protocolo de tres-pasos de Shamir**.

– *Versión clásica*. Este protocolo pretende enviar el mensaje m de A a B.

$$\begin{array}{ccc} & A \quad \underrightarrow{E_A(m)} \quad B & \\ A \quad \underleftarrow{E_B(E_A(m))} \quad B & & \\ & A \quad \underrightarrow{E_B(m)} \quad B & \end{array} \tag{2.10}$$

Es fundamental suponer que la función criptográfica utilizada cumple para cada pareja de usuarios, $E_A \cdot E_B = E_B \cdot E_A$.

– *Versión con curvas elípticas*. Está basado en el protocolo de *Massey-Omura*. Sea E una curva elíptica sobre $\mathbb{F}_q$, $N = \#E(q)$. Sea $P \in E$ el mensaje que el usuario A quiere enviar a B. Cada usuario U tiene una llave privada n_U tal que $mcd(n_U, N) = 1$.

$$\begin{array}{ccc} & A \quad \underrightarrow{n_A \cdot P} \quad B & \\ A \quad \underleftarrow{n_B(n_A \cdot P)} \quad B & & \\ & A \quad \underrightarrow{n_B \cdot P} \quad B & \end{array} \tag{2.11}$$

2.2.7 Criptografía basada en emparejamientos

Un grupo G con orden n (cardinalidad) y generador g es usualmente denotado por $\mathrm{G} = \langle g \rangle$. Si $\mathcal{O}$ es el punto en el infinito en G, entonces $g^i \in \mathrm{G}$ para $i = 1$ hasta $n - 1$ y $g^n = \mathcal{O}$.

La criptografía basada en emparejamientos (PBC, por sus siglas en inglés) se basa en funciones de emparejamiento que mapean pares de puntos en una curva elíptica en un campo finito [46]. En PBC, la operación central es el emparejamiento, un mapeo $e : \mathrm{G}_1 \times \mathrm{G}_2 \to \mathrm{G}_T$, donde G_1, G_2 y G_T son grupos algebraicos abstractos de orden r.

Un emparejamiento bilineal es definido sobre grupos y que constituyen en la operación que afecta fuertemente a la eficiencia y seguridad de esquemas criptográficos basados en emparejamientos. En

la práctica $\mathrm{G}_1 = \langle g_1 \rangle$, $\mathrm{G}_2 = \langle g_2 \rangle$ son subgrupos de una curva elíptica con un orden primo r. G_T es una extensión del grupo multiplicativo del campo finito $\mathbb{F}_{q^k}$. El parámetro k se refiere al grado de incrustación de la curva elíptica, es el entero positivo más pequeño tal que r se divide entre $q^k - 1$. Un emparejamiento bilineal es una eficiente función computable [49]: $e : \mathrm{G}_1 \times \mathrm{G}_2 \to \mathrm{G}_T$.

Las propiedades principales de los emparejamientos bilineales son:

- **Bilinealidad.**

$$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}, \quad \forall g_1 \in \mathbf{G}_1, g_2 \in \mathbf{G}_2, \{a, b\} \in \mathbb{Z}_r^* \tag{2.12}$$

- **No degeneración.**

$$e(g_1^a, g_2^b) \neq 1 \tag{2.13}$$

- **Computabilidad.** Existen algoritmos eficientes para computar $e(g_1, g_2)$.

PBC permite construir protocolos criptográficos de más alto nivel, como el Cifrado Basado en Identidad (IBE, por sus siglas en inglés), que permite al remitente cifrar un mensaje sin necesidad de que la clave pública del receptor haya sido certificada y distribuida por adelantado. IBE utiliza alguna forma de identificación de persona (o entidad) para generar una llave pública. Esto podría ser una dirección de correo electrónico, por ejemplo [47].

Cifrado basado en atributos

El Cifrado Basado en Atributos (ABE, por sus siglas en inglés) es una primitiva efectiva para lograr un control de acceso de grano fino, donde los datos cifrados debe ser legible solo por un grupo de usuarios que satisfagan una determinada política de acceso [4]. Se construye a partir del esquema IBE, reemplazando el uso de una identidad por un conjunto de atributos que validan si la entidad está certificada y con acceso.

Los sistemas ABE usan una estructura de acceso $\mathbb{A}$ restringiendo las capacidades de descifrado de los destinos previstos de un texto cifrado. La estructura de acceso es definida por una expresión lógica sobre un conjunto de atributos pertenecientes al universo $\mathcal{U}$. $\mathbb{A}$ específica un subconjunto no vacío del conjunto potencia $\mathcal{P}(U)$. Cada conjunto en $\mathbb{A}$ es un conjunto autorizado de atributos permitidos para descifrar los datos, mientras que los conjunto en $\mathcal{P}(U)$ pero no en $\mathbb{A}$ son conjuntos no autorizados [49].

La complejidad del cifrado ABE depende principalmente del número de atributos asociados con la llave en esquemas ABE de política llave (KP-ABE, por sus siglas en inglés) o del texto cifrado en esquemas ABE de política de texto cifrado (CP-ABE, por sus siglas en inglés), pero es independiente del número de usuarios en el sistema. ABE está conceptualmente más cerca de un control de acceso basado en roles. Los sistemas ABE, generalmente, constan de 4 principales etapas en su implementación [49]:

1. **Configuración.** Se seleccionan los parámetros del emparejamiento, se define la estructura de acceso y se crean la llave pública PK y la llave privada MK para especificar el nivel de seguridad ζ. PK es usada para cifrado y MK es usada para la generación de llave privada.

2. **Cifrado.** Toma como entrada un mensaje M, una estructura de acceso $\mathbb{A}$ y PK para cifrar M, generando CT.

3. **Generación de llave.** Toma como entrada MK y un conjunto de atributos S. Genera la llave de sesión SK, relacionada con S, destinada para descifrar CT.

4. **Descifrado.** Toma como entrada SK y CT. Recupera M de CT, sí y sólo sí, SK fue derivado de un conjunto de atributos autorizado en la estructura de acceso $\mathbb{A}$ usada al cifrar M.

DET-ABE

DET-ABE es un esquema de seguridad construido sobre el concepto de sobres digitales criptográficos [49]. DET-ABE usa un cifrado simétrico y uno de llave pública. El cifrado simétrico

transforma el mensaje M en texto cifrado CT por medio de operaciones SE_k para cifrado y SD_k para descifrado, tal que $CT = SE_k(M)$ y $M = SD_k(CT)$. Ambas operaciones utilizan la misma llave simétrica k y la protección de dicha clave es crucial para garantizar el servicio de confidencialidad sobre la información importante que se cifra. Un cifrado de llave pública utiliza dos llaves, una de dominio público para el cifrado PE_{PK} y la otra privada para el descifrado PD_{SK}. En este caso, $CT = PE_{\mathsf{PK}}(M)$ y $M = PD_{\mathsf{SK}}(CT)$.

El funcionamiento de un sistema utilizando DET-ABE es el siguiente: el servidor encargado del sitio web aloja a la autoridad de confianza que reparte las llaves secretas. Cada usuario completa, inicialmente, un proceso de registro con el servidor, en el que se le asigna una llave secreta en función de sus atributos; algunos ejemplos de atributos en esta situación podrían ser "mayor de edad", "miembro del club con categoría A/B/C", "persona con tarjeta de crédito registrada", entre otros. Después, para acceder a cada recurso protegido del sitio web, el servidor habrá definido anteriormente una política de acceso para ese determinado recurso, por ejemplo "miembro del club con categoría A/B/C" y "personas con tarjeta de crédito registrada" ó "mayor de edad". Los usuarios deben tener atributos que satisfagan las políticas para poder acceder a los recursos.

La verificación de la política, dados los atributos del usuario, es matemática. Esto es, se verifica una condición a partir de una serie de operaciones en el emparejamiento y en las curvas elípticas involucradas, usando la llave privada del usuario, texto cifrado y la política de control de acceso.

En esta tesis, DET-ABE utiliza un cifrado simétrico ligero como Lightweight Encryption Algoritm (LEA) y CP-ABE como cifrador de llave pública.

3

Estado del arte

En este capítulo se presenta una revisión de los trabajos relacionados con el tema principal de esta tesis. El capítulo se encuentra organizado de la siguiente forma. Primero se presenta una revisión de los trabajos relacionados con base en los servicios de seguridad que se han considerado para una WBAN. Después, se discuten los trabajos previos indicando los algoritmos que se han considerado para proveer servicios de seguridad en una WBAN. A continuación, se presenta una revisión de los trabajos en la literatura que han reportado implementaciones de prototipos de WBAN, y la medida en la que se han evaluado en dichos prototipos algoritmos criptográficos para la provisión de servicios de seguridad. Finalmente, se presenta una discusión de cómo el trabajo de investigación realizado en esta tesis contrasta con los trabajos previos.

3.1 Servicios de seguridad en WBAN

Las WBANs son redes inalámbricas cuya función es monitorear la condición física de una persona remotamente. Dado que los datos obtenidos de los signos vitales monitoreados (ritmo cardíaco,

presión arterial, saturación de oxígeno en la sangre, etc.) son sensibles, puede resultar atractivo para un tercero acceder al medio de comunicación inalámbrica y obtener una ventaja al capturarlos y utilizarlos [68]. Por ejemplo, para un proveedor de seguros médicos la información accedida proveniente de la WBAN le puede resultar en una ventaja para la oferta o el costo de sus pólizas.

Algunos autores [2, 50, 58, 63, 64, 68, 72] coinciden en que los servicios de seguridad que deberían garantizarse en WBANs son la triada CIA (Confidencialidad, Integridad, Autenticación). Además, consideran al control de acceso como otro servicio de seguridad principal para una WBAN, dado que varios usuarios (médicos, enfermeras, pacientes, etc.) interactúan en la WBAN para acceder a los datos.

- **Confidencialidad.** El servicio de confidencialidad es considerado el servicio más importante [68]. Este servicio proporciona protección a los datos, en caso de ser capturados por algún atacante. Dado que las WBANs transmiten información muy sensible y personal sobre el estado de salud del paciente, la confidencialidad protege la privacidad de esos datos, haciéndolos ininteligibles para una entidad no autorizada. Existen diversos algoritmos criptográficos encargados de garantizar la confidencialidad de los datos a través del cifrado. Además, se garantiza que solamente las entidades autorizadas entiendan los datos transferidos al aplicar el descifrado de los datos. La herramienta más efectiva para garantizar el servicio de confidencialidad son los cifradores simétricos. En el caso de una WBAN, al ser entorno de cómputo con restricciones computacionales, se recomienda utilizar algoritmos criptográficos ligeros, dado que son conscientes de las limitaciones computacionales. Algunos ejemplos de estos cifradores son: **LEA** [30], **AES** [26], **PRESENT** [17], **CLEFIA** [65], entre otros.

- **Integridad.** Mantener la integridad de los datos es fundamental en una WBAN. La confidencialidad no los protege de modificaciones externas, debido a que la información se puede modificar ilícitamente cuando los datos se transmiten en una WBAN convencional. La integridad garantiza que los datos no serán intercambiados o alterados por algún atacante, en

caso contrario, se desechan. Esto se logra a través de protocolos de autenticación de datos como son las funciones hash [41]. Al garantizar la integridad, las WBANs obtienen una robustez contra alteraciones por ruido o interferencia que puedan sufrir los datos durante su transmisión. La pérdida de integridad ocurre si un nodo malicioso agrega fragmentos adicionales o manipula los datos dentro de un paquete [68]. En el contexto de criptografía ligera, las funciones hash que se ha propuesto son **SPONGENT** [16], **QUARK** [10], **PHOTON** [28], entre otros.

- **Autenticación.** Debido a la sensibilidad de los datos transmitidos en una WBAN, es necesario utilizar protocolos de autenticación para verificar que los datos fueron emitidos por una entidad de confianza y autorizada [32]. Es esencial que se verifique que los datos fueron enviados por un nodo sensor confiable. La autenticación de datos se puede lograr mediante el uso de técnicas simétricas, como obtención de MACs [35], o por esquemas de criptografía asimétrica.

- **Control de acceso** El control de acceso es una política de privacidad para evitar el acceso no autorizado a los datos del paciente. En WBANs, diferentes usuarios como médicos, enfermeras, farmacias, compañías de seguro, entre otros, podrían acceder a los datos médicos del paciente y tomar ventaja. Por lo tanto, se requiere un control de acceso basado en roles para imponer diferentes privilegios de acceso para diferentes usuarios mediante políticas de acceso [32]. Existe un enfoque de la criptografía que se encarga del control de acceso de grano fino llamado ABE [19, 29].

En la Tabla 3.1 se presenta a manera de resumen trabajos representativos en el estado del arte donde se describen los servicios de seguridad que se han considerado, usando el modelo de referencia de WBAN de tres capas. La Tabla 3.1 revela que los cuatro servicios de seguridad no se han considerado en el diseño de WBAN ni tampoco se ha considerado la seguridad en las tres capas del modelo WBAN. Los servicios de seguridad más utilizados en esta revisión de la literatura son confidencialidad y autenticación, seguidos por el servicio de control de acceso como el tercero más utilizado e integridad el último. El servicio de integridad está implícito en el de autenticación, sin

embargo, el servicio de integridad podría implementarse de manera independiente sin necesidad de la autenticación. Todos los trabajos revisados solamente se enfocaron en la capa 1 del modelo de WBAN, debido a que en esa capa se encuentra la generación y tráfico de datos del paciente. Sin embargo, para que una WBAN sea segura se debe proteger los datos desde la emisión hasta su punto de entrega final, lo cual no se cubren en los trabajos previos. La cantidad de servicios de seguridad garantizados en cada capa depende de los recursos computacionales disponibles y la necesidad del entorno, es decir, si se implementa una WBAN en un entorno donde se tiene la seguridad de que la red no será vulnerada, solamente bastaría con garantizar la confidencialidad de los datos.

Tabla 3.1: Servicios de seguridad considerados en trabajos relacionados con WBAN.

Trabajo	Modelo WBAN		
	Capa 1	Capa 2	Capa 3
[52], 2014	{Confidencialidad, Control de acceso}	-	-
[51], 2017	{Confidencialidad}	-	-
[6], 2017	{Confidencialidad}	-	-
[1], 2018	{Confidencialidad, Autenticación}	-	-
[7], 2019	{Autenticación, Integridad, Control de acceso}	-	-
[53], 2019	{Autenticación}	-	-
[19], 2019	{Confidencialidad, Control de acceso}	-	-
[25], 2019	{Autenticación, Integridad}	-	-
[31], 2019	{Autenticación, Integridad, Control de acceso}	-	-
Esta tesis, 2020	**{CIA, Control de acceso}**	**{CIA}**	**{CIA, Control de acceso}**

Los servicios de seguridad como los descritos hasta ahora y considerados en trabajos previos de WBAN son generalmente provistos mediante algoritmos criptográficos. Un mismo servicio puede proveerse por más de un algoritmo criptográfico en alguna de las dos familias de algoritmos criptográficos. En la Tabla 3.2 se resumen los algoritmos utilizados por los trabajos relacionados para garantizar los diferentes servicios de seguridad en una WBAN. Para la garantizar la confidencialidad se han utilizado algoritmos criptográficos simétricos y ligeros, con excepción de AES y Twofish,

que son simétricos y de propósito general. Para autenticación, la mitad de los trabajos reportaron garantizarla y la mayoría de ellos utilizaron un enfoque asimétrico. Solamente tres trabajos reportaron garantizar la integridad, dos de ellos utilizando un enfoque asimétrico, con firmas digitales bajo diferentes técnicas y uno utilizando un enfoque simétrico. Para garantizar el control de acceso, todos los trabajos que reportan garantizarlo coinciden en utilizar ABE. Durante la revisión se observó que el nivel de seguridad no es reportado en el 40 % de los trabajos revisados. Además, el nivel de seguridad de la mayoría de los trabajos que lo reportan es obsoleto, de 80 bits [12] (existe una página web que evalúa requerimientos de seguridad mínimos en un sistema[1]).

Tabla 3.2: Algoritmos criptográficos más utilizados para proveer servicios de seguridad en WBANs.

Trabajo	Servicios de seguridad				Nivel de
	Confidencialidad	Autenticación	Integridad	Control de acceso	seguridad (bits)
[52], 2014	AES	-	-	ABE	128
[51], 2017	PRESENT	-	-	-	80
[6], 2017	LEA	-	-	-	128
[1], 2018	KBS/KAISC	MAC	-	-	-
[7], 2019	-	ECC	Firma digital	ABE	80
[53], 2019	-	ECC	-	-	-
[19], 2019	Twofish	-	-	ABE	-
[25], 2019	-	PKC	SHA2	-	-
[31], 2019	-	ECC	ABE	ABE	80
Esta tesis, 2020	**LEA**	**MAC**	**SPONGENT**	**ABE**	**$\geq$ 128**

3.2 Prototipos WBAN

En la literatura existen trabajos relacionados que abordan la problemática de desarrollar prototipos de WBAN, cuyo objetivo principal es garantizar la seguridad de los signos vitales de los pacientes,

[1] https://www.keylength.com/en/compare/

recolectados por los nodos sensores y transmitidos por canales inalámbricos a una estación base.

- En [6] se propone una arquitectura de diseño para garantizar una transmisión segura de datos desde un nodo sensor a un dispositivo móvil como estación base, considerando el uso de energía eficiente en una WBAN. La solución propuesta cubre la comunicación en la capa 1 del modelo WBAN, es decir, la recolección de los signos vitales del paciente y la transmisión a la estación base.

  El proceso es el siguiente: el paciente usará sensores para detectar sus signos vitales, como la frecuencia del pulso, la temperatura, la frecuencia respiratoria y la presión arterial, etc. Estos datos recolectados son cifrados utilizando *LEA*, para garantizar la confidencialidad, privacidad. Después del cifrado, los datos se transmiten a la estación base.

  Los algoritmos de cifrado se implementaron en la red de sensores corporales en lenguaje JavaScript. Las lecturas que se tomaron en la implementación son datos de frecuencia cardíaca y el microcontrolador que usó es una CPU de 32 de bits Intel Curie como dispositivo de hardware por la peculiaridad de ser de bajo consumo. Únicamente se sensó el ritmo cardíaco. Se utilizó la Máquina Virtual de Bajo Nivel Emscripten para compilar códigos C y C++ en JavaScript. Se utilizó también la plataforma Johny Five para la programación del microcontrolador usando JavaScript.

- En [19] se propone un esquema usando el algoritmo simétrico Twofish y un esquema CPABE-CSC. La propuesta considera la actualización de políticas de control de acceso, pero solo se consideran estructuras que usan compuertas AND. Para la experimentación se utilizó un radio ChipconCC1000 en un mote Crossbow MICA2DOT, el cuál utiliza 28.6 μJ para recibir un byte y 59.2 μJ para transmitir un byte. Las métricas reportadas son: tamaño del mensaje, consumo de energía en comunicaciones y costo computacional asociado al tiempo de ejecución. Como resultado de la experimentación realizada se reportó el desempeño de tres procesos: cifrado, descifrado y actualización de políticas. EL prototipo reportado solo provee los servicios de

confidencialidad y control de acceso.

- En [25] se propone un sistema para el control de acceso en WBAN. El prototipo consiste de un dispositivo wearable, smartwatch K18, con suficiente capacidad computacional para realizar procesos criptográficos. La solución se encuentra fija dentro del dispositivo wearable. Se utiliza un algoritmo ligero para el cifrado de datos y SHA2 como algoritmo hash para el servicio de integridad. En esta propuesta se utilizó una tarjeta de memoria donde se almacenó los códigos fuentes de los algoritmos criptográficos que se implementaron en el dispositivo para su posterior ejecución. No se reportan resultados esperados ni experimentaciones con el prototipo. Los autores mencionan que también cubren el servicio de confidencialidad en su prototipo, pero no describen el algoritmo que usaron para ello.

- En [51] se propone un prototipo de WBAN que recopila datos de la frecuencia cardíaca a través de una transmisión ECG. Se emplea el algoritmo PRESENT para el cifrado de datos, reportando un nivel de seguridad de 80 bits. Se utiliza el mote TelosB como nodo sensor y una PC como estación base. Las métricas de interés evaluadas son el consumo de energía y el ciclo de trabajo. En los procesos de cifrado y descifrado de datos. El nivel de seguridad usado de 80-bits, actualmente obsoleto, y se garantiza únicamente la confidencialidad de los datos.

- En [52] se propone un prototipo que cubre dos servicios de seguridad: confidencialidad y control de acceso. Se utilizó AES como algoritmo para el cifrado de datos con un nivel de seguridad de 128 bits. Para el control de acceso se utilizó ABE con políticas de Control de Acceso Basado en Etiquetas (LBAC, por sus siglas en inglés). Sin especificar cuál, se utiliza un wearable como nodo sensor y teléfono Google Nexus 4 como estación base, siendo éste un prototipo para dispositivos basados en Android. Las métricas de interés en la experimentación fueron el tiempo de ejecución y consumo de energía en los procesos de inicialización, cifrado y descifrado de los datos. Para medir el consumo de energía se utilizó una aplicación dedicada a separar los procesos que el teléfono inteligente realiza. Esto es para tener un mejor control de las variables

al momento de medir la energía.

- En [70] se propone la construcción de un prototipo WBAN sin especificar los servicios de seguridad que se deben garantizar. El prototipo usa un procesador de señal digital (DSP, por sus siglas en inglés) como nodo sensor. En el trabajo se menciona el uso de un conjunto de primitivas criptográficas para el módulo de seguridad. Sin embargo, no se hace mención de cuáles son esas primitivas. Además, se reporta un módulo de administración, un módulo de servicio de datos y un módulo de transmisión de datos. En el trabajo citado, se midió el tamaño de la carga útil de los paquetes y su impacto asociado a la distancia de transmisión y reintentos de transmisión.

En la Tabla 3.3 se presenta un resumen de las características más relevantes de los prototipos WBAN previamente reportados en la literatura, incluyendo el número de sensores utilizados en la capa 1 del modelo de WBAN. La mayoría de los trabajos revisados reportan haber construido un prototipo de WBAN, lo cual incluye operar en la capa 1 garantizando al menos un servicio de seguridad. Solamente dos trabajos desplegaron la capa 2 del modelo WBAN al enviar la información de la estación base a un servidor o aplicación. El número máximo de sensores que se utilizaron en la capa 1 fue uno solo, cada trabajo con diferente sensor obteniendo datos, en la mayoría, del ritmo cardíaco.

Tabla 3.3: Trabajos relacionados sobre prototipos WBAN, tanto modelos o prototipos reales, construidos y evaluados físicamente o en simulación.

Trabajo	Tipo de enfoque	# sensores en capa 1	Modelo WBAN		
			Capa 1	Capa 2	Capa 3
[52], 2014	Prototipo	1	✓	-	-
[51], 2017	Prototipo	1	✓	-	-
[70], 2017	Prototipo	1	✓	-	-
[6], 2017	Prototipo	1	✓	✓	-
[1], 2018	Modelo	-	-	-	-
[7], 2019	Modelo	-	✓	-	-
[53], 2019	Simulación	1	✓	-	-
[19], 2019	Prototipo	1	✓	-	-
[25], 2019	Prototipo	1	✓	✓	-
[31], 2019	Modelo	-	✓	-	-
Esta tesis, 2020	**Prototipo**	**3**	✓	✓	✓

La Tabla 3.4 extiende a la Tabla 3.3, para proporcionar detalles de los prototipos implementados. En la tabla se muestran los detalles del sensor utilizado, el dispositivo usado como estación base y las métricas que se usaron para evaluar el prototipo. Como se puede observar, los prototipos reportados se limitan al uso de un solo sensor y se enfocan solo en el despliegue de la capa 1 del modelo de WBAN.

Tabla 3.4: Detalles de los prototipos WBAN reportados en la literatura.

Trabajo	Nodos sensores	Estación base	Sistema	Métricas			Método para consumo de energía
				Tiempo	Memoria	Energía	
[52], 2014	Wearable	Smartphone	-	✓	-	✓	Aplicación que usa un modelo de energía DevScope
[51], 2017	TelosB mote	-	-	-	-	✓	Estimación de consumo de energía (potencia-mW)
[70], 2017	DSP	-	-	✓	-	-	-
[6], 2017	Arduino 101	PC	-	✓	-	✓	No reportado
[7], 2019	Intel PXA270	-	-	✓	-	-	-
[53], 2019	AVISPA	-	-	✓	-	-	-
[19], 2019	MICA2DOT mote	-	-	✓	-	✓	No reportado
[25], 2019	Smartwatch K18	Java Card	-	-	-	-	-
[31], 2019	MICA2	-	-	✓	-	✓	Estimación de consumo de energía mediante la complejidad computacional
Esta tesis, 2020	**Galaxy Watch LaunchPad CC3220SF Raspberry Pi 3**	**Smartphone**	**Web**	✓	✓	✓	**Estimación de consumo de energia (Amperio-hora)**

3.3 Comparación con el estado del arte

Aunque los trabajos relacionados han desarrollado WBAN, la mayoría de ellos lo hace con algoritmos y arquitecturas de hardware diferentes a las utilizadas en este trabajo de tesis. Además en los trabajos relacionados no se implementa una WBAN en todas sus capas ni se garantizan todos los servicios de seguridad requeridos en una WBAN. Por esta razón, no es posible realizar una comparación directa entre los trabajos relacionados y esta tesis, la comparación no sería justa dado que los dispositivos y algoritmos utilizados son diferentes.

3.4 Discusión

En la literatura se han propuesto algunos prototipos de WBAN segura, pero se han limitado a algunos servicios de seguridad y a propuestas de modelos evaluados solo en simulación. El nivel de seguridad que han usado los trabajos relacionados de WBANs actualmente se considera obsoleto, por lo que esas propuestas podrían considerarse vulnerables. Para el servicio de integridad y de autenticación, se han usado primitivas como las funciones hash de la familia SHA. Sin embargo, en la literatura y en otros contextos de redes inalámbricas se han propuestos funciones hash ligeras como los basados en la familia **SPONGENT**. En esta tesis proponemos usar este tipo de funciones con el fin de obtener realizaciones ligeras sin pérdida de eficacia en la provisión del servicio de integridad. Usando esta primitiva como base, proponemos usar **HMAC** como algoritmo para proveer el servicio de autenticación, el cual usa como base un algoritmo hash que es este caso es ligero. Los trabajos que garantizan el control de acceso, coinciden en utilizar **ABE** para garantiza control de acceso de grano fino çriptográfico"basado en el uso de políticas de control de acceso. En esta tesis retomamos esta idea pero usamos construcciones más eficientes que las reportadas en la literatura, principalmente las que usan emparejamientos bilineales asimétricos que permiten obtener niveles de seguridad igual o mayor a 128-bits. Se utiliza **DET-ABE** como algoritmo para el control de acceso con un cifrador simétrico ligero, el mismo que se utiliza para garantizar la confidencialidad.

En esta tesis proponemos la construcción de un prototipo WBAN considerando las tres capas del modelo de WBAN y garantizando servicios de seguridad en cada capa, formando una WBAN segura. Al hablar de capas en una WBAN no se refiere al modelo OSI, sino a la estructura de la WBAN. La capa 1 se construye utilizando tres nodos sensores que monitorean el ritmo cardíaco, saturación de oxígeno en la sangre y la temperatura corporal. Los nodos sensores se conectan a una estación base, un teléfono inteligente, a través de Bluetooth. La capa 2 consiste en la comunicación de la estación base a un servidor de almacenamiento y la capa 3 se construyó como un sistema web que permite el acceso a los datos recabados de los nodos sensores por parte de entidades autorizadas.

Los algoritmos criptográficos utilizados para garantizar los servicios de seguridad se implementan en los dispositivos utilizados en la WBAN. Para contrastar los resultado obtenidos en esta tesis, se obtuvieron las mismas métricas que han reportado los trabajos revisados, *tiempo de ejecución*, *memoria consumida* y *consumo de energía*.

El prototipo WBAN construido y evaluado en esta tesis contempla los cuatro servicios identificados como esenciales en una WBAN con un nivel de seguridad mínimo de 128 bits. En cada una de las capas se midió el impacto generado por los algoritmos criptográficos para determinar cuál es el costo para garantizar los servicios de seguridad. Se utilizaron tres nodos sensores encargados de monitorear tres signos vitales diferentes. Además, se realizaron evaluaciones de cada servicio de seguridad para determinar el costo e impacto de cada uno de ellos.

En el capítulo siguiente se define y detalla la metodología de diseño de una WBAN segura. Primeramente, se define el modelo de WBAN segura basado en abstracciones para garantizar confidencialidad, integridad, autenticación y control de acceso. Luego, con base en lo revisado y discutido en la literatura, se presentan las especificaciones algorítmicas de cada servicio de seguridad en la WBAN donde se incluyen los algoritmos criptográficos utilizados para garantizar cada servicio. Después, se presenta el diseño de un prototipo WBAN segura con base en el modelo propuesto usando tres nodos sensores. Finalmente, se presentan los detalles del despliegue del prototipo resaltando las fases, algoritmos criptográficos y dispositivos móviles que lo componen.

4

Diseño de una red inalámbrica de área corporal segura

En este capítulo se describe el flujo de diseño para construir una WBAN segura. El capítulo se encuentra organizado de la siguiente forma: con base en el capítulo anterior y para cubrir los servicios de seguridad requeridos en una WBAN se describe el esquema de seguridad propuesto en esta tesis para proteger los datos desde que se producen en los nodos sensores y hasta que se acceden por usuarios autorizados. El esquema propuesto usa algoritmos de cifrado, generación de hash, generación de MACs y cifrado basado en atributos en las capas correspondiente en el modelo WBAN. Una vez definido el esquema de seguridad, se describen los algoritmos seleccionados para proveer cada uno de los servicios de seguridad y evaluar el desempeño del prototipo de WBAN y del esquema de seguridad propuestos.

4.1 Esquema de seguridad para WBAN

Para determinar el modelo de una WBAN segura, primero se definió un esquema de seguridad basado en abstracciones asociadas a los servicios de seguridad requeridos en una WBAN, que se han discutido en el Capítulo 3. Cada servicio de seguridad se garantiza a través de un mecanismo de defensa criptográfico, es decir, un algoritmo criptográfico.

Las abstracciones están definidas de acuerdo con la notación mostrada en la Tabla 4.1. Para garantizar la confidencialidad se requiere de un algoritmo criptográfico encargado de cifrar datos utilizando una llave secreta compartida entre las entidades involucradas. Se refirió a este proceso con la notación E. El servicio de integridad se obtiene mediante un algoritmo criptográfico de hash, denotado como H. La autenticación se garantiza a través de un algoritmo que obtiene códigos MAC de los datos de entrada, denotado como MAC. Finalmente, el control de acceso a datos se obtiene mediante el cifrado de los datos usando políticas de control de acceso, denotado como ABE.

La única restricción es que los algoritmos específicos usados para la realización de las abstracciones garanticen el servicio de seguridad que se requiere y definan las mismas operaciones. Por ejemplo, para desplegar E, es necesario que el algoritmo sea simétrico, esto es que se requiera de una llave simétrica usada en las dos operaciones definidas por E, cifrar y descifrar.

En la Tabla 4.1 se muestran, a manera de resumen, las abstracciones utilizadas para garantizar servicios de seguridad en el esquema de seguridad de WBAN. Cada abstracción define un conjunto de operaciones, por ejemplo cifrar o descifrar datos D mediante una llave simétrica k, obtener códigos MAC de datos utilizando la misma llave simétrica o cifrar y descifrar datos utilizando una política de control de acceso P.

Tabla 4.1: Esquema de seguridad de WBAN basado en abstracciones.

Abstracción	Descripción	Operación	Servicio de seguridad
E	Cifrador simétrico por bloques	ENC(k, D) DEC(k, C_D)	Confidencialidad
H	Hash de datos	$GEN(D)$	Integridad
MAC	Código de autenticación de mensajes	GEN(k, D) VER(σ, k, D)	Autenticación
ABE	Cifrador basado en atributos	ENC(P, k) DEC(SK$_U, C_P$)	Control de acceso

En E.ENC, k es una llave simétrica y D son datos a cifrar. En E.DEC, se utiliza la misma llave simétrica que E.ENC, y C_D que es el texto cifrado, es decir, es el resultado de la operación E.ENC. H.GEN(D) produce el hash de los datos D. MAC.GEN(k, D) utiliza una llave simétrica k y datos D para generar el código de autenticación de D. Para la verificación, MAC.VER(σ, k, D) utiliza σ que es el resultado de MAC.GEN(k, D) y la misma llave simétrica y datos. Finalmente, ABE.ENC(P, K_a) utiliza P que es una política de control de acceso y llave simétrica k_a. En ABE.DEC(SK$_U, C_P$), SK$_U$ es una llave de acceso generada con base en los atributos de un usuario U_j y C_P es el texto cifrado resultante de ABE.ENC.

4.2 Modelo de WBAN segura

Con el esquema de seguridad propuesto, se puede definir el modelo de una WBAN segura basado en tres capas. El esquema permite garantizar servicios de seguridad en cada una de las capas de una WBAN. Con base en las abstracciones definidas en el esquema de seguridad, para el modelo de WBAN se utilizan las abstracciones para determinar en cuál capa del modelo de WBAN segura se implementan las operaciones.

Tabla 4.2: Esquema de seguridad para el modelo de WBAN segura.

Operación	Servicio de seguridad	Capa de WBAN
$C_D = E.\text{ENC}(k_i, D)$	Confidencialidad	1 y 3
$D = E.\text{DEC}(k_i, C_D)$	Confidencialidad	1 y 3
$h_i = H.GEN(C_D)$	Integridad	1 y 2
$\sigma = \text{MAC.GEN}(k_i, h_i)$	Autenticación	Todas
$\{0,1\} = \text{MAC.VER}(\sigma, k_i, h_i)$	Autenticación	2 y 3
$C_P = \text{ABE.ENC}(P, k_i)$	Control de acceso	2 y 3
$k_i = \text{ABE.DEC}(\text{SK}_U, C_P)$	Control de acceso	2 y 3

En la Tabla 4.2 se observa las notaciones definidas para el modelo de WBAN segura. El esquema de seguridad de la Tabla 4.1 es la base del modelo de WBAN propuesto. Se utilizan algunas notaciones que permiten resumir los procesos que se realizan en las capas de una WBAN. En la Tabla 4.2, k_i es una llave secreta compartida, SK_U es una llave secreta de acceso asignada a un usuario U_j, P es una política de control de acceso y D son los datos de los sensores.

4.2.1 Pre-requisitos del modelo de WBAN segura

Para que este modelo pueda funcionar correctamente, es necesario tener en cuenta algunas consideraciones. En la capa 1 actúan tanto los sensores (S_i) como la BS. Cada S_i comparte una k_i con la BS para poder cifrar o descifrar los datos que se transfieren. k_i es asignada a cada dispositivo cuando se encuentran fuera de línea. S_i se conectan a través de Bluetooth a la BS para establecer la comunicación y transferencia de datos.

En la capa 2, BS se comunica con el sistema, alojado en la capa 3, a través de Internet. La política de control de acceso P que se aplica sobre k_i cuando se cifra en la BS está a cargo de una entidad de confianza (TA), mediante el algoritmo DET-ABE, la cual se obtiene durante la fase de configuración cuando todos los dispositivos están fuera de línea. La política de control de acceso P se define tomando en cuenta quiénes son los usuarios que tendrán acceso a los datos, es decir, se

asigna una serie de atributos A unidos con una conjunción lógica para permitir o excluir el acceso a los datos de los sensores a entidades específicas.

En la capa 3 actúa el sistema y la TA. Esta última es la responsable, también, de generar las llaves de acceso SK_U para usuarios U_j con base en los atributos que posee, mismos que les permitirán o negarán el acceso a los datos cifrados con políticas de acceso.

Durante el funcionamiento de la WBAN segura, se utilizan otras operaciones que no se mencionaron en la Tabla 4.2, debido a que son operaciones independientes de los servicios de seguridad. Estas operaciones se explican en la Tabla 4.3.

Tabla 4.3: Operaciones independientes utilizadas en el esquema de seguridad de una WBAN.

Operación	Descripción
loadKey()	Carga en memoria la llave de cifrado simétrica k_i compartida.
getSigns()	Comienza con el monitoreo de S_i y obtiene los signos vitales D.
send(D)	Envío de los datos D.
generatePolicies()	Generación de políticas de control de acceso.
getPolicies()	Obtención de la política de control acceso.
searchKey(ID_i)	Búsqueda de llave simétrica asociada al ID_i de S_i.
storage(C_D, C_P)	Almacenamiento de C_D y C_P.
requestKey(ID_U)	Solicitud de generación de llave de acceso.
assignAttributes(ID_U)	Asigna los atributos asociados al ID_U de U_j.
createKey(A_j)	Generación de llave secreta de U_j con base en sus atributos.
save(SK_U)	Almacenamiento de la llave secreta de U_j.

4.2.2 Capa 1: recolección de datos

En la capa 1 del modelo WBAN segura se requiere garantizar los principales servicios de seguridad: *confidencialidad*, *integridad*, *autenticación* y *control de acceso*. La triada CIA se aplica en los nodos sensores S_i, después de recolectar los datos de los signos vitales D, éstos se cifran y autentican para

su posterior envío a la BS.

La BS obtiene las políticas de acceso que se aplicarán a los datos sensados, durante la fase de configuración cuando está fuera de línea. Cuando la BS recibe los datos, se verifica que éstos son auténticos, mediante la operación MAC.GEN. El control de acceso a los datos se realiza cifrando mediante ABE.ENC la llave simétrica compartida con S_i. Esto garantiza que solo usuarios U_j que cumplan con las políticas aplicadas podrán acceder a la llave de cifrado y por tanto, descifrar los datos. El acceso a k_i se realiza directamente en código, no es posible aislar la llave y obtenerla por un tercero o por el mismo usuario U_j para su posterior distribución. La interacción entre el nodo sensor S_i y la BS para la recolección de datos biomédicos cifrados y autenticados se muestran en la Figura 4.1.

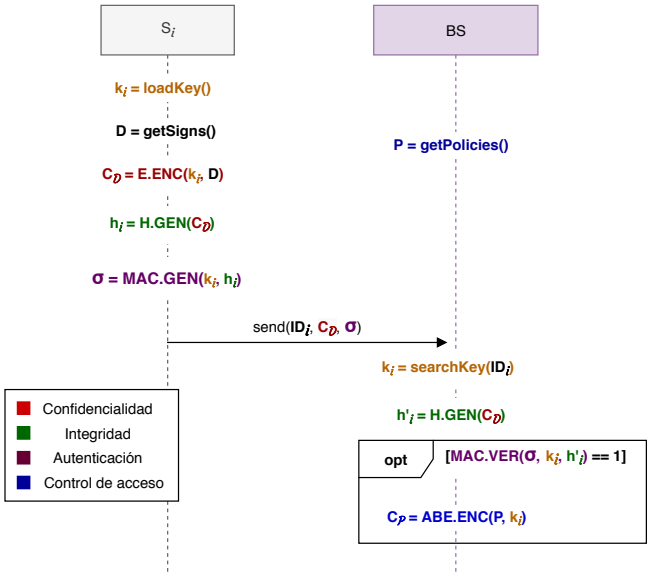

Figura 4.1: Modelo de WBAN segura (capa 1).

El motivo de generar la MAC de los datos cifrados es para garantizar la integridad de los mismos, esto permite recibir solamente datos auténticos en caso de sufrir un ataque de falsificación. En el caso que se aplique la generación de MAC a los datos en claro, la integridad está directamente en los datos en claro, al cifrarlos, los nuevos datos pierden la integridad y son vulnerables a los ataques

de falsificación.

4.2.3 Capa 2: comunicación

La capa 2 del modelo de WBAN segura abarca la comunicación y transferencia de datos desde la BS hasta el almacenamiento de los datos. La BS realiza el envío de C_D y C_P, previamente autenticados, al sistema. En el sistema, se verifican los datos cifrados recibidos mediante la operación MAC.VER; si son auténticos, se procede a almacenarlos en el repositorio de datos. Esta interacción se puede observar en la Figura 4.2.

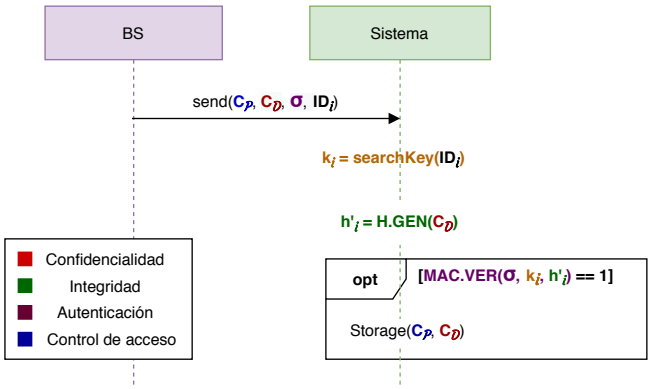

Figura 4.2: Modelo de WBAN segura (capa 2).

Esta capa tiene el rol de conectar la capa de recolección de datos con la capa de aplicación, por lo cual se realizan procedimientos particulares que le permiten transportar los datos desde el origen hasta el destino.

4.2.4 Capa 3: aplicación

La capa 3 del modelo de WBAN segura consta de la generación de llave de acceso hasta la obtención de los datos por parte de los usuarios desde el repositorio. Particularmente, para el almacenamiento de los datos, el sistema primero debe validar los datos recibidos y verificar que la fuente de datos es confiable.

Para que un usuario U_j pueda obtener los datos, éste realiza la petición de la llave de acceso a la autoridad de confianza TA. La TA le asigna los atributos, previamente definidos, al U_j que realiza la petición y genera k_{U_j}. Con k_{U_j}, un U_s puede consultar los datos en el sistema. Selecciona los datos que desea obtener y proporciona su k_{U_j}, si los atributos cumplen con P aplicado sobre los datos cifrado, U_j podrá visualizar dichos datos. En la Figura 4.3 se puede observar la interacción de esta segunda parte.

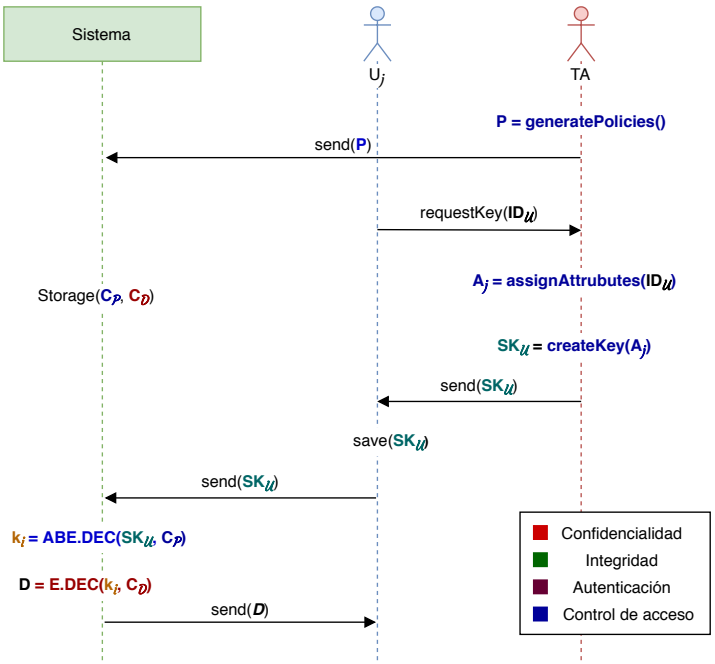

Figura 4.3: Modelo de capa 3 de una WBAN segura.

La TA toma un rol importante en esta capa, dado que es la que se encarga de generar las llaves pública PK y privada MK del sistema, además de generar llaves de sesiones para los usuarios que necesiten acceder a los datos.

El proceso de acceso a los datos por los usuarios se realiza posteriormente a la generación de llaves de sesión del usuario que necesita obtener los datos almacenados. El único requisito es la llave, dado que con los atributos asignados debe satisfacer la política de acceso con la que se cifró la llave simétrica para descifrar los datos.

4.3 Algoritmos de criptografía para servicios de seguridad

Los algoritmos de criptografía para garantizar los servicios de seguridad requeridos en WBANs, se discutieron en el Capítulo 3. Existe una rama de la criptografía, como se mencionó en la Sección 2.2, que se encarga de estudiar algoritmos que son conscientes de las limitaciones computacionales del entorno en el que se implementan, con base en ello y en las recomendaciones de la literatura, se realizó la selección de los algoritmos criptográficos ligeros para utilizarse en el despliegue del modelo de WBAN segura discutido en la sección anterior. En la Tabla 4.4 se presenta un resumen y justificación de la selección de algoritmos criptográficos ligeros en este proyecto de tesis.

Tabla 4.4: Algoritmos de criptografía ligera seleccionados.

Algoritmo	Servicio de seguridad	Justificación de selección
LEA	Confidencialidad	Es un estándar ISO en criptografía ligera.
PRESENT	Confidencialidad	Es un estándar ISO en criptografía ligera.
SPONGENT	Integridad	Función hash ligera basada en permutaciones de PRESENT.
QUARK	Integridad	Función hash ligera basada en los cifradores ligeros Gain y KATAN.
HMAC	Autenticación	Es simple y permite utilizar una función hash ligera.
LightMAC	Autenticación	Es un estándar ISO en criptografía ligera.
ABE	Control de acceso	Garantiza el control de acceso de grano fino.

4.3.1 Algoritmos ligeros para confidencialidad

Los algoritmos seleccionados para el servicio de confidencialidad, todos, son cifradores por bloques. Esto permite procesar paquetes de datos que se generan en los nodos sensores y se cifran antes de ser enviados a la BS. Los algoritmos difieren en cuanto al tamaño de bloque que procesan y nivel de seguridad. Cada uno de estos algoritmos realizan procedimientos diferentes, conservando la ligereza en sus operaciones.

LEA

LEA es un cifrador de bloque de 128 bits que opera en 4 ramas de 32 bits cada una. Las únicas operaciones utilizadas son la adición modular de 32 bits ($\boxplus$), OR exclusivo ($\oplus$) y rotación (ROL_i: rotación de $i-$bits a la izquierda, ROR_i: rotación de $i-$bits a la derecha) siguiendo una estructura **ARX** (Adición, Rotación y operación XOR). Las funciones se muestran en la Figura 4.4, donde el bloque de datos se divide en 4 ramas expresados como X_i, el resultado de la generación de llaves es RK_i el cual contiene un valor para cada ronda que se opera con X_i. La llave se agrega en ambas rutas de datos que van en cada adición modular.

El esquema de la llave también sigue el paradigma ARX: las constantes se agregan en el módulo 2^{32} al estado de llave y las diferentes palabras se rotan.

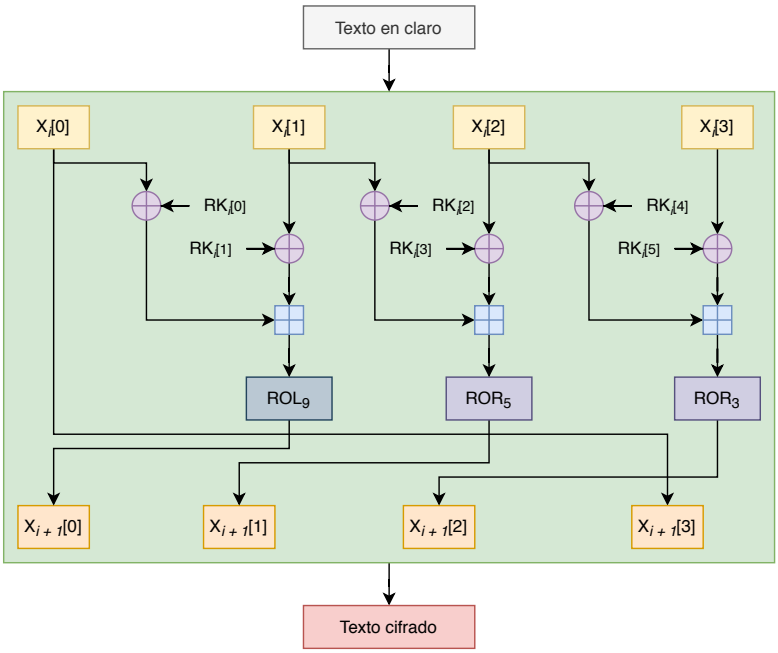

Figura 4.4: Diagrama a bloques de LEA.

La especificación algorítmica está divida en dos algoritmos. El Algoritmo 1 es la generación de llaves, recibe de entrada un vector mk, dividido en 4 ramas cuando su tamaño es de 128 bits como se observa en el Algoritmo 1. LEA proporciona una constante δ para la generación de llaves, que

está constituida por la expresión hexadecimal de $\sqrt{766995}$, donde 76, 69 y 95 son códigos ASCII de L, E y A.

Algorithm 1 Generación de rondas de llave RK de 128 bits para LEA.

Entrada: *mk*: vector de bytes; puede ser vacío, δ: constante para generación de llave

Salida: RK: matriz con las rondas de llave generadas

$T[i] \leftarrow mk[i]$ for $0 < i < 4$
for $i \leftarrow 0$ until 24 **do**
    $T[0] \leftarrow ROL_1(T[0] + ROL_i(\delta[i \bmod 4]))$
    $T[1] \leftarrow ROL_3(T[1] + ROL_{i+1}(\delta[i \bmod 4]))$
    $T[2] \leftarrow ROL_6(T[2] + ROL_{i+2}(\delta[i \bmod 4]))$
    $T[3] \leftarrow ROL_{11}(T[3] + ROL_{i+3}(\delta[i \bmod 4]))$
    $RK_i \leftarrow (T[0], T[1], T[2], T[1], T[3], T[1])$
end for
return RK

En el Algoritmo 2 se observa la generación de llaves de 6 ramas cuando su tamaño es de 192 bits.

Algorithm 2 Generación de rondas de llave RK de 192 bits para LEA.

Entrada: *mk*: vector de bytes; puede ser vacío, δ: constante para generación de llave

Salida: RK: matriz con las rondas de llave generadas

$T[i] \leftarrow mk[i]$ for $0 < i < 6$
for $i \leftarrow 0$ until 28 **do**
    $T[0] \leftarrow ROL_1(T[0] + ROL_i(\delta[i \bmod 6]))$
    $T[1] \leftarrow ROL_3(T[1] + ROL_{i+1}(\delta[i \bmod 6]))$
    $T[2] \leftarrow ROL_6(T[2] + ROL_{i+2}(\delta[i \bmod 6]))$
    $T[3] \leftarrow ROL_{11}(T[3] + ROL_{i+3}(\delta[i \bmod 6]))$
    $T[4] \leftarrow ROL_{13}(T[4] + ROL_{i+4}(\delta[i \bmod 6]))$
    $T[5] \leftarrow ROL_{17}(T[5] + ROL_{i+5}(\delta[i \bmod 6]))$
    $RK_i \leftarrow (T[0], T[1], T[2], T[3], T[4], T[5])$
end for
return RK

Finalmente, la generación de llaves de 8 ramas en caso de tener un tamaño de 256 bits se puede observar en el Algoritmo 3.

Algorithm 3 Generación de rondas de llave RK de 256 bits para LEA.

Entrada: *mk*: vector de bytes; puede ser vacío, δ: constante para generación de llave

Salida: RK: matriz con las rondas de llave generadas

$T[i] \leftarrow mk[i]$ for $0 < i < 8$
for $i \leftarrow 0$ until 32 **do**
    $T[6i \bmod 8] \leftarrow ROL_1(T[6i \bmod 8] + ROL_i(\delta[i \bmod 8]))$
    $T[6i+1 \bmod 8] \leftarrow ROL_3(T[6i+1 \bmod 8] + ROL_{i+1}(\delta[i \bmod 8]))$
    $T[6i+2 \bmod 8] \leftarrow ROL_6(T[6i+2 \bmod 8] + ROL_{i+2}(\delta[i \bmod 8]))$
    $T[6i+3 \bmod 8] \leftarrow ROL_{11}(T[6i+3 \bmod 8] + ROL_{i+3}(\delta[i \bmod 8]))$
    $T[6i+4 \bmod 8] \leftarrow ROL_{13}(T[6i+4 \bmod 8] + ROL_{i+4}(\delta[i \bmod 8]))$
    $T[6i+5 \bmod 8] \leftarrow ROL_{17}(T[6i+5 \bmod 8] + ROL_{i+5}(\delta[i \bmod 8]))$
    $RK_i \leftarrow (T[6i \bmod 8], T[6i+1 \bmod 8], T[6i+2 \bmod 8], T[6i+3 \bmod 8], T[6i+4 \bmod 8], T[6i+5 \bmod 8])$
end for
return RK

Para el proceso de cifrado se utiliza RK generado y los datos a cifrar separado en bloques de 128 bits como se especifica en el Algoritmo 4. El descifrado de datos es el proceso inverso.

Algorithm 4 Cifrado de bloque de datos de 128 bits usando LEA.

Entrada: *X*: bloque de datos de 128 bits, *RK*: rondas de llave, *r*: número de rondas

Salida: X: bloque de datos de 128 bits cifrado

for $i \leftarrow 0$ until $r-1$ **do**
    $X_{i+1}[0] \leftarrow ROL_9((X_i[0] \oplus RK_i[0]) + (X_i[1] \oplus RK_i[1]))$
    $X_{i+1}[1] \leftarrow ROL_5((X_i[1] \oplus RK_i[2]) + (X_i[2] \oplus RK_i[3]))$
    $X_{i+1}[2] \leftarrow ROL_3((X_i[2] \oplus RK_i[4]) + (X_i[3] \oplus RK_i[5]))$
    $X_{i+1}[3] \leftarrow X_i[0]$
end for
return X

PRESENT

Este cifrador es una red de sustitución y permutación (SPN, por sus siglas en inglés). PRESENT está orientado a bits y es bastante simple. Sin embargo, dado que las permutaciones orientadas a bits no son compatibles con el software, el objetivo de PRESENT es claramente una implementación de hardware. Su S-box fue seleccionada por sus buenas propiedades criptográficas, así como por su pequeña huella de hardware.

El tamaño del bloque es de 64 bits y el tamaño de la llave puede ser 80 o 128 bits. La capa no lineal se basa en un único S-box de 4 bits que se diseñó teniendo en cuenta las optimizaciones de hardware. PRESENT está destinado a ser utilizado en situaciones donde se desea un bajo consumo de energía y una alta eficiencia de chip. El diagrama que describe las fases que se utilizan en el procedimiento se pueden observar en la Figura 4.5.

- **addRoundKey.** Dada una llave de ronda $K_i = k^i_{63} \dots k^i_0$ para $1 < i < 32$ y el estado actual, es decir, los datos que se procesan $b_{63} \dots b_0$, la operación addRoundKey consiste para $0 < j < 63$

$$b_j \rightarrow b_j \oplus k^i_j \tag{4.1}$$

- **sBoxLayer**. La S-box utilizada es una S-box $S : \mathbb{F}^4_2 \rightarrow \mathbb{F}^4_2$ de 4 a 4 bits. La acción de esta caja en notación hexadecimal está dada por la siguiente tabla.

Tabla 4.5: Valores de S-box utilizada en PRESENT.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Para esta fase, el estado actual es considerado como 16 palabras de 4 bits $w_{15} \dots w_0$ donde $w_i = b_{4*i+3}||b_{4*i+2}||b_{4+i+1}||b_{4*i}$ para $0 < i < 15$ y la salida $S[w_i]$ proporciona los valores de estado actualizados de una manera obvia.

- **pLayer**. El bit de permutación utilizado es dado por la siguiente tabla. Bit i del estado es movido a la posición del bit $P(i)$.

Tabla 4.6: Valores del bit de permutación utilizado en PRESENT.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

- **Registro de llave y actualización.** El registro de llave se gira 61 posiciones de bit a la izquierda, los cuatro bits más a la izquierda se pasan a través de la S-box actual, y el valor del contador de ronda i se opera mediante un OR-exclusivo con los bits de K con el bit menos significativo de i a la derecha.

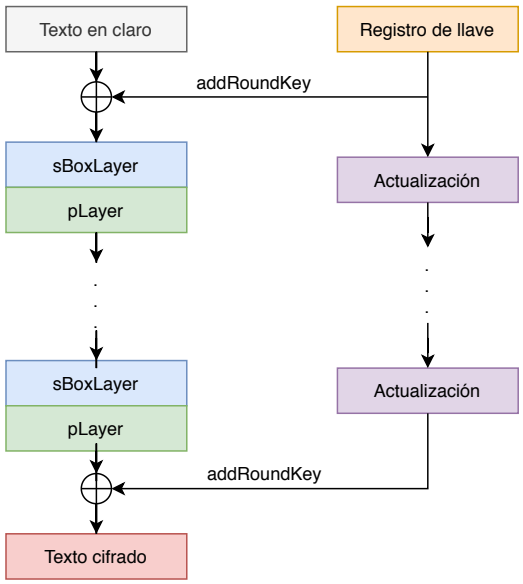

Figura 4.5: Diagrama a bloques de PRESENT.

Siguiendo con el diagrama de PRESENT observado en la Figura 4.5, en el Algoritmo 5 se presenta la secuencia que sigue cada bloque en las 31 iteraciones hasta cifrar el bloque.

Algorithm 5 Cifrado de bloques de datos de 64 bits usando PRESENT.

Entrada: X: bloque de datos de 64 bits, *mk*: vector de bytes; puede ser vacío, r: número de rondas

Salida: X: bloque de datos de 64 bits cifrado

```
1: K_r ← generateRoundKeys(mk)
2: for i ← 1 until r do
3:     addRoundKeys(X, K_i)
4:     sBoxLayer(X)
5:     pLayer(X)
6: end for
7: addRoundKeys(X, K_r)
8: return X
```

4.3.2 Algoritmos ligeros para integridad

Los algoritmos seleccionados forman parte de la familia de funciones hash que utilizan la estructura de esponja. Cada uno de los algoritmos realiza procedimientos diferentes, con la misma estructura.

Construcción de esponja

En el contexto de la criptografía, la construcción de esponja es un modo de operación, basado en una permutación (o transformación) de longitud fija y en una regla de relleno, que construye una función de mapeo de entrada de longitud variable a salida de longitud variable. Tal función se llama función de esponja. Toma como entrada un elemento de $\mathbb{Z}_2^*$, es decir, una cadena binaria de cualquier longitud, y devuelve una cadena binaria con cualquier longitud solicitada, es decir, un elemento de $\mathbb{Z}_2^n$ con n un valor proporcionado por el usuario.

La construcción de esponja es una construcción iterativa simple para construir una función F con entrada de longitud variable y longitud de salida arbitraria basada en una permutación (o transformación) de longitud fija f que opera en un número fijo b de bits. Esta construcción opera en un estado $b = r + c$ bits. El valor r se llama bitrate y el valor c la capacidad. Una función de esponja se construye a partir de tres componentes:

1. Un estado b, que contiene bits.

2. Una función $f : \{0,1\}^{|bits|} \rightarrow \{0,1\}^{|bits|}$ que transforma la memoria de estado (a menudo es una permutación pseudoaleatoria de los valores de estado $2^{|bits|}$).

3. Una función de relleno llamada Pad.

La función Pad agrega suficientes bits a la cadena de entrada para que la longitud de la entrada sea un múltiplo entero de r. La entrada se puede dividir en bloques r bits.La estructura de la construcción de esponja se observa en la Figura 4.6.

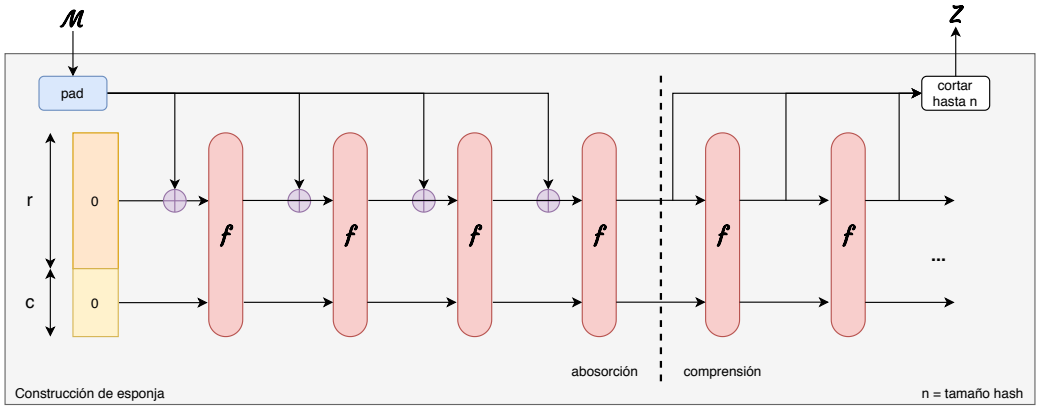

Figura 4.6: Estructura de la construcción de esponja.

La construcción de esponja procede en dos fases:

- En la fase de absorción, los bloques de entrada de r bits son XOR en los primeros r bits del estado, intercalados con aplicaciones de la función f. Cuando se procesan todos los bloques de entrada, la construcción de la esponja cambia a la fase de compresión.

- En la fase de compresión, los primeros r bits del estado se devuelven como bloques de salida, intercalados con aplicaciones de la función f. El número de bloques de salida es elegido a voluntad por el usuario.

Los últimos c bits del estado nunca se ven directamente afectados por los bloques de entrada y nunca salen durante la fase de compresión.

SPONGENT

SPONGENT se basa en una construcción de esponja, es decir, un diseño iterativo simple que toma una entrada de longitud variable y puede producir una salida de una longitud arbitraria basada en una permutación π_b que opera en un estado de un número fijo b de bits. El tamaño del estado interno $b = r + c \geq n$ se llama ancho, donde r es bitrate y c la capacidad. La permutación es una versión modificada de PRESENT. El número de rondas de la permutación de tipo PRESENT varía de 45 para SPONGENT-88 a 140 para SPONGENT-256.

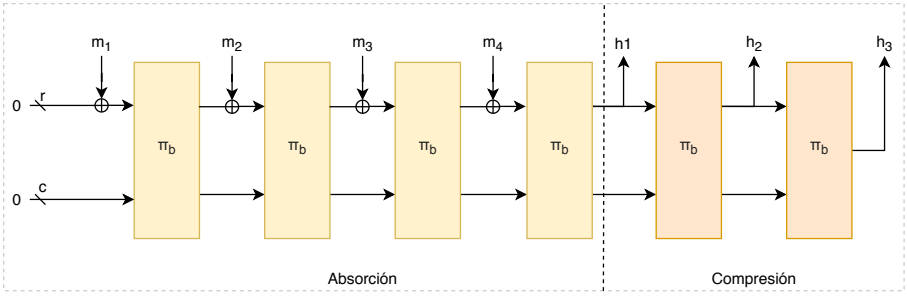

Figura 4.7: Diagrama del proceso de SPONGENT.

En SPONGENT, el b-bit 0 se toma como el valor inicial antes de la fase de absorción. El mensaje se rellena primero con un solo 1 bit seguido de un número necesario de 0 bits hasta un múltiplo de r bits. Luego se corta en bloques de mensajes de r bits que se graban en los primeros r bits del estado, intercalados con aplicaciones de la permutación π_b. Una vez que todos los bloques de mensajes han sido absorbidos, los primeros r bits del estado se devuelven como salida, intercalados con aplicaciones de la permutación π_b, hasta que se devuelven n bits. Este procedimiento se puede observar en la Figura 4.7.

QUARK

QUARK es una función hash ligera, basada en la construcción de esponja e inspirada en los cifrados ligeros Grain y KATAN [10], la familia de funciones hash QUARK se compone de las

tres instancias U-QUARK, D-QUARK y S-QUARK. QUARK puede ser usado en mensajes de autenticación, cifrado de flujo o cifrado autenticado.

QUARK utiliza la construcción de esponja mostrada en la Figura 4.6. Una instancia de QUARK es parametrizada por un bitrate r (o tamaño de bloque), una capacidad c y un tamaño de salida n. La longitud $b = r + c$ de una construcción de esponja es el tamaño de su estado interno. Este estado se denota como $s = (s_0, \cdots, s_{b-1})$ donde s_0 se refiere al primer bit del estado.

Dado un estado inicial de b bits predefinido (especificado por cada instancia de QUARK, en la Tabla 4.7 se pueden observar los parámetros en cada instancia), el procesamiento de un mensaje m se realiza en tres paso:

1. **Inicialización:** el mensaje se rellena agregando un bit '1' seguido del número mínimo de bits '0' para alcanzar una longitud que sea múltiplo de r.

2. **Fase de absorción:** los bloques de mensajes de r bits son operados mediante XOR con los últimos r bits del estado (es decir, $s_{b-r}, \ldots, s_{b-2}, s_{b-1}$), intercalados con aplicaciones de la permutación P. La fase de absorción comienza con un XOR entre el primer bloque y el estado, y termina con una llamada a la permutación P.

3. **Fase de comprensión:** los últimos r bits del estado se devuelven como salida, intercalados con aplicaciones de la permutación P, hasta que se devuelven n bits. La fase de compresión comienza con la extracción de r bits, y también termina con la extracción de r bits.

Tabla 4.7: Parámetros de las instancias de QUARK.

Instancia	Bitrate (r)	Capacidad (c)	Longitud (b)	Rondas ($4b$)	Tamaño de hash (n)
U-QUARK	8	128	136	544	136
D-QUARK	16	160	176	704	176
S-QUARK	32	224	256	1024	256

4.3.3 Algoritmos ligeros para autenticación

Los algoritmos seleccionados forman parte de la primitiva criptográfica MAC, descrita en la Sección 2.2.4. Un enfoque está basado en obtener el MAC mediante una hash ligera, mientras que el otro enfoque aplica procedimientos que lo hacen ligero.

HMAC

Un código de autenticación de mensajes en llave-hash (HMAC, por sus siglas en inglés) es una construcción específica para calcular un MAC que implica una función hash en combinación con una llave criptográfica secreta. Como cualquier MAC, puede ser utilizado para verificar simultáneamente la integridad de los datos y la autenticación de un mensaje. Cualquier función hash, tales como SPONGENT o QUARK, puede ser utilizada para el cálculo de un HMAC; el algoritmo MAC resultante se denomina HMAC-SPONGET o HMAC-QUARK en consecuencia. La fuerza criptográfica del HMAC depende de la potencia criptográfica de la función de hash subyacente, el tamaño de su salida de hash y el tamaño y calidad de la llave.

Una función hash iterativa rompe un mensaje en bloques de un tamaño fijo e itera sobre ellos con una función de compresión. Por ejemplo, SPONGENT y QUARK operan en bloques de 128-bit. El tamaño de la salida de HMAC es el mismo que el de la función de hash subyacente (128 ó 136 bits en el caso de SPONGENT o QUARK, respectivamente), aunque se puede truncar si se desea. La estructura de HMAC se observa en la Figura 4.8.

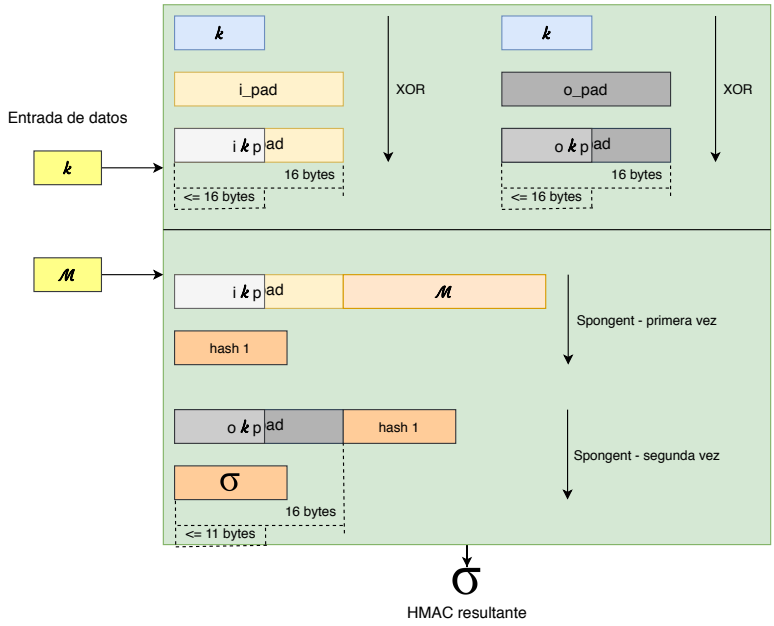

Figura 4.8: Diagrama a bloques de la estructura de HMAC.

Un HMAC se define como:

$$\text{HMAC}(k, M) = H\Big((k \oplus opad)||H\big((k \oplus ipad)||M\big)\Big) \tag{4.2}$$

Donde:

- H es la función hash.
- k es una llave secreta rellena a la derecha con ceros adicionales al tamaño del bloque de entrada de la función hash, o el hash de la llave original si es más largo que el tamaño de bloque.
- M es el mensaje a ser autenticado.
- $||$ denota concatenación.
- $\oplus$ denota disyunción exclusiva (XOR).
- $opad$ es el relleno exterior (0x5c5c5c, un bloque de largo hexadecimal constante).

- $ipad$ es el relleno interior (0x363636, un bloque de largo hexadecimal constante).

LIGHTMAC

LIGHTMAC es un algoritmo para la generación de MACs basado en un cifrado de bloques, donde la longitud del mensaje no tiene ningún efecto en el límite de seguridad. LIGHTMAC no solo ofrece autenticación compacta para plataformas con recursos limitados, sino que también permite implementaciones paralelas de alto rendimiento [40].

Un cifrador a bloque es una función $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$, donde $E(K,\cdot)$ define una permutación para $K \in \{0,1\}^k$. El entero n es el tamaño del bloque de E denotado como $E_K(X)$ que significa $E(K,X)$. El símbolo 0^n representa la cadena de n-bits que solamente contiene ceros. Dado una cadena A de tamaño n y un entero $t \leq n$, entonces $\lfloor A \rfloor_t$ denota el t bit menos significante de A. LIGHTMAC acepta dos uniformes e independientes llaves K_1 y K_2 generadas de $\{0,1\}^k$ y un mensaje M con un tamaño de al menos $2^s(n-s)$ bits. Produce una salida de tamaño de t bits. El Algoritmo 6 describe cómo se genera la salida.

Para un entero $1 \leq i \leq 2^s$, i_s representa algún s-bit constante con la propiedad que si $1 \leq i < j \leq 2^s$ entonces $i_s \neq j_s$. Para obtener el MAC, LIGHTMAC genera etiquetas usando el Algoritmo 6 y verificación de pares mensaje-etiqueta (M,T) se realiza comparando LIGHTMAC (M) con T: si los dos son iguales, la verificación es exitosa.

Los parámetros de LIGHTMAC son los enteros s y t, la representación de i_s y el cifrado de bloque E, que implícitamente fija k y n. Los parámetros deben acordarse antes de que comience una sesión, y permanecer constantes durante.

Algorithm 6 Generación de códigos de mensajes basado en cifrado de datos.

Entrada: $K_1, K_2 \in \{0,1\}^k$: llaves generadas, $M \in \{0,1\}^{\leq 2^s(n-s)}$: mensaje

Salida: $T \in \{0,1\}^t$: MAC de tamaño t

1: $V \leftarrow 0^n \in \{0,1\}^n$
2: $M[1]M[2]\dots M[\ell] \xleftarrow{n-s} M$
3: **for** $i = 1$ **to** $\ell - 1$ **do**
4: $\quad V \leftarrow V \oplus E_{K_1}(i_s M[i])$
5: **end for**
6: $V \leftarrow V \oplus (M[\ell]10^*)$
7: $T \leftarrow \lfloor E_{K_2}(V) \rfloor_t$
8: **return** T

4.3.4 Algoritmo para control de acceso

Para garantizar el servicio de control de acceso, se utilizó el algoritmo DET-ABE. DET-ABE usa un cifrado simétrico y uno de llave pública. El cifrado simétrico transforma los datos D en texto cifrado C_D por medio de operaciones $E.\text{ENC}(k_i, D)$ para cifrado y $E.\text{DEC}(k_i, C_D)$ para descifrado, tal que $C_D = E.\text{ENC}(k_i, D)$ y $D = E.\text{DEC}(k_i, C_D)$. Ambas operaciones utilizan la misma llave simétrica k_i y la protección de dicha llave es crucial para garantizar el servicio de confidencialidad sobre la información importante que se cifra. Un cifrado de llave pública utiliza dos llaves, una de dominio público para el cifrado PK, en este caso se utiliza P como llave pública, y la otra privada para el descifrado SK_U, que pertenece a un usuario U_j. En este caso, $C_P = \text{ABE.ENC}(P, k_i)$ y $k_i = \text{ABE.DEC}(\text{SK}_U, C_P)$. En la implementación de DET-ABE se consideraron las siguientes fases:

- **Inicialización:** se generan los parámetros públicos pms que van a ser comunes a los usuarios del sistema (por ejemplo, el conjunto total de atributos U), así como la llave secreta MK de la TA que repartirá las llaves secretas SK_U a los usuarios U_j.
- **Obtención de llaves:** U_j demuestra a la TA que posee un subconjunto A_U de atributos. Como respuesta, obtiene una llave secreta SK_U.
- **Cifrado:** los datos D recolectados por los sensores son enviados a la BS donde se verifica la

autenticación y posteriormente se cifra la llave k_i mediante una política de control de acceso P, que siempre puede describirse como una familia Γ de subconjuntos de U, aquellos subconjuntos permitirán el descifrado correcto. El resultado del protocolo de cifrado es un texto cifrado C_P.

- **Descifrado:** U_j cuyo subconjunto de atributos A_U pertenece a la familia Γ puede utilizar su llave secreta SK_U para descifrar C_D y recuperar la llave simétrica de cifrado k_i, para poder acceder a los datos D.

4.4 Resumen

En este capítulo se diseñó el modelo de WBAN segura basado en las 3 capas que compone a una WBAN. Para que la WBAN sea segura, en cada capa se debe garantizar servicios de seguridad para proteger los datos que se generan, transmiten y almacenan. A la vez, cada servicio de seguridad es proveído por algoritmos de criptografía. Sin embargo, los algoritmos criptográficos convencionales no son adecuados para la implementación en los dispositivos que actúan en una WBAN debido a su alto costo computacional. Bajo ese contexto, mediante algoritmos de criptografía ligera se proveen los servicios de seguridad requeridos en una WBAN: confidencialidad se provee mediante un cifrador de datos, integridad se garantiza a través de funciones hash, autenticación es garantizada mediante códigos de autenticación de mensajes y control de acceso lo provee un cifrado basado en atributos. Todos los algoritmos criptográficos seleccionados tienen un enfoque ligero y proveen un nivel de seguridad de al menos 128 bits.

5

Experimentación y resultados

En este capítulo se describen los detalles de implementación, validación y evaluación del prototipo de WBAN segura con base en el modelo propuesto en el Capítulo 4. Primero se presenta una descripción de los dispositivos utilizados para la construcción del prototipo, resaltando sus características principales. A continuación, se presenta una descripción de la implementación de WBAN segura por cada capa, indicando los dispositivos considerados en cada una. Después se detallan los experimentos comenzando con el establecimiento de las métricas de interés. Se plantearon experimentos divididos en tres casos de uso. El CU1 consistió en evaluar el desempeño de los algoritmos criptográficos utilizados en la capa 1 del modelo de WBAN segura al garantizar servicios de seguridad. En el CU2 se evaluó el desempeño de los algoritmos implementados en la BS al garantizar el control de acceso. En el CU3 se evaluó el desempeño del sistema, es decir, el acceso a los datos por parte de un usuario. Finalmente, se presentan los resultados obtenidos en cada experimento y una discusión de los mismos para evaluar el desempeño del esquema de WBAN segura propuesto en esta tesis.

5.1 Dispositivos utilizados

En el despliegue del prototipo de WBAN y esquema de seguridad en cada capa, se ha considerado la implementación de los algoritmos criptográficos para niveles de seguridad recomendados en estándares internacionales. En la Tabla 5.1[1] se observan niveles de seguridad y el año hasta el que se sugiere utilizarlos de acuerdo con organismos internacionales reconocidos. Cabe mencionar que entre mayor sea el nivel de seguridad es más difícil de vulnerar el sistema. Además, el nivel de seguridad es proporcional a los recursos computacionales demandados por el algoritmo. En la Tabla 5.1 también se muestra que el nivel de seguridad de 80 bits, el cual al día de hoy es obsoleto en todos los estándares internacionales.

Tabla 5.1: Niveles de seguridad recomendados por estándares internacionales.

Lapso de tiempo	Nivel de seguridad (bits)	Algoritmos simétricos	Curva elítica (bits)	Hash
Legacy[2]	80	PRESENT-80	160	PHOTON-80 SPONGENT-88
2019 - 2030 y más	128	PRESENT-128 LEA-128	256	PHOTON-128 SPONGENT-128
2019 - 2030 y más	192	LEA-192	384	PHOTON-224 SPONGENT-224
2019 - 2030 y más	256	LEA-256	512	PHOTON-256 SPONGENT-256

El equipo de hardware del prototipo de WBAN segura son sensores y microprocesadores embebidos en tarjetas programables que se utilizaron para obtener los signos vitales de una persona. Se utilizó un teléfono inteligente como estación base para la recepción y envío de datos y, finalmente, se usó una computadora de escritorio que sirvió como servidor, alojando el sistema para almacenar los datos

[1] https://www.keylength.com/

[2] Los algoritmos y las longitudes de llave para el nivel de seguridad de 80 bits se pueden emplear debido a su uso en aplicaciones heredadas. No se utilizarán para aplicar protección criptográfica (por ejemplo, cifrado).

y permitiendo el acceso a ellos por parte de usuarios. En la Tabla 5.2 se puede observar, a manera de resumen, los dispositivos sensores utilizados en el prototipo de WBAN segura implementado.

Tabla 5.2: Dispositivos sensores utilizados en el prototipo de WBAN segura.

Sensores	Signo vital sensado	Servicio de seguridad	Lenguaje de programación	Comunicación con la BS
Galaxy Watch	Ritmo cardíaco	CIA	JavaScript	Bluetooth
TI LaunchPad 3220SF	Temperatura corporal	CIA	C/C++	Bluetooth
Raspberry Pi 3	Saturación de oxígeno en la sangre	CIA	Python	Bluetooth

La arquitectura del sensor TI LaunchPad 3220SF permite ejecutar algoritmos criptográficos únicamente con nivel de seguridad de 128 bits, debido que para la ejecución de niveles más altos, sus especificaciones como memoria flash de 1 MB y RAM de 256 KB no son suficientes. Sin embargo, tanto el Galaxy Watch como la Raspberry Pi 3 cuentan con especificaciones suficientes como 1 GB de memoria RAM y CPU Dual-Core 1.15 GHz y Quad Core 1.2GHz, respectivamente. Las especificaciones de estos dos sensores son suficientes para ejecutar los algoritmos en los tres niveles de seguridad: 128, 192 y 256.

Los dispositivos mencionados en la Tabla 5.2 son los sensores S_i de la capa 1 del modelo de WBAN. En las capas 2 y 3 del modelo de WBAN actúan otros dispositivos los cuales son la estación base y el sistema, en este caso una computadora de escritorio. Las características principales de estos dispositivos se observan en la Tabla 5.3. Lo relevante de las características de estos dispositivos es que comparten el lenguaje de programación, lo que facilita la comunicación entre ellos y las tecnologías de comunicación inalámbricas.

Tabla 5.3: Resumen de características de los dispositivos utilizados como estación base y sistema.

Dispositivo	Procesador	Conectividad	Memoria RAM	Lenguaje de programación	Plataforma de desarrollo	Capa de WBAN
Samsung Galaxy A6+	Snapdragon 450 1.8 GHz Octa core	Bluetooth v4.2, Wi-Fi 802.11 a/b/g/n DualBand	3 GB	Java	Android	2
Hp Pavilion	AMD A10 3.2 GHz	Bluetooth v4, Wi-Fi 802.11 b/g/n	12 GB	Java	Java Server	3

5.2 Implementación del prototipo de WBAN segura

Como se ha descrito en el Capítulo 4, el modelo de WBAN segura está basado en 3 capas: recolección de datos, comunicación y aplicación. El prototipo construido se muestra gráficamente en la Figura 5.1, donde se observa el diseño de WBAN segura empleando los dispositivos descritos en secciones anteriores y con todos los actores descritos en el Capítulo 4.

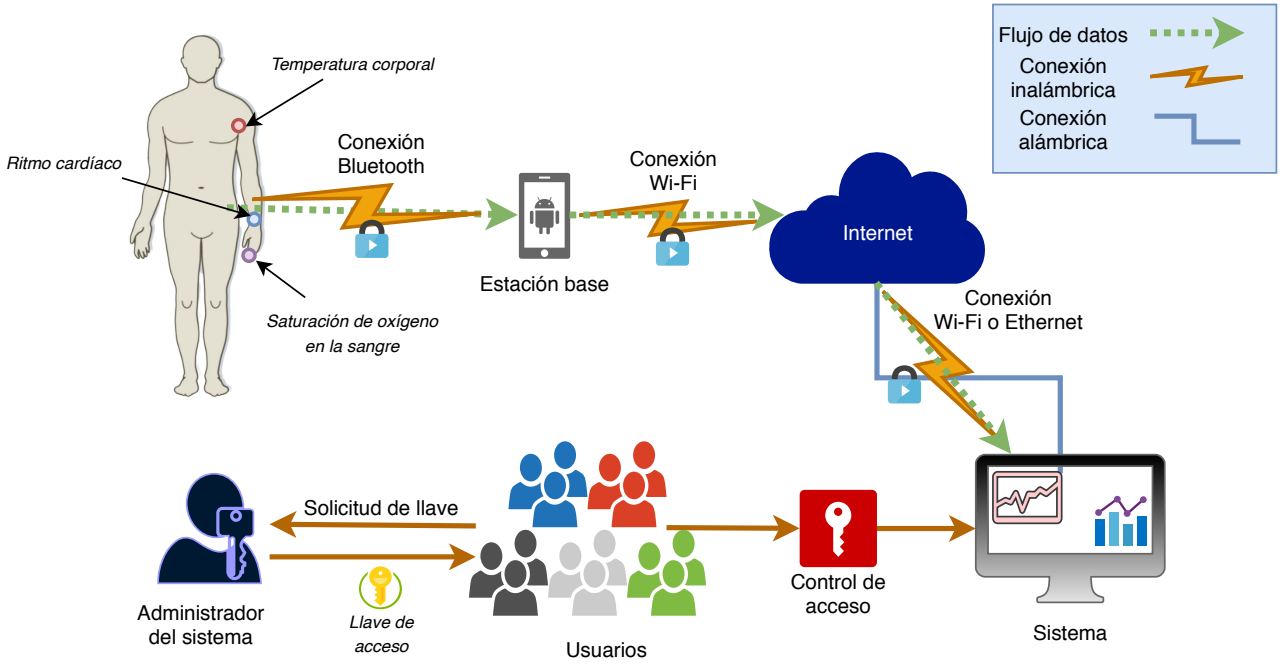

Figura 5.1: Diagrama del prototipo WBAN segura.

Cada etapa del prototipo contiene tres aspectos que la componen: adquisición de datos, servicios de seguridad y comunicación de datos. En cada una de las capas se utilizan diferentes servicios y tecnologías para su correcto funcionamiento.

5.2.1 Despliegue de la etapa 1: recolección de datos

La primer etapa consiste en la recolección de datos por medio de nodos sensores que están en constante monitoreo de los signos vitales de un usuario. Cada sensor opera a una velocidad de sensado diferente.

- **Adquisición de datos.** Para adquirir los datos, se utilizaron tres sensores diferentes, debido a que se monitorean tres signos vitales:

    1. *Ritmo cardíaco:* se utiliza un Galaxy Watch de Samsung como nodo sensor para el ritmo cardíaco, aprovechando su enfoque en el cuidado de la salud. En la literatura [55] se ha definido que para este signo vital las muestras tienen una frecuencia de 250 Hz y usando una resolución de 16 bits, se tiene una tasa de datos de 4 Kbps para lecturas de ECG, mientras que para el ritmo cardíaco la tasa de datos es de 64 bps con una frecuencia de 4 Hz y una resolución de 16 bits [5]. Los datos recabados son numéricos de tipo entero, dado que son pulsos del corazón en un intervalo de tiempo, normalmente, por minutos.
    2. *Saturación de oxígeno en la sangre:* para sensar este signo vital, fue necesario utilizar la tarjeta programable Raspberry Pi 3 añadiendo el sensor *MAX30100*, que permite obtener tanto el ritmo cardíaco como la saturación de oxígeno en la sangre. La tasa de datos que se obtiene es de . Los datos recabados son bps con una frecuencia de 1 hz y una resolución de 16 bits [66]. numéricos de tipo flotante, con 4 decimales de precisión. Esto se debe a que el nivel de saturación de oxígeno en la sangre se mide en porcentaje.
    3. *Temperatura corporal:* para obtener la temperatura corporal de una persona se utiliza la tarjeta programable, Texas Instruments CC3220SF Launchpad combinado con el sensor

de temperatura DS18B20 que tiene una precisión de $\pm 0{,}5$ grados. La temperatura se toma con una frecuencia de 0.2 Hz y usando una resolución de 16 bits, dando una tasa de datos de 2.4 bps [55]. Los datos recabados de este signo vital son numéricos de tipo flotante con 2 decimales de precisión. La temperatura se mide en grados Celsius.

- **Servicios de seguridad.** La seguridad que se garantiza en esta etapa es semicompleta, es decir, se garantizan 3 de los 4 servicios de seguridad requeridos en una WBAN segura, estos son: *confidencialidad*, *integridad* y *autenticación*.

  En la estación base, que es un teléfono Samsung Galaxy A6+, se garantizan los 4 servicios de seguridad. Se utilizan los mismos algoritmos y niveles de seguridad, incluyendo llaves secretas, que en los nodos sensores. Adicionalmente, para garantizar el control de acceso, se utiliza ABE, generando políticas de acceso y cifrando la llave simétrica, que se utilizó para cifrar los datos, con las políticas generadas. Todos los algoritmos criptográficos (cifrador simétrico, hash y ABE), incluyendo curvas elípticas, deben usar un tamaño de llave que proporcione un nivel de seguridad consistente de acuerdo a la Tabla 5.1.

  Los datos de signos vitales recolectados se procesan para proporcionar seguridad a esos datos y enviarlos a una estación base. Este procedimiento está dividido en 7 fases: *configuración*, *sensado*, *cifrado de datos*, *autenticación de datos*, *emisión*, *recepción y verificación*, *cifrado de llave simétrica y emisión de datos*.

  1. **Configuración.** Es la fase de inicialización del modelo. Consiste en repartir las llaves simétricas que se usarán en la WBAN, cuando tanto los nodos sensores como la estación base están fuera de línea. El nivel de seguridad utilizado determina el tamaño de las llaves simétricas en uso en esta etapa. La estación base obtiene las políticas de acceso determinadas por el sistema. Finalmente, se despliegan los nodos sensores y se conecta la estación base.
  2. **Sensado.** Esta fase se encarga de comenzar a recolectar datos utilizando los nodos

sensores desplegados anteriormente, comprobando la conexión con la estación base.

3. **Cifrado de datos.** Cuando se tienen los datos de los signos vitales, comienza la fase del cifrado de los datos. Se utiliza un bloque de n-bits, 128 bits utilizando LEA o 64 bits utilizando PRESENT, para almacenar los datos y aplicar el cifrado utilizando la llave simétrica previamente proporcionada.
4. **Autenticación de datos.** Los datos cifrados pasan a la fase de autenticación, la cual consiste en generar la MAC de los datos cifrados utilizando una hash ligera.
5. **Emisión.** Cada nodo sensor envía tanto los datos cifrados, MAC y ID a la estación base donde se procesan.
6. **Recepción y verificación.** La estación base recibe los datos cifrados de los sensores y los verifica, aplicando el algoritmo de autenticación.
7. **Cifrado de llave simétrica y emisión de datos.** Después de comprobar la autenticidad de los datos, la llave simétrica disponible desde la estación base se cifra utilizando *ABE*, con las políticas de control de acceso. Finalmente, los datos cifrados recibidos y la llave simétrica cifrada se envían a la etapa 3: aplicación o al sistema.

- **Comunicación de datos.** Todos los dispositivos utilizados en esta etapa tiene capacidades de conectividad tanto de Wi-Fi 802.11 b/g/n 2.4 GHz como de Bluetooth Low Energy v4.2 o superior. Los sensores se comunican con la estación base mediante una interfaz Bluetooth, enviando paquetes de datos de 128 bits.

  El proceso de envío de un paquete de datos desde el nodo sensor hasta la estación base es el siguiente:

  1. El valor obtenido del nodo sensor de ritmo cardíaco es un número de 16 bits, normalmente. Dado que los algoritmos criptográficos procesan bloques de datos, en un buffer se almacenan estas lecturas hasta completar un bloque válido para el cifrador, por ejemplo,

de 128 bits.

2. El bloque de datos se pasa al cifrador. Utilizando la llave simétrica compartida se realiza el proceso de cifrar el bloque de datos, dando como resultado un bloque de datos cifrados del mismo tamaño, 128 bits. El nivel de seguridad que se utilizan en los algoritmos criptográficos es de 128 bits.

3. El bloque de datos cifrado se envía al algoritmos para autenticación. Este algoritmo criptográfico también utiliza una llave simétrica para realizar el procesamiento. El resultado de este algoritmo es un bloque de autenticación de 128 bits.

4. El ID que se le asignó a cada sensor es sencillo, un número entero de 8 bits. En este caso específico, 01.

5. Se envían los bloques de datos mediante Bluetooth desde el nodo sensor hasta la estación base.

5.2.2 Despliegue de la etapa 2: comunicación

Esta etapa de comunicación comprende el envío de datos desde la estación base y la recepción en la etapa de aplicación. El envío de los datos se realiza mediante una conexión a Internet, debido a que la comunicación no es local. Tanto los datos cifrados como la llave simétrica cifrada son empaquetados en un archivo JSON, esto permite la serialización de los datos y proporciona una estructura común en comunicaciones vía Internet.

- **Adquisición de datos.** En esta etapa, la obtención de los datos sucede cuando la estación base recibe los datos provenientes de los sensores y envía dichos datos al sistema a través de un servicio web. Para ello, la estación base envía un archivo de tipo JSON, que contiene todos los datos pertinentes, además de un encabezado que define el tipo de tecnología de comunicación que se utiliza en este enlace.

- **Servicios de seguridad.** En esta capa no se ejecuta ningún algoritmo criptográfico. Cuando se reciben los datos del lado del sistema, se verifica su autenticidad, por lo que se garantiza la integridad y autenticidad de los datos a lo largo de la comunicación en Internet. Cuando el sistema recibe los datos, se almacenan en un repositorio.

- **Comunicación de datos.** El sistema proporciona un servicio web REST que consume la estación base. Este servicio está desarrollado en un servidor web Java que utiliza el sistema para la comunicación. Permite enlazar una comunicación segura, a través de tecnologías JSON, y a la vez, garantizar una serialización y deserialización de los datos manteniendo la integridad de los mismos. Toda la comunicación se realiza a través de Internet.

En la capa de comunicación, no se realizó un diseño como tal, sin embargo, se definió el protocolo de comunicación entre la estación base y el sistema. Este protocolo seleccionado es Wi-Fi (estándar IEEE 802.11), debido a que que están diseñadas para proporcionar acceso inalámbrico en zonas con un rango típico de hasta 100 metros. Esto proporciona a los usuarios la capacidad de moverse dentro de un área de cobertura local y permanecer conectado a la red. Además, se hace uso de Internet que potencia esta comunicación.

5.2.3 Despliegue de la etapa 3: aplicación

En la última etapa, aplicación, actúa el sistema, que es el encargado de administrar los datos recolectados por los sensores y mantener el control de acceso a los mismos por los usuarios finales. El sistema proporciona un servicio web, el cual consulta la estación base y envía los datos. Con los datos recibidos, se autentican y de ser correctos, se almacenan en un repositorio.

- **Adquisición de datos.** El sistema utiliza metadatos que permiten el manejo los datos recabados por los sensores, para después localizarlos. Para obtener los datos del repositorio del sistema, se solicita una llave secreta de acceso. Esta llave tiene un nivel de seguridad

de 128 bits y es generada por el administrador del sistema que actúa como la autoridad de confianza en el esquema DET-ABE.

- **Servicios de seguridad.** En esta etapa se garantizan los 4 servicios de seguridad. Se descifra la llave simétrica que fue cifrada con DET-ABE por la BS, usando la llave secreta de acceso del usuario, realizando un control de acceso y garantizando la autenticación de la llave que hasta este momento mantiene seguro los datos recabados por los sensores. Finalmente, se descifran los datos de los sensores, garantizando la confidencialidad e integridad de los datos hasta el final. Los servicios de seguridad garantizados en esta etapa son desde la perspectiva del usuario de los datos.

- **Comunicación de datos.** La comunicación entre la estación base y el sistema se realiza vía Internet, mediante un servicio web proporcionado por el sistema. Este servicio requiere parámetros como datos cifrados y llave simétrica cifrada. Cuando la estación base consume el servicio, estos parámetros se convierten en un archivo JSON que contiene el flujo de datos y al recibirlo se deserializa obteniendo el tipo de datos original. Además, esta etapa tiene comunicación directa con los usuarios que solicitan acceso a los datos.

La etapa 3 del modelo de WBAN segura se encarga de utilizar los datos transferidos por las etapas anteriores y hacerlos disponibles a usuarios finales. En esta etapa actúa una autoridad de confianza, que es la encargada de generar las llaves de acceso de los usuarios, en este caso, se implementa como un usuario administrador del sistema. Esta etapa, igual a la etapa 1, se conforma de 4 fases: *configuración*, *recepción y almacenamiento de datos*, *generación de llaves de acceso* y *obtención datos*; que ayudan al despliegue de la WBAN.

1. **Configuración.** Es la fase inicial, la cual consiste en definir los parámetros de ABE, tal como el emparejamiento bilineal, el nivel de seguridad, atributos, generar las políticas de acceso y asignar los atributos a cada usuario del sistema. Además, designar una autoridad de confianza. La autoridad de confianza genera la llave pública y maestra del sistema.

2. **Recepción y almacenamiento de datos.** Los datos enviados desde la estación base se reciben en el sistema. Éstos entran en un proceso de verificación de los datos recibidos. Después de la comprobación, se almacenan en un repositorio específico dedicado para la consulta de los datos.

3. **Generación de llaves de acceso.** La autoridad de confianza se encarga de generar para cada usuario una llave de acceso, dependiendo de los atributos que les asignaron.

4. **Obtención de datos.** Con la llave de acceso, una entidad puede acceder a los datos biomédicos en claro disponibles en el sistema. Se ingresa al repositorio, se seleccionan los datos que desea obtener y se proporciona la llave de acceso, si el usuario tiene los atributos necesarios para cumplir con la política con la que fue cifrada la llave simétrica, podrá descifrarla. Con la llave simétrica correcta, el usuario que solicita el acceso, podrá descifrar los datos sensados y visualizarlos.

5.3 Definición de experimentos

Para evaluar el desempeño de los algoritmos criptográficos en el modelo de WBAN segura propuesto se diseñaron tres experimentos, uno por cada capa de la WBAN, la cual para la experimentación se definió como caso de uso (CU). Se utilizó la notación CU1, CU2 y CU3 para referirse al caso de uso en la capa que sucede.

5.3.1 Métricas de interés

En esta tesis, las métricas de interés son el tiempo de ejecución, memoria consumida y consumo de energía; estas últimas, particularmente para evaluar las operaciones de seguridad de datos en la Capa 1 de la WBAN, donde se utilizan dispositivos con capacidades y recursos computacionales limitados. El tiempo de ejecución de un algoritmo es una medida comúnmente utilizada para comparaciones

y medir el desempeño de los algoritmos respecto a la autonomía de los dispositivos utilizados. Las tres métricas consideradas en esta tesis son las comúnmente usadas en trabajos relacionados, aunque no en todos los trabajos reportan todas las métricas. La experimentación realizada es con fines de evaluación y comparación.

Tiempo de ejecución

Se denomina tiempo de ejecución al intervalo de tiempo en el que un programa de computadora se ejecuta en un sistema operativo. Este tiempo se inicia con la puesta en memoria principal del programa, por lo que el sistema operativo comienza a ejecutar sus instrucciones.

El tiempo de ejecución es una función del "tamaño"de los datos de entrada a procesarse. Así, por ejemplo, en un programa de ordenamiento el tamaño natural de medida para la entrada es el número de elementos a ordenar. En esta tesis, el tamaño de la entrada está dado por diversos factores, por ejemplo:

- Cifrador simétrico: El tiempo de ejecución es afectado por el nivel de seguridad usado.
- Función hash: El tiempo de ejecución es afectado por el nivel de seguridad usado.
- HMAC: El tiempo de ejecución es afectado por el tiempo de ejecución de la función hash.
- ABE: El tiempo de ejecución es afectado por el nivel de seguridad usado al igual que el número de atributos en la política de control de acceso.

Memoria consumida

El consumo de memoria representa la cantidad de memoria que utiliza un programa en particular durante su ejecución. Este término se explica por sí mismo, ya que cada aplicación se basa en la memoria subyacente para almacenar instancias de variables. Cuantas más variables use un algoritmo, mayor será su consumo de memoria. Por lo tanto, es una suposición común que las aplicaciones que requieren más memoria son más costosas.

Consumo de energía

El consumo de energía en este caso en particular se calcula utilizando el concepto **Amperio-hora**[3], debido a que se mide el consumo de energía de la batería de un dispositivo. Un amperio-hora es una unidad de carga eléctrica y se abrevia como *Ah*. Indica la cantidad de carga eléctrica que pasa por los terminales de un dispositivo de almacenamiento de energía eléctrica, por ejemplo un condensador o una batería.

El amperio-hora representa la cantidad de electricidad que, en una hora, atraviesa un conductor por el que circula una corriente continua de 1 amperio (1 amperio-hora (Ah) = 3600 Coulombs (C)). Se emplea para evaluar la capacidad de una batería, o de cualquier otro dispositivo capaz de almacenar energía eléctrica, es decir, la cantidad de electricidad que puede almacenar durante la carga y devolver durante la descarga.

En las baterías es normal el uso del miliamperio hora (mAh), que es 0.001 Ah, o lo que es lo mismo 3.6 C. Esto indica la máxima carga eléctrica que es capaz de almacenar la batería. A más carga eléctrica almacenada, más tiempo tardará en descargarse. El tiempo de descarga viene dado por la expresión:

$$\textit{tiempo de descarga } (h) = \frac{\textit{carga eléctrica batería } (mAh)}{\textit{consumo eléctrico dispositivo } (mA)} \tag{5.1}$$

De la misma forma, se puede hallar el consumo eléctrico de un dispositivo:

$$\textit{consumo eléctrico dispositivo } (mA) = \frac{\textit{carga eléctrica batería } (mAh)}{\textit{tiempo de descarga } (h)} \tag{5.2}$$

La unidad del Sistema Internacional de Unidades para medir la energía acumulada en una batería es el Joule; sin embargo, dado que el voltaje nominal de una batería es fijo, se utiliza el Ah como unidad de carga, haciendo referencia al tiempo de carga y descarga de la batería.

[3]https://energyeducation.ca/encyclopedia/Ampere_hour

Para calcular la energía almacenada en la batería, se multiplica la intensidad de corriente que pasa por la batería por su tensión o voltaje.

$$(x\ Ah * \frac{3600\ s}{1\ h} * y\ V) = z\ J \tag{5.3}$$

5.3.2 CU1: Envío de datos desde el nodo sensor hasta estación base

Este experimento se realiza en la capa 1 del modelo WBAN. El objetivo es medir el impacto de los algoritmos criptográficos ligeros en cada nodo sensor y comparar el desempeño de los algoritmos en cada servicio de seguridad. Por ende, el proceso se realiza de forma independiente en cada sensor. Aunado a esto, se compara la tasa de datos recibida en la estación base por cada sensor con la tasa de datos reportada en la literatura.

Los experimentos para los 3 sensores comparten configuraciones previas al despliegue. En cada sensor se comparte y almacena una llave simétrica para cifrado y autenticación de los datos que se usarán en los algoritmos utilizados. Estas llaves también son almacenadas en la estación base, junto con el ID de cada sensor, dado que la estación base almacena todas las llaves compartidas y el ID facilita la búsqueda y recuperación de dichas llaves. Estas llaves y todos los algoritmos criptográficos utilizan un nivel de seguridad de 128, 192 y 256 bits, excepto el sensor de temperatura que solamente se utiliza un nivel de seguridad de 128 bits. En la Tabla 5.4 se puede observar un resumen de los detalles de la experimentación en este CU.

Tabla 5.4: Detalles de la experimentación del CU1.

Dispositivo sensor	Servicios de seguridad	Niveles de seguridad (bits)	Métricas de interés
Galaxy Watch	CIA	128, 192, 256	Tiempo de ejecución, memoria y energía consumida
Raspberry Pi 3	CIA	128, 192, 256	Tiempo de ejecución y memoria consumida
TI LaunchPad CX3020SF	CIA	128	Tiempo de ejecución, memoria y energía consumida

Cada sensor ejecutará el mismo experimento de forma individual e independiente. Cada experimento se guió del siguiente procedimiento:

1. Compartir la llave simétrica, con la que se cifrarán y descifrarán los datos, entre el nodo sensor y la estación base.

2. Los algoritmos deben estar implementados tanto en la estación base como en el nodo sensor.

3. Después de conectarse vía Bluetooth, el nodo sensor S_i comienza a recabar datos D del signo vital que están monitoreando, y se almacenan en un buffer hasta completar un bloque de 128 bits. Una vez completado, el bloque se cifra utilizando la llave de cifrado simétrica k_i, se obtiene el código de autenticación σ de los datos y posteriormente se envían a la BS la tupla $T_{S_i} = \{ID_i, C_D, \sigma\}$.

4. En la BS se recibe T_{S_i}.

5. Se mide el tiempo de ejecución, memoria y energía consumida por los algoritmos que garantizan la seguridad de los datos en los sensores. Además, se compara la tasa de transmisión de datos con lo reportado en la literatura.

En la experimentación del CU1, con fines de evaluación del impacto de los servicios de seguridad en el monitoreo de los signos vitales, se utilizaron dos conjuntos de algoritmos para garantizar los

servicios de seguridad. El objetivo de este experimento es proporcionar una alternativa de algoritmos ligeros para garantizar los mismos servicios de seguridad que los utilizados en el CU1.

Los algoritmos seleccionados forman parte de estándares en criptografía ligera ISO/IEC 29192-2:2019[4] e ISO/IEC 29192-6:2019[5], que son **PRESENT** un cifrador ligero y **LIGHTMAC** cifrado autenticado, respectivamente. El nivel de seguridad utilizado en los algoritmos es de 128 bits, debido a que PRESENT solamente cuenta con niveles de seguridad de 80 y 128 bits.

5.3.3 CU2: envío de datos desde estación base hasta el sistema

Este experimento une las 3 etapas del modelo de WBAN segura. Comienza cuando se reciben los datos de S_i en la BS. En este experimento, la fase de configuración se comparte con el experimento anterior tanto en los niveles de seguridad como las llaves criptográficas en los nodos sensores. La BS obtiene las políticas de control de acceso P generadas por el sistema. La conexión entre la BS y el sistema se realiza mediante Internet, el sistema despliega un servicio web REST que consume la BS para establecer la conexión y realizar el envío de datos. En la Tabla 5.5 se resumen los detalles de este experimento.

Tabla 5.5: Detalles de la experimentación del CU2.

Dispositivo	Servicios de seguridad	Niveles de seguridad (bits)	Métricas de interés
Samsung Galaxy A6+	CIA, control de acceso	128, 192, 256	Tiempo de ejecución, memoria consumida
HP Pavilion	Control de acceso, autenticación	128, 192, 256	Tiempo de ejecución

El objetivo del experimento es medir el impacto de los procesos que involucran algoritmos criptográficos ligeros en la BS dentro de la WBAN segura y comparar el desempeño de los algoritmos

[4]https://www.iso.org/standard/78477.html
[5]https://www.iso.org/standard/71116.html

cuando se generan 4, 8 y 16 atributos para definir la política P para el cifrado de k_i. El procedimiento que realiza la BS cuando interactúa con el sistema se describe de la siguiente manera:

1. Utilizando el ID$_i$ del sensor, se busca y carga la k_i asociada.

2. Cuando se obtiene k_i, se procede a validar la autenticación de los datos recibidos, de ser válidos, se cifra k_i utilizando una política P para el acceso de los usuarios autorizados.

3. P es generada en el sistema y obtenida en la BS.

4. Se envía al sistema $\{C_D, C_P, \sigma\}$. Además, se envía el ID de S_i también.

5. Cuando el sistema recibe los datos, busca la llave k_i y verifica la autenticación de los datos recibidos, de ser válidos, los almacena en un repositorio específico.

6. Se mide el tiempo de ejecución, memoria y energía consumida por los algoritmos que garantizan la seguridad de los datos en la estación base.

5.3.4 CU3: acceso a los datos por usuarios desde sistema

Con los datos almacenados en un repositorio específico, los usuarios U_j autorizados pueden acceder a ellos realizando, antes, una petición para la generación de una llave de usuario k_{U_j} que le servirá para obtener los datos. k_{U_j} es proporcionada por el administrador del sistema mediante los atributos del usuario U. Para generar las llaves de usuario, se establecen los parámetros de seguridad para el algoritmo ABE. Dado que ABE utiliza emparejamientos bilineales, los parámetros son nivel de seguridad de 128 y 192 para emparejamientos bilineales simétricos, mientras que para emparejamientos bilineales asimétricos los niveles de seguridad son 128, 192 y 256 bits.

El objetivo de este experimento es validar el correcto funcionamiento de la WBAN segura, es decir, es un experimento que permite probar la correctitud desde la generación de datos, su protección con algoritmos criptográficos ligeros hasta la obtención de los datos en texto claro por los usuarios

autorizados correspondientes. En este experimento se utilizó la computadora HP Pavilion como servidor donde además se generaron tanto las llaves del sistema como las de los usuarios. Los niveles de seguridad utilizados fueron de 128, 192 y 256 bits, midiendo el tiempo de ejecución de la generación de llaves y del acceso a los datos. El procedimiento que se realiza en este experimento es el siguiente:

1. TA genera las llaves pública PK y privada MK para el sistema.
2. Un usuario U_j realiza una petición solicitando una llave de sesión k_{U_j} a TA.
3. TA genera k_{U_j} para U_j, usando los atributos correspondientes a ese usuario. Los atributos son tomados de un universo A.
4. U_j entra al sistema, selecciona los datos que necesita obtener y solicita acceso proporcionando su llave k_{U_j}.
5. Primero se descifra k_i, utilizando k_{U_j}, sí y sólo sí los atributos de U_j coinciden con la política de control de acceso P con la que fue cifrada k_i.
6. Después de obtener k_i, se descifran los datos C_D y se proporciona a U_j los datos en claro.

5.4 Resultados

En esta sección se muestran los resultados de los experimentos definidos en las secciones previas. Para visualizar el desempeño de los algoritmos criptográficos utilizados, se utilizaron gráficas que permiten observar el comportamiento.

5.4.1 Resultados de CU1

La presentación de los resultados del primer caso de uso está dividida en varias partes. Primero se presenta los resultados obtenidos del desempeño de los algoritmos criptográficos ligeros en cada uno de los sensores, obteniendo todas las métricas de interés. Después, se presentan nuevos resultados

utilizando los mismo sensores pero con diferentes algoritmos criptográficos, comparando ambos resultados.

Sensor de ritmo cardíaco

Se utilizó el sensor de ritmo cardíaco como punto de partida en las experimentaciones, en las cuales se obtuvieron tiempo de ejecución, memoria consumida y consumo de energía. Estos experimentos tuvieron dos entrada de datos, la primera fue el nivel de seguridad y la segunda el servicio de seguridad garantizado. En la Figura 5.2 se observa el tiempo de ejecución que se obtuvo al termino de los experimentos involucrando todas las entradas.

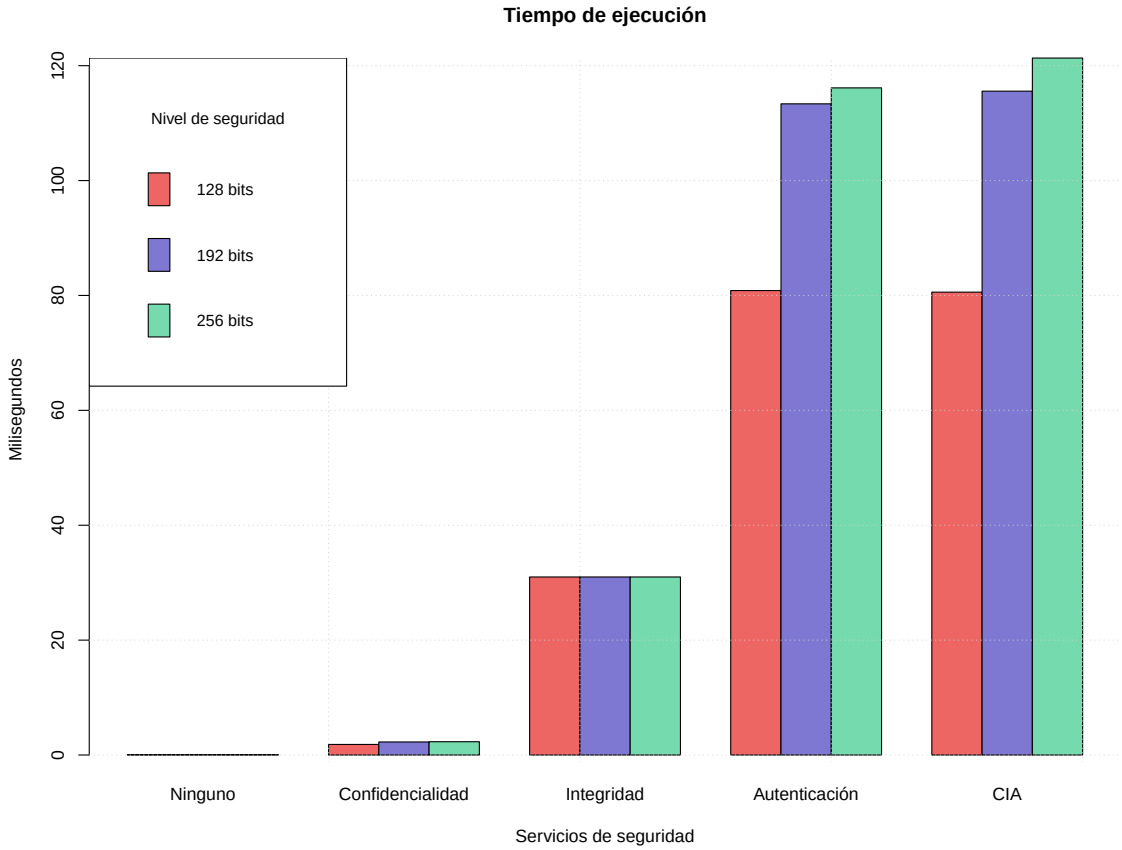

Figura 5.2: Tiempo de ejecución en el sensor de ritmo cardíaco.

Al involucrar en un proceso el uso de algoritmos de criptografía, aunque sean ligeros, se sabe que habrá una demanda de recursos computacionales mayor que lo que se requiere sin el uso de los mismos. Lo observado en la Figura 5.2 es la relación que tienen los algoritmos criptográficos respecto a la demanda de tiempo de ejecución. La diferencia entre garantizar todos los servicios y no hacerlo es considerable, es decir, si se toma la primer y última columna de la gráfica en la Figura 5.2, se puede observar el crecimiento notable en el tiempo de ejecución de al menos dos órdenes de magnitud. El tiempo de integridad se mantiene debido a que se procesa en bloques de 128 bits y únicamente aumenta el número de rondas conforme aumenta el nivel de seguridad. Esto no quiere decir que una solución WBAN segura implique necesariamente todos los servicios de seguridad; lo recomendable es que se garanticen todos. En la Figura 5.2 se observa que el costo por garantizar solo la confidencialidad es mucho menor que al garantizar confidencialidad y autenticación, este último servicio domina el tiempo de ejecución. La tasa de transferencia cuando la WBAN no utiliza servicios de seguridad es de 203.86 Kbps debido al llenado a tope de la carga útil de Bluetooth, mientras que cuando se garantiza la triada CIA en la WBAN, la tasa de transferencia baja considerablemente a 198.59 bps. Esto significa que los algoritmos tienen un alto impacto en el sensor al procesar los datos a la velocidad por default en el sensor. En la literatura se ha reportado que en una WBAN el sensor de ritmo cardíaco tiene una tasa de transferencia de 64 bps, sin utilizar servicios de seguridad. Lo que se reporta con este experimento es que la tasa de transferencia al garantizar los servicios de seguridad, a pesar de que los algoritmos demandan un costo adicional, la tasa de datos se mantiene por arriba de lo reportado en la literatura. Sin embargo, la solución se puede adaptar a como mejor convenga en el entorno que se realice y seleccionar el o los servicios de seguridad requeridos.

Por otro lado, la relación en el consumo de memoria entre nivel de seguridad y garantizar o no un servicio de seguridad no es significativo. En la Figura 5.3 se observan los resultados de memoria consumida durante el procesamiento y envío de los datos. Lo que el experimento revela es que es necesario contar con suficiente memoria, que en este caso fue de alrededor de 10 MB. Este comportamiento sucede debido a que el dispositivo asigna un espacio de memoria fijo a la aplicación

para ejecutar los procesos de los algoritmos criptográficos.

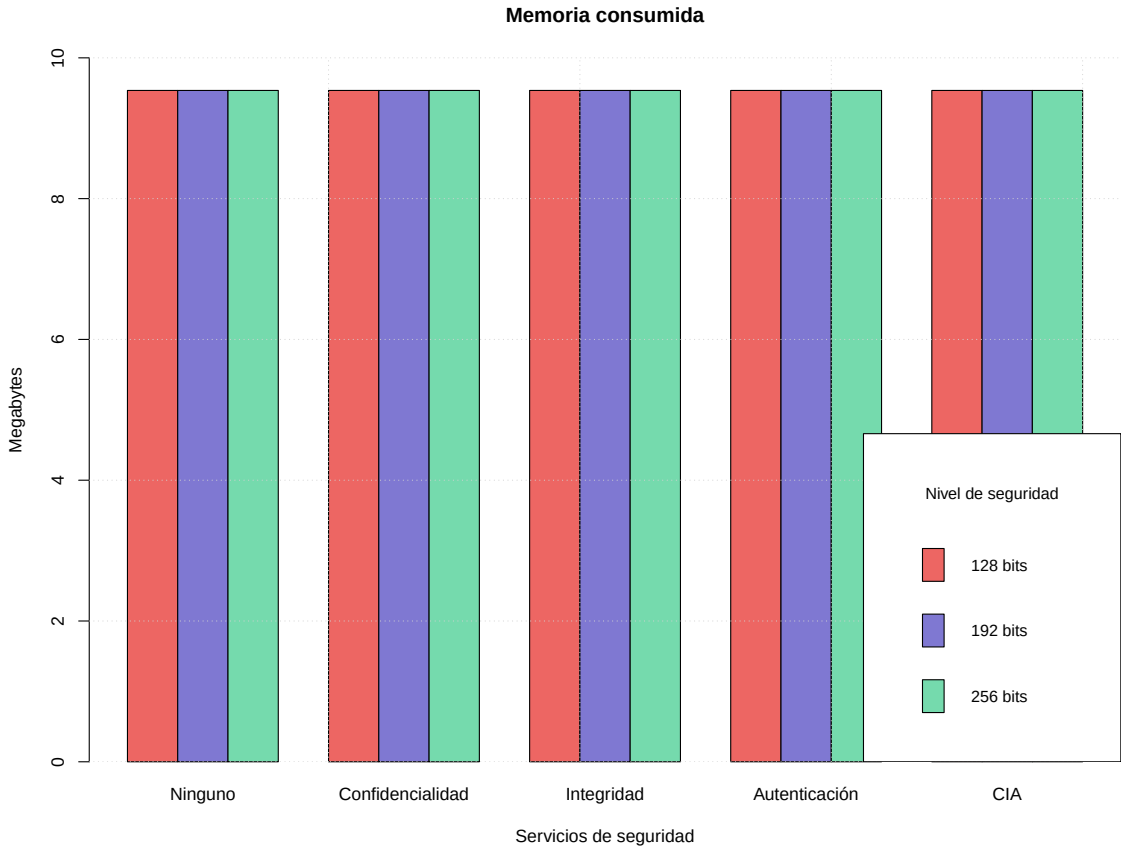

Figura 5.3: Memoria consumida en el sensor de ritmo cardíaco.

Para la última métrica obtenida se realizó un experimento diferente. Basado en la Ecuación 5.2 para obtener el consumo de miliamperios de una batería de un dispositivo electrónico; se decidió enviar 2,000 paquetes desde el sensor hasta la estación base. Se seleccionó ese número de paquetes debido a que durante la obtención del tiempo de ejecución, al llegar a 2,000 paquetes, la distribución de los resultados, visualmente se vuelve normal. Sin embargo, después de realizar la prueba de normalidad de Shapiro Wilks, resultó que la distribución no es normal. Al término de este experimento se obtuvo la cantidad de miliamperios se consume cuando se garantiza seguridad y cuando no se hace. Los parámetros para la ecuación se obtuvieron al medir el tiempo que se tardó en enviar todos los

paquetes y el porcentaje de batería consumido en ese lapso de tiempo. En la Figura 5.4 se observa los resultados obtenidos y la relación que existe entre la demanda de energía según el servicio de seguridad garantizado.

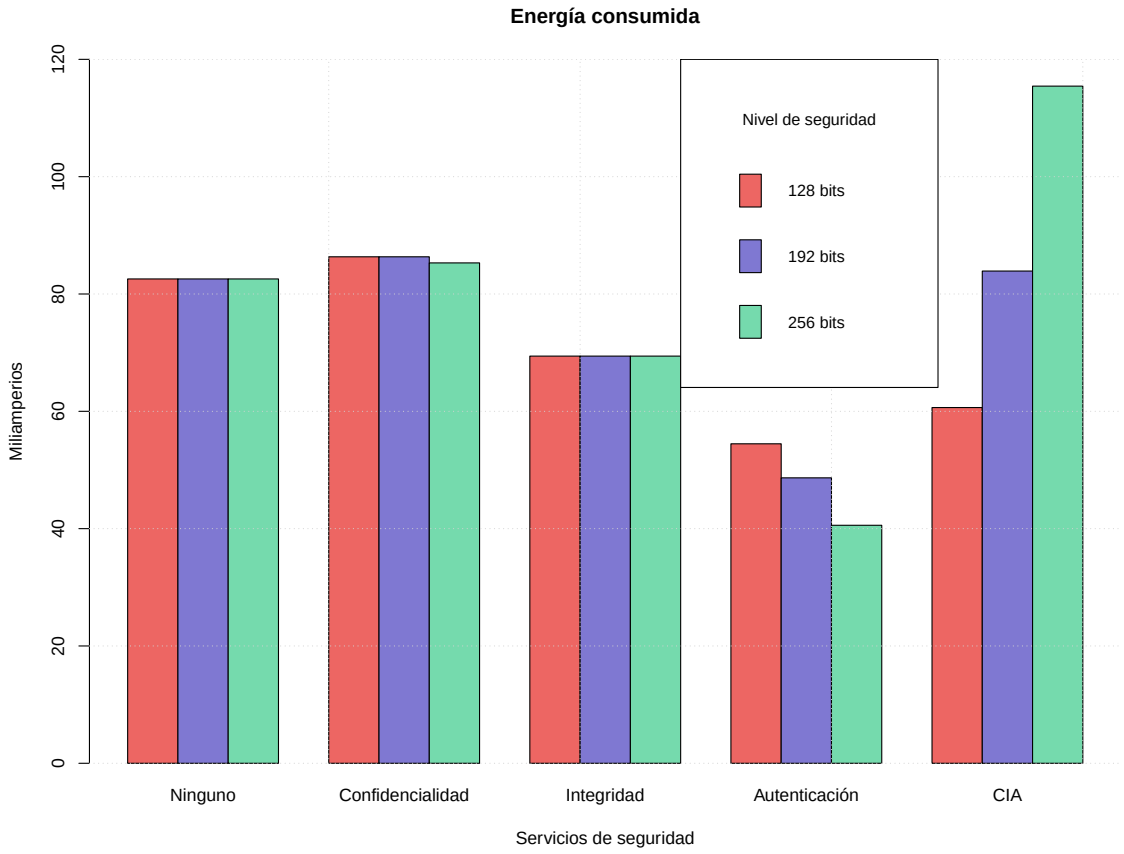

Figura 5.4: Energía consumida de la batería del sensor de ritmo cardíaco.

Los resultados mostrados en la Figura 5.4 se obtuvieron utilizando la Ecuación 5.2. En ella se observa que existe un bajo impacto en el consumo de energía cuando solo se garantiza la confidencialidad. Cuando se garantizan todos los servicios de seguridad, se observa el comportamiento esperado, el consumo de energía aumenta conforme aumenta el nivel de seguridad dado que se consumió un mayor porcentaje en la batería del dispositivo. El comportamiento en el consumo de energía reflejado en la ejecución del servicio de autenticación es opuesto al esperado, desde el punto

de vista de seguridad, ya que la energía disminuye cuando el nivel de seguridad (y tiempo de ejecución) aumenta. Con esto se concluye que el tiempo de ejecución es un factor importante en el consumo de energía, debido a que cuando un algoritmo tiene un tiempo de procesamiento prolongado, el consumo de energía se reduce sí y sólo sí, el porcentaje de batería consumido es el mismo. En otras palabras, cuando dos procesos consumen un mismo porcentaje de la batería, el tiempo es un factor para determinar cuál será el que más mA consuma dependiendo su duración.

Sensor de saturación de oxígeno en la sangre

Los experimentos para el sensor de saturación de oxígeno en la sangre se realizaron repitiendo los mismos niveles de seguridad, tanto en tiempo de ejecución como en memoria consumida. Los resultados obtenidos en este sensor, en cuanto al tiempo, están dados en segundos. Esto implica una gran diferencia entre los resultados obtenidos por el sensor de ritmo cardíaco que esta dado en milisegundos. En la Figura 5.5 se observa la relación del tiempo de ejecución con los servicios de seguridad.

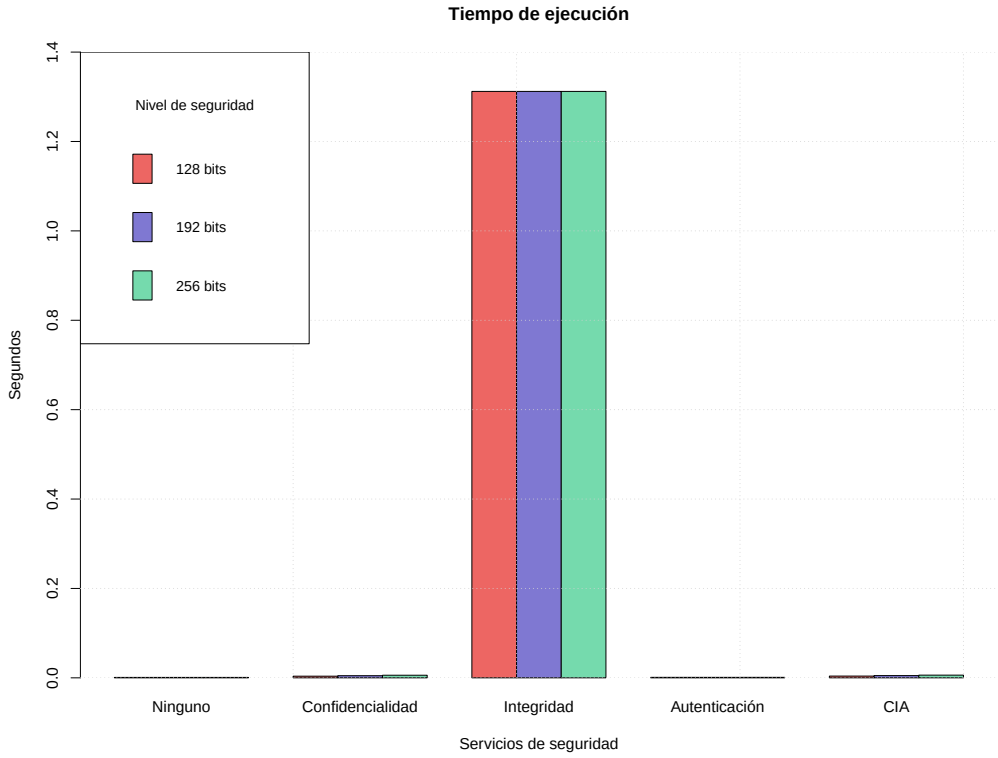

Figura 5.5: Tiempo de ejecución en el sensor de saturación de oxígeno en la sangre.

En las Figuras 5.2 y 5.5 se puede comprobar que el servicio de seguridad que menos tiempo demanda es la confidencialidad, debido al cifrador LEA que se utiliza. El cambio exponencial que se observa en la Figura 5.5, al pasar de la confidencialidad a la integridad se debe a los procedimiento realizados en ese servicio; y como es de esperarse, al consumir tanto tiempo la integridad, la autenticación consume más tiempo debido a que dentro de la autenticación incluye la integridad al utilizar la misma función hash que se usa para el servicio de integridad. Debido a cuestiones de implementación, el comportamiento observado en el servicio de Integridad en la Figura 5.5 aumenta de forma exponencial a diferencia del resto de los servicios de seguridad. No se determinó la causa con exactitud, la implementación fue realiza bajo la referencia oficial publicada por el autor del algoritmo y porque en el lenguaje implementado se utiliza una estructura de clases y objetos.

En el caso de la memoria consumida, sucede un fenómeno igual que lo observado en la Figura 5.3,

es muy bajo el impacto en el consumo de memoria en este sensor. Esto se observa en la Figura 5.6. Esto se debe a que el sistema operativo proporciona un espacio de memoria fijo para los procesos que se realiza. Esto quiere decir, que a la memoria que se utiliza en el sensor para ejecutar los procesos, no le importa si se garantizan servicios de seguridad o no, el consumo es el mismo para los procesos solicitados. Para el caso de este sensor, la memoria requerida es menor comparado con el sensor de ritmo cardíaco, de menos de 5 MB, prácticamente la mitad. En este caso, el sistema operativo asigna una espacio fijo al dispositivo para poder ejecutar los procesos de seguridad necesarios.

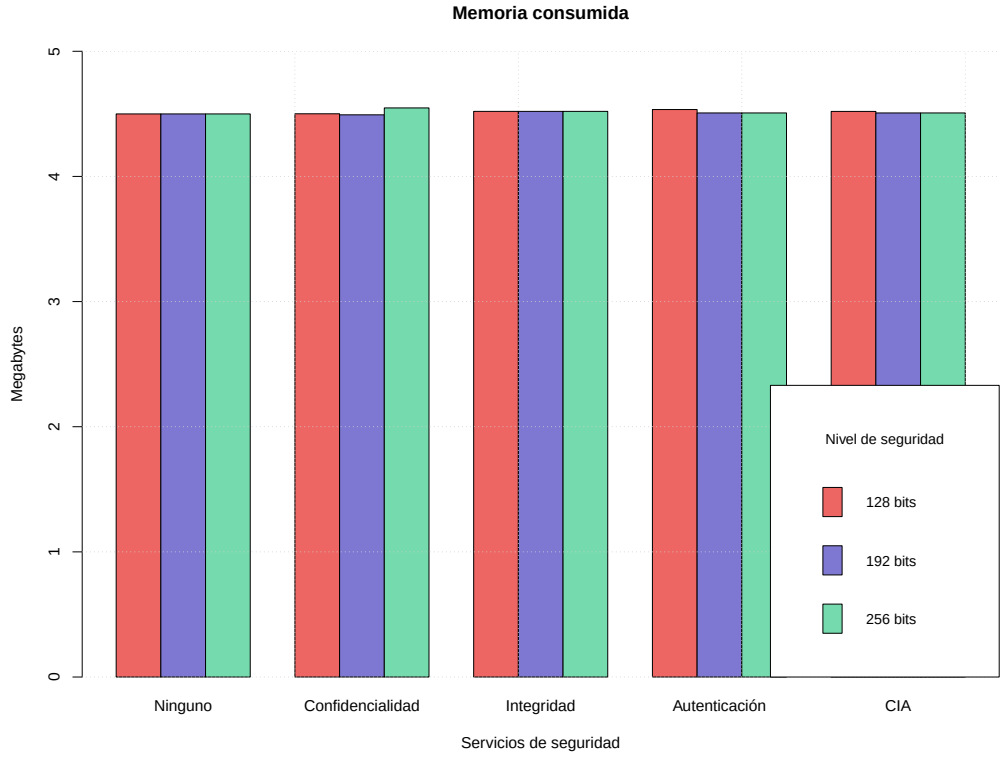

Figura 5.6: Memoria consumida en el sensor de saturación de oxígeno en la sangre.

En el caso de este sensor no se obtuvieron resultados de la medición del consumo de energía debido a que no es posible aislar la ejecución solamente del proceso criptográfico, sino que al tratarse de un sistema operativo en ejecución, están inmersas otras tareas que contabilizan en el consumo de energía, como las funciones de comunicaciones de Wi-Fi.

Sensor de temperatura corporal

En el sensor de temperatura, cuya arquitectura solamente permite ejecutar algoritmos con nivel de seguridad de 128 bits, se realizó el mismo experimento los resultados mostrados en la Figura 5.7. Cabe resaltar la eficiencia del algoritmo de confidencialidad en este dispositivo, debido a que obtiene el mismo tiempo de ejecución que cuando no se garantiza seguridad. Este comportamiento se ha estado aproximando en los experimentos con los dispositivos anteriores donde la confidencialidad tiene una diferencia menor en tiempo a cuando no se garantiza seguridad. Además, garantizar solamente autenticación es lo mismo que garantizar todos los servicios de seguridad en este dispositivo.

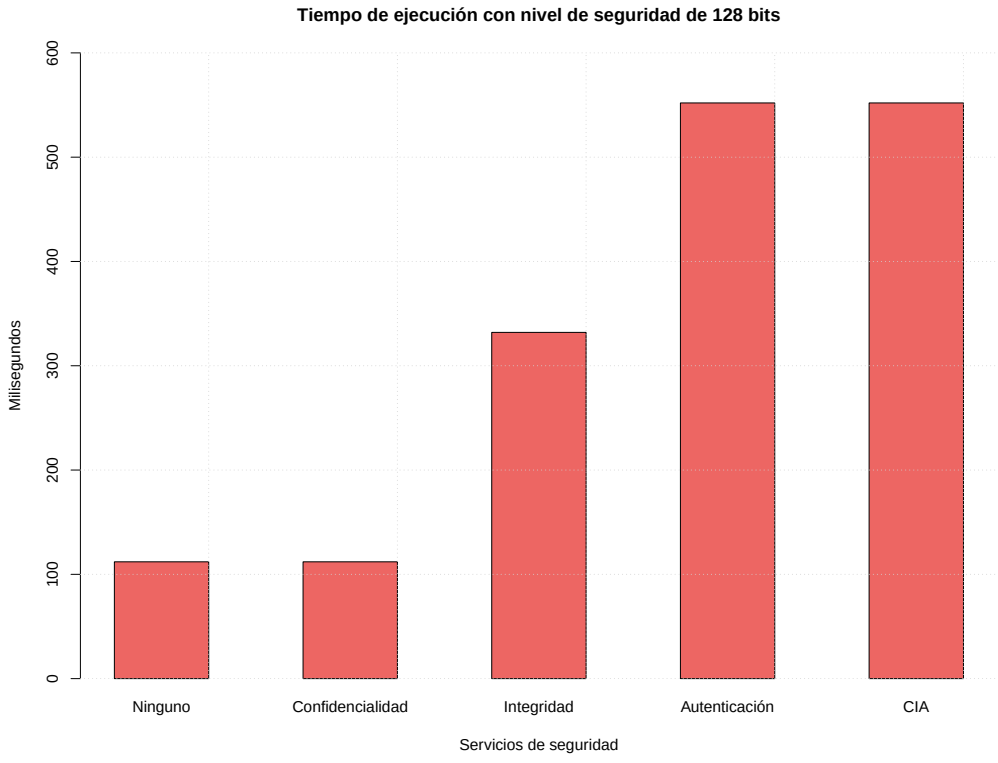

Figura 5.7: Tiempo de ejecución en el sensor de temperatura con nivel de seguridad de 128 bits.

A diferencia de los sensores anteriores, el consumo de memoria en este sensor es mucho menor, en el orden de los KB. La razón de esta reducción es debido a la buena gestión de memoria en el

sensor de temperatura y a la comunicación directa con el microprocesador. Los valores obtenidos en esta experimentación se pueden observar en la Figura 5.8.

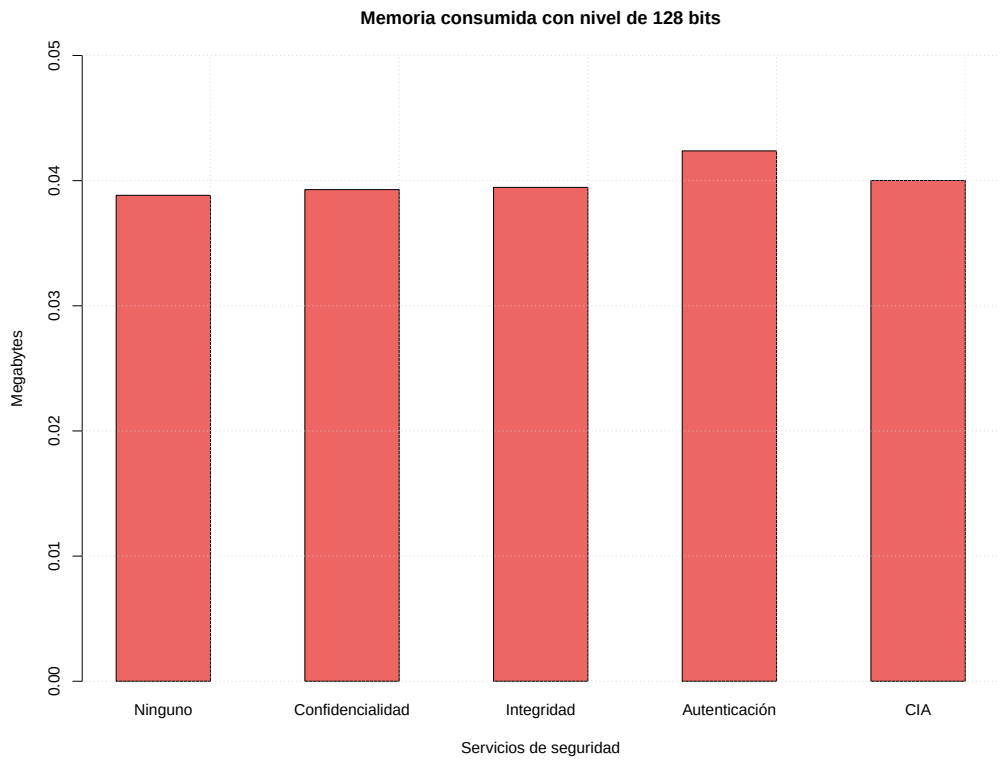

Figura 5.8: Memoria consumida en el sensor de temperatura con nivel de seguridad de 128 bits.

El consumo de energía en este sensor se observa en la Figura 5.9. A pesar de ser el servicio de seguridad con mejor desempeño en tiempo de ejecución, la confidencialidad es el servicio de seguridad que más energía consume. Al contrario que la autenticación que es el servicio que más tiempo consume y el que demanda menor cantidad de energía. Esto se debe a que cuando se garantiza la confidencialidad la ejecución es más rápida que cuando se garantiza la autenticación, es un comportamiento similar a lo que sucedido en la Figura 5.2. Sin embargo, en este caso tanto la confidencialidad como no garantizar seguridad tienen el mismo tiempo, por ende deberían tener el mismo consumo de energía, pero cuando se garantiza la confidencialidad se ejecutan más procesos que solamente el sensado de los datos, esto provoca que el consumo de energía aumente en la

confidencialidad. Como se esperaba, el consumo de energía mayor sucede cuando se garantizan 3 servicios de seguridad, lo mismo que pasó con el tiempo de ejecución. Sin embargo, los valores observados en la Figura 5.9 son menores al consumo de energía del sensor de ritmo cardíaco observado en la Figura 5.4.

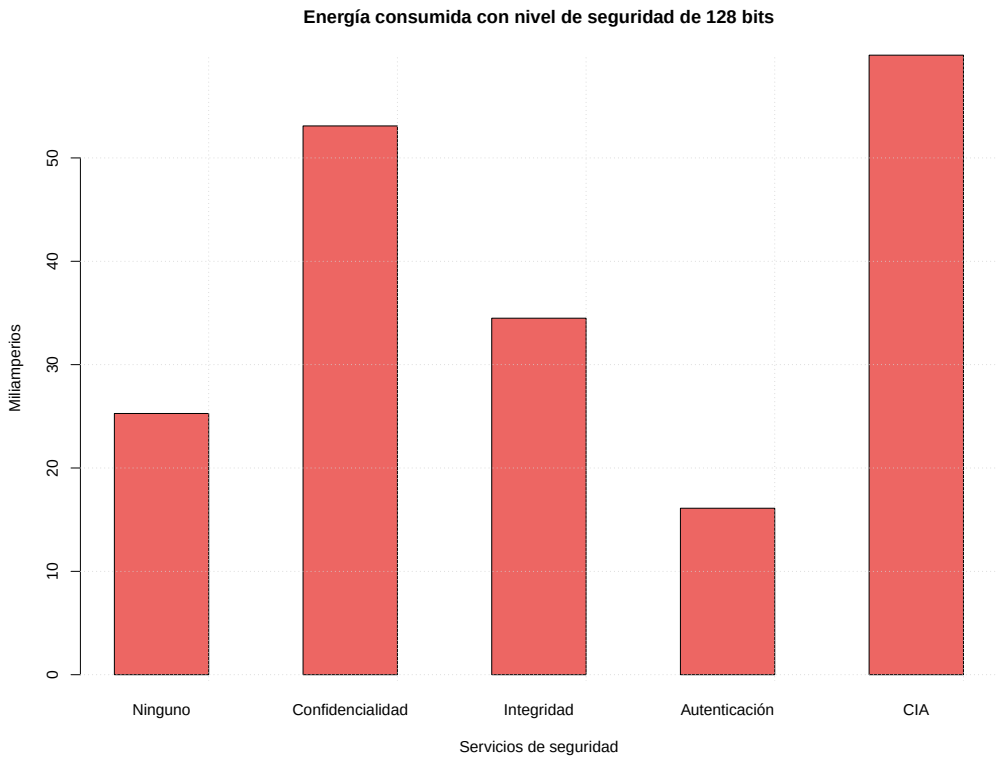

Figura 5.9: Consumo de energía en el sensor de temperatura con nivel de seguridad de 128 bits.

A manera de resumen, los resultados de tiempo de ejecución obtenidos de los sensores durante la experimentación se observan en la Tabla 5.6. En ella se observan los datos recabados de cada sensor con los diferentes servicios de seguridad. Todos los valores están expresados en segundos debido a que el servicio de seguridad que demandó más tiempo fue de 1.31 s.

Tabla 5.6: Tiempo de ejecución en los sensores durante la experimentación.

Dispositivo	Nivel de seguridad (bits)	Tiempo de ejecución (s) en servicios de seguridad				
		Ninguno	Confidencialidad	Integridad	Autenticación	CIA
Galaxy Watch	128	0.00008	0.0018	0.031	0.081	0.081
	192	0.00008	0.0023	0.031	0.1134	0.1156
	256	0.00008	0.0023	0.031	0.1161	0.1213
Raspberry Pi	128	0.00095	0.0037	1.31	0.0011	0.0039
	192	0.00095	0.0048	1.31	0.0011	0.005
	256	0.00095	0.0059	1.31	0.0011	0.006
TI LaunchPad CX3020SF	128	0.112	0.112	0.332	0.552	0.552

Para resumir la experimentación del consumo de memoria, en la Tabla 5.7 se observan los datos obtenido de todos los sensores en la conclusión del experimento. Resalta el bajo consumo de memoria del nodo sensor TI LaunchPad, a pesar de no tener un consumo uniforme. El nodo sensor Galaxy Watch resalta la uniformidad de su consumo, el cual fue suficiente para los procesos que se realizaron.

Tabla 5.7: Consumo de memoria en los sensores durante la experimentación.

Dispositivo	Nivel de seguridad (bits)	Consumo de memoria (MB) en servicios de seguridad				
		Ninguno	Confidencialidad	Integridad	Autenticación	CIA
Galaxy Watch	128	9.54	9.54	9.54	9.54	9.54
	192	9.54	9.54	9.54	9.54	9.54
	256	9.54	9.54	9.54	9.54	9.54
Raspberry Pi	128	4.5	4.5	4.52	4.55	4.52
	192	4.5	4.5	4.52	4.51	4.51
	256	4.5	4.55	4.52	4.51	4.51
TI LaunchPad CX3020SF	128	0.039	0.039	0.039	0.042	0.040

Finalmente, en la Tabla 5.8 se observa un resumen de los resultado obtenidos al concluir el

experimento del consumo de energía. Cabe mencionar que este experimento se realizó en dos nodos sensores, Galaxy Watch y TI LaunchPad, debido a que el nodo sensor Raspberry Pi incorpora un sistema operativo el cual se inicia al ejecutar un proceso y eso influye en su consumo. En ambos casos resalta el consumo considerable de energía que realiza el dispositivo cuando no se garantizan servicios de seguridad, dado que cuando se garantizan algunos servicios de seguridad se consume menos energía en el caso del Galaxy Watch.

Tabla 5.8: Energía consumida de la batería en los sensores durante la experimentación.

Dispositivo	Nivel de seguridad (bits)	Consumo de energía (mA) en servicios de seguridad				
		Ninguno	Confidencialidad	Integridad	Autenticación	CIA
Galaxy Watch	128	82.57	86.34	69.41	54.46	60.64
	192	82.57	86.34	69.41	48.66	83.91
	256	82.57	85.3	69.41	40.57	115.44
TI LaunchPad CX3020SF	128	25.27	53.1	34.5	61.42	59.94

5.4.2 Comparación de algoritmos criptográficos ligeros

Se realizó un experimento con fines de comparación entre dos suites de algoritmos criptográficos ligeros. La primera suite son los algoritmos utilizados en la experimentación anterior, siendo éstos los principales algoritmos recomendados en esta tesis. La segunda suite de algoritmos son PRESENT, QUARK y LIGHTMAC. Cada uno de ellos cumple con garantizar el servicio de confidencialidad, integridad y autenticación, respectivamente. Se debe resaltar que esta experimentación solamente se realizó con el nivel de seguridad de 128 bits, debido a que PRESENT únicamente cuenta con niveles de seguridad de 80 y 128 bits.

Tabla 5.9: Resumen de algoritmos utilizados en la experimentación.

Servicio de seguridad	Suite 1	Suite 2
Confidencialidad	LEA	PRESENT
Integridad	SPONGENT	QUARK
Autenticación	HMAC	LIGHTMAC

En la Tabla 5.9 se observan las dos suites de algoritmos que se utilizaron en este experimento. Ambas suites contienen 3 algoritmos para garantizar confidencialidad, integridad y autenticación. Además, ambas tienen al menos 2 algoritmos que son considerados como estándar en criptografía ligera en la norma ISO/IEC 29192.

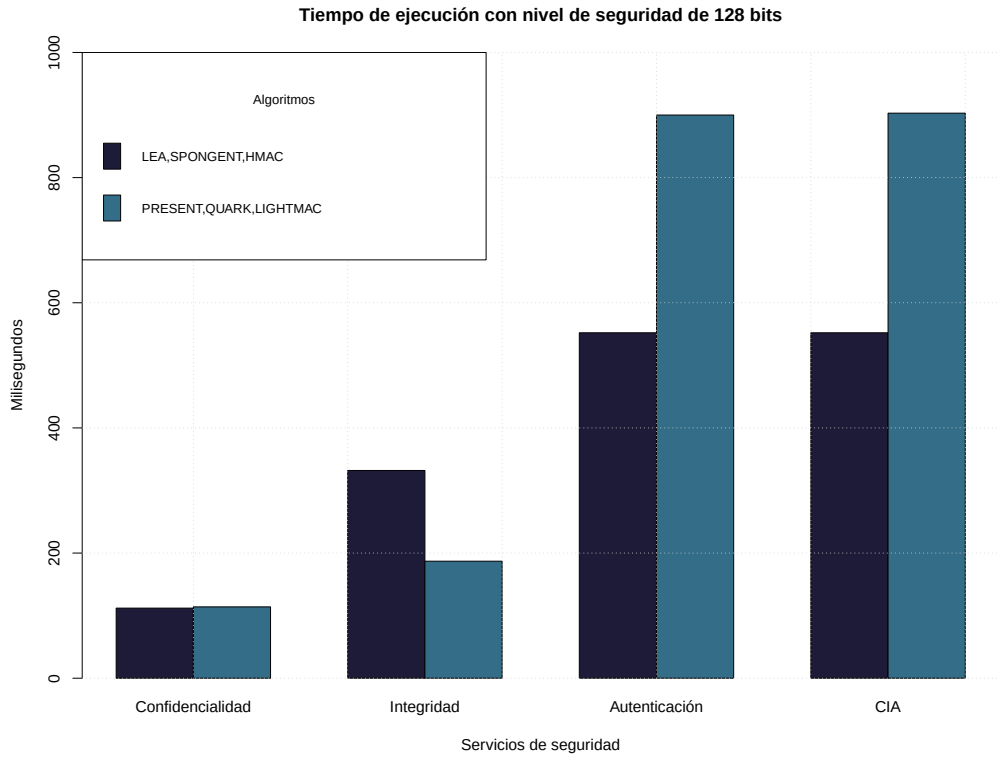

Figura 5.10: Comparación en tiempo de ejecución entre los algoritmos de criptografía ligera utilizando el sensor de temperatura.

En la Figura 5.10 se observa una clara ventaja en tiempo entre una suite y otra, estos resultados son en el sensor de temperatura. Al garantizar la confidencialidad, los algoritmos de cifrado LEA y PRESENT tienen un desempeño muy parecido, la diferencia mínima entre ellos son 2 ms. En el caso del servicio de integridad, SPONGENT es un 20.43 % más lento que QUARK. Sin embargo, en el caso del servicio de autenticación LIGHTMAC resulta ser mucho más costoso que que HMAC-SPONGENT, y dicho impacto se mantiene cuando se garantizan los tres servicios de seguridad.

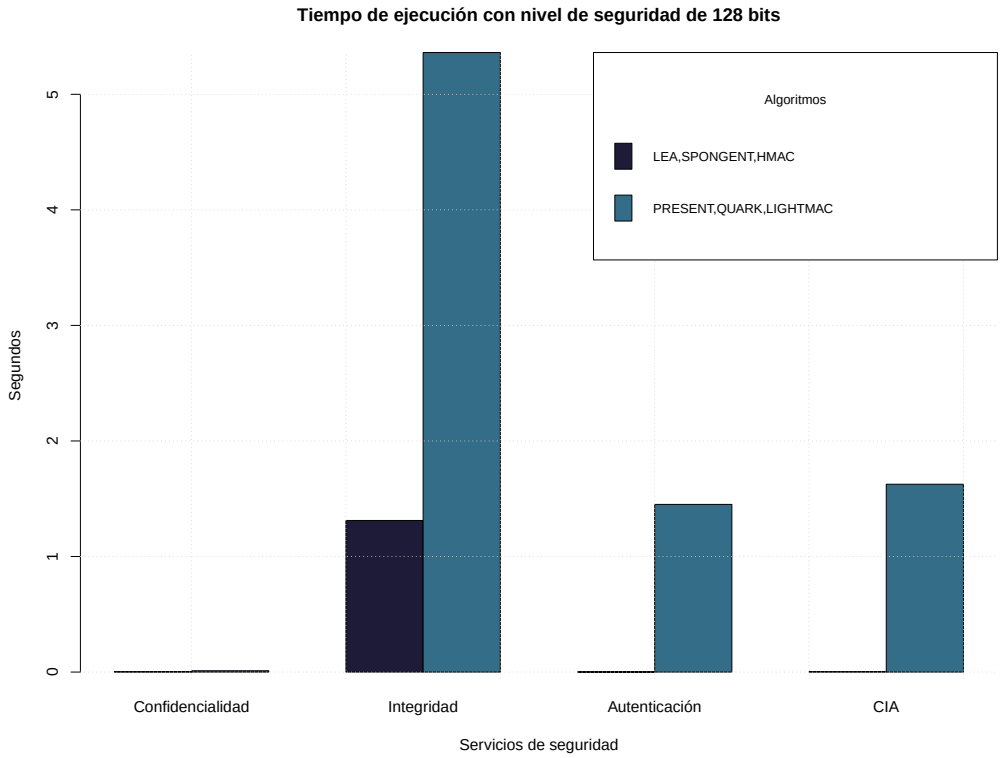

Figura 5.11: Comparación en tiempo de ejecución entre los algoritmos de criptografía ligera utilizando el sensor de saturación de oxígeno en la sangre.

En la Figura 5.11 se observa nuevamente que la suite 1 tiene un mejor desempeño sobre la suite 2, cuando la evaluación se realiza sobre el sensor de saturación de oxígeno en la sangre. También se puede observar que al contrario que el resultado obtenido con el sensor de temperatura, la integridad en la suite 2 tiene un costo mayor en el tiempo de ejecución que en la suite 1, debido a las mismas

causas que el algoritmo de integridad en la suite 1 observado en la Figura 5.6 y para una evaluación justa ambos algoritmos se tomaron de la misma fuente. Para el resto de los servicios en el sensor de saturación de oxígeno en la sangre, el crecimiento en el tiempo de ejecución es en un orden de magnitud mayor.

A manera de resumen, en la Tabla 5.10 se observan los resultados del experimento de comparación entre los algoritmos implementados en los nodos sensores. Los resultados obtenidos en el sensor de temperatura se mantuvieron por debajo de 1 s, en ambas implementaciones de las suites comparadas. En el sensor de saturación de oxígeno en la sangre resaltan los resultado de la integridad en ambas suites, siendo éste el servicio que más tiempo demanda en esta comparación. Como se observó en las Figuras 5.10 y 5.11, la suite con mejor desempeño en la mayor parte de los servicios garantizados resultó ser la suite 1, con la que se realizó toda la experimentación anterior.

Tabla 5.10: Comparación en tiempo de ejecución entre suites de algoritmos en los nodos sensores.

Dispositivo	Suite	Nivel de seguridad (bits)	Tiempo de ejecución (s) en servicios de seguridad			
			Confidencialidad	Integridad	Autenticación	CIA
Raspberry Pi 3	1	128	0.0037	1.31	0.0011	0.0039
	2		0.0113	5.3616	1.452	1.6256
TI LaunchPad CX3020SF	1	128	0.112	0.332	0.552	0.552
	2		0.114	0.187	0.9	0.903

5.4.3 Resultados de CU2

En la capa 2 de la WBAN, la estación base transfiere los datos hasta el sistema a través de un servicio web mediante Internet. Antes de realizar el envío, la estación base cifra la llave simétrica utilizando el algoritmo DET-ABE. En este experimento, se midió el desempeño del algoritmo en la estación base al cifrar la llave simétrica en tres niveles de seguridad: 128, 192 y 256 bits. Además, se utilizó tres configuraciones de números de atributos (4, 8 y 16) para definir la política de control de acceso con la que se cifró la llave simétrica.

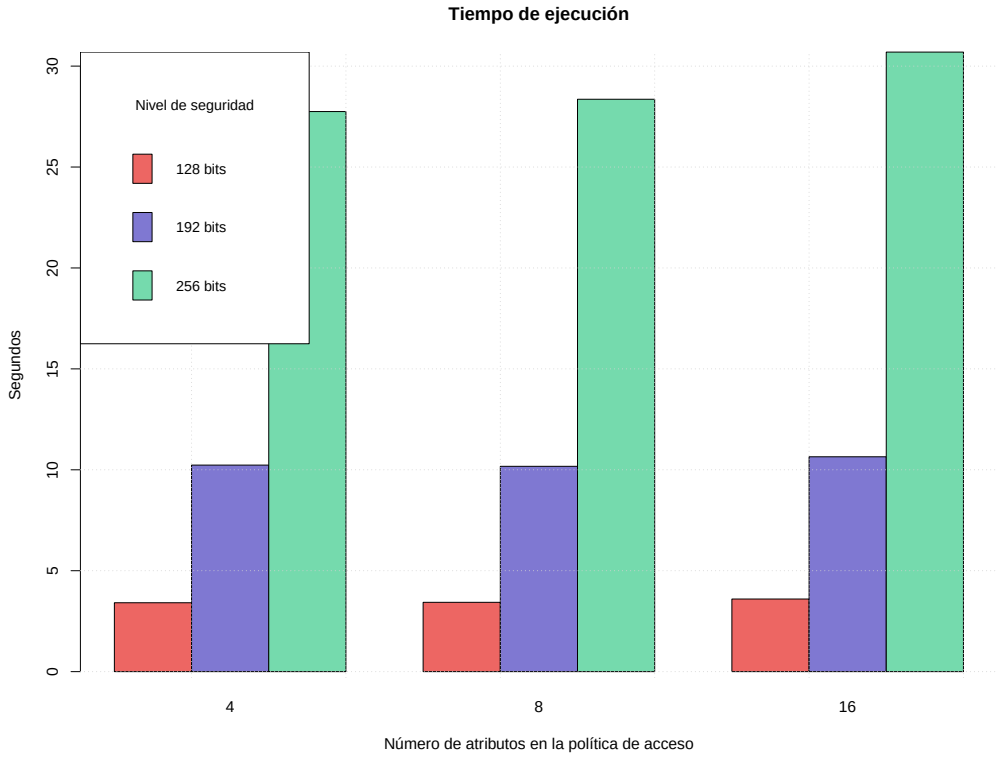

Figura 5.12: Tiempo de cifrado basado en atributos de llave simétrica.

En la Figura 5.12 se observa el tiempo que se tomó la estación base para cifrar la llave simétrica a lo largo del experimento. Sobresale que el número de atributos en la política de acceso tiene un impacto mínimo en el tiempo de procesamiento conforme aumentan los niveles de seguridad. Cabe resaltar que se utilizó un enfoque asimétrico en el algoritmo ABE, debido a que en la Figura 5.14 se demuestra que un enfoque asimétrico es más rápido que un enfoque simétrico en todos los niveles de seguridad, incluso el enfoque asimétrico cuenta con el nivel de 256 bits a diferencia del enfoque simétrico. En esta tesis se realiza la implementación de sobres digitales para el transporte seguro de la llave del cifrador ligero LEA, al cifrarla con una política de control de acceso usando CP-ABE.

La memoria consumida por la estación base en este experimento es dinámica. Esta es la razón del comportamiento observado en la Figura 5.13. La máquina virtual de Java se encarga de la gestión de memoria asignando a cada proceso lo necesario y liberando memoria cuando ya no se utiliza.

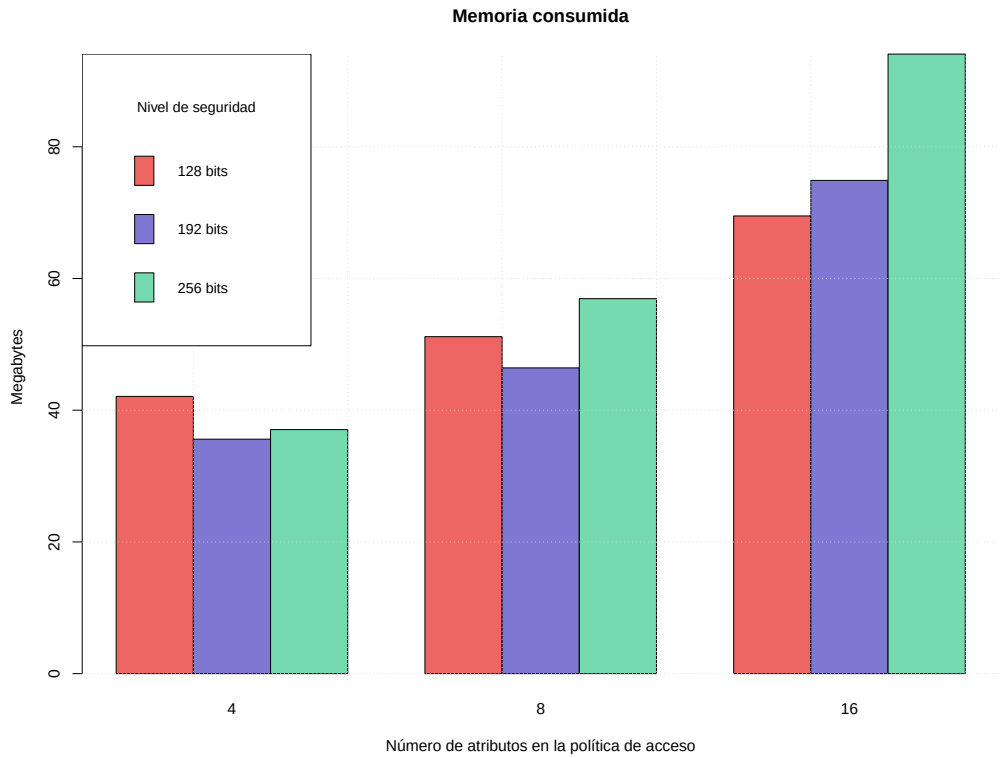

Figura 5.13: Memoria consumida durante el cifrado de la llave simétrica en la estación base.

Además de la gestión de Java se puede observar que el algoritmo DET-ABE demanda mayor cantidad de memoria en comparación con los algoritmos en los sensores, donde para el caso del mayor consumo es aproximadamente 3 veces menor que el nivel seguridad con menor consumo de memoria en la estación base.

5.4.4 Resultados de CU3

La generación de las llaves de usuario son parte del sistema y está a cargo de una autoridad de confianza. Como parte de la experimentación en este caso de uso, se midió el tiempo de ejecución que le toma al algoritmo DET-ABE generar llaves con niveles de seguridad de 128 y 192 bits con enfoque simétrico y de 128, 192 y 256 bits con enfoque asimétrico. Estas configuraciones del algoritmo aplicando 4, 8 y 16 atributos de un usuario en la llave de acceso.

En este experimento, al enfoque simétrico se le denomina con el prefijo *A* y al enfoque asimétrico con el prefijo *F*, seguido del nivel de seguridad que se midió. En la Figura 5.14 se observa el comportamiento de ambos enfoques al generar las llaves de acceso con 4, 8 y 16 atributos.

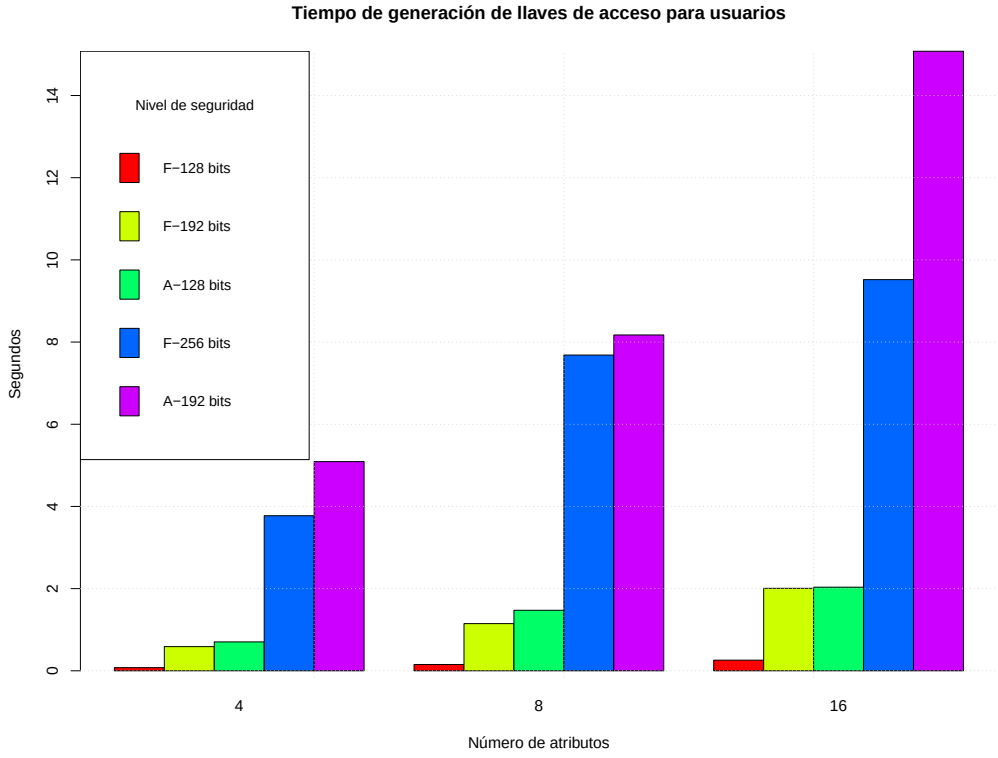

Figura 5.14: Tiempo de generación de llaves de acceso.

En la Figura 5.14 se observa que el enfoque simétrico demanda mayor tiempo de ejecución a diferencia del asimétrico, incluso cuando se compara con el nivel de seguridad de 256 bits. El comportamiento observado, respecto al incremento del tiempo por el número de atributos que se agrega a la llave, es el esperado debido a linealidad del número de atributos y al costo que éstos demandan. Si se observa cada enfoque con los niveles de seguridad por separado, cada uno de ellos tiene un comportamiento lineal, excepto el enfoque A-192 cuyo comportamiento es exponencial.

Después de que un usuario obtiene su llave de acceso, en cualquier momento podría acceder a los datos que tiene permitido. A este proceso se le llama descifrado de los datos. En la Figura 5.15

se puede observar el tiempo que le tomaría a un usuario acceder a los datos en diferentes niveles de seguridad y con una política de control de acceso con diferentes números de atributos.

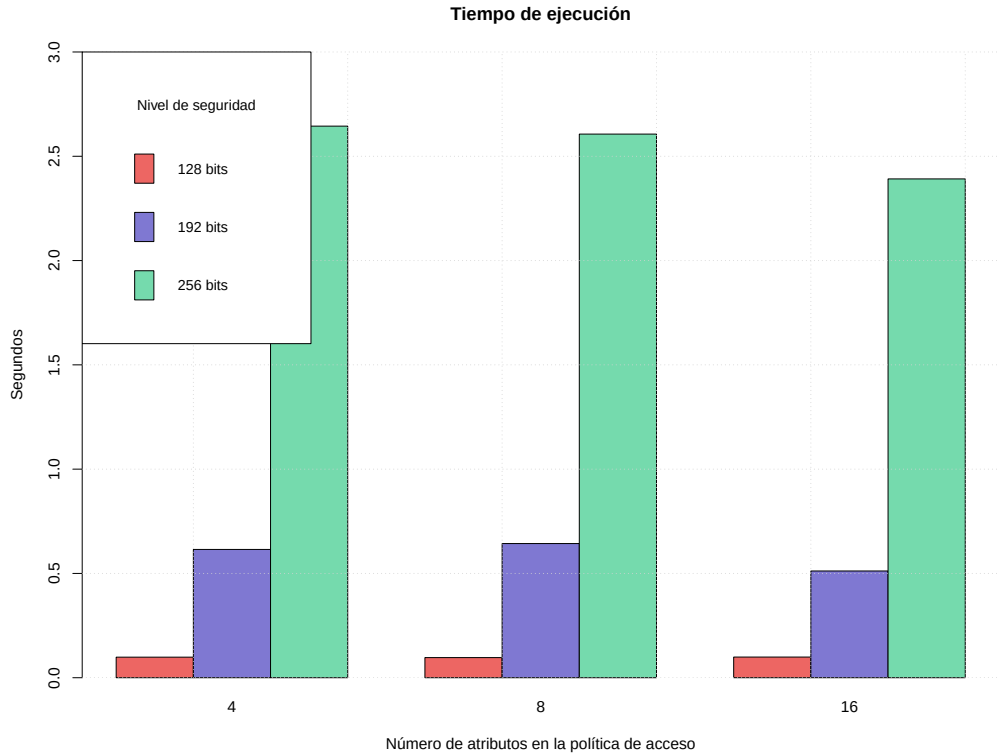

Figura 5.15: Tiempo de acceso a los datos por parte de un usuario.

En la Figura 5.15 se observa un comportamiento muy similar al observado en la Figura 5.12 en cuanto a la relación entre los niveles de seguridad para el cifrado con DET-ABE. Sin embargo, el tiempo que se tarda en descifrar los datos es mucho menor al tiempo que se tarda en cifrarlos. Esto se puede corroborar al observar el tiempo máximo con nivel de seguridad de 256 bits en el descifrado es la mitad del menor tiempo con nivel de seguridad de 128 bits en el cifrado de los datos. El comportamiento observado tanto en la Figura 5.12 como en la Figura 5.15 es el esperado, debido a que conforme aumenta el nivel de seguridad, los algoritmos utilizados emplean más rondas de procesamiento lo que se traduce en una demanda de tiempo mayor.

5.5 Resumen

En este capítulo se implementó el prototipo de WBAN segura, describiendo los dispositivos utilizados y se validó y evaluó su factibilidad al garantizar servicios de seguridad mediante algoritmos de criptografía ligera. Los dispositivos son diferentes, cada uno con un lenguaje de programación distinto, por ende, los resultados son variables. Sin embargo, a lo largo de toda la evaluación de los servicios de seguridad, el servicio con mejor desempeño fue la confidencialidad dado que obtuvo un tiempo de ejecución menor en los experimentos.

6

Conclusiones y trabajo futuro

En esta tesis se propuso un modelo de WBAN segura basada en 3 capas. En cada una de las capas del modelo de WBAN segura se garantizan servicios de seguridad mediante algoritmos de criptografía ligera. Mediante una evaluación entre dos suites de algoritmos criptográficos ligeros y con base en la literatura se seleccionaron los algoritmos. Se evaluó el desempeño de los algoritmos criptográficos ligeros mediante casos de uso en una WBAN segura.

Durante la realización de los experimentos se observó un patrón presente en los resultados. Este patrón es el servicio de confidencialidad el cual requiere menos tiempo de procesamiento. Este fenómeno se repitió en los resultados presentados, incluso cuando se utilizó la segunda suite de algoritmos. Esto se pude observar en las Figuras 5.10 y 5.11. El desempeño de la confidencialidad se vio reflejado en los tres nodos sensores que conformaron la WBAN.

Además, la tendencia a la uniformidad del consumo de la memoria también se hizo presente en las experimentaciones, excepto en la experimentación del CU2 donde se puede observar la gestión de memoria que realiza Java, proporcionando solamente lo necesario en cada proceso. Sobresale que

a pesar de una distribución que tiende a ser uniforme en el consumo de memoria de los sensores, el sensor de temperatura es el que consume hasta un 99 % menos memoria a diferencia de los otros dos.

Durante el desarrollo de la tesis se han cumplido los objetivos particulares propuestos en el Capítulo 1. El primero se cumplió al definir un modelo de WBAN segura, permitiendo la garantizar servicios de seguridad requeridos en una WBAN. El segundo objetivo que se cumplió fue la construcción de un prototipo de WBAN segura donde se incluyeron algoritmos de criptografía ligera para garantizar cada uno de los servicios de seguridad. Finalmente, con las experimentaciones realizadas y presentadas en el Capítulo 5 para los casos de uso de una WBAN segura, se cumplió el tercer objetivo al evaluar el impacto que genera cada algoritmo criptográfico y cada servicio de seguridad, con diferentes niveles de seguridad en una WBAN. Además se realizó una comparación entre dos suites de algoritmos de criptografía ligera para comprobar bajo las mismas condiciones, cuáles algoritmos de criptografía ligera tienen mejores prestaciones.

Una WBAN segura demanda recursos computacionales adicionales a los que utiliza sin seguridad. Sin embargo, el costo es asumible si se toma en cuenta la tasa de datos reportado en la literatura, dado que en una WBAN segura se alcanza una tasa de datos superior a lo reportado en la literatura. Además, la WBAN segura se ajusta a las necesidades y recursos disponibles, es decir, no necesariamente se requerirá garantizar todos los servicios de seguridad para una solución específica. Garantizando al menos un servicio de seguridad, los datos se pueden mantener seguros. Esto hace que la solución sea flexible a los recursos computacionales disponibles en un entorno WBAN. Adicionalmente, los algoritmos de criptografía ligera utilizados para garantizar servicios de seguridad no están forzosamente ligados; esto quiere decir que si en un futuro se publican nuevos algoritmos que tienen un mejor desempeño que los propuestos en esta tesis, se podrán intercambiar y, además, mejorar en rendimiento de la WBAN segura.

Al concluir esta tesis, se comprobó que para que una WBAN segura funcione correctamente y con el mejor desempeño posible, es necesario que tanto la arquitectura de red que incluye topología

y tecnologías de comunicación, como las implementaciones de los algoritmos criptográficos ligeros debe realizar con las herramientas que proporcionen la mejor gestión de los recursos disponibles.

Como trabajo futuro se proponen los siguientes puntos:

- Explorar el desempeño en WBAN seguras de los algoritmos criptográficos ligeros seleccionados como estándar en criptografía ligera a cargo de NIST.
- Determinar dispositivos sensores con mejores prestaciones en recursos computacionales que no afecten el desempeño de los algoritmos criptográficos ligeros implementados.
- Utilizar tecnologías de comunicación más recientes que demuestren tener un mejor desempeño en transferencia de datos y que se incluyan en dispositivos sensores.

6.1 Limitaciones

En este trabajo de tesis se diseñó y creó un prototipo de WBAN segura donde se estudió la factibilidad de implementar servicios de seguridad en cada una de las capas de la WBAN. Las limitaciones encontradas son las siguientes:

- Trabajar con diferentes lenguajes de programación tiene un grado de dificultad alto debido a los diferentes tipos de datos manejados en cada lenguaje.
- El sistema web implementado se enfocó en la generación de llaves de usarios por parte de una autoridad de confianza y el almacenamiento de los datos recolectados por los sensores. El acceso de los datos se hizo directa y no visual en el sistema web.

Bibliografía

[1] Agha, D. e., Khan, F. H., Shams, R., Rizvi, H. H., and Qazi, F. (2018). A Secure Crypto Base Authentication and Communication Suite in Wireless Body Area Network (WBAN) for IoT Applications. *Wireless Personal Communications*, 103(4):2877–2890.

[2] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., and Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*, 18(2):113–122.

[3] Al-Sarawi, S., Anbar, M., Alieyan, K., and Alzubaidi, M. (2017). Internet of Things (IoT) communication protocols: Review. In *ICIT 2017 - 8th International Conference on Information Technology, Proceedings*, pages 685–690. Institute of Electrical and Electronics Engineers Inc.

[4] Alaba, F. A., Othman, M., Hashem, I. A. T., and Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88:10–28.

[5] Alam, M. M. and Hamida, E. B. (2014). Surveying wearable human assistive technology for life and safety critical applications: Standards, challenges and opportunities.

[6] Alshamsi, A. Z. and Barka, E. S. (2017). Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks. In *2017 International Conference on Informatics, Health & Technology (ICIHT)*, pages 1–7. IEEE.

[7] Arfaoui, A., Boudia, O. R. M., Kribeche, A., Senouci, S.-M., and Hamdi, M. (2019). Context-aware access control and anonymous authentication in WBAN. *Computers & Security*, page 101496.

[8] Asam, M., Jamal, T., Adeel, M., Hassan, A., Butt, S. A., Ajaz, A., and Gulzar, M. (2019). Challenges in wireless body area network. *International Journal of Advanced Computer Science and Applications*, 10(11):336–341.

[9] Ashton, K. (2009). That 'Internet of Things' Thing. *RFiD Journal*, 22:97–114.

[10] Aumasson, J.-P., Henzen, L., Meier, W., and Naya-Plasencia, M. (2013). Quark: A Lightweight Hash. *Journal of Cryptology*, 26(2):313–339.

[11] Ball, J. J. W., Dains, J. E., Flynn, J. A., Solomon, B. S., Stewart, R. W., and Ball, J. J. W. (2019). *Seidel's guide to physical examination : an interprofessional approach*. ELSEVIER, 9th edition.

[12] Barker, E. (2020). Recommendation for key management:. Technical report, National Institute of Standards and Technology, Gaithersburg, MD.

[13] Bellare, M., Bellare, M., Canetti, R., and Krawczyk, H. (1996). Keying hash functions for message authentication. 1109:1–15.

[14] Bhende, M., Wagh, S. J., and Utpat, A. (2014). A quick survey on wireless sensor networks. In *Proceedings - 2014 4th International Conference on Communication Systems and Network Technologies, CSNT 2014*, pages 160–167. IEEE Computer Society.

[15] Black, J. (2011). Authenticated Encryption. In *Encyclopedia of Cryptography and Security*, pages 52–61. Springer US.

[16] Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varıcı, K., and Verbauwhede, I. (2011). spongent: A Lightweight Hash Function. pages 312–325. Springer, Berlin, Heidelberg.

[17] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., and Vikkelsoe, C. (2007). PRESENT: An Ultra-Lightweight Block Cipher. In Paillier,

P. and Verbauwhede, I., editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, pages 450–466, Berlin, Heidelberg. Springer Berlin Heidelberg.

[18] Brekke, I. J., Puntervoll, L. H., Pedersen, P. B., Kellett, J., and Brabrand, M. (2019). The value of vital sign trends in predicting and monitoring clinical deterioration: A systematic review. *PLoS ONE*, 14(1).

[19] Chandrasekaran, B., Balakrishnan, R., and Nogami, Y. (2019). TF-CPABE: An efficient and secure data communication with policy updating in wireless body area networks. *ETRI Journal*.

[20] Chatterjee, S., Das, A. K., and Sing, J. K. (2014). A novel and efficient user access control scheme for wireless body area sensor networks. *Journal of King Saud University - Computer and Information Sciences*, 26(2):181–201.

[21] Chen, L. (2017). Cryptography Standards in Quantum Time: New wine in old wineskin? *IEEE security & privacy*, 15(4):51–57.

[22] Chenthara, S., Ahmed, K., Wang, H., and Whittaker, F. (2019). Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. *IEEE Access*, 7:74361–74382.

[23] Dhanvijay, M. M. and Patil, S. C. (2019). Internet of Things: A survey of enabling technologies in healthcare and its applications. *Computer Networks*, 153:113–131.

[24] Díaz, C. (2017). ¿Qué es la salud electrónica ("e-Salud")? *Cátedra Conacyt - Infotec*.

[25] Diez, F. P., Touceda, D. S., Cámara, J. M. S., and Zeadally, S. (2019). Lightweight Access Control System for Wearable Devices. *IT Professional*, 21(1):50–58.

[26] Dworkin, M. J. (2001). FIPS 197, Advanced Encryption Standard (AES). *Network Security, National Institute of Standards and Technology*, 197(12):6028.

[27] Ghaboosi, K., Xiao, Y., and Robertson, J. J. (2008). Overview of IEEE 802.15.1 Medium Access Control and Physical Layers. In *Emerging Wireless LANs, Wireless PANs, and Wireless MANs: IEEE 802.11, IEEE 802.15, 802.16 Wireless Standard Family*, pages 105–134. John Wiley & Sons, Inc.

[28] Guo, J., Peyrin, T., and Poschmann, A. (2011). The PHOTON Family of Lightweight Hash Functions. pages 222–239. Springer, Berlin, Heidelberg.

[29] Hassan, M., Katangur, A., and Kar, D. (2017). A secure body sensor network architecture with CP-ABE based fine-grained data access control. In *ACM International Conference Proceeding Series*. Association for Computing Machinery.

[30] Hong, D., Lee, J.-K., Kim, D.-C., Kwon, D., Ryu, K. H., and Lee, D.-G. (2014). LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. pages 3–27. Springer, Cham.

[31] Hong, J., Liu, B., Sun, Q., and Li, F. (2019). A combined public-key scheme in the case of attribute-based for wireless body area networks. *Wireless Networks*, 25(2):845–859.

[32] Javadi, S. S. and Razzaque, M. A. (2013). Security and Privacy in Wireless Body Area Networks for Health Care Applications. In Khan, S. and Khan Pathan, A.-S., editors, *Wireless Networks and Security: Issues, Challenges and Research Trends*, pages 165–187. Springer Berlin Heidelberg, Berlin, Heidelberg.

[33] K., J. and Desai, A. (2016). IoT: Networking Technologies and Research Challenges. *International Journal of Computer Applications*, 154(7):1–6.

[34] Karapistoli, E., Pavlidou, F. N., Gragopoulos, I., and Tsetsinas, I. (2010). An overview of the IEEE 802.15.4a Standard. *IEEE Communications Magazine*, 48(1):47–53.

[35] Krawczyk, H., Canetti, R., and Bellare, M. (1997). HMAC: Keyed-Hashing for Message Authentication.

[36] Kumar, A., Srivastava, V., Singh, K., and Hancke, G. P. (2015). Current Status of the IEEE 1451 Standard-Based Sensor Applications. *IEEE Sensors Journal*, 15:2505–2513.

[37] Kumar, N. R., Harish, S. S., Poovarasan R, and Jagadish D (2017). A Comparative Analysis of Symmetric and Asymmetric Key Cryptography. *International Research Journal of Engineering and Technology*, pages 375–377.

[38] Kwak, K. S., Ullah, S., and Ullah, N. (2010). An overview of IEEE 802.15.6 standard. In *2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)*, pages 1–6. IEEE.

[39] Lara-Nino, C. A., Diaz-Perez, A., and Morales-Sandoval, M. (2018). Elliptic Curve Lightweight Cryptography: A Survey. *IEEE Access*, 6:72514–72550.

[40] Luykx, A., Preneel, B., Tischhauser, E., and Yasuda, K. (2016). A MAC Mode for Lightweight Block Ciphers. pages 43–59. Springer, Berlin, Heidelberg.

[41] Manayankath, S., Srinivasan, C., Sethumadhavan, M., and Megha Mukundan, P. (2016). Hash-One: a lightweight cryptographic hash function. *IET Information Security*, 10(5):225–231.

[42] Masdari, M. and Ahmadzadeh, S. (2016). Comprehensive analysis of the authentication methods in wireless body area networks. *Security and Communication Networks*, 9(17):4777–4803.

[43] Mavroeidis, V., Vishi, K., Zych, M. D., and Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *arXiv e-prints*, page arXiv:1804.00200.

[44] Mazinga, A. and Mukonyezi, I. (2017). A Survey on Wireless Sensor Networks.

[45] McKay, K. A., Bassham, L., Turan, M. S., and Mouha, N. (2017). Report on lightweight cryptography. Technical report, National Institute of Standards and Technology, Gaithersburg, MD.

[46] Menezes, A. and Menezes, A. (2005). An introduction to pairing-based cryptography.

[47] Miret, J. M., Sadornil, D., and Tena, J. G. (2018). Pairing-Based Cryptography on Elliptic Curves. *Mathematics in Computer Science*, 12(3):309–318.

[48] Mok, W. Q., Wang, W., and Liaw, S. Y. (2015). Vital signs monitoring to detect patient deterioration: An integrative literature review. *International Journal of Nursing Practice*, 21:91–98.

[49] Morales-Sandoval, M., Gonzalez-Compean, J. L., Diaz-Perez, A., and Sosa-Sosa, V. J. (2018). A pairing-based cryptographic approach for data security in the cloud. *International Journal of Information Security*, 17(4):441–461.

[50] Naik, M. R. K. and Samundiswary, P. (2016). Wireless body area network security issues — Survey. In *2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, pages 190–194.

[51] Narmadha, T., Kalaiarasi, M., and Meenakshi, M. (2018). Lightweight secure ECG transmission in wireless body area networks - PRESENT cipher based implementation. In *Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, ICCSP 2017*, volume 2018-January, pages 1066–1070. Institute of Electrical and Electronics Engineers Inc.

[52] Picazo-Sanchez, P., Tapiador, J. E., Peris-Lopez, P., and Suarez-Tangi, G. (2014). Secure publish-subscribe protocols for heterogeneous medical wireless body area networks. *Sensors (Switzerland)*, 14(12):22619–22642.

[53] Polai, M., Mohanty, S., and Sahoo, S. S. (2019). A Lightweight Mutual Authentication Protocol for Wireless Body Area Network. In *2019 6th International Conference on Signal Processing and Integrated Networks, SPIN 2019*, pages 760–765. Institute of Electrical and Electronics Engineers Inc.

[54] Ranea, A. (2016). *Curvas Elípticas en Criptografía*. PhD thesis, Universidad de Granada.

[55] Reyes Cruz, L. A. (2017). *Análisis del impacto del número de usuarios y tasa de datos ofrecida en el traspaso entre resumideros de una WBAN/WPAN enfocada a aplicaciones de sistemas del cuidado de la salud*. PhD thesis, Centro de Investigación Científica y de Educación Superior de Ensenada, Baja California.

[56] Rotger, L. H., Coma, J. R., and Tena-Ayuso, J. G. (2012). Criptografía con curvas elípticas. Technical report, Universitat Oberta de Catalunya, España.

[57] Roy, M., Chowdhury, C., and Aslam, N. (2019). Security and privacy issues in wireless sensor and body area networks. In *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, pages 173–200. Springer International Publishing.

[58] Saleem, S., Ullah, S., and Yoo, H. (2009). On the Security Issues in Wireless Body Area Networks. *JDCTA*, 3:178–184.

[59] Salehi, S. A., Razzaque, M. A., Tomeo-Reyes, I., and Hussain, N. (2016). IEEE 802.15.6 standard in wireless body area networks from a healthcare point of view. In *Proceedings - Asia-Pacific Conference on Communications, APCC 2016*, pages 523–528. Institute of Electrical and Electronics Engineers Inc.

[60] Salman, T. and Jain, R. (2015). Networking protocols and standards for internet of things. *Internet of Things and Data Analytics Handbook (2015)*, 7.

[61] Sayed, A. and Kamal, M. (2017). *Internet of Things Applications, Challenges and Related Future Technologies*.

[62] Shah, A. and Engineer, M. (2019). A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications: Proceedings of ICSICCS-2018. pages 283–293.

[63] Shihong, Z., Yanhong, X., Honggang, W., Zhouzhou, L., Shanzhi, C., and Bo, H. (2017). A Survey on Secure Wireless Body Area Networks. *Security and Communication Networks*, 2017:9.

[64] Shikha, P. and Naveen, B. (2014). Security Issues in Wireless Body Area Network. *International Journal of Computer Science and Mobile Computing*, 3(4):1171–1178.

[65] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and Iwata, T. (2007). The 128-Bit Blockcipher CLEFIA (Extended Abstract). pages 181–195. Springer, Berlin, Heidelberg.

[66] Shu, M., Yuan, D., Zhang, C., Wang, Y., and Chen, C. (2015). A MAC protocol for medical monitoring applications of wireless body area networks. *Sensors (Switzerland)*, 15(6):12906–12931.

[67] Singh, S., Sharma, P. K., Moon, S. Y., and Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*.

[68] Siva, K. R. and Venkateswari, R. (2019). Security Challenges and Solutions for Wireless Body Area Networks. pages 275–283. Springer, Singapore.

[69] Song, E. Y. and Lee, K. B. (2010). IEEE 1451.5 standard-based wireless sensor networks. In *Lecture Notes in Electrical Engineering*, volume 64 LNEE, pages 243–271.

[70] Su, X., Li, C., and Yuan, X. (2017). IEEE 802.15.6-based Prototype System for WBAN: Design and Implementation.

[71] Turan, M. S., McKay, K. A., Çalık, , Chang, D., and Bassham, L. (2019). Status report on the first round of the NIST lightweight cryptography standardization process. Technical report, National Institute of Standards and Technology, Gaithersburg, MD.

[72] Usman, M., Asghar, M. R., Ansari, I. S., and Qaraqe, M. (2018). Security in Wireless Body Area Networks: From In-Body to Off-Body Communications. *IEEE Access*, 6:58064–58074.

[73] Villegas González, J., Villegas Arenas, A., and Villegas González, V. (2012). Semiología de los signos vitales: Una mirada novedosa a un problema vigente. Technical Report 2.

[74] WHO (2016). Global diffusion of eHealth: Making universal health coverage achievable. Technical report.