Protocolos para la seguridad de la información en eHealth

Criptografía en entornos mHeath

Alexandra Rivero García

Departamento de Ingeniería Informática y de Sistemas
Universidad de La Laguna

Memoria para la obtención del grado de
Doctor en Ingeniería Informática

Directora: Dra. Candelaria Hernández Goya

Codirectora: Dra. Pino Caballero Gil

Agosto 2020

Agradecimientos

Me gustaría dar las gracias por el apoyo en estos años a mi Madre, es la persona más increíble que conozco, a mi hermano, que es mi persona favorita y a Iván, mi compañero de batallas y de vida.

Gracias también a Cande y a Pino, no podía tener mejores directoras de Tesis y a los integrantes de ese grupo de investigación llamado Cryptull. La humildad, el esfuerzo y el trabajo constante han sido los pilares para esta tesis.

Muchos momentos vividos, desde ese inicio con Paco ganando concursos, pasando por el hombre semáforo, la llegada de Jonay hasta la invasión de los palmeros con Jose, Josué y mi querida Nay. Existen personas con las que tienes una conexión en la que las palabras no son necesarias, y con ella me pasa. ¡Plancton power! Marisa, Óscar y Jesús... cuánto no pasamos juntos al final, cuantas complicidades surgieron con personas que viven al otro lado del mapa. Rafael, ¡gracias a ti también!, que gran apoyo has sido sin saberlo. A ustedes amigas, que han sido un apoyo en todo este tiempo: Tati, Mar, Chloe, Yodra e Isa.

Abuela Esther, abuelo Fefe, abuelo Manolo, abuela Teresa esto es por ustedes.

Resumen

El avance de la tecnología ha traído consigo la evolución de herramientas en diversos ámbitos, entre ellos destaca el de la medicina. La medicina actual posee unas herramientas que hace 30 años eran impensables, lo que hace que su funcionamiento sea completamente diferente. Gracias a esta fusión de medicina y tecnología encontramos en nuestro día a día nuevos términos, como eHealth o mHealth, que hacen referencia a esta simbiosis, en la que se benefician tanto los usuarios, como todas las áreas que trabajan en la protección y actuación de la salud y seguridad de las mismas. En esta tesis doctoral se ha trabajado en varias líneas con el objetivo de mejorar la seguridad de la información en varios sistemas mHealth intentando que las soluciones propuestas sean extrapolables a otros entornos. En primer lugar se propone una herramienta destinada al diagnóstico, tratamiento y monitorización de niños con trastorno de déficit de atención que se apoya en un sistema experto y usa cifrado basado en identidad para la protección de la información de los pacientes. En segundo lugar, se incluye una solución centrada en aportar mejoras en dos de los problemas fundamentales de la seguridad de la información de los datos médicos: la gestión segura de la información de los pacientes y la identificación de los mismos dentro del entorno hospitalario. La solución planteada para el problema de identificación se basa en la utilización de pulseras NFC que almacenan un identificador asociado al paciente y que es generado a través de una función HMAC. En el tercer trabajo se analiza de nuevo el problema de identificación de las personas pero esta vez en entornos de emergencia en los que no se cuenta con redes de comunicaciones estables. Además se propone un sistema de clasificación de víctimas en dichos entornos cuyo objetivo es mejorar la gestión de recursos sanitarios en estos escenarios. Como cuarta aportación se presenta un sistema de mejora de la trazabilidad y de la gestión de pequeñas emergencias y eventos cotidianos basada en el uso de blockchain. Para terminar con las aportaciones de esta tesis, se presenta un esquema criptográfico que mejora los esquemas actuales de seguridad utilizados para dispositivos del entorno sanitario que poseen poca capacidad computacional.

La finalidad general perseguida en esta tesis es aportar mejoras al uso de la medicina actual a través de sistemas mHealth en los que se presta especial atención a la seguridad de la información. Concretamente se incluyen medidas para la protección

de la integridad de los datos, identificación de personas, autenticación y no repudio de la información.

La realización de esta tesis doctoral ha contando con financiación del Gobierno de Canarias a través de una beca predoctoral FPI.

Abstract

The advance of technology has brought with it the evolution of tools in various fields, among which the medical field stands out. Today's medicine has tools that 30 years ago were unthinkable making its functioning completely different. Thanks to this fusion of medicine and technology new terms concerning this symbiosis, such as eHealth or mHealth, may be found in our daily lives. Both users and all the areas that work in the protection and performance of health and safety benefit from it. In this doctoral thesis we have worked in several lines with the aim of improving information security in several mHealth systems trying to make the proposed solutions extrapolable to other environments. Firstly, a tool, supported by an expert system and using identity-based encryption for the protection of patient information, for the diagnosis, treatment and monitoring of children with attention deficit disorder is proposed. Second, a solution focused on geared towards enhancing solutions for two of the fundamental problems of medical data information security: the secure management of patient information and the identification of patients within the hospital environment, is included. The solution proposed for the identification problem is based on the use of NFC bracelets that store an identifier associated with the patient and is generated through an HMAC function. In the third work, the problem of identification is again analyzed, but this time in emergency environments where no stable communication networks are present. It also proposes a system for the classification of victims whose objective is to improve the management of health resources in these scenarios. The fourth contribution is a system for improving the traceability and management of small emergencies and everyday events based on the use of blockchains. To conclude with the contributions of this thesis, a cryptographic scheme which improves security in healthcare devices with little computing capacity is presented.

The general aim of this thesis is providing improvements in current medicine through mHealth systems, paying special attention to information security. Specifically, measures for the protection of data integrity, identification, authentication and non-repudiation of information are included.

The completion of this doctoral thesis has been funded through a pre-doctoral FPI grant from the Canary Islands Government.

Índice general

Índice de figuras

Índice de cuadros

Capítulo 1

mHealth: gestión y protección de los datos de salud

La rápida evolución de la sociedad de la información es consecuencia de la proliferación de nuevas tecnologías y de su aplicación en diversos ámbitos. Este avance ha impulsado la mejora de las Tecnologías de la Información y la Comunicación (TICs). El uso intensivo de tecnologías móviles en los últimos años ha jugado uno de los papeles principales en este progreso proporcionando aportaciones novedosas en múltiples escenarios.

Uno de esos escenarios es el de la medicina y más concretamente, la gestión y atención al paciente. La integración de las nuevas tecnologías en el manejo de los datos médicos y la atención de pacientes ha permitido el desarrollo de diversas herramientas tecnológicas; son muchas las áreas en las que se ha integrado el uso de tecnologías en el ámbito sanitario, valgan como ejemplo: la identificación de pacientes, el registro de actividades médicas y de salud de los pacientes (diagnóstico y tratamiento), la organización y coordinación del personal sanitario.

La aparición de Internet en la época de los 90s trajo consigo la acuñación de una gran cantidad de e-términos, como por ejemplo: e-commerce, e-mail, etc. La aparición del término eHealth (eSalud) [32] corresponde al uso de las TICs para mejorar el sistema sanitario y la atención de la salud (health en inglés).

Actualmente eHealth es un término ampliamente reconocido que hace referencia a todos los aspectos que pueden afectar al cuidado de la salud. Por un lado, incluye los elementos directamente relacionados con los pacientes, como puede ser su seguimiento y diagnóstico, como también el intento de mejorar aspectos relevantes para los profesionales de la salud: acceso a la historia clínica, prescripción de recetas electrónicas, tratamiento y monitorización de los pacientes e incluso la propia formación de los profesionales de la salud.

Como se comentaba con anterioridad, la irrupción masiva del uso de los dispositivos móviles ha afectado a múltiples áreas, concretamente en el ámbito eHealth, ha potenciado su abanico de posibilidades. El término mHealth [26] ha surgido con el fin de identificar el uso de eHealth apoyado en la tecnología móvil.

La sinergia surgida de la fusión de las TICs y la medicina permiten una práctica diferente de la misma, incrementando aspectos tales como su productividad, precisión y eficiencia, tanto a nivel del tratamiento de patologías médicas como de gestión de los datos médicos. Un avance significativo que conlleva la adopción de métodos y herramientas basados en mHealth es la generación de una interacción entre paciente y médico que supera las barreras geográficas y temporales. También acorta los tiempos de espera, evitando desplazamientos e incluso permitiendo el diagnóstico y tratamiento a distancia (telemedicina), mejorando además los procesos de gestión de los datos de los pacientes, haciendo posible un acceso ubicuo desde cualquier lugar o centro médico. Esta ubicuidad de los datos fomenta la transparencia de los mismos, tanto a nivel de paciente permitiendo el acceso a su propia historia clínica, como a nivel de la información a la que el personal sanitario tiene acceso.

Todas estas mejoras ayudan y promueven que la práctica médica pueda ser desarrollada en cualquier lugar donde se requiera: centros hospitalarios, puestos sanitarios, en la vía pública, el hogar, centros recreativos, escuelas, lugares de trabajo, etc

Dadas las características de los datos a gestionar en el entorno sanitario y a la normativa que regula el acceso a los mismos, cualquier proceso soportado por el uso de las TICs en medicina debe realizarse teniendo en cuenta un aspecto fundamental, la inclusión de servicios de seguridad de la información.

Gracias a la Ley Orgánica de protección de datos, nuestra historia clínica es considerada un elemento de carácter privado. La legislación publicada en el Boletín Oficial del Estado (BOE-A-2018-16673, número 294) [45], por la que se aprueba el Reglamento de desarrollo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de carácter personal recoge que estos datos son especialmente sensibles. Concretamente ampara todos los datos de los individuos que hagan referencia a la salud física o mental de las personas sin tener restricción de tiempo, es decir, de forma presente, futura o incluso pasada.

Toda esta información debe ser confidencial y todo acceso a la misma debe ser autorizado de forma legal. No sólo esto, además se debe garantizar en todo momento tanto la intimidad personal, como la familiar del paciente. Todo personal sanitario que acceda a los datos del paciente debe de estar advertido de estas políticas, para que puedan actuar en consecuencia, de tal forma que se garanticen los derechos del mismo.

La protección de esta información se considera un valor ético y jurídico amparado por la propia Constitución Española, requiriendo su cumplimiento por parte de cual-

quier profesional sanitario. Es por esto que la seguridad de los datos tratados en este entorno es fundamental para cualquier sistema eHealth o mHealth.

Existe una clasificación sobre los tipos de datos de la salud que se pueden encontrar en los sistemas eHealth [76]. A continuación se describen cada uno de ellos para poder entender el contexto en el que se engloban los sistemas sanitarios actuales.

Registros de salud universales (Universal Health Records, UHR), este término hace referencia al conjunto que aglutina todos los datos que guardan alguna relación con el paciente [75]. Esta es toda la información que posee un médico o un centro hospitalario para la atención del paciente. Dentro de este enorme conjunto de datos podemos distinguir tres subconjuntos, uno en el lado del paciente y otros dos en el lado del personal sanitario, los cuales están también asociados al paciente.

Registros de salud personales (Personal Health Records, PHR), son los datos que encontramos en el lado del paciente [1]. Concretamente este subconjunto de información hace referencia a todos los datos de las personas que puedan influir en menor o mayor medida en su vida cotidiana y en su salud. Es decir, se encuentran datos del tipo molestias o dolores del paciente en un momento concreto, el ejercicio físico que realiza a diario, tipo de ejercicio, la cantidad de pasos diarios o incluso las pulsaciones. Este subconjunto puede ser compartido o no con el personal sanitario en algún momento concreto, pero aglutina tal cantidad de información que la mayor parte de las veces es imposible su registro completo, a menos que el paciente se encuentre bajo cuidado hospitalario y se le esté haciendo una monitorización continua. A partir de este subconjunto se generan los dos subconjuntos a los que el personal sanitario tiene acceso, los registros de la salud electrónicos y los registros médicos electrónicos.

Registros de la salud electrónicos (Electronic Health Recods, EHR), es el subconjunto formado por todos aquellos datos que se obtienen directamente del paciente, como pueden ser resultados de pruebas o analíticas [101].

Registros médicos electrónicos (Electronic Medical Records, EMR), este subconjunto de datos se relaciona con los EHR pero con un pequeño matiz, son las conjeturas que se han podido sacar de los EHR como diagnósticos e incluso tratamientos [19].

Información de la salud privada (Private Health Information, PHI), este conjunto de datos se refiere a aquellos que no se relacionan directamente con el estado del paciente, pero son básicos para cualquier interacción con los mismos. El grupo de PHI está formado por todos aquellos datos que posee el personal médico para poder contactar e identificar al paciente, como por ejemplo: DNI, nombre, apellido, foto, número de teléfono, identificadores biométricos, etc [83].

Para entender mejor todos los tipos de datos que existen en los esquemas de eHealth podemos observar un resumen de la clasificación que se ha explicado en los párrafos anteriores en la Figura 1.1.

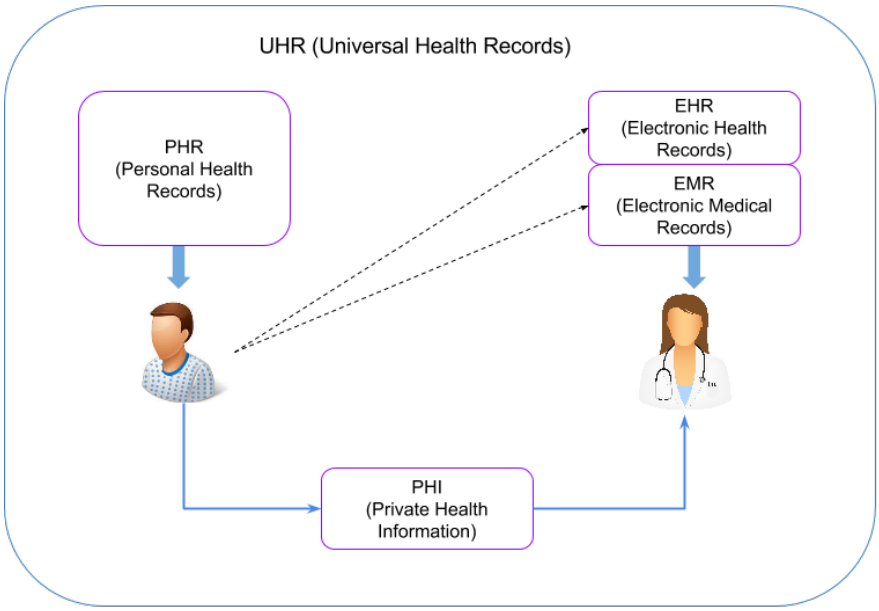


Figura 1.1 Esquema de los datos de la salud

Como se puede observar hay una gran cantidad de datos de la salud de diversa índole, mantener su seguridad es una tarea esencial regulada por ley pero nada trivial. La seguridad de estos datos se debe mantener bajo cualquier circunstancia, incluso en entornos extremos como pueden ser situaciones de emergencia en las que no se cuente con acceso a infraestructuras de comunicación o los recursos sean limitados. Esta cuestión se aborda en las aportaciones [72] y [70].

Igualmente se debe garantizar la seguridad de los dispositivos que rodean a las personas en el ámbito de la salud aunque posean limitaciones de batería o de baja capacidad de cómputo. En las aportaciones [74] y [71] se trata esta cuestión.

Esta tesis plantea la necesidad de entender la seguridad de la información como uno de los pilares en el diseño y desarrollo de sistemas eHealth.

Capítulo 2

Fundamentos tecnológicos y primitivas criptográficas

En primer lugar se presenta el concepto de Internet de las cosas, aspecto fundamental en el desarrollo de esta tesis. Se hará hincapié en la utilización dispositivos en el entorno de la salud, prestando especial atención a los dispositivos de baja capacidad computacional y a los dispositivos médicos implantables. Se realizará un análisis de las tecnologías de comunicación utilizadas en el desarrollo de las soluciones propuestas. Además, se incluyen algunos principios y primitivas criptográficas necesarias para poder evaluar el funcionamiento de las aportaciones presentadas.

2.1. Internet de las cosas

El concepto de Internet de las Cosas (IoT, Internet of Things) surge hace algunos años con la idea de englobar todo el fenómeno de gadgets y tecnología que nos rodea actualmente. Concretamente, se puede definir como una red compleja que es resiliente, adaptable y auto configurada que interconecta diversos dispositivos a la red de Internet mediante la utilización de estándares de comunicación. Su definición formal la podemos encontrar en [61]. Allí se profundiza en los conceptos relacionados con la identificación inequívoca de los dispositivos que componen la red, su localización y su estatus. El objetivo final de la IoT es lograr la interconectividad omnipresente de todo nuestro entorno persiguiendo expandir la capacidad de acceso a la información en "cualquier momento", en "cualquier lugar" y a "cualquier cosa" [20].

No se puede hablar de IoT sin hacer referencia a la cantidad de datos que genera y que requieren ser gestionados. Gracias a la flexibilidad de las capacidades de comunicación que tienen asociadas, ha aumentado de forma exponencial la cantidad de datos que se pueden crear, recopilar y transmitir.

Según un informe de la organización noruega de investigación SINTEF [84], en los últimos dos años el 90 % de los datos generados en el mundo se han creado con un ritmo de más de 205.000GB/s [42], lo que implica que cada día creamos una cantidad ingente de datos a un ritmo desenfrenado. No sólo esto, según otro estudio realizado por la empresa americana Gartner [34], a finales del año 2020 tendremos en el mundo mas de 25.000 dispositivos IoT conectados. La predicción es que se facilitará la recogida de datos, el análisis de los mismos, su pre-planificación, su gestión y hasta la toma de decisiones inteligentes de forma autónoma.

Los nodos finales de la IoT, no sólo son los encargados de la recogida de datos, su característica más importante es que tienen capacidad de comunicación con su entorno. Se pueden representar como fuentes de datos que pueden alimentar servidores en el backend. Todos los dispositivos autónomos que tengan esta capacidad de comunicación, como los relojes inteligentes, se engloban dentro del ámbito de la IoT; sin embargo, se suele relacionar más este término a grandes sistemas de comunicación de sensores, como pueden ser los que componen diferentes estaciones meteorológicas para controlar el estado de diferentes zonas de una ciudad.

Estos datos pueden ser también de índole sanitaria, de comercios menores y hasta pueden estar relacionados con las infraestructuras de transporte y del sector industrial.

Gracias a la extracción inteligente de información desde diferentes dispositivos, la IoT puede proporcionar servicios muy valiosos que pueden llegar a tener un impacto significativo en la producción social y en la vida de las personas.

El manejo de tanta información hace que la protección de los datos intercambiados sea una prioridad, como reflejan estudios realizados por en Centro Criptológico Nacional (CCN) [13]. El hecho de poseer cada día más interconexiones aumenta exponencialmente la dificultad de incluir herramientas eficientes y robustas para la protección de la información.

La arquitectura de IoT es bastante diversa, podemos encontrarnos sistemas que puede ser físicos, virtuales o híbridos. Además, generalmente están constituidos por un conjunto muy heterogéneo de elementos: dispositivos (sensores y actuadores principalmente), tecnologías de comunicación, servicios en la nube, protocolos específicos de la IoT, usuarios, desarrolladores e incluso una capa empresarial.

Seguidamente se incluye un apartado en el que se describe uno de los paradigmas más utilizados en la IoT, las redes de sensores. Se presta especial atención a las características y capacidades de los dispositivos que las forman ya que estas cuestiones afectan directamente a la hora de proponer soluciones de seguridad.

2.1.1. Dispositivos

Las redes de sensores (WSNs, Wireless Sensor Networks) [52] son una pieza fundamental dentro del desarrollo de la IoT. Sin embargo, su definición resulta compleja. Se

puede definir como el conjunto de sensores que envían información directamente a la infraestructura pública de Internet. Concretamente, una WSNs se genera mediante una serie de nodos que actúan como sensores conectados entre sí a través de comunicaciones inalámbricas, tal y como se describe en el artículo [31] .

Las redes de sensores son uno de los componentes claves de la IoT puesto que habilitan la interconexión de dispositivos con limitaciones importantes, ayudando así a su comunicación con objetos virtuales para la mejora de la gestión inteligente de la información y los recursos. Además, aportan soluciones de automatización de aplicaciones en entornos inteligentes.

Una de las principales características de estas redes es que suelen tener una estructura ad-hoc con una serie de componentes heterogéneos. Pueden estar formados entre otros, por nodos, actuando como sensores o como puerta de enlace, dispositivos móviles e incluso servidores, o bases de datos en la nube. Un despliegue típico de una red de sensores inalámbricos se compone de tres tipos de nodos: nodos de usuario (U), nodos de puerta de enlace conocidos también con el nombre de gateway, máster o pasarela (G), y nodos de sensores (S).

La arquitectura típica de las redes de sensores se basa en la conexión de varios dispositivos captadores de información con otro dispositivo que actúa como router o maestro del resto, el cual es el encargado de almacenar la información y enviarla a través de Internet. En este caso, la comunicación interna entre sensores y el nodo maestro junto con el envío de datos de este nodo a la nube se entiende como un sistema IoT.

Los sensores son los encargados de detectar o captar la información que les rodea, captan posibles eventos/cambios en los parámetros que miden, procesan los datos recogidos de su entorno y los envían a una pasarela. Es este nodo el que tiene el control de envío de los datos de los diferentes sensores.

Un ejemplo puede ser una estación meteorológica que monitoriza y envía información de variables climatológicas constantemente. En este caso, la información se envía de forma periódica a la nube, en la que estará el servidor encargado de procesar estos datos y representarlos a través de cualquier interfaz gráfica.

En las redes de sensores inalámbricos esta conexión a Internet no se realiza de forma directa, sino que poseen dispositivos específicos para conectarse con la nube y el resto de servicios de la IoT.

Los sensores pueden remitir las señales con la información de forma colectiva o ad-hoc; concretamente, en las redes de sensores heterogéneas (HWSNs, Heterogeneous Wireless Sensor Networks) [82] los sensores pueden tener bastantes restricciones de potencia, ancho de banda, recursos de memoria, conectividad o incluso alcance, denominándose dispositivos restringidos.

Dentro de las aplicaciones de las redes HWSN, los nodos gateway si suelen tener asociadas una capacidad mayor y más recursos.

Una de las principales preocupaciones en relación con estos sensores, y en particular las aplicaciones de las HWSN, es su vulnerabilidad a la explotación maliciosa.

En los dispositivos de la IoT el coste de incluir protección criptográfica puede afectar gravemente al rendimiento de los sensores. Es por ello, que la criptografía aplicada en estos dispositivos debe limitarse al uso de primitivas tales como funciones hash y operaciones basadas en clave simétrica, dado que tienen un coste computacional inferior a otras alternativas.

Dentro de los dispositivos de baja capacidad computacional, podemos encontrar unos cuyo funcionamiento es crítico dentro del entorno médico. Estos son los dispositivos médicos implantables (IMDs, Implantable Medical Devices), los cuales monitorizan y actúan sobre diversas condiciones fisiológicas de los pacientes que los utilizan. Dentro de este conjunto de dispositivos se incluyen: marcapasos, desfibriladores cardíacos implantables, sistemas de administración de medicamentos, neuro-estimuladores, etc. Estos dispositivos los utilizan millones de personas en su día a día para ayudar a controlar múltiples dolencias, como puede ser la arritmia cardíaca, la diabetes o incluso la enfermedad de Parkinson [2].

La penetración de los IMDs continúa creciendo, hay un estudio realizado en Estados Unidos que confirma que en ese país existen más de 25 millones de ciudadanos que actualmente dependen de ellos para sus funciones vitales [80]. El crecimiento se ve estimulado no sólo por la necesidad de atención geriátrica, sino también por la aparición de nuevas terapias para afecciones crónicas que van desde la diabetes pediátrica tipo 1 hasta la anorgasmia y otras disfunciones sexuales. Muchos de estos IMDs soportan la medición de diversas telemetrías y la monitorización remota de diversas características mediante enlaces inalámbricos de largo alcance y gran ancho de banda. Actualmente existen dispositivos IMDs que permiten la intercomunicación e interoperabilidad entre diferentes tipos de sensores de forma automática [36].

A pesar de todos estos avances en las tecnologías de los dispositivos médicos implantables, la seguridad y privacidad de los mismos sigue siendo limitada, llegando en algunos casos a afectar la propia seguridad médica y la eficacia del tratamiento. Los métodos establecidos para proporcionar seguridad no previenen por ejemplo, los fallos intencionados que pueden ser denominados ataques, basados en repetición o problemas de privacidad.

Equilibrar la seguridad y la privacidad con la eficacia de estos dispositivos es cada vez más importante y mucho más a medida que van evolucionando las tecnologías.

2.2. Tecnologías de comunicación inalámbrica.

La mayoría de propuestas incluidas en esta tesis requieren el uso de tecnologías inalámbricas para sustentar las implementaciones. Es por esto, que se incluye a continuación una pequeña introducción al estado actual de las tecnologías de este conjunto que han sido utilizadas en el desarrollo de esta tesis doctoral.

2.2.1. Near Field Communication.

Near Field Communication (NFC) [12] es una tecnología inalámbrica de alcance ultracorto que se puede entender como una extensión de la tecnología RFID (Radio Frequency IDentification) [51] cuya utilización actual está bastante extendida, sobretodo en el entorno de la tecnología móvil para la realización de pagos. Esta tecnología fue aprobada en 2003 como un estándar ISO (ISO 14443) y actualmente ya se utiliza de forma práctica en múltiples soluciones como llaves de hoteles o de vehículos, tarjetas de identificación, tickets electrónicos, tarjetas bancarias, etc.

A diferencia de otras tecnologías inalámbricas más conocidas como RFID, Bluetooth o Wi-Fi, NFC no está orientada a la transmisión de datos de forma continua y fluida. Se necesita que los dos dispositivos a interaccionar estén en contacto durante un instante, permitiendo el intercambio de información de una forma rápida y puntual. A grandes rasgos, esta tecnología puede verse como una combinación de RFID y tarjetas inteligentes sin contacto.

Podemos extraer como características principales de esta tecnología las siguientes:

- Funciona en la banda de 16.56 MHz, la cual es una frecuencia libre.
- Se basa en RFID, se puede entender como una extensión de esta.
- Tolera la transmisión de datos en diferentes velocidades 106 kbit/s, 212 kbit/s o 42 4kbit/s, según soporten los dispositivos.
- No está diseñada para la transferencia masiva de información.
- Permite la interacción entre dispositivos a menos de 10cm, en el que uno de los cuales puede funcionar de forma pasiva (tarjetas sin alimentación).
- Tecnología abierta y basada en estándares.
- Sencilla y segura. Basta con que el usuario acerque los dispositivos para establecer la comunicación y alejarlos para interrumpirla.

Aunque el factor distancia para transmitir información pueda parecer en un primer momento una limitación, realmente es la clave de esta tecnología. La necesidad de proximidad entre dispositivos limita el tipo de ataques a desarrollar.

Near Field Communication Forum o el NFC Forum [24] surgió para promover el uso de esta tecnología, mediante una serie de especificaciones que garantizan la interoperabilidad entre los diferentes dispositivos y servicios que utilicen NFC, además de mejorar la divulgación del uso de esta tecnología. Se formó en el año 2004 por tres compañías pioneras de esta tecnología: Philips, Sony y Nokia y actualmente cuenta con más de 170 miembros. Entre ellos se encuentran los principales fabricantes de dispositivos móviles, desarrolladores de aplicaciones, instituciones financieras, etc. Esta asociación sin ánimo de lucro intenta establecer un marco de trabajo adecuado para el desarrollo de aplicaciones interoperables y seguras e intentan marcar el camino por el que continuar investigando.

La utilización de esta tecnología en sistemas de pago e intercambio de datos hace que la seguridad se plantee como un objetivo crucial. Para ello se definen diferentes estándares enmarcadas en el ISO/IEC 180003 para el intercambio de datos entre dispositivos y para el almacenamiento de información en etiquetas. Las especificaciones propuestas por el NFC Forum son el referente que define el marco de trabajo para que los interesados en esta tecnología puedan crear y desarrollar productos. La creación de NFC Forum ha sido fundamental para la estandarización de la tecnología NFC y su gran aceptación en el mercado.

A continuación se describe con mayor detalle el funcionamiento de NFC, sus modos de comunicación, así como las ventajas de su utilización. Los dispositivos NFC pueden operar en dos modos diferentes al establecer la comunicación: modo activo y modo pasivo. Esto posibilita el despliegue de esta tecnología en muchos escenarios, con múltiples casos de uso.

- **Modo Activo.** Este modo se consigue cuando cada uno de los dispositivos que participa en el intercambio de información genera su propio campo electromagnético (emulando el paradigma de comunicación peer-to-peer), reconociéndose automáticamente. En la Figura 2.1 se muestra un ejemplo de funcionamiento de este modo de comunicación.

  Cabe puntualizar que para que un dispositivo pueda escuchar la respuesta de otro debe desactivar su campo electromagnético temporalmente. Además, se debe tener en cuenta que ambos participantes necesitan poseer una fuente de energía para generar este campo.

- **Modo Pasivo.** En este modo, sólo uno de los dispositivos genera el campo electromagnético, mediante su fuente de alimentación. Gracias a esta acción se puede iniciar la conexión que permitirá al dispositivo que está en modo pasivo aprovechar la energía del campo para alimentar su circuito, generar la señal de respuesta y así poder transferir los datos. Este modo de operación es el implementado por la tecnología RFID. El funcionamiento de este modo se describe en la Figura 2.2.

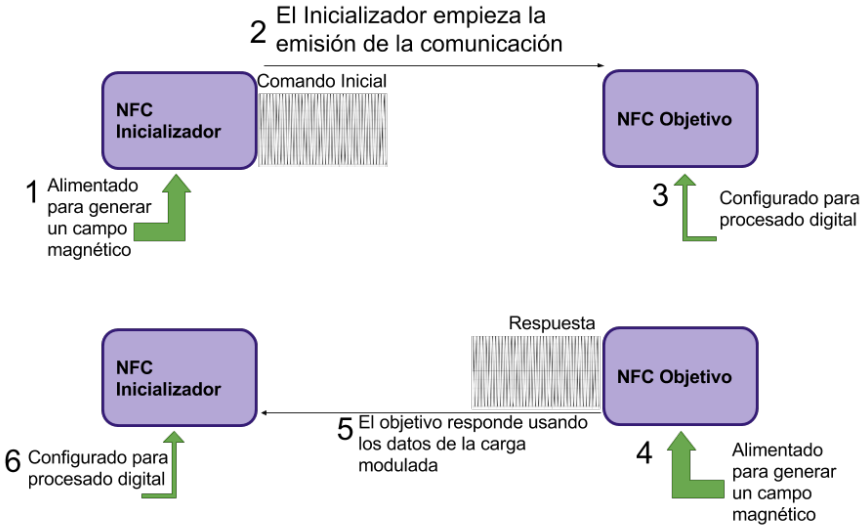


Figura 2.1 Comunicación activa en NFC

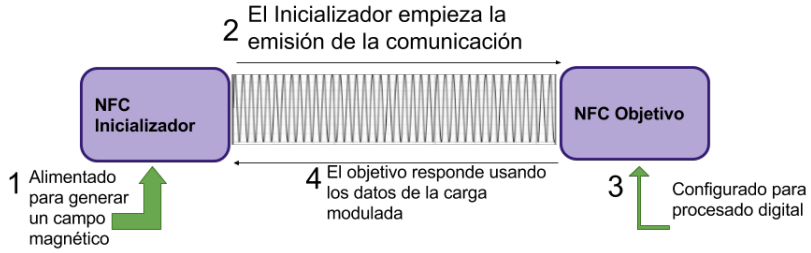


Figura 2.2 Comunicación pasiva en NFC

Cuadro 2.1 Comparación de etiquetas NFC

Chips	Estándar	Memoria	Velocidad	Coste
Tipo 1 [89]	ISO/IEC 14443-3 A [43]	96B - 2KB	106Kb/s	Bajo
Tipo 2 [90]	ISO/IEC 14443-3 A	48B - 2KB	106Kb/s	Bajo
Tipo 3 [91]	JIS X6319-4 [47]	2KB	212-424Kb/s	Alto
Tipo 4 [92]	ISO/IEC 14443-4 A/B	32KB	106-424Kb/s	Medio-Bajo
Tipo 5 [65]	ISO/IEC 15693 [44]	64KB	26,5Kb/s	Bajo

Existen tres configuraciones diferentes para utilizar NFC, característica que la diferencia de otras tecnologías inalámbricas. Estas son modo emulación de tarjeta inteligente, peer-to-peer y lectura/escritura de tarjeta. Por un lado, el modo emulación de tarjeta se utiliza para que cualquier dispositivo NFC pueda actuar como una tarjeta o etiqueta inteligente. Por otro lado, el modo peer-to-peer es el utilizado para el intercambio de datos entre los dispositivos NFC, puntualizando que siempre será poca cantidad de información. Se suele utilizar sobretodo para establecer los parámetros de configuración para el establecimiento de alguna comunicación inalámbrica con otra tecnología. Finalmente, el último modo de comunicación, el de lectura/escritura de tarjetas es el que permite a los dispositivos leer o escribir las etiquetas NFC.

Otro aspecto característico de la tecnología NFC es el uso de etiquetas, elementos pasivos que se pueden utilizar para almacenar información mediante cualquier dispositivo NFC que pueda leer y escribir en ellas. El modo de funcionamiento de estas etiquetas es bastante sencillo: cuando un usuario con su dispositivo (puede ser su teléfono móvil), toca una etiqueta con este, una pequeña cantidad de energía del dispositivo alimenta la electrónica de la tarjeta. De este modo la etiqueta se activa y puede emitir la información que contiene al dispositivo que la ha alimentado. NFC Forum ha definido cinco tipos básicos de etiquetas. Cada tipo de etiqueta se caracteriza por tener un formato y una capacidad diferente. No solo se define la estructura de las mismas sino también los protocolos para su lectura y escritura. En la tabla 2.1 se muestran algunas características de cada tipo de etiqueta.

2.2.2. Bluetooth

Bluetooth [99] nombre comercial de la tecnología IEEE 802.15.1, es una tecnología inalámbrica para comunicaciones de corto y medio alcance que funciona en el rango de la radiofrecuencia de 2,4 GHz a 2,48 GHz y permite la posibilidad de transmitir datos en full dúplex, es decir establece una comunicación bidireccional entre las partes implicadas [77].

Se estima que en el año 2021 se contará con 48 billones de dispositivos conectados a IoT, de los cuales el 30 % de los mismos usarán conexiones Bluetooth [5].

En el año 2010 con la versión 4.0 de Bluetooth aparece Bluetooth Low Energy (BLE) [11], cuya principal característica es una mejora sustancial con respecto a sus versiones predecesoras, poseer un consumo inferior de energía y de costes de implementación.

Esta tecnología de bajo consumo requiere de un nuevo hardware y por lo tanto no es compatible con los dispositivos Bluetooth anteriores a esta especificación. Esto, sin embargo, no impide que se pueda establecer una conexión P2P entre dispositivos BLE y dispositivos de versiones anteriores de Bluetooth, lo que ocurre es que estos dispositivos de versiones antiguas no se van a poder beneficiar de las nuevas características de bajo consumo desarrolladas para esta última versión.

La distancia máxima a la que, en teoría, podrán interactuar dos dispositivos BLE es de hasta 100 metros, aspecto innovador con respecto a las versiones anteriores en la que el rango máximo eran 30 metros.

A principios del presente año se ha anunciado la especificación de la última versión de Bluetooth, concretamente la versión 5.1 [6], la cual parece estar diseñada para mejorar la localización de los dispositivos como si de un GPS para interiores se tratase, con un margen de error de apenas unos cuantos centímetros.

Con el paso de las diferentes versiones de Bluetooth, su seguridad ha ido variando hasta llegar a los diferentes mecanismos incorporados en las últimas especificaciones de entre las que destacan la utilización de curvas elípticas y la utilización del AES [14]. A partir de Bluetooth 4.0 se introducen mejoras significativas incorporando el cifrado AES (Advanced Encryption Standard) de 128 bits con CCM (Counter with CBC-MAC). Además, en el emparejamiento entre dispositivos que implementan esta versión se utiliza una clave a largo plazo o LTK (Long-Term Key), en lugar de una clave de enlace o LK (Link Key) como sucedía en las anteriores versiones. La LTK se genera utilizando un protocolo de transporte de claves mientras que la LK se genera aplicando un protocolo de acuerdo y establecimiento de claves.

2.2.3. Wi-Fi

Wi-Fi [57] es una tecnología de comunicación inalámbrica que permite conectar dispositivos electrónicos a una red de área local, Wireless LAN (WLAN) [68].

Los mecanismos de seguridad implantados en estos casos son WPA, WPA2 y WPA3. Además, el futuro de esta tecnología es muy prometedor, ya que están apareciendo nuevos estándares que ofrecen características que hasta ahora eran imposibles para la Wi-Fi convencional. Continúan apareciendo nuevas variantes como por ejemplo: Wi-Fi IBSS (Independent Basic Service Set) [27] que permite comunicar diferentes dispositivos sin necesidad de tener puntos de acceso, Wi-Fi Direct, una de las más utilizada en la que los dispositivos interconectados pueden asumir el rol de punto de acceso o cliente

Cuadro 2.2 Comparación de tecnologías inalámbricas de corto alcance

Característica	NFC	BLE	RFID	Wi-Fi
Establecimiento de la comunicación	$\leq$ 0.1s	6s	$\leq$ 0.1s	-
Velocidad de transmisión	424-848kbps	32Mbps	424kbps	300 Mbps
Alcance	10cm	100m	$\geq$ 3m	820m
Consumo de baterías	bajo	bajo	bajo	medio
Coste de implantación	medio	medio	bajo	medio
Experiencia de usuarios	contacto	configuración	automático	configuración

dependiendo de las necesidades, y White-Fi [35] que pretende mejorar la velocidad de las comunicaciones mediante la utilización de otros espectros de comunicación.

Todos estos nuevos estándares son compatibles con las versiones anteriores y se caracterizan además de por su mayor velocidad junto con una mejora en el rendimiento del consumo de batería. En el caso de WiFi IBSS, las comunicaciones se pueden realizar en modo ad-hoc mientras que el denominado White-Fi está pensado para desarrollar la tecnología Wi-Fi en la banda blanca de TV (802.11af y 802.22).

Wi-Fi Direct [54] tiene por objetivo establecer una verdadera conexión P2P entre usuarios haciendo uso de la tecnología Wi-Fi. Además, extiende la arquitectura añadiendo dos nuevas capacidades. La primera de ellas, conocida como Group Owner, hace que un dispositivo que actúe haciendo uso de esta propiedad pueda establecer múltiples conexiones P2P con diferentes dispositivos, los cuales hacen uso de la propiedad Group Client. Un dispositivo establecido como Group Client funciona de manera similar a un dispositivo cliente en las conexiones Wi-Fi tradicionales, con la capacidad añadida de poder establecer una conexión P2P con un Group Owner.

La gran ventaja de Wi-Fi Direct es que todos los cambios necesarios con respecto a la tecnología Wi-Fi tradicional son llevados a cabo a nivel de software, siendo el mas importante de ellos el uso de un nuevo firmware. Todo esto asegura una retrocompatibilidad con los dispositivos Wi-Fi de la tecnología tradicional, lo que hace que esta tecnología pueda extenderse en mayor medida en un futuro próximo.

Una vez introducidas las tecnologías inalámbricas usadas en las diferentes soluciones planteadas en esta tesis, a continuación se incluye una breve comparativa con el objetivo de justificar la elección de una determinada tecnología en un escenario concreto. Para ello en la tabla 2.2 se puede consultar un resumen de las características de NFC frente a otras tecnologías inalámbricas [64].

Según las características mostradas en la tabla y dependiendo de las prioridades del usuario y del tipo de solución a desarrollar, se debe optar por una tecnología de corto alcance u otra. Por ejemplo, la velocidad de transferencia ofrecida por Bluetooth

es superior a la de NFC. Sin embargo, se debe tener en cuenta que ambas tecnologías han sido diseñadas para ser desplegadas en escenarios diferentes. El que NFC posea un rango de cobertura muy pequeño hace que el establecimiento de la conexión entre los diferentes dispositivos sea más eficiente que el de otras tecnologías, y no solo esto, sino que el uso de recursos del dispositivo es sumamente menor que, por ejemplo el de Bluetooth.

Otro aspecto interesante a destacar de los datos de la tabla anterior, es el paralelismo entre algunas características de RFID y NFC. La principal diferencia que añade NFC frente a RFID es el permitir que dos dispositivos puedan establecer una comunicación peer-to-peer de forma activa, facilitando así el intercambio de datos entre ellos. También es cierto que al poseer NFC un rango de acción más pequeño proporciona a la comunicación mejoras en la seguridad y en la privacidad. Todo esto unido a la rapidez y facilidad de uso que tiene NFC, hace que RFID se vea desplazada frente a esta nueva tecnología.

2.3. Criptografía basada en Curvas Elípticas

En esta sección se incluye una pequeña introducción a la criptografía basada en curvas elípticas junto con algunos otros fundamentos matemáticos utilizados en esta tesis.

2.3.1. Principios de Curvas Elípticas

Una de las ventajas asociadas al uso de las curvas elípticas (EC, Elliptic Curves) [9] es la posibilidad de crear criptosistemas robustos con menor necesidad de recursos que los tradicionales. Gracias a esta característica se consigue trabajar con longitudes de claves menores, repercutiendo positivamente en la eficiencia de los criptosistemas. Se consigue una mayor rapidez de cálculo con un menor consumo de memoria y un ahorro significativo en la transferencia de información.

Las curvas elípticas utilizadas se pueden representar usando la representación de Weierstrass [10] sobre un campo finito $\mathbb{F}_p$, siendo p un número primo: $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + ab + b\} \cup \{\bigcirc\}$ donde $a, b \in \mathbb{F}_p, 4a^3 + 27b^2 \neq 0$ y $\bigcirc$ representa el punto del infinito.

Se debe puntualizar que la implementación de la curva resulta mucho más sencilla cuando se usa $p = 2$. Si definimos el conjunto de puntos de la curva $E(\mathbb{F}_p)$, las operaciones definidas por la suma de dos puntos y el producto de un entero y un punto de la curva se obtiene un grupo $< E(\mathbb{F}_p), + >$. De esta forma se define el orden de un punto $P \in E(\mathbb{F}_p)$ como el menor entero m que verifica $m * P = \bigcirc$ y el cofactor se define como $\#E(\mathbb{F}_p)/m$.

2.3.2. El problema del logaritmo discreto en curvas elípticas

Se considera un grupo cíclico $\{0, P, 2P, 3P, ...\}$, para cualquier punto P en una curva elíptica en donde la operación kP se denomina multiplicación escalar, siendo k un entero. El problema del logaritmo discreto en curvas elípticas (ECDLP, Elliptic Curve Discrete Logarithm Problem) [37] consiste en conseguir el valor de k, dados los puntos kP y P. Resolver este problema de ECDLP con estos parámetros es inviable actualmente desde el punto de vista computacional y es por esto que es la base del esquema propuesto.

2.3.3. El problema de decisión de Diffie-Hellman con curvas elípticas

Se define $\mathbb{G}_{\mathbb{T}}$ como un grupo cíclico de orden q, generado por un punto P, el cual no es singular y pertenece a la curva elíptica $E(\mathbb{F}_{\mathbb{p}})$ cuya fórmula es $y^2 = x^3 + \alpha x + \beta$ definida sobre el cuerpo finito $\mathbb{F}_{\mathbb{p}}$, en donde $p \geq 3$ y es primo. Los elementos de $\mathbb{G}_{\mathbb{T}}$ son puntos sobre $E(\mathbb{F}_{\mathbb{p}})$ del tipo $xP, x \in \mathbb{Z}_{\mathbb{q}}$. Se definen las coordenadas del punto $Q \in E(\mathbb{F}_{\mathbb{p}})$ de la forma $Q.x$ y $Q.y$.

El problema de decisión de Diffie-Helman (ECDDH, Elliptic Curve Decision Diffie–Hellman) [7], consiste en averiguar si $cP = abP$, dada la distribución (aP, bP, cP) y siempre que se cumpla (aP, bP, abP), a, b, $c \in \mathbb{Z}_{\mathbb{q}}$.

El modelo ROR (siglas que vienen de Real-Or-Random) hace referencia a la creación de oráculos basados en la idea del "mundo ideal" mediante el cual los textos son aleatorizados de una forma perfecta. En este modelo ROR esto se define como un experimento asociado al oráculo $Test_{\mathbb{G}_T}$, en donde se pide que se seleccione de forma aleatoria y uniforme un bit b y retorne $aP, bP, cP, aP, bP \in \mathbb{G}_{\mathbb{T}}$ cuanto el bit seleccionado cumpla $b = 0$. El objetivo del adversario A es adivinar el valor de b. Si A tiene como salida b', entonces podemos definir que la ventaja que posee es $Adv^{ecddh}_{\mathbb{G}_{\mathbb{T}}}(A) = 2 \cdot Pr[b' = b] - 1$, lo que implica que tiene muy poca probabilidad de adivinar el valor de b debido a la complejidad asociada al problema de Diffie-Hellman basado en curvas elípticas que se explicará en los siguientes apartados.

2.3.4. Diffie-Hellman basado en Curvas Elípticas

Teniendo en cuenta el grupo aditivo previamente comentado ($\mathbb{G}$,+), de orden q y siendo P un generador de G se puede considerar el problema de Diffie-Hellman [85] basado en Curvas Elípticas (ECDH, Elliptic Curve Diffie-Hellman) [50]. La fortaleza de este problema se basa en que dados un punto generador P, unos valores desconocidos seleccionados al azar $a, b \in \mathbb{Z}_q$ y sabiendo aP y bP, calcular abP tiene una gran dificultad. Concretamente no existe un algoritmo probabilista polinomial que permita a un adversario calcular abP con una probabilidad alta.

2.4. Criptografía basada en Identidad

En esta sección se explicarán los conceptos fundamentales sobre criptografía basada en identidad, dado que la misma ha sido utilizada en varias de las soluciones propuestas en esta esta tesis. Estos esquemas encajan totalmente en el entorno sanitario, y aportan un valor añadido a la seguridad de los datos médicos de una forma relativamente sencilla.

La criptografía basada en identidad (IBC, IDentity-based Cryptography) define esquemas de clave asimétrica en los que cualquier parámetro conocido asociado a la identidad de un usuario puede ser tomado como clave pública. Este identificador debe ser conocido, público y único. Generalmente, suele extraerse de información tal como el nombre, el correo electrónico o la identificación sanitaria del usuario. En todos los sistemas basados en identidad se debe de contar con un servidor generador de las claves privadas a utilizar (PKG, Private Key Generator).

La principal mejora aportada por este tipo de esquemas criptográficos es la simplificación en la gestión de las claves, ya que mediante la utilización de un sistema basado en identidad no es necesario definir una infraestructura de clave pública (PKI, Public Key Infraestructure). Además de esto, unas de las principales características que aportan estos esquemas son su baja complejidad computacional y su eficiencia en términos de memoria y usabilidad.

La primera aportación relacionada con este tipo de propuestas fue la publicación de Shamir [81] en los años 80s, en donde proponía un sistema que evitaba la gestión de certificados en esquemas de clave asimétricos. Desde esa primera aportación se planteó la búsqueda de criptosistemas en los que cualquier texto pudiese utilizarse como clave pública válida.

El principio matemático fundamental utilizado en estos sistemas son los emparejamientos bilineales [93]. Este concepto se define a continuación. Dados dos grupos cíclicos $\mathbb{G}$ y $\mathbb{G}_T$ de orden q, un primo grande, en donde $\mathbb{G}$ es un grupo aditivo de puntos de una curva elíptica $\mathbb{F}_p$ ($\mathbb{G}$,+) y $\mathbb{G}_T$ es un subgrupo multiplicativo de $\mathbb{F}^*_{\mathbb{p}^2}$ ($\mathbb{G}_T$,*). Se dice que existe un emparejamiento bilineal simétrico de la forma $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, si y solo sí se cumplen las propiedades:

- Bilinear: para cualquier selección de puntos $P, Q \in \mathbb{G}$, si seleccionamos dos valores $a, b \in \mathbb{Z}$, se debe de cumplir que $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$
- No-degenerativo: si existen $P_1, P_2 \in \mathbb{G}$ de tal forma que $e(P_1, P_2) \neq 1$, significa que si P es generador de $\mathbb{G}$ entonces $\hat{e}(P, P)$ es generador de Q;
- Computable: debe de existir un algoritmo eficiente que pueda ejecutar $\hat{e}(P, Q)$, para cualquier $P, Q \in \mathbb{G}$.

Boneh y Franklin definieron por primera vez un esquema IBC [8] basado en emparejamientos de Weil [33] utilizando un enfoque práctico.

A partir de esta propuesta, se han introducido múltiples sistemas basados en IBC, así como diversas variantes basadas en la misma idea. De hecho, han surgido esquemas basados en identidad específicos para casi cada servicios de seguridad: esquemas de cifrado basados en identidad [100], [87], [28], esquemas de firma basados en identidad (Identity-Based Signature, IBS) [18], [23], esquemas de firma y cifrado basados en Identidad (Identity-Based SignCryption, IBSC) [17], [94], protocolos de acuerdos de claves basados en Identidad (ID-based Key Agreement protocols, IKA) [67], [53] e incluso protocolos de autenticación e intercambio de claves basados en identidad (Id-Based Authenticated and Key Exchange, IBAKE) [97], [55].

2.4.1. Esquemas de cifrado (Identity Base Encryption, IBE)

El sistema IBC más utilizado en la actualidad para proteger la confidencialidad se basa en el esquema propuesto por Boneh-Franklin [8]. En el entorno de esta tesis, la clave pública propuesta es el número de colegiado de cada médico dado que éste es un identificador único y público que poseen todos los doctores.

Todos los IBE están compuestos por cuatro algoritmos principales, que son los pasos que definen el funcionamiento de estos esquemas. Se incluye a continuación una descripción general de dichos algoritmos.

- **Setup.** Esta es la fase de inicialización del entorno, es por eso que la primera acción a realizar es la creación del par de claves asociadas al generador PKG: la clave pública (master public key, mpk) y la privada (master secret key, msk).

  Para ello, a partir de un parámetro de seguridad dado $k \in \mathbb{Z}$ se genera un número entero primo q, dos grupos $\mathbb{G}_1$ y $\mathbb{G}_1$ de orden q y un emparejamiento bilineal $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$.

  Posteriormente, se elige de forma aleatoria un generador $P \in \mathbb{G}_1$, un entero $s \in \mathbb{Z}_q$ que será la msk, y se crea a partir de esta la mpk de la forma sP. Finalmente se eligen las funciones hash que se utilizarán.

- **Extract.** Esta fase es la encargada de la generación de las claves secretas de los participantes. Antes que nada, se debe de tener en cuenta el identificador del usuario (ID), que al normalizarlo mediante el uso de una función hash actuará como clave pública de la forma $Q_{ID} = HASH(ID)$.

  Finalmente para la creación de la clave privada del usuario, se necesita combinar la msk con la clave pública del usuario obteniendo en ese caso: $S_{ID} = msk \times Q_{ID}$
  El envío de estas claves se debe realizar bajo un canal de comunicaciones seguro,

ya que los datos intercambiados en esta comunicación son fundamentales para la confidencialidad en las siguientes conexiones.

- **Encrypt.** Este es el paso para cifrar toda la información que se quiera intercambiar. Para ello se utiliza como clave de cifrado la clave pública del receptor y la msk. Es decir, si un usuario con identificación ID_a quiere enviar un mensaje m a un usuario con identificador ID_b, el emisor debe de calcular la clave pública Q_{ID_b} y cifrar m con esta clave.

- **Decrypt.** Esta fase se realiza de forma similar que la anterior, pero con el objetivo inverso. En este caso el receptor ID_b debe utilizar su clave privada (S_{ID_b}) para poder descifrar el mensaje m. Una vez descifrado el mensaje, existe un proceso de verificación del mismo mediante emparejamientos bilineales.

2.4.2. Esquemas de firma y cifrado

Una de las variantes del algoritmo anterior es el de añadirle al IBE un sistema de firmas. Para poder abordar estas medidas surgen las alternativas de firma-cifrado basadas en identidad (IBSC, Id-Based SignCryption). Una de las propuestas más conocidas en este ámbito es el de los autores Malone-Lee [59].

Los pasos a realizar en este tipo de especificaciones son: Setup, Extract, Signcryption y Unsigncryption y se describen a continuación.

- **Setup y Extract.** Estos pasos son exactamente iguales a los del algoritmo anterior. En el paso del Setup se definen las claves del servidor y los parámetros a utilizar y en el Extract se generan las claves de usuario.

- **Signcryption.** En este paso es donde se cifran y se firman los mensajes. En el caso de que el usuario ID_a quiera enviar el mensaje m al usuario ID_b, el usuario emisor debe cifrar con la clave pública del usuario receptor Q_{ID_b} y firmar con su clave privada, que en este caso sería S_{ID_a}.

- **Unsigncryption.** Este algoritmo es el encargado de descifrar el mensaje enviado con la clave privada del receptor S_{ID_b}. Finalmente se comprueba la integridad del mensaje gracias a la clave pública del emisor Q_{ID_a}.

  Cabe puntualizar que existen dos tipos de verificación, por un lado se comprueba la integridad del mensaje recibido, y por otro lado se verifica la identidad del emisor.

2.4.3. Criptografía basada en identidad jerárquica

La criptografía basada en identidad jerárquica (HIBE, Hierarchical Identity-Based Encryption) es un sistema que incorpora una jerarquía organizativa. Estos esquemas

utilizan árboles jerárquicos para poder controlar los accesos. Con estos esquemas una identidad en el nivel k del árbol de jerarquías puede emitir claves privadas para sus identidades descendientes, pero no puede descifrar mensajes destinados a otras identidades.

Este tipo de sistemas soporta mecanismos como la delegación de permisos o la revocación de acceso, esto se produce gracias a que los usuarios pueden recibir claves privadas restringidas, las cuales sólo permiten la delegación a una profundidad limitada. Con esta estructura se mejora la escalabilidad del sistema IBE y facilita las tareas de delegación y revocación de claves privadas.

Los pasos que se tienen que tener en cuenta en este esquema de cifrado son: Setup, KeyGen, Encrypt, Decrypt, KeyUpdate, KeyDelegate y Revoke.

- **Setup.** Como en otros sistemas IBE, en este primer paso se realiza la generación de los parámetros de inicialización del sistema. Siguiendo los procedimientos de los esquemas basados en identidad lo primero en generarse son las claves maestras del PKG (msk y mpk). Un paso característico de este tipo de cifrados es la definición de la profundidad máxima de los árboles de jerarquía k y la generación de una lista de revocación vacía (RL).

- **KeyGen.** Este paso es similar a los Extract de otros IBEs, ya que es la función que genera las claves para cada uno de los usuarios participantes. Sin embargo, posee una característica diferenciadora, y es el hecho de que se define el nivel de profundidad $|k$ asociado a cada usuario. Si el usuario $ID_{|k}$ es un nodo padre, los parámetros se inicializan para que coincidan con el msk de la siguiente manera: $S_{ID_{|k}} = msk$. En el caso en el que no sea del tipo nodo padre, si no de uno de sus hijos, la clave se genera la clave $S_{ID_{|k-1}}$.

- **Encrypt.** Esta es la función encargada de cifrar los mensajes m y para ello se utiliza, como en otros sistemas IBE, el identificador del receptor, que en este caso dependerá del árbol de permisos que posea $ID_{|k}$. A parte, la utilización de la mpk es fundamental para la creación del texto cifrado CM.

- **Decrypt.** Este es el algoritmo de descifrado en el que mediante el CM se intentará obtener el mensaje original m. Para ello se asume que el algoritmo de cifrado utilizado ha sido el que explicamos en el punto anterior y se utiliza la clave secreta del receptor $S_{ID_{|k}}$.

- **KeyUpdate.** En este paso se realiza la actualización de la lista de revocación RL. El PKG reconstruye todo el el sistema de nodos, y calcula de nuevo el árbol correspondiente. Estas modificaciones actualizan las estructuras de las claves públicas y envían esta nueva información representada como KU al grupo de usuarios

afectados. Todo esto se realiza siempre en un tiempo t el cual se calcula de nuevo en cada actualización del KU definiendo de esta forma la siguiente ejecución de este paso, o lo que es lo mismo, el tiempo de expiración del árbol de permisos.

- **DecKeyGen.** Este algoritmo es ejecutado por cada usuario para actualizar su propia información de claves KU. Con la información de la clave privada del usuario $S_{ID_{|k}}$ y la información actualizada de KU, el sistema genera una nueva clave de descifrado $D_{sk_{ID_{|k}}}$. Esta clave es la necesaria para descifrar la información sobre si un usuario concreto con identificador ID ha sido revocado o no.
- **KeyDelegate.** Este paso lo puede realizar cada nodo interno del árbol, recibe como entrada la clave secreta de un usuario $S_{ID_{|k}}$ y su identificador ID y crea una nueva clave privada para la identidad del mismo.
- **Revoke.** Este es el paso por el que la lista de revocación RL y la información del sistema se actualizan. Para poder conseguir esto es necesario contar con el identificador del usuario que queremos actualizar ID.

2.5. Primitivas criptográficas de autenticación

La autenticación de los datos médicos es uno de los principales hitos que se intenta alcanzar en entornos relacionados con la salud. Es por esto, que en esta sección hablaremos de algunas de las primitivas criptográficas de autenticación utilizadas a lo largo del desarrollo de esta tesis.

2.5.1. Códigos de autenticación de mensajes basado en hashes

Unas de las herramientas criptográficas más utilizadas para proteger la integridad de los datos es la de los códigos de autenticación de mensajes basado en hashes o HMAC (Hash Message Authentication Code) [86]. Con estos sistemas se calcula un código de autenticación para cada mensaje aplicando una función hash con una clave secreta.

Se puede utilizar un HMAC para verificar la integridad y la autenticidad de los datos de forma simultánea. Las funciones hash que se utilizan actualmente para el cálculo de los HMAC suelen ser las de la familia SHA, siendo una de las más utilizadas la SHA3-512. La fortaleza criptográfica de un HMAC depende del tamaño de la clave secreta que se utilice, y de hecho el ataque más común contra un HMAC es mediante fuerza bruta para descubrir la clave secreta usada.

Una vez se tengan definidos los parámetros a utilizar, la clave y las funciones hash, el primer paso para crear un HMAC es la generación de dos vectores de 64 bytes (ipad y opad) de acuerdo con las especificaciones publicadas en [4]. Estos vectores tienen unos valores por defecto definidos en esta etapa de inicialización, cuya finalidad, es

la generación dos nuevos vectores del mismo tamaño, gracias a la realización de una operación XOR a nivel de bit con los valores de la clave definida. Se suele utilizar la msk para este tipo de operaciones, pero también se puede crear una nueva clave secreta cuyo único fin sea el de validar estas operaciones. Los resultados se denotan como $ipad_k$ y $opad_k$. En la Figura 2.3 se muestra este proceso.

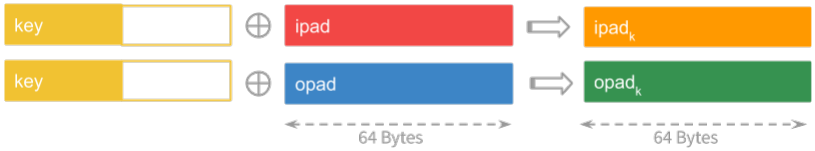


Figura 2.3 Generación de claves HMAC

Después de tener los parámetros de inicialización creados se procede a la generación del código en si. Concretamente se concatena la clave $ipad_k$ con la información que queremos salvaguardar y se facilita como entrada a una función hash (Figura 2.4). La salida de esta primera función hash, se concatena con la clave $opad_k$ y se introduce en una segunda función hash. Esta salida será finalmente el código HMAC requerido.

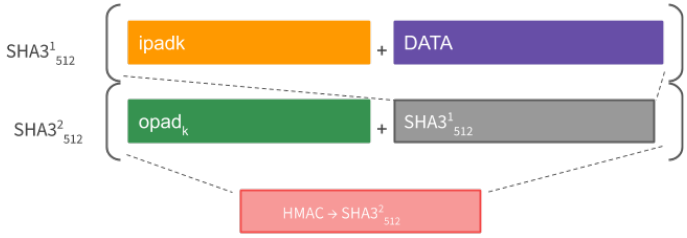


Figura 2.4 Operaciones hash en HMAC

En resumen, para la creación de los códigos se utiliza la expresión global:
$HMAC(DATA, key) = HASH(opadkey||(HASH(ipadkey||DATA)))$
Estos sistemas fueron una parte de la solución de los trabajos presentados en [72] y [70].

2.5.2. Tokens de autenticación

La especificación JWT (JSON Web Token) [48] es un estándar que se utiliza para verificar la autenticidad de la información intercambiada entre dos partes, así como la autenticación de los usuarios que participan en dicho intercambio. Este estándar proporciona una forma compacta de mejorar la seguridad de los sistemas utilizando el formato JSON como estructura de intercambio.

Estos tokens se suelen intercambiar en base 64 y siempre poseen la misma estructura: un encabezado (header), un contenido (payload) y una firma (signature). Todas las partes suelen ir concatenadas y separadas por puntos [49]. Seguidamente se describe el contenido de cada uno de sus elementos.

- Encabezado: es el lugar en donde se añade toda la información de los algoritmos a utilizar, así como el tipo de token. Uno de los algoritmos más utilizados es el HS256 que utilizar como hash la función SHA256. Ejemplo: { “alg” : “HS256”, “typ” : “JWT” }
- Contenido: es el contenido en sí del token. Aquí se añaden los atributos del token así como cierta información relevante para el manejo del mismo. Concretamente el campo “iat” hace referencia al timestamp del token y es un campo obligatorio para poder verificar los tiempos de expiración. Ejemplo: { “id” : “78456524V”, “name” : “Alexandra Rivero”, “iat” : 1516239022}
- Firma: en esta última parte es donde se encuentra la información que permite verificar si el contenido de los apartados anteriores es el adecuado o ha sido modificado. Para la verificación del token es necesario poseer una clave secreta de 256 bits, como fija el estándar.

Finalmente, se puede concluir que para la creación de un token de este estilo se debe de seguir el esquema HMACSHA256{ (header)$_{64}$ + “.” + (payload)$_{64}$, $secretkey$ }.

El resultado codificado de este ejemplo sería de la forma:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJpZCI6Ijc4NDU2NTI0ViIsIm5hbWUiOiJBbGV4YW5kcmEgUml2ZXJvIiwiaWF0IjoxNTE2MjM5MDIyfQ.
Me2pr5XBJTiDcx3RE6R1tgiiFb1QY1uPkJS3kApdl7E

A través de este procedimiento, es posible controlar, por un lado la autenticidad de los usuarios, y por otro lado, la información intercambiada entre los usuarios del sistema. Este sistema es utilizado en la propuesta presentada en el trabajo [74].

2.6. Autenticación e intercambio de claves

La necesidad de definir servicios de autenticación e intercambio de claves en el entorno sanitario es también abordada en esta tesis. Por este motivo se incluye a con-

tinuación una descripción de los mecanismos actuales definidos para estos servicio y su clasificación.

2.6.1. Intercambio de claves autenticadas

Existen varias propuestas de protocolos de intercambio de claves autenticadas (AKE, Authenticated Key Exchange) para aplicaciones actuales [25], y [96]. Una variante ampliamente utilizada, debido principalmente a que son más fáciles de utilizar con usuarios, son los sistemas AKE con contraseña (PAKE, Password Authenticated Key Exchange) [3], [16] y [78]. Son especialmente recomendados cuando los dispositivos que intervienen en el proceso cuentan con recursos limitados, como es el caso de los nodos que intervienen en IoT, dado que su eficiencia es una de sus características principales.

Se suelen utilizar los protocolos AKE para proveer de autenticación y control de acceso a aplicaciones de red. Gracias a la mejora aportada por los PAKE, los usuarios pueden intercambiar una clave basada en el conocimiento de un sistema compartido de baja entropía, que sería una contraseña.

Dentro de estos sistemas AKE existen los que poseen múltiples participantes. Unos de los más utilizados son aquellos en los que intervienen tres tipos de participantes, los conocidos como 3-AKE. Estos permiten compartir claves privadas con un tercero de confianza, posibilitando la generación de una clave de sesión. Esta es una de las bases de las propuestas utilzadas en el trabajo [72].

2.6.2. Intercambio de claves autenticadas basadas en identidad

Este tipo de protocolos de intercambio de claves autenticadas basada en identidad (IBAKE, Identity-Based AKE) se diferencian de los protocolos AKE tradicionales en que las claves intercambiadas no siguen el esquema tradicional de PKI, si no que utilizan la información de las identidades de las personas para la creación de las mismas.

Como en otros esquemas basados en identidad, existen una serie de algoritmos (setup, extract, mutual authentication y session key generation) que definen los pasos a seguir para utilizar este protocolo. Estos pasos son los descritos seguidamente.

- **Setup.** Este primer paso sigue los esquemas tradicionales de IBE en donde se realiza la definición de los parámetros de inicialización del sistema y se generan las claves maestras del PKG (msk y mpk).

- **Extract.**

  Como en otros casos, este algoritmo genera las claves para cada uno de los usuarios participantes. Sin embargo posee una característica diferenciadora, y es el hecho de que toda la comunicación entre el usuario y el PKG pasa a través de una pasarela o un servidor central. Cabe puntualizar que en la generación de la

clave privada participan, tanto la pasarela como el PKG de manera que la clave que se obtiene es la del grupo pgk_{ID}.

- **Mutual authentication.**

  Este es el algoritmo encargado de que los participantes se autentiquen mutuamente de manera que cada uno de ellos pueda confiar en el otro. Para ello algunos cálculos son realizados por parte del cliente, otros por la pasarela y el PKG es el encargado de verificar el emparejamiento del mapeo bilineal. Si la verificación no es correcta, el PKG envía la notificación de "cerrar" al servidor para finalizar la comunicación. En caso de ser correcta, el servidor genera una tupla, que se envía al cliente, que autentica al servidor.

  Si esta otra autenticación resulta correcta, el cliente genera un parámetro para su propia autenticación frente al servidor y lo envía de vuelta al servidor intermedio, que verifica la autenticación de usuario. Si todo está bien, tanto el cliente como el servidor continúan con el siguiente paso, que es la generación de la clave de sesión.

  Hay que tener en cuenta que el paso de verificación se realiza en el segundo servidor.

- **Session key generation.** Esta última etapa permite la generación de una clave de sesión que permite la comunicación entre los participantes. Este paso sólo se realiza una vez todas las partes estén autenticadas. Esta clave compartida se genera al mismo tiempo en el lado del cliente y en el lado del servidor. A partir de este momento, los mensajes intercambiados se cifran utilizando la clave de sesión generada.

2.7. Blockchain

En esta sección se realizará una pequeña introducción a una de las tecnologías clasificada como una de las más prometedoras dentro de la seguridad de la información, Blockchain. Se explicará de forma muy breve como funciona esta tecnología y el potencial que tiene para el futuro inmediato de los sistemas distribuidos.

Blockchain o cadena de bloques [98], es una de las herramientas más disruptivas de los últimos años siendo catalogada como una revolución en el entorno de la seguridad informática y la criptografía. En términos generales, blockchain es una base de datos descentralizada que almacena un registro de activos y transacciones u operaciones a través de una red informática [38]. Específicamente, puede verse como una red P2P que está asegurada a través de primitivas criptográficas robustas. Cada elemento perteneciente a una cadena de bloques contiene una marca de tiempo y un enlace a un elemento anterior. De esta manera, una vez sellado este ítem, es teóricamente

imposible modificarlo. Por tanto, la información insertada en la cadena de bloques es persistente una vez que se inserta en el sistema.

La aplicabilidad de esta tecnología en el entorno de las criptomonedas es fundamental, debido a que todas las operaciones realizadas quedan identificadas y certificadas mediante la cadena de bloques. Las transacciones se llevan a cabo cuando se obtiene la marca de tiempo (timestamp). Este proceso proporciona al sistema un mecanismo de registro de tiempo que permite la posibilidad de mantener un histórico con toda la información generada.

Los bloques contienen transacciones confirmadas. Cada bloque contiene el enlace al bloque anterior y cierta información relacionada con la propia transacción (personas involucradas en la operación, cantidad de monedas intercambiadas, etc). No solo esto, en caso de necesitar añadir un bloque a la blockhain, este se añade al último nodo mediante el enlace de su sucesor. De esta forma contamos con una lista doblemente enlazada distribuida por la red. Estos enlaces son generados mediante la utilización de funciones hash.

Un ejemplo claro de todo lo que se ha descrito hasta este momento puede verse en la Figura 2.5, donde se ilustra el doble enlace mencionado.

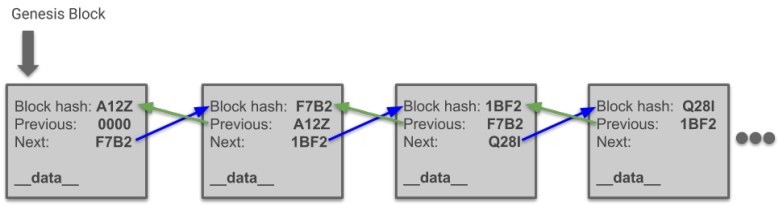


Figura 2.5 Ejemplo de cadena de bloques.

El bloque maestro, el primer bloque, se denomina bloque génesis y se caracteriza por el hecho de que el el valor del enlace que apunta al bloque anterior es '00000'.

En una cadena de bloques, un token se define como una representación de un activo físico o digital construido sobre una moneda virtual. Los tokens incluyen algunas propiedades específicas como: un nombre, un símbolo, el número inicial de unidades acuñadas, el número máximo de unidades, la divisibilidad (porque un token puede ser divisible en unidades más pequeñas o ser indivisible) y un enlace a un valor o activo físico o virtual.

Los elementos de la cadena de bloques están replicados en los diferentes nodos participantes, ya que lo que subyace es una base de datos distribuida. Esto justifica que sea imposible falsificar sus elementos, ya que todos los datos se encuentran general-

mente en varios servidores, y su sincronización ocurre casi simultáneamente. Además, si se consigue una falsificación con uno de los registros, debería ser fácil detectarla a través de los códigos que enlazan los bloques y de esta forma se puede evitar que esta información fraudulenta se extienda.

Antes de incluir una operación en un bloque, se realiza la operación de verificación, la cual es realizada siempre por los llamados mineros. Estos verificadores son ordenadores dedicados, no sólo a mantener una copia de los datos, sino también a validar el acuerdo que debe realizarse por parte de los nodos.

2.7.1. Contratos inteligentes.

En el mundo real la definición de un contrato se basa en la creación de un acuerdo entre dos o más partes incluyendo un conjunto de requisitos y condiciones de ejecución aceptadas por los firmantes.

Los contratos inteligentes extienden este concepto a los programas informáticos, los cuales ejecutan acuerdos establecidos entre dos o más partes cuando se produce una condición pre-establecida o pre-programada [56]. Debido a su naturaleza, un contrato inteligente es válido sin la necesidad de autoridades. Es decir, estos nuevos contratos se ejecutan y se llevan a cabo generalmente de forma automática y autónoma, sin la intervención de terceros pero también admiten su creación y ejecución por personas físicas y/o jurídicas. Las principales características de los contratos inteligentes son la descentralización, la persistencia y la transparencia.

La tecnología Blockchain permite compartir este código con todos los nodos de la red, garantizando que no pueda ser modificado.

Dentro de el ecosistema de los contratos inteligentes, existen unos elementos clave llamados oráculos, los cuales son los actuadores que permiten que el contrato interactúe con el mundo real y su entorno. Los oráculos se consideran herramientas autónomas que permiten actualizar los estados internos de un contrato inteligente a través de información externa, generalmente obtenida a través de APIs específicamente diseñadas para este fin.

Muchas de las últimas propuestas de implementación de contratos inteligentes se basan en Ethereum [30]. Esta opción es una de los más utilizadas dentro de las cadenas de bloques públicas y utiliza una divisa criptográfica llamada Éter. Solidity [29] es el lenguaje utilizado en Ethereum, siendo sus principales características el ser estático y orientado a objetos.

Capítulo 3

Contribuciones

En este capítulo se explicarán todas las aportaciones realizadas en esta tesis. Concretamente, se destacarán las cuatro publicaciones en revistas con índice de impacto JCR aceptadas y publicadas. Además, para completar el ámbito de desarrollo de este trabajo, se incluye un trabajo remitido a una revista que actualmente se encuentra en revisión.

Todas las propuestas presentadas se orientan en aportar servicios de seguridad a sistemas mHealth para solventar algunos de los problemas que dichos sistemas presentan en la actualidad.

En este capítulo se encontrará en primer lugar un sistema para el apoyo del tratamiento y monitorización de niños con trastorno de déficit de atención. Posteriormente se describirán dos soluciones novedosas para la identificación de pacientes, una de ellas para entornos controlados como pueden ser entornos hospitalarios y la otra para la identificación de víctimas en entornos de emergencia, concretamente en grandes catástrofes. Esta última propuesta agrega un valor añadido en la clasificación de víctimas y el establecimiento de comunicaciones seguras entre el personal médico que se encuentra en el lugar afectado. Seguidamente, se explicará un sistema basado en el uso de blockchain para la mejora de la trazabilidad y gestión de pequeñas emergencias y eventos cotidianos que ocurren en las ciudades. Finalmente, se presentará una propuesta de mejora de la seguridad de los dispositivos con poca capacidad computacional que pueden encontrarse en sistemas eHealth. Por último se realizará el análisis de los ataques encontrados en los sistemas actuales así como la presentación de las soluciones aportadas.

3.1. A secure mHealth application for attention deficit and hyperactivity disorder.

La solución aportada en el artículo presentado en esta sección [74] se corresponde una herramienta móvil destinada a la mejora de la vida de los niños y familiares que sufren el trastorno de déficit de atención e hiperactividad. Este trabajo se encuentra en el Apéndice A, y fue publicado en la revista Expert Systems en abril de 2019, la cual pertenece al cuartil Q2 según Journal Citation Reports.

Actualmente, existen diferentes métodos que contemplan el uso de aplicaciones móviles para el tratamiento de las personas que sufren algunos trastornos neurológicos con el fin de ayudar a mejorar su día a día. Además, las técnicas de gamificación aplicadas a este tipo de herramientas representan una forma fundamental para potenciar el compromiso del usuario en la promoción de sus habilidades cognitivas; sobretodo cuando hablamos de niños. Una aplicación móvil que permita la integración de los diferentes perfiles de las personas involucradas en el Trastorno por Déficit de Atención e Hiperactividad (TDAH) puede facilitar la relación entre la persona afectada y su entorno, tal y como explica [73]. Se debe puntualizar que el Trastorno por Déficit de Atención (TDA) no siempre va ligado con un componente de Hiperactividad, pero en la mayoría de los casos van enlazados, es por ello que aludiremos desde este momento a este trastorno de la forma TDA/H.

La propuesta presentada en este apartado de la tesis incluye una aplicación móvil que puede ser utilizada como una herramienta para mejorar el tratamiento del TDA/H, tal y como se indica en el trabajo de [95]. Una de las principales funcionalidades de la aplicación propuesta es la integración de diferentes perfiles de usuarios, con el objetivo de compartir datos relevantes entre ellos. Los perfiles que se tienen en cuenta en la solución aportada en esta tesis son: padres o cuidadores (tutores), personal médico, paciente y profesores del mismo.

El sistema propuesto en este trabajo proporciona a los tutores un cuestionario inicial de diagnóstico mediante el cual respondiendo algunas preguntas sobre el comportamiento y las características del paciente se puede tener una primera aproximación sobre si los pacientes poseen o no el TDA/H, para ello se ha seguido el estándar propuestos en Europa, el ICD-10 [62].

Posteriormente, los datos recogidos son evaluados por el personal médico, que se encargará de diagnosticar si el paciente sufre o no de la enfermedad. Durante esta evaluación, tanto los padres como el personal médico pueden utilizar un sistema experto para ayudar en el diagnóstico del TDA/H. Si se diagnostica TDA/H, las respuestas al cuestionario se utilizan para estimar el nivel de TDA/H que puede sufrir el paciente.

Después de analizar los resultados, el personal médico envía la evaluación obtenida a los tutores del paciente. Los tutores podrán registrar al/a niño/a en la aplicación móvil,

y desde este momento los pacientes pueden acceder a diferentes actividades disponibles para ayudarles a mejorar sus funciones cognitivas (memoria, atención, lenguaje, percepción, resolución de problemas o planificación).

Para ayudar en el correcto desarrollo cognitivo del paciente con TDA/H se han incluido tres tipos de juegos en la aplicación móvil. Los juegos pueden utilizarse para enriquecer el proceso de enseñanza y aprendizaje, pero es importante definir el enfoque correcto para utilizarlos en beneficio de la educación. Concretamente, en la propuesta presentada en este trabajo, los juegos implementados se basan en diferentes estudios de psicología [58], y en esta aplicación se han desarrollado: juego de colores, memoria y cálculos matemáticos.

En el campo de la mHealth hay muchas soluciones que se apoyan en la utilización de sistemas expertos basados en redes bayesianas para predecir la probabilidad de padecer una determinada enfermedad a partir de un conjunto de variables. El sistema presentado en el artículo del que hablamos en esta sección, incluye una herramienta que, mediante diferentes puntuaciones, estiman el nivel de TDA/H del paciente a través de un sistema experto que determina el resultado gracias a un conjunto de variables. Esto proporciona a los médicos un mecanismo de pre-clasificación que les permite clasificar mediante prioridades qué pacientes requieren una atención más inmediata y cuales no. Con los datos generados por la aplicación, se realiza una clasificación aproximada de los niños con necesidades más urgentes a partir del uso de la técnica de clasificación Naive Bayes [60]. El teorema bayesiano proporciona una forma de calcular las probabilidades posteriores a partir de las probabilidades anteriores, y la probabilidad de los valores dados.

En el desarrollo de la aplicación propuesta se siguieron las directrices establecidas por el Open Web Application Security Project (OWASP) para la autenticación de usuarios [66]. OWASP proporciona una guía con un conjunto de reglas y directrices destinadas a mejorar la seguridad de las aplicaciones.

Cabe puntualizar que todo el manejo de los datos de los pacientes se ha realizado mediante la puesta en marcha de un sistema de cifrado basado en identidad, concretamente se ha utilizado un sistema jerárquico basado en identidad (HIBE) [46]. Mediante el uso de este sistema los padres son los encargados de darles permiso a los médicos sobre los datos de la salud de sus hijos, estableciendo ellos la cantidad de información que puede ver cada uno de los participantes sanitarios que intervienen, así como el tiempo de expiración de este permiso.

3.2. Patients' Data Management System Protected by Identity-Based Authentication and Key Exchange

El segundo artículo presentado en este capítulo [72] se puede consultar en el Apéndice B. Ha sido publicado en la revista Sensors en el año 2017 la cual pertenece al cuartil Q1 según Journal Citation Reports. Presenta una solución para mejorar la identificación y el acceso a los datos médicos de las personas hospitalizadas mediante el uso de la tecnología NFC y los dispositivos móviles.

En la mayoría de los sistemas de salud actuales, cuando un paciente llega a un hospital, el primer paso a realizar por el personal sanitario es identificarlo. La identificación del paciente se realiza normalmente mediante la verificación de una tarjeta de identificación sanitaria. A continuación, el paciente es evaluado por un miembro del personal sanitario que analiza la información recogida durante el ingreso y añade los resultados de las nuevas evaluaciones si es necesario para que posteriormente el paciente pueda ser atendido por un especialista.

Antes de cada una de estas acciones, se debe repetir el proceso de identificación del paciente lo cual tiene varios inconvenientes. Los médicos deben revisar el registro del paciente antes de tratarlo, para ello, dependiendo del caso particular, pueden realizar dicha consulta a través de documentación impresa o mediante el uso de un ordenador. Si se utiliza documentación en papel, normalmente se genera como un lote para un conjunto de pacientes. Por ejemplo, se pueden imprimir tres historias clínicas a la vez para que un médico pueda revisar y atender a esos tres pacientes uno tras otro. Una vez atendidos, el médico debe dejar los registros y repetir el proceso con un nuevo grupo de pacientes. Este tipo de procedimiento produce información heterogénea debido a que algunos datos pueden ser actualizados desde ordenadores mientras que otros se mantienen en formato papel, es decir, la información no siempre se actualiza en tiempo real. Con este sistema tradicional, los trabajadores sanitarios deben manejar una gran cantidad de documentación, lo que conlleva un consumo considerable de tiempo y recursos. Por otro lado, cada miembro del personal médico tiene que visitar a varios pacientes en cada turno, lo que puede generar identificaciones erróneas de pacientes, con graves consecuencias en algunos casos.

Una de las soluciones propuestas en el trabajo [72] consiste en un sistema seguro basado en pulseras NFC y dispositivos móviles que permiten evitar los problemas de identificación errónea del paciente así como mejorar la eficiencia del servicio médico en la atención al paciente.

La propuesta implica cambios sustanciales con respecto al flujo de registro del sistema tradicional. Cuando se realiza la identificación del paciente por primera vez, se le asigna una pulsera NFC. Esta pulsera no se utiliza para almacenar datos sensibles de pacientes sino únicamente para guardar el identificador del mismo. Este identifi-

cador se genera a través de un proceso en el que se tienen en cuenta datos como el identificador físico de la pulsera y el número de registro del paciente, concretamente el identificador es la salida de un HMAC.

Mediante el uso de este mecanismo cualquier miembro del personal médico con los permisos adecuados puede acceder a la historia clínica, identificando al paciente con el simple gesto de acercar un dispositivo móvil a la pulsera. Gracias al uso de pulseras, el sistema evita confusiones en la identificación de pacientes y aumenta la eficiencia en el desarrollo de las tareas médicas. Además, las pulseras son totalmente reutilizables, por lo que cuando un paciente abandona el hospital, su pulsera se restablece para ser utilizada por otro paciente.

El sistema está diseñado para trabajar con dos servidores separados. Por un lado, un servidor intermedio gestiona los permisos de acceso a los datos de los pacientes en base a los turnos del personal médico. Por otro lado, el segundo servidor utiliza un Generador de Claves Privadas (PKG, Private Key Generator) para gestionar la información relacionada con las claves.

Se propone usar dos servidores físicos diferentes para añadir una nueva capa de seguridad en la gestión de las claves. Con esta separación, se pueden añadir diferentes cortafuegos a cada servidor de forma independiente y se pueden aplicar diferentes reglas de seguridad en las comunicaciones entre ellos.

La protección de las comunicaciones se logra a través de un esquema basado en la identidad, concretamente un esquema AKE [88].

3.3. IBSC System for Victims Management in Emergency Scenarios

Este tercer artículo que compone esta tesis [70] es el único que no está publicado en una revista con índice de impacto en la actualidad. Concretamente fue presentado en 2018 en el congreso internacional The Twelfth International Conference on Digital Society and eGovernments celebrado en Roma, Italia. Se incluye en este documento debido a que pertenece a una de las líneas de trabajo de la tesis más destacadas. En él se presenta una solución para la identificación de víctimas en entornos de emergencia basada en NFC y dispositivos móviles. Este trabado se puede ver en el Apéndice C, y ha sido presentado a un congreso internacional y actualmente, una mejora de esta investigación, ha sido enviada para una revista científica.

El objetivo principal de esta propuesta es mejorar la gestión del personal sanitario en situaciones de emergencia, lo que repercute en una mejor y más eficiente atención a las víctimas. Para lograr este objetivo, el sistema incluye diferentes aspectos. Uno de los más significativos es la implementación de algoritmos para la clasificación de las víctimas en escenarios de emergencia. Estos métodos se conocen tradicionalmente

como triaje. Un triaje puede definirse como un proceso simple, completo, objetivo y rápido cuyo fin es obtener una evaluación clínica inicial de las víctimas y de esta forma poder evaluar sus capacidades de supervivencia inmediata de las personas y priorizarlas de acuerdo a su gravedad [69]. En todos los sistemas de clasificación de víctimas se realizan dos pasos: un primer triaje o triaje simple cuyo objetivo es obtener una evaluación global de la capacidad de supervivencia de la víctima en tan sólo unos segundos, y un segundo triaje, en el que el personal médico evalúa el estado de cada paciente: lesiones, moretones y heridas. El primer triaje se realiza en la zona afectada de la emergencia, posteriormente se traslada a las víctimas a un Puesto Médico Avanzado (AMP, Advanced Medical Positions) donde se realiza el segundo triaje. Finalmente las víctimas son evacuadas a centros hospitalarios. En los métodos tradicionales de triaje, el resultado se almacena en etiquetas de papel de 10x20cm, donde el personal médico escribe la clasificación y el resultado del triaje con un bolígrafo.

En el sistema planteado, los médicos tienen un mapa en sus teléfonos móviles que les ayuda en todo momento a decidir la ruta a seguir para atender a las víctimas. Esta ruta se basa en la gravedad de las lesiones. De este modo, se evitan la duplicidad en la asignación de recursos a las víctimas y las decisiones se toman en función de la prioridad.

La generación de la ruta se desarrolla en dos etapas. La primera consiste en la evaluación del área afectada aplicando el método de triaje START para obtener una clasificación de las víctimas basada en etiquetas de colores. Cada color define la prioridad de la víctima, este resultado de color se almacena en las etiquetas NFC. Un miembro del personal médico es quien asigna las etiquetas NFC a las víctimas. Todas estas etiquetas contienen el resultado del triaje, es decir, el color de la clasificación del triaje, junto con la ubicación y el identificador físico de las tarjetas, mediante la utilización de un HMAC. Al final de este paso el sistema genera un mapa con la ubicación de cada víctima y el resultado de su triaje.

La segunda etapa se basa en la atención de la víctima teniendo en cuenta los resultados del primer triaje.

La aplicación incluye un chat de emergencia, mediante el cual se puede establecer un canal de comunicación alternativo para el envío de información. Todas las comunicaciones realizadas mediante este chat utilizan un sistema de cifrado y firma basado en identidad, en el que el número de colegiados es la clave pública de las mismas.

En la generación de las rutas de los médicos, se crea un grafo no dirigido a partir de los puntos definidos durante el triaje. Hay tantos puntos como pacientes en el mapa, estos son los vértices del grafo generado y los caminos que los conectan son las aristas, cuyo costes serán las distancias.

El sistema genera un grafo para cada color de triaje, el objetivo principal es tratar a los pacientes en función de sus lesiones. Una vez generado cada grafo se asignan la

cantidad de recursos que se necesitan, en este caso los recursos son médicos (número de médicos $\#d$) que asistirán a los pacientes. La primera aproximación del grafo se realiza basándose en la triangulación de Delaunay [22].

El siguiente paso es la realización de clústers para que cada médico tenga una zona que atender, y una ruta. En la propuesta el sistema genera un $k-partition$ [40], donde k es el número de médicos. El sistema asigna a cada médico, dependiendo de la ubicación, el nodo de mayor prioridad y más cercano.

A continuación, el sistema analiza la trayectoria de cada subgrafo. Este es el problema conocido como el Problema del Viajante de Comercio (TSP) [41] y se resuelve a través de un Algoritmo Genético [63].

Gracias a la división del trabajo y la creación de rutas automáticas para cada médico basado en las prioridades de las víctimas, se consigue mejorar la planificación de la emergencia, así como la reducción de los tiempos de asistencia.

3.4. Using blockchain in the follow-up of emergency situations related to events

En este cuarto artículo presentado en esta tesis [71] nos adentraremos en una solución basada en una de las tecnologías con más auge en la actualidad, la conocida cadena de bloques o blockchain. El documento publicado se encuentra en el Apéndice D y ha sido publicada en una revista de impacto en Diciembre de 2019, concretamente en la revista Software: Practice and Experience, la cual pertenece al cuartil Q2 de acuerdo con el Journal Citation Reports.

Concretamente mediante este trabajo se propone un sistema descentralizado de bajo coste mediante el uso práctico de blockchain que permite reforzar la seguridad en grandes eventos en caso de emergencia. La propuesta consiste en utilizar contratos inteligentes para la mejora de la gestión y monitorización de eventos que pueden ocurrir cotidianamente en las ciudades, sirviendo de apoyo para el manejo de recursos y el seguimiento del estado de las mismas.

La idea detrás de la propuesta es asociar las incidencias a los bloques en un contrato inteligente. Una vez que cualquier miembro de las organizaciones de emergencia detecta un incidente, se genera un nuevo bloque, el cual será incluido en la blockchain después de ser validado por el personal cercano. A continuación, se emiten alertas al resto del personal de emergencia que se ha asignado al evento. Como resultado, el personal de emergencia tiene acceso a la información del evento y puede actuar en función de ella. Debemos puntualizar que el contrato inteligente tiene que ser creado por algún miembro autorizado de un cuerpo de emergencia.

Inicialmente, la información sobre el evento y el personal de emergencia asignado se envía al contrato inteligente. Una vez que el evento está en la cadena de bloques,

el primer paso es la asignación de diferentes recursos de los servicios de emergencia a las áreas específicas para ayudar a preservar la seguridad civil.

Para evitar la congestión de la red, se ha previsto un sistema de comunicación alternativo para el personal de los servicios de emergencia y soportado por teléfonos móviles. Los datos compartidos a través de este nuevo canal de comunicación deben ser protegidos, para ello se ha propuesto en este trabajo un nuevo sistema de cifrado y firma basado en identidad. Soporta dos modos de comunicación diferentes: P2P y difusión. Cuando se activa el modo de emergencia, es necesario compartir la información pública de algunos usuarios que participan en el evento, como lo es su identificador. Esta información se comparte usando el modo baliza de BLE. Cada participante tiene una lista de identificadores (IDs) correspondientes a personas cercanas que están participando en el evento, la cual debe de ser pública para verificar quiénes son los participantes legítimos. Esto se consigue incluyendo dicha lista en el contrato inteligente.

En este trabajo se crea un nuevo tipo de esquema denominado: sistema de firma y cifrado basada en la identidad de los eventos, debido a que la identidad utilizada para las comunicaciones serán, no sólo la de los participantes, si no también la del evento en el que participan.

Cuando un miembro del personal de emergencia es asignado a un evento, el sistema genera credenciales específicas y claves para compartir datos. Los usuarios pueden obtener desde la aplicación móvil su propia ubicación, las ubicaciones de sus compañeros y el área de alcance del evento.

El sistema está diseñado para permitir que el personal de emergencias pueda enviar información de forma directa a un usuario específico o de forma masiva. La información del evento puede ser actualizada y enviada a la cadena de bloques tantas veces como sea necesario, generando un nuevo bloque que contenga la referencia al identificador del evento.

3.5. Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks

Este último trabajo presentado en esta sección [79] incluye una propuesta para la búsqueda de vulnerabilidades en una red de sensores y la presentación de diversas soluciones que eviten estas debilidades. Esta aportación se puede ver en el Apéndice E, la cual ha sido publicada en la revista Information systems en el año 2020, la cual pertenece al cuartil Q3 de acuerdo con el Journal Citation Reports.

Recientemente se han propuesto múltiples protocolos de autenticación e intercambio de claves autenticadas (AKE) y protocolos PAKE para redes de sensores heterogéneas. Los protocolos AKE se utilizan ampliamente en aplicaciones de red para

autenticación y control de acceso. Además, los protocolos PAKE permiten a los usuarios intercambiar y establecer una clave criptográfica segura basada en el conocimiento de una contraseña compartida de baja entropía.

En 2016, Chang-Le [15] propuso un protocolo 3-PAKE de dos factores, diseñado para solventar las vulnerabilidades de un protocolo anterior propuesto por Turkanovic. Basados es esta solución [21] y [39] realizaron un estudio de este protocolo, encontraron algunas vulnerabilidades y propusieron un protocolo mejorado. En la publicación incluida en el apéndice E se analizan esos tres trabajos, y se demuestra que los tres protocolos continúan siendo vulnerables.

El modelo de seguridad para los protocolos 3-PAKE asume que el comportamiento por parte del gateway es honesto pero curioso, es decir, confiable para permitir el intercambio de claves de sesión, pero no debería tener acceso a ellas.

Entre las vulnerabilidades encontradas en los protocolos analizados, se pueden destacar: debilidades en los flujos de comunicación, ataques semánticos, ataques de obtención de la clave de sesión mediante el acceso al gateway, ataques al anonimato de los usuarios, ataques de diccionario sin conexión y suplantación de identidad mediante la utilización de un sensor corrupto.

Una vez detectadas estas vulnerabilidades, se propusieron tres nuevas soluciones. Se definió un protocolo básico al que se le añadieron nuevas funcionalidades, lo cual incrementaba su complejidad computacional, concretamente se crearon los protocolos $\mathcal{P}_1$, $\mathcal{P}_2$ y $\mathcal{P}_3$, en donde $\mathcal{P}_1$ es el más sencillo y $\mathcal{P}_3$ el más seguro, pero más costoso.

El $\mathcal{P}_1$ se basa en un protocolos de intercambio de claves cifradas (EKE, Encrypted Key Exchange), en donde el cifrado se utiliza para enlazar los datos del usuario con el usuario, mientras que la autenticación se utiliza para enlazar los datos del servidor con el propio servidor. Esta primera aproximación carece de protección contra ataques de diccionario sin conexión, privacidad de las claves de sesión ni “forward secrecy”.

La siguiente propuesta es el protocolo $\mathcal{P}_2$, el cual mejora al anterior resolviendo las vulnerabilidades mencionadas.

Finalmente el protocolo $\mathcal{P}_3$ es una extensión del $\mathcal{P}_2$ que consigue un sistema completo 3-PAKE con anonimato para los usuarios.

En resumen, utilizando las tecnologías de identificación por radiofrecuencia (RFID y NFC), se propuso un nuevo protocolo 3-PAKE $\mathcal{P}_1$ que está diseñado para ser práctico, eficiente y abordar las limitaciones de las aplicaciones inalámbricas heterogéneas. A partir de este, se amplió para obtener los protocolos $\mathcal{P}_2$ y $\mathcal{P}_3$ los cuales posee características de seguridad adicionales. Estos protocolos son seguros en el modelo ROR previamente comentado y ofrecen protección contra una amplia gama de amenazas.

Capítulo 4

Conclusiones y líneas futuras

El objetivo del desarrollo de esta tesis ha sido la mejora de la seguridad de los entornos médicos, mediante el uso de herramientas criptográficas tales como la Criptografía Basada en Identidad y Blockchain.

Destacan las cuatro publicaciones en revistas con índice de impacto JCR aceptadas y publicadas durante el desarrollo de esta tesis.

Con el objetivo de completar el ámbito de desarrollo de la investigación realizada, también se añade un trabajo previo, remitido a una revista que actualmente se encuentra en fase de revisión.

Las publicaciones comparten un eje común: la definición, adaptación, implementación y validación de diversas primitivas criptográficas basadas en identidad en el entorno sanitario.

Dichas primitivas posibilitan el desarrollo de múltiples servicios de seguridad de la información orientados y adaptados a la complejidad de requerimientos del entorno mHealth.

Con esta tesis se justifica que el uso de la Criptografía Basada en Identidad en este entorno es especialmente adecuado por diversas razones que justificaremos a continuación. Por un lado, cada una de las aportaciones presentan soluciones a problemas detectados actualmente en este escenario, aportando diversas aproximaciones para escenarios complejos mediante la utilización de mecanismos de identificación, autenticación y validación de mensajes.

La colaboración con empresas externas del sector, así como las estancias internacionales realizadas le han dado un enfoque mucho más completo a la definición de soluciones. La creación de prototipos con las soluciones planteadas han permitido corroborar la funcionalidad de la investigación generada, dando un enfoque real y práctico a todo lo aportado.

Como resumen de todo el trabajo de esta tesis, podemos destacar algunas de las novedades aportadas en cada una de las propuestas que se presentan en este docu-

mento. La solución propuesta en el [74] se basa en un sistema móvil de apoyo a la detección y seguimiento de pacientes con TDHA. Para poder garantizar la seguridad de la información de los datos médicos utilizados en esta solución, se ha propuesto un esquema HIBE adaptado, para que la gestión de los datos médicos estén siempre bajo el control de los padres, apoyándonos en la utilización de tokens para el control de acceso. En la propuesta presentada en el documento [72], se presenta un sistema que pretende mejorar la eficacia de la atención de pacientes dentro del marco de la hospitalización médica. Concretamente se presenta un sistema de identificación de pacientes mediante el algoritmo HMAC y la utilización de pulseras NFC. Además, se propone una esquema de comunicación segura dentro del entorno hospitalario mediante la utilización de un sistema criptográfico basado en ID-AKE.

La única propuesta que se presenta en esta tesis que no es una aportación aceptada en una revista científica indexada es [70]. Se ha querido incluir debido a que ha sido una de las ideas planteadas desde el inicio del desarrollo de esta tesis y posee un gran potencial para poder mejorar la identificación de personas en situaciones de emergencia. Concretamente se pretende realizar una clasificación de víctimas en entornos hostiles mediante un triaje que es almacenado en etiquetas NFC, de esta forma, se puede tener un seguimiento del paciente offline y al llegar al hospital se puede leer toda la historia clínica de la emergencia mediante la lectura de la etiqueta.

La propuesta presentada en [71] pretende mostrar las posibilidades que nos aporta una tecnología como el Blockchain en la gestión de incidentes que ocurren en nuestro día a día. Esta aportación se apoya en la utilización de los contratos inteligentes así como de un sistema de comunicaciones peer-to-peer basados en BLE al que se le añade una capa de seguridad criptográfica mediante la utilización de IBSC. El uso de sensores médicos dentro del ámbito de mHealth es fundamental, cada día poseemos más mecanismos de monitorización para afrontar nuevas mejoras en la medicina, es por esto, que la propuesta presentada en el [79] pretende demostrar las vulnerabilidades que poseen algunos de los sistemas actuales de comunicaciones entre sensores (HWSN) y propone nuevos diseños criptográficos más seguros.

Una línea de trabajo que aún no ha sido explorada en profundidad es la seguridad en dispositivos médicos implantables. Durante la estancia realizada en la Florida State University se desarrolló una primera aproximación a diferentes ataques basados en descincronización de este tipo de dispositivos. Dados los avances que se han realizado en estos dispositivos y su cada vez mayor penetración, esta línea de trabajo merece sin duda un análisis profundo.

Capítulo 5

Conclusions and future work

The basis of the development of this thesis has been to give a practical approach to improving the safety of medical environments, by using technology in a safe way.

The four publications in journals with JCR impact index accepted and published since the beginning of this thesis are noteworthy. In addition, in order to complete the scope of development of the research carried out, a previous work, submitted to a journal that is currently under review, is also added.

The publications share a common axis: the definition, adaptation, implementation and validation of various identity-based cryptographic primitives. These primitives enable the development of multiple information security services oriented and adapted to the complexity of requirements of the mHealth environment.

With this thesis it is justified that the use of Identity-based Cryptography in this environment is specially suitable for several reasons that we will justify next. On the one hand, each of the contributions present solutions to problems currently detected in this scenario, providing different approaches for complex scenarios through the use of mechanisms for identification, authentication and validation of messages.

The collaboration with external companies in the sector, as well as the international stays carried out, have given a much more complete approach to the definition of solutions. The creation of prototypes with the proposed solutions has allowed to corroborate the functionality of the generated research, giving a real and practical approach to everything achieved.

All of these contributions are supported by their publication in prestigious journals and are added to the appendices of this document.

As a summary of all the work of this thesis, we can highlight some of the novelties contributed in each of the proposals presented in this document. The solution proposed in [74] is based on a mobile system to support the detection and monitoring of patients with ADHD. In order to guarantee the security of the information of the medical data used in this solution, an adapted HIBE scheme has been proposed, so that the

management of the medical data is always under the control of the parents, supported by the use of tokens for access control. In the proposal presented in the paper [72], a system is presented that aims to improve the efficiency of patient care within the framework of medical hospitalisation. Specifically, it presents a system for identifying patients using the HMAC algorithm and the use of NFC bracelets. In addition, a secure communication scheme within the hospital environment is proposed through the use of a cryptographic system based on ID-AKE.

The only proposal presented in this thesis that is not an accepted contribution in an indexed scientific journal is [70]. It has been included because it has been one of the ideas raised since the beginning of the development of this thesis and it has a great potential to improve the identification of people in emergency situations. Specifically, it is intended to carry out a classification of victims in hostile environments by means of a triage that is stored in NFC tags. In this way, it is possible to have a follow-up of the patient offline and when arriving at the hospital, all this medical history of the emergency can be read by reading the tag.

The proposal presented in [71] aims to show the possibilities that a technology like the Blockchain brings to the management of incidents that occur in our daily lives. This contribution is based on the use of intelligent contracts as well as a peer-to-peer communication system based on BLE to which a cryptographic security layer is added through the use of IBSC. The use of medical sensors within the scope of mHealth is fundamental, every day we have more monitoring mechanisms to address new improvements in medicine, which is why the proposal presented in [79] aims to demonstrate the vulnerabilities that some of the current systems of communications between sensors (HWSN) have and proposes new cryptographic designs more secure.

One line of work that has not yet been explored in depth is safety in implantable medical devices. During the stay at Florida State University, a first approach to different attacks based on the decynchronisation of this type of device was developed. Given the advances that have been made in these devices and their increasing penetration, this line of work undoubtedly deserves a thorough analysis.

Bibliografía

[1] Abd-alrazaq, A. A., Bewick, B. M., Farragher, T., and Gardner, P. (2019). Factors that affect the use of electronic personal health records among patients: A systematic review. *I. J. Medical Informatics*, 126:164–175.

[2] Amar, A. B., Kouki, A. B., and Cao, H. (2015). Power approaches for implantable medical devices. *Sensors*, 15(11):28889–28914.

[3] Becerra, J. (2019). *Provable Security Analysis for the Password Authenticated Key Exchange Problem*. PhD thesis, University of Luxembourg, Luxembourg.

[4] Bellare, M., Canetti, R., and Krawczyk, H. (1996). Message authentication using hash functions: The hmac construction. *RSA Laboratories' CryptoBytes*, 2(1):12–15.

[5] Bluetooth (2019a). Bluetooth 5. go faster. go further.

[6] Bluetooth (2019b). Bluetooth core specification v5.1. feature overview.

[7] Boneh, D. (1998). The decision diffie-hellman problem. In *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, pages 48–63.

[8] Boneh, D. and Franklin, M. K. (2003). Identity-based encryption from the weil pairing. *SIAM J. Comput.*, 32(3):586–615.

[9] Bos, J. W., Costello, C., Longa, P., and Naehrig, M. (2016). Selecting elliptic curves for cryptography: an efficiency and security analysis. *J. Cryptographic Engineering*, 6(4):259–286.

[10] Brier, E. and Joye, M. (2002). Weierstraß elliptic curves and side-channel attacks. In *Public Key Cryptography, 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002, Paris, France, February 12-14, 2002, Proceedings*, pages 335–345.

[11] Bulic, P., Kojek, G., and Biasizzo, A. (2019). Data transmission efficiency in bluetooth low energy versions. *Sensors*, 19(17):3746.

[12] Cao, Z., Chen, P., Ma, Z., Li, S., Gao, X., Wu, R., Pan, L., and Shi, Y. (2019). Near-field communication sensors. *Sensors*, 19(18):3947.

[13] CCN-CERT (2019). Ccn-cert ia-13/19 resumen ejecutivo. [online] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html.

[14] CCN-STIC (2018). Guía de seguridad de las tic ccn-stic 837. ens.seguridad en bluetooth. [online] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2707-ccn-stic-837-ens-seguridad-en-bluetooth/file.html.

[15] Chang, C. and Le, H. (2016). A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Trans. Wireless Communications*, 15(1):357–366.

[16] Chang, T. Y., Hwang, M., and Yang, C. C. (2017). Password authenticated key exchange and protected password change protocols. *Symmetry*, 9(8):134.

[17] Chen, H., Li, Y., and Ren, J. (2013). A practical identity-based signcryption scheme. *I. J. Network Security*, 15(6):484–489.

[18] Chen, H. and Zhang, C. (2019). Identity-based signatures in standard model. *Acta Inf.*, 56(6):471–486.

[19] Cheng, M., Li, L., Ren, Y., Lou, Y., and Gao, J. (2019). A hybrid method to extract clinical information from chinese electronic medical records. *IEEE Access*, 7:70624–70633.

[20] Chuah, J. W. (2014). The internet of things: An overview and new perspectives in systems design. In *2014 International Symposium on Integrated Circuits (ISIC), Singapore, December 10-12, 2014*, pages 216–219.

[21] Das, A. K., Kumari, S., Odelu, V., Li, X., Wu, F., and Huang, X. (2016). Provably secure user authentication and key agreement scheme for wireless sensor networks. *Security and Communication Networks*, 9(16):3670–3687.

[22] de Berg, M., Cheong, O., van Kreveld, M., and Overmars, M. (2008). Delaunay triangulations. *Computational Geometry: Algorithms and Applications*, pages 191–218.

[23] Dearlove, C. (2016). Identity-based signatures for mobile ad hoc network (MANET) routing protocols. *RFC*, 7859:1–17.

[24] Definition, N. R. T. (2006). Nfc forum technical specification.

[25] Diffie, W., van Oorschot, P. C., and Wiener, M. J. (1992). Authentication and authenticated key exchanges. *Des. Codes Cryptogr.*, 2(2):107–125.

[26] Edirisinghe, R., Stranieri, A., and Wickramasinghe, N. (2020). A taxonomy for mhealth. In *Virtual and Mobile Healthcare: Breakthroughs in Research and Practice*, pages 823–842. IGI Global.

[27] Emam, A., Mtibaa, A., and Harras, K. A. (2018). Message in a bottle: Extending communication coverage via boat-to-boat wifi communication. In *Proceedings of the 13th Workshop on Challenged Networks, CHANTS@MobiCom 2018, New Delhi, India, October 29, 2018*, pages 63–69.

[28] Emura, K., Katsumata, S., and Watanabe, Y. (2019). Identity-based encryption with security against the KGC: A formal model and its instantiation from lattices. In *Computer Security - ESORICS 2019 - 24th European Symposium on Research in Computer Security, Luxembourg, September 23-27, 2019, Proceedings, Part II*, pages 113–133.

[29] Ethereum (2019a). Solidity. https://solidity-es.readthedocs.io/es/latest/#. Accessed: Thu, 24 Sep 2019.

[30] Ethereum (2019b). Web3.js. https://web3js.readthedocs.io/en/1.0/. Accessed: Thu, 24 Sep 2019.

[31] Forster, A. (2016). *Introduction to wireless sensor networks*. John Wiley & Sons.

[32] García-Holgado, A., Marcos-Pablos, S., and García-Peñalvo, F. J. (2019). A model to define an ehealth technological ecosystem for caregivers. In *World Conference on Information Systems and Technologies*, pages 422–432. Springer.

[33] Garefalakis, T. (2002). The generalized weil pairing and the discrete logarithm problem on elliptic curves. In *LATIN 2002: Theoretical Informatics, 5th Latin American Symposium, Cancun, Mexico, April 3-6, 2002, Proceedings*, pages 118–130.

[34] Gartner (2019). Empresa consultora y de investigación de las tecnologías de la información gartner. [online] https://www.gartner.com/en.

[35] Gopal, S., Kaul, S. K., and Roy, S. (2018). Optimizing city-wide white-fi networks in TV white spaces. *IEEE Trans. Cogn. Comm. & Networking*, 4(4):749–763.

[36] Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., and Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy (S&P 2008), 18-21 May 2008, Oakland, California, USA*, pages 129–142.

[37] Hankerson, D. and Menezes, A. (2011). Elliptic curve discrete logarithm problem. In van Tilborg, H. C. A. and Jajodia, S., editors, *Encyclopedia of Cryptography and Security, 2nd Ed*, pages 397–400. Springer.

[38] Hasanova, H., Baek, U., Shin, M., Cho, K., and Kim, M. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *Int. Journal of Network Management*, 29(2).

[39] He, J., Yang, Z., Zhang, J., Liu, W., and Liu, C. (2018). On the security of a provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *International Journal of Distributed Sensor Networks*, 14(1) (2018).

[40] Hespanha, J. P. (2004). An efficient matlab algorithm for graph partitioning. *Santa Barbara, CA, USA: University of California*.

[41] Hoffman, K. L., Padberg, M., and Rinaldi, G. (2013). Traveling salesman problem. In *Encyclopedia of operations research and management science*, pages 1573–1578. Springer.

[42] Hou, J., Qu, L., and Shi, W. (2019). A survey on internet of things security from data perspectives. *Computer Networks*, 148:295–306.

[43] ISO/IEC 14443-3 (2018). Cards and security devices for personal identification - Contactless proximity objects.

[44] ISO/IEC 15693-1:2018 (2018). Cards and security devices for personal identification - Contactless vicinity objects - Part 1: Physical characteristics.

[45] Jefatura del Estado de España (2018). Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. [online] https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf.

[46] Jia, H., Chen, Y., Lan, J., Huang, K., and Wang, J. (2018). Efficient revocable hierarchical identity-based encryption using cryptographic accumulators. *Int. J. Inf. Sec.*, 17(4):477–490.

[47] JIS X 6319-4:2016 (2016). Specification of implementation for integrated circuit(s) cards - Part 4: High speed proximity cards (Foreign Standard).

[48] Jones, M. B., Bradley, J., and Sakimura, N. (2015a). JSON web token (JWT). *RFC*, 7519:1–30.

[49] Jones, M. B., Campbell, B., and Mortimore, C. (2015b). JSON web token (JWT) profile for oauth 2.0 client authentication and authorization grants. *RFC*, 7523:1–12.

[50] Joux, A. (2004). A one round protocol for tripartite diffie-hellman. *J. Cryptology*, 17(4):263–276.

[51] Kheir, M., Piuri, V., Karmakar, N., and You, I. (2019). IEEE access special section: Radio frequency identification and security techniques. *IEEE Access*, 7:172152–172155.

[52] Kochhar, A. and Kumar, N. (2019). Wireless sensor networks for greenhouses: An end-to-end review. *Computers and Electronics in Agriculture*, 163.

[53] Konstantinou, E., Klaoudatou, E., and Kamparmpakis, P. (2011). Performance evaluation of id-based group key agreement protocols. In *Sixth International Conference on Availability, Reliability and Security, ARES 2011, Vienna, Austria, August 22-26, 2011*, pages 377–384.

[54] Lee, J. H., Park, M., and Shah, S. C. (2018). Wi-fi direct based mobile ad hoc network. *CoRR*, abs/1810.06964.

[55] Li, X., Yang, D., Zeng, X., Chen, B., and Zhang, Y. (2019). Comments on "provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model". *IEEE Trans. Information Forensics and Security*, 14(12):3344–3345.

[56] Liu, J. and Liu, Z. (2019). A survey on security verification of blockchain smart contracts. *IEEE Access*, 7:77894–77904.

[57] López-Pérez, D., García-Rodríguez, A., Giordano, L. G., Kasslin, M., and Doppler, K. (2019). IEEE 802.11be extremely high throughput: The next generation of wi-fi technology beyond 802.11ax. *IEEE Communications Magazine*, 57(9):113–119.

[58] López-Villalobos, J., Serrano-Pintado, I., Andrés-De, J. L., Sánchez-Mateos, J., Alberola-López, S., and Sánchez-Azón, M. (2010). Usefulness of the stroop test in attention deficit hyperactivity disorder. *Revista de neurologia*, 50(6):333–340.

[59] Malone-Lee, J. (2002). Identity-based signcryption. *IACR Cryptology ePrint Archive*, 2002:98.

[60] McCallum, A., Nigam, K., et al. (1998). A comparison of event models for naive bayes text classification. In *AAAI-98 workshop on learning for text categorization*, volume 752-1, pages 41–48. Citeseer.

[61] Minerva, R., Biru, A., and Rotondi, D. (2015). Towards a definition of the internet of things (iot). *IEEE Internet Initiative*, 1(1):1–86.

[62] mondiale de la santé, O., Organization, W. H., and WHO (1992). *The ICD-10 classification of mental and behavioural disorders: clinical descriptions and diagnostic guidelines*, volume 1. World Health Organization.

[63] Mudaliar, D. N. and Modi, N. K. (2013). Unraveling travelling salesman problem by genetic algorithm using m-crossover operator. In *Signal Processing Image Processing & Pattern Recognition (ICSIPR), 2013 International Conference on*, pages 127–130. IEEE.

[64] NFC (2019). Nfc and contactless technologies. [online] https://nfc-forum.org/what-is-nfc/about-the-technology/.

[65] NFC, O. (2011). Type 5 tag operation specification.

[66] OWASP (2019). Owasp.org. [Online; accessed 13-November-2019].

[67] Park, Y., Park, Y., and Moon, S. (2013). Privacy-preserving id-based key agreement protocols for cluster-based manets. *IJAHUC*, 14(2):78–89.

[68] Peng, M., Kai, C., Cheng, X., and Zhou, Q. F. (2019). Network planning based on interference alignment in density wlans. *IEEE Access*, 7:70525–70534.

[69] Rivero-García, A., Hernández-Goya, C., Santos-González, I., and Caballero-Gil, P. (2014). Fasttriaje: A mobile system for victim classification in emergency situations. In *WEBIST 2014 - Proceedings of the 10th International Conference on Web Information Systems and Technologies, Volume 1, Barcelona, Spain, 3-5 April, 2014*, pages 238–242.

[70] Rivero-Garcıa, A., Santos-González, I., Goya, C. H., and Caballero-Gil, P. (2018). Secure communication system for emergency services in network congestion scenarios. *ICDS 2018*, page 63.

[71] Rivero-García, A., Santos-González, I., Hernández-Goya, C., and Caballero-Gil, P. (2019). Using blockchain in the follow-up of emergency situations related to events. *Software: Practice and Experience*.

[72] Rivero-García, A., Santos-González, I., Hernández-Goya, C., Caballero-Gil, P., and Yung, M. (2017). Patients' data management system protected by identity-based authentication and key exchange. *Sensors*, 17(4):733.

[73] Rodillo, B. E. (2015). Trastorno por déficit de atención e hiperactividad (tdah) en adolescentes. *Revista Médica Clínica Las Condes*, 26(1):52–59.

[74] Rodríguez-Pérez, N., Caballero-Gil, P., Rivero-García, A., and Toledo-Castro, J. (2018). A secure mhealth application for attention deficit and hyperactivity disorder. *Expert Systems*, page e12431.

[75] Roehrs, A., da Costa, C. A., and da Rosa Righi, R. (2017). Omniphr: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, 71:70–81.

[76] Roehrs A, da Costa CA, Righi RD and de Oliveira KS (2017). Personal health records: A systematic literature review. *J Med Internet Res*, 71:70–81.

[77] SA, I. (2018). 802.15.1-2005 - ieee standard for information technology– local and metropolitan area networks– specific requirements– part 15.1a: Wireless medium access control (mac) and physical layer (phy) specifications for wireless personal area networks (wpan). [online] https://standards.ieee.org/standard/802_15_1-2005.html.

[78] Santos-González, I., Rivero-García, A., Burmester, M., Munilla, J., and Caballero-Gil, P. (2020). Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks. *Inf. Syst.*, 88.

[79] Santos-González, I., Rivero-García, A., Burmester, M., Munilla, J., and Caballero-Gil, P. (2020). Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks. *Information Systems*, 88:101423.

[80] Selvam, S. (2017). Imaging biomaterial-associated inflammation. In *Monitoring and Evaluation of Biomaterials and their Performance In Vivo*, pages 47–68. Elsevier.

[81] Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, pages 47–53.

[82] Sharma, D. and Bhondekar, A. P. (2018). Traffic and energy aware routing for heterogeneous wireless sensor networks. *IEEE Communications Letters*, 22(8):1608–1611.

[83] Shi, P. and Zhang, W. (2015). Private information in healthcare utilization: specification of a copula-based hurdle model. *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, 178(2):337–361.

[84] SINTEF (2019). Organización de investigación independiente sintef. [online] https://www.sintef.no/.

[85] Steiner, M., Tsudik, G., and Waidner, M. (1996). Diffie-hellman key distribution extended to group communication. In *CCS '96, Proceedings of the 3rd ACM Conference on Computer and Communications Security, New Delhi, India, March 14-16, 1996*, pages 31–37.

[86] Tilborg, H. C. A. V. and Jajodia, S., editors (2011). *Encyclopedia of Cryptography and Security, 2nd Ed.* Springer.

[87] Tseng, Y., Tsai, T., Huang, S., and Huang, C. (2018). Identity-based encryption with cloud revocation authority and its applications. *IEEE Trans. Cloud Computing*, 6(4):1041–1053.

[88] Tseng, Y.-M., Huang, S.-S., Tsai, T.-T., and Tseng, L. (2015). A novel id-based authentication and key exchange protocol resistant to ephemeral-secret-leakage attacks for mobile devices. *International Journal of Distributed Sensor Networks*, 2015:76.

[89] Type 1, N. F. T. S. (2009). Type 1 tag operation specification.

[90] Type 2, N. F. T. S. (2009). Type 2 tag operation specification.

[91] Type 3, N. F. T. S. (2009). Type 3 tag operation specification.

[92] Type 4, N. F. T. S. (2009). Type 4 tag operation specification.

[93] van Tilborg, H. C. A. and Jajodia, S. (2011). Bilinear pairings. In van Tilborg, H. C. A. and Jajodia, S., editors, *Encyclopedia of Cryptography and Security, 2nd Ed*, page 82. Springer.

[94] Wang, X., Zhang, Y., Gupta, B. B., Zhu, H., and Liu, D. (2019). An identity-based signcryption on lattice without trapdoor. *J. UCS*, 25(3):282–293.

[95] Whalen, C. K. (1989). Attention deficit and hyperactivity disorders. In *Handbook of child psychopathology*, pages 131–169. Springer.

[96] Wu, T., Lee, Z., Obaidat, M. S., Kumari, S., Kumar, S., and Chen, C. (2020). An authenticated key exchange protocol for multi-server architecture in 5g networks. *IEEE Access*, 8:28096–28108.

[97] Xie, Q., Wong, D. S., Wang, G., Tan, X., Chen, K., and Fang, L. (2017). Provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model. *IEEE Trans. Information Forensics and Security*, 12(6):1382–1392.

[98] Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2019). Blockchain technology overview. *CoRR*, abs/1906.11078.

[99] Zeadally, S., Siddiqui, F., and Baig, Z. A. (2019). 25 years of bluetooth technology. *Future Internet*, 11(9):194.

[100] Zhou, Y., Yang, B., Hou, H., Zhang, L., Wang, T., and Hu, M. (2019). Continuous leakage-resilient identity-based encryption with tight security. *Comput. J.*, 62(8):1092–1105.

[101] Ziebell, R., Albors-Garrigos, J., Schultz, M., Schoeneberg, K., and Marin, M. R. P. (2019). ehr cloud transformation: Implementation approach and success factors. *IJIIT*, 15(1):1–21.

Apéndice A

A secure mHealth application for attention deficit and hyperactivity disorder

Received: 1 August 2018 | Revised: 12 March 2019 | Accepted: 28 April 2019
DOI: 10.1111/exsy.12431

WILEY Expert Systems

SPECIAL ISSUE PAPER

A secure mHealth application for attention deficit and hyperactivity disorder

Nayra Rodríguez-Pérez | Pino Caballero-Gil | Alexandra Rivero-García | Josué Toledo-Castro

Department of Computer Engineering and Systems, University of La Laguna, San Cristóbal de La Laguna, Spain

Correspondence
Nayra Rodríguez-Pérez, Department of Computer Engineering and Systems, University of La Laguna, San Cristóbal de La Laguna, Spain.
Email: mrodripe@ull.edu.es

Present Address
Nayra Rodríguez-Pérez, Department of Computer Engineering and Systems, University of La Laguna, San Cristóbal de La Laguna, S/C de Tenerife 38200, Spain

Funding information
Caja Canarias Foundation, Grant/Award Number: 2015 - DIG02-INSITU; MOTAM, Grant/Award Number: IDI-20160465; and TESIS2015010102

Abstract

Nowadays, many people have smartphones, the fact that encourages the development of new tools to address different problems. One of its consequences is the recent growth of mHealth, a term that refers to the practice of medicine based on the use of mobile devices for medical and health purposes. This work describes a new mHealth tool to improve memory and cognitive abilities through gamification and serious games. In particular, a mobile application here is proposed to help children that suffer from attention deficit hyperactivity disorder (ADHD). This application integrates the four profiles involved in this disorder: children, parents, teachers, and medical staff. With it, parents can discover if their children suffer the disorder, and children can improve their cognitive abilities through games of different types. Besides, the security aspect of the proposal is emphasized to highlight its importance in mHealth. Thus, the developed tool includes various cryptographic mechanisms to protect the confidentiality of communications and the authenticity of users and data.

KEYWORDS
ADHD, gamification, mobile application, mHealth, security

1 | INTRODUCTION

Currently, different methods can be used to assist in the treatment of some particular neurological disorders in order to help improve daily life. Besides, gamification techniques applied to this type of tools represent a fundamental way to enhance user engagement in the promotion of his/her cognitive abilities. A mobile application that allows the integration of the different profiles of people involved in attention deficit and hyperactivity disorder (ADHD) can facilitate the relationship between the affected person and his/her environment, as Rodillo (2015) explains. ADHD is a neurobiological disorder associated with a high functional, personal, and social impact. It is a chronic condition that begins in childhood and often persists in adolescence and adulthood age. It is characterized by symptoms such as inattention, hyperactivity, and impulsivity (Stevenson et al., 2007). These symptoms cause difficulties in multiple areas such as family functioning, academic, social, or work development (Campbell, 2000).

ADHD is the most prevalent psychopathology in childhood worldwide, and in fact, it is considered one of the most common childhood disorders (Polanczyk, De Lima, Horta, Biederman, & Rohde, 2007). Prevalence studies vary depending on diagnostic techniques, age, and the type of assessed population. Overall, it affects approximately 3-7% of the world's children. This rate decreases progressively as the age of the patient progresses. There are also variations depending on gender, sociocultural level, subtypes, and so forth. It is important to differentiate between the possible diagnosis of ADHD disorder and natural behaviour in children such as not paying attention, hearing little, or being very active. For this reason, parents and teachers should consult a medical specialist to obtain correct and complete clinical evaluation.

Currently, there are different methods to treat this disorder, based primarily on behavioural therapies, in addition to medication (Ota & DuPaul, 2002) and for National Collaborating Centre for Mental Health (Great Britain) (2011). The most common schemes consist of a progressive practice of specific tasks, recreational activities, and learning exercises oriented to the affected areas to improve the cognitive capacity of patients with

Abbreviations: ADHD, Attention Deficit Hyperactivity Disorder.

ADHD. These activities are based on daily exercise through tasks that stimulate different cognitive areas with games of calculation, attention, or reasoning.

The proposal presented here is composed of an interactive mobile application that can be used as a tool to improve the treatment of ADHD, as indicated in Whalen (1989) work. This scheme implies the creation of a network of people involved in child care, which allows the collection of data by the medical professional that can be visualized and evaluated to schedule possible intervention plans. Thus, one of the main functionalities of the application is the integration of different user profiles, with the aim of sharing relevant data among them. The main user profiles are the following:

- Parents. This role is played by parents or tutors of young people who may suffer ADHD. Through the application, they will be able to perform an initial prediagnosis and monitor their children progress.
- Medical staff. This role can be played by doctors, psychologists, psychiatrists, or educators involved in the treatment of a patient with ADHD. They will have access to the results obtained in the tests carried out by the tutors and will be able to track the follow-up of the progress of registered patients.
- Children. This role includes children that may suffer ADHD, so they will have access to different games whose final objective is the development and stimulation of various cognitive abilities.
- Teachers. A questionnaire on the patient's behaviour at school is available to teachers. They also have a chat to communicate with the patient's family members.

Currently, in many treatments of patients with neuro-behavioural disorders, the assessment for both diagnosis and treatment is still being carried out with pencil and paper. Recently, several mobile applications have been designed not only to replace traditional pen-and-papers methods but also to provide more accurate, objective, direct, and reliable recordings. The proposal described here has both goals and unites in a single scheme a tool to identify the symptoms to make a prediagnosis of ADHD, inform about ADHD, exercise cognitive abilities as part of ADHD treatment, follow up and evaluate the progress of ADHD symptomatology, update the planning of activities according to progress, and communicate with other involved actors.

The proposed application provides the tutors with an initial questionnaire consisting of questions about the behaviour and characteristics of the patient, which are based on the main criteria used to diagnose ADHD: DSMV-IV in the United States (SHAPSE, 2008) and ICD-10 in Europe (mondiale de la santé, O., Organization, W. H., & WHO, 1992). Subsequently, the gathered data are evaluated by medical staff, who will be responsible for diagnosing whether the patient suffers from the disorder or not. During this evaluation, both parents and medical staff can use an expert system to help in the diagnosis of ADHD. If ADHD is diagnosed, the responses of the questionnaire are used to estimate the ADHD level that the patient may suffer. After evaluating the results, the medical staff sends the obtained evaluation to the patient's tutors. Tutors will be able to register the child in the mobile application. For this purpose, some user data must be provided to guarantee his/her access to the mobile application. After registration, patients can access different multimodal activities available to help them improve their cognitive functions (memory, attention, language, perception, problem-solving, or planning).

The most important skills in the treatment of ADHD are memory and attention. Improving working memory produces positive effects by enhancing the ability of children with ADHD not to get distracted so quickly and decreasing hyperactivity, what helps improve school performance (Klingberg, Forssberg, & Westerberg, 2002). Work memory training sessions should be accompanied by feedback as a form of immediate reinforcement (Beck, Hanson, Puffenberger, Benninger, & Benninger, 2010). This is important because it is proven that to minimize ADHD symptoms, children must be motivated and stimulated effectively (Shaw & Lewis, 2005).

Early ADHD diagnosis and appropriate treatment may encourage a positive evolution. Therefore, the proposed application is intended to improve the quality of life of patients and their families, and their treatment through activities and exercises that strengthen their mental development. For this type of mHealth applications, it is necessary to establish a high level of security because medical data are defined as specially protected information and therefore must comply with the fundamental principles of protection. Thus, in the definition and implementation of the proposal, security has been treated as a key aspect.

This work is structured as follows. Section 2 describes some of the work related to the topic. The proposed system is detailed in Section 3, including the definition of the mobile application and the implemented games. Section 4 presents some details of the security protocols used in the proposal. Finally, Section 5 outlines some conclusions and future lines of research.

2 | RELATED WORKS

MHealth involves the use of mobile devices, communication technologies and networks, sensors, and so forth, for health care practice (Istepanian, Jovanov, & Zhang, 2004; Liu, Zhu, Holroyd, & Seng, 2011). MHealth applications can be used to improve the efficacy of health care service and promote the quality of health research (Kumar et al., 2013). This type of tools has proven to be useful especially to provide treatments for different neurological disorders. Mainly due to the widespread use of smartphones in modern society, great emphasis is being placed on the growth that has taken place in the development of mobile applications based on mHealth, with the aim of learning and supporting the treatment of different types of neurological disorder (East & Havard, 2015). For instance, mobile applications have been proposed for the treatment of eating disorders (Juarascio, Manasse, Goldstein, Forman, & Butryn, 2015; Fairburn & Rothwell, 2015).

With respect to ADHD, there are several mobile applications with different approaches. Some have an informative nature, promoting education and guaranteeing the quality of care through checklists (Psychiatry-Pocket, 2018; Adult-ADHD, 2018). Others provide mobile quizzes for ADHD diagnosis (ADHD-Test, 2018). Another group of applications allows the tracking and management of ADHD symptomatology (School-Psychology-Tools, 2018). Finally, there are several recently published apps that focus on games for ADHD treatment (Jumpy-Car, 2018; Magic-Land ; 2018). A recent project funded by the European Commission, entitled Web Health Application for ADHD Monitoring, is aimed at the use of technology in the ADHD intervention (Spachos et al., 2014).

Several papers have studied the effects of gamification on mobile learning applications for children. The effect of a language-based gamification application has been used as a source of study to examine the effect on first graders (Rachels & Rockinson-Szapkiw, 2018). Another paper includes a review of the characteristics and content quality of mHealth applications for bipolar disorder (Nicholas, Larsen, Proudfoot, & Christensen, 2015). Regarding gamification, the effects of this approach deployed in a learning management system were compared with those of a social networking site (De-Marcos, Domínguez, Saenz-de Navarrete, & Pagés, 2014).

With regard to the security of mHealth applications, many studies highlight the need to protect the medical data of users. Thus, mobile application developers must always consider the recommendations to comply with current privacy and security legislation (Martínez-Pérez, De La Torre-Díez, & López-Coronado, 2015), because the lack of security in mobile applications can cause serious data privacy problems that may have a huge impact on users (Jain & Shanbhag, 2012). Data leakage is one of the main problems in mHealth applications (Casati & Visconti, 2018). Nowadays, the development of mobile applications is usually performed according to a user-centric approach where privacy, security, and trust must be protected to ensure trouble-free functionality (Akram, Chen, López, Sauveron, & Yang, 2018).

The system proposed here involves an improvement over existing ones mainly because it includes the integration of the main actors in ADHD. In particular, a tool is provided with the aim of helping in the prediagnosis process of the disorder, and in the detection, monitoring and support during the ADHD treatment. Moreover, the designed and implemented system integrates security mechanisms to protect data integrity and user communications, and a Bayesian classifier to predict the probability of suffering ADHD according to a set of variables.

3 | PROPOSED SYSTEM

The proposal presented here is intended to serve as a tool that allows the diagnosis, follow-up, and improvement of the life of patients that suffer from ADHD. The first need of the family members is to resolve the uncertainty of whether their child may suffer from the disorder has been taken into account in the development of the application. Another aim is to help in the treatment and to favour the patient evolution. Moreover, it also defines a link among the main profiles involved in ADHD, in order to allow the flow of information among them. The developed system aims to unify the main functionalities in this type of medical applications. A secure mobile application is proposed that includes different functions for every proposed user profile. These roles are defined by the children's tutors, the medical team, and the children themselves. The main functionalities of this application are the early detection of the disorder through different questionnaires, the follow-up by a medical team of the evolution of those affected, and the treatment of cognitive functions such as attention or memory.

As shown in the general outline of the proposed system (see Figure 1), it has been designed following a client-server architecture. Thus, it has two main components: a web application and a mobile application. The web application is responsible for managing the users registered in the platform. The system administrator accesses the user views for each of the proposed application profiles. The views show a list of the users registered in a database for each available user profile (parents, medical staff, children, and teachers). Each profile has different privileges to access the data.

The main contribution of the proposal described here is the creation of a system that allows early diagnosis and monitoring of ADHD. On one hand, it combines the roles of the people who participate in the treatment of these disorders, thanks to the use of mobile devices. Parents can at any time assess their children's abilities as well as maintain direct communication with the medical team. All the mechanisms used in this system are presented as innovative solutions for the different problems detected in current proposals. On the other hand, the described system includes gamification mechanisms and serious games that help to improve the affected abilities in a fun and entertaining way for children suffering from this disorder. In particular, in this proposal, a Bayesian expert system has been implemented. The proposal has been developed by specialists in the sector, under the criteria of an expert knowledge on the treated condition. The mobile application focuses on their consultations and treatments, indicating a better monitoring of users. The dataset used in Table 4 is composed of the scores obtained by completing the proposed questionnaire and multiple sessions with the implemented games performed by a sample of potential users.

In the field of expert systems, the aim is to improve the prediagnosis of potential patients through completing several questionnaires without the need for an in-person formal medical appointment with the medical team. In this regard, the completion of questionnaires by the tutors together with the interaction with the proposed supervised mind games may improve the response time in the detection and treatment of ADHD of potential patients. In addition, it facilitates the repetition of ADHD tests and the proposal of new questionnaires by the medical team. On the other hand, although the prediagnosis system can rely on an expert system, the final decision corresponding to a potential patient, based on the initial questionnaire, is always carried out by the medical team. In this regard, it can be said that the system is proposed as a support for medical decision making.

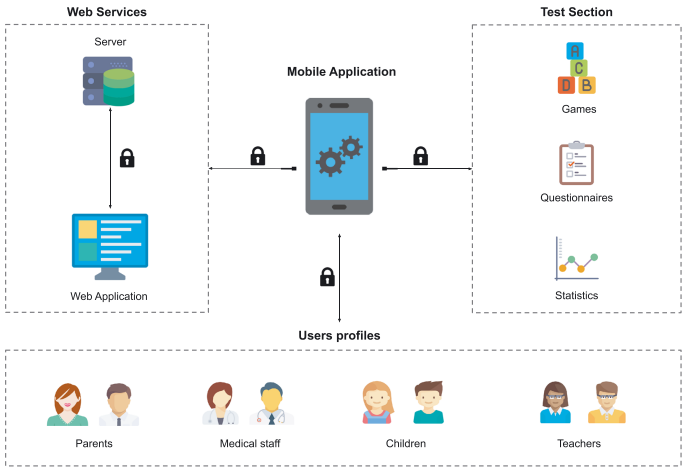


FIGURE 1 General outline of the proposed system

With respect to other aforementioned applications, the defined system pays special attention to the implementation of a more efficient remote prediagnosis method of ADHD method, and of a treatment platform designed to favour the analysis of the patient' progress, as well as the unification of all the necessary functionalities to improve the treatment.

The web application connects to an external cloud server in which queries are made to the database for different tasks, such as user identification and registration for each of the proposed user profiles. The Android operating system has been used for the development of the proposed system. The web application has been implemented on JavaScript, NodeJS, and Express. With respect to the database characteristics, a nonrelational document-oriented database (MongoDB) has been used that facilitates scaling information of the system and avoids SQL injection attacks. Regarding the web service, an API has been designed through the Representational State Transfer (REST) constrains. In this regard, JSON Web Token (JWT) standard has been used to verify the authenticity of the provided data and the authentication of users. In terms of the development, Git has been used for version control, and npm packages such as Gulp and Browsersync to automate coding tasks and accelerate the deployment of new code changes completed.

Once the potential user is signed up to the system through the implemented mobile application, the initial questionnaire is sent to the cloud server through secure requests using the Volley library (Android). The result of the questionnaire is notified to the corresponding medical staff through the client web application. In addition to studying the results of the questionnaires, the medical team analyses the results of the interactions of the potential patient with the proposed mind games and obtains medical conclusions, so that the database is updated with them. As a result, several interactive and linear charts implemented with Highcharts Javascript library are updated aiming to make the representation and interpretation of patient treatment results more efficient. On the mobile application side, HTTP GET requests are handled using Volley to obtain new medical conclusions made by the medical staff. In this way, the tutors can access the patient's information about prediagnosis and treatment at all times.

The proposed communication system is one of the most important aspects of the system because it implies a channel of direct and guided communication among the participants. Thus, because the security of this channel is very important, a hierarchical identity-based encryption has been proposed to protect it (De Caro & Iovino, 2011).

3.1 | Mobile application

The mobile application has been designed for the four main user profiles involved in ADHD (parents, children, medical staff, and teachers). The integration among the four profiles and the communications among them in a secure way have been the two main objectives of this work. The diagram shown in Figure 2 represents the main flow of the mobile application. Users registration in the system can be done either in the web application or in the mobile application. For security and integrity reasons, members of the medical staff and teachers are registered through the web application to verify their identities when the administrator enters them into the system. On the other hand, the relatives of the patient can register directly through the mobile application. In addition, from this profile, parents can register their children after diagnosis by doctors so that they can access the games integrated in the application.

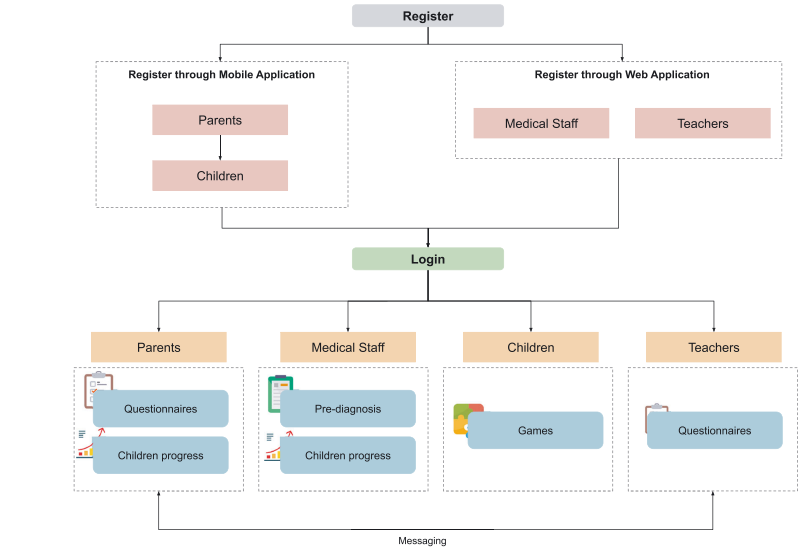


FIGURE 2 Flow chart scheme of the mobile application

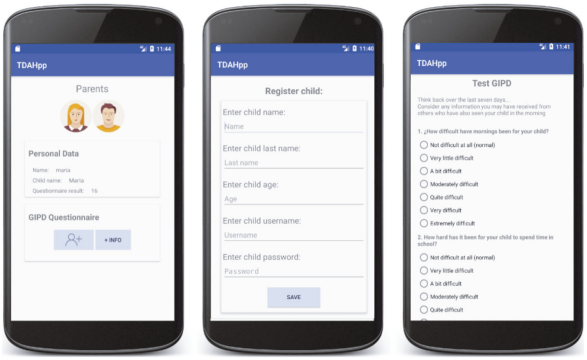


FIGURE 3 Screenshots of the parents profile

First, the parents' profile is defined for any tutor of the children, so that he/she can use it to consult an initial prediagnosis of their children, possibly backed by an expert system, receive the final diagnosis made by the medical staff, monitor the child's progress if he/she is under treatment, and communicate with the corresponding medical staff. Thus, the mobile application provides tutors with an initial questionnaire with children behaviour-based questions that includes several sets of questionnaires to assess the behaviour of the child in different situations and times of the day.

In this regard, in the first integrated questionnaires version of the system, the Global Impression of Perceived Difficulties (GIPD) scale was chosen as initial questionnaire for tutors, see Figure 3. The mobile application allows the tutors to answer this questionnaire and retrieve the results in order to send them to the cloud server. The purpose of the GIPD scale, composed of five items, is to assess the difficulties present in a child with ADHD in order to obtain information about the patient's symptoms and quality of life (Wehmeier, Schacht, Dittmann, & Döpfner, 2008). The scale assesses the difficulties encountered in the week prior to the assessment at different times of the day: in the morning, at school,

FIGURE 4 Screenshots of the medical staff profile

while doing homework, at night, throughout the day, and at night. The result of this initial questionnaire can be used to feed an expert system in the application, which provides a preliminary conclusion directly to the tutors. At the same time, the result of this initial questionnaire reaches the Web service, where it is stored in the database so that a member of the medical staff can evaluate it, to finally diagnose whether or not the patient suffers from the disease. After the diagnosis, from their role, the tutors can register a new user account for their child, indicating the necessary data for his/her login in the mobile application in order to have access to the games.

On the other hand, the profile of the medical staff includes the group of doctors, psychologists, or psychiatrists involved in the diagnosis or treatment of ADHD patients. Its main function is to carry out a follow-up study of assigned patients affected by ADHD. Medical staff can sign in to the system through the mobile application in order to access all answers of tutors or relatives once they have completed the questions proposed in the pre-diagnosis questionnaire. Depending on the obtained scores, the medical staff can make a prediagnosis on whether the corresponding potential patient suffers from ADHD or not, possibly relying on an expert system. Once this user profile is logged, two patient lists are displayed on the interface, one with undiagnosed patients (and therefore without an assigned physician) and another with patients assigned to the physician who is logged in (Figure 4). For each of the assigned patients, the mobile application allows the doctor to analyse their progress and visualize their corresponding data. In the information linked to each affected child, the doctor has access to the score obtained in the questionnaire completed by his/her tutors, and the scores obtained by the child in different games, allowing the visual analysis of his/her progression.

The mobile application also integrates the role of teachers (corresponding to the educational institution associated with the patient). This profile is fundamental as a source of information about the child's behaviour with regard to school background. Teachers of students with cognitive-behavioural disorders such as ADHD usually appreciate the collaboration with the family environment. In this regard, the mobile application is intended to promote communication and cooperation between both profiles, due to their participation in the evolution and learning of the child.

Finally, the users of the mobile application associated with the children profile are ADHD patients (potential or confirmed). Once this user profile signs in to the system, he/she has access to a gamification-based tool to help improve the treatment of ADHD through a series of games/activities that allow training cognitive and capacitive abilities (care, memory, or concentration). One of the main purposes taken into account when choosing the games for the application was to reinforce the effort rather than the achievement of results.

3.2 | Games

This work proposes the introduction of apps to help in the treatment of ADHD. Validation tests have been carried out on the mobile application on the basis of a functional perspective and technological performance, with the aim of analysing its reliability, usability, resource consumption, and other relevant aspects. Once the app is adopted by medical teams in an extensive way, specific details will be obtained on the effectiveness of gamification in the detection of ADHD based on validation by experimental results. After that, better thresholds will be established based on the results obtained from multiple tests.

Three main types of games have been included in the proposed mobile application system to help in the correct development of children's cognitive activities. Games can be used to enrich the teaching and learning process, but it is important to define the correct approach to use them for educational benefit. The activities initially included in the implemented application can be classified into colour sets, card games, and mathematical games (see Figure 5).

First, colour games are based on the identification of text and colours. The operation consists of showing the user a word with the text in a certain colour on a background of another colour, so that children must identify this colour among four proposed possible options. The

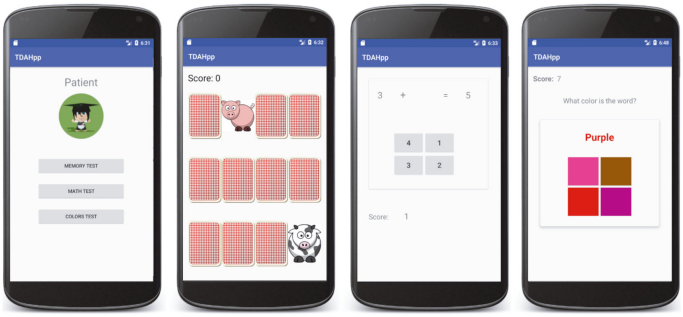


FIGURE 5 Screenshots of some games

TABLE 1 Training set

ADHD diagnosis	+	+	+	+	-	-	-	-
Questionnaire score	12	11	12	10	6	8	7	9

effectiveness of this game has been studied in different psychology papers such as López-Villalobos et al. (2010), where a measure of selective attention that requires interference resolution, response inhibition, and response selection, called the Stroop effect, is applied to semantic inference in the reaction time of this type of tasks. In particular, a delay in word colour processing has been identified in cases such as ADHD, which increases the reaction time and the error possibility.

Second, a game is proposed to improve children memory in a fun way in which concentration, attention, and focus are also trained. Its main function is to retain images and evoke stimuli that develop and strengthen children memory. A set of cards are shown face down on the board and the user must click on a couple of them to reveal them before they are either eliminated if it is a match, or hidden otherwise.

Finally, a game based on mathematical operations has also been included with the aim of developing mathematical thinking in those affected by ADHD. It is conceived as a didactic strategy that, in addition to helping concentration, exercises mental speed. Mathematics is chosen as the subject in this game due to the anxiety that this type of task usually produces in children with attention problems, concentration, or learning difficulties. The game consists of several mathematical operations that change as the child manages to do each of them. The main panel displays a mathematical operation hiding one of the elements, so the child must perform mental calculations to guess the missing element and choose it from the four options available.

3.3 | Classifier

Expert systems based on Bayesian networks are used in the mHealth field to predict the probability of suffering from a certain condition based on a set of variables. In this regard, they allow processing and interpreting the data to extract accurate knowledge to improve decision making in a more efficient way. Those systems are used to deal with problems related to uncertainty when a prior knowledge does not determine a conclusion but the relationship among the variables of a domain.

The proposed system includes a tool to produce numerical scores that can be used to estimate the level of ADHD through an expert system that determines a result from a set of symptoms. This provides physicians with a preclassification mechanism that allows them to visualize patients who require as a higher priority than the rest. This generates a much faster and more effective form of diagnosis than the existing evaluation methods in which patients face repeated questionnaires and continuous visits to the hospital, which can affect results and slow down progress.

The proposed application generates a series of data related to the obtained scores and the progress of the patients in the games available in the application. With the data generated by the application, an approximate classification of the children with the most urgent needs is made based on the use of the Naïve Bayes classifier technique (McCallum & Nigam, 1998). This probabilistic classification algorithm is based on the Bayesian theorem with naive assumptions of independence. The Bayesian theorem provides a way to calculate the posterior $P(A|B)$ probabilities from the prior probabilities $P(A)$ and$P(B)$, and the probability of B given A.

$$P(A|B) = \frac{P(A)P(B|A)}{P(B)}. \quad (1)$$

The application of the Naïve Bayes classifier to classify whether a child suffers from ADHD based on the answers to a questionnaire is briefly explained with a simple example. First, a training set is defined, for example (see Table 1).

TABLE 2 Mean and variance

ADHD diagnosis	+	-
Mean of questionnaire score	11,25	0,9167
Variance of questionnaire score	7,5	1,6667

TABLE 3 Average score in the games included in the system

Games	Max. score	Average score	Min. score
1. Maths	5	2	0
2. Colors	10	5	0
3. Cards	6	3	0
Questionnaires	15	10	5

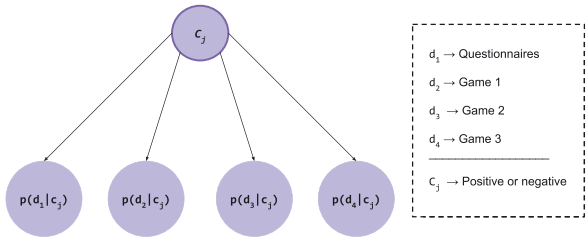


FIGURE 6 Probability classes

Using a Gaussian distribution assumption, the mean and variance are computed (see Table 2).

Assuming equiprobable cases with prior probabilities $P(+) = P(-) = 0,5$ based on the knowledge of frequencies in the cases of users of the application, in order to use the Naïve Bayes classifier on a sample of questionnaire score of value 8, the following formulas are applied:

$$P_{posterior}(+) = \frac{P_{prior}(+) \cdot P(score|+)}{P_{prior}(+) \cdot P(score|+) + P_{prior}(-) \cdot P(score|-)}, \quad (2)$$

$$P_{posterior}(-) = \frac{P_{prior}(-) \cdot P(score|-)}{P_{prior}(+) \cdot P(score|+) + P_{prior}(-) \cdot P(score|-)}, \quad (3)$$

where only the numerators are necessary to obtain a diagnosis. Thus, since using the parameters of normal distribution (4) so the predicted diagnosis is that the child does not suffer from ADHD.

$$P(score|+) = 1,3112 \cdot 10^{-3} \leq P(score|-) = 2,8669 \cdot 10^{-1}. \quad (4)$$

In particular for this system, the scores obtained in the games included in the application and the results of the questionnaire carried out by the tutors are computed according to this model. Each of the games has a range of scores from which each of the following characteristics is obtained:

- Initial questionnaire score (tutors)
- Math test score
- Colours test score
- Cards test score

For this particular model, the mean of the score values has been used to establish the theoretical threshold for a positive or negative ADHD diagnosis. The scores shown in Table 3 are established as a first approximation for this version of the system. Thus, when the scores are below the established threshold, a positive ADHD diagnosis is considered, whereas a negative progress is deduced.

On the basis of the Bayesian definition used in this system, a prior distribution training process has been carried out of the different characteristics proposed for the system, in order to determine an approximate classification of the users with the greatest evidences of suffering from ADHD.

A Bayesian network is represented by a directed acyclic graph in which each node represents a random variable that has a conditional probability function associated with it. The image shown in Figure 6 represents the characteristics caused by a class with a specific probability, using a structure of a simple Bayesian classifier with four variables. For this scheme, the independence of the proposed attributes is assumed because there is no relationship between them. The structure of this Bayesian network is based on a strong constraint: All the attributes that describe the cases are independent of each other given the value of the class.

TABLE 4 Values obtained in a data set

Questionnaires	Score maths	Score colors	Score cards	Diagnosis ADHD
25	2	5	1	positive
10	4	8	6	negative
30	2	2	1	positive
28	1	5	2	positive
10	4	8	5	negative
5	5	10	6	negative
33	1	4	2	positive
15	4	6	4	negative

TABLE 5 Gaussian parameters obtained in a training set

Games	Average positive	Variance positive	Average negative	Variance negative
1. Maths	1,6	0,3	4,2	0,2
2. Colors	4,2	1,7	8	2
3. Cards	1,8	0,7	5,4	0,8

The class will correspond to the unknown variable, the objective of the inference and its directed edges represent conditional dependences between variables and the class. The classification shall be carried out by inferring on the graph the subsequent probability of each of the values of the class, and selecting the value that maximizes this probability. Each node represents one of the variables d1, d2, …, dn, and each edge represents a direct dependency relationship between these variables. Thus, the estimate with all attributes is calculated using Equation (5).

$$P(d|cj) = P(d1|cj) * P(d2|cj) * P(d3|cj) * P(d4|cj). \quad (5)$$

Multiple tests have been done with the games and questionnaires available in the system to obtain a preliminary data set with which to make probability measurements. This dataset is obtained through the interaction of different potential patients with the implemented mobile tool and is evaluated by the proposed classifier and the expert knowledge consulted by specialists in the sector, whose objective is to provide the final diagnosis. These specialists have cooperated in the development of the implemented mobile application since its inception, in order to obtain a useful tool for better monitoring of potential or confirmed patients. Once expert knowledge is applied to the data set obtained from the games, it produces different positive and negative ADHD diagnosis scores. In this way, it is possible to train the tool through a Gaussian distribution where the mean and variance of each of the scores obtained in the games included in the system are obtained from the training set (see Tables 4 and 5). In this regard, the data represented in Table 4 is obtained through the use and interaction of the mobile application by a relevant sample of users, taking into account several use sessions.

By combining the processing of the results obtained in the different tests by the medical team and the evaluation of the classification process the speed of the application of a treatment for this pathology can be increased. The main objective of applying a classification method by the medical staff is to acquire knowledge from the data and be able to prioritize users with greater needs to be treated. In the web application of the system, the medical team is shown a list with the priority of the patients established through the Naïve Bayes classifier technique.

3.4 | Web service

The developed tool also has a web application for the administration of the users registered in the platform and the analysis of the obtained results. The web service is designed for two types of users: the system administrator and the medical staff. The system administrator is responsible for managing all users registered on the platform, viewing their personal information, removing users and authorizing access to the system. Doctors and teachers can only be registered in the application by the administrator to prevent unauthorized users from registering with those roles in the system.

The system manager accesses the user views for each of the application profiles (see Figure 7). The views show a list of the users registered in the database for each available profile (children, parents, medical staff, and teachers) from where he/she can view, delete, edit, and so forth.

Medical staff can also access the web service to view the progress of their patients. From this profile, the list of patients included in the system is displayed. For each of them, the probability of suffering from ADHD is shown in an ordered list with the highest priority patients first. In addition, by clicking on each of them, graphs with his/her progress in the different games of the system are shown (Figure 8).

4 | SECURITY OF THE PROPOSED SYSTEM

4.1 | Protection of data and communications

MHealth makes it possible to perform medical procedures, such as diagnoses, examinations, or treatment monitoring through mobile devices. The use of mobile devices for medical treatment requires a high level of responsibility to comply with the legal requirements for the protection of medical information. It is necessary to find the balance between the two opposing concepts of the guarantee of access to information and the

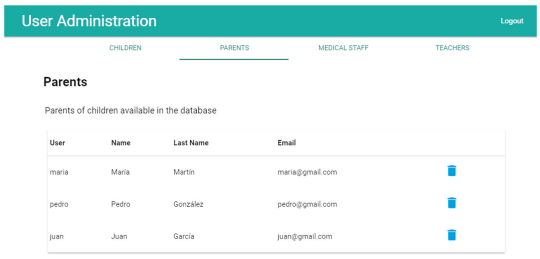


FIGURE 7 Administrator view of the web service

FIGURE 8 Medical staff view of the web service

protection of confidentiality and privacy of users. In addition, it is important to use a security model that guarantees the protection of medical information and complies with the new data protection regulations under the General Data Protection Regulation GDPR (2018).

In particular, health data are considered sensitive information that requires the highest level of protection, so their protection is of great importance, as detailed in Papageorgiou et al. (2018). This feature is essential to establish good compliance with the GDPR, which is intended to enhance and unify data protection for all individuals within the European Union and to restore the control over personal data by citizens as a primary objective. Because the developed application deals with medical and health data, it meets the requirement that all users of the system are informed about the use of their personal data. It includes a consent option so that the user can access all his/her personal information used or stored by the application. The purpose of the data processing is well defined in the application: no data are collected that is not used in the application and is not used for purposes other than those indicated. The user is informed of the use of his/her data at all times. Besides, additional measures are used to provide a high level of security in the processing of personal data.

In the development of the proposed system, the security of communications was addressed as one of the main issues. In order for the entire communication process to be managed securely when transferring data over the Internet, a series of security measures and best practices were taken. This was done mainly by using the HTTPS protocol, which provides Transport Layer Security (TLS) encryption so that requests and responses exchanged between client and server are encrypted with the Advanced Encryption Standard (McGrew & Bailey, 2012).

4.2 | Authentication token

The development of the proposed application followed the guidelines established by the Open Web Application Security Project (OWASP) for user authentication (OWASP, 2018). OWASP is a guide of rules and guidelines aimed at improving the security of applications. The used guidelines include the implementation of user authentication tokens and HTTPS requests. In addition, additional authentication mechanisms are executed on the server side. A checking procedure is performed to prevent the use of weak passwords, and key generation routines are established to generate strong enough passwords.

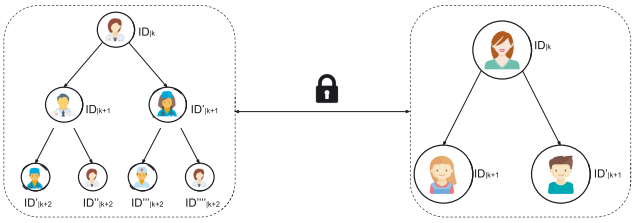


FIGURE 9 Identities scheme

Authentication tokens are used to guarantee the authenticity of the data issued in the exchange of information between the web application and the server. The generated tokens are containers of information regarding the user authentication. In general, the process is as follows: When a user logs in and sends his/her data to the server, the server generates a token encrypted with a secret key and then sends this encrypted token back to the user. Then, the token is sent in each request from the user. The server checks the token signature and verifies its information by decrypting it with the secret key. After this, if everything is correct, the information requested by the user is sent. The token is composed of attributes that identify the user, as well as the expiration date of the token and its validity.

The standard used in the system is the JSON Web Token (JWT) through the HS256 algorithm that uses the SHA256 hash function, JSON-Web-Token (2018). The token is composed of three general fields:

- Header, which contains the used algorithm and type of token.

$$\{\text{“}alg\text{”} : \text{“}HS256\text{”}, \text{“}typ\text{”} : \text{“}JWT\text{”}\}.$$

- Payload, with attributes that identify the user, as well as the expiration date of the token and its validity.

$$\{\text{“}sub\text{”} : \text{“}1234567890\text{”}, \text{“}name\text{”} : \text{“}JohnDoe\text{”}, \text{“}iat\text{”} : 1516239022\}.$$

- Verify signature, which contains the above elements encrypted with the secret key used for the token verification.

$$\{HMACSHA256(Encode(header) + \text{“.”} + Encode(payload), secret) secretEncoded\}.$$

Through this procedure, it is possible to control the authenticity of users and information exchanged among users of the system.

4.3 | Secure communication between different profiles

In the proposed system, a communication channel has been implemented to establish communication between the medical staff and the family of the affected children through a chat. The security of this channel is one of the most important objectives of the system, on the one hand because medical information is involved, and on the other hand because children may need to use it, so parents must have control of everything at all times.

In this work, an Identity-Based Encryption (IBE) has been implemented to achieve this objective. The purpose of IBE schemes is the use of any arbitrary string, such as a public identification such as email, identity card number, as a public key. Specifically, a Hierarchical Identity-Based Encryption (HIBE; Jia, Chen, Lan, Huang, & Wang, 2018) is used in the proposed scheme. This system supports revocation and delegation, because users can receive restricted private keys that allow delegation only to a limited depth in order to improve the scalability of the IBE scheme and facilitate private key delegation and revocation.

Figure 9 shows an example of the identities and the hierarchy used in the system. The left side represents an example of medical staff structure, where a main doctor controls the system while other people work in the same team (more doctors, nurses, psychologists, etc). On the right side, a family example is shown, with a tutor/mother/father of some patients, who in this case are two children.

The proposed system includes a central server with all the information, a Private Key Generator (*PKG*) that is a different server to generate medical staff private keys, and a mobile application. The identification of the participants are the emails used to be part of the system.

The implementation of the revocable HIBE is based on the following algorithms:

- *Setup* (k). This algorithm generates the system initialization parameters and the first level keys, k being the maximum hierarchy depth. This step takes place in the *PKG*. A master secret key (*msk*) is generated and, from it, a master public key (*mpk*), and an empty Revocation List (RL) that will be a set of parameters are generated.

- *KeyGen* ($sk_{ID_{lk}}$, *mpk*, ID_{lk+1}). This function generates the keys for each user in the PKG. To do this, the depth level of the user is obtained. If it belongs to a parent node, that is, if it is the parent of the child or the doctor responsible for the patient, the parameters are initialized to match the *msk* as follows: $sk_{ID_k} = msk$. If the user is a patient or a member of the medical team to whom the clinical case has been delegated, the following key is generated $sk_{ID_{k+1}}$.
- *Encrypt* (ID_{lk}, *M*, *mpk*). To encrypt messages, this function is used to generate as output the ciphered message *CM* from the identity, a message *M* and the parameters of the public key *mpk* and the *ID* of the receiver as input.
- *Decrypt* ($sk_{ID_{lk}}$, *CM*, *mpk*). The decryption algorithm is responsible for obtaining the original message *M* using the secret key $sk_{ID_{lk}}$, the ciphered message *CM* and the different parameters obtained from the public key *mpk*.
- *KeyUpdate* (*msk*, *RL*). In this step, the update of the *RL* is performed so that the output is the key update information *KU* at some time *t*. *DecKeyGen* ($sk_{ID_{lk}}$, *KU*). In this algorithm with a private key $sk_{ID_{lk}}$ and key update information KU, the system generates a decryption key $Dsk_{ID_{lk}}$. This decryption key can be used to decrypt or to know if an ID has been revoked.
- *KeyDelegate* ($sk_{ID_{lk}}$, ID_a). This step takes a private key for the identity ID and a user identity ID_a. Based on that information, the algorithm generates a new private key for the identity ID_a.
- *Revoke*(*ID*, *RL*). In his step, the system updates the revocation list RL and the state information of the system. To achieve this, the addition of a specific ID is performed.

Note that the steps *KeyGen*, *KeyUpdate*, *KeyDelegate* and *KeyDelegate* are performed through a secure channel based on user authentication tokens and HTTPS requests.

5 | CONCLUSIONS

The rapid deployment of smart mobile devices and their great potential have fostered the growth of mHealth through the emergence of a wide variety of mobile applications that require secure interfaces. This work includes the description of an Android mobile application that has been developed to integrate the four profiles of actors involved in ADHD: parents, teachers, medical staff, and children. The application includes three types of games that can be accessed through the children profile. Scores of games are estimated using a Naïve Bayes classifier and stored so that medical staff can track the results and progress of each patient. Parents can access to a prediagnosis system and track the results of their children. Teachers also have their own profile to provide information about children's behaviour through a questionnaire and access to a chat to communicate with parents. Finally, different functionalities of monitoring and generation of a final diagnosis for the medical staff have been integrated in the application so that when doctors access their profile, they can see two lists: with unassigned patients, and with their assigned patients and their results. In addition, different measures have been taken into account to achieve secure communications because it is important to guarantee that the data of the users of the proposed application cannot get compromised under any circumstances. Medical information requires a high level of protection, so in the development of the proposed system, different security measures have been applied to provide the application with privacy, confidentiality, and authenticity protection.

A chat has been included in the application to establish secure communications between users. As aforementioned, the security of this channel is one of the most important objectives of this work, so a HIBE is used in the proposed scheme to provide revocation and delegation features. Thanks to key delegation, both parents and doctors are in control of submitted and stored information. In particular, restricted private keys can be used to allow delegation only to a limited number of users in order to improve the scalability of the identity-based encryption scheme and to facilitate revocation.

This is part of a work in progress. The preliminary results of some experiments that are being carried out with real cases to evaluate the proposed tool are promising. Besides, as future work, further improvements are foreseen in the functionalities of the application and the security protocol used for communications between users.

ACKNOWLEDGEMENTS

Research supported by the CajaCanarias Foundation, the Centre for the Development of Industrial Technology, the Ministry of Economy, Industry, Commmerce and Knowledge, the European Social Fund and the University of La Laguna, under Projects DIG02-INSITU, IDI-20160465, and TESIS2015010102.

AUTHOR CONTRIBUTION

The authors equally contributed to this study.

ORCID

Nayra Rodríguez-Pérez https://orcid.org/0000-0002-7728-1360
Pino Caballero-Gil https://orcid.org/0000-0002-0859-5876
Alexandra Rivero-García https://orcid.org/0000-0003-1946-3403
Josué Toledo-Castro https://orcid.org/0000-0002-0245-8555

REFERENCES

ADHD-Test (2018). ADHS test application. https://play.google.com/store/apps/details?id=com.adhd.adhdtest. [Online; accessed 24-July-2008].

Adult-ADHD (2018). Adult ADHD add tips and support. https://itunes.apple.com/us/podcast/adult-adhd-add-tips-and-support/id988935339?mt=2. [Online; accessed 27-July-2008].

Akram, R. N., Chen, H.-H., López, J., Sauveron, D., & Yang, L. T. (2018). Security, privacy and trust of user-centric solutions. *Future Generation Computer Systems*, *80*, 417–420.

Beck, S. J., Hanson, C. A., Puffenberger, S. S., Benninger, K. L., & Benninger, W. B. (2010). A controlled trial of working memory training for children and adolescents with ADHD. *Journal of Clinical Child & Adolescent Psychology*, *39*(6), 825–836.

Campbell, S. B. (2000). Attention-deficit/hyperactivity disorder. In *Handbook of Developmental Psychopathology*. Boston, MA: Springer, pp. 383–401.

Casati, L., & Visconti, A. (2018). The dangers of rooting: data leakage detection in android applications. *Mobile Information Systems*, *2018*, Article ID 6020461, 9 pages.

De Caro, A., & Iovino, V. (2011). JPBC: Java pairing based cryptography. In *Proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC 2011*, IEEE, Kerkyra, Corfu, Greece, pp. 850–855. http://gas.dia.unisa.it/projects/jpbc/

De-Marcos, L., Domínguez, A., Saenz-de Navarrete, J., & Pagés, C. (2014). An empirical study comparing gamification and social networking on e-learning. *Computers & Education*, *75*, 82–91.

East, M. L., & Havard, B. C. (2015). Mental health mobile apps: from infusion to diffusion in the mental health social system. *JMIR mental health*, *2*(1), e10.

Fairburn, C. G., & Rothwell, E. R. (2015). Apps and eating disorders: a systematic clinical appraisal. *International Journal of Eating Disorders*, *48*(7), 1038–1046.

GDPR (2018). General data protection regulation. https://www.eugdpr.org/. [Online; accessed 26-June-2008].

Istepanian, R. S., Jovanov, E., & Zhang, Y. (2004). Guest editorial introduction to the special section on m-health: beyond seamless mobility and global wireless health-care connectivity. *IEEE Transactions on Information Technology in Biomedicine*, *8*(4), 405–414.

JSON-Web-Token (2018). Jwt.io. https://jwt.io/. [Online; accessed 09-July-2008].

Jain, A. K., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. *IT Professional*, *14*(5), 28–33.

Jia, H., Chen, Y., Lan, J., Huang, K., & Wang, J. (2018). Efficient revocable hierarchical identity-based encryption using cryptographic accumulators. *International Journal of Information Security*, *17*(4), 477–490. https://doi.org/10.1007/s10207-017-0387-8

Juarascio, A. S., Manasse, S. M., Goldstein, S. P., Forman, E. M., & Butryn, M. L. (2015). Review of smartphone applications for the treatment of eating disorders. *European Eating Disorders Review*, *23*(1), 1–11.

Jumpy-Car (2018). Jumpy card adhd. https://play.google.com/store/apps/details?id=pt.ivopintoo.jumpy.car.adhd.free. [Online; accessed 28-July-2008].

Klingberg, T., Forssberg, H., & Westerberg, H. (2002). Training of working memory in children with ADHD. *Journal of clinical and experimental neuropsychology*, *24*(6), 781–791.

Kumar, S., Nilsen, W. J., Abernethy, A., Atienza, A., Patrick, K., Pavel, M., ..., & Swendeman, D. (2013). Mobile health technology evaluation: the mhealth evidence workshop. *American journal of preventive medicine*, *45*(2), 228–236.

Liu, C., Zhu, Q., Holroyd, K. A., & Seng, E. K. (2011). Status and trends of mobile-health applications for iOS devices: a developer's perspective. *Journal of Systems and Software*, *84*(11), 2022–2033.

López-Villalobos, J., Serrano-Pintado, I., Andrés-De, J. L., Sánchez-Mateos, J., Alberola-López, S., & Sánchez-Azón, M. (2010). Usefulness of the Stroop test in attention deficit hyperactivity disorder. *Revista de neurologia*, *50*(6), 333–340.

Magic-Land (2018). Magic land adhd. https://www.apkmonk.com/app/com.jankopia.magiclandadhd/. [Online; accessed 22-July-2008].

Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: a review and recommendations. *Journal of medical systems*, *39*(1), 181.

McCallum, A., & Nigam, K. (1998). A comparison of event models for Naive Bayes text classification. In *AAAI-98 Workshop on Learning for Text Categorization*. Madison, Wisconsin; *752*, pp. 41–48.

McGrew, D., & Bailey, D. (2012). AES-CCM cipher suites for transport layer security (TLS).

mondiale de la santé, O., Organization, W. H., & WHO (1992). *The ICD-10 classification of mental and behavioural disorders: clinical descriptions and diagnostic guidelines*, Vol. 1. Geneva: World Health Organization.

National Collaborating Centre for Mental Health (Great Britain), National Institute for Health, Clinical Excellence (Great Britain), British Psychological Society, & Royal College of Psychiatrists (2011). *Common Mental Health Disorders: Identification and Pathways to Care*: RCPsych Publications.

Nicholas, J., Larsen, M. E., Proudfoot, J., & Christensen, H. (2015). Mobile apps for bipolar disorder: a systematic review of features and content quality. *Journal of medical Internet research*, *17*(8), e198.

OWASP (2018). Owasp.org. https://www.owasp.org/. [Online; accessed 13-July-2008].

Ota, K. R., & DuPaul, G. J. (2002). Task engagement and mathematics performance in children with attention-deficit hyperactivity disorder: effects of supplemental computer instruction. *School Psychology Quarterly*, *17*(3), 242.

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018). Security and privacy analysis of mobile health applications: the alarming state of practice. *IEEE Access*, *6*, 9390–9403.

Polanczyk, G., De Lima, M. S., Horta, B. L., Biederman, J., & Rohde, L. A. (2007). The worldwide prevalence of ADHD: a systematic review and metaregression analysis. *American journal of psychiatry*, *164*(6), 942–948.

Psychiatry-Pocket (2018). Psychiatry pocket application. https://play.google.com/store/apps/details?id=com.bbi.psychiatry_apocketcards, [Online; accessed 20-July-2008].

Rachels, J. R., & Rockinson-Szapkiw, A. J. (2018). The effects of a mobile gamification app on elementary students—Spanish achievement and self-efficacy. *Computer Assisted Language Learning*, *31*(1-2), 72–89.

Rodillo, B. E. (2015). Trastorno por déficit de atención e hiperactividad (tdah) en adolescentes. *Revista Médica Clínica Las Condes*, *26*(1), 52–59.

SHAPSE, S. N. (2008). The diagnostic and statistical manual of mental disorders.

School-Psychology-Tools (2018). School psychology tools. https://itunes.apple.com/es/app/school-psychology-tools/id435891534?mt=8, [Online; accessed 27-July-2008].

Shaw, R., & Lewis, V. (2005). The impact of computer-mediated and traditional academic task presentation on the performance and behaviour of children with adhd. *Journal of Research in Special Educational Needs*, *5*(2), 47–54.

Spachos, D., Chifari, A., Chiazzese, G., Merlo, G., Doherty, G., & Bamidis, P. (2014). WHAAM: A mobile application for ubiquitous monitoring of ADHD behaviors. In *2014 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)*, IEEE, Thessaloniki, Greece, pp. 305–309.

Stevenson, J., Everson, P., Williams, D., Hipskind, G., Grimes, M., & Mahoney, E. (2007). Attention deficit/hyperactivity disorder (ADHD) symptoms and digit ratios in a college sample. *American Journal of Human Biology*, *19*(1), 41–50.

Wehmeier, P. M., Schacht, A., Dittmann, R. W., & Döpfner, M. (2008). Global impression of perceived difficulties in children and adolescents with attention-deficit/hyperactivity disorder: reliability and validity of a new instrument assessing perceived difficulties from a patient, parent and physician perspective over the day. *Child and adolescent psychiatry and mental health*, *2*(1), 10.

Whalen, C. K. (1989). Attention deficit and hyperactivity disorders. In *Handbook of Child Psychopathology*. Boston, MA: Springer, pp. 131–169.

AUTHOR BIOGRAPHIES

Nayra Rodríguez-Pérez graduated as Computer Science Engineer in 2017 from the University of La Laguna and belongs to the CryptULL research group. She has participated in the research projects of the group and in various conferences. Her main expertise is in mobile development security.

Pino Caballero-Gil graduated with a BSc and a PhD in Mathematics from the University of La Laguna in 1990 and 1995, respectively. Since 1990 she has been with the University of La Laguna at the Department of Statistics, Operations Research and Computation where she is Full Professor of Computer Science and Artificial Intelligence. Her area of expertise includes security of wireless networks, cryptanalysis and cryptographic protocols. She leads the CryptULL research group devoted to the development of projects on Cryptology. She has authored many refereed conference papers, journal articles and books.

Alexandra Rivero-García is a PhD student in Secure Mobile Application Development. She graduated as Computer Science Engineer in 2013 from the University of La Laguna and belongs to the CryptULL research group. During her research period, she has participated in various national and international conferences and in the research projects of the group. Her main expertise is in computer security and reliability and computer communications.

Josué Toledo-Castro graduated as Computer Science Engineer in 2017 from the University of La Laguna. He is a member of CryptULL research group and participates in its research projects. His area of interest includes the development of secure mobile applications and wireless sensor networks (Internet of Things) in emergency situations and he has attended to different national and international conferences.

How to cite this article: Rodríguez-Pérez N, Caballero-Gil P, Rivero-García A, Toledo-Castro J. A secure mHealth application for attention deficit and hyperactivity disorder. *Expert Systems*. 2019;e12431. https://doi.org/10.1111/exsy.12431

Apéndice B

Patients' data management system protected by Identity-Based Authentication and Key Exchange

sensors

MDPI

Article

Patients' Data Management System Protected by Identity-Based Authentication and Key Exchange

Alexandra Rivero-García [1], Iván Santos-González [1], Candelaria Hernández-Goya [1], Pino Caballero-Gil [1,*] and Moti Yung [2]

[1] Department of Computer Engineering and Systems, University of La Laguna, 38206 Tenerife, Spain; ariverog@ull.edu.es (A.R.-G.); jsantosg@ull.edu.es (I.S.-G.); mchgoya@ull.edu.es (C.H.-G.)
[2] Computer Science Department, Snapchat and Columbia University, New York, NY 10027, USA; moti@cs.columbia.edu
* Correspondence: pcaballe@ull.edu.es

Academic Editor: Vittorio M. N. Passaro
Received: 31 January 2017; Accepted: 28 March 2017; Published: 31 March 2017

Abstract: A secure and distributed framework for the management of patients' information in emergency and hospitalization services is proposed here in order to seek improvements in efficiency and security in this important area. In particular, confidentiality protection, mutual authentication, and automatic identification of patients are provided. The proposed system is based on two types of devices: Near Field Communication (NFC) wristbands assigned to patients, and mobile devices assigned to medical staff. Two other main elements of the system are an intermediate server to manage the involved data, and a second server with a private key generator to define the information required to protect communications. An identity-based authentication and key exchange scheme is essential to provide confidential communication and mutual authentication between the medical staff and the private key generator through an intermediate server. The identification of patients is carried out through a keyed-hash message authentication code. Thanks to the combination of the aforementioned tools, a secure alternative mobile health (mHealth) scheme for managing patients' data is defined for emergency and hospitalization services. Different parts of the proposed system have been implemented, including mobile application, intermediate server, private key generator and communication channels. Apart from that, several simulations have been performed, and, compared with the current system, significant improvements in efficiency have been observed.

Keywords: identity-based cryptosystem; identity-based authentication and key exchange; mHealth; keyed-hash message authentication code; Android; NFC

1. Introduction

One of the most innovative paradigms of the last years in the healthcare sector is the integration of mobile devices in the practice of medicine and public health, known as mHealth. Its significance stems from the flexibility provided by the use of mobile devices. However, the potential security problems that arise from the use of mobile devices and their wireless interface must be carefully addressed due to the strict privacy requirements of medical data. In the work [1], a few recommendations to solve some of these problems are explained in detail.

This paper presents a secure and distributed system for the management of patients' data in emergency and hospitalization services with the primary goal of improving efficiency and security. In particular, several cryptographic protocols are used to protect the confidentiality of the communications and the access control to patient records.

The risk of patient misidentification is an issue to which health authorities pay a lot of attention, in order to try to avoid dangerous consequences such as medication errors, incorrect surgical procedures,

etc. [2]. In spite of that, statistical data on this subject are worrying. For example, in the UK, the National Health Service received more than 24,000 statements on misidentifications of patients in 2006–2007 [3].

One of the bases of the proposal is the use of Near Field Communication (NFC) [4], specifically NFC wristbands, for automatic patient identification. Unlike other technologies such as Radio Frequency IDentification (RFID) [5], Bluetooth or Wi-Fi [6], NFC is not oriented to continuous data transmission because it requires a temporal contact between the devices that interact in order to allow the exchange of information in a quick and timely manner. Although at first glance the distance factor for transmitting information may seem a limitation, it is actually a key point of this technology. The need for proximity between devices limits the types of attacks that can be launched. In addition, not requiring pairing between devices facilitates its use by medical staff.

Apart from the NFC wristbands , the other main components of the system are: a mobile device associated to each member of the medical staff, the intermediate server that hosts a web service, an NFC reader and writer for allocating wristbands once patients have been identified, and a second server in charge of producing information to protect the exchange of information.

This work is organized as follows. Section 2 provides some related works while Section 3 gives a general description of the proposed system. The topic of patient identification through NFC tags and keyed-Hash Message Authentication Code (HMAC) schemes in emergency and hospitalization services is dealt with in Section 4. The protection of communications between the medical staff and the intermediate server through Identity-Based Authentication and Key Exchange is proposed in Section 5. A brief security analysis is provided in Section 6. The implementation of parts of the proposal and simulations of the system are explained in Section 7. Finally, a few conclusions and future works close the paper.

2. Related Works

Recently, different solutions to solve specific problems in the management of the patients' data have been proposed. The security in healthcare applications is one of the most important points, even more when wireless sensor networks are used [7]. The specific case of wireless body area networks is very useful in healthcare, as shown in [8], where sensors are wearable devices that allow for obtaining, computing and distributing information about patients.

The data shared by these networks are usually stored as electronic health records so that the protection of the privacy of these records is very important. In the work [9], a system using an attribute-based infrastructure is proposed to preserve the privacy of the data. In that system, the registration of patients and doctors is performed with a username and a password, and the identification of the patient is a private user-index.

The so-called Personal Health Record (PHR) facilitates the management of medical records in a centralized way. One of the improvements obtained with the use of PHR is that patients can analyse their own information. In the work [10], a proposal of this kind of system is proposed based on the use of PHR in cloud computing, where an attribute-based encryption protocol is used to obtain the information. However, in that paper, the identification of patients and authentication of doctors are not explained.

Sharing medical care information in a secure way is proposed in the work [11], thanks to the use of role-based secure messaging services. The main problem of this approach is that a specific e-mail provider is used, and that the authentication is based on external tools.

In the paper [12], the authors introduce a mutual authentication scheme to improve the security of automatic systems for medication through RFID bracelets and cryptography based on elliptic curves. However, the used protocol does not provide a mechanism for session key generation to protect confidentiality.

There are proposals for medical systems that base their operation on the use of NFC bracelets. In the work [13], an example is shown where it is assumed that every day each patient uses a bracelet. If there is an emergency that requires checking of medical data, these are read using a mobile

application. A disadvantage of that application is that any user who has the application could perform an information query because there is no security mechanism implemented.

In the work [14], a system for the management of medical staff rounds is described that uses NFC wristbands and mobile devices. However, it does not specify whether security services are deployed or not.

The authors of the publication [15] developed an attack on a mutual authentication system based on RFID tags defined in [16]. Specifically, they show that it is possible to trace the tags so the protection of patient privacy is not guaranteed. At the same time, a new protocol is defined that solves the privacy problem and improves the efficiency of the system. An authentication scheme for the RFID tag is introduced, but it does not take into account the security of RFID readers. Apart from this, the server used to manage the information is also in charge of generating and storing the keys.

The proposal presented here includes automatic patient identification, mutual authentication between server and medical staff, and protection of confidentiality in the communications between the mobile device and the server. Confidentiality between the mobile device and wristband is warranted by the need for proximity to establish the NFC connection. Thus, this integration of security tools provides a robust solution that improves patient management and daily routine of medical staff.

3. System Overview

In most current health systems, when a patient arrives at a hospital, the fist step that the staff must do is to identify her/him. Patient identification is usually performed through the verification of a health identification card. Then, the patient is evaluated by a healthcare staff member who analyses the information collected during admission and adds the results of new assessments if required. Afterwards, the patient may be seen by a specialist. Before each one of these actions, the process of patient identification must be repeated. This current system has several drawbacks. Doctors must check the patient record before assisting her/him. In order to do it, depending on the particular case, they can make such a consultation through printed documentation or by using a computer. If paper documentation is used, it is usually generated as a batch for a set of patients. For example, three medical records may be printed at a time so that a doctor can check and attend those three patients one after the other. Once they are attended, the doctor should leave the records and repeat the process with a new group of patients. This arrangement produces heterogeneous information because some data may be updated on computers while other data are kept in printed format.

In addition, updates made by doctors are not changed in the central system in real time. In this approach, health workers have to deal with a lot of documentation, which leads to consuming considerable time and resources. On the other hand, each member of the medical staff has to visit several patients at each turn, which may generate wrong patient identifications, with serious consequences in some cases.

A solution to these issues is described in this work, which consists in the implementation of a secure system based on NFC wristbands and mobile devices that allow for eliminating patient misidentification and rationalizing the use of time in patient care.

The proposal involves substantial changes with respect to the traditional system. When patient identification is performed for the first time, an NFC wristband is assigned to him/her. Specifically, the NTAG21x ICs [17] wristband, which follows the pattern set by the NFC Forum (association that regulates the NFC standards) [18] is recommended here. This wristband will not be used to store any sensitive patient data. The only data stored on the wristband is an identifier assigned by the server. This identifier is generated through a process that will be discussed below. Such a generation takes into account the physical identifier of the wristband (similar to the Media Access Control (MAC) address number of computers) together with the patient record number. Note that this information will be written on the wristband in a completely secure way.

This wristband can be deployed both in the inpatient and emergency areas. It can be even assigned before the patient arrives to hospital, in the ambulance, where the identification and the writing procedures could be done through a mobile phone.

The data stored in the wristband allow any member of the medical staff with the right permissions access to the patient record identifying the patient with the simple gesture of bringing a mobile device close to the wristband. Thanks to the use of wristbands, the system prevents confusion when identifying patients and increases efficiency in the development of medical tasks. In addition, wristbands are fully recyclable, so when a patient leaves the hospital, its wristband is reset to be used by another patient.

The system is designed to work with two separated servers, here referred to as the intermediate server and second server. On the one hand, the intermediate server manages access permissions to patients' data on the basis of medical staff shifts. On the other hand, the second server uses a Private Key Generator (PKG) to manage the information related to keys.

The use of two different physical servers is proposed to add a new security layer in the management of the keys. With this separation, different firewalls can be added to each server independently and different secure rules can be applied in the communications between them. Specifically, the limitation of the communication of the private key server to intra-communication (intranet communications) is advisable. In other words, the communication of the PKG with the extranet can be denied and just some interactions with the intermediate server can be allowed through, for example, an intranet. In this way, if the intermediate server is corrupted by an attacker, both the private key generator and the server keys should not be involved. Although having two servers is more expensive than having just one, since nowadays the value of a dedicated server in the cloud is about $50 a year, we consider that this is a very low value when compared with the security that it brings to the proposed system.

The protection of patients' data is a paramount objective in the healthcare environment. This is why security is one of the pillars of the described solution. A keyed-Hash Message Authentication Code (HMAC) is applied for automatic patient identification, and IDentity-based (ID-based) cryptography is used to protect confidentiality of patient records.

The security of the communication between doctors and the intermediate server is based on an ID-based Authentication and a Key Exchange (AKE) scheme that provides mutual authentication between doctors and the server through a PKG. Next, the details on how these security tools are used in the proposed framework are included.

4. Automatic Patient Identification

As aforementioned, when a patient arrives at a hospital, the first step is the identification through his/her credentials. After that, in the proposal, an NFC wristband is assigned to him/her so that each patient is identified through an HMAC generated by the intermediate server by using the physical identifier of the wristband and the patient record number. If a patient does not have a medical record in the system, it is automatically created with some basic fields, such as name, age, country, etc.

The generation of the HMAC can be seen in Figure 1. The system sends the physical identifier of the wristband to the intermediate server, and two 64-byte arrays denoted as $ipad$ and $opad$ are generated as in the work [19], where some default values are assigned to them during the initialization of the HMAC generation. New arrays denoted by $ipad_{msk}$ and $opad_{msk}$ are generated through an bit level exclusive OR operation on $ipad$ and $opad$ respectively, and the master secret key (msk). Then, with the physical identifier of the wristband Tag ($idTag$) and the Patient Record Number ($PatRecN$), the system uses a SHA3-512 hash function [20] to generate the $HMAC$ value. Firstly, the hash function is applied to the concatenation of $ipad_{msk}$, $idTag$ and $PatRecN$. Secondly, the output of this hash function concatenated with the $opad_{msk}$ is the input to another hash function so that the $HMAC$ is the final result. This output is stored in the NFC wristband to be used as patient identifier.

When trying to access to a patient data, his/her NFC wristband must be read through a doctor's device, which sends the data obtained from the wristband, corresponding to the physical identifier of the wristband and the *HMAC*, to the server. The server verifies the authenticity of the bracelet and the doctor's access permissions. If the verification is positive, the authentication protocol described later is used each time a member of the medical staff needs to access to patients' data.

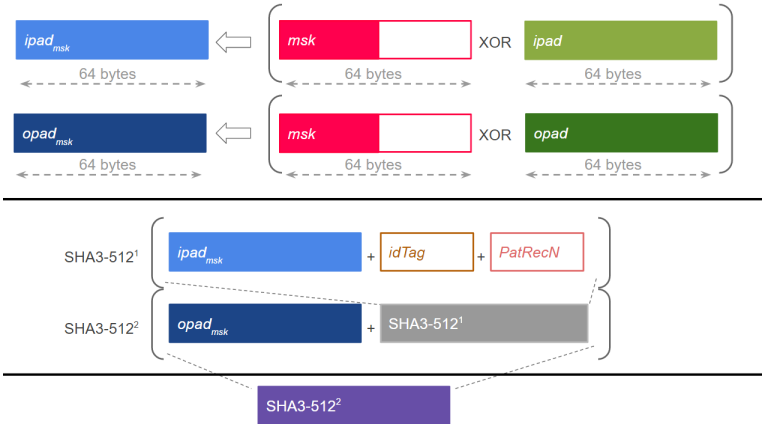


Figure 1. Keyed-hash message authentication code Generation.

The protection of communications is achieved through an ID-based scheme. In this type of public key cryptography schemes, any text can act as a valid public key with a PKG. The main reason to choose this approach for the proposal is the simplification of management because in this way it is not necessary to define a public key infrastructure. Furthermore, an ID-based scheme was chosen because of its low computational complexity and its efficiency in terms of memory and usability.

The description of all the steps of the communication flow during a medical record consultation between the participants in the system is included below (see Figure 2):

1. A member of the hospital admission staff receives the basic patient's data.
2. This patient's information is sent to the intermediate server. The identification of the patient is analysed at the server. If the patient is registered in the system, the server stores any new information and the system sends the verification to the web application. Otherwise, the server generates a new user identification and stores the corresponding data.
3. The assignation of a wristband to a patient starts with the reading of the physical identification of the tag *idTag* through an NFC reader.
4. The *idTag* is sent from the web application to the intermediate server, which links the *idTag* with the patient's medical record of number *PatRecN* and sends these values to the PKG in the second server.
5. The PKG generates the *HMAC* value with *idTag*, *PatRecN* and the pre-calculated values $ipad_{msk}$ and $opad_{msk}$. The *HMAC* value is sent to the intermediate server, which sends it to the web application.
6. The *HMAC* value is stored in the NFC tag of the patient's wristband.
7. When a doctor wants to identify a patient, he/she has to touch the NFC wristband with his/her mobile device to read both *idTag* and *HMAC*.

8. The stored values are sent from the mobile device to the intermediate server where the wristband is identified. The medical record is then loaded.
9. The intermediate server sends to the second server *idTag*, *HMAC* and *PatRecN*.
10. The PKG analyses and verifies the association, and the result of this verification is sent to the intermediate server.
11. If the *HMAC* verification is right, the server sends the medical record values to the mobile device where the doctor can read, edit or add data. The values corresponding to a patient can be modified until a new patient's wristband is read.

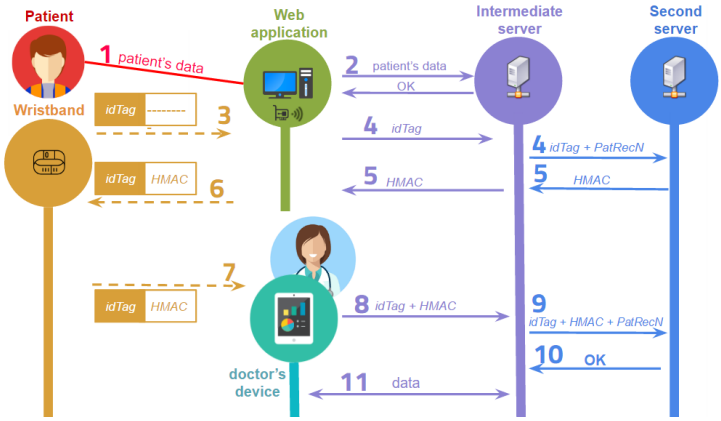


Figure 2. Medical record consultation.

5. Secure Communication

Communications between the mobile device of each member of the medical staff and the intermediate server are encrypted with an ID-based scheme.

A crucial element of the proposal is the Private Key Generator in the second server because it is in charge of generating private keys for medical staff. The identifier used in the system for each member of the medical staff is the corresponding number of registered medical practitioner. Specifically, the system is based on the proposal described in [21], but adapted to a more secure infrastructure where the PKG and the intermediate server are separated.

As seen in Figure 3, on the one hand, there are different devices assigned to doctors, which are smartphones or tablets with NFC reader and Wi-Fi. On the other hand, each patient has an NFC wristband. The intermediate server is the controller of the communication between the medical staff and the PKG. In particular, the intermediate server has a public Application Programming Interface (API) for doctors' communication and other hospital computers and a private API for communication with the PKG. Finally, the PKG is in charge of the authentication and verification of each communication. This is why server keys are stored in the PKG.

The protection of communications is achieved through an ID-based scheme. The first approach of this type of scheme was proposed by Shamir [22] in 1985 to avoid certificate management in asymmetric key systems. In this public key cryptography schemes, any text can be used as a valid public key. Specifically, the public key is usually extracted from some user's identity information, such as name, email or health identification. Following Shamir's idea, Boneh and Franklin proposed a practical

ID-based encryption system [23] based on the Weil pairing. Starting from this proposal, multiple ID-based schemes have been introduced. Some basic ID-based schemes may be identified depending on the type of security service to be implemented: ID-based encryption schemes [24–26], ID-based signature schemes [27,28], ID-based signcryption schemes [29,30], ID-based group key exchange protocols [31,32] and ID-based AKE [33,34].

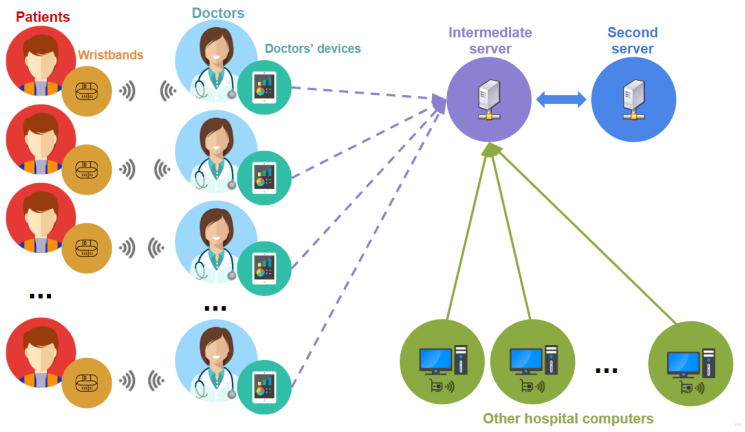


Figure 3. System's communication flow.

In the proposed system, mobile devices are used to manage patients' information. These devices have energy and computing capability limitations, so they should not depend on heavy cryptographic computations. Taking this into account, some protocols based on a client-server paradigm have been applied. One of the most used techniques to reduce the online cost is offline pre-computation. In the offline pre-computation used in this proposal, a few random values called ephemeral secrets are required to perform some operations in advance. These values are stored in the memory of the mobile device until the system requires them in the online step.

The attack called Ephemeral-Secret-Leakage (ESL) [35,36] might be launched in the online step. In order to be resistant to ESL attacks, the present proposal uses an ID-based AKE protocol that does not use bilinear pairings. Specifically, the scheme is based on the ESL-secure ID-based AKE protocol [21] that uses an ESL-secure signature scheme [37] to manage the client-to-server authentication and the Tate pairing [38], which is faster than the basic Weil pairing [39].

The notations used within this paper are introduced below:

- G, G_T : cyclic groups;
- P, P' : generators of the group G;
- $\hat{e}$: a bilinear map from $G \times G$ to G_T;
- msk : randomly selected master secret key;
- mpk : master public key;
- ID : IDentification of a registered medical practitioner;
- pgk_{ID} : private group key of the medical practitioners with ID;
- H_1, H_2, f : hash functions;
- $\{0,1\}^n$: space of all n-length binary vectors;
- $\{0,1\}^*$: space of all binary strings of any length;
- G^* : multiplicative group $G \backslash \{0\}$;

- $x \xleftarrow{r} S$: an element x is randomly selected from a set S;
- $||$: concatenation;
- $==$: comparison.

Next, the mathematical basis used in the system is described.

Considering two cyclic groups $(G, +)$ and $(G_T, \cdot)$ of the same prime order q, there is a symmetric bilinear map pairing $\hat{e} : G \times G \rightarrow G_T$ with the following properties:

- Bilinear: $\forall P, Q \in G$ and $\forall a, b \in \mathbb{Z}$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$;
- Non-degenerate: $\exists P_1, P_2 \in G$ that $\hat{e}(P_1, P_2) \neq 1$. This means that if P is generator of G, then $\hat{e}(P, P)$ is a generator of Q;
- Computable: There exists an efficient algorithm to compute $\hat{e}(P, Q), \forall P, Q \in G$.

Let a cyclic group $(G, +)$ have prime order q and P' be a generator of G; then, the following mathematical assumption based on the so-called Elliptic Curve Diffie-Hellman (ECDH) [40] problem can be considered. Given $P', aP', bP' \in G$ for unknown $a, b \in \mathbb{Z}_q$, the ECDH problem consists of computing abP'. No probabilistic polynomial time exists to allow an adversary to compute abP' with a non-negligible probability.

Two different types of hash functions are used.

On the one hand, two map-to-point hash functions:

$$H_1 : \{0,1\}^* \rightarrow G^*, H_2 : \{0,1\}^* \rightarrow G^*.$$

On the other hand, a one-way hash function:

$$f : \{0,1\}^* \rightarrow \{0,1\}^n,$$

where the size of the message is defined by n.

We assume that to concatenate a point P to a number N, the coordinates (P_x, P_y) of the point P are concatenated separately so that $P||N$ is equivalent to $P_x||P_y||N$.

The four steps needed for the ID-based AKE scheme are: Setup, Extract, Mutual Authentication and Session Key Generation.

- Setup: The initial parameters are established and the PKG in the second server generates the master public key mpk and the master secret key msk. For that, a prime q based on some private data $k \in \mathbb{Z}$, two groups G and G_T of order q and a symmetric bilinear pairing map $\hat{e} : G \times G \rightarrow G_T$ are selected. $P \in G$ is randomly chosen and the hash functions H_1, H_2 and f are used (see Figure 4).

$$msk \xleftarrow{r} \mathbb{Z}_q^*$$
$$mpk = msk \cdot P$$

Figure 4. Setup phase.

- Extract: The private group key for each member of the medical staff based on its ID is generated. The intermediate server generates a random number l, and sends it together with ID to the second server. Then, the PKG computes different values to obtain a private group key pgk_{ID}, which is calculated taking into account the master private key mpk. Finally, in the intermediate server, a secure channel is created based on an ECDH to share the private information with the doctor. A session key is generated to encrypt the information, obtaining an encrypted message C with a Snow 3G stream cipher algorithm [41] (see Figure 5).

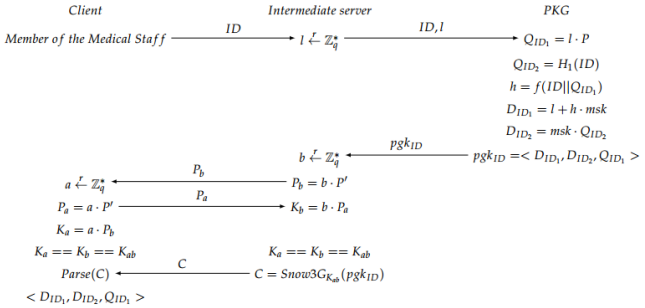


Figure 5. Extract phase.

- Mutual Authentication: Some offline computations are performed by the client to be able to perform mutual authentication. After the extract phase, the client generates and sends to the server a 3-tuple. Then, the server parses the tuple to obtain the values, and generates some new parameters. Afterwards, the server sends all the information to the PKG, who is in charge of the verification of the bilinear map pairing. If the verification is OK, the PKG sends a parameter to the server, otherwise a call "close" is sent back to the server to finish the communication. If the verification was OK, the server generates a tuple, which is sent to the client, which authenticates the server. If this authentication is OK, the client generates a parameter for its own authentication against the server and sends it back to the intermediate server, which verifies the user authentication (see Figure 6). If everything is OK, both client and server continue to the next step, which is the session key generation.

  Note that in the verification step carried out in the second server, the PKG checks whether the condition $\hat{e}(P,V) == \hat{e}(W_1,W)\hat{e}(mpk,W_2)$ is fulfilled in order to accept the communication. The justification of that condition is explained below:

$$\begin{aligned}
\hat{e}(P,V) &= \hat{e}(P, T + D_{ID_2}) \\
&= \hat{e}(P, (r + D_{ID_1}) \cdot W + D_{ID_2}) \\
&= \hat{e}(P, (r + l + h \cdot msk) \cdot W + msk \cdot Q_{ID_2}) \\
&= \hat{e}(P, (r + l) \cdot W + msk \cdot (h \cdot W + Q_{ID_2}) \\
&= \hat{e}(P, (r + l) \cdot W) \cdot \hat{e}(P, msk \cdot (h \cdot W + Q_{ID_2})) \\
&= \hat{e}(P \cdot (r + l), W) \cdot \hat{e}(P \cdot msk, h \cdot W + Q_{ID_2}) \\
&= \hat{e}(P \cdot r + P \cdot l, W) \cdot \hat{e}(mpk, h \cdot W + Q_{ID_2}) \\
&= \hat{e}(U_1 + Q_{ID_1}, W) \cdot \hat{e}(mpk, W_2) \\
&= \hat{e}(W_1, W) \cdot \hat{e}(mpk, W_2).
\end{aligned}$$

- Session Key Generation: When both server and client have been mutually authenticated, the session key (see Figure 7) is generated, at the same time, on the client side and on the server side. Afterwards, the exchanged messages are encrypted using the produced session key. In particular, the communication exchange between server and doctor is performed using the stream cipher SNOW 3G [42] using the obtained session key.

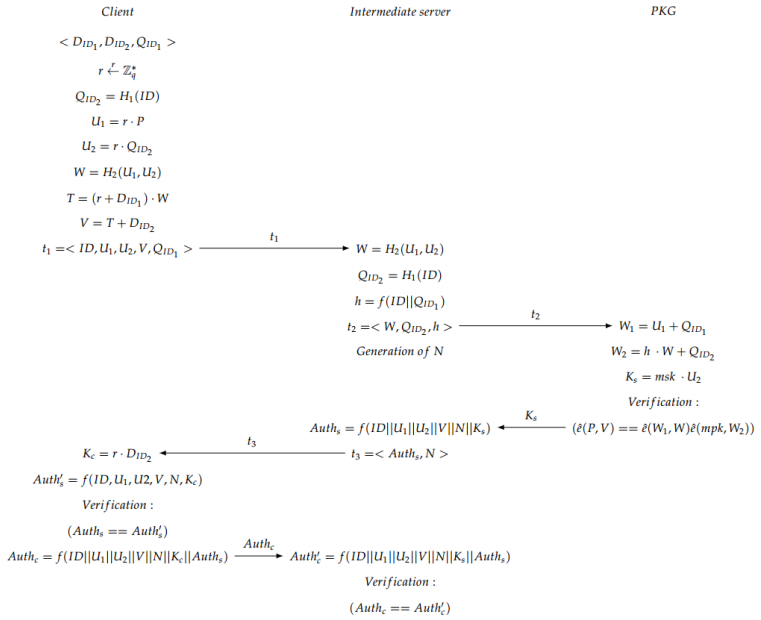


Figure 6. Mutual authentication phase.

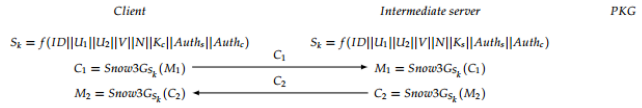


Figure 7. Session key generation.

6. Security Analysis

This section includes a brief review on the protection provided by the system against different types of attacks.

A spoofing attack and/or cloning of the card would be hardly successful in the proposal, since these types of attacks involve the generation of the HMAC, but this generation requires the server master private key, the ID of a registered medical practitioner and the patient record number. Even if an external attacker obtains this information, the combination between the physical identifier of the NFC wristband and the patient record number is unique.

If the attacker corrupts the data of the wristband, the system can easily detect it because the server can know that the information used by the attacker does not coincide with the stored data. Thus, one of the strong points of the proposal is that the data saved on the NFC wristbands are not sensitive data.

If an attacker wants to emulate the wristband with an Android device, the attack is detected because the application is restricted only to read passive NFC tags.

Denial of Service attacks based on overloading the server with a large number of false requests are restricted because only those requests associated to the ID of a registered medical practitioner will take effect. Once the corresponding private key is assigned, additional requests from the same number will not be attended.

Regarding Man in the Middle attacks, they would be easily detectable because the number of members who are allowed to make requests to the server is limited to those who are working at the time of the request.

Regarding ESL attacks, the corresponding security level is based on the primitive of the ESL-secure ID-AKE protocol for mobile client-server environments included in the scheme proposed. In addition, there is a client-to-server authentication that prevents an adversary can impersonate a legitimate medical staff person to share information with the server through the use of the ECDH problem. In the case of the server-to-client authentication, the same reasoning is applicable. The protection is provided through a mutual authentication scheme and a SNOW 3G stream cipher with shared secret key obtained by an ECDH scheme. Apart from this, a key agreement procedure is defined to obtain the key required to encrypt all the communications between the server and the clients through the same stream cipher. This key agreement provides protection under known-session-key attacks. Finally, an implicit implicit key confirmation is used based on a random oracle model, in order to offer partial forward secrecy in this model.

The system design includes two servers, the intermediate server and the second server with the private key generator. The use of two different physical servers is proposed to have an additional security layer for key management. In this way, firewalls can be added independently to each server, and different secure rules can be applied in the communications between them. In other words, the communication of the private key generator with the Extranet might be denied, and just some interactions with the intermediate server might be allowed through, for example, an Intranet. Furthermore, if the intermediate server is corrupted by an attacker, the key generator will not be affected.

7. Performance Analysis

Some basic prototypes of the proposal have been implemented on the client side, and the implementation is mainly formed by a web and a mobile application. On the server side, the prototype contains a data server and the private key generator. The web application is in charge of the management of patients' and doctors' information, and of the assignment of doctors to patients (see Figure 8).

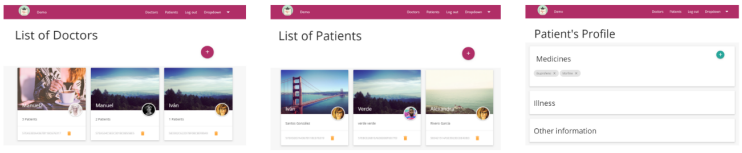


Figure 8. Web application.

Thanks to the mobile application, doctors can easily identify and analyse the patient record. The integration of the application with the NFC sensor of the smartphones has been implemented for the Android platform in order to read and write NFC tags in a secure way (see Figure 9).

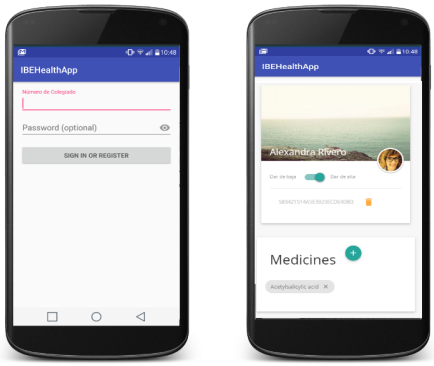


Figure 9. Mobile application. (**left**) View of registration; (**right**) View of patient data.

The data model for patient information is based on the clinic history containing is information related with affiliation data and health care data. Among the information related to the health, medical staff can analyse: reason for consultation (or hospitalization), personal history (allergies, habits, medical history, surgical history, family history, social history or current treatment), family background, current illness, anamnesis by organs, physical exploration results, differential diagnosis, supplementary tests, diagnostic trial and even the current therapeutic plan.

In the back-end side, the server was implemented based on a Model-View-Controller design pattern and with a non-relational database. On the one hand, the public access to the server was limited to restrict the access to the PKG, generated by a REpresentational State Transfer (REST) API. On the other hand, the internal communication between the server and the PKG is generated by a local REST API that has external restrictions, which means that a query can be generated only in the local site of the server.

The prototypes have undergone some tests. Since the HMAC generation depends on the server computer capabilities, different traces of the communication system were collected and evaluated. During these tests, the intermediate server was a computer with a quad core processor (Intel(R) Core(TM) i7-3537U CPU @ 2000 GHz) (Intel Corporation, Santa Clara, CA, USA), 4 GB of RAM memory, 1 TB of storage memory and the Windows 10 Pro version (×64 bits). This computer was used to access to the web application (see Figure 8) and patients' data. The private key generator was a similar computer, with an Intel i7-4702MQ processor (Intel(R) Core(TM) CPU @ 2000 GHz) (Intel Corporation, Santa Clara, CA, USA), 8 GB of RAM memory, 1 TB of storage memory and Windows 10 operating system version (×64 bits).

As the client, a Samsung Galaxy S6 (Samsung Electronics, Suwon, Korea) with Exynos 7420 octa core processor (Samsung Electronics, Suwon, Korea) (4 × 2.1 GHz Cortex-A57 4 × 1.5 GHz Cortex-A53), 3 GB of RAM memory, 32 GB of storage memory and the 6.0 Android version was used. In these experiments, an amount of 100 data packets were collected to be analysed in order to obtain results related with the overall response time.

The network used to perform all the tests was made up of a Tp-link TL-WR841N Wi-Fi router that theoretically offers a maximum transfer rate of 300 Mbps and an Internet connection of 100 Mbps. All communications were tested in the laboratory with the prototypes, obtaining a transmission time of less than 1 s. Taking these results into account, it may be stated that less than a minute is necessary both to assign a NFC wristband to a patient and to read patients' data.

Apart from implementing different parts of the proposal to show its feasibility, several simulations of its behaviour in a real environment have been done to measure some parameters that indicate improvements with respect to the current system.

One of the most important points of this proposal is to save time on the tasks of the medical staff. Currently, before assisting a patient, the doctor must review the patient record, which, in many cases, is printed and located in specific areas.

The mobility feature of the devices used in the proposed system allows for reducing the time spent by medical staff on roaming because they will not need to go to the documentation area and so they can attend patients without limitations.

Some simulations on the distribution of a floor in a real hospital (see Figure 10) have been performed. In this example, the orange zones are the areas where the hospital has the documentation areas for the doctors.

Figure 10. Hospital map.

For the simulations, the map of the floor was divided into four parts so that each one was run in a quarter of the map. A grid map of each part was generated to evaluate the route that doctors follow to visit each patient (see Figure 11). The best route in the current system consists of visiting patients located in adjoining rooms. In the simulation, it is assumed that there are two patients in each room.

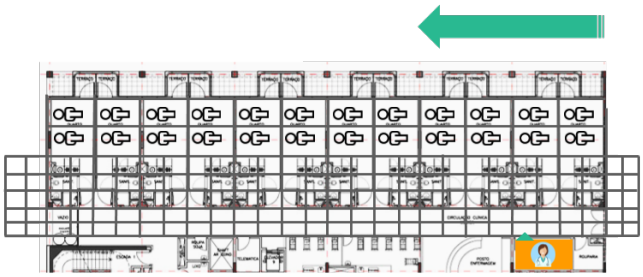


Figure 11. Grid map of the simulated area.

The time required for the doctor's route depends on the number of patients that a doctor can visit at once, that is to say, the size of the batches of patients that he/she has to visit before going back to the documentation area. In the proposed system, the time required for the doctor's route is always constant because it is assumed that he/she does not have to go to the documentation area. In Figure 12, a representation of the grid units covered by the physician can be observed. Blue bars reflect the grids covered in the current system while red ones show those required by the proposed system.

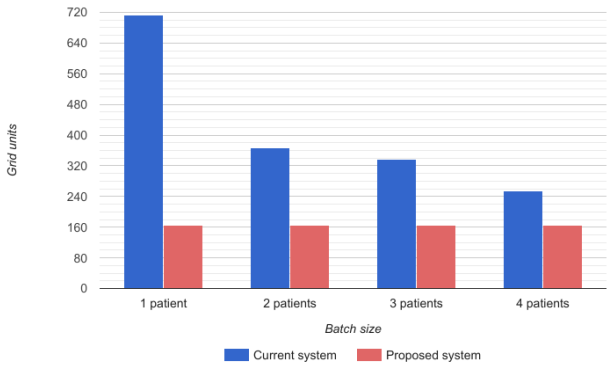


Figure 12. Time required for a doctor's route.

The improvement observed in the time consumed by each doctor in the route to attend patients in batches is increased by the saving on the time that the identification of patients requires since, with the proposed system, this identification is automatic thanks to the mobile devices of doctors and NFC wristbands of patients.

8. Conclusions

The identification of patients in emergency and hospitalization services is a major problem in the healthcare sector. The secure and efficient management of patient records is another key point. These two issues are addressed in this work through the proposal of a distributed framework for the secure management of patients' information.

The proposed system is based, on the one hand, on NFC wristbands assigned to patients and mobile devices assigned to medical staff, and, on the other hand, on two servers to manage patients' data and to generate private keys separately.

A modification of an ID-based Authentication and Key Exchange Protocol resistant to Ephemeral-Secret-Leakage attacks for mobile devices is presented in this paper to provide mutual authentication between server and health staff. Specifically, the proposed protocols include client-to-server authentication, server-to-client authentication, key agreement, implicit key confirmation and secure channel to share keys.

This is part of a work in progress. All the curves used in the performed beta implementation were chosen according to the National Institute of Standards and Technology suggestions [40] over $\mathbb{F}_p$, but in the next implementations, new curves over $\mathbb{F}_p^2$, and in particular the new curve called $Four\mathbb{Q}$, will be used to try to improve efficiency [43] in the implementation of the ECDH protocol on the most used processors in current smartphones. Furthermore, a future version of the system will include a robust and secure anonymity scheme based on pseudonyms. The issue of non-traceability of patients is also an open issue.

Finally, although some simulations were generated and the system was tested in the laboratory with some medical staff, in the immediate future, the system will be deployed in a real hospital to analyse the real improvements contributed by this proposal compared with the traditional method.

Acknowledgments: Research was supported by TESIS2015010102, TESIS2015010106, RTC-2014-1648-8, TEC2014-54110-R, MTM2015-69138-REDT, DIG02-INSITU and IDI-20160465.

Author Contributions: All the authors conceived the system, developed the algorithms and wrote the paper. Alexandra Rivero-García and Iván Santos-González performed the experiments. Candelaria Hernández-Goya, Pino Caballero-Gil and Moti Yung revised the work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Oakes, R.; Allen, C. mHealth Security: Best Practices and Industry Trends. Available online: http://www.oracle.com/us/corporate/profit/archives/opinion/011813-oakes-allen-1899091.html (accessed on 29 March 2016).
2. World Health Organization. *Field Review of Patient Safety Solutions*; World Health Organization: Geneva, Switzerland, 2008.
3. Pablo-Comeche, D.; Buitrago-Vera, C.; Meneu, R. Identificación inequívoca de pacientes. Evaluación del lanzamiento y su implantación en los hospitales de la Agencia Valenciana de Salud. *Med. Clín.* **2010**, *135*, 1–6. (In Spanish)
4. Want, R. Near field communication. *IEEE Pervasive Comput.* **2011**, *3*, 4–7.
5. Klaus, F. *RFID Handbook: Radio-Frequency Identification Fundamentals and Applications*; Wiley: Hoboken, NJ, USA, 1999.
6. Lee, J.S.; Su, Y.W.; Shen, C.C. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. In Proceedings of the 33rd Annual Conference of the IEEE Industrial Electronics Society, Taipei, Taiwan, 5–8 November 2007; pp. 46–51.
7. Kumar, P.; Lee, H.J. Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors* **2011**, *12*, 55–91.
8. Crosby, G.V.; Ghosh, T.; Murimi, R.; Chin, C.A. Wireless body area networks for healthcare: A survey. *Int. J. Ad Hoc Sens. Ubiquitous Comput.* **2012**, *3*, 1–26.
9. Narayan, S.; Gagné, M.; Safavi-Naini, R. Privacy preserving EHR system using attribute-based infrastructure. In Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, Chicago, IL, USA, 4 October 2010; pp. 47–52.
10. Li, M.; Yu, S.; Ren, K.; Lou, W. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Singapore, 7–10 September 2010; pp. 89–106.
11. Mont, M.C.; Bramhall, P.; Harrison, K. A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care. technology for privacy in health care. In Proceedings of the IEEE International Workshop on Database and Expert Systems Applications, 1–5 September 2003; pp. 432–437.
12. Jin, C.; Xu, C.; Zhang, X.; Li, F. A Secure ECC-based RFID Mutual Authentication Protocol to Enhance Patient Medication Safety. *J. Med. Syst.* **2015**, *40*, 1–6.
13. HealthID. Peace of Mind While Managing Your Health, 2016. Available online: https://www.healthid.com (accessed on 25 December 2016).
14. Köstinger, H.; Gobber, M.; Grechenig, T.; Tappeiner, B.; Schramm, W. Developing a NFC based patient identification and ward round system for mobile devices using the android platform. In Proceedings of the IEEE Point-of-Care Healthcare Technologies, Bangalore, India, 16–18 January 2013; pp. 176–179.
15. Lee, C.I.; Chien, H.Y. An Elliptic Curve Cryptography-Based RFID Authentication Securing E-Health System. *Int. J. Distrib. Sens. Netw.* **2015**, *2015*, 642425.
16. He, D.; Kumar, N.; Chilamkurti, N.; Lee, J.H. Lightweight ECC Based RFID Authentication Integrated with an ID Verifier Transfer Protocol. *J. Med. Syst.* **2014**, *38*, 1–6.
17. NXPSemiconductors. NTAG213/215/216. NFC Forum Type 2 Tag Compliant IC with 144/504/888 Bytes User Memory, 2015. Available online: http://www.nxp.com (accessed on 25 December 2016).
18. NFCForum. Official Web Page, 2016. Available online: http://nfc-forum.org/ (accessed on 25 December 2016).
19. Bellare, M.; Canetti, R.; Krawczyk, H. Message authentication using hash functions: The HMAC construction. *RSA Lab. CryptoBytes* **1996**, *2*, 12–15.
20. Bertoni, G.; Daemen, J.; Peeters, M.; van Assche, G. The Keccak SHA-3 Submission. Available online: http://keccak.noekeon.org/Keccak-submission-3.pdf (accessed on 31 March 2017).

21. Tseng, Y.M.; Huang, S.S.; Tsai, T.T.; Tseng, L. A novel ID-Based authentication and key exchange protocol resistant to ephemeral-secret-leakage attacks for mobile devices. *Int. J. Distrib. Sens. Netw.* **2015**, *2015*, 898716.
22. Shamir, A. Identity-based cryptosystems and signature schemes. In Proceedings of Workshop on the Theory and Application of Cryptographic Techniques, Paris, France, 9–11 April 1984; pp. 47–53.
23. Boneh, D.; Franklin, M. Identity-based encryption from the Weil pairing. In Proceedings of the Annual International Cryptology, Santa Barbara, CA, USA, 19–23 August 2001; pp. 213–229.
24. Das, M.L.; Saxena, A.; Gulati, V.P. A dynamic ID-based remote user authentication scheme. *IEEE Trans. Consum. Electron.* **2004**, *50*, 629–631.
25. Paterson, K.G. ID-based signatures from pairings on elliptic curves. *Electron. Lett.* **2002**, *38*, 1025–1026.
26. Gentry, C.; Silverberg, A. Hierarchical ID-based cryptography. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 1–5 December 2002; pp. 548–566.
27. Zhang, F.; Kim, K. ID-based blind signature and ring signature from pairings. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 1–5 December 2002; pp. 533–547.
28. Choon, J.C.; Cheon, J.H. An identity-based signature from gap Diffie-Hellman groups. In Proceedings of the International Workshop on Public Key Cryptography, Miami, FL, USA, 6–8 January 2003; pp. 18–30.
29. Boyen, X. Multipurpose identity-based signcryption. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2003; pp. 383–399.
30. Li, X.; He, M.X.; Luo, D.W. ID-based Signcryption Scheme. *Comput. Eng.* **2009**, *35*, 144–146.
31. Choi, K.Y.; Hwang, J.Y.; Lee, D.H. Efficient ID-based group key agreement with bilinear maps. In Proceedings of the International Workshop on Public Key Cryptography, Hong Kong, China, 13–15 December 2006; pp. 130–144.
32. Wu, T.Y.; Tseng, Y.M.; Tsai, T.T. A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants. *Comput. Netw.* **2012**, *56*, 2994–3006.
33. Zhu, R.W.; Yang, G.; Wong, D.S. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices. *Theor. Comput. Sci.* **2007**, *378*, 198–207.
34. Scott, M. Authenticated ID-based Key Exchange and remote log-in with simple token and PIN number. *IACR Cryptol. ePrint Arch.* **2002**, *2002*, 164.
35. LaMacchia, B.; Lauter, K.; Mityagin, A. Stronger security of authenticated key exchange. In Proceedings of the International Conference on Provable Security, Wollongong, Australia, 1–2 November 2007; pp. 1–16.
36. Islam, S.H. A provably secure ID-based mutual authentication and key agreement scheme for mobile multi-server environment without ESL attack. *Wirel. Pers. Commun.* **2014**, *79*, 1975–1991.
37. Tseng, Y.M.; Tsai, T.T.; Huang, S.S. Leakage-free ID-based signature. *Comput. J.* **2015**, *58*, 750–757.
38. Galbraith, S.D.; Harrison, K.; Soldera, D. Implementing the tate pairing. In Proceedings of the International Algorithmic Number Theory Symposium, Sydney, Australia, 7–12 July 2002; pp. 324–337.
39. Miller, V.S. The Weil pairing, and its efficient calculation. *J. Cryptol.* **2004**, *17*, 235–261.
40. Cheon, J.H. Security analysis of the strong Diffie-Hellman problem. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, 28 May–1 June 2006; pp. 1–11.
41. Kitsos, P.; Selimis, G.; Koufopavlou, O. High performance ASIC implementation of the SNOW 3G stream cipher. In Proceedings of the 16th IFIP WG 10.5/IEEE International Conference on Very Large Scale Integration (VLSI-SoC 2008), Rhodes Island, Greece, 13–15 October 2008; pp. 13–15.
42. Santos-González, I.; Rivero-García, A.; Caballero-Gil, P.; Hernández-Goya, C. Alternative Communication System for Emergency Situations. In Proceedings of the International Conference on Web Information Systems and Technologies (WEBIST 2014) , Barcelona, Spain, 3–5 April 2014; pp. 397–402.
43. Álvarez, R.; Santonja, J.; Zamora, A. Algorithms for Lightweight Key Exchange. In Proceedings of the 10th International Conference on Ubiquitous Computing and Ambient Intelligence, Gran Canaria, Spain, 29 November–2 December 2016; Part II, pp. 536–543.

Apéndice C

IBSC system for victims management in emergency scenarios

IBSC System for Victims Management in Emergency Scenarios

Alexandra Rivero-García, Iván Santos-González, Candelaria Hernández-Goya and Pino Caballero-Gil
Departamento de Ingeniería Informática y de Sistemas, Universidad de La Laguna, Tenerife, Spain

Keywords: Identity-based Signcryption, Keyed-Hash Message Authentication Code, Security, Triage, Emergency.

Abstract: This work describes an optimized system designed to help the greatest number of injured people in emergency situations, using the shortest possible time and cost. It is composed of a mobile application (assigned to medical staff and helpers), a web service and Near Field Communication wristbands assigned to victims. The mobile application is devoted to providing medical staff with the geolocation of victims as well as with an assistant indicating the best route to follow in order to take care of them based on the severity of their conditions and based on a triage method. Resolution of the routes is solved based on a classical problem, a Travelling Salesman Problem, using a k-parition algorithm to divide the huge number of victims in different clusters. Thus, each doctor has a specific area to assist victims. Besides, doctors can use a functionality of the application to contact their peers through a video call when additional help is needed. The proposal combines an keyed-Hash Message Authentication Code scheme to protect Near Field Communication tags and an IDentity-Based Cryptosystem to the wireless communication. Specifically an IDentity-Based Signcryption is used for communication confidentiality, authenticity and integrity, both among peers, and between server and medical staff.

1 INTRODUCTION

The communication technologies used in smartphones and the power of these devices can help in many complex scenarios. Smartphones are used to support different daily tasks, their small size and high performance is a huge advantage. This paper presents a platform for improving logistics of medical staff in emergency situations in a distributed way. In particular, it is based on data obtained from a triage application developed in (Rivero-Garcıa et al., 2014), where a mobile system for victim classification in emergency situations was implemented.

The definition of triage can be described as follows. A simple, complete, objective and fast process to obtain an initial clinical assessment of people with the objective of evaluating their immediate survival capacities and prioritizing them according their severity is a triage. In order to achieve the classification, all triage systems distinguish two steps. The first triage or simple triage is used for the generation of a classification based on the severity of injuries of the victims evaluating their survival skills in some seconds. The second triage is where medical staff analyses each patient's state: bruises, wounds and injuries. Specifically, in this work, Simple Triage and Rapid Treatment Algorithm (START) method is used as first triage. Its output is the victim's classification based on coloured tags, where each colour defines the priority of the victim: black, dead or irrecoverable victims; red, victims requiring immediate care; yellow, victims requiring urgent care but who can wait for treatment from half an hour to one hour; green, victims who are not seriously injured. They can wait for treatment more than an hour. Here the use of Near Field Communication (NFC) is proposed to deal with the triage result. NFC stickers are used to save triage results based on the generation of a keyed-Hash Message Authentication Code (HMAC) scheme. Furthermore, the route to attend victims for each doctor is shown through a map in their smartphones based on the priorities of victims and they can share information peer-to-peer with their colleagues in the affected area. All these communications are protected through an IDentity-based (ID-based) cryptography, specifically a ID-Based Signcryption scheme (IBSC).

This work is organized as follows. Section 2 provides some preliminaries while Section 3 gives a global view of the proposal. Then, Section 4 sketches the system that is used to make decisions. The topic of victim identification through NFC tags and HMAC schemes is dealt in Section 5. The protection of security related to the medical staff through an IBSC scheme is proposed in Section 6. A brief security ana-

Rivero-García, A., Santos-González, I., Hernández-Goya, C. and Caballero-Gil, P.
IBSC System for Victims Management in Emergency Scenarios.
DOI: 10.5220/0006298702760283
In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pages 276-283
ISBN: 978-989-758-245-5

lysis is provided in Section 7. Finally, a few conclusions and future works close the paper.

2 PRELIMINARIES

There are still some weaknesses in emergencies management. The integration of new technologies into emergency situations management and medical care has allowed the development of tools that help to the coordination between medical staff in emergency scenarios. There are different proposals designed to help to find missing persons after a large-scale disaster. Such as People Locator and ReUnite (of Medicine at NIH, 2017), Google person finder (Google, 2017) and Safety Check of Facebook (Facebook, 2017). All these systems try to verify and share the status of people after some disaster, specifically the proposal of Facebook share all the information with the victim's friends in this social network.

Some organizations are working to provide different solutions related to emergency situations. One of then is Sahana foundation (Foundation, 2017) project aims to provide a set of modular, web-based disaster management applications. This project includes tools for synchronization between multiple instances: a Missing Person Registry, Request and Pledge Management System and Volunteer coordination. Since this proposal is a web-based framework, it has the problem of relying on communication to the centralized web-server, and thus cannot take advantage of mobile nodes. There are no solutions to the identification of victims. The unique identification of affected people is a requirement for any emergency triage. Barcodes are a possibility because they facilitate mechanical reading (Neuenschwander et al., 2003). Barcodes are cheap and easy to create, they can be generated just using a standard printer. But in an emergency situation having a printer in the affected zone is not realistic. Radio Frequency IDentification (RFID) is a very useful technology for victim identification as it is explained in (Inoue et al., 2006) and in (Baracoda, 2017). Two types of tags exists, passive tags, that use the energy received from the reader to send the identifier, and active tags, that include a battery to increase its distance range. The problem of this kind of communication is that a RFID reader is needed and no security tools were provided. In (Gao et al., 2007) a specific triage tag technology is proposed. These electronic triage tags use noninvasive biomedical sensors to continuously monitor the vital signs of a patient and deliver pertinent information to first responders. These are not triage tag for emergency situations.

The use of NFC (Near Field Communication)(Want, 2011a) is one of the bases of the proposed system, specifically NFC stickers, for automatic patient identification. Unlike other technologies as RFID (Zou et al., 2014), Bluetooth or Wi-Fi (Lee et al., 2007), NFC is not oriented to the continuous data transmission. It is necessary a temporally contact between the devices that interact to allow the exchange of information in a quick and timely way. Although, at first, the distance factor for transmitting information may seem a limitation it is actually the key in this technology. The need for proximity between devices limits the types of attacks to develop. Besides, not requiring pairing between devices facilitates its use by health staff. NFC devices may operate in two different modes. On the one hand, in the active mode each device generates its own electromagnetic field (emulating the communication paradigm peer-to-peer). On the other hand, in the passive mode one device generates the electromagnetic field with its own power supply. In this way, it enables that other device starts the connection taking energy from the field generated to power its circuit. Then the passive device generates the response signal and transfers the data. This mode of operation matches with the RFID communication model and it is the one used in this proposal.

3 GLOBAL VIEW

The main objective of the proposal is to generate a tool to save as many time as possible in emergency situations. Therefore, doctors have a map in their mobile phones that helps them in every moment to decide the route to patients. This route is based on the severity of the injuries. Thus, collisions of doctors to assist the same patient are avoided and decisions are taken based on priority.

Two stages in the route generation are made. The first one consists in the evaluation of the affected area applying START triage method to obtain a victims' classification based on coloured tags. This is generated by the first aid team, where there are medical staff, firefighters or even rescue services.

As we mentioned previously, each colour defines the priority of the victim: black, dead or irrecoverable victims; red, victims requiring immediate care; yellow, victims requiring urgent care but who can wait for treatment from half an hour to one hour; green, victims who are not seriously injured. They can wait for treatment more than an hour. This colour result is stored on tags. In this case NFC (Want, 2011b) tags, specifically NFC stickers are used to save the triage

result. Note the proposed work uses NFC stickers but multiple kind of NFC tags can be used, depending on the emergency and the victims state. Each triage has a location in the central server. At the end of this step the system has a map with the location of each victim and their triage like in figure1.

Figure 1: Victims' location.

The second stage is based on the victim's attention taking into account the results of the triage priorities. In this step the victims' locations given by the first triage is essential being the starting point. A graph of each colour is generated based on the victim's location in a map. Victims represent nodes and the routes to reach them are de edges. Each edge has a cost. This cost is the distance between two nodes calculated through the Haversine Formula (Knox, 2015), where $cos_{\gamma_{AB}\Delta\lambda} = cos(\gamma_A) \cdot cos(\gamma_B) \cdot hvsin(\Delta\lambda)$, then:

$$hvsin(\frac{d}{R}) = hvsin(\gamma_A - \gamma_B) + cos_{\gamma_{AB}\Delta\lambda} \quad (1)$$

Where hvsin is the haversine function:

$$hvsin(\theta) = sen^2(\frac{\theta}{2}) = \frac{1 - cos(\theta)}{2} \quad (2)$$

d is the distance between two points (over the bigger circle of the sphere), R is the sphere radio, in our case the Earths radio, γ_A is the latitude of the point A, γ_B is the latitude of the point B and $\Delta\lambda$ is the difference of the longitudes.

Finally, if $sen_{\gamma_{AB}} = sen(\gamma_A) \cdot sen(\gamma_B)$ and $cos_{\gamma_{AB}} = cos(\gamma_A) \cdot cos(\gamma_B)$, the distance ($d$) is:

$$d(A,B) = R * arccos(sen_{\gamma_{AB}} + cos_{\gamma_{AB}} * cos(\Delta\lambda)) \quad (3)$$

All information related to the patients who must be attended by a doctor is done through a mobile application. It indicates to the medical staff through a map his/her current location and the next patient to assist.

The application has enabled a feature called "emergency support". With this function when a doctor or nurse requires additional help from peers he/she can activate this mode. When they activate this feature all health personnel in the affected area receives the notification and simply by clicking on it, they can start a video call or a chat to help his/her colleague. This functionality was designed to support healthcare workers and improve the use of time in transfers between patients. Note that this feature opens a communication channel between two partners through a video streaming. Due to the high amount of information exchanged the connection will take place by Long Term Evolution (LTE)(Sesia et al., 2009), specifically LTE-Direct to ensure adequate and secure communication between nodes that connect.

In the moment in which a doctor has just treat a victim, he/she can take his/her mobile and read the tag, mark the point as completed and check next victim status. When the doctor arrives to the location of the new victim, the node is automatically marked on the map as being in the care process but he/she can read the sticker to be sure of the authenticity of the node. The period devoted to reach a new node is called "travelling time". Doctors can receive notifications called "emergency support" when they are in this "travelling time" to avoid constant notifications that may mislead the staff in the middle of an assistance.

4 DECISION-MAKING SYSTEM

First of all, in the generation of doctors' routes, an undirected graph is created from the points defined during the triage. There are as many points as patients on the map, these are the vertices of our graph. The edges will be defined undirected between the vertices. This distance between points will be the cost of the edge. The system generates one graph for each triage colour, the main objective is treating patients based on their injuries. First of all, the patients with red triage are care, then patients with yellow triage and finally the ones with green triage. Once each graph is generated, the amount of resources and the place where they are needed. In this case resources are doctors (number of doctors #d) that will assist patients. Their position at all time is known. Specifically a graph based on the Delaunay Triangulation (de Berg et al., 2008) is created (as in figure 2) .

Initially, the system divides into clusters the red graph. At the end, there are as many subgraphs as doctors in the emergency area. Specifically our system generates a $k-partition$ based on (Hespanha, 2004), where k is the number of doctors (#d). The system assigns to each doctor, depending on the location, the node that is the highest priority and closest to the coloration performed. That is, the nearest doctor

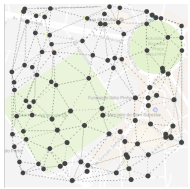


Figure 2: Graph based on Delaunay Triangulation.

is distributed for each partition, excluding the doctors already assigned. This is a quick solution for distributing to doctors in different areas. If a new node is generated, the system automatically add it to the nearest cluster, and a new doctor's route is recalculated.

Definition 1. *k-partition. Consider $G = (V, E)$ as an undirected graph with the set V as vertex and the set E as edges and where the edge cost function is $c : E \to [0, \infty)$. A $k-$partition of V is a collection $P = \{V_1, V_2, ..., V_k\}$ of k disjoint subsets of V, whose union equals V. The cost associated with P is defined by:*

$$C(P) = \sum_{i \neq j} \sum_{(v,\bar{v}) \in E, v \in V_i, \bar{v} \in j} \bar{c}(v, \bar{v})$$

The $l-$bounded Graph Partitioning ($l-GP$) problem is based on finding a $k-$partition P that minimizes $C(P)$, with no more than l vertices in each partition. The problem is based on the MAX$k-$CUT problem (de Sousa et al., 2016) that find a partition for F that maximizes the reward for a edge-reward given as $r : V \times V \to [0, \infty)$, where $r(v, \bar{v}) = r(\bar{v}, v), \forall v, \bar{v} \in V$. We considered a variation of this problem called Hypergraph Max k-CUT (HMkC) problem (Ageev and Sviridenko, 2000) with the sizes of parts given and for a set of k integers $s_1, s_2, ..., s_k$ adds the constraint $|V_i| = s_i, \forall i$.

Note if there are red nodes (number of red nodes $\#r$) the other colours are not considered. When these victims are attended the yellow nodes(y) are taken into account and finally green nodes(g).

When the graph is divided as in figure (figure 3) the system assign one doctor for each zone. Then the system analyses the path of each subgraph. This is the problem known as the Travelling Salesman Problem (TSP) (Hoffman et al., 2013) and we solve this through a Genetic Algorithm (Mudaliar and Modi, 2013).

These methods are adaptive and may be used to solve optimisation and search problems. They are inspired by the behaviour of the species to evolve and belong to the group of genetic algorithms.

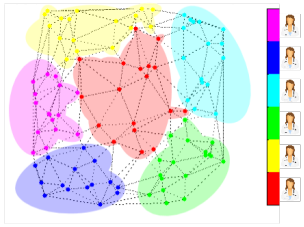
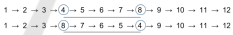


Figure 3: k-Partition graph.

Populations are made up of different individuals. In the problem posed here when talking about individuals we refer to victims / possible routes that can be obtained.

A simulation has been carried out in order to validate the use of this approach to build the routes. For each subgraph a population of 100 individuals is randomly generated. A selection of the best four individuals (the lowest cost route) is made. From them the parts that routes have in common are selected as parents for generating the new population and children are generated by permuting the order of the part that does not match.

Once the new population is generated, random mutations based on three different operations as shown in the figure 4 are made. This iteration is repeated 1000 times before getting the final result.



(a) Flip operation

(b) Swap operation

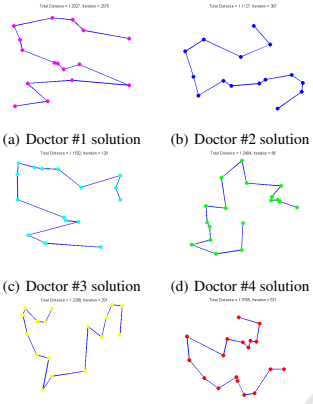
(c) Slide operation

Figure 4: Operations to generate mutations.

Finally, once the genetic algorithm is applied to each subgraph obtained after the partition, the different routes for each doctor are obtained, such as it is illustrated in figure 5.

The number of iterations and the population size was chosen based on the results of time and costs we obtained in different simulations. These values are an approximation that can be adjusted at any time. Thus, a graph of routes is generated for each doctor,

IoTBDS 2017 - 2nd International Conference on Internet of Things, Big Data and Security



(a) Doctor #1 solution (b) Doctor #2 solution

(c) Doctor #3 solution (d) Doctor #4 solution

(e) Doctor #5 solution (f) Doctor #6 solution

Figure 5: Routes of Doctors.

based on the combination of different subgraphs that are produced with patients of the same priority level. At the time of generating the graph of the following categories (colours), the last vertex added to the previous graph is the starting point of the new graph. This generation of separated subgraphs is based on the regulations when applying triage schemes because patients may be attended in order depending of the severity of injuries. If a patient walks, and a medical staff re-triages her/him, the system updates the information and the mobile application updates the NFC tag if it is necessary.

The incorporation of new medical staff or new casualties does not cause any problems or additional cost. If more nodes are added to the graph the doctors' routes are updated paying attention to the new characteristics of the affected area. The routes will be reseted and each doctor can continue his/her work without worrying about such distractions. Given a constraint, doctors who are in the "travelling time" will not receive the route update until he/she has attend next victim, this will the starting point of the route this is never stored in the NFC tag.

5 VICTIMS IDENTIFICATION: NFC TAGS AND HMAC SCHEME

A member of the medical staff is who assign NFC tags to victims in the system proposed. All of these tags contain the result of the triage, that is to say the colour of the triage classification, jointly with the location and the result of a HMAC generated by the server, the physical identifier of the NFC tag (idTag) and some server data explained later in the paper. The stored information will serve as patient identification both in for triage as well as in the medical records generated later on at the hospital. If some data is gathered the system sends it to the server

The use of smartphones helps in the identification of patients through NFC stickers by using phones as NFC readers. Apart of this, devices send the physical tag identifier to the server. In the server, two 64 bytes arrays are generated (Smart, 2016). They are *ipad* and *opad* arrays, and they have default values defined at the initialization stage. The new arrays are generated through a XOR operation combining the previous values and the Master Secret Key (msk). The results are *ipadkey* y *opadkey* arrays (figure 6). After that, the HMAC value is generated with the physical tag identifier and the triage colour result T_{result} (it is a letter for each colour: B, black; R, red; Y, yellow and G, green), so the system applies a hash function to the concatenation of these fields and the *ipadkey*. The output of this hash concatenated with the *opadkey* is the input to another hash function.

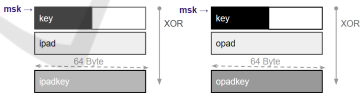


Figure 6: HMAC Keys Generation.

The global function may be described as:

$$H1 = HASH(ipadkey||idTag||T_{result})$$

$$HMAC(Tid, msk) = HASH((opadkey)||H1)$$

The hash function chosen for the implementation is a $SHA3_{512}$. The final output will be the identifier that the will be saved in the NFC sticker tag, as you can see in figure 7.

When a doctor or a member of the medical staff want to access to the triage result of a patient, in the affected zone, he/she has to read the NFC sticker through the mobile application which sends the data of the physical tag identifier and HMAC to the server. The server is who verifies the authenticity of the tag

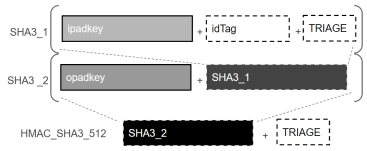


Figure 7: HMAC Hash Operation.

and generates a new node. The doctors can see all the nodes in the mobile phone, specifically the nodes on his/her routes.

6 MEDICAL STAFF SECURITY: IBSC SCHEME

Different communications modes are supported related with medical staff. On the one hand, the communication with the server (to check NFC tags authenticity and synchronizing routes) and, on the other hand the communication between them (video-calls and chats). Authentication against the server and peers and integrity of shared data is included. In both communication modes an ID-Based Signcryption scheme (IBSC) is used in order to achieve secure communications. This complex cryptosystem is a combination of ID-Based Encryption (IBE) and ID-Based Signature (IBS) that provides private and authenticated delivery of information between two parties in an efficient way with a composition of an encryption scheme with a signature scheme (Boyen, 2010). This approach offers the advantage of simplifying management by not having to define a public key infrastructure. This type of scheme was chosen due to its low computational complexity, efficiency in terms of memory and its usability.

A crucial part of the proposal is a Private Key Generator (PKG), a server in charge of generating health staff private keys. The identifier of medical staff is the number of registered medical practitioners and for nurses the same (*ID*). Next, we describe the mathematical basic tools used as well as the notation included in their description.

Definition 2. *Considering two cycling groups $(G,+)$ and $(V,\cdot)$ of the same prime order q. P is a generator of G and there is a bilinear map paring $\hat{e}: G\times G\to V$ satisfying the following conditions:*

- *Bilinear: $\forall P,Q\in G$ and $\forall a,b\in\mathbb{Z}$, $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$*
- *Non-degenerate: $\exists P_1,P_2\in G$ that $\hat{e}(P_1,P_2)\neq 1$. This means if P is generator of G, then $\hat{e}(P,P)$ is a generator of Q.*
- *Computability: there exists an algorithm to compute $\hat{e}(P,Q),\forall P,Q\in G$*

Some hash functions denoted as follows are also needed: $H_1:\{0,1\}^*\to G^*, H_2:\{0,1\}^*\to\mathbb{Z}_q^*, H_3:\mathbb{Z}_q^*\to\{0,1\}^n$, where the size of the message is defined by *n*. The signcryption scheme used is the ID-Based Signcryption Scheme (IDSC) proposed in (Malone-Lee, 2002). Next we describe some basic notation used: $x\xleftarrow{r}S$ stands for an element x randomly selected from a set S, $x\leftarrow y$ denotes the assignation of the value y to x and $||$ is used for concatenation.

The steps needed for the signcryption scheme are the following:

- **SETUP:** The initial parameters are established and the server generates the master public key (*mpk*) and the master secret key (*msk*). For that a prime q based on some private data $k\in\mathbb{Z}$, two groups G and V of order q and a bilinear pairing map $\hat{e}: G\times G\to V$ are selected. $P\in G$ is selected randomly and the hash functions H_1, H_2 and H_3 are also chosen.

$$msk\xleftarrow{r}\mathbb{Z}_q^*$$
$$mpk\leftarrow msk\cdot P$$

- **EXTRACT (*ID*):** In this step, the secret key for each member of the medical staff based on their ID is generated. The public key $Q_{ID}\in G$ and the secret key $S_{ID}\in G$ are calculated taking into account the *msk*. It should be pointed out that this key exchange between server and the doctor is performed using the stream cipher SNOW3G (Santos-González et al., 2014) under the session key obtained through an Elliptic Curve Diffie-Hellman (ECDH)(Bos et al., 2014). the safety of following connections as you can see in figure **??**.

$$Q_{ID}\leftarrow H_1(ID)$$
$$S_{ID}\leftarrow msk\cdot Q_{ID}$$

- **SIGNCRYPTION (S_{ID_a}, ID_b, m):** All the messages $m\in\{0,1\}^n$ will be encrypted and signed. The receiver's public key is generated taking into account ID_b and then the message is signed with S_{ID_a} and encrypted with Q_{ID_b} giving as result σ (a t-uple of three components: c, T, U).

$$Q_{ID_b}\leftarrow H_1(ID_b)$$
$$x\xleftarrow{r}\mathbb{Z}_q^*$$
$$T\leftarrow x\cdot P$$

IoTBDS 2017 - 2nd International Conference on Internet of Things, Big Data and Security

$$r \leftarrow H_2(T||m)$$
$$W \leftarrow x \cdot mpk$$
$$U \leftarrow r \cdot S_{ID_a} + W$$
$$y \leftarrow \hat{e}(W, Q_{ID_b})$$
$$k \leftarrow H_3(y)$$
$$c \leftarrow k \oplus m$$
$$\sigma \leftarrow (c, T, U)$$

- **UNSIGNCRYPTION (ID_a, S_{ID_b}, σ):** If everything is right, the message $m \in \{0,1\}^n$ is returned. Otherwise, if there are some problems in the signature or in the encryption of m, $\perp$ is returned. The sender's public key is generated taking into account ID_a and then the message is unencrypted with S_{ID_b}.

$$Q_{ID_a} \leftarrow H_1(ID_a)$$
$$split \quad \sigma \quad as \quad (c, T, U)$$
$$y \leftarrow \hat{e}(S_{ID_b}, T)$$
$$k \leftarrow y$$
$$m \leftarrow k \oplus c$$
$$r \leftarrow H_2(T||m)$$

Verification:

$$\hat{e}(U, P) == \hat{e}(Q_{ID_a}, mpk)^r \cdot \hat{e}(T, mpk)$$

Note: if the verification is successful m is returned, otherwise $\perp$ is returned.

7 SECURITY ANALYSIS

The proposed scheme provides protection against different attacks. In this sections some of them are presented. On the one hand, a spoofing attack and/or cloning of the card will be hardly successful since it would involve the generation of the HMAC described taking into account the master key of the server and the ID card. Even if an outsider obtains this information, it should be noted that the physical identifier of a NFC tag is unique to each element. On the other hand, if someone emulate a NFC card from an Android device, in this operating system, the emulated device goes from being passive to being active. So the attack would be detected since the application has the restriction that only read NFC tags that are passive. At the time of its implementation in Android are different and completely distinguishable communications.

Attacks related to make multiple requests to the server, called Denial of Service (DoS) attack, are restricted because only requests associated with a number of legitimate members of the medical staff will take effect. Once the corresponding private key is assigned, more requests of this kind will be not attended.

Finally, the typically "Man in the Middle" attack which conveys a successful authentication to the server with an identifier of legitimate members of the medical staff is improbable. This false identification would be easily detectable because the number of members who can make requests to the server is limited to those who are working at the time of the request. This authentication is one of the most important points on every cloud computing system based on mobile phones (Alizadeh et al., 2016).

8 CONCLUSIONS AND FUTURE WORK

In this work, a system has been presented to may to improve logistics and attention of casualties in extreme situations. The priority is to serve the greatest number of injuries using the shortest possible time and cost. The tool consists on a mobile application, NFC tags and a web service. The mobile application helps health staff to know in every moment the position of the victim and where they must go. Specifically the system create a graph based on the Delaunay Triangulation and uses a $k-partition$ to divide it in clusters. Different subgraphs are obtained, as many ones as doctors in the emergency area. When the graph is divided the system assign one doctor for each zone. Then the system analyses the path of each subgraph through a Genetic Algorithm to solve it like a TSP. The system has an "emergency support" tool to contact peers through a video call when doctors require additional support. Data security is a key objective, so for this reason a HMAC scheme is used to protect NFC tags and an ID-Based Signcryption is used for the communications. A first approach has been implemented in Android and Nodejs with NFC tags. More functionalities can be added to the server, such as statistics, a real-time map with events, etc. Thus, this task is part of a work in progress.

ACKNOWLEDGEMENTS

Research supported by TESIS2015010102, TESIS2015010106, RTC-2014-1648-8, TEC2014-

54110-R, MTM-2015-69138-REDT and DIG02-INSITU.

REFERENCES

Ageev, A. A. and Sviridenko, M. I. (2000). An approximation algorithm for hypergraph max k-cut with given sizes of parts. In *Algorithms-ESA 2000*, pages 32–41. Springer.

Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., and Sakurai, K. (2016). Authentication in mobile cloud computing: A survey. *Journal of Network and Computer Applications*, 61:59–80.

Baracoda (2017). Idbluean efficient way to add rfid reader/encoder to bluetooth pda and mobile phones. Available online: http://www.baracoda.com (accessed on 15 February 2017).

Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., and Wustrow, E. (2014). Elliptic curve cryptography in practice. In *International Conference on Financial Cryptography and Data Security*, pages 157–175. Springer.

Boyen, X. (2010). *Identity-based signcryption*. Springer.

de Berg, M., Cheong, O., van Kreveld, M., and Overmars, M. (2008). Delaunay triangulations. *Computational Geometry: Algorithms and Applications*, pages 191–218.

de Sousa, V. J. R., Anjos, M. F., and Le Digabel, S. (2016). Computational study of valid inequalities for the maximum k-cut problem.

Facebook (2017). Facebook safety check. Available online: https://www.facebook.com/about/safetycheck/ (accessed on 15 February 2017).

Foundation, S. (2017). Open source disaster management software. Available online: https://sahanafoundation.org/ (accessed on 15 February 2017).

Gao, T., Massey, T., Selavo, L., Crawford, D., Chen, B.-r., Lorincz, K., Shnayder, V., Hauenstein, L., Dabiri, F., Jeng, J., et al. (2007). The advanced health and disaster aid network: A light-weight wireless medical system for triage. *Biomedical Circuits and Systems, IEEE Transactions on*, 1(3):203–216.

Google (2017). Google person finder web page. Available online: https://google.org/ (accessed on 15 February 2017).

Hespanha, J. P. (2004). An efficient matlab algorithm for graph partitioning. *Santa Barbara, CA, USA: University of California*.

Hoffman, K. L., Padberg, M., and Rinaldi, G. (2013). Traveling salesman problem. In *Encyclopedia of operations research and management science*, pages 1573–1578. Springer.

Inoue, S., Sonoda, A., Oka, K., and Fujisaki, S. (2006). Emergency healthcare support: Rfid-based massive injured people management. In *Proceedings of the fourth International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications, Irvine, CA*.

Knox, R. W. (2015). Marcq saint-hilaire without tears. *The International Hydrographic Review*, 52(2).

Lee, J.-S., Su, Y.-W., and Shen, C.-C. (2007). A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi. In *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE*, pages 46–51. IEEE.

Malone-Lee, J. (2002). Identity-based signcryption. *IACR Cryptology ePrint Archive*, 2002:98.

Mudaliar, D. N. and Modi, N. K. (2013). Unraveling travelling salesman problem by genetic algorithm using mcrossover operator. In *Signal Processing Image Processing & Pattern Recognition (ICSIPR), 2013 International Conference on*, pages 127–130. IEEE.

Neuenschwander, M., Cohen, M. R., Vaida, A. J., Patchett, J. A., Kelly, J., and Trohimovich, B. (2003). Practical guide to bar coding for patient medication safety. *AMERICAN JOURNAL OF HEALTH SYSTEM PHARMACY*, 60(8):768–779.

of Medicine at NIH, N. L. (2017). People locator and reunite web page. Available online: https://lpf.nlm.nih.gov/ (accessed on 15 February 2017).

Rivero-Garcıa, A., Hernández-Goya, C., Santos-González, I., and Caballero-Gil, P. (2014). Fasttriaje: A mobile system for victim classification in emergency situations.

Santos-González, I., Rivero-García, A., Caballero-Gil, P., and Hernández-Goya, C. (2014). Alternative communication system for emergency situations. In *WEBIST (2)*, pages 397–402.

Sesia, S., Toufik, I., and Baker, M. (2009). *LTE: the UMTS long term evolution*. Wiley Online Library.

Smart, N. P. (2016). Hash functions, message authentication codes and key derivation functions. In *Cryptography Made Simple*, pages 271–294. Springer.

Want, R. (2011a). Near field communication. *IEEE Pervasive Computing*, (3):4–7.

Want, R. (2011b). Near field communication. *IEEE Pervasive Computing*, (3):4–7.

Zou, Z., Chen, Q., Uysal, I., and Zheng, L. (2014). Radio frequency identification enabled wireless sensing for intelligent food logistics. *Phil. Trans. R. Soc. A*, 372(2017):20130313.

Apéndice D

Using blockchain in the follow-up of emergency situations related to events

Received: 30 March 2019 | Revised: 17 October 2019 | Accepted: 28 October 2019
DOI: 10.1002/spe.2779

SPECIAL ISSUE PAPER

WILEY

Using blockchain in the follow-up of emergency situations related to events

Alexandra Rivero-García | **Iván Santos-González** | **Candelaria Hernández-Goya** | **Pino Caballero-Gil**

Departament of Computer Science and Systems, University of La Laguna, Tenerife, Spain

Correspondence
Alexandra Rivero-García, Departament of Computer Science and Systems, University of La Laguna, Tenerife, Spain.
Email: ariverog@ull.edu.com

Funding information
Centre for the Development of Industrial Technology (CDTI), Grant/Award Number: C2017/3-9 (UNICRINF); European Regional Development Fund (ERDF), Grant/Award Number: RTI2018-097263-B-I00 (ACTIS); Government of the Canary Islands, Grant/Award Number: TESIS2015010102 and TESIS-2015010106

Summary

This paper describes a decentralized low-cost system designed to reinforce personal security in big events in case of emergency. The proposal consists of using smart contracts supported by blockchain in the management of events. An alternative communication channel that does not require any cloud service is also provided with the aim of improving the coordination of emergency services. Peers may use this emergency support tool to interact with each other through a chat when additional support is required. Since information security is mandatory in this scenario, identity-based signcryption schemes are here used to guarantee communication confidentiality, authenticity, and integrity. Depending on the communication mode (peer-to-peer or broadcast), different signcryption methods are used. A first implementation of the proposal has produced promising results.

KEYWORDS

Android, blockchain, emergencies, identity-based signcryption, smart contract

1 | INTRODUCTION

The number of massive events in the cities is constantly increasing due to flood risk, protest march, a concert, a fire, etc, and all of them has to be controlled by the rescue staff (police, firefighters, medical staff, etc). The fast evolution of the communication technologies has generated multiple new approaches in different scenarios where the use of smartphones to backing the different daily tasks, due to their small size and high performance, is more important every day. One of the most important things of this small tools is that they are equipped with very powerful communication technologies that can help in different scenarios, including the aforementioned.

The emergence of blockchain technology has driven the introduction of decentralized data structures in multiple scenarios. Its main point of interest is the possibility of storing huge amounts of data in network nodes, enabling them to verify and approve any transaction. Integrity protection of the information stored in this data structure is also guaranteed.

This paper presents a decentralized low-cost model based on blockchain and on the establishment of an alternative communication channel to improve the intervention of emergency services without requiring any cloud service. In particular, the use of a permissioned blockchain is a fundamental issue in this proposal because write permission is granted only to qualified members while the information generated for an event may be accessible and verifiable by all personnel involved in it, at any moment. In particular, only authorized staff can read the blocks, execute a smart contract, and verify new blocks. This approach facilitates coordination among emergency services, because thanks to this, if the event is generated by someone that below to a specific organization, the rest of the organizations can verify in every moment the generated event without the necessity of a specific global system. Moreover, everyone can access to the information of the

event and manage the information for the coordination in a private way supposing it an important advantage in relation to the process used nowadays.

The idea behind the proposal is to associate incidents with blocks in a smart contract. Once any member of emergency organizations detects an incident, a new block is generated to be include in the blockchain after been validated by nearby staff. Then, alerts are issued to the rest of the assigned emergency staff. As a result of this, the emergency staff has access to the event information and may act depending on it. The smart contract has to be created by some authorized member of an emergency body. Initially, formatted information regarding the event and the assigned emergency staff is sent to the smart contract. Part of this information is related to the security of the communication among workers, based on the event information. Once the event is in the blockchain, the first step is the assignment of different emergency service resources to specific areas to help to preserve civil security.

We can see an example in Figure 1 where there are three simultaneous events: a cultural event with a large flow of people in green, a protest march in orange, and an area with the high risk of flood in blue. All these events are verified and different types of emergency service workers must be assigned to the different zones.

When an event is generated, the assigned emergency staff may access the block and some preshared information related to the event. Based on this information, workers can participate via mobile phones in a generic event chat associated to the specific event to share information related to coordination.

Currently, communications among emergency services are carried out mostly by radio frequency. Here, the use of two different wireless technologies through smartphones: Bluetooth Low Energy (BLE)[1] and Wi-Fi Direct[2] are proposed. In cases of network congestion, the system will declare "emergency mode," and the communications will proceed directly through these technologies in registered smartphones. Two communication modes are supported: peer-to-peer (P2P) mode, where the system establishes a direct channel through Wi-Fi Direct between two registered participants, and broadcast mode, where the system shares a message through BLE with all the recipients simultaneously.

Since this work deals with critical situations, communication security is essential. That is why an identity-based encryption scheme is here proposed.[3] Specifically, an identity-based signcryption (IBSC) scheme based on the geolocation, and the public identification of emergency service workers is used. All shared messages are signed and encrypted with this scheme. The used signcryption scheme is a combination of an ID-based signcryption scheme[4] and an ID-based signcryption scheme for multiple receivers.[5]

In the proposal, communication is done through two different technologies using smartphones: BLE[1] and Wi-Fi Direct.[2] The features described below will be taken into account to choose the alternative. When possible, the channel created by Wi-Fi Direct, due to its higher rate of speed and its greater range, will be used. BLE has a transmission rate of 25 Mbps and Wi-Fi Direct has a transmission rate of 250 Mbps. The maximum range of BLE Communication is 60 m, while Wi-Fi

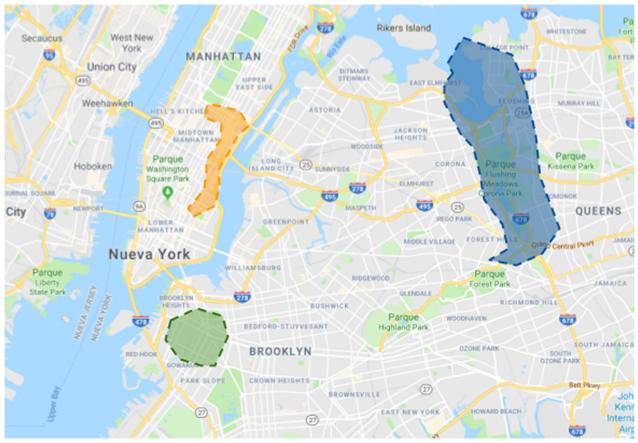


FIGURE 1 Geolocation of events [Colour figure can be viewed at wileyonlinelibrary.com]

Direct has a range of 200 m. In the same range of Wi-Fi, Wi-Fi Aware improves the performance of Wi-Fi Direct. Wi-Fi Aware[6] is only available for the latest version of Android[7] and as a preview mode.

This paper is structured as follows. Section 2 includes a review of publications related to the proposed system. In Section 3, some preliminaries are explained while the proposed system is introduced in Section 4. The event generation using blockchain-based smart contracts is defined in Section 5, jointly with the details of the used communication scheme and its formal description. Section 6 deals with the description of the elements included in the implementation. Finally, Section 7 ends the paper, summarizing the main contributions of the proposal.

2 | RELATED WORKS

This paper describes an application of smart contracts in the secure management of emergencies in large events. Today, most communications deployed in emergency situations are based on RF technology, which can be considered a poor solution because it only allows audio to be shared on a specific frequency, and it is not possible to group and share media data effectively.

On the one hand, some solutions based on the modeling and evaluation of emergency management support system has been created. In the work of d'Oro et al,[8] a use of case based on a complex edge computing is proposed. On the other hand, multiple solutions based on Wi-Fi Direct have been proposed, such as that in the work of Motta and Pasquale,[9] where the potential of Wi-Fi Direct in the implementation of mobile P2P systems is evaluated.

That work includes some examples of the use of Wi-Fi Direct to share text messages, to disseminate information. A middleware for P2P networking is used to distribute hash tables to search for peers. Conti et al[10] proposed generating opportunistic networks over Wi-Fi Direct by studying the latency at the link layer. That is an extension of Camps-Mur et al,[11] where multiple groups are generated and experimental measurements are presented to confirm the suitability of Wi-Fi Direct for P2P systems.

The use of Wi-Fi Direct for alternative communication in emergency situations was proposed by Santos-González et al,[12] but not for communication among emergency services. The main goal of that application is to share the geolocation of victims when they are isolated. A first implementation may be found at the work of Rivero-García et al,[13] where a partial solution for communication in emergencies according to a centralized model was proposed.

The approach here described differs from others in that it takes into account the distribution, assignment, and location of human resources in big events, and information security is addressed as a global requirement. Blockchain is included as an specific tool to address security aspects.

Regarding blockchain background, the first application of the concept was in the finance scenario.[14] A decentralized model to share information, including the concept of transaction is also described there.

Two other more recent contributions to the health and sanitary setting using blockchain are the works of Ekblaw et al[15] and Dubovitskaya et al.[16] The first one describes a prototype to allow patients to have access to all their medical data through the integration of data and medical providers according to different roles. The second paper aims to improve the process of data sharing between researchers and health care providers.

The work of Radanović and Likić[17] provides a complete analysis of the use of blockchain in medicine. Although it points out scalability and data access control as general obstacles, it identifies several promising groups of applications in that scenario. For instance, the management of electronic health records is highlighted as one of these areas of interest.

Some initiatives, such as Hyperledger, have been used to develop different solutions based on blockchain for healthcare and Internet of Things (IoT). A very detailed analysis of the use of IoT and blockchain has been created on the work.[18] There, the authors analyze all the blockchain mechanisms for IoT security. The work of Cha et al[19] presents a solution based on the monitorization of IoT sensors in a connected gateway for BLE. Patients may control which users have access to their data through a mobile application.

In the work of Guo et al,[20] a secure attribute-based signature scheme is proposed to store medical health records in a blockchain and to manage the access to this information based on the attributes of each user. There, multiple authorities are allowed to access to the blockchain, limiting the accessible data set. In a similar way, Yue et al[21] proposed the use of blockchain to preserve privacy of medical data.

Another solution based on the use of smart contracts in health care is given in the work of Griggs et al,[22] where patients are monitored to detect events related to medical conditions. This system allows sending notifications when conditions change and a record of activities is also provided.

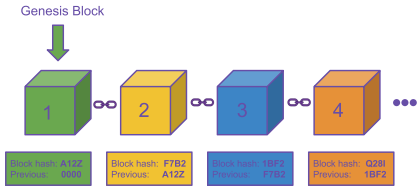


FIGURE 2 Blockchain example [Colour figure can be viewed at wileyonlinelibrary.com]

3 | PRELIMINARIES

3.1 | Blockchain

Roughly speaking, blockchain is a decentralized database that stores a registry of assets and transactions across a computer network. Specifically, it can be seen as a P2P network that is secured through strong cryptography. Each item holds a timestamp and a link to a previous document. In this manner, once this item is sealed, it is theoretically impossible to modify it. Hence, the information inserted in the blockchain is persistent once it is inserted in the system.

A transaction takes place when the timestamp is obtained. This procedure provides the blockchain with a time registration mechanism, enabling the possibility of knowing the timeline of information generation.

Blocks represent confirmed transactions. Each block contains a code linking it to the previous block, some information related to the transaction (involved people, amount of cryptocurrencies, etc), and another code linking it to the next block. Both codes are computed with a hash function used to generate a chain. A basic example is shown in Figure 2, where relations between blocks according to their hash codes are illustrated.

There is a main block that is the first one named genesis block. This block is identified because the hash value of its previous block is '0000.' In a blockchain, a token is a representation of a physical or digital asset built on some native currency. Blockchain tokens include some specific properties like a name, a symbol, the initial number of minted units, the maximum number of units, the severability (because a token can be divisible into smaller units or be indivisible), and a link either to an underlying physical or virtual value or asset, or to give it power to perform some action.

3.2 | Smart contracts

A contract is an agreement between two or more parties, including a set of requirements and execution conditions accepted by the endorsers. Up to now, contracts have been written documents subject to the laws. Smart contracts extend this concept to computer programs that execute agreements established between two or more parties when a preprogrammed condition happens.

Due to its nature, a smart contract is valid without the need of authorities because it is a code. Blockchain technology makes possible to share this code with all network nodes, guaranteeing that it cannot be modified. Hence, the main features of smart contracts are decentralization, persistence, and transparency.

Many of the latest implementation proposals for smart contracts are based on Ethereum. This option operates on a distributed computing platform based on a public blockchain using a cryptocurrency called ether. Solidity is the language used in Ethereum. It is a statically typed object-oriented language similar to Java in its syntax.

3.3 | Identity-based signcryption

Identity-based encryption (IBE) avoids typical problems related to certificates in public key cryptography because public keys are information used to identify users of the system (email address, social security number, personal identifier, etc). Thus, the use of an IBE scheme allows the user to encrypt data with the public identifier associated to the receiver, and to decrypt the message, the recipient will use private information that only he/she knows.

Based on this idea, some variants can be found in the scientific literature. For example, IBSC schemes where a composition of an encryption scheme with a signature scheme is defined. This combination allows the system to guarantee integrity, confidentiality, authenticity and nonrepudiation efficiently and in a single step.

The best known IBSC schemes are based on bilinear pairings on elliptic curves.

3.4 | Bilinear pairing

A bilinear pairing can be defined as follows. Let $(\mathbb{G}, +)$ and $(\mathbb{G}_{\mathbb{T}}, \cdot)$ be two cycling groups of the same prime order q. Let P be a generator of $\mathbb{G}$ and $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{T}}$ be a bilinear map pairing that satisfies the following conditions:

- *Bilinear*, $\forall P, Q \in \mathbb{G}$ and $\forall a, b \in \mathbb{Z}$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
- *Nondegenerate*, $\exists P_1, P_2 \in \mathbb{G}$ such that $\hat{e}(P_1, P_2) \neq 1$. This means that if P is a generator of $\mathbb{G}$, then $\hat{e}(P, P)$ is a generator of $\mathbb{G}_{\mathbb{T}}$.
- *Computability*, there exists an algorithm to compute $\hat{e}(P, Q), \forall P, Q \in \mathbb{G}$.

3.5 | Elliptic curve discrete logarithm problem

Let us consider the cyclic group $\{0, P, 2P, 3P, \dots\}$ for any point P on an elliptic curve where the operation kP is called scalar multiplication, being k an integer. The elliptic curve discrete logarithm problem (ECDLP) consists in finding k, given the points kP and P. Solving the ECDLP for appropriate parameters is computationally infeasible, and is the basis of the proposed scheme.

4 | GLOBAL SYSTEM VIEW

The main idea behind the proposal is to put forward a permissioned blockchain to monitor risk level in big events and to improve the deployment of material and human resources if an emergency occurs. Permissioned blockchains are those in which transaction processing is carried out by a list of known and authorized participants (see Figure 3).

Participant entities may be hospitals, emergency services, police stations, health centers, fire stations, and forest guards and other governmental authorities, such us municipalities, local, state, or national authorities.

The process presented here starts when a member of an emergency body detects an incident and generates a notification by using his/her smartphone to be send to his/her organization. This notification contains the geolocation, the kind of incident, and the estimated level of risk. The proposed signcryption scheme is applied on this notification to guarantee its confidentiality, integrity, and authenticity.

Once the corresponding entity verifies the identity of the person who sent the notification, it generates the smart contract and requests ratification from other members belonging to the organization located near the incident. If any ratification is received, a new block is generated and inserted into the blockchain with the corresponding output of the smart contract. Consequently, all the participating entities may access to the incident information through the blockchain (see Figure 4).

After adding the incident to the blockchain, resource allocation to limit possible risks is carried out. The resource inventory assigned to the incident is made publicly available by including it in the smart contract.

The system uses a permissioned blockchain to distribute keys for secret communication during the event. The personnel may access the blocks, and a chat service where they may participate because they have some preshared information, is

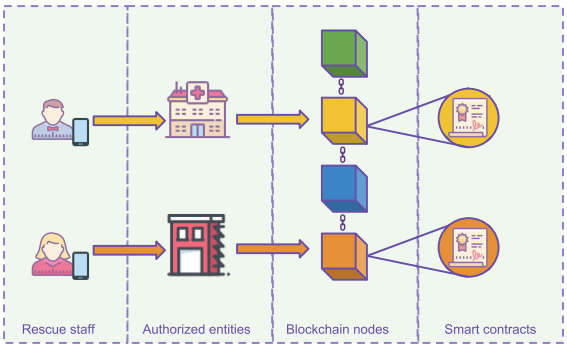


FIGURE 3 Block generation process [Colour figure can be viewed at wileyonlinelibrary.com]

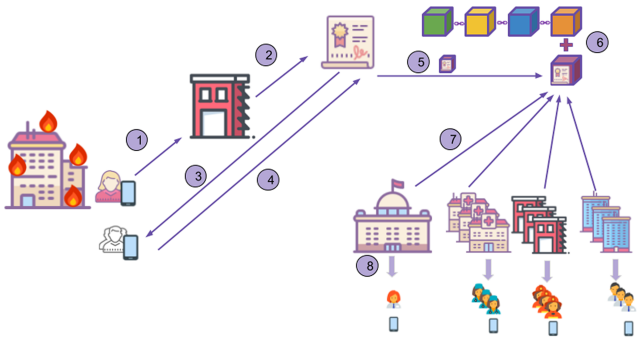


FIGURE 4 Flow of the event generation [Colour figure can be viewed at wileyonlinelibrary.com]

enabled for the event. Thus, the participants do not need any native token because the assets are the specific resources (staff, machinery, etc) owned by the entities. To make it possible, the created network has to have at least the 50% of the users of the blockchain to have consensus and write new blocks. This is possible because this blockchain is used only in the emergency and most of the users are there.

To prevent network congestion, an alternative communication system for emergency service staff and supported by mobile phones is provided. It supports two different communication modes: P2P and broadcast.

When the emergency mode is activated, it is necessary to share some users' public information regarding user's ID. This information is shared here through BLE using beacon mode (see Figure 5). Every participant has a list of identifiers (IDs) corresponding to nearby people. This list must be made publicly available to verify who the legitimate participants are. This is achieved by including such a list in the smart contract.

Data shared through this new communication channel must be protected. An ID-based signcryption scheme is implemented to complete this task in both communication modes. Participating in secure communications is possible only when possessing an identifier included in the smart contract list.

There is a central application (mobile application) to handle the event and distributing information among the participant staff. Its management is collaborative, and all the entities involved in the event may participate in it. The initialization steps are as follows. First, the authorized entity generates the event and assigns different types of resources to the event. Specific information that allows staff participation in the chat system is also provided.

A unique identifier randomly generated is assigned to each event together with its geolocation. To prevent the generation of false multiple events, it is considered that a range of some miles refer to the same event. When a member of the emergency staff is assigned to an event, the system generates specific credentials and keys to share data. Users may get from the mobile application their own location, theirs peers' locations, and the scope area of the event.

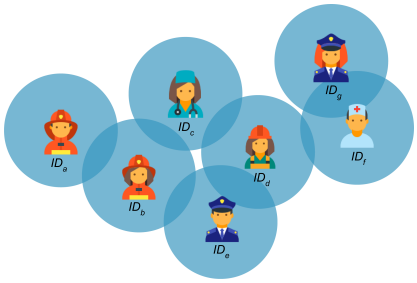


FIGURE 5 Sharing identifiers through beacon mode [Colour figure can be viewed at wileyonlinelibrary.com]

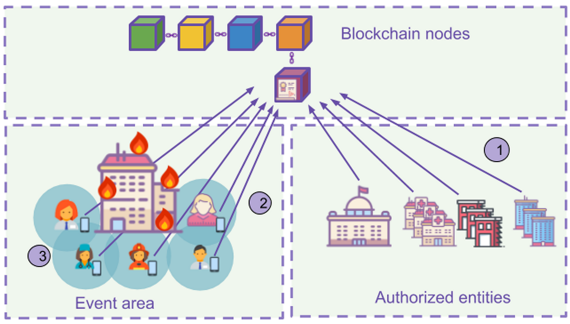


FIGURE 6 Information access [Colour figure can be viewed at wileyonlinelibrary.com]

The system is designed to allow that emergency staff with heterogeneous communication capabilities may interact and have access to shared information. The event information can be updated and sent to the blockchain as many times as needed by generating a new block containing the reference to the event identifier (eventID). Figure 6 describes how the information may be accessed.

Among the relevant fields included in the smart contacts we have the identifier of the person who generates the event (generator), the entity to which this person belongs, and the rules (privacyPolicy) to access the smart contract. Apart from that, the system defines some values like the identifier of the event (eventID) and its geolocation (location).

Events are classified by using a code in the contract denoted as kind (fire, climate phenomenon, seismic phenomenon, volcanic phenomenon, flooding, pollution, etc) to estimate what resources it requires. State represents the status of the event: created (refers to the state in which a person sends the creation of the event before receiving confirmation from the rest of the participants), verified (is used when a real event exists and some staff is working in it), and inactive (is the state used when an event is finished). *State* represents the status of the event:

- *Created* refers to the state in which a person sends the creation of the event, but there is still no confirmation from the rest of the participants.
- *Verified* is used when a real event exists where some staff is working.
- *Inactive* is the state used when an event is finished.

There are two fields that refer to the staff assigned to the event: participants stores the identifiers of the people who participate in the event, and numParticipants stores the number of participants. Note that each user has an identification (IDentity) associated to his/her own address (user) and also an entity to which he/she belongs.

Related to the event generation, the contract also includes when the event was generated (EventGeneration()). If people nearby confirm the event, the contract includes (EventConfirmed()); otherwise, it includes (EventAborted()).

Several functions related to the internal operation of the smart contract and the evolution of the event exist. One of the most important fields for the communication system is getIDs(), which is used to disseminate staff public identification. Besides, getSharedData() allows users to generate the communication with some specific preshared security information. An example of the smart contract used in the proposed system is shown in Algorithm 1.

5 | EMERGENCY COMMUNICATION SCHEME

As it has been mentioned before, an IBSC scheme is used with the aim of guaranteeing communication security. The rationale behind this selection was its low computational complexity and its high efficiency in terms of memory and usability.

This communication system allows sharing text, images, and audio. Emergency service staff is provided with two variants of IBSC to share information. When the information exchange involves P2P mode, an ID-based signcryption is used. Otherwise, in broadcast mode, an ID-based multireceiver signcryption scheme is implemented.

The features described below were taken into account when choosing the communication technology to be used. The channel is supported by Wi-Fi Direct whenever possible, due to its higher speed rate and greater range. A second option

```
pragma solidity 0.4.16;

contract Event {
  address entity;
  address generator;
  address public privacyPolicy;
  string public eventID;
  string public location;
  string kind;
  uint riskLevel;
  enum State { Created, Verified, Inactive }
  State public state;
  Worker[] public participants;
  uint public numParticipants;
  struct Worker{
    address entity;
    address user;
    string IDentity;
    string enventID;
  }
  ...
  modifier onlyEntity(){...}

  event EventGeneration(eventID) {...}
  event EventConfirmed();
  event EventAborted();

  function Event onlyEntity (string _eventID, address _privacyPolicy, string _location, string _kind, uint
      _riskeLevel) {...}
  function UpdateParticipants(string _eventID, address _privacyPolicy, Workers[] _participants, uint
      numParticipants, Worker _participant, address _entity) {...}
  function UpdateState(string _eventID, uint _riskeLevel, State _state) {...}
  function UpdateAccess (string _eventID, address _privacyPolicy) {...}
  function kill onlyEntity (string _eventID) {...}
  function getIDs (string _eventID, address _privacyPolicy, Worker _participant) {...}
  function getSharedData (string _eventID, address _privacyPolicy, Worker _participant) {...}
  ...
}
```

Algorithm 1 Pseudo-code of the smart contract to generate an event

is BLE technology, where the transmission rate is of 25 Mbps (while Wi-Fi Direct has a transmission rate of 250 Mbps). Another important difference between these technologies that justifies the previous preference refers to the maximum range of BLE, which is 60 m, while Wi-Fi Direct has a range of 200 m.

To define this communication system it is required to share some users' public information when emergency mode is activated. This information is user's ID, and it is shared through BLE using beacon mode (see Figure 5). Every person has a list of identifiers (IDs) corresponding to nearby people; this list is published in a smart contract so that the participants can be verified.

The use of BLE allows generating lists containing peers *IDs* that may used when P2P communications is required. When a member of the emergency service receives a new *ID*, he/she checks if it is included in the smart contract list. If the *ID* is not in it, it is not yet included in the contract. Otherwise, it is accepted and stored.

To make this section more understandable, Table 1 has been added to define some notations.

TABLE 1 Notations used

Notation	Meaning
msk	master secret key
mpk	master public key
H_i	cryptographic hash function (digest)
$H_i(x\|\|y)$	digest of the concatenation of bit-strings x and y
$x \xleftarrow{r} X$	x is selected uniformly at random from set X
$x \oplus y$	bitwise XOR of bitstrings x, y of equal length
$\hat{e}(x, y)$	bilinear map paring of x and y
$x \cdot P$	multiplication of the point P times x
$x \xleftarrow{r} S$	stands for an element x randomly selected from a set S
$x \leftarrow y$	assignment of the value y to x
$a\|\|b$	is used for concatenation of a and b

5.1 | Initialization

At the end of this stage, all the staff participating in the event must be registered, regardless of the organization to which they belong.

Some elements and basic notation necessary for a detailed description of the system are described below.

$$H_1 : \{0,1\}^* \to G^*, H_2 : \{0,1\}^* \to \mathbb{Z}_q^*, H_3 : \mathbb{Z}_q^* \to \{0,1\}^n,$$

$$H_4 : \{0,1\}^n \to \{0,1\}^{|m|}, H_5 : G \times G \times \{0,1\}^n \times Z_q^* \times Z_q^* \times \ldots \times Z_q^* \to Z_q^*,$$

where n is the length of the message m and q is a prime number. This initialization phase is carried out in each organization for each person in the system.

- Setup: In this first step, the server initializes the parameters to generate its own keys: master public key (mpk) and master secret key (msk). This server plays the role of private key generator (PKG). To achieve it, some private data are necessary: $k \in \mathbb{Z}$ to generate a prime q based on it, two groups $\mathbb{G}$ and $\mathbb{G}_\mathbb{T}$ of order q and a bilinear pairing map $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_\mathbb{T}$ are selected. Next, $P \in \mathbb{G}$ is randomly chosen and five hash functions are also defined.
  Finally, server keys are generated: $msk \xleftarrow{r} \mathbb{Z}_q^*$ and $mpk \leftarrow msk \cdot P$.
- After Extract:
  In this step, staff identification is carried out. Public key $Q_{ID} \in G$ is generated through a hash function applied on the corresponding ID, $Q_{ID} \leftarrow H_1(ID)$.
  Private key S_{ID}, used for communications with the server $S_{ID} \in G$, is calculated taking into account the msk, $S_{ID} \leftarrow msk \cdot Q_{ID}$. In the proposal, key exchange between server and staff is done using the stream cipher SNOW3G under the session key obtained through an elliptic curve Diffie-Hellman (ECDH) scheme.

5.2 | Event generation

This phase is carried out by the organization of the user that generated the alert. The information is stored in the blockchain. Each one of the generated events has a unique identifier, $ID_e \xleftarrow{r} \mathbb{Z}_q^*$ and some location coordinates, lat and lon. In this stage, the public key for this event $Q_{IDe} \in G$ is generated as

$$Q_{IDe} \leftarrow H_1(ID||ID_e||lat||lon).$$

Then, the secret key for this event corresponds with $S_{IDe} \leftarrow msk \cdot Q_{IDe}$. To share that private information a secure channel is created, specifically in this system, the ECDH was implemented. This protocol is a variation of the original Diffie-Hellman protocol, which uses the properties of the elliptic curves defined over finite fields.

In this way, the operation of this protocol is based on the fact that two users agree beforehand on the use of a prime number p, an elliptic curve E defined over Z_p, and a point $P \in E$. Then, the users A and B, in this case a doctor (A) and the server (B), choose as secret keys two random numbers belonging to Z_p. The doctor select $a \in Z_p$ and the server $b \in Z_p$; these are the secret keys Sk_a and SK_b of them. Later, both of them obtain their public keys multiplying their secret keys by previously agreed point P, obtaining the shared key SK. See Table 2 for the specification of the shared key generation.

To compute the shared key, the next step is the exchange between them their public keys by multiplying their private key by the public key of the other user/server, obtaining both the same shared key.

TABLE 2 Data information related to steps

Steps	Medical staff	Entity server
0: Initialization	p, E, P, Z_p	p, E, P, Z_p
1: Secret key generation	$Sk_a \xleftarrow{r} a \in Z_p$	$Sk_b \xleftarrow{r} b \in Z_p$
2: Public key generation	$Pk_a \leftarrow a \cdot P$	$Pk_b \leftarrow b \cdot P$
3: Information exchange	Pk_b	Pk_a
4: Shared key generation	$K_a = a \cdot Pk_b$	$K_b = b \cdot Pk_a$
5: Confirmation	$SK == K_a$	$SK == K_b$

5.3 | P2P communication scheme in an event

The proposed scheme can be used in direct communications between two users. The main use of case of this mode is the communication between two doctors in a direct way. For example, if a doctor has a question about a specific point of the emergency or something related to a victim, they can establish a communication channel with this P2P mode. In such a case, the steps are the following:

- Single signcryption:
  All the messages $m \in \{0,1\}^n$ are encrypted and signed. Receiver's public key is generated taking into account his/her identification and the pre-shared data (ID_e, lat and lon): $Q_{ID_{e_b}} \leftarrow H_1(ID_b||ID_e||lat||lon)$. Then, some operations are developed giving as result σ (a tuple of three components: c, T, U). T is generated as $x \xleftarrow{r} \mathbb{Z}_q^*$ and $T \leftarrow x \cdot P$. Then, the signature using sender's private key ($S_{ID_{e_a}}$) is denoted as U. It is obtained as follows: $r \leftarrow H_2(T||m)$, $W \leftarrow x \cdot mpk$, and $U \leftarrow r \cdot S_{ID_{e_a}} + W$. Finally, the encrypted message is denoted as c, and it is generated as $y \leftarrow \hat{e}(W, Q_{ID_{e_b}})$, $k \leftarrow H_3(y)$, $c \leftarrow k \oplus m$.
- Single unsigncryption:
  First of all, sender's public key is generated taking into account IDe_a and the preshared information as

$$Q_{ID_a} \leftarrow H_1(IDe_a||ID_e||lat||lon_e).$$

  Then, σ is parsed as (c, T, U). If everything is right, the message $m \in \{0,1\}^n$ is returned. Otherwise, if any problem in the signature or in the encryption of m is detected, $\perp$ is returned. The verification consists of

$$\hat{e}(U, P) == \hat{e}(Q_{ID_{e_a}}, mpk)^r \cdot \hat{e}(T, mpk)$$

  Thus, the user calculates

$$y \leftarrow \hat{e}(S_{ID_{e_b}}, T), k \leftarrow y, m \leftarrow k \oplus c, r \leftarrow H_2(T||m)$$

5.4 | Broadcast communication scheme in an event

The proposed scheme can be used when someone wants to share a message. In this case, the main use of case of this mode is the communication with everybody around a point. For example, if a doctor want to share some planning order or some alert from their location, he/she can generate a broadcast message by the use of this mode. In such cases, the steps are the following:

- Broadcast signcryption: In the broadcast mode, there are n receivers, so the sender is identified by IDe_a and the receivers by

$$IDe_1, IDe_2, \ldots, IDe_n.$$

  All the broadcast messages $m \in \{0,1\}^n$ are encrypted and signed. Sender's public key is generated as $Q_{ID_{e_a}} \leftarrow H_1(ID_a||ID_e||lat||lon)$. Then, some operations are developed, giving as result σ (a t-uple of components: $c, T, U, V, W, X, a_0, \ldots a_n - 1$). Then, the sender selects some random numbers $r \xleftarrow{r} \mathbb{Z}_q^*$, $r' \xleftarrow{r} \mathbb{Z}_q^*$, $s \xleftarrow{r} \mathbb{Z}_q^*$, and $p \xleftarrow{r} \mathbb{Z}_q^*$ and then, it operates:

$$T \leftarrow r \cdot Q_{ID_{e_a}}, U \leftarrow r \cdot P, X \leftarrow r' \cdot T, J \leftarrow r' \cdot mpk.$$

  Receivers' public keys are generated taking into account all the identifications $ID_1, ID_2, \ldots, ID_n$, as follows:

$$f(x) = \prod_{i=0}^{n}(x - v_i) + p(mod\, q) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n.$$

  With $Qe_i \leftarrow H_1(ID_i||ID_e||lat||lon)$, $y_i \leftarrow \hat{e}(Q_i, J)$, and $v_i \leftarrow H_2(y_i)$. Then, it calculates $V \leftarrow s \cdot H(p)$, the key k as $k \leftarrow H(s)$ and the encrypted message c as $c \leftarrow k \oplus m$. Finally, an authenticator h is generated as $h \leftarrow H_5(c, X, U, V, a_0, a_1, \ldots, a_{n-1})$ and $W \leftarrow (r' + h)r \cdot S_{ID_a}$.
- Multiple receiver unsigncryption:
  In this step, two verifications are carried out, but first of all, σ is parsed as $c, T, U, V, W, X, a_0, \ldots a_n - 1$ and $h \leftarrow H_5(c, X, U, V, a_0, a_1, \ldots, a_{n-1})$. The first verification is the public verification to check that the ciphertext is valid:

$$\hat{e}(W, P) == \hat{e}(X + hT, mpk)$$

FIGURE 7 Web application [Colour figure can be viewed at wileyonlinelibrary.com]

Otherwise, the ciphertext has been damaged or is invalid, and $\perp$ is returned. The second verification is

$$\hat{e}(W, Qe_i) == \hat{e}(X + hT, S_{IDe_i})$$

This is to check if ID_i is one of the receivers chosen by the sender and if the ciphertext is valid. Otherwise, the receiver quits the decryption process and $\perp$ is returned. To generate the message, some operations are generated: $y_i \leftarrow \hat{e}(S_{IDe_b}, U)$, $v_i \leftarrow H_2(y_i)$, $p \leftarrow f(v_i)$, $s \leftarrow V \oplus H_3(p)$, $k \leftarrow H_4(s)$, and $m \leftarrow k \oplus c$.

6 | IMPLEMENTATION AND ANALYSIS

A first implementation of the proposal has been developed to obtain a prototype as a proof-of-concept. The smart contract has been implemented using Solidity (Ethereum coding language) on a permissioned blockchain where only authorized entities are assigned writing permission.

This approach allows emulating a permissioned blockchain without the need to spend real money. In this prototype, the user interface is managed by a decentralized web application (DApp), which allows user interaction with the smart contract on the blockchain (see Figure 7).

Moreover, an exhaustive analysis about the performance of the BLE communications has been done. In this case, using the Opportunistic Network Environment simulator (ONE)[23] a total of 300 people have been randomly deployed over an area of $2km^2$. This tool allows selecting different communication technologies, interfaces, node behavior, node speed, node deployment, simulation time, etc. Using the different parameters available on the tool, the behavior of BLE technology in this scenario has been simulated.

In Figure 8, the range and communication links of the BLE technology in the simulated area can be observed. Moreover, to obtain enough and precise data about the BLE technology in this kind of situations, the simulation has been repeated 10 times. An important measurement that have to be taken into account in this kind of scenarios is the average of communications reached. This measure allows us to know how many nodes have received communications by part of the rest of the nodes of the system, fact that is important because if this measurement is extrapolated we can know the the isolated nodes of the network.

The other measurement taken is the average of communications received by a node. This is an important measurement because it allows to know how many communications receive in average every node of the system during the simulation time.

The obtained results can be observed in Table 3, where the an amount of 2646.2 communications of the system have been reached in average. Moreover, during the simulated time 17.4 nodes were isolated supposing it only the 5.6% of the communications. Finally, an amount of 8.82 communications have been received by each node of the system in average during the simulated scenario, supposing it that every node of the system will communicate or will be communicated every 7 minutes approximately.

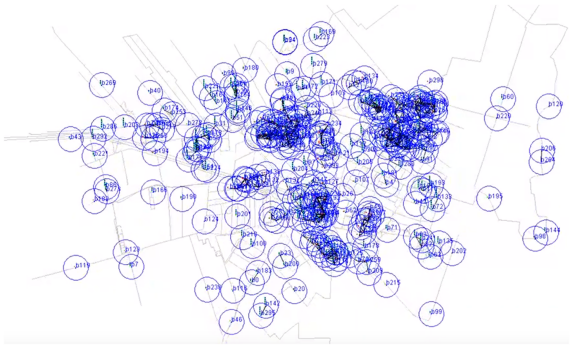


FIGURE 8 BLE simulated scenario [Colour figure can be viewed at wileyonlinelibrary.com]

TABLE 3 Bluetooth Low Energy communication results in the simulated scenario

Communications reached	2646.2
Isolated nodes	17.4
Communications received by node	8.82

Security is one of the priorities to protect the system against attacks such as denial of service (DoS), man in the middle (MitM), and impersonation. DoS attacks are limited because only requests associated with a legitimate number of members of the emergency services take effect. On the other hand, the typical MitM attack, which conveys a successful authentication to the server with a legitimate identifier is very improbable, since once the legitimate user private key is assigned to the server, further requests of this kind will not be taken care of. Impersonation will be easily detectable because the number of members who can make requests to the server is limited to those who are working at the time of the request.

An analysis of efficiency related to the technologies coverage, their range, and their transmission efficiency was developed. A beta prototype has been also implemented with Wi-Fi Aware but in the preview mode of the technology.

The elements of the blockchain are replicable on different computers, since what underlies is a distributed database. This justifies that it is impossible to falsify its elements, since all the data are generally found in several servers, and its synchronization occurs almost simultaneously. In addition, if a falsification is achieved with one of the registers, it should be easy to detect it through the codes that link the blocks and prevent it from spreading.

Before including a transaction into a block, it is always verified. This verification is carried out by miners, which are computers dedicated not only to keep a copy of the data but also to validate nodes' agreement.

Thus, since the validators of this kind of blockchain are known, there is no risk of successful 51% attack.

Smart contracts are executed and enforced automatically and autonomously without the intervention of third parties. What is more, a smart contract can be created and executed by individuals and/or legal entities but by machines or other programs that work autonomously.

Due to its nature, a smart contract is valid without the need of authorities because it is a code. Blockchain technology makes possible to share this code with all network nodes, guaranteeing that it cannot be modified. Hence, the main features of smart contracts are decentralization, persistence and transparency.

The so-called oracles are elements that allow the smart contract to interact with the real world. They are autonomous tools that allow updating the internal states of a smart contract through external information, usually obtained with APIs. In the proposal here described, oracles are smart devices used by the emergency services.

The oracles also work autonomously. However, it must be taken into account that the source used by the oracle is a third party that must be trusted, and that could be corrupted by its owner, crack, or could simply fail your server, something that has negative implications.

An Android mobile application was developed to improve communication between emergency services in extreme situations (see Figure 9). This implementation has been tested tested through the generation of some random events located on a map and assigning ad hoc users to generated events. Smart contracts were developed with Solidity,[24] and

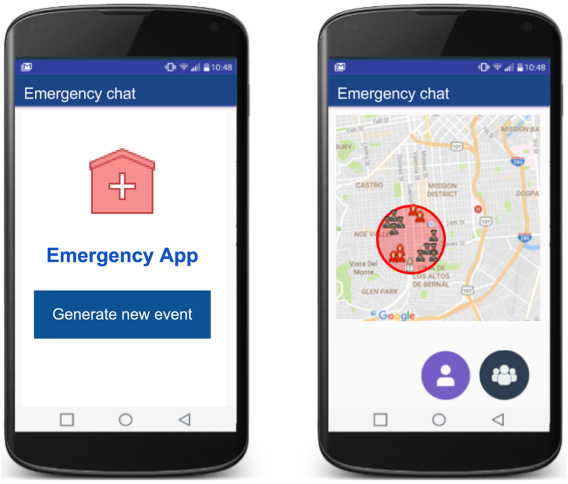


FIGURE 9 Developed prototype [Colour figure can be viewed at wileyonlinelibrary.com]

deployed using Truffle Suite[25] On the server side, we use nodejs[26] with WEB3JS[27] to connect with the smart contracts trough Ganache[28] and Drizzle[29] on the front-end.

The prototype requires communication with the PKG only at the initialization stage where the key generation is performed. Afterwards, users can share messages with their own keys and with the preshared information related to the event. An alternative scheme with direct communications without requiring central server is deployed. Note that this approach can be used when communications are saturated.

7 | CONCLUSIONS AND FUTURE WORK

In this paper, a decentralized low-cost model has been proposed, which supports the monitoring of risk levels in big events, aiming at improving resource allocation and staff coordination in case of emergency.

The proposed system is based on blockchain and on the establishment of an alternative communication channel for sharing information while the emergency situation. An important feature of this system is the no need for cloud services.

The system generates automatically the preshared data related to the event to which the staff is assigned.

The proposal includes a web application used to manage all emergency services and incidents that are generated and publicly notified through its inclusion in a smart contract and in the blockchain. Hence, once the information regarding an event is included in this structure, anybody may consult it and its validation remains guaranteed.

A mobile application with an ubiquitous Wi-Fi Direct chat has been implemented where communication security is based on the use of identity-based cryptography. BLE in beacon mode is used to support identity exchange among participants. Emergency services are able to know, through the mobile application, where the event is located and where they must be deployed, as well as their peers location.

The main objective for which an alternative communication channel is proposed is that emergency personnel can share information, either in P2P or broadcast mode, when an incident at a big event saturates the network. ID-based signcryption has been included to guarantee integrity, confidentiality, authenticity, and nonrepudiation in communications. A beta prototype has been implemented with Wi-Fi Aware, which is available only on Android 8 and in the preview mode of this technology. The possible incorporation of LTE-Direct depends on the Native Development Kit because at this moment this code is private. As part of work in progress, a real test with emergency staff is planned so that the smart contract can change to improve the model according to the results. As future work, more functionalities will be added to the server, such as statistics, private chats based on roles, etc. In the short term, the system modeling and the smart

contract definition are expected to be improved based on the results of real field tests to be developed involving emergency personnel. The possibility of adding new functionalities to the system, such as obtaining and analyzing relevant statistics for emergency management and the definition of private chats based on roles are issues under study.

ACKNOWLEDGEMENTS

This research was funded by the Centre for the Development of Industrial Technology (CDTI) under project C2017/3-9 (UNICRINF), by the Spanish Ministry of Science, Innovation and Universities (MCIU), the State Research Agency (AEI) and the European Regional Development Fund (ERDF) under project RTI2018-097263-B-I00 (ACTIS), and by the Government of the Canary Islands through TESIS2015010102 and TESIS-2015010106 grants.

CONFLICT OF INTEREST

The authors declare no potential conflict of interests.

ORCID

Alexandra Rivero-García https://orcid.org/0000-0003-1946-3403

REFERENCES

1. Panwar G, Misra S. *Inside Bluetooth Low Energy*. Norwood, MA: Artech House; 2017.
2. Shen W, Yin B, Cao X, Cai LX, Cheng Y. Secure device-to-device communications over WIFI direct. *IEEE Network*. 2016;30:4-9.
3. Boneh D, Franklin MK. Identity-based encryption from the Weil pairing. In: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology; 2003; London, UK.
4. Malone-Lee J. Identity-based signcryption. http://eprint.iacr.org/2002/098. 2002.
5. Selvi SSD, Vivek SS, Srinivasan R, Rangan CP. An efficient identity-based signcryption scheme for multiple receivers. Paper presented at: International Workshop on Security; 2009; Toyama, Japan.
6. Das D, Huang P-K, Elad O, Qi EH, Park M. Radio resource allocation in wi-fi aware neighborhood area network data links. 2019.
7. documentation dA. Wi-Fi aware on Android. https://developer.android.com/guide/topics/connectivity/wifi-aware. 2019.
8. d'Oro EC, Colombo S, Gribaudo M, Iacono M, Manca D, Piazzolla P. Modeling and evaluating a complex edge computing based systems: an emergency management support system case study. *IoT*. 2019;6. https://doi.org/10.1016/j.iot.2019.100054
9. Motta R, Pasquale J. Wireless P2P: problem or opportunity. In: Proceedings of the Second IARIA Conference on Advances in P2P Systems; 2010; Florence, Italy.
10. Conti M, Delmastro F, Minutiello G, Paris R. Experimenting opportunistic networks with wifi direct. In: Proceedings of the IFIP Wireless Days; 2013; Valencia, Spain.
11. Camps-Mur D, Garcia-Saavedra A, Serrano P. Device-to-device communications with Wi-Fi Direct: overview and experimentation. *IEEE Wirel Commun*. 2013;20;96-104.
12. Santos-González I, Rivero-García A, Caballero-Gil P, Hernández-Goya C. Alternative communication system for emergency situations. In: Proceedings of the 10th International Conference on Web Information Systems and Technologies; 2014; Barcelona, Spain.
13. Rivero-García A, Santos-González I, Goya CH, Caballero-Gil P. Secure communication system for emergency services in network congestion scenarios. 2018.
14. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. 2009.
15. Ekblaw A, Azaria A, Halamka JD, Lippman A. A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data. In: Proceedings of IEEE Open & Big Data Conference; 2016; Washington, DC.
16. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and trustable electronic medical records sharing using blockchain. Paper presented at: American Medical Informatics Association Annual Symposium; 2017; Washington, DC.
17. Radanović I, Likić R. Opportunities for use of blockchain technology in medicine. 2018.
18. Minoli D, Occhiogrosso B. Blockchain mechanisms for IoT security. *IoT*. 2018;1-2:1-13. https://doi.org/10.1016/j.iot.2018.05.002
19. Cha S, Chen J, Su C, Yeh K. A blockchain connected gateway for BLE-based devices in the internet of things. *IEEE Access*. 2018;6:24639-24649.
20. Guo R, Shi H, Zhao Q, Zheng D. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access*. 2018;6:11676-11686.
21. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J Med Syst*. 2016;40:218.
22. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J Med Syst*. 2018;42:130.
23. Keränen A, Ott J, Kärkkäinen T. The ONE simulator for DTN protocol evaluation. In: Proceedings of the 2nd International Conference on Simulation Tools and Techniques; 2009; Rome, Italy.

24. Ethereum. Solidity. 2019. https://solidity-es.readthedocs.io/es/latest/#. Accessed: September 24, 2019.
25. Suite TruffleBlockchainGroup2019Truffle. Truffle suite. 2019. https://www.trufflesuite.com/. Accessed: September 24, 2019.
26. Foundation Node. js. Node.js. 2019. https://nodejs.org. Accessed: September 24, 2019.
27. Ethereum. Web3.js. 2019. https://web3js.readthedocs.io/en/1.0/. Accessed: September 24, 2019.
28. Ganache TruffleBlockchainGroup2019. Ganache. 2019. https://github.com/trufflesuite/ganache. Accessed: September 24, 2019.
29. Drizzle TruffleBlockchainGroup2019. Drizzle. 2019. https://github.com/trufflesuite/drizzle. Accessed: September 24, 2019.

How to cite this article: Rivero-García A, Santos-González I, Hernández-Goya C, Caballero-Gil P. Using blockchain in the follow-up of emergency situations related to events. *Softw: Pract Exper*. 2019;1–15. https://doi.org/10.1002/spe.2779

Apéndice E

Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks

Information Systems 88 (2020) 101423

Contents lists available at ScienceDirect

Information Systems

journal homepage: www.elsevier.com/locate/is

Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks

Iván Santos-González [a,*], Alexandra Rivero-García [a], Mike Burmester [b], Jorge Munilla [c], Pino Caballero-Gil [a]

[a] Department of Computer Engineering and Systems, University of La Laguna, 38206 Tenerife, Spain
[b] Department of Computer Science, Florida State University, Tallahassee, FL 32306, USA
[c] Department of Communication Engineering, Universidad de Málaga, 29071 Málaga, Spain

HIGHLIGHTS

- We analyze three recently proposed heterogeneous 3-PAKE protocols.
- We discuss 3-PAKE models suitable for heterogeneous wireless sensor networks (HWSN).
- We propose novel 3-PAKE protocols for HWSN applications that are provably secure.
- These protocols offer additional security features.
- These protocols are lightweight, efficient and flexible.
- We discuss practical issues.

ARTICLE INFO

Article history:
Received 5 November 2018
Received in revised form 5 July 2019
Accepted 30 July 2019
Available online 7 September 2019
Recommended by Mathias Fischer

Keywords:
Password authenticated key exchange
Heterogeneous wireless sensor networks
Provable security

ABSTRACT

Several three-party password authenticated key exchange (3-PAKE) protocols have recently been proposed for heterogeneous wireless sensor networks (HWSN). These are efficient and designed to address security concerns in ad-hoc sensor network applications for a global Internet of Things framework, where a user may request access to sensitive information collected by resource-constrained sensors in clusters managed by gateway nodes. In this paper we first analyze three recently proposed 3-PAKE protocols and discuss their vulnerabilities. Then, based on Radio Frequency Identification technologies we propose a novel 3-PAKE protocol for HWSN applications, with two extensions for additional security features, that is provably secure, efficient and flexible.

1. Introduction

Heterogeneous wireless sensor networks (HWSN) are a key component of the Internet of Things (IoT) that enables the interconnection of constrained sensor devices in the physical world with virtual objects for intelligent information and resource management. These networks exploit novel technologies and visions to support automation for smart environment applications, and have an ad-hoc or loosely defined structure with heterogeneous components, such as constrained sensor nodes, gateway nodes, mobile devices and Internet components (servers, etc.). Constrained devices are typically embedded systems with restricted computation, communication, memory and power resources. In an IoT environment, they are used as sensor nodes to monitor physical events.

A major concern with IoT based applications, and in particular HWSN applications, is their vulnerability to malicious exploitation. While strong cryptographic protection can be afforded to Internet components and less constrained IoT devices (for handshakes and stateful connections to control transmissions), the cost of protecting constrained IoT devices can severely impair their performance. For these, protection may have to be restricted to the use of hash functions and symmetric-key operations.

Several authentication and authenticated key exchange (AKE) protocols for HWSN applications, as well as password AKE (PAKE) protocols, have recently been proposed, *e.g.*, [1–7]. These address security concerns, are efficient, and have been designed for a global IoT framework where a user node can access sensitive information collected by resource-constrained sensor nodes in clusters managed by gateway nodes. AKE protocols are widely deployed in real world network applications for authentication and access control. PAKE protocols make it possible for users to

* Corresponding author.
E-mail addresses: jsantosg@ull.edu.es (I. Santos-González), ariverog@ull.edu.es (A. Rivero-García), burmester@ca.fsu.edu (M. Burmester), munilla@ic.uma.es (J. Munilla), pcaballe@ull.edu.es (P. Caballero-Gil).

https://doi.org/10.1016/j.is.2019.101423
0306-4379/

exchange a key based on the knowledge of a shared low-entropy password.

Related work. In 2018 three lightweight three-party PAKE (3-PAKE) protocols for HWSN applications were proposed: (*i*) A two-factor (password, smartcard) authentication protocol for IoT enabled devices in distributed cloud computing environments, by Amin et al. [4]; this addresses weaknesses of several earlier 3-PAKE protocols and is proven secure using a BAN logic [8] tool (AVISPA). (*ii*) A three-factor (password, smartcard, biometrics) anonymous authentication protocol in which the identitifier of the user is encrypted using public key encryption, by Xiong Li et al. [5]; this is also proven secure using a BAN logic tool. (*iii*) A two-factor (password, mobile device) authentication protocol designed for Wireless Medical Sensor Network applications, in which sensors are placed in, or on the patient's body, by Wu et al. [6]; this is proven secure using the ProVerif tool.[1] It should be noted that security tools such as AVISPA and ProVerif are *not* intended for proving security, but for vulnerability analysis. Such tools only provide heuristic security. In fact Wenting Li et al. [7] have shown that all three protocols have several vulnerabilities.

A number of practical AKE and PAKE protocols for multi-party settings have been proposed that are provably secure in a strong adversarial model. These include 3-AKE as well as 3-PAKE protocols with symmetric and asymmetric versions [9–11], and can be adapted for HWSN applications where the service providers (sensor nodes) are resource-constrained (limited processing power, communication bandwidth/range, etc.), or have hardware limitations (no clocks or unsynchronized clocks, etc.), while gateway nodes enable secure communication with the user's device (*e.g.*, a cellphone). In 2016, Chang–Le [12] proposed a two-factor 3-PAKE protocol, designed to address vulnerabilities of an earlier protocol proposed by Turkanovic et al. [3]. This protocol is proven secure using the Real-Or-Random (ROR) formalization model [11]. Das et al. [13] analyzed this protocol, found some vulnerabilities and proposed an improved protocol. He et al. [14] also analyzed the Chang–Le protocol and proposed an improved protocol. We analyze these three protocols and show that they are still vulnerable to security threats.

Our contribution. In this paper we discuss the vulnerabilities of three recent heterogeneous 3-PAKE protocols [12–14] and show that they cannot be considered to be secure. We then propose a novel 3-PAKE protocol for HWSN applications with two extensions that addresses these vulnerabilities as well as the restricted computation power and broadcast range constraints of sensor devices, and is provably secure, efficient and flexible.

Outline. We start in Section 2 by defining the communication model for HWSN, focusing on security issues for multi-party heterogeneous settings, and briefly describe the semantic security Real-Or-Random (ROR) formalization for 3-PAKE applications. In Sections 3–5 we analyze the 3-PAKE protocols proposed by Chang–Le [12], Das et al. [13] and He et al. [14] for HWSN. We then present in Section 6 a novel 3-PAKE protocol for HWSN settings that is provably secure in the RoR model, and two extensions that capture additional security features such as offline dictionary attack protection, session key privacy with respect to the gateway, forward secrecy and user anonymity, and discuss practical issues. In Section 7 we conclude with a review of the main results.

2. Preliminaries

In this section we describe the communication model for HWSN applications and the semantic security formalization that we shall be using.

[1] http://proverif.inria.fr.

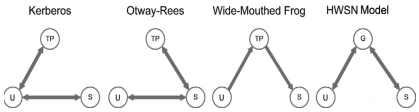


Fig. 1. Protocol flows of four common models for 3-AKE.

2.1. HWSN communication model

A typical wireless sensor network (WSN) deployment involves three types of nodes: user nodes (U), gateway nodes (G), and sensor nodes (S). Sensor nodes detect ambient environmental events/changes, process collected data and send data to gateway nodes that make the data available to user nodes. Sensor nodes may send signals collectively or in an ad hoc manner. In heterogeneous WSN (HWSN), sensor nodes may have restricted power/bandwidth/ memory resources and short-range connectivity, while there are no such constraints for gateway and user nodes.

2.2. 3-AKE protocols

Several 3-AKE protocols have been proposed in the literature. These enable parties that share private keys with a trusted third party to exchange a session key. Fig. 1 shows the flows of four common 3-AKE models that involve a user U, a sensor S, and a trusted third party TP or gateway G, that depend on how TP or G interacts with the other parties. The first three models, Kerberos [15], Otway–Rees [16], and Wide-Mouthed Frog [8] are well established. With the HWSN model, gateway G controls the flows to clusters of sensors S, and interacts with users U and sensors S. G may also relay flows of S to address constraints on sensor resources. This model is appropriate for IoT applications.

2.3. Semantic security in the ROR model for 3-PAKE protocols

We briefly describe the semantic security Real-Or-Random (ROR) formalization [11] for 3-PAKE, that builds on the Bellare–Pointcheval–Rogaway model [10]. This uses a setting with concurrent sessions controlled by the adversary $\mathcal{A}$ and is based on simulation and indistinguishability.

Let $\mathcal{P} = (U, G, S)$ be a 3-PAKE protocol with dictionary D. All parties, including the adversary $\mathcal{A}$, are modeled by probabilistic polynomial-time algorithms. $\mathcal{A}$ controls the communication channels and may eavesdrop, block, modify and/or inject messages in any communication between parties. During the execution of $\mathcal{P}$, an instance of party $X \in \{U, G, S\}$ is modeled by an oracle Π_X^i. Let $X, Y \in \{U, G, S\}$, $X \neq Y$. The capabilities of adversary $\mathcal{A}$ are modeled by queries to oracles:

- Execute $(\Pi_U^i, \Pi_G^t, \Pi_S^j)$: models passive attacks and returns the messages exchanged by instances $\Pi_U^i, \Pi_G^t, \Pi_S^j$ during the execution of the protocol.
- Send $(\Pi_X^i; m)$: models active attacks and returns the message instance that Π_X^i generates upon receiving m. Send (Π_U^i) returns the first message instance of the session that Π_U^i generates.
- Corrupt (Π_X^i) returns the non-ephemeral information stored on instance Π_X^i (the long-term keys).
- Reveal (Π_X^i) returns the internal ephemeral state of a yet incomplete session (*e.g.,* the random exponents of a Diffie–Hellman key exchange, but excludes subroutines that use long-term keys) [17]; or, the current ephemeral state of an instance of a completed session (*e.g.,* the session keys).

Instance Π_X^i *accepts* if it goes into accept mode after receiving the last expected message. Protocol executions are defined by session identifiers *sid*, and instances Π_X^i by partner identifiers *pid*. Π_X^i, Π_Y^j are *partnered* if both accept, have the same *sid* and *pid*, and if no other instance with the same *pid* accepts.

2.3.1. Semantic security

This is defined by an experiment involving oracle Test where at the beginning a bit b is chosen uniformly at random:

- Test(Π_U^i) (Test(Π_S^j)): returns $\perp$ if instance Π_U^i (Π_S^j) and its partner Π_S^j (Π_U^i) have not accepted. If either instance is corrupted, it returns the real session key. Otherwise, it returns the real session key if $b = 1$, and a random key (of equal length) if $b = 0$. If $b = 0$ the partner instance returns the same key.

Adversary $\mathcal{A}$ has access to oracles Execute and Send, and has to guess bit b. Let b' be the output of $\mathcal{A}$. The advantage of $\mathcal{A}$ is: $\mathsf{Adv}_{\mathcal{P}}^{ror\text{-}ake}(\mathcal{A}) = 2 \cdot \Pr[b' = b] - 1$. For *semantic* security this must be a negligible fraction of the security parameter. We take the security parameter to be the length of the keys.

2.3.2. Session key privacy with respect to the gateway G

The security model for 3-PAKE protocols assumes an honest-but-curious G, trusted to enable the exchange of session keys, but should not have access to these. Session key privacy with respect to G is defined by an experiment [11] involving oracle TestPair where a bit b is chosen at random uniformly.

- TestPair(Π_U^i, Π_S^j): returns $\perp$ if instances Π_U^i, Π_S^j do not share the same key. Otherwise, it returns the real session key if $b = 1$ and a random key if $b = 0$.

$\mathcal{A}$ is given the password and keys of U and S, has access to oracles Execute, Send(Π_U^i) and Send(Π_S^j), and must guess bit b. If $\mathcal{A}$ outputs b' then the advantage of $\mathcal{A}$ is: $\mathsf{Adv}_{\mathcal{P}}^{kp}(\mathcal{A}) = 2 \cdot \Pr[b' = b] - 1$. For session key privacy with respect to gateway G this must be negligible.

2.3.3. Forward secrecy for sensor S

This refers to the privacy of the session key of S when the private key of S is compromised. Adversary $\mathcal{A}$ has access to oracles Execute, Send, Corrupt(Π_S^j), and experiment Test(Π_U^i), and must guess bit b. If $\mathcal{A}$ outputs b' then the advantage of $\mathcal{A}$: $\mathsf{Adv}_{\mathcal{P}}^{fs}(\mathcal{A}) = 2 \cdot \Pr[b' = b] - 1$ must be negligible.

2.3.4. Session-state reveal protection

This refers to the protection against leakage of the current state of instance Π_U^i (Π_S^j) during a protocol session (such as the numbers generated for encryption/authentication). The capability of $\mathcal{A}$ is modeled by queries to oracle Reveal(Π_U^i) (Reveal(Π_S^j)). $\mathcal{A}$ has access to oracles Execute, Corrupt and Test(Π_U^i) (Test(Π_S^j)) and must guess bit b. For protection against session-state reveal attacks, the advantage of $\mathcal{A}$: $\mathsf{Adv}_{\mathcal{P}}^{ssr}(\mathcal{A}) = 2 \cdot \Pr[b' = b] - 1$ must be negligible.

2.3.5. Dictionary attacks

These can be *online* or *offline*. Adversary $\mathcal{A}$ has a password dictionary D and tries to find the password of U. With online attacks, $\mathcal{A}$ is active and has access to oracles Send, Execute and Test(Π_U^i). Let q_s be the number of Send queries (attempted logins) and $|D|$ the size of the dictionary. For resistance against online dictionary attacks we require that the advantage of $\mathcal{A}$: $\mathsf{Adv}_{\mathcal{P},D}^{da\text{-}on}(\mathcal{A}) \leq q_s/|D|$. With offline attacks, $\mathcal{A}$ is passive and has access to oracle Execute. For resistance against offline dictionary attacks we require that: $\mathsf{Adv}_{\mathcal{P},D}^{da\text{-}off}(\mathcal{A}) \leq 1/|D|$ (no better than guessing).

2.3.6. Hash oracle h

Parties have access to a cryptographic hash function $h : \{0,1\}^* \rightarrow \{0,1\}^n$ of length n, modeled by a random oracle H that when queried with string x returns a uniformly random string $h(x)$ if x is the first such query, and the same string $h(x)$ otherwise. Adversary $\mathcal{A}$ can distinguish the output of $h(x)$ from random when there are collisions. According to the birthday paradox, the probability of a collision when q_h hashes are computed is approximately $q_h^2/(2|\mathsf{H}|)$ where $|\mathsf{H}|$ is the number of different outputs of oracle H.

2.3.7. Session unlinkability and unlinkability for user U

This is defined by an experiment involving oracle Test and two oracles Out, In: Out(Π_U^s) returns outgoing messages, while In(Π_U^v) returns incoming messages. A bit b is selected at random uniformly. Let U_1, U_2 be users with $U_1 = U_2$ when $b = 0$, and $U_1 \neq U_2$ when $b = 1$. When queried, Test returns messages m_1^b, m_2^b of Out($\Pi_{U_1}^s$), Out($\Pi_{U_2}^t$) for completed sessions. Adversary $\mathcal{A}$ has access to oracle Execute and must guess bit b. For *session unlinkability of outgoing messages* the advantage of $\mathcal{A}$: $\mathsf{Adv}_{\mathcal{P},U^{out}}^{unl}(\mathcal{A})$ must be negligible. Similarly for *session unlinkability of incoming messages*: $\mathsf{Adv}_{\mathcal{P},U^{in}}^{unl}(\mathcal{A})$ must be negligible. For *unlinkability of outgoing/incoming messages* there is no requirement for the session(s) to be completed.

2.4. Elliptic curve decision Diffie–Hellman problem

Let $\mathcal{G}_P$ be the cyclic group of order an n-bit prime q, generated by a point P on a nonsingular elliptic curve $E(\mathbb{F}_p)$ of the form $y^2 = x^3 + \alpha x + \beta$ over a finite field $\mathbb{F}_p$, $p > 3$ prime. The elements of $\mathcal{G}_P$ are points on $E(\mathbb{F}_p)$ of the form xP, $x \in Z_q$. We denote the coordinates of point $Q \in E(\mathbb{F}_p)$ by $Q.x$, $Q.y$.

The elliptic curve decision Diffie–Hellman (ECDDH) problem is to decide if $cP = abP$, given distributions (aP, bP, cP) and (aP, bP, abP), $a, b, c \in Z_q$. In the ROR model this is defined by an experiment involving oracle $\mathsf{Test}_{\mathcal{G}_P}$, which when queried selects a bit b at random uniformly, and returns $aP, bP, cP, aP, bP \in_R \mathcal{G}_P$ with $cP = abP$ when $b = 1$, while $cP \in_R \mathcal{G}_P$ when $b = 0$. The goal of adversary $\mathcal{A}$ is to guess b. If $\mathcal{A}$ outputs b' then the advantage of $\mathcal{A}$ is: $\mathsf{Adv}_{\mathcal{G}_P}^{ecddh}(\mathcal{A}) = 2 \cdot \Pr[b' = b] - 1$. The ECDDH assumption is that this problem is hard.

In the following three sections we shall analyze three recent 3-PAKE protocols: the Chang–Le protocols [12], the He et al. protocol [14] and the Das et al. protocol [13].

3. Analysis of the Chang–Le 3-PAKE protocols for HWSN

We use the notation in Table 1. The parties involved are: the user U_i, the smart card SC, the gateway G and the sensor S_j.

Pre-deployment

Gateway G assigns to each sensor S_j it controls an identifier id_j and a secret key $f_j = h(id_j \| x_g)$, where x_g is a master key of G for generating keys. The values (id_j, f_j) are written to the memory of S_j.

User registration (Fig. 2)

Let (id_i, pw_i) be an identifier and password of user U_i. U_i selects a random number r_i, computes the masked password $mp_i = h(r_i \| pw_i)$, and sends $(id_i \| mp_i)$ to G. G selects a random number r_i', and computes the: masked identifier $mi_i = h(r_i' \| id_i)$, secret key $f_i = h(mi_i \| x_g)$, and encrypted masked password $e_i = mp_i \oplus f_i$. Then G writes $(mi_i \| e_i)$ to a smart card SC and issues it to U_i. U_i writes the value r_i to SC.

Table 1
Notation.

G, S_j, U_i, SC	Gateway, sensor, user, smart card
x_g, h	Master key of G, cryptographic hash function (digest)
$h(x \parallel y)$	Digest of the concatenation of bitstrings x, y
$x \in_R X$	x is selected uniformly at random from set X
Z_q, Z_q^*, q prime	$\{0, 1, \ldots, q-1\}$, $\{1, 2, \ldots, q-1\}$
$x \oplus y$	Bitwise XOR of bitstrings x, y of equal length
id_j, f_j	Identifier and long-term secret key of S_j
id_i, pw_i, f_i, y_i	Identifier, password, long-term secret key, temporal credential of U_i
mi_i, mp_i, e_i	Masked id, masked pwd, encrypted masked pwd of U_i
F_{ij}, R_{ij}, z_i, z_g, z_j	Encryptions
n_i, a_j, F_{ij}, H_j, E_i	Message digests
r_i, r_i'	Random numbers
t_1. t_2. t_3, t_4, Δt	Timestamps, time delay for timestamps
k_i, k_j, sk	Random keys chosen by user U_i, sensor S_i, session key
$Q.x$, $Q.y$	The x and y coordinates of point Q on an elliptic curve $E(\mathbb{F}_p)$
n	Security parameter (length of the keys and digests)

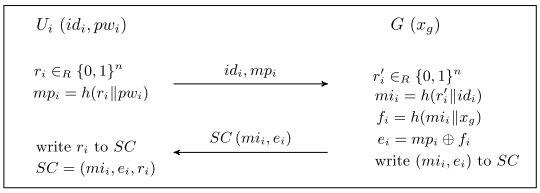


Fig. 2. User registration for the Chang–Le protocols.

3.1. Protocol $\mathcal{P}_{cl}$ (Fig. 3)

1. U_i inputs the identifier and password (id_i. pw_i) to SC that computes $mp_i = h(r_i \| pw_i)$, $f_i = e_i \oplus mp_i$ and $y_i = h(f_i \| t_1)$, where t_1 is the current timestamp. Then SC selects a random key k_i, and computes $z_i = k_i \oplus y_i$, and $n_i = h(y_i \| mi_i \| id_i)$. U_i sends to S_j: mi_i, z_i, n_i. t_1.
2. S_j verifies timestamp t_1 by checking that $|t_1 - t_c| \leq \Delta t$, where t_c is the current timestamp, and if valid, computes $a_j = h(f_j \| n_i \| t_2)$, where t_2 is the current timestamp, and sends G: id_j, mi_i, n_i, a_j, t_1, t_2.
3. G checks timestamps t_1, t_2 as before, and if valid, computes $f_i = h(mi_i \| x_g)$, $f_j = h(id_j \| x_g)$, $y_i = h(f_i \| t_1)$, and checks: $n_i \stackrel{?}{=} h(y_i \| mi_i \| id_i)$, $a_j \stackrel{?}{=} h(f_j \| n_i \| t_2)$. If valid, G encrypts y_i as $F_{ij} = y_i \oplus h(f_j \| t_3)$, t_3 a current timestamp, and computes $H_j = h(y_i)$ and $E_i = h(f_i \| n_i)$, and sends to S_j: F_{ij}, H_j, E_i, t_3.
4. S_j checks timestamp t_3 and if valid, computes $y_i = F_{ij} \oplus h(f_j \| t_3)$ and verifies $H_j \stackrel{?}{=} h(y_i)$. If valid, S_j selects a random key k_j, computes the key $k_i = z_i \oplus y_i$, and $R_{ij} = h(k_i \| t_4) \oplus k_j$, with t_4 the current timestamp, and sends to U_i: R_{ij}, E_i, t_4. Then it computes the session key $sk = h(k_i \oplus k_j)$.
5. SC checks timestamp t_4 and $E_i \stackrel{?}{=} h(f_i \| n_i)$. If valid, it computes the key $k_j = R_{ij} \oplus h(k_i \| t_4)$. Then it computes the session key $sk = h(k_i \oplus k_j)$.

Chang–Le [12] also proposed a variant $\mathcal{P}_{eccl}$ of this protocol that uses the elliptic curve Diffie–Hellman key agreement. For this variant: in Step 1, $k_i \leftarrow aP.x$, with $a \in_R Z_q^*$, q prime, P a generator of group $\mathcal{G}_P$ (Section 2.4); in Step 4, $k_j \leftarrow bP.x$, with $b \in_R Z_q^*$; finally, in Step 4 and Step 5 the session key is $sk \leftarrow h(abP.x)$.

3.2. Flaws and weaknesses of the Chang–Le protocols

3.2.1. Attacks on the semantic security of protocols $\mathcal{P}_{cl}$ and $\mathcal{P}_{eccl}$

The encrypted value z_i in the first flow (flow 1) of $\mathcal{P}_{cl}$ (and $\mathcal{P}_{eccl}$) is not authenticated. Adversary $\mathcal{A}$ can substitute z_i in flow 1 by $z_i' = z_i \oplus r$, $r \neq 0$, resulting in sensor S_j and user U_i computing different session keys without knowing it: S_j computes $sk' = h(k_i \oplus k_j \oplus r)$ in Step 4 while U_i computes $sk = h(k_i \oplus k_j)$ in Step 5. Similarly, the encrypted value R_{ij} in flow 4 is not authenticated. $\mathcal{A}$ can substitute R_{ij} by $R_{ij}' = R_{ij} \oplus r'$, $r' \neq 0$, resulting in U_i computing $sk' = h(k_i \oplus k_j \oplus r')$ in Step 5 while S_j has computed $sk = h(k_i \oplus k_j)$ in Step 4.

These attacks are captured in the ROR formalization with Send queries (Section 2.3.1). For the first attack, $\mathsf{Send}(\Pi_{S_j}^t; \langle mi_i, z_i', n_i, t_1 \rangle)$ is used in a session $(\Pi_{U_i}^s, \Pi_{S_j}^t, \Pi_G^u)$. In this session, instance $\Pi_{S_j}^t$ and partner $\Pi_{U_i}^s$ receive their last message and $\Pi_{U_i}^s$ goes into accept mode having computed $sk = h(k_i \oplus k_j)$, while $\Pi_{S_j}^t$ has computed $sk' = h(k_i \oplus k_j \oplus r)$. Consequently, $\mathsf{Test}(\Pi_{U_i}^s)$, $\mathsf{Test}(\Pi_{S_j}^t)$ return the same key in the random case ($b = 0$) but different keys in the real case ($b = 1$). Then $\mathsf{Adv}_{\mathcal{P},\mathcal{A}}^{ror\text{-}ake}(\mathcal{A}) = 1$, and we do not get semantic security. The second attack is similar: $\mathsf{Send}(\Pi_{U_i}^s, \langle mi_i, R_{ij}', E_i, t_4 \rangle)$ is used in a session $(\Pi_{U_i}^s, \Pi_{S_j}^t, \Pi_G^u)$. $\Pi_{U_i}^s$ and partner $\Pi_{S_j}^t$ receive their last message, and $\Pi_{S_j}^t$ computes $sk = h(k_i \oplus k_j)$ while $\Pi_{U_i}^s$ computes $sk' = h(k_i \oplus k_j \oplus r')$. Again $\mathsf{Test}(\Pi_{U_i}^s)$, $\mathsf{Test}(\Pi_S^t)$ return different keys in the real case, and $\mathsf{Adv}_{\mathcal{P}_{cl}}^{ror\text{-}ake}(\mathcal{A}) = 1$.

3.2.2. Attacks on session key privacy with respect to G of protocol $\mathcal{P}_{cl}$

In the ROR formalization the behavior of an honest-but-curious gateway G is defined in terms of oracles $\mathsf{Execute}$, $\mathsf{Send}(U_i)$, $\mathsf{Send}(S_j)$ and experiment $\mathsf{TestPair}$ (Section 2.3.2). For protocol $\mathcal{P}_{cl}$, the adversary $\mathcal{A}$ is given the keys f_i, f_j of U_i, S_j, and queries oracle $\mathsf{Execute}$ to get z_i, t_1, R_{ij}, t_4 from flows 1,4. Then $\mathcal{A}$ can compute $y_i = h(f_i \| t_1)$, $k_i = y_i \oplus z_i$, $k_j = R_{ij} \oplus h(k_i \| t_4)$, and the session key $sk = h(k_i \oplus k_j)$, and therefore $\mathsf{Adv}_{\mathcal{P},D}^{kp}(\mathcal{A}) = 1$.

3.2.3. Attacks on user anonymity

User U_i uses the pseudonym mi_i in $\mathcal{P}_{cl}$ (and $\mathcal{P}_{eccl}$). Since pseudonyms are not updated in each session, the adversary can

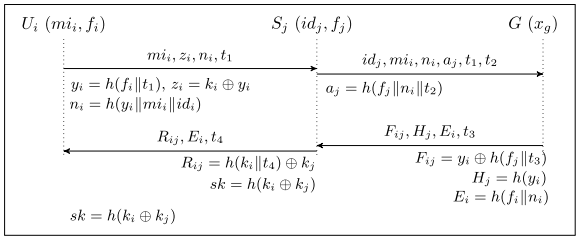


Fig. 3. The Chang–Le protocol $\mathcal{P}_{cl}$.

link the flows of U_i in different sessions and use traffic analysis to undermine the anonymity of U_i.

4. The He et al. 3-PAKE protocol

The He et al. protocol $\mathcal{P}_{he}$ [14] is a modification of the Chang–Le protocol designed to address an impersonation attack that exploits the time delay Δt of timestamps, and a session-state reveal attack. We briefly describe these attack for protocol $\mathcal{P}_{cl}$ using the ROR formalization.

An impersonation attack that uses a corrupted sensor. Adversary $\mathcal{A}$ first queries oracle Corrupt($\Pi^t_{S_j}$) that returns the secret key f_j of sensor S_j. Then $\mathcal{A}$ queries Send($\Pi^s_{U_i}$) in a session ($\Pi^s_{U_i}$, $\Pi^t_{S_j}$, Π^u_G) to get the first message $m_1 = \langle mi_i, z_i, n_i, t_1\rangle$ with $z_i = k_i \oplus y_i$, $y_i = h(f_i\|t_1)$ (Fig. 3). Finally $\mathcal{A}$ queries Send($\Pi^t_{S_j}$, m_1) to get $m_2 = \langle id_j, mi_i, n_i, n_j, t_1, t_2\rangle$, and Send($\Pi^v_G$, m_2) to get $m_3 = \langle F_{ij}, H_j, E_i, t_3\rangle$, with $F_{ij} = y_i \oplus h(f_j\|t_3)$. Now $\mathcal{A}$ can compute $h(f_j\|t_3)$ using f_j and therefore get the temporal identifier $y_i = f(f_i\|t_1)$ of U_i that is sufficient to impersonate U_i.

First $\mathcal{A}$ queries Send($\Pi^s_{S_v}$, m'_1), $S_v \neq S_j$, with $m'_1 = \langle mi_i, z'_i, n'_i, t_1\rangle$, $z'_i = k'_i \oplus y_i$, k'_i random, $n'_i = h(y_i\|mi_i\|id_v)$, to get m'_2; then Send(Π^t_G, m'_2) to get $m'_3 = \langle F_{iv}, H_v, E'_i, t_3\rangle$; and finally Send($\Pi^s_{S_v}$, m'_3) to get $m'_4 = \langle R'_{iv}, E'_i, t_4\rangle$, with $R'_{iv} = k_v \oplus h(k'_i\|t_4)$. $\mathcal{A}$ knows k'_i and can therefore get k_v and the session key $sk = h(k'_i \oplus k_v)$. Note that the validity of this attack depends on the freshness of the temporal identifier y_i: it is only valid until $t_1 + \Delta t$.

A session-state reveal attack. Adversary $\mathcal{A}$ first queries oracle Reveal($\Pi^s_{U_i}$) that returns the secret key k_i for a session sid, and then oracle Execute($\Pi^s_{U_i}$, Π^u_G, $\Pi^t_{S_j}$) for the same session to get $m_4 = \langle R_{ij}, t_4\rangle$. $\mathcal{A}$ can now compute the session key $sk = h(k_i \oplus k_j)$, using $k_j = R_{ij} \oplus h(k_i\|t_4)$.

4.1. Protocol $\mathcal{P}_{he}$

This is essentially the same as the Chang–Le protocol except that,

1. the temporal identifier y_i of user U_i in flow 1 is replaced by an identifier that links the session of U_i to the sensor S_j: $Y_i = h(f_i\|mi_i\|id_j)$, and
2. the messages that U_i, S_j exchange are part of the session key: $sk = h(baP.x\|aP.x\|mi_i\|id_j\|t_1\|t_4)$.

4.2. Flaws and weaknesses of the He et al. protocol

4.2.1. Attacks on semantic security

These are similar to the semantic security attacks on the Chang–Le protocols, allowing for the modifications above. Again the encrypted value z_i in flow 1 of $\mathcal{P}_{he}$ (Fig. 3, with $k_i \leftarrow aP.x$, $y_i \leftarrow Y_i = h(f_i\|mi_i\|id_j)$ and $sk \leftarrow sk = h(baP.x\|aP.x\|mi_i\|id_j\|t_1\|t_4)$), and the encrypted value R_{ij} in flow 4 are not authenticated. Adversary $\mathcal{A}$ can substitute z_i by $z'_i \neq z_i$, (R_{ij} by $R'_{ij} \neq R_{ij}$), resulting in user U_i accepting while computing a different session key from sensor S_j, so that oracles Test($\Pi^s_{U_i}$) and Test($\Pi^t_{S_j}$) return different keys in the real case, while in the ideal case they return the same key. Then $\mathsf{Adv}^{ror\text{-}ake}_{\mathcal{P}_{cl}}(\mathcal{A}) = 1$.

4.2.2. Attacks on user anonymity

The pseudonym mi_i of user U_i is not updated and therefore an adversary can link the flows of U_i from different sessions using traffic analysis.

5. The Das et al. 3-PAKE protocol

Das et al. [13] proposed a 3-PAKE protocol $\mathcal{P}_{das}$ that addresses some of the vulnerabilities of the Chang–Le protocols discussed in Section 3 by using biometrics. For this purpose a fuzzy extractor (Gen, Rep) is used, with:

- Gen: on input biometrics bio_i, outputs a biometric key σ_i and a public reproduction parameter τ_i, and
- Rep: on input biometrics bio'_i and parameter τ_i, outputs the key σ_i, provided the Hamming distance of bio_i and bio'_i is less than an error-tolerance threshold t.

Pre-deployment and user registration

As with the Chang–Le protocols, gateway G assigns to each sensor S_j an identifier id_j and secret key $f_j = h(id_j\|x_g)$. The smart card SC stores the values: mi_i, e^*_i, g_i, mpb_i, τ_i, where $e^*_i = e_i \oplus h(id_i\|r_i\|\sigma_i)$, $e_i = mp_i \oplus f_i$, $mp_i = h(r_i\|pw_i)$, $mi_i = h(r'_i\|id_i)$, r_i, r'_i random numbers, $f_i = h(mi_i\|x_g)$, $g_i = r_i \oplus mb_i$, $mb_i = h(id_i\|\sigma_i)$, $mpb_i = h(id_i\|r_i\|pw_i\|\sigma_i)$, and t is the error tolerance. This makes it possible for SC to authenticate U_i: on input id_i, pw_i, bio'_i, the smart card computes: $\sigma^*_i = Rep(bio'_i, \tau_i)$, $mb^*_i = h(id_i\|\sigma^*_i)$, $r^*_i = g_i \oplus mb^*_i$, $mp^*_i = h(r^*_i\|pw_i)$, $mpb^*_i = h(id_i\|r^*_i\|pw_i\|\sigma^*_i)$, and authenticates U_i when $mpb^*_i = mpb_i$ (which happens when the Hamming distance of bio_i and bio'_i is bounded by the error tolerance t).

5.1. Protocol $\mathcal{P}_{das}$ (Fig. 4)

1. U_i inserts SC in a terminal and inputs (id_i, pw_i) and an imprint bio'_i into a sensor at the terminal. SC then computes $\sigma^*_i = Rep(bio'_i, \tau_i)$, $mb^*_i = h(id_i\|\sigma^*_i)$, $r^*_i = g_i \oplus mb^*_i$, $mp^*_i = h(r^*_i\|pw_i)$, $mpb^*_i = h(id_i\|r^*_i\|pw_i\|\sigma^*_i)$, and accepts U_i as authenticated if $mpb^*_i = mpb_i$. Otherwise it aborts. If U_i is authenticated then SC computes: $f_i = e^*_i \oplus mp^*_i \oplus h(id_i\|r^*_i\|\sigma^*_i) = h(mi_i\|x_g)$, $K_i = aP$, $a \in Z_q$ a random number, $x_i = h(f_i\|t_1)$, t_1 a current timestamp, $y_i = h(id_j\|x_i)$, $v_i =$

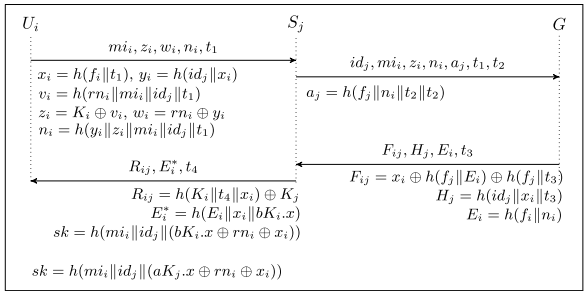


Fig. 4. The Das et al. protocol $\mathcal{P}_{das}$.

$h(rn_i\|z_i\|mi_i\|id_j\|t_1)$, $z_i = (K_i.x, K_i.y) \oplus (v_i, 0) \pmod q$, $w_i = rn_i \oplus y_i$, rn_i a random number, and $n_i = h(y_1\|z_i\|mi_i\|id_j)$. Then SC sends to S_j: mi_i, z_i, w_i, n_i, t_1.

2. S_j checks timestamp t_1, and if valid, computes $a_j = h(f_j\|n_i\|t_1\|t_2)$, where t_2 is the current timestamp, and sends G: $id_j, mi_i, n_i, a_j, t_1, t_2$.
3. G checks timestamp t_2 and if valid, computes $f_j = h(id_j\|x_g)$, $f_i = h(mi_i\|x_g)$, $x_i = h(f_i\|t_1)$, $y_i = h(id_j\|x_i)$, and checks: $n_i \stackrel{?}{=} h(y_i\|z_i\|mi_i\|id_j)$, $a_j \stackrel{?}{=} h(f_j\|n_i\|t_1\|t_2)$. G aborts if these are not valid. Otherwise it accepts U_i, and computes $E_i = h(f_i\|n_i)$, $F_{ij} = x_i \oplus h(f_j\|E_i) \oplus h(f_j\|t_3)$, t_3 a current timestamp, and $H_j = h(id_j\|x_i\|t_3)$, and sends to S_j: F_{ij}, H_j, E_i, t_3.
4. S_j checks timestamp t_3 and if valid, computes $x_i = F_{ij} \oplus h(f_j\|E_i) \oplus h(f_j\|t_3)$, and verifies $H_j \stackrel{?}{=} h(id_j\|x_i\|t_3)$. If valid, S_j accepts U_i, computes $y_i = h(id_j\|x_i)$, $rn_i = w_i \oplus y_i$, $K_i = z_i \oplus h(rn_i\|mi_i\|id_j\|t_1)$, selects a random number $b \in Z_q$, computes the key $K_j = bP$, $R_{ij} = h(K_i\|t_4\|x_i) \oplus K_j$, with t_4 the current timestamp, $E_i^* = h(E_i\|x_i\|bK_i.x)$, and sends to U_i: R_{ij}, E_i^*, t_4. Then S_j computes the session key $sk = h(mi_i\|id_j\|bK_i.x \oplus rn_i \oplus x_i)$.
5. SC checks timestamp t_4 and if valid computes $E_i = f(f_i\|n_i)$, $K_j = R_{ij} \oplus h(K_i\|t_4\|x_i)$, and checks $E_i^* \stackrel{?}{=} h(E_i\|x_i\|aK_j.x)$. If valid, it accepts and computes the session key $sk = h(mi_i\|id_j\|aK_j.x \oplus rn_i \oplus x_i)$. Note that $aK_j = bK_i = abP$.

5.2. Flaws and weaknesses of the Das et al. protocol

5.2.1. An offline dictionary attack that uses corrupted smart cards & biosensors

The imprint bio_i of user U_i is an immutable key that cannot be treated as a secret, unlike password pw_i. Passwords may be weak and are vulnerable to social engineering attacks, but can be updated. This will reduce the impact of such attacks. This is not the case with biometric imprints that can be accessed in different ways, (*e.g.,* by using forged smart cards.

If adversary $\mathcal{A}$ has access to an imprint bio_i' of user U_i, the identifier id_i and the values: $mi_i, e_i^*, g_i, mpb_i, \tau_i$ from a stolen smart card SC, then $\mathcal{A}$ can get: $mb_i = h(id_i\|\sigma_i)$, $r_i = g_i \oplus mb_i$, and use these for an offline dictionary attack. We show how this is done using the ROR formalization.

$\mathcal{A}$ queries oracles Corrupt(SC) and Corrupt($BioSensor$) to get $mi_i, e_i^*, g_i, mpb_i, \tau_i, t$, and id_i, bio_i' and computes mb_i and r_i. Then, for any $pw' \in D$, with D a password dictionary, $\mathcal{A}$ checks $mbp_i \stackrel{?}{=} h(id_i\|r_i\|pw_i'\|\sigma_i)$.[2] If this is valid then $pw' = pw_i$; otherwise $\mathcal{A}$ repeats the calculation for another password in D.

5.2.2. An impersonation attack that uses a corrupted sensor

This is an extension of the He et al. attack (Section 4) that exploits temporal credentials. First $\mathcal{A}$ queries oracle Corrupt($\Pi_{S_j}^t$) to get the secret key f_j of S_j, and then instantiates a session $(\Pi_{U_i}^s, \Pi_{S_j}^t, \Pi_G^u)$ using oracle Send to get the messages (Fig. 4): $m_1 = \langle mi_i, z_i, w_i, n_i, t_1\rangle$, $m_2 = \langle id_j, mi_i, z_i, n_i, n_j, t_1, t_2\rangle$ and $m_3 = \langle F_{ij}, H_j, E_i, t_3\rangle$, with $F_{ij} = x_i \oplus h(f_j\|E_i) \oplus h(f_j\|t_3)$. $\mathcal{A}$ can now compute the temporal key x_i of U_i from F_{ij} and the temporal credential $y_i = h(id_j\|x_i)$ of U_i for sensor S_j, that are sufficient to impersonate U_i.

First $\mathcal{A}$ queries Send($\Pi_{S_v}^s, m_1'$), $S_v \neq S_j$, with $m_1' = \langle mi_i, z_i', w_i', n_i', t_1\rangle$, where $z_i' = a'P.x \oplus v_i'$, $a' \in Z_q$, $v_i' = h(rn_i'\|mi_i\|id_v\|t_1)$, $w_i' = rn_i' \oplus y_i$, $n_i' = h(y_i\|z_i'\|mi_i\|id_v)$, to get m_2'; then Send(Π_G^t, m_2') to get m_3', and then Send($\Pi_{S_v}^s, m_3'$) to get $m_4' = \langle R_{iv}, E_i', t_4\rangle$, with $R_{iv} = h(a'P.x\|t_4\|x_i) \oplus cP.x$. $\mathcal{A}$ knows $a'P.x$ and x_i, so can get $cP.x$ from R_{iv}, and then compute the session key $sk = h(a'cP.x)$.

5.2.3. Attacks on user anonymity

The pseudonym mi_i of user U_i is not dynamic and an adversary can link sessions using traffic analysis.

6. A novel 3-PAKE protocol for HWSN and extensions

In this section we describe a novel heterogeneous 3-PAKE protocol and two extensions that addresses the vulnerabilities of the protocols discussed in Sections 3–5. We start with the basic protocol.

6.1. Communication model for heterogeneous 3-AKE protocols (Fig. 5)

We employ the HWSN model described in Section 2.2. This is more appropriate for IoT applications and addresses the heterogeneous communication and computation constraints of user U, gateway G and sensor S. Typically, S has restricted computation power and broadcast range, and cannot process multiple queries concurrently, while no such constraints exist for U and G. This model captures real world applications where a user wants to access sensitive data collected by sensors in an IoT environment.

[2] In the Das et al. protocol [13] the password pw_i and biometrics bio_i' are updated, but not the identifier id_i. If the identifier is also updated then a *double dictionary* attack over all pairs (id_i, pw_i) should be used.

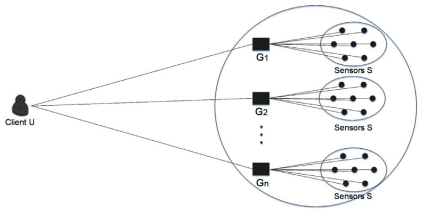


Fig. 5. Communication model for HWSN.

6.2. Pre-deployment and user registration

We employ the pre-deployment and user registration protocols in Sections 3 and 5 (as in [3,12]), using a secure channel. We do not discuss trust management policies for resource management, typically based on user attributes and credentials.

6.3. The basic heterogeneous 3-PAKE protocol $\mathcal{P}_1$

With encrypted key exchange (EKE) protocols [18], encryption is used to link the user's data to the user while authentication is used to link the server's data to the server. Fig. 6 shows the flows of protocol $\mathcal{P}_1$ that uses such an approach. In this protocol the gateway G relays the messages of user U_i and sensor S_j to address the fact that sensors may be resource constrained and restricted to short range transmissions. Below we briefly describe it. In the following sections we shall consider extensions that capture session key privacy, forward secrecy, offline dictionary attack protection and anonymity.

In protocol $\mathcal{P}_1$ the user U_i sends in flow 1 to gateway G the encryption $z_i = k_i \oplus h(f_i\|id_j\|t_1)$ of key $k_i \in_R \{0,1\}^n$ using the temporal credential $h(f_i\|id_j\|t_1)$, and G decrypts z_i and re-encrypts it as $z_g = k_i \oplus h(f_j\|mi_i\|t_2)$, using the temporal credential $h(f_j\|mi_i\|t_2)$, which it sends in flow 2 to sensor S_j. This encryption uses the private key f_j of S_j, so S_j can decrypt it to get k_i. These encryptions as well as the encryption z_j of key $k_j \in_R \{0,1\}^n$ of S_j in flow 3 are timestamped. In the last flow, G relays the values z_j, z_g, mac_j to U_i together with the timestamps t_2, t_3.

Note that $mac_j = h(v)$, $v = (k_i \oplus k_j\|k_i\|mi_i\|id_g\|id_j\|z_i\|z_g\|z_j\|t_1\|t_2\|t_3)$, authenticates the messages of U_i and S_j, and that if the adversary substitutes any of z_i, z_g, z_j with different values then U_i will not accept since it will compute a different value for the concatenation v and hence mac_j will not be validated. The session key is $sk = h(v\|1)$. We now formally prove the security of this protocol.

6.4. Security of protocol $\mathcal{P}_1$ in the ROR model

$\mathcal{P}_1$ is based on the EKE protocol of Bresson *et al.* [18], a variant of the Bellovin and Merrit password-based protocol for which we have semantic security in the ROR model.

Theorem 6.1. *Let q_h be the number of hash queries made by adversary $\mathcal{A}$ and $|\mathsf{H}|$ the number of different outputs of oracle H. Then the advantage of $\mathcal{A}$ in protocol $\mathcal{P}_1$ in the ROR model is:* $\mathsf{Adv}^{ror\text{-}ake}_{\mathcal{P}_1}(\mathcal{A}) \leq q_h^2/|\mathsf{H}|$.

Proof. The proof involves a sequence of experiments Exp_i, $i = 0, 1, 2, 3$, with oracle Test, in which the success probability $Pr[succ_i]$ of $\mathcal{A}$ is shown to be bounded close to 1/2, starting with Exp_0 that corresponds to a real attack in the random oracle model.

Exp_0. We have: $\mathsf{Adv}^{ror\text{-}ake}_{\mathcal{P}_1}(\mathcal{A}) = 2 \cdot Pr[succ_0] - 1$.

Exp_1. This models passive attacks. $\mathcal{A}$ has access to oracle Execute and must guess the value of bit b of Test. The difference between Exp_1 and Exp_0 is that $\mathcal{A}$ can exploit dependencies between transmitted messages to distinguish the session key from a random key. Since the messages z_i, z_g, z_j simulate one-time-pad encryptions and mac_j uses a random hash function, $\mathcal{A}$ cannot use these to distinguish the session key from random. It follows that $Pr[succ_0] = Pr[succ_1]$.

Exp_2. This models active attacks in which $\mathcal{A}$ exploits hash collisions to get U_i, S_j to accept different session keys. We modify the simulation in the previous experiment so that all execution instances in which a collision occurs are halted and $\Pi^a_{U_i}$ does not accept. The difference between Exp_2 and Exp_1 is that $\mathcal{A}$ can use substitution attacks to exploit hash collisions: for example, to substitute one of the encryptions z_i by $z_i' \neq z_i$, and get the same value for mac_j. $\mathcal{A}$ has access to oracles Execute, Send and Test, and must guess the bit b. Let q_h be the number of hash queries. Then (see Section 2.3.6), $Pr[succ_1] - Pr[succ_2] \leq q_h^2/(2|\mathsf{H}|)$.

Exp_3. This models active attacks in which $\mathcal{A}$ substitutes messages to get U_i, S_j to accept different session keys (see Section 2.3.1). We modify the simulation of the Send oracle in the previous experiment so that its output is uniformly random, and the session key is uniformly random. $\mathcal{A}$ has access to oracles Execute, Send and Test. The difference between Exp_3 and Exp_2 is that $\mathcal{A}$ can use substitution attacks: for example, query oracle $\mathsf{Send}(\Pi^b_{S_j})$ with an encryption $z_i' \neq z_i$ that will result in U_i, S_j computing different session keys. However mac_j authenticates all transmitted messages, so when U_i checks it, it will be rejected (if S_j used z_i (z_i') in mac_j then U_i will check it using z_i' (z_i)). Thus $Pr[succ_3] = Pr[succ_2]$. Finally note that in Exp_3 all oracles have been simulated and return uniformly random values, and the session key is random. So the success probability of $\mathcal{A}$ is $Pr[succ_3] = 1/2$.

Combining these we get that the advantage of $\mathcal{A}$ is: $\mathsf{Adv}^{ror\text{-}ake}_{\mathcal{P}_1}(\mathcal{A}) = 2 \cdot Pr[succ_0] - 1 = 2 \cdot \sum_{i=0}^{2}(Pr[succ_i] - Pr[succ_{i+1}]) \leq q_h^2/|\mathsf{H}|$. □

6.4.1. Session-state reveal attacks

In these attacks the adversary can access the ephemeral state of incomplete sessions, such as the keys k_i, k_j computed by the U_i, S_j (see Section 2.3.4). To prevent such attacks, gateway G sends, additionally, in the last flow the message $w_g = h(f_i\|id_j\|t_3) \oplus h(f_j\|mi_i\|t_3)$, and includes the credential $h(f_j\|mi_i\|t_3)$ in the array v of the session key (U_i can compute this from w_g).

To show that protocol $\mathcal{P}_1$ with this modification addresses such attacks using the ROR formalization we employ one more experiment Exp_4 that models session-state reveal attacks in the proof of Theorem 4.1.

Exp_4. $\mathcal{A}$ has access to oracles Execute and Reveal and must guess the value of bit b of Test. From $\mathsf{Reveal}(\Pi^s_{U_i})$ and $\mathsf{Reveal}(\Pi^t_{S_j})$, $\mathcal{A}$ can get the random numbers k_i, k_j, but cannot get the temporal credential $h(f_j\|mi\|t_3)$ from w_g. Therefore $\mathcal{A}$ cannot compute the session key $sk = h(v\|1)$, and $Pr[succ_4] = Pr[succ_3]$.

If adversary $\mathcal{A}$ steals the smart card SC, then $\mathcal{A}$ can use it for an *online* dictionary attack by inputting to SC a password pw' selected randomly from a password dictionary D (as in [12]). This attack increases the advantage of $\mathcal{A}$ by: $q_s/|D|$, where q_s is the number of Send queries (permitted login attempts). However, we do not have *offline* dictionary attack protection (as in Section 5.2), nor forward secrecy, because if $\mathcal{A}$ corrupts S_j, then $\mathcal{A}$ can access key f_j of S_j to decrypt z_g, z_j and get k_i, k_j, w_g, and then compute the session key.

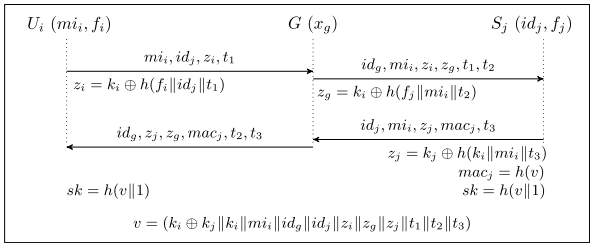


Fig. 6. The heterogeneous 3-PAKE protocol $\mathcal{P}_1$.

6.5. The heterogeneous 3-PAKE protocol $\mathcal{P}_2$

Protocol $\mathcal{P}_2$ extends protocol $\mathcal{P}_1$ to address session key privacy attacks, forward secrecy and offline dictionary attacks (Section 2.3), by using an elliptic curve Diffie–Hellman session key as in the Chang–Le protocol $\mathcal{P}_{ecc1}$ and Das et al. protocol $\mathcal{P}_{das}$ (Section 5). The flows of this protocol are shown in Fig. 7, with a detailed description following.

1. U_i inputs (id_i, pw_i) to SC. SC computes $mp_i = h(r_i \| pw_i)$, $f_i = e_i \oplus mp_i$ and $y_i = h(f_i \| id_j \| t_1)$, where t_1 is a current timestamp. Then U_i selects $aP \in \mathcal{G}_p$, $a \in_R Z_q^*$, computes $z_i = aP.x \oplus y_i$, and sends to G: mi_i, id_i, z_i, t_1.
2. G verifies timestamp t_1, and if valid, computes $f_i = h(mi_i \| x_g)$, $f_j = h(id_j \| x_g)$, $y_i = h(f_i \| id_j \| t_1)$, $aP.x = z_i \oplus y_i$ and $z_g = aP.x \oplus h(f_j \| mi_i. \| t_2)$, where t_2 is a current timestamp. Then G sends to S_j: id_g, mi_i, z_i, z_g, t_1, t_2.
3. S_j verifies t_2, and if valid, computes $aP.x = z_g \oplus h(f_j \| mi_i \| t_2)$. Then S_j selects $bP \in \mathcal{G}_p$, $b \in_R Z_q^*$, and computes $z_j = bP.x \oplus h(aP.x \| mi_i \| t_3)$, $abP.x$. Let $v = (abP.x \| aP.x \| mi_i \| id_g \| id_j \| z_i \| z_g \| z_j \| t_1 \| t_2 \| t_3)$ $mac_j = h(v)$. S_j sends to G: id_j, mi_i, z_j, mac_j, t_3, and computes the session key $sk = h(v\|1)$.
4. G verifies t_3 and if valid, sends to U_i: id_g, z_j, z_g, mac_j, t_2, t_3.
5. U_i verifies t_3 and if valid, computes $bP.x = z_j \oplus h(aP.x \| t_3)$, $abP.x$.[3] Then U_i checks if: $mac_j \stackrel{?}{=} h(v)$, where $v = (abP.x \| aP.x \| mi_i \| id_g \| id_j \| z_i \| z_g \| z_j \| t_1 \| t_2 \| t_3)$. U_i accepts if this is valid, and computes the session key $sk = h(v\|1)$.

6.6. Security of protocol $\mathcal{P}_2$ in the ROR model

6.6.1. Session key privacy with respect to gateway G

This is defined in terms of an experiment that involves oracle TestPair (Section 2.3.2). Adversary $\mathcal{A}$ has access to oracles Corrupt(Π_G^j), Execute and TestPair. From Corrupt(Π_G^j) and Execute, $\mathcal{A}$ gets the long-term key f_i and the encrypted values z_i, z_j, and can decrypt them to get $aP.x$, $bP.x$. Since the session key sk uses the EC Diffie–Hellman key $abP.x$, distinguishing sk from random reduces to the ECDDH assumption. Thus, the advantage of $\mathcal{A}$ is $\mathsf{Adv}_{\mathcal{P}}^{kp}(\mathcal{A}) \leq \mathsf{Adv}_{\mathcal{G}_p}^{ecddh}(\mathcal{A})$.

6.6.2. Forward secrecy for sensor S_j

This is defined in terms of an experiment that involves Test (Section 2.3.3). $\mathcal{A}$ has access to oracles Corrupt(Π_S^t), Execute, Send, and must guess the bit b. $\mathcal{A}$ gets the long-term key f_j of S_s from Corrupt($\Pi_{S_j}^t$) and the encryptions z_g, z_j from Execute, and as in the previous case, $\mathcal{A}$ can compute: $aP.x$, $bP.x$. Again distinguishing the session key from random reduces to the ECDDH assumption. Thus, the advantage of $\mathcal{A}$ is $\mathsf{Adv}_{\mathcal{P}}^{fs}(\mathcal{A}) \leq \mathsf{Adv}_{\mathcal{G}_p}^{ecddh}(\mathcal{A})$.

[3] There are two points on the EC other than ∞ with x-coordinate $bP.x$: bP, $-bP$. However abP, $-abP$ have the same x-coordinate: $abP.x$.

6.6.3. Offline dictionary attacks that use corrupted smart cards

These are defined in terms of oracle Corrupt(SC) and Execute (Section 2.3.5). $\mathcal{A}$ has a password dictionary D and selects $pw' \in D$. $\mathcal{A}$ gets id_i, e_i, r_i from Corrupt(SC), the encrypted values z_i, z_j and mi_i, id_j, mac_j, t_1, t_3 from Execute, and then computes $mp_i' = h(pw' \| r_i)$, for $pw' \in D$, and the key $f_i' = e_i \oplus pw'$, and uses this to decrypt z_i to get $a'P.x$ and z_j to get $b'P.x$. However computing the Diffie–Hellman key $a'b'P.x$ to check correctness using mac_j reduces to the ECDDH assumption. Thus again $\mathsf{Adv}_{\mathcal{P},D}^{da\text{-}aff}(\mathcal{A}) \leq \mathsf{Adv}_{\mathcal{G}_p}^{ecddh}(\mathcal{A})$.

Theorem 6.2. *Let q_h be the number of hash queries and q_s the number of* Send *queries made by adversary $\mathcal{A}$, and let $|\mathsf{H}|$ be the number of different outputs of oracle H, and $|D|$ the size of the dictionary. Then the advantage of $\mathcal{A}$ in protocol $\mathcal{P}_2$ in the ROR model is:* $\mathsf{Adv}_{\mathcal{P}_2}^{ror\text{-}ake}(\mathcal{A}) \leq 2 \cdot \mathsf{Adv}_{\mathcal{G}_p}^{ecddh} + q_h^2/|\mathsf{H}| + (1 + q_s)/|D|$.

Proof. This follows from Theorem 6.1, and the bounds on: $\mathsf{Adv}_{\mathcal{P}}^{kp}(\mathcal{A})$ for session key privacy, $\mathsf{Adv}_{\mathcal{P},D}^{da\text{-}on}(\mathcal{A})$ for online dictionary attacks, and $\mathsf{Adv}_{\mathcal{P},D}^{da\text{-}off}(\mathcal{A})$ for offline dictionary attacks. □

6.7. Biometric authentication

Protocol $\mathcal{P}_2$ can be modified to get three-factor authentication by adding biometric authentication and having gateway G validate all factors (solutions for which the smart card SC authenticates biometrics are vulnerable to SC theft and corruption attacks as shown in Section 5.2.1). Fig. 8 shows the modifications to the user registration protocol in Section 3.

Modifications for three-factor authentication

Only the first step of protocol $\mathcal{P}_2$ needs to be modified.

1. U_i inputs (id_i, pw_i) to SC and imprint bio_i' to a sensor. SC computes $\sigma_i = Rep(bio_i', \tau_i)$ using the tolerance rate t, $mpbi_i = h(r_i \| pw_i \| \sigma_i)$, $f_i = e_i \oplus mpbi_i$ and $y_i = h(f_i \| id_j \| t_1)$, where t_1 is a current timestamp. Then U_i selects $aP \in \mathcal{G}_p$, $a \in_R Z_q$, computes $z_i = aP.x \oplus y_i$, and sends to G: mi_i, id_i, z_i, t_1.

6.8. A heterogeneous 3-PAKE protocol $\mathcal{P}_3$ with user anonymity

Anonymity for user U_i refers to the difficulty of identifying U_i from protocol transcripts, and in particular, linking transcripts of U_i. For our applications we are not concerned with the anonymity of gateway G whose function is to provide a secure interface to sensors S_j, nor with the anonymity of sensor S_j. We distinguish two versions of $\mathcal{P}_3$: $\mathcal{P}_{31}$ and $\mathcal{P}_{32}$.

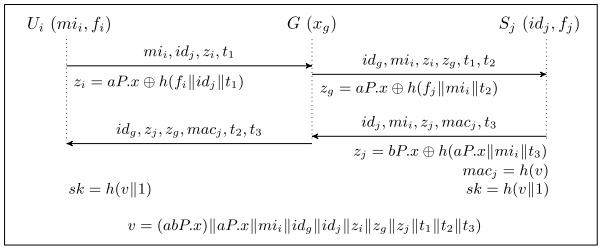


Fig. 7. The heterogeneous 3-PAKE protocol $\mathcal{P}_2$.

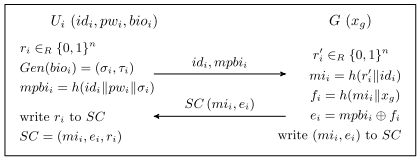


Fig. 8. User registration modifications for three-factor authentication in protocol $\mathcal{P}_2$.

In protocol $\mathcal{P}_{31}$ the pseudonym mi_i that U_i and G share is replaced by two randomized pseudonyms $ps_i = h(f_i \| ctr)$, $ps_g = h(f_i \| ctr + 1)$, where ctr is a counter. To protect against desynchronization failure or attacks, we use an approach first proposed for Radio Frequency Identification (RFID) [19]: G stores two values of the pseudonym ps_i, the current value ps^{cur} and an earlier value ps^{old}, as well as ps_g, while U_i stores only ps_i. Both U_i and G store the counter ctr that is used to update ps_i, ps_g. Initially $ps^{cur} = ps_i$ and $ps^{old} = \lambda$. Fig. 9 shows the flows of protocol $\mathcal{P}_{31}$.

In flow 1, U_i uses the pseudonym ps_i. G checks if $ps_i \stackrel{?}{=} ps^{cur}$ or $ps_i \stackrel{?}{=} ps^{old}$. If ps_i=ps^{cur} (corresponding to the case when the previous session was completed successfully), then G updates the stored pseudonyms: $ps^{old} \leftarrow ps^{cur}$, $ps^{cur} \leftarrow h(f_i \| ctr + 2)$, $ps_g \leftarrow h(f_i \| ctr + 1)$, and the counter: $ctr \leftarrow ctr + 2$. If $ps_i = ps^{old}$ (corresponding to the case when the previous session was not completed successfully), then G does not update the stored pseudonyms, nor the counter. In flow 2, G replaces the pseudonym mi_i by a random number rn (there is no need for sensor S_j to know who the user is) and in flow 3, S_j uses this number as an identifier. Finally in flow 4, G replaces the identifier id_g by pseudonym ps_g. If U_i receives flow 4, then it checks if $ps_g \stackrel{?}{=} h(f_i \| cnt+1)$. If this holds, then U_i updates the stored values: $cnt \leftarrow cnt + 2$, $ps_i \leftarrow h(f_i \| ctr)$; else it aborts.

In protocol $\mathcal{P}_{32}$ the pseudonym mi_i is encrypted using an elliptic curve Diffie–Hellman key. Gateway G publishes the public key $Y_g = y_g P$, and U_i uses the encryption of mi_i as a randomized pseudonym $ps_i = (c_i, c_2)$ where $c_1 = x_i P.x$, $x_i \in_R Z_q$, $c_2 = mi_i \oplus h(x_i Y_g.x \| t_1)$, when sending messages to G, while G uses the pseudonym $ps_g = h(x_i Y_g.x)$ when sending messages to U_i. As in protocol $\mathcal{P}_{31}$, random numbers rn are used to identify AKE sessions with sensor S_j.

6.9. User unlinkability for protocols $\mathcal{P}_{31}$, $\mathcal{P}_{32}$ in the ROR model

We only discuss unlinkability for user U_i (Section 2.3.7), and note that the other security aspects of protocols $\mathcal{P}_{31}$, $\mathcal{P}_{32}$ are shared with protocol $\mathcal{P}_2$, and discussed in Section 6.6.

The difference between $\mathcal{P}_{31}$ and $\mathcal{P}_2$ is that: in flow 1 the pseudonym mi_i of U_i is replaced by the pseudorandom ps_i; in flows 2,3, mi_i is replaced by the pseudorandom number n_g, and in flow 4 the identifier id_g of G is replaced by the pseudorandom ps_g. We get session unlinkability of outgoing and incoming user messages because these values cannot be distinguished from random by the adversary. Note that session unlinkability provides only unlinkability between successful executions: incomplete executions can be linked because the same pseudonym is re-used (but to keep it so, requires continuous disruption by the adversary: the link is lost once the protocol executes successfully).

In $\mathcal{P}_{32}$ the pseudonym ps_i is an encryption of mi_i and ps_g the digest of a Diffie–Hellman key. G can decrypt ps_i by computing $y_g c_1 = x_i Y_g.x$ and then $mi_i = c_2 \oplus h(y_g c_1 \| t_1)$, and U_i can compute $ps_g = h(x_i Y_g.x)$. It is easy to see that unlinkability is reduced to the ECDDH assumption. This protocol provides full unlinkability.

6.10. Practical issues

6.10.1. Implicit authentication, dos attacks

AKE protocols authenticate exchanged keys, not entities. This means that adversary $\mathcal{A}$ can try to impersonate user U_i by selecting any value z'_i for the encryption of U_i, and using it in flow 1 of protocol $\mathcal{P}_1$. This is a valid flow and will be processed by gateway G and sensor S_j, and eventually $\mathcal{A}$ will get flow 4. $\mathcal{A}$ cannot compute the session key (nor distinguish it from random), so this is not a threat to semantic security. However it may lead to a DoS attack. If DoS attacks are a concern then it is possible to prevent them by adding a MAC in the first flow to authenticate user U_i. It is easy to see that if this uses a key that is based on the password pw_i of U_i, and stored on the smart card SC, then when SC is stolen, offline dictionary attacks will be possible (as in Section 5.2 with the Das et al. protocol). Thus, the key must be independent of pw_i. The solution we propose is to use a new key $\hat{f}_i = h(mi_i \| x_g \| 1)$, that the gateway stores on the smart card SC together with (mi_i, e_i, r_i). Then $mac_i = h(\hat{f}_i \| z_i \| t_1)$ is added to flows 1,2. G checks it, and if it is not valid, the session is aborted. For this application, mac_i must be included in the concatenated string v, and from a security point of view, regarded as a nonce.

6.10.2. Lightweight applications

The protocols proposed in this paper use timestamps. The communication model for heterogeneous 3-PAKE protocols (Section 2.1) assumes that user U_i and gateway G have adequate resources for cryptographic protection, while sensors S_j are

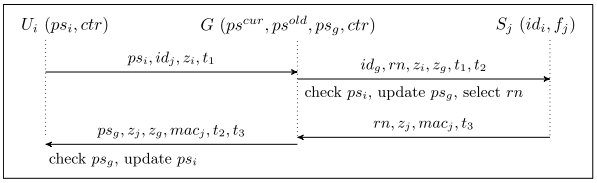


Fig. 9. The heterogeneous 3-PAKE protocol $\mathcal{P}_{31}$ with user anonymity.

Table 2
Computation cost comparison with lightweight protocols.

	Li et al. [1]	$\mathcal{P}_{cl}$ [12]	$\mathcal{P}_1$
User	$9t_h + 6t_{XOR}$	$7t_h + 4t_{XOR}$	$5t_h + 3t_{XOR}$
Sensor	$5t_h + 3t_{XOR}$	$5t_h + 4t_{XOR}$	$4t_h + 2t_{XOR}$
Gateway	$12t_h + 6t_{XOR}$	$8t_h + 1t_{XOR}$	$4t_h + 2t_{XOR}$

Table 3
Computation cost comparison with EC-based protocols.

	$\mathcal{P}_{ecl}$ [12]	$\mathcal{P}_{he}$ [14]	$\mathcal{P}_{das}$ [13]	$\mathcal{P}_2$
User	$2t_{mul} + 7t_h$	$2t_{mul} + 6t_h$	$2t_{mul} + 12t_h$	$2t_{mul} + 5t_h$
Sensor	$2t_{mul} + 5t_h$	$2t_{mul} + 5t_h$	$2t_{mul} + 9t_h$	$2t_{mul} + 4t_h$
Gateway	$9t_h$	$8t_h$	$10t_h$	$4t_h$

Table 4
Comparison of security features.

	$\mathcal{P}_{cl}$	$\mathcal{P}_{ecl}$	$\mathcal{P}_{he}$	$\mathcal{P}_{das}$	$\mathcal{P}_1$	$\mathcal{P}_2$	$\mathcal{P}_3$
Mutual authentication	✓	✓	✓	✓	✓	✓	✓
HWSN architecture	×	×	×	✓	✓	✓	✓
Passive attacks	✓	✓	✓	✓	✓	✓	✓
Replay attacks	✓	✓	✓	✓	✓	✓	✓
Session key integrity	×	×	×	✓	✓	✓	✓
Session key privacy	×	×	×	✓	×	✓	✓
Offline dictionary attacks	×	×	×	×	✓	✓	
User pseudonym	✓	✓	✓	✓	✓	✓	✓
User anonymity (unlink)	×	×	×	×	×	×	✓
Vulnerability to lost SC	×	×	×	✓	×	×	✓
Forward secrecy	×	✓	✓	×	×	✓	✓

resource-constrained. In particular they may not have an internal clock mechanism or maintain synchronized time. For such applications we can replace timestamp t_3 in flows 3,4 of protocols $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, by a nonce rn_j, and have S_j keep track of time by using a timer (*e.g.*, a discharging capacitor), that upper bounds processing time. If the bound is Δ^*, then when G receives flow 3, it verifies the time delay by checking that $|t_c - t_2| < 2\Delta t + \Delta^*$, where t_c is the current time.

6.10.3. Performance analysis

We evaluated the performance of the proposed protocols $\mathcal{P}_1$, $\mathcal{P}_2$ in terms of computation cost. Table 2 compares protocol $\mathcal{P}_1$ with its lightweight counterparts: the C. Li et al. [1] protocol and the first Chang–Le [12] protocol $\mathcal{P}_{cl}$.

Table 3 compares protocol $\mathcal{P}_2$ with the second Chang–Le protocol $\mathcal{P}_{ecl}$, the He et al. [14] protocol $\mathcal{P}_{he}$ and the Das et al. [13] protocol $\mathcal{P}_{das}$, that are based on elliptic curves. In Tables 2 and 3, t_{mul}, t_h and t_{XOR} denote the times required to perform an elliptic curve point multiplication, a hash operation, and an XOR operation, respectively. Note that t_{XOR} is small compared to t_{mul} and t_h.

Finally, Table 4 compares several security features of the protocols $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, the Chang–Le [12] protocols $\mathcal{P}_{cl}$, $\mathcal{P}_{ecl}$, the He et al. [14] protocol $\mathcal{P}_{he}$, and the Das et al. [13] protocol $\mathcal{P}_{das}$. The main conclusion from Table 4 is that the proposed protocol $\mathcal{P}_3$ offers more security features than the other protocols, and in particular supports user anonymity and forward secrecy. We note that the two variants $\mathcal{P}_{31}$ and $\mathcal{P}_{32}$ of $\mathcal{P}_3$ support different levels of unlinkability: the first uses pseudorandom identifiers while the second uses asymmetric encryption to encrypt identifiers.

7. Conclusions

We analyzed three recently proposed heterogeneous 3-PAKE protocols using the ROR security model and have shown that they are not secure. While there are several approaches to extend PAKE protocols to three-party heterogeneous settings, there are inherent challenges that have to be addressed because of the restricted computation capabilities of sensors and their limited broadcast range. Based on RFID technologies we proposed a novel 3-PAKE protocol $\mathcal{P}_1$ that is designed to be practical, efficient and address the constraints of heterogeneous wireless applications, and then extended it to get protocols $\mathcal{P}_2$ and $\mathcal{P}_3$ that capture additional security features. These protocols are provably secure in the ROR model and offer protection against a range of threats. In particular, $\mathcal{P}_2$ offers offline dictionary attack protection, session key privacy with respect to an honest-but-curious gateway, and forward secrecy, while the protocols $\mathcal{P}_3$ offers anonymity for the user.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This material is based upon work supported in part by the Spanish Ministry of Economy and Competitiveness through the Project TEC2014-54110-R. The first and second authors are supported by the Government of the Canary Islands, Spain through the Grants TESIS2015010102 and TESIS2015010106. The third author's contribution is based upon work supported by the National Science Foundation, USA under Grants DUE 1241525, DGE 1565215, and by the NSA/DOD, USA under Grants H98230-17-1-0419, H98230-17-1-0322, H98230-19-1-0309.

References

[1] C. Li, C. Weng, C. Lee, An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks, Sensors 13 (8) (2013) 9589–9603.
[2] W. Shi, P. Gong, A new user authentication protocol for wireless sensor networks using elliptic curves cryptography, Int. J. Sci. Nature 9 (4) (2013) 730831.

[3] M. Turkanovic, B. Brumen, M. Hölbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Netw. 20 (2014) 96–112.
[4] R. Amin, N. Kumar, G. Biswas, R. Iqbal, V. Chang, A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment, Future Gener. Comput. Syst. 78 (2018) 1005–1019.
[5] X. Li, J. Niu, S. Kumari, F. Wu, A.K. Sangaiah, K.-K.R. Choo, A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments, J. Netw. Comput. Appl. 103 (2018) 194–204.
[6] F. Wu, X. Li, A.K. Sangaiah, L. Xu, S. Kumari, L. Wu, J. Shen, A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks, Future Gener. Comput. Syst. 82 (2018) 727–737.
[7] W. Li, B. Li, Y. Zhao, P. Wang, F. Wei, Cryptanalysis and security enhancement of three authentication schemes in wireless sensor networks, Wirel. Commun. Mobile Comput. 2018 (2018).
[8] M. Burrows, M. Abadi, R.M. Needham, A logic of authentication, ACM Trans. Comput. Syst. 8 (1) (1990) 18–36.
[9] M. Bellare, P. Rogaway, Provably secure session key distribution: the three party case, in: Proceedings 27th Annual ACM Symposium on Theory of Computing, 1995, pp. 57–66.
[10] M. Bellare, D. Pointcheval, P. Rogaway, Authenticated key exchange secure against dictionary attacks, in: Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Proceedings, 2000, pp. 139–155.
[11] M. Abdalla, P. Fouque, D. Pointcheval, Password-based authenticated key exchange in the three-party setting, in: Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Proceedings, 2005, pp. 65–84.
[12] C. Chang, H. Le, A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks, IEEE Trans. Wirel. Commun. 15 (1) (2016) 357–366.
[13] A.K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, X. Huang, Provably secure user authentication and key agreement scheme for wireless sensor networks, Secur. Commun. Netw. 9 (16) (2016) 3670–3687.
[14] J. He, Z. Yang, J. Zhang, W. Liu, C. Liu, On the security of a provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks, Int. J. Distrib. Sens. Netw. 14 (1) (2018).
[15] C. Neuman, S. Hartman, T. Yu, K. Raeburn, The Kerberos Network Authentication Service (V5), RFC 4120, Internet Engineering Task Force, 2005, pp. 1–138.
[16] D.J. Otway, O. Rees, Efficient and timely mutual authentication, Oper. Syst. Rev. 21 (1) (1987) 8–10.
[17] R. Canetti, H. Krawczyk, Analysis of key-exchange protocols and their use for building secure channels, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2001, pp. 453–474.
[18] E. Bresson, O. Chevassut, D. Pointcheval, New security results on encrypted key exchange, in: Public Key Cryptography - PKC 2004, 2004, pp. 145–158.
[19] M. Burmester, J. Munilla, Lightweight RFID authentication with forward and backward security, ACM Trans. Inf. Syst. Secur. 14 (1) (2011) 11:1–11:26.