UNIVERSIDAD DE MURCIA

FACULTAD DE INFORMÁTICA

A Data-centric Security Architecture for the Integration of Constrained Devices into IoT Scenarios

Arquitectura de Seguridad centrada en Datos para la Integración de Dispositivos Restringidos en Escenarios del IoT

D. Salvador Pérez Franco

2020

Universidad de Murcia

Facultad de Informática

Arquitectura de Seguridad centrada en Datos para la Integración de Dispositivos Restringidos en Escenarios del IoT

Tesis Doctoral

Presentada por:
Salvador Pérez Franco

Supervisada por:
Dr. Antonio Fernando Skarmeta Gómez
Dr. José Luis Hernández Ramos

Murcia, Abril de 2020

University of Murcia

Faculty of Computer Science

A Data-centric Security Architecture for the Integration of Constrained Devices into IoT Scenarios

Ph.D. Thesis

Authored by:
Salvador Pérez Franco

Supervised by:
Dr. Antonio Fernando Skarmeta Gómez
Dr. José Luis Hernández Ramos

Murcia, April 2020

A mis Padres, a Ti

Agradecimientos

Como cualquier tesis doctoral, la realización de ésta es fruto de un gran esfuerzo y dedicación. Sin embargo, su consecución no hubiese sido posible sin la ayuda desinteresada de cada una de las personas citadas en las siguientes líneas.

En primer lugar, a mis directores, Antonio y José Luis, por su compromiso y dirección desde el comienzo de esta tesis. Principalmente, agradecer sus revisiones y valiosas sugerencias en esos momentos en los que asomaban las dudas. Ellos han sido un ejemplo de trabajo y dedicación.

A mi familia, por su paciencia y comprensión, por su apoyo incondicional y, en especial, por su cariño durante todo este camino que han compartido conmigo.

Al resto de compañeros del Departamento con los que he colaborado para el desarrollo de la investigación, en particular, Dan, Sara, Rafa, Jorge, Ramón, Jesús y José Santa.

Por último, me gustaría recordar también al grupo de I+D+i en el que participé durante mi estancia en Italia, por acogerme como uno más del equipo y apoyar los inicios de esta tesis doctoral.

"Hazlo o no lo hagas, pero no lo intentes"

Contents

Capítulo 1

Resumen

1.1. Motivación y Objetivos

La evolución de Internet está impulsando la expansión del paradigma del *Internet de las Cosas* (IoT) [4], transformando la forma en que vivimos. El término IoT fue introducido por Kevin Ashton en 1999 [2] para denotar un ecosistema constituido por un elevado número de dispositivos heterogéneos interconectados (*cosas*) que recopilan, intercambian y procesan datos relacionados con su entorno. Hoy en día, el paradigma IoT está teniendo un fuerte impacto en la sociedad, alentando la aparición de nuevos escenarios que prometen mejorar nuestra calidad de vida. En este sentido, un reciente informe realizado por la compañía *IoT Analytics* pronostica que el número de dispositivos conectados a Internet ascienda de los 21.200 millones actuales a 34.200 en el año 2025 [35], como se muestra en la Figura 1.1.

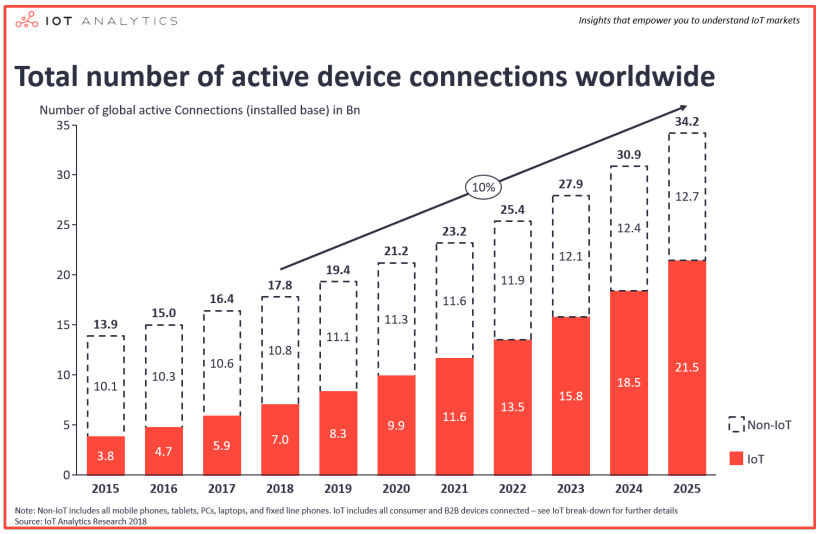

Figura 1.1: Estimación del número de dispositivos conectados a Internet[1]

El IoT se fundamenta principalmente en el intercambio masivo de grandes volúmenes de información proveniente de diferentes dispositivos que actúan como fuentes de datos. Por ello, es considerado como el principal impulsor de la era del *Big Data* [14], donde la información es un activo clave de gran valor económico y social [42]. Así, la integración del IoT con técnicas de *Big Data* posibilita el

[1] `https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/`

desarrollo de nuevos servicios que hacen uso de los datos compartidos para inferir nuevo conocimiento y, en consecuencia, tomar decisiones más eficientes en ámbitos como el transporte o la sanidad. Sin embargo, el despliegue de estos servicios aún presenta ciertos desafíos relacionados con el tratamiento de tales datos, especialmente en el caso de información de carácter personal, donde un uso inadecuado podría vulnerar la privacidad de las personas. De hecho, el estudio realizado por el organismo *Mobile Ecosystem Forum* (MEF) [53] constató que la pérdida de privacidad y la seguridad son las principales preocuaciones de la sociedad derivadas de la expansión del IoT, como refleja la Figura 1.2.

Figura 1.2: Principales preocupaciones de la sociedad relacionadas con el IoT[2]

En este sentido, la Unión Europea (UE) ha presentado diferentes instrumentos legales, como son la directiva *"Network and Information Security"* (NIS)[3], la ya implantada *"General Data Protection Regulation"* (GDPR)[4] y la reciente regulación *"Cybersecurity Act"*[5], con el fin de abordar los problemas de seguridad y privacidad en una sociedad cada vez más dependiente de la tecnología. Además de estas iniciativas legislativas, existen otros esfuerzos adicionales que se centran en el contexto IoT. En particular, la Comisión Europea (CE) presentó el dictamen *"Opinion 8/2014 on the Recent Developments on the Internet of Things"*[6], que describe un conjunto de desafíos de seguridad relacionados con la protección de datos en entornos del IoT. Adicionalmente, propone una serie de recomendaciones para abordar tales desafios, y la adopción del enfoque *Privacy by Design and Default* [43] como requisito fundamental para la preservación de la privacidad de las personas. De manera similar, la *European Union Agency For Network And Information Security* (ENISA) recoge en el informe *"Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures"*[7] información detallada sobre las amenazas de seguridad más relevantes del IoT, definiendo además un conjunto de buenas prácticas para solventar o, al menos, mitigar tales riesgos. Estos esfuerzos e iniciativas de la UE, junto con otros similares como la *Alliance for Internet of Things Innovation* (AIOTI)[8] o el *International Energy Research Centre* (IERC)[9], son un fiel reflejo de la importancia que Europa atribuye a la seguridad y privacidad en el contexto IoT.

La materialización de esfuerzos regulativos y legales sobre escenarios del IoT exige la aplicación de diferentes soluciones complementarias que permitan abordar las preocupaciones de seguridad y privacidad identificadas en estos ecosistemas de compartición de datos. Solo así se logrará incrementar la confianza de las personas y fomentar el despliegue de los escenarios IoT a gran escala. En este sentido, las soluciones de seguridad adoptadas deben adecuarse a las particularidades inherentes de tales escenarios, en particular:

- **Heterogeneidad del IoT**. Los escenarios del IoT representan entornos basados en la compartición masiva de información, que es habilitada a través de la integración y coexistencia de una

[2] https://mobileecosystemforum.com/2016/04/07/trust-related-concerns-hamper-consumer-adoption-iot/
[3] https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[4] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[5] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[6] https://www.pdpjournals.com/docs/88440.pdf
[7] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport
[8] https://aioti.eu/
[9] http://www.ierc.ie/

amplia variedad de tecnologías en las diferentes capas de la pila de protocolos IoT [57]. Así, dado el alto grado de heterogeneidad presentado por estos escenarios, se precisa la aplicación de soluciones de seguridad en los niveles superiores para la protección del intercambio de datos, de manera que tales soluciones sean independientes de las tecnologías y protocolos en las capas subyacentes.

- **Restricciones de recursos**. Gran parte de los dispositivos desplegados en un escenario IoT presentan limitaciones en términos de capacidad de computación, memoria y consumo de energía [11]. Adicionalmente, las comunicaciones entre tales dispositivos suelen realizarse a través de redes con bajo ancho de banda, donde la *unidad de transmisión máxima* (MTU) es limitada (p.ej., en IEEE 802.15.4 [54], la MTU es de 127 bytes). Estas restricciones dificultan el uso de primitivas criptográficas fuertemente demandantes en recursos. Por tanto, se requieren soluciones de seguridad adaptadas a entornos restringidos, es decir, soluciones ligeras y eficientes que permitan reducir el consumo de recursos y ancho de banda de red.

- **Presencia de entidades intermedias**. La integración de ciertas entidades intermedias en las comunicaciones (p.ej., proxies) tiene por objetivo paliar los problemas de rendimiento derivados de las limitaciones de los dispositivos y redes en escenarios del IoT. Si bien los proxies permiten mejorar la eficiencia y escalabilidad, su presencia puede convertirse en un incoveniente cuando se requiera asegurar la protección de los datos desde el emisor al receptor (seguridad extremo-a-extremo) [26]. Así, deben considerarse soluciones capaces de garantizar la protección de los datos extremo-a-extremo, incluso en presencia de entidades intermedias.

- **Comunicaciones en grupo**. El modelo de comunicación uno-a-muchos permite que un emisor comparta datos con un conjunto de receptores mediante el envío de un único mensaje, reduciendo así la sobrecarga de red y el consumo de recursos. En este sentido, el *patrón publicación/subscripción* es ampliamente utilizado en el contexto IoT para la realización de las comunicaciones en grupo, como en [68, 73]. Sin embargo, dicho modelo de comunicación complica la aplicacion de enfoques de seguridad concebidos para comunicaciones uno-a-uno, como la tradicional criptografía simétrica o asimétrica. Por tanto, se requieren soluciones de seguridad que ofrezcan un alto grado de flexibilidad, de manera que puedan ser aplicables también para la protección de comunicaciones uno-a-muchos.

De acuerdo con las particularidades mencionadas, el conjunto de soluciones adoptadas tiene por objetivo la gestión de la seguridad en escenarios del IoT, de manera que se garantice la protección de la información durante todo su ciclo de vida en estos entornos de compartición de datos. Adicionalmente, tales soluciones deben basarse en estándares existentes, así como en recientes enfoques propuestos por grupos de estandarización y organizaciones de relevancia que presentan especial interés en aspectos de seguridad, como el *Internet Engineering Task Force* (IETF)[10] o el *European Telecommunications Standards Institute* (ETSI)[11].

Así, los desafíos y requisitos de seguridad y privacidad presentados anteriormente han sido los principales impulsores del desarrollo de esta tesis, motivando el desarrollo de una **Arquitectura de Seguridad centrada en Datos para la Integración de Dispositivos Restringidos en Escenarios del IoT**. En consecuencia, se establecieron los siguientes objetivos:

- Obj1. Análisis de los requisitos de seguridad y privacidad en escenarios del IoT, considerando las particularidades previamente mencionadas de estos entornos de compartición de datos.

- Obj2. Análisis de las recomendaciones, estándares y propuestas existentes en la literatura para asegurar la protección de los datos en escenarios del IoT, identificando sus limitaciones y restricciones.

[10] `https://www.ietf.org/topics/security/`
[11] `https://www.etsi.org/committee/cyber`

- Obj3. Diseño y desarrollo de un mecanismo que habilita el intercambio seguro de datos entre grupos de entidades en escenarios del IoT.
- Obj4. Diseño y desarrollo de un mecanismo que habilita el establecimiento de asociaciones de seguridad extremo-a-extremo en escenarios del IoT.
- Obj5. Despliegue y evaluación de las soluciones de seguridad desarrolladas con el objetivo de demostrar su viabilidad en escenarios del IoT.
- Obj6. Propuesta de una arquitectura de seguridad para garantizar la protección de datos durante todo su ciclo de vida en escenarios del IoT.

En este sentido, el análisis de requisitos de seguridad y privacidad en diferentes escenarios del IoT permitieron identificar la necesidad de soluciones de protección de datos eficientes y efectivas para estos entornos de compartición de datos. Además, se constató que muchos de los estándares y propuestas existentes no se ajustaban adecuadamente a las particularidades inherentes a estos escenarios, como son la heterogeneidad de tecnologías, las restricciones de recursos de los dispositivos, la presencia de proxies y las comunicaciones uno-a-muchos. Así, de acuerdo a las conclusiones derivadas de este análisis, surgió la necesidad de diseñar una arquitectura que tiene por objetivo garantizar la seguridad de la información durante todo su ciclo de vida en el contexto IoT. Así, la arquitectura propuesta en esta tesis engloba diferentes soluciones de la capa de aplicación cuya combinación asegura la protección de los datos en escenarios del IoT. En particular, la arquitectura integra un enfoque criptográfico ligero, flexible y escalable basado en el esquema de cifrado *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) [9], con el fin de habilitar la compartición segura de información entre grupos de entidades. Adicionalmente, dicho enfoque es extendido con un mecanismo de intercambio de claves basado en un reciente esfuerzo de estandarización del IETF conocido como *Ephemeral Diffie-Hellman Over COSE* (EDHOC) [27], que permite el establecimiento de asociaciones de seguridad en estos escenarios restringidos. Cabe resaltar que este mecanismo considera la realización de una fase previa de bootstrapping, en la que las diferentes entidades obtienen sus correspondientes credenciales y claves para unirse a la red de manera segura. En este sentido, se ha considerado el servicio de boostrapping *Low-Overhead CoAP-EAP* (LO-CoAP-EAP) [21] debido a que fue específicamente diseñado para el contexto IoT. Finalmente, se propuso la realización de un análisis de rendimiento de las diferentes soluciones integradas en la arquitectura, para demostrar su viabilidad y ventajas frente a otros enfoques planteados actualmente para escenarios del IoT.

Los objetivos anteriormente definidos impulsaron el desarrollo de esta tesis doctoral, y su consecución derivó en el conjunto de resultados presentado es la siguiente sección.

1.2. Resultados

En esta sección se detalla el conjunto de trabajos desarrollados para la consecución de los objetivos que fueron planteados al comienzo de la tesis doctoral. Además, estos trabajos han sido presentados en forma de publicaciones en conferencias y revistas de alto impacto, las cuales recogen gran parte de los resultados logrados durante la realización de esta tesis, como se muestra en la Tabla 1.2.

En concreto, se llevó a cabo la identificación de los principales desafíos de seguridad y privacidad derivados de la realización de los escenarios del IoT, tomando como base trabajos de investigación previos [72, 78]. Del mismo modo, se examinó el conjunto de contramedidas propuesto en [58] con el fin de solventar, o al menos mitigar, tales desafíos. Cabe destacar que las conclusiones derivadas de este trabajo fueron incluidas como parte del proyecto europeo Horizon H2020 ARMOUR[12], el cual tenía por objetivo proporcionar soluciones de seguridad testadas y certificadas para fomentar así el despliegue a gran escala del IoT [91].

[12] `https://www.armour-project.eu/`

Nro.	Resultado	Objetivo	Publicación
1	Identificación de los principales desafíos de seguridad y privacidad en escenarios del IoT, así como estudio de soluciones potenciales que permitan abordar, al menos de manera parcial, tales desafíos	Obj1, Obj2	[91], [87], [90], [88], [84]
2	Diseño e implementación de una solución flexible que permite la compartición segura de datos entre grupos de entidades en escenarios del IoT	Obj3	[84]
3	Diseño e implementación de un enfoque ligero de la solución para la compartición segura de datos en grupo previamente desarrollada, con el fin de mejorar la eficiencia y escalabilidad en escenarios del IoT	Obj3	[89], [92], [88]
4	Diseño e implementación de una solución de intercambio de claves ligera que permite el establecimiento de asociaciones de seguridad extremo-a-extremo en escenarios IoT	Obj4	[90], [94], [93]
5	Diseño e implementación de una versión reducida de la solución de intercambio de claves anteriormente implementada, con el fin de reducir tanto el consumo de recursos en dispositivos restringidos como la sobrecarga de red en escenarios del IoT	Obj4	[90]
6	Diseño e implementación de extensiones a tecnologías de bootstrapping para el IoT, con el objetivo de establecer el material criptográfico requerido por las soluciones de intercambio de claves desarrolladas	Obj4	[87]
7	Evaluación de las soluciones propuestas mediante su instanciación en diferentes escenarios del IoT, para verificar su viabilidad y adecuación en estos entornos restringidos de compartición de datos	Obj5	[90], [87], [88], [84], [85], [86]
8	Integración de las soluciones propuestas para llevar a cabo el diseño de una arquitectura destinada a proteger los datos compartidos durante todo su ciclo de vida en escenarios del IoT	Obj6	[90], [87], [88], [84]

Tabla 1.1: Resultados alcanzados durante la realización de la tesis

Los desafíos y contramedidas identificados anteriormente fueron utilizados como punto de partida para el diseño de un enfoque de seguridad basado en el esquema de cifrado CP-ABE, cuya arquitectura es presentada en [84]. Este enfoque se fundamenta en el concepto de *bubble*, que representa un grupo de entidades compartiendo información bajo ciertas condiciones. Así, para llevar a cabo la diseminación segura de datos dentro de una *bubble* en particular, se establece el uso de CP-ABE, de manera que las entidades mantienen el control sobre cómo se comparte su información. Posteriormente, se diseñó e implementó un nuevo mecanismo más ligero de este esquema de cifrado llamado SymCpAbe [84,88,89,92]. Para ello, se propuso la combinación de CP-ABE con la criptografía de clave

simétrica, mejorando la eficiencia y escalabilidad mientras se mantiene la flexibilidad y expresividad del esquema CP-ABE original. Asimismo, estas soluciones para la compartición segura de datos en grupo fueron desplegadas y evaluadas en escenarios reales del IoT, donde un gran volumen de datos es compartido entre diferentes entidades heterogéneas, desde un sensor con restricciones de recursos hasta un servicio de alto nivel basado en datos. Para ello, se hizo uso de diferentes componentes de la plataforma FIWARE[13] con el fin de favorecer la compatibilidad e interoperabilidad con otros despliegues IoT existentes. Dicha evaluación permitió demostrar la aplicabilidad e idoneidad de la solución propuesta en estos entornos restringidos de compartición de datos. Asimismo, resaltar que los resultados obtenidos fueron presentados en el ámbito de dos proyectos europeos, en concreto, FP7 SocIoTal[14] y CHIST-ERA Use-IT[15].

Adicionalmente, se consideró la integración de un mecanismo de intercambio de claves complementario al enfoque anterior. En particular, este mecanismo permite a las entidades establecer asociaciones de seguridad, que confirman la legitimidad de las entidades para participar en el proceso de compartición de datos en grupo. Sin embargo, la presencia habitual de proxies en el contexto IoT se convirtió en un nuevo desafío a superar para garantizar el establecimiento de dichas asociaciones de seguridad entre las entidades implicadas. Si bien los proxies permiten mejorar la escalabilidad y eficiencia en las comunicaciones, su presencia también tiene su parte negativa: rompen el modelo de seguridad extremo-a-extremo. Para abordar este desafío, se llevó a cabo el diseño y desarrollo de un mecanismo de intercambio de claves ligero basado en EDHOC, cuyos mensajes son encapsulados y transportados a través del protocolo de comunicación *Constrained Application Protocol* (CoAP) [81]. Así, mediante este enfoque, se habilita el establecimiento de asociaciones de seguridad extremo-a-extremo entre dos entidades en escenarios del IoT, incluso en presencia de otras entidades intermedias, como proxies [90]. Posteriormente, dicha solución de intercambio de claves fue propuesta en [93, 94] como un proceso alternativo a la configuración manual para la distribución y actualización de claves de sesión en arquitecturas *Long Range Wide Area Network* (LoRaWAN) [69]. Paralelamente, se desarrolló una versión compacta de este mecanimo (CompactEDHOC), en la que se suprime la negociación de los parámetros de seguridad requeridos por el enfoque original. En su lugar, estos parámetros de seguridad son almacenados en una entidad *resource directory* [82], reduciendo aún más el consumo de recursos en dispositivos restringidos y la sobrecarga de red. Adicionalmente, se realizó una evaluación de rendimiento de ambas soluciones basadas en EDHOC, con el objetivo de demostrar sus ventajas frente a otros enfoques similares que son ampliamente utilizadas en la actualidad para el contexto IoT, como el *handshake* del protocolo *Datagram Transport Layer Security* (DTLS).

Sin embargo, la aplicación de estos mecanismos de intercambio de claves basados en EDHOC evidenció la falta de una fase anterior en la que llevar a cabo el establecimiento de las credenciales de autenticación requeridas para su ejecución. Esto motivó el trabajo presentado en [87], donde se propone la integración de tecnologías de bootstrapping [5] para la derivación y cálculo de tales credenciales a partir de cierto material criptográfico generado en dicho proceso de boostrapping. Adicionalmente, con el fin de evaluar el nivel de seguridad ofrecido por estas soluciones de intercambio de claves, en [85] se propuso el uso de un enfoque de testing automatizado que permite simplificar tal proceso de evaluación. Así, tomando como punto de partida esta publicación, en [86] se definió una metodología basada en el enfoque *Model-Based Testing* (MBT) [7] para evaluar diferentes propiedades de seguridad de los mecanismos basados en EDHOC propuestos. En este sentido, es importante hacer notar que la información obtenida a partir de esta evaluación fue utilizada para detectar y resolver ciertos errores de implementación.

El conjunto de estas soluciones ha impulsado el diseño de la arquitectura de seguridad planteada en esta tesis, con el fin de garantizar la protección de los datos compartidos en escenarios del IoT. En este sentido, los resultados presentados en esta sección proporciona una visión general del plan de trabajo seguido para la consecución de los objetivos previamente establecidos. Esta visión es posteriormente ampliada en el Capítulo 3, donde se desarrollan de manera detallada las soluciones propuestas.

[13] `https://www.fiware.org/`
[14] `https://cordis.europa.eu/project/id/609112`
[15] `http://useit.eu.org/`

1.3. Conclusiones y Trabajos Futuros

La expansión del IoT se está viendo impulsada con la llegada de recientes tecnologías de comunicación, como el 5G, que posibilitan el intercambio masivo de información entre un elevado número de dispositivos heterogéneos interconectados. Esta evolución de Internet está alentando la aparición de nuevos escenarios, los cuales representan ecosistemas donde diferentes dispositivos físicos desplegados detectan y comparten datos sobre su entorno con el propósito de transformar y mejorar servicios cotidianos, como los sistemas de transporte o sanidad. Sin embargo, la realización de este paradigma de *sociedad basada en datos* [61] presenta importantes desafíos de seguridad relacionados con el tratamiento de información de carácter personal, pudiéndose vulnerar la privacidad de los participantes. En consecuencia, la protección de los datos es considerada como un aspecto clave para incrementar la confianza de las personas y lograr el desarrollo de los escenarios del IoT a gran escala.

En este sentido, determinados organismos de estandarización han llevado a cabo análisis sobre los problemas de seguridad y privacidad derivados de la aplicación del IoT, proporcionando recomendaciones sobre cómo abordarlos y lograr así ecosistemas seguros y confiables. Si bien tales recomendaciones no son jurídicamente vinculantes, la recientemente implantada GDPR tiene por objetivo regular, a nivel legislativo, la protección de información personal, así como la forma en que las organizaciones la procesan, almacenan y eliminan. Sin embargo, la aplicación de enfoques de seguridad que aseguren el cumplimiento de esta regulación en escenarios del IoT no es trivial, dadas las particularidades inherentes a estos ecosistemas de compartición de datos.

De acuerdo a tales particularidades, esta tesis doctoral presenta una Arquitectura de Seguridad centrada en Datos para la Integración de Dispositivos Restringidos en Escenarios del IoT. El desarrollo de esta arquitectura se fundamenta en un análisis realizado sobre los problemas de seguridad y privacidad en el contexto IoT. Las conclusiones derivadas de dicho análisis constataron la necesidad de nuevos enfoques destinados a hacer frente a los desafíos de seguridad y privacidad detectados en estos entornos de compartición de datos restringidos, más allá de la típica criptografía de clave simétrica y de clave pública. Así, la arquitectura propuesta integra diferentes soluciones ligeras, flexibles y escalables adaptadas a las particularidades de los escenarios del IoT, permitiendo garantizar la seguridad de los datos durante todo su ciclo de vida.

En particular, se ha diseñado e implementado un enfoque basado en el esquema de cifrado CP-ABE, que permite la compartición segura de datos dentro de un grupo específico de entidades definido como *bubble*. Adicionalmente, se ha presentado una nueva versión híbrida de este enfoque llamada SymCpAbe, que combina la criptografía simétrica para el cifrado de la información, con la criptografía basada en atributos para la diseminación de datos en grupo. De esta forma, se logra mejorar la eficiencia y escalabilidad de la versión original. Asimismo, la realización de los enfoques propuestos se basa en diferentes componentes de la plataforma FIWARE, facilitando su compatibilidad e interoperabilidad con otros despliegues IoT existentes. Con el fin de verificar su adecuación en escenarios del IoT, este enfoque fue comparado con el esquema CP-ABE sobre un escenario real de *smart building*. Los resultados obtenidos demostraron las ventajas de la solución propuesta, logrando un equilibrio entre eficiencia, flexibilidad y escalabilidad.

Del mismo modo, se ha llevado a cabo el diseño e implementación de una solución basada en el protocolo de intercambio de claves EDHOC, con el objetivo de permitir el establecimiento de asociaciones de seguridad extremo-a-extremo entre pares de entidades en escenarios del IoT. Para ello, el enfoque propuesto considera el transporte de mensajes EDHOC sobre el protocolo de comunicación CoAP, que es la solución sugerida por el propio draft de este enfoque de intercambio de claves. Cabe señalar que, debido a su eficiencia y ligereza, esta solución ha sido integrada en una arquitectura LoRaWAN para cubrir la falta de un mecanismo de actualización de claves de sesión en este tipo de redes. En paralelo, se ha diseñado y desarrollado una versión más reducida del enfoque propuesto (CompactEDHOC), que se fundamenta en la extracción de los parametros de seguridad y su almacenamiento previo en una entidad *resource directory*. Los resultados de evaluación de ambos enfoques han evidenciado las ventajas de estas propuestas frente a otras soluciones de intercambio de claves actuales, como el protocolo de *handshake* de DTLS.

Sin embargo, estas soluciones basados en EDHOC requieren de credenciales pre-establecidas que habiliten la autenticación durante su ejecución. En este sentido, el draft de EDHOC no aborda tal aspecto, por lo que resulta necesario considerar otros enfoques de seguridad complementarios que permitan establecer estas credeciales. Para tal fin, se ha adoptado el servicio de boostrapping LO-CoAP-EAP, debido a que había sido diseñado y testado en escenarios IoT. En particular, se realizó una extensión de LO-CoAP-EAP que habilita la derivación de las credenciales de autenticación requeridas por las soluciones propuestas, es decir, una clave simétrica compartida o los correspondientes pares de claves privada/pública. Finalmente, la integración de LO-CoAP-EAP con los enfoques basados en EDHOC fue evaluada sobre un caso de uso IoT real, demostrando su adecuación en estos escenarios restringidos.

Las soluciones de seguridad anteriormente presentadas posibilitaron el cumplimiento de los objetivos definidos al comienzo de esta tesis doctoral. Así, la combinación de tales soluciones dio como resultado una arquitectura de seguridad que, considerando las particularidades de los escenarios del IoT, asegura la protección de la información en estos entornos de compartición de datos. Adicionalmente, esta arquitectura se presenta como un excelente punto de partida para la realización de futuros trabajos relacionados con aspectos de seguridad y privacidad en el contexto IoT.

En este sentido, se propone el diseño y desarrollo de mecanismos que permitan la distribución del cifrado y descifrado CP-ABE en diferentes nodos *edge*, los cuales trabajan de manera cooperativa para la realización de dichas operaciones criptográficas. De esta forma, se consigue reducir aún más el consumo de recursos, lo que permite mejorar el rendimiento del enfoque propuesto para la compartición segura de datos en grupo. Adicionalmente, se propone extender este enfoque mediante la inclusión de esquemas de firma basados en identidad [33] con el fin de proteger la integridad de la información compartida. Del mismo modo, se plantea examinar los esfuerzos de investigación realizados por el grupo de trabajo *Authentication and Authorization for Constrained Environments* (ACE)[16], para la incorporación de modelos de autorización que permitan abordar aspectos relacionados con el control de acceso en escenarios del IoT [29].

Por otra parte, se plantea revisar el desarrollo de los enfoques basados en EDHOC, así como llevar a cabo su actualización a partir de la última especificación de dicho protocolo. Asimismo, se propone la extensión de estos enfoques mediante el desarrollo de un mecanismo de reinicio que permita mejorar el proceso de refresco de asociaciones de seguridad previamente establecidas. Ambas modificaciones prometen incrementar el rendimiento de los enfoques de intercambio de claves propuestos en términos de eficiencia y optimización del uso de recursos. Finalmente, otra prometedora línea de investigación planteada es la integración del protocolo *Object Security for Constrained RESTful Environments* (OSCORE) [28], que ha sido recientemente estandarizado. De esta forma, se logra enriquecer aún más la arquitectura presentada en esta tesis y, por consiguiente, aprovechar todas las ventajas que ofrecen los enfoques de seguridad de la capa de aplicación en el contexto IoT.

1.4. Estructura de la Tesis

Esta tesis doctoral está organizada siguiendo el modelo de compendio de publicaciones y la mención de doctorado internacional reconocidos por la normativa vigente. Por consiguiente, el Capítulo 1 presenta un resumen en castellano en el que se describe la motivación de la investigación desarrollada, así como los objetivos que se establecieron al inicio de dicha investigación. Además, se ofrece una visión general del conjunto de resultados logrados a la conclusión de la tesis y su vinculación con los objetivos previamente definidos. De manera similar, el Capítulo 2 ofrece una versión en inglés del resumen presentado en el capítulo anterior. Adicionalmente. el Capítulo 3 profundiza en los principales desafíos que motivaron el desarrollo de esta tesis. Además, se describe la arquitectura propuesta para superar tales desafíos, detallando los diferentes mecanismos de seguridad desarrollados que la integran. Por su parte, el Capítulo 4 incluye las cuatro publicaciones que componen esta tesis docotoral, en particular:

[16] `https://datatracker.ietf.org/wg/ace/about/`

- *Protecting Personal Data in IoT Platform Scenarios Through Encryption-Based Selective Disclosure*. Esta publicación señala la confianza de los usuarios como aspecto clave para conseguir el despliegue de los escenarios del IoT en la sociedad. En consecuencia, se define el concepto de *bubble*, que representa a un grupo de de entidades donde la información es compartida bajo ciertas restricciones de seguridad, siguiendo las preferencias de los propietarios de datos. La materialización de este concepto se basa en el uso de la criptografía basada en atributos, de manera que la información compartida dentro de una *bubble* es protegida mediante una política de acceso CP-ABE. Asimismos, una clave utilizada para acceder a la información está asociada al conjunto de atributos de la entidad correspondiente. Adicionalmente, este enfoque es evaluado sobre un escenario real de *smart building* a través del uso de componentes de la plataforma FIWARE. Los resultados obtenidos de la evaluación demuestran la aplicabilidad y beneficios de este enfoque en escenarios del IoT.
- *A Lightweight and Flexible Encryption Scheme to Protect Sensitive Data in Smart Building Scenarios*. Siguiendo la línea de investigación del trabajo anterior, esta publicación destaca la gran cantidad de información que se comparte en el contexto IoT. Esta información posibilita la realización de nuevos servicios basado en datos, los cuales están destinados a mejorar la calidad de vida de las personas. Sin embargo, parte de esta información es de carácter sensible, lo que podría dañar la privacidad de los individuos implicados si no se adoptan las acciones apropiadas. Así, se resalta la necesidad de soluciones de seguridad que permitan a los propietarios de los datos establecer qué requisitos deben cumplir los servicios interesados en acceder a sus datos. Con el fin de afrontar este desafío, se presenta un enfoque de cifrado ligero y escalable llamado SymCpAbe, que combina la eficiencia de la criptografía de clave simétrica y la flexibilidad del esquema criptográfico CP-ABE. Además, el enfoque propuesto es evaluado en un escenario real de *smart building*, y los resultados revelan sus ventajas frente al esquema CP-ABE original para la compartición segura de datos en grupo en escenarios del IoT.
- *Application Layer Key Establishment for End-to-End Security in IoT*. Esta publicación se centra en la necesidad de soluciones que habiliten la protección de datos entre dos puntos finales en el contexto IoT, incluso en presencia de entidades intermedias (p.ej., proxies). Para cubrir esta necesidad, se presenta una primera solución basada en el protocolo EDHOC, que permite el establecimiento de asociaciones de seguridad entre pares en escenarios restringidos. Adicionalmente, se propone una versión compacta del enfoque anterior llamada CompactEDHOC. En esta segunda solución, los parámetros de seguridad son almacenados previamente en un componente *resource directory*, por lo que su negociación es eliminada del enfoque original. Así, esta optimización permite reducir aún más la sobrecarga de red y el consumo de recursos de los dispositivos, mejorando así el rendimiento para el establecimiento de asociaciones de seguridad de extremo-a-extremo en escenarios del IoT.
- *Architecture of Security Association Establishment Based on Bootstrapping Technologies for Enabling Secure IoT Infrastructures*. Esta publicación revela la falta de un mecanismo previo que habilite el establecimiento de credenciales de autenticación requerido por las soluciones presentadas en el trabajo anterior. Para abordar tal carencia, se considera la integración de tecnologías ligeras de bootstrapping en una fase previa, en particular, el servicio LO-CoAP-EAP. De esta manera, cuando el proceso de bootstrapping concluye, los puntos finales poseen cierto material criptográfico que les permite derivar sus credenciales de autenticación. Así, estas entidades son capaces de ejecutar la correspondiente solución basada en EDHOC para el establecimiento y actualización de asociaciones de seguridad extremo-a-extremo. Además, este enfoque es desplegado y evaluado sobre un escenario real de *smart building*, donde los resultados obtenidos revelan las ventajas de su aplicación en el contexto del IoT.

Finalmente, el Capítulo 5 recoge la bibliografía relacionada con este documento, en particular, las publicaciones referenciadas (Sección 5.1) y las publicaciones realizadas durante el desarrollo de esta tesis doctoral (Sección 5.2).

Chapter 2

Abstract

2.1. Motivation y Objectives

The evolution of the Internet is driving the expansion of the *Internet of Things* (IoT) paradigm [4], transforming our everyday life. The term IoT was introduced by Kevin Ashton in 1999 [2] to denote an ecosystem consisting of a high number of interconnected heterogeneous devices (*things*) that collect, exchange, and process data related to their environment. Nowadays, the IoT paradigm is having a strong impact on the society, encouraging the emergence of new scenarios that promise to improve our quality of life. In this sense, a recent report presented by the *IoT Analytics* enterprise predicts that the number of devices connected to the Internet will rise from the current 21.2 billion to 34.2 in the year 2025 [35], as shown in Figure 2.1.

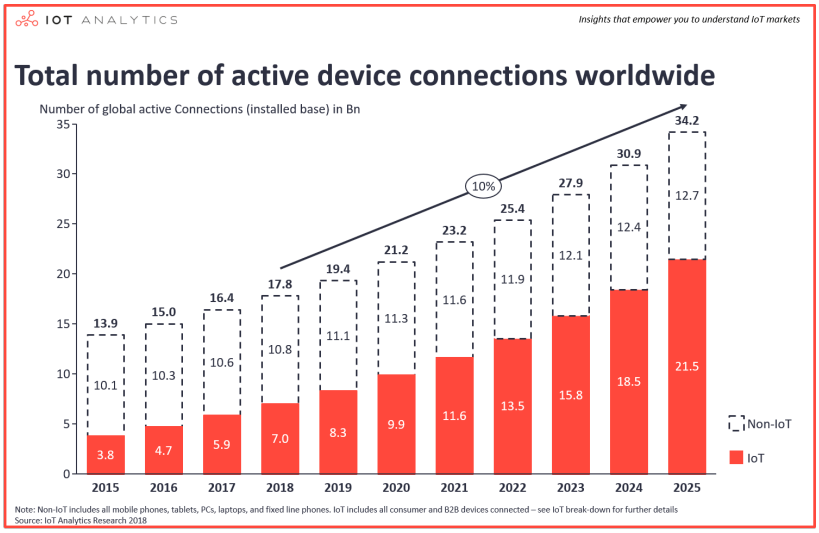

Figure 2.1: Estimation of the number of devices connected to the Internet[1]

The IoT is mainly based on the massive exchange of large volumes of information coming from different devices that act as data sources. For this reason, such paradigm is considered as the main driver of the *Big Data* era [14], where information is a key asset with a great economic and social value [42]. Thus, the integration of the IoT with *Big Data* techniques enables the development of new services that make use of shared data to infer new knowledge and make more efficient decisions

[1] `https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/`

accordingly in diverse areas such as transport or healthcare. Nevertheless, the deployment of these services still presents certain challenges related to the treatment of such data, especially in case of personal information, where an improper use could violate people's privacy. In fact, the study presented by the *Mobile Ecosystem Forum* (MEF) organization [53] determined that privacy loss and security are the main society's concerns derived from the IoT expansion, as reflected in Figure 2.2.

Figure 2.2: Main society's concerns related to the IoT[2]

In this sense, the European Union (EU) has presented different legal instruments, such as the *"Network and Information Security"* (NIS) directive[3], the already implemented *"General Data Protection Regulation"* (GDPR)[4] and the recent *"Cybersecurity Act"* regulation[5], in order to address security and privacy issues in an increasingly technology-dependent society. Along with these legislative initiatives, there are other additional efforts that focus on the IoT context. Specifically, the European Commission (EC) presented the *"Opinion 8/2014 on the Recent Developments on the Internet of Things"*[6], which describes a set of security challenges related to data protection in IoT environments. Furthermore, this opinion proposes a series of recommendations to overcome such challenges, as well as the adoption of the *Privacy by Design and Default* approach [43] as a core requirement for people's privacy preservation. Similarly, the *European Union Agency For Network And Information Security* (ENISA) includes in the *"Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures"* report[7] detailed information on the most relevant IoT security threats, also defining a set of good practices to solve or, at least, mitigate these risks. These EU efforts and initiatives, along with similar ones such as the *Alliance for Internet of Things Innovation* (AIOTI)[8] or the *International Energy Research Center* (IERC)[9], reveal the importance that Europe gives to security and privacy in the IoT context.

The implementation of regulatory and legals efforts on IoT scenarios demands to apply different complementary solutions that allow to address the security and privacy concerns identified in these data sharing ecosystems. It will be possible to increase people's confidence and encourage the deployment of IoT scenarios on a broad scale. In this sense, the adopted security solutions must be adapted to the inherent particularities of such scenarios, in particular:

- **IoT heterogeneity**. IoT scenarios represent environments based on the massive information sharing, which is enabled through the integration and coexistence of a wide variety of technologies at different layers of the IoT protocol stack [57]. Thus, given the high degree of heterogeneity presented by these scenarios, it is required the application of security solutions at the higher levels in order to protect data exchange, so that such solutions are independent of technologies and protocols at the underlying layers.

[2] https://mobileecosystemforum.com/2016/04/07/trust-related-concerns-hamper-consumer-adoption-iot/
[3] https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[4] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[5] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[6] https://www.pdpjournals.com/docs/88440.pdf
[7] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport
[8] https://aioti.eu/
[9] http://www.ierc.ie/

- **Resource constraints**. Most devices deployed in an IoT scenario present limitations in terms of computing capability, memory and power consumption [11]. Additionally, communications between such devices are typically carried out over low bandwidth networks, where the *maximum transmission unit* (MTU) is limited (e.g., in IEEE 802.15.4 [54], the MTU is 127 bytes). These constraints hinder the use of heavily resource-demanding cryptographic primitives. Therefore, security solutions adapted to constrained environments are required, that is, lightweight and efficient solutions that reduce both resource consumption and network bandwidth.

- **Presence of intermediate entities**. The integration of certain intermediate entities in communications (e.g., proxies) is aimed to alleviate performance issues derived from device and network limitations in IoT scenarios. While proxies allow to improve efficiency and scalability, their presence can become an inconvenience when data protection from the sender to the receiver is needed (end-to-end security) [26]. Thus, there is a need to consider solutions capable of ensuring end-to-end data protection, even in presence of intermediate entities.

- **Group communications**. The one-to-many communication model allows a sender to share data with a set of receivers by using a single message, thus reducing both network overhead and resource consumption. In this sense, the *publish/subscribe pattern* is widely employed in the IoT context for group communications, as in [68, 73]. Nevertheless, this communication model hinders the application of security approaches designed for one-to-one communications, such as traditional symmetric or asymmetric cryptography. Therefore, security solutions offering a high degree of flexibility are required, so that they can also be applied to protect one-to-many communications.

According to the mentioned particularities, the set of adopted solutions aims to control security in IoT scenarios, so that it is guaranteed the protection of information throughout its whole lifecycle in such data sharing environments. Additionally, these solutions should be based on existing standards, as well as recent approaches proposed by standardization groups and relevant organizations specially interested in security aspects, such as the *Internet Engineering Task Force* (IETF)[10] or the *European Telecommunications Standards Institute* (ETSI)[11].

Thus, the security and privacy challenges and requirements presented above have been the main drivers of the development of this thesis, motivating the development of a **A Data-centric Security Architecture for the Integration of Constrained Devices into IoT Scenarios**. Consequently, the following objectives are established:

- Obj1. Analysis of the security and privacy requirements in IoT scenarios, considering the previously mentioned particularities of these data sharing environments.

- Obj2. Analysis of recommendations, standards and proposals in the literature to ensure data protection in IoT scenarios, identifying their limitations and restrictions.

- Obj3. Design and development of a mechanism that enables to securely exchange data between groups of entities in IoT scenarios.

- Obj4. Design and development of a mechanism that enables the establishment of end-to-end security association in IoT scenarios.

- Obj5. Deployment and evaluation of the implemented security solutions, in order to demonstrate their viability in IoT scenarios.

- Obj6. Proposal for a security architecture to guarantee protection of data during its whole lifecycle in IoT scenarios.

[10] `https://www.ietf.org/topics/security/`
[11] `https://www.etsi.org/committee/cyber`

In this sense, the analysis of security and privacy requirements in different IoT scenarios allowed to identify the need for efficient and effective data protection solutions for these data sharing environments. Furthermore, it was found that many of existing standards and proposals did not adequately fit with the particularities inherent to these scenarios, such as technological heterogeneity, devices' resource constraints, presence of proxies and one-to-many communications. Thus, according to the conclusions derived from this analysis, the need arose to design an architecture intended to guarantee the security of information during its entire lifecycle in the IoT context. Thus, the architecture proposed in this thesis encompasses different application layer solutions whose combination ensures data protection in IoT scenarios. Particularly, the architecture integrates a lightweight, flexible and scalable cryptographic approach based on the *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) scheme [9], in order to secure information exchange between groups of entities. Additionally, this approach is extended with a key exchange mechanism based on a recent IETF standardization effort known as *Ephemeral Diffie-Hellman Over COSE* (EDHOC) [27], which enables the establishment of security associations in these constrained scenarios. It should be noted that this mechanism considers the realisation of a previous bootstrapping phase, where entities obtain their corresponding credentials and keys to securely join the network. In this sense, the *Low-Overhead CoAP-EAP*(LO-CoAP-EAP) boostrapping service [21] is considered due to it was specifically designed for the IoT context. Eventually, a performance analysis of the different security mechanisms integrated in the architecture is performed, with the aim of demonstrating their feasibility and advantages compared to other solutions currently proposed for IoT scenarios.

The previous objectives promoted this thesis, and its realisation led to the set of results presented in the following section.

2.2. Results

This section details the set of works produced to attain the objectives established at the beginning of the thesis. Furthermore, these works have been presented in several publications, such as conferences and high-impact journal, which collect much of the results achieved during this thesis, as shown in Table 2.2.

Specifically, we performed the identification of the main security and privacy challenges derived from the realisation of IoT scenarios by considering previous research works [72, 78]. Similarly, the set of countermeasures proposed in [58] was examined in order to solve, or at least mitigate, such challenges. It should be pointed out that the conclusions collected from this work were included as part of the European project Horizon H2020 ARMOUR[12], which was aimed to provide tested and certified security solutions to promote the large-scale deployment of the IoT [91].

The challenges and countermeasures previously identified were used as a starting point for designing a security approach derived from the CP-ABE encryption scheme, whose architecture was included in [84]. This approach is based on the *bubble* concept, which represents a group of entities sharing information under certain conditions. Thus, in order to carry out the secure data dissemination into a specific *bubble*, the use of CP-ABE is considered, so that entities are able to maintain control over how their information is shared. Subsequently, a more lightweight mechanism of this encryption scheme named SymCpAbe was designed and presented in [84, 88, 89, 92]. Such works propose to combine CP-ABE with symmetric key cryptography, so that efficiency and scalability is improved while flexibility and expressiveness of the original CP-ABE scheme is still leveraged. Furthermore, these solutions for secure group data sharing were deployed and evaluated in real IoT scenarios, where a large volume of data is shared between different heterogeneous entities, from a sensor with resource constraints to a high-level data-driven service. In order to perform these deployments, different components of the FIWARE platform[13] were used, thus facilitating compatibility and interoperability with other existing IoT deployments. This evaluation allowed to demonstrate the applicability and suitability of the

[12] `https://www.armour-project.eu/`
[13] `https://www.fiware.org/`

Nro.	Result	Objective	Publication
1	Identification of the main security and privacy challenges in IoT scenarios, as well as the study of potential solutions that allow to address, at least partially, such challenges	Obj1, Obj2	[91], [87], [90], [88], [84]
2	Design and implementation of a flexible solution that allows to securely share data between groups of entities in IoT scenarios	Obj3	[84]
3	Design and implementation of a lightweight approach to the previous solution for enabling secure group data sharing, in order to improve efficiency and scalability in IoT scenarios	Obj3	[89], [92], [88]
4	Design and implementation of a lightweight key exchange solution that enables the establishment of end-to-end security associations in IoT scenarios	Obj4	[90], [94], [93]
5	Design and implementation of a reduced version to the previous key exchange solution, in order to further reduce both resource consumption by constrained devices and network overhead in IoT scenarios	Obj4	[90]
6	Design and development of extensions to bootstrapping technologies designed for the IoT, in order to establish the cryptographic material required by the implemented key exchange solutions	Obj4	[87]
7	Evaluation of the proposed solutions by instantiating them on different IoT scenarios, with the aim of verifying their feasibility and adequacy in these restricted data sharing environments	Obj5	[90], [87], [88], [84], [85], [86]
8	Integration of the proposed solutions with the purpose of designing an architecture intended to secure shared data during their entire lifecycle in IoT scenarios	Obj6	[90], [87], [88], [84]

Table 2.1: Results achieved during this thesis

proposed solution in these constrained data sharing environments. Likewise, it should be highlighted that obtained results were presented within the scope of two European projects, in particular, FP7 SocIoTal[14] and CHIST-ERA Use-IT[15].

Additionally, the integration of a key exchange mechanism complementary to the previous approach was considered. Particularly, this mechanism allows entities to establish security associations, which confirm entities' legitimacy to participate in the group data sharing process. However, the common presence of proxies in the IoT context became a new challenge to be addressed, in order to ensure the establishment of such security associations between the involved entities. While proxies

[14] `https://cordis.europa.eu/project/id/609112`
[15] `http://useit.eu.org/`

improve scalability and efficiency in communications, their presence also has its downside: they break the end-to-end security model. To overcome this challenge, a lightweight EDHOC-based key exchange mechanism was designed and developed, whose messages were encapsulated and transported through the communication protocol *Constrained Application Protocol* (CoAP) [81]. Thus, this approach enables the establishment of end-to-end security associations between two entities in IoT scenarios, even in the presence of other intermediate entities, such as proxies [90]. Afterwards, such key exchange solution was proposed in [93, 94] as an alternative process to the manual configuration for distributing and updating session keys in *Long Range Wide Area Network* (LoRaWAN) architectures [69]. In parallel, a compact version of this mechanism was developed (CompactEDHOC), in which the security parameter negotiation required by the original approach is suppressed. Instead, these security parameters are stored in a resource directory entity [82], further reducing resource consumption on constrained devices and network overhead. Additionally, a performance evaluation of both EDHOC-based solutions was performed, with the aim of demonstrating their advantages over other similar approaches that are widely used in the IoT context, such as the *handshake* of the *Datagram Transport Layer Security* (DTLS) protocol [19].

Nevertheless, the application of the EDHOC-based key exchange mechanisms evidenced the lack of a previous phase, in which authentication credentials required for their execution are established. This fact motivated the work presented in [87], where integration of bootstrapping technologies [5] is suggested with the aim of deriving these credentials from certain cryptographic material generated by the boostrapping process. Furthermore, in order to assess the level of security offered by these key exchange solutions, [85] proposed the use of an automated testing approach that allows to simplify such evaluation process. Thus, considering this publication, [86] defined a methodology based on the *Model-Based Testing* (MBT) approach [7] to evaluate different security properties of the EDHOC-based mechanisms. In this sense, it is important to note that information obtained from this evaluation was used to detect and resolve certain implementation errors.

The set of these solutions fostered the design of the security architecture presented in this thesis, which focuses on protecting shared data in IoT scenarios. In this sense, the results exposed in this section provide an overview of the work plan that was followed to achieve the objectives previously established. This vision is subsequently expanded in Chapter 3, where solutions integrating the proposed security architecture are detailed.

2.3. Conclusions and Future Work

The expansion of the IoT is being driven with the arrival of recent communication technologies, such as 5G, which enable the massive exchange of information among a large number of interconnected heterogeneous devices. This evolution of the Internet is encouraging the emergence of new scenarios, which represent ecosystems where different deployed physical devices detect and share data about their environment. This fact enables to transform and improve daily services, such as transportation or healthcare systems. However, the realisation of this *data-driven society* [61] paradigm presents important security challenges related to the treatment of personal information, which may violate the privacy of the participants. Consequently, data protection is considered a key aspect to increase people's trust and to achieve the development of IoT scenarios on a large scale.

In this sense, certain standardization bodies have carried out analysis about security and privacy issues, which are derived from the application of the IoT. As result, they provide recommendations on how to address such issues and achieve secure and reliable ecosystems. Although these recommendations are not legally binding, the recently implemented GDPR aims to regulate, in legislative terms, the protection of personal information, as well as the way organizations process, store and delete it. However, the application of security approaches that ensure compliance with this regulation in IoT scenarios is not trivial, given the particularities inherent in these data sharing ecosystems.

According to such particularities, this thesis presents a Data-centric Security Architecture for the Integration of Constrained Devices into IoT Scenarios. The development of this architecture is based

on an analysis performed on security and privacy challenges in the IoT context. The conclusions derived from this analysis confirmed the need for new security approaches that allow to address such challenges, beyond the typical symmetric and public key cryptography. Thus, the proposed architecture integrates different lightweight, flexible and scalable solutions adapted to the particularities of IoT scenarios, guaranteeing data security during its whole lifecyclecle.

Particularly, an approach based on the CP-ABE encryption scheme has been designed and implemented, allowing secure data sharing within a specific group of entities defined as *bubble*. Additionally, a new hybrid version of this approach named SymCpAbe has been presented, which combines symmetric cryptography for information encryption, with attribute-based cryptography for group data dissemination. This way, efficiency and scalability of the original version have been improved. Further, the realisation of such approaches are based on different components of the FIWARE platform, thereby facilitating its compatibility and interoperability with other existing IoT deployments. With the aim of verifying its suitability in IoT scenarios, the proposed approach was compared with the CP-ABE scheme on a real *smart building* scenario. The obtained results demonstrated the advantages of this solution for secure data sharing in IoT scenarios, achieving a trade-off between efficiency, flexibility and scalability.

Similarly, a solution based on the EDHOC key exchange protocol was designed and implemented, in order to enable the establishment of end-to-end security associations between two endpoints in IoT scenarios. For this purpose, the proposed approach considers to transport the EDHOC messages over the CoAP communication protocol, which is the solution suggested by the current draft of such key exchange approach. It should be pointed out that, due to its efficiency and lightness, this solution was integrated into a LoRaWAN architecture to cover the lack of a mechanism for updating session keys in this type of networks. In parallel, a more reduced version of the proposed approach was designed and developed (CompactEDHOC), which is based on extracting the security parameters and their previous storage in a resource directory entity. Evaluation results of both solutions showed the advantages of these proposals compared to other current key exchange solutions, such as the DTLS *handshake* protocol.

However, these EDHOC-based solutions require pre-established credentials that enable authentication during their execution. In this sense, the EDHOC draft does not address this aspect, so it is necessary to consider other complementary security approaches that allow to establish such credentials. Accordingly, the LO-CoAP-EAP bootstrapping service was adopted, due to it had been designed and tested on IoT scenarios. Particularly, a LO-CoAP-EAP extension was implemented, which enables to derive the authentication credentials required by the proposed solutions, that is, a shared symmetric key or the corresponding private/public key pairs. Eventually, the integration of LO-CoAP-EAP with the EDHOC-based approaches was evaluated on a real IoT use case, demonstrating its suitability in these constrained scenarios.

The previous security mechanisms enabled to meet the objectives defined at the beginning of this thesis. Thus, the combination of such solutions resulted in a security architecture that, considering the particularities of IoT scenarios, ensures the protection of information in these data sharing environments. Additionally, this architecture is presented as an excellent starting point for future work related to security and privacy aspects in the IoT context.

In this sense, the design and development of mechanisms to allow distributing the CP-ABE encryption and decryption in different *edge* nodes is proposed. Specifically, these *edge* nodes are intended to work cooperatively to carry out such cryptographic operations. This way, resource consumption is further reduced, thus improving the performance of the proposed approach for the secure group data sharing. Additionally, this approach may be extended by considering identity-based signature schemes [33], in order to protect the integrity of shared information. Similarly, the study of research efforts in the scope of the *Authentication and Authorization for Constrained Environments* (ACE) work group[16] is suggested. Particularly, authorisation models could be incorporated to address issues related to access control in IoT scenarios [29].

[16] `https://datatracker.ietf.org/wg/ace/about/`

Furthermore, reviewing and updating the development of the implemented key exchange approaches from the last EDHOC specification is proposed. Likewise, these solutions could be extended by developing and integrating a resumption mechanism that allows to improve the refresh process of previously established security associations. Both modifications assure to increase the performance of the proposed EDHOC-based approaches in terms of efficiency and optimization of resource use. Finally, another promising line of research is related to the integration of the *Object Security for Constrained RESTful Environments* (OSCORE) protocol [28], which has been recently standardised. This way, the architecture presented in this thesis would be further enriched, thereby leveraging all the advantages offered by application layer security approaches in the IoT context.

2.4. Thesis Structure

This thesis is organized following the publication compendium model and the international mention recognized by the current regulations. Accordingly, Chapter 1 presents a summary in Spanish that describes the motivation of the performed research, as well as the objectives that were established at the beginning of such research. Additionally, this chapter provides an overview of the set of results achieved at the conclusion of this thesis and its relationship with the previously defined objectives. Similarly, Chapter 2 offers an English version of the summary presented in the previous chapter. Furthermore, the Chapter 3 delves into the main challenges that motivated the development of this thesis. In addition, the proposed architecture to overcome such challenges is described, detailing the different developed security mechanisms that integrate it. Moreover, the Chapter 4 includes the four publications that comprise this thesis, in particular:

- *Protecting Personal Data in IoT Platform Scenarios Through Encryption-Based Selective Disclosure.* This publication identifies the users' trust as a key aspect to achieve the deployment of IoT scenarios in the society. Consequently, the concept of *bubble* is defined, which represents a group of entities where information is shared under certain security restrictions, following the preferences of data owners. The realisation of this concept is based on the use of attribute-based cryptography, so that information shared within a *bubble* is protected by using a CP-ABE access policy. Likewise, a key employed to access information is associated with the set of attributes of the corresponding entity. Additionally, this approach is evaluated on a real *smart building* scenario by considering certain components of the FIWARE platform. According to the obtained results, applicability and benefits of this approach in IoT scenarios is demonstrated.

- *A Lightweight and Flexible Encryption Scheme to Protect Sensitive Data in Smart Building Scenarios.* Following the research line of the previous work, this publication highlights the large amount of information to be shared in the IoT context. This information enables the emergence of new data-driven services, which are intended to improve people's life quality. However, part of this shared information is sensitive, which could violate privacy of involved individuals if not appropriate actions are adopted. Accordingly, security solutions that allow data owners to establish what requirements must be met by the services interested in accessing their data are required. In order to overcome this challenge, a lightweight and scalable encryption approach named SymCpAbe is presented, which combines efficiency of the symmetric key cryptography and flexibility of the CP-ABE cryptographic scheme. Furthermore, the proposed solution is evaluated on a real *smart building* scenario, and results reveal its advantages against the original CP-ABE scheme for secure group data sharing in IoT scenarios.

- *Application Layer Key Establishment for End-to-End Security in IoT.* This publication focuses on the need for solutions intended to data protection between two endpoints in the IoT context, even in the presence of intermediate entities (e.g., proxies). In order to meet this need, a first solution based on the EDHOC protocol is presented, which enables the establishment of end-to-end security associations in constrained scenarios. Additionally, a compact version of the previous

approach named CompactEDHOC is proposed. In this second solution, the security parameters are previously stored in a resource directory component, so their negotiation is removed from the original version. This way, this optimisation allows to further reduce network overhead and device resource consumption, thereby improving the performance for the establishment of end-to-end security associations in IoT scenarios.

- *Architecture of Security Association Establishment Based on Bootstrapping Technologies for Enabling Secure IoT Infrastructures.* This publication reveals the lack of a previous mechanism to establish the authentication credentials required by the EDHOC-based solutions presented in the previous work. In order to address this gap, the integration of lightweight bootstrapping technologies in a preceding phase is considered, particularly, the LO-CoAP-EAP service. This way, endpoints are able to derive their credentials by using certain cryptographic material established during the bootstrapping phase. From this point on, such endpoints are enabled to execute the specific EDHOC-based solution for establishing and updating end-to-end security associations. Furthermore, this approach is deployed and evaluated on a real *smart building* scenario, where obtained results reveal the advantages of its application in the IoT context.

Finally, the Chapter 5 collects the bibliography related to this document, in particular, the referenced publications (Section 5.1) and the publications elaborated during the development of this thesis (Section 5.2).

Chapter 3

Introduction

The integration of the so-called *Internet of Things* (IoT) [4] in the society is fostering the emergence of new scenarios where a large volume of data collected by heterogeneous physical devices is shared and employed to enhance everyday services, such as transport systems, health care or energy efficiency. This technological evolution towards a data-driven society [61] also leads to new cybersecurity and data-protection risks and challenges, which could ultimately impact citizens' safety. Therefore, there is a need to design and integrate different security mechanisms with the aim of protecting people through an adequate use of their data.

The IoT promotes the trend toward a hyper-connected world encompassing different technologies to enable the integration of physical devices into the Internet. According to this vision, the IoT arises as an essential technological driver that encourages the realization of new scenarios where data detected by these devices in a certain environment can be used for the development of innovative data-driven services. In turn, such services make use of such incoming data and make more effective decisions accordingly (e.g., regarding energy consumption or emergency management). From the security point of view, protecting the access to data, especially those ones highly sensitive, is presented as a key element to be addressed to the sustainable realisation of these new IoT scenarios, where additionally different actors could be involved with potential conflicting interests. On the one hand, companies require a huge amount of data with the aim of providing rich experiences and customised services to users. On the other hand, users should be enabled to maintain the control on how their data are shared and under what circumstances. Furthermore, the integration of everyday devices on the Internet means that users will be more exposed to security and privacy risks. Indeed, many of these devices will often operate on behalf of their owners, sharing data without their explicit consent. This fact, along with the amount and sensitivity degree of shared information, gives rise to significant security and privacy challenges. Actually, sharing data from certain devices, such as healthcare appliances, takes users' privacy to a broader dimension [32], which may have implications for their safety if appropriate countermeasures are not implemented.

In a common IoT scenario, deployed devices are in charge of capturing information about their surrounding environment. These devices are characterised by having strong resource constraints [12] and operating over *Low-Power and Lossy Network* (LLNs), which envisage the use of proxies for improving scalability and efficiency in communications [26]. Additionally, collected information is shared with a group of interested data-driven services through a central data exchange platform. The aim of this component is to remain IoT devices and services decoupled, thereby allowing to carry out the information exchange process asynchronously. This way, both resource consumption by constrained devices and network overhead are reduced. Nevertheless, these particularities of IoT scenarios, that is, the resources and networks constraints, the presence of intermediates entities (proxies and data exchange platforms) and the need for enabling group data sharing, become an obstacle that hinders protecting information in these ecosystems.

In this sense, there are different security approaches that may be adapted and jointly integrated to

properly secure data in IoT scenarios. Specifically, the *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) approach [9] enables a source to share certain information with a group of interested receivers through a data exchange platform, while security between involved entities is still ensured (end-to-end security). Additionally, this approach provides two main properties to be leveraged in these constrained scenarios. On the one hand, unlike symmetric key cryptography, CP-ABE does not require involved entities to share symmetric keys, which could be unfeasible given the huge number of devices and data-driven services expected in IoT scenarios. On the other hand, CP-ABE is seamlessly applicable to provide confidentiality in *one-to-many* configurations (even in the presence of a exchange platform), since a piece of information can be encrypted and shared with multiple entities by using a single message. However, it should be pointed out that advantages provided by this cryptographic approach come at the expense of performance, which could hamper its application into resource-constrained devices. Moreover, while this solution enables protection in group data sharing, it could be further enriched by considering a key exchange mechanism that allows entities to establish end-to-end security associations. This way, entities are previously authenticated and enabled to join the data sharing process.

In particular, the *Internet Engineering Task Force* (IETF) proposes the use of the *Datagram Transport Layer Security* (DTLS) protocol [19] as mechanism to establish security associations between two entities. Indeed, the Constrained Application Protocol (CoAP) [81] defines a binding with this security approach to protect communications in constrained environments. Nevertheless, DTLS is not able to establish end-to-end security associations in IoT scenarios due to the common presence of proxies, which need to access specific CoAP headers to fulfill their functionality. Therefore, these associations finish at each proxy, so that only hop-by-hop security is provided [26]. To overcome this issue, the IETF has recently founded the *Lightweight Authenticated Key Exchange* (LAKE) WG[1], which is focused on producing lightweight authenticated key exchange mechanisms to establish end-to-end security associations in IoT scenarios, even in the presence of intermediate entities. In this sense, the *Ephemeral Diffie-Hellman over COSE* (EDHOC) protocol [27] is proposed in the scope of the LAKE working group as a solution at the application layer to be employed in such constrained environments, since it fits with resources and networks constraints envisaged in the IoT context.

Accordingly, this thesis provides an architecture focused on protecting shared data during their lifecyle in IoT scenarios. The design of this architecture is performed through the adaptation and combination of a set of recent data-centric security solutions and proposals, in order to overcome scalability, flexibility and performance issues. On the one hand, the proposed architecture integrates a hybrid approach based on the CP-ABE scheme named SymCpAbe, which enables and secure group data sharing in constrained environments. Particularly, this approach combines the lightness and efficiency of symmetric key cryptography to protect data, with the expressiveness and flexibility of CP-ABE to distribute the corresponding symmetric keys. On the other hand, an EDHOC-based mechanism is also included to complement and enrich the previous approach. Such mechanism is aimed to establish end-to-end security associations that confirm entities' legitimacy to join data sharing process. Additionally, a compact version of this key exchange approach named CompactEDHOC is developed, which is based on extracting the negotiation of security parameters and storing them in a resource directory entity [82]. Consequently, this version enables to further reduced the network overhead and device resource consumption regarding the original approach in IoT scenarios.

Moreover, it should be pointed out that the EDHOC-based solutions provide different authentication modes, particularly, based on pre-shared keys, on raw public keys and on certificates. However, the EDHOC specification does not define how these authentication credentials are established. To fill this gap, the proposed architecture considers the integration of bootstrapping technologies, such as the *Low-Overhead CoAP-EAP*(LO-CoAP-EAP) bootstrapping service [21] or the *Protocol for Carrying Authentication for Network Access* (PANA) [16], so that authentication credentials are derived from certain cryptographic material generated by this bootstrapping process.

The structure of this chapter is as follows: Section 3.1 describes the main entities and interactions

[1] `https://datatracker.ietf.org/wg/lake/about/`

identified in IoT scenarios, as well as the particularities inherent to these data sharing ecosystems. Section 3.2 points out other relevant works in literature that are focused on addressing security and privacy issues in IoT scenarios. Furthermore, the proposed architecture is presented in Section 3.3, offering a detailed explanation of the integrated security solutions. Finally, Section 3.4 provides an overview of the main conclusions derived from this thesis.

3.1. Data Sharing in the IoT

The IoT paradigm is transforming our daily life by fostering the emergence of new scenarios, which offer a wide set of high-level services intended to improve people's life quality.

Considering this context, the literature provides different works that study the impact of the IoT in our society, presenting several examples of these new IoT scenarios. An example of them is the *Mobile Crowd Sensing* (MCS) [45]. In such a case, the movement inherent to the use of devices acting as gateways (e.g., smartphones or cars) allows them to obtain, process and disseminate data that are detected by deployed sensors without the need for additional infrastructure. This information is then distributed to certain data-driven services through a central platform, in order to enable real-time applications, such as traffic monitoring or incidents reporting. Similarly, in the context of *E-health* [44], the use of wearable sensors composing *Wireless Body Area Networks* (WBANs) allows patient's status to be detected and shared with the medical staff in hospitals or medical centres. Actually, the use of WBANs enables a wide range of e-health services, such as health monitoring or immediate action in case of medical emergencies. Moreover, *Smart Buildings* [52] represent heterogeneous environments where a high volume of information coming from different data sources (e.g., RFID readers or temperature sensors) is shared with a group of data-driven services through a data exchange platform. In turn, these services employ the incoming information to extract certain knowledge that enables the realisation of new applications related to energy saving, emergency management or environmental comfort.

Based on the previous examples, a common IoT scenario can be considered as a data sharing ecosystem where evidences detected by several deployed devices are transformed into meaningful information. In addition, such information is employed for the deployment of new data-driven services. Thus, Figure 3.1 provides a high-level overview of this data sharing ecosystem, identifying four main entities involved on it. Specifically, *Data Sources* are responsible for detecting and monitoring their surrounding environment. They typically represent battery-powered and resource-constrained devices (e.g., sensors) that are physically deployed in a certain area. These entities are usually grouped to compose *Wireless Sensor Networks* (WSNs), where communications are performed through network technologies specially designed to constrained data sharing ecosystems. In this sense, *IPv6 over Low power Wireless Personal Area Networks* (6LoWPAN) [56] is considered the main technology for short-range networks, while *Low-Power Wide-Area Network* (LP-WAN) [49] solutions, such as *LoRa Wide Area Networks* (LoRaWAN) [69] or Sigfox[2] are proposed for long-range networks. Furthermore, at an intermediate level, *Gateways* are responsible for transforming and formatting data coming from *Data Sources*, which is further published on an *IoT Platform* for its dissemination. Thus, the *IoT Platform* represents a central data storage where all the information received from *Gateways* is managed and provided to the group of interested data-driven *Services*. Finally, these *Services* use incoming information to infer new knowledge by applying data mining techniques [75], so that they are able to make more effective and efficient decisions accordingly.

Furthermore, two phases to complete the data sharing process are also identified. On the one hand, the first phase is focused on the data exchange from the *Data Source* to the corresponding *Gateway*. A key aspect to be considered is that both *Data Sources* and networks embraced in this first phase usually present strong resource restrictions, as already mentioned. Therefore, data exchanges with the *Gateway* should be performed by using protocols intended to work in constrained environments. In this sense, the IETF proposes CoAP as the main application layer protocol aimed to provide

[2] `https://www.pdpjournals.com/docs/88440.pdf`

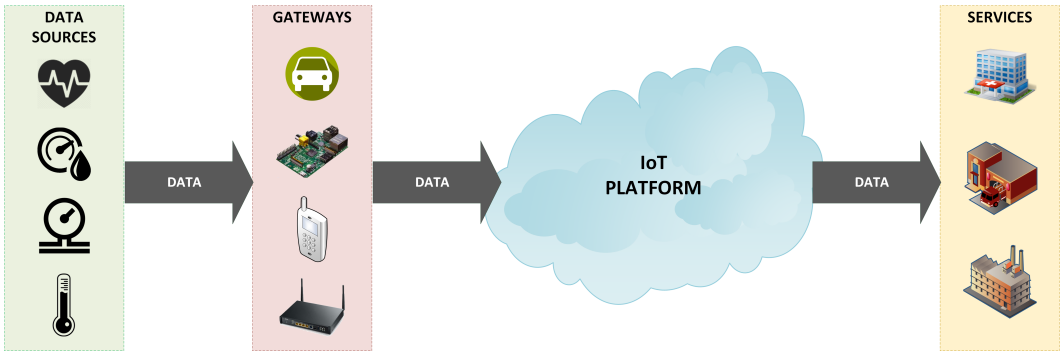

Figure 3.1: Overview of a common IoT scenario

one-to-one communications in scenarios accommodating resource-constrained devices. Additionally, it should be pointed out that CoAP communications are often performed through proxies, whose aim is to reduce both the response time of CoAP requests and the use of the network bandwidth. This way, proxies allow to improve scalability and efficiency in communications. For the sake of clarity, note that Figure 3.1 does not show these intermediate entities between *Data Sources* and *Gateways*, but their presence in IoT scenarios is assumed. On the other hand, the second phase is focused on the data exchange from the *Gateway* to the group of interested data-driven *Services*. As already pointed out, communications among these entities are performed through an *IoT Platform*, which usually provides a *publish/subscribe service* as data sharing model. Thus, considering this data sharing model, a piece of information can be shared with a set of interested entities by using only one message. This provides two advantages: efficiency in data sharing is improved; and constrained devices are able to save resources thanks to the platform maintains involved entities uncoupled. In this sense, there are different protocols to implement the publish/subscribe pattern and enable one-to-many communications through the *IoT Platform*, such as the *Advanced Message Queuing Protocol* (AMQP) [70] or *Message Queue Telemetry Transport* (MQTT) [71]. Their selection will depend on practical aspects of the particular IoT scenario.

From the security point of view, the treatment of shared data is a key aspect to be considered in IoT scenarios, especially in case of sensitive information, such as personal data. Accordingly, there is a need for considering different complementary security solutions that enable to secure the data sharing process in these constrained environments. Additionally, such security solutions should be properly adapted, in order to meet with a set of non-functional requirements derived from the particularities of these scenarios. Specifically, these requirements are focused on:

- *Scalability (R1).* The application of scalable security mechanisms to properly protect information is crucial due to the large amount of data to be exchanged among data sources and data-driven services in IoT scenarios.

- *Lightness (R2).* Security mechanisms must be adapted to different types of devices, such as sensors, smartphones or back-end servers. Therefore, they have to be lightweight enough, in terms of resource consumption, so that resource-constrained devices are able to execute them.

- *Efficiency (R3).* IoT scenarios envisage a huge volume of data to be exchanged among heterogeneous devices with different capabilities, as already mentioned. Thus, security mechanisms have to be efficient, so that their application continues providing a good performance during the data sharing process.

- *Flexibility (R4).* In IoT scenarios, a sender is able to share a piece of information with a group of receivers by using a single message, following the publish/subscribe pattern. Then, security

mechanisms should provide a high degree of flexibility with the aim of adapting to this data sharing model.

- *Interoperability (R5).* Security mechanisms should be based on the use of consolidated standards in order to ease the integration with other IoT infrastructures. This is a key aspect for improving interoperability and, thereby, fostering the deployment of IoT scenarios on a broad scale.

The need for securing data sharing process in IoT scenarios has fostered the design and development of the architecture presented in this thesis. In this sense, different data-centric security solutions have been integrated, which fit the inherent particularities of these constrained environments. Thus, the combination of such security solutions allows to ensure protection of data during their whole life-cycle. Additionally, a more detailed description of the proposed architecture and the embedded security mechanisms is provided in Section 3.3.

3.2. Related Work

The advent of recent communication technologies is aimed to satisfy the demanding data sharing requirements in IoT scenarios. However, security and privacy challenges in such new data-driven ecosystems can be further aggravated due to the pervasiveness and ubiquity enabled by these technologies. This fact has attracted a significant interest from the research community, which is reflected by several related publications. Thus, based on the phases previously identified to complete the data sharing process in IoT scenarios, the following subsections summarize different proposals addressing security and privacy concerns on these new data sharing environments.

As already mentioned, CoAP represents the application layer standard proposed by the IETF for enabling communications in IoT constrained environments, due to its very low overhead and simplicity. From the security point view, this protocol specifies a binding to the DTLS protocol to protect communications between two CoAP endpoints. Accordingly, the scientific literature reports works that study the DTLS adoption for establishing security associations in the IoT landscape. Particularly, [39] describes a mutual authentication security scheme for IoT based on DTLS and UDP/IPv6 protocols. However, the implemented scheme makes use of the *Rivest–Shamir–Adleman* (RSA) algorithm, which is unsuitable on resource-constrained devices due to the size of cryptographic material and computation requirements. In this direction, [34] presents a preliminary overhead estimation for the DTLS handshake with certificate authentication. Additionally, authors detail three design aspects, specifically, certificate pre-validation, session resumption and handshake delegation, to reduce such overhead. Furthermore, [63] proposes a lightweight CoAP-DTLS scheme by using different 6LoWPAN header compression mechanisms to decrease message overhead. In such a way, authors achieve to reduce 6LoWPAN fragmentation, while DTLS security is still provided. Similarly, [62] describes a DTLS-based architecture intended to secure communications in cloud-connected IoT scenarios, considering the different DTLS authentication modes: pre-shared keys, raw public keys and certificates. However, DTLS cannot ensure end-to-end security properties due to CoAP communications are usually performed through proxies for improving scalability and efficiency. Actually, this protocol is only able to provide hop-by-hop security since DTLS security associations must be terminated at each proxy, as already mentioned. In order to mitigate this issue, [41] presents an approach aimed to make DTLS feasible in multi-hops IoT scenarios. Nevertheless, the proposed approach requires to add messages forwarding functionality in the intermediate entities, which limits its applicability on a large scale.

Unlike the previous DTLS-based proposals, enabling security at the application layer emerges as a solution to ensure end-to-end security, even in presence of proxies or other intermediate entities, as proposed in [24]. In this direction, [76] proposes a hybrid architecture that combines transport and object-based security. In addition to these works, [26] provides a set of security requirements, which are defined from a threat analysis to CoAP communications through proxies. Additionally, according to the results of such analysis, authors propose to enable CoAP communication protection at the application layer by using an object-centric security mechanism. In terms of standardisation, the IETF

standardised object-based security through the *CBOR Object Signing and Encryption* (COSE) protocol [36], which, in turn, makes use of the *Concise Binary Object Representation* (CBOR) [13]. Based on COSE, the *Object Security for Constrained RESTful Environments* (OSCORE) approach [28] is a recently standardised application layer protocol aimed to secure end-to-end CoAP messages in IoT scenarios, guaranteeing data confidentiality and integrity. To fulfil with its functionality, OSCORE needs a lightweight and authenticated key exchange protocol to establish the so-called security context, as pointed in [47]. For this purpose, EDHOC [27] is a key exchange protocol intended to establish end-to-end security associations between two endpoints in constrained environments. While this approach is under standardisation process, EDHOC has been already proposed in different recent works. Specifically, [15] provides an authorisation and authentication framework integrating an EDHOC-based key agreement approach with the OAuth standard [31]. Likewise, [40] considers this key exchange protocol to carry out the certificate enrollment stage in IoT scenarios. Similarly, EDHOC is also considered in our previous work [93], where this key exchange protocol is proposed as mechanism to derive and update cryptographic material in LoRaWAN networks. However, all of these proposals do not address the establishment of authentication credentials required to execute EDHOC. In order to deal with such purpose, it is necessary to consider other complementary approaches that allow to launch EDHOC.

In this sense, there are different works that propose the use of cryptographic material obtained during a previous bootstrapping phase to enable a security association protocol, such as DTLS [6, 22, 38]. Based on it, we consider the integration of bootstrapping technologies with EDHOC, so that the required authentication credential are derived from the cryptographic material generated by the bootstrapping process. From the standardisation perspective, the *Protocol for Carrying Authentication for Network Access* (PANA) [16] is widely considered as the main bootstrapping protocol in the IoT context, as shown [18, 65–67]. Nevertheless, authors in [20] demonstrate that PANA was not designed for constrained IoT scenarios. Accordingly, they propose a lightweight bootstrapping approach that is envisaged to cope with resource-constrained devices, which is named as LO-CoAP-EAP [21]. Additionally, the proposed approach is evaluated on real devices to prove its suitability in constrained environments. Therefore, our solution integrates the LO-CoAP-EAP mechanism to derive the security credentials required to carry out the EDHOC protocol. Furthermore, we design and implement a reduced version of EDHOC by using a resource directory component [82], in order to further reduce the overhead and processing of this emerging key exchange approach.

Moreover, as already defined in the previous section, devices acting as data sources share a huge volume of information about their surrounding environment with groups of data-driven services through a central IoT platform. Despite the already mentioned advantages that this data sharing model provides in constrained scenarios, its application also involves two challenges to be considered. On the one hand, the presence of the central platform becomes an obstacle to ensure that only authorized entities are able to access the information, due to this component access to all the data being shared. On the other hand, interactions between devices and services are usually based on short-lived asynchronous communications. Therefore, beyond typical multicast solutions [46, 60, 83], there is a need to adopt more flexible and scalable security approaches that allow to address these challenges.

In this direction, *Attribute-Based Encryption* (ABE) [64] has received a notable attention due to its high level of flexibility and expressiveness compared to traditional symmetric and asymmetric cryptography. In ABE systems, entities are represented by identity attributes. Additionally, there are two alternative schemes to protect data. On the one hand, *Key-Policy Attribute-Based Encryption* (KP-ABE) [23] allows to encrypt data by using a set of attributes, while private keys are associated with logical combinations of attributes. Considering this scheme, authors in [80] provide a lightweight version of KP-ABE to be employed in constrained devices. To achieve this, the proposed scheme is based on the use of *Elliptic Curve Cryptography* (ECC) [30] rather than bilinear pairings. On the other hand, the *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) scheme [9] allows to encrypt data under certain logical combination of attributes (access policy), while private keys of participants are associated with sets of identity attributes. Thus, data will be accessible only to those entities whose private keys meet the access policy employed in the encryption process.

Currently, there are already previous works considering the CP-ABE integration in the IoT con-

text, such as [59, 68, 73]. Specifically, these works propose the use of such encryption scheme with the publish/subscribe communication pattern to secure group data sharing in IoT scenarios. However, the direct application of CP-ABE mainly presents two practical challenges. Firstly, the size of the private keys and ciphertexts is a limiting factor to the application of this scheme in restricted scenarios. In order to address this issue, [3] proposes an adapted CP-ABE version that provides constant-size ciphertexts under any access policy used for encryption. Likewise, [25] proposes a CP-ABE scheme with constant-size secret keys independently of the number of identity attributes. Secondly, the use of expensive cryptographic primitives makes unfeasible the CP-ABE deployment on resource-constrained devices. In this sense, the scientific literature reports studies evaluating CP-ABE feasibility on devices with different features. Particularly, [77] presents a performance analysis about the CP-ABE application on a laptop and a smartphone. Results demonstrate that computers are able to execute this scheme with an acceptable performance, but its use on smartphones or similar devices is still challenging when a high level of security is required (e.g., 112-bits or higher [37]). Similar to this work, [1] provides an optimized CP-ABE implementation (ANDRABEN)[3] based on [8], which is analysed on certain devices, such as *Intel Galileo Gen 2*, *Intel Edison*, *Raspberry Pi 1 Model B* and *Raspberry Pi Zero*. While authors conclude that a reasonable performance in these devices can be achieved, they do not consider its application on a real IoT scenario, where a huge amount of data need to be protected. Thus, scalability could be limited.

According to the previous results, different works propose to delegate the expensive CP-ABE cryptographic operations to more powerful entities, in order to alleviate the burden on resource-constrained devices. Specifically, [74] proposes a scheme where a device with resource limitations delegates the CP-ABE encryption operation to certain set of assistant nodes, assuming that these are trusted. Subsequently, results are returned to such device, in order to compute the corresponding ciphertext. Nevertheless, note that all data are sent to assistant nodes without protection, so that if these entities are compromised, data could be disclosed. Following this approach, [79] presents an extended CP-ABE scheme that allows resource-constrained devices to delegate the CP-ABE decryption operation to a cloud platform. However, authors do not verify its application in scenarios where devices have to handle large amounts of data. Moreover, another complementary line of research to achieve the CP-ABE application in IoT scenarios is focused on combining flexibility provided by this scheme with efficiency of symmetric key cryptography. In this sense, [55] describes a solution where data are encrypted by using the AES algorithm with symmetric keys, which are, in turn, protected with the CP-ABE scheme. The resulting AES ciphertext along with the corresponding CP-ABE encrypted key are subsequently stored on a cloud service. In such a way, only those entities whose private keys meet the access policy used to encrypt the particular CP-ABE symmetric key are able to access AES encrypted data. Similarly, [73] describes a new approach using the AES algorithm to protect data, which are further shared with groups of entities by following the publish/subscribe pattern. In this case, groups are managed by a controller entity, so that every time a new symmetric key is computed and protected with CP-ABE, such entity generates *key-update* messages to notify the corresponding group. However, even though these solutions allow to deploy the CP-ABE scheme on constrained environments, their use in real IoT scenarios envisaging several data to be shared is still challenging. Unlike such CP-ABE based proposals, the approach of this thesis follows an attribute-based key distribution process by integrating standard mechanisms to represent and send the cryptographic material to be used. Furthermore, the resulting approach has been comprehensively evaluated over a publish/subscribe system and considering the European FIWARE platform[4].

All of these research proposals partially address some of the main security requirements in the IoT context that were identified in Section 3.1. However, there is still a need to provide a holistic solution encompassing different approaches to enable security in the data sharing process, which was described in the previous section. To address this gap, the security architecture presented in this thesis is intended to face the security challenges identified in constrained scenarios. Next section provides a detailed description of this architecture and the integrated security mechanisms.

[3] `https://spritz.math.unipd.it/projects/andraben/`

[4] `https://www.fiware.org/`

3.3. Data-centric Security Architecture for the IoT

The data sharing process in IoT scenarios requires the integration of solutions that allow to properly protect information exchanges, from data sources to interested data-driven services. This set of solutions must adequately fit with the particularities inherent to these ecosystems, such as technological heterogeneity, devices' resource constraints, presence of proxies and group communications. Consequently, this thesis provides an architecture intended to enable protection of information during its entire lifecycle in IoT scenarios. Towards this end, the proposed architecture integrates different data-centric security solutions, whose combination allows to secure the data sharing process. Specifically, the proposed approaches are conceived for the application layer in order to ensure end-to-end security, even in the presence of intermediate entities such as proxies. Furthermore, enabling data protection at this upper layer makes these approaches independent of the underlying technologies. Moreover, the integrated solutions must also meet the set of non-functional requirements described at the end of Section 3.1. In particular, these solutions are adapted to be deployed in devices with resource constraints, in order to achieve lightweight and efficient versions that allow to save resources in constrained scenarios (R1, R2, R3). In addition, such approaches enable a flexible mechanism to provide security in one-to-many communications, that is, from a data source to multiple services (R1, R4). Likewise, the proposed approaches are developed under the umbrella of different standardisation bodies, such as the IETF[5] and ETSI[6], which favour the interoperability with other IoT deployments (R5).

Accordingly, Figure 3.2 shows an overview the architecture presented in this thesis, specifying the security solutions implemented by each involved entity. In particular, *Data Source* and *Gateway* integrate the solutions based on LO-CoAP-EAP and EDHOC, while *Gateway*, *IoT Platform* and *Service* embed the SymCpAbe approach. Additionally, and for the sake of clarity, an *Infrastructure* layer is displayed, which represents the set of backbone components intended to enable the data sharing process, particularly, *Proxy*, *Gateway* and *IoT Platform*. Below, we provide a detailed description of the processes required between such components for a secure data sharing process.

3.3.1. End-to-end Security Association Establishment

The data sharing process begins when the *Data Source* exchanges information with the corresponding *Gateway* (phase 1), as already mentioned. However, before the *Data Source* is able to start such information exchange, this entity needs to be previously authenticated and joined to the network by running a bootstrapping process. Particularly, this bootstrapping process envisages the *Data Source* makes use of certain cryptographic material statically configured in its manufacturing domain to derive new dynamic credentials. Then, by employing such credentials, this entity is able to securely joins to the deployment domain network through the *Gateway*. In this direction, the PANA protocol [16] is widely considered to provide the bootstrapping service. Indeed, the *Zigbee Alliance*[7] specifies the use of this bootstrapping protocol in conjunction with the *Extensible Authentication Protocol* (EAP) [17] to carry out the authentication process. Nevertheless, PANA was not specifically designed for the IoT context, as demonstrated in [20]. Therefore, the architecture proposed in this thesis integrates a lightweight bootstrapping protocol intended to constrained environments, concretely, LO-CoAP-EAP [21]. Unlike PANA-based proposals, LO-CoAP-EAP is better suited to the networks' and devices' limitations, and achieves a trade-off among scalability, flexibility and performance. Additionally, this protocol also allows to reuse the deployment of CoAP, which is the standard proposed for enabling communications in IoT scenarios. This fact avoids to add any other specific technology aimed to perform the bootstrapping process, which burden of involved endpoints is further alleviated.

Once the *Data Source* is properly authenticated and deployed in the IoT scenario through the bootstrapping process, the next step is to establish a security association between this entity and the

[5] `https://www.ietf.org/topics/security/`
[6] `https://www.etsi.org/committee/cyber`
[7] `https://zigbeealliance.org/`

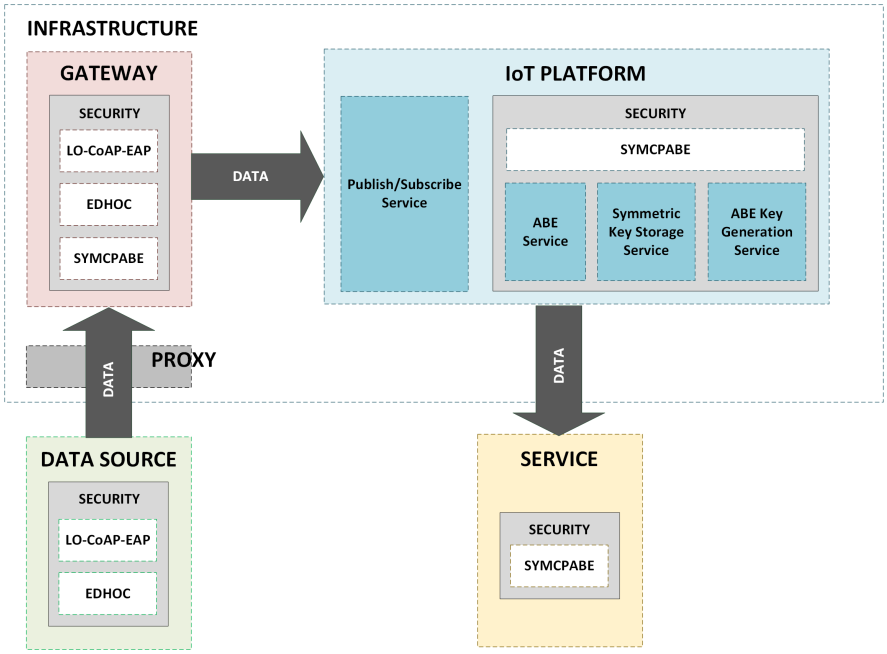

Figure 3.2: Overview of the proposed data-centric security architecture for IoT scenarios

corresponding *Gateway* to protect their data exchanges. As already mentioned, the use of DTLS in these constrained environments cannot provide end-to-end security between the two involved endpoints due to the common presence of proxies, so only hop-by-hop security is ensured. It should be pointed out that, while hop-by-hop security could be sufficient in certain IoT scenarios, there are many others where it is not. For example, in the e-health context, a device acting as the data source is expected to share sensitive personal information with the gateway. Therefore, proxies could perform security attacks over such information without being detected by the DTLS protocol, such as *eavesdropping*, *message manipulation* or *message injection*. In order to face this issue, security at the application layer emerges as a potential solution with the aim of ensuring data protection, even in the presence of proxies. This way, end-to-end security is provided in those IoT scenarios where it is required. At this point, it is worth noting that security solutions at this upper layer could still be employed in combination with other security protocols at another lower layer, such as the DTLS itself, as necessary.

Based on the need of enabling end-to-end security, in the scope of the recently-established LAKE working group, the EDHOC protocol [27] has specially attracted the interest from academia and industry due to its flexibility and lightness to be integrated in constrained environments. Indeed, this protocol is being currently evaluated to be standardised. Specifically, EDHOC is a lightweight key exchange protocol that can be considered as the alternative to the DTLS handshake at the application layer. It aims to establish a security association between two endpoints for enabling further security mechanisms intended to protect their subsequent data communications. Towards this end, EDHOC is based on the use of the *Elliptic Curve Ephemeral Diffie-Hellman* algorithm (ECDHE) [48], which envisages a new ephemeral key pair every time this key exchange protocol is launched. This way, the perfect forward secrecy property is ensured. In turn, the ECDHE algorithm employs *Elliptic Curve Cryptography* (ECC) [10], which leads a lower computational cost for involved endpoints running EDHOC. Furthermore, this protocol defines a three-message exchange to fulfil with its functionality, which must be authenticated in order to identify the involved endpoints and prevent certain security attacks, such as *impersonation*. In this sense, EDHOC supports the same authentication modes as the DTLS handshake protocol, in particular, authentication with pre-shared keys, raw public keys and certificates.

Accordingly, two approaches based on this key exchange protocol are integrated in the architecture presented in this thesis. The first one implements the pure EDHOC approach, while the second one, named CompactEDHOC, represents a reduced version of such approach by extracting the security parameter negotiation and store them in a resource directory entity. Note that, for the sake of clarity, this resource directory component is not included in the Figure 3.2, but its presence is assumed. Accordingly, these EDHOC-based solutions enable the *Data Source* and the corresponding *Gateway* to be able to establish a security association, specifically, a shared symmetric key, by which both entities will encrypt and protect data to be exchanged. It should be pointed out that such security association could be further considered as an enabler to other standardised application-layer security solutions, such as OSCORE [28], which represents part of the future work derived from this thesis.

3.3.2. Secure Group Communications

Following with the Figure 3.2, the second phase of the data sharing process encompasses the exchange of the information received from the *Data Source* between the *Gateway* and the group of interested data-driven *Services*. As already mentioned, this data sharing model is enabled by using a publish/subscribe protocol, such as AMQP [70] or MQTT [71], which envisages the use of a central platform responsible for managing data storing and forwarding among involves entities. Accordingly, traditional security solutions, such as the symmetric and public key cryptography, are not considered, since these approaches were originally designed to protect information exchanges between two entities and not one-to-many communications. Instead, the use of the CP-ABE scheme [9] is considered as a starting point to secure group data sharing. Specifically, this scheme allows to encrypt a piece of information that will be only accessible by the set of authorised entities, which properly fits with data sharing publish/subscribe model envisaged.

Nevertheless, the advantages provided by CP-ABE come at the expense of performance, since it requires to execute highly resource-demanding cryptographic operations to encrypt and decrypt data. Therefore, the direct application of this scheme in IoT scenarios could be limited. In order to overcome this challenge and still leverage flexibility and expressiveness of CP-ABE, a new approach named SymCpAbe is implemented, which combines symmetric key cryptography with attribute-based cryptography to achieve a trade-off between efficiency and scalability. Under this approach, symmetric keys are used to protect data, while these keys are CP-ABE encrypted by using access policies defined by the data owner. Thus, an entity interested in obtaining the original data first needs to decrypt the corresponding symmetric key by using its CP-ABE private key. Then, if its private key satisfies the access policy, the entity will get such symmetric key and, therefore, the original data. Furthermore, SymCpAbe is based on the use of recent IETF standards to represent the cryptographic material. Particularly, *JSON Web Key* (JWK) [51] and *JSON Web Algorithms* (JWA) [50] are employed to represent the required cryptographic keys and algorithms, respectively. This way, interoperability with other security solutions is improved. Consequently, this security approach is integrated in the proposed architecture, with the aim of ensuring end-to-end security in data exchanges between the *Gateway* and the group of interested data-driven *Services*, even in the presence of the intermediate *IoT Platform*.

While SymCpAbe provides an efficient and scalable way to enable security in group communications, this approach requires to extend the *IoT Platform* with new services, in particular, the *ABE Key Generation Service*, the *Symmetric Key Storage Service* and the *ABE Service* (as shown in Figure 3.2). The *ABE Key Generation Service* is responsible for generating the CP-ABE private keys for the data-driven services; the *Symmetric Key Storage Service* stores the CP-ABE encrypted symmetric keys, making them accessible to those entities interested in certain type of protected data; and the *ABE Service* aims to assist the *Gateway* to perform the CP-ABE encryption of the symmetric keys. Additionally, the inclusion of these services gives rise to further aspects to be considered. One of them focuses on the *ABE Service*, which acts as an assistant component intended to encrypt the symmetric keys that will be later employed for data protection. In this case, it is assumed that this service is authenticated and authorized by both the *Publish/Subscribe Service* and the *Symmetric Key Storage*

Service, in order to control access to data. Moreover, the establishment of a symmetric key and its subsequent storage require an additional messages exchange, which potentially involves a greater network overhead. Nevertheless, with SymCpAbe, data are protected by using symmetric cryptography instead of with the CP-ABE scheme, which represents a significant bandwidth saving.

3.3.3. Architecture Instantiation

Once the integrated security solutions have been described, Figure 3.3 shows the instantiation of the proposed architecture, identifying the main interactions among the entities to provide security in the data sharing process.

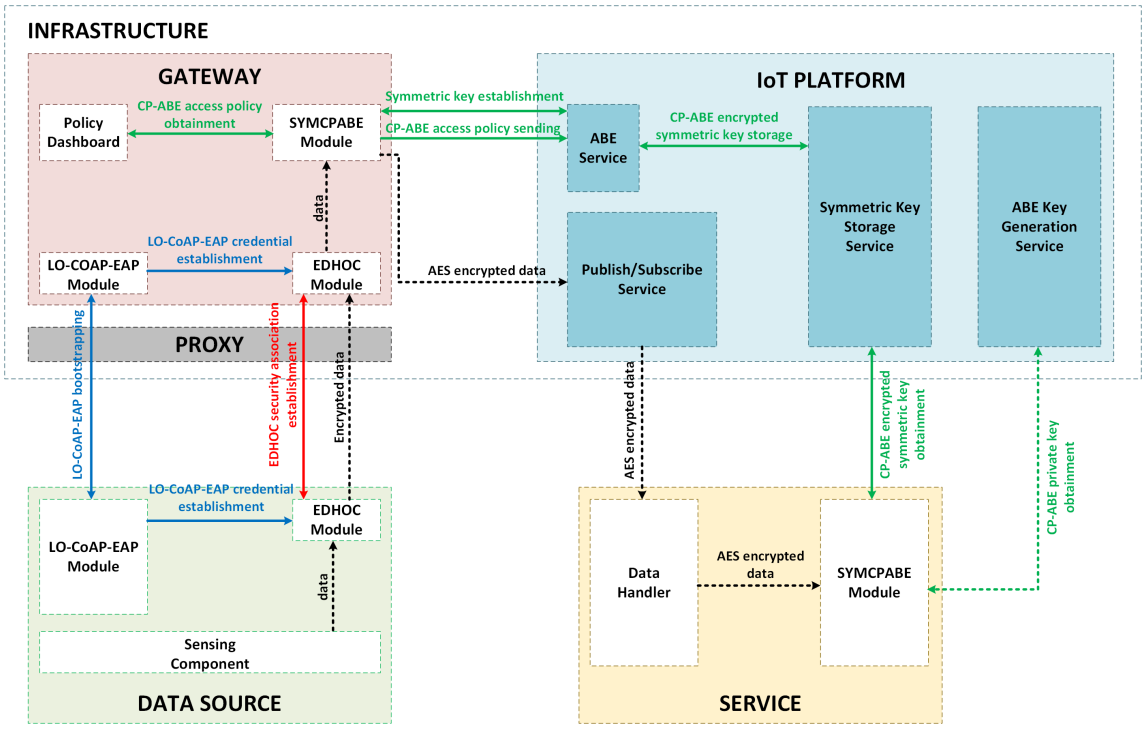

Figure 3.3: Instantiation of the proposed data-centric security architecture

Accordingly, when the *Data Source* is physically deployed in the scenario, this entity firstly runs the bootstrapping process with the corresponding *Gateway*, in order to join to the network and be able to participate in the data sharing process. To do this, both entities make use of their *LO-CoAP-EAP modules*, which allow to complete such bootstrapping process. Once this phase is successfully finished, these modules are also responsible for forwarding certain cryptographic material derived from such bootstrapping process to the *EDHOC modules* of the *Data Source* and the *Gateway*. Subsequently, these entities execute the authentication credential establishment process by employing such cryptographic material, whose result depends on the selected EDHOC authentication mode. Thus, a pre-shared key or the corresponding public keys are set in the *Data Source* and the *Gateway*. When these entities are in possession of their authentication credentials, they launch one of the implemented EDHOC-based solutions, whose messages are encapsulated and transported as CoAP payloads. In case of success, a new security association between the *Data Source* and the *Gateway* is established, in particular, a shared symmetric key, which will be further used to protect their subsequent communications. It should be clarified that such security association should be updated from time to time in order to minimise the amount of data disclosed in case of a successful cyberattack. This updating process only requires to relaunch the corresponding EDHOC-based approach, while the bootstrapping

and the authentication credential establishment are only executed once, concretely, when the data source is deployed in the scenario.

The security association previously established allows the *Data Source* to securely share data about its surrounding environment, which are detected through its *Sensing Component*. Towards this end, its *EDHOC module* protects the sensed data by using the shared symmetric key previously established by the EDHOC-based solution. Then, such encrypted data are sent to the *Gateway* that performs the decryption process in its corresponding *EDHOC module*. The decrypted data are later forwarded to its *SYMCPABE module*, which enables secure group data sharing functionality in the *Gateway*. Once there, the *Gateway* interacts with the *ABE Service* in order to establish a new symmetric key between them. If this process is success, the *Gateway* retrieves the CP-ABE access policy associated to the data coming from the *Data Source*. Note that such access policy has been previously defined in the *Policy Dashboard*, which represents a central point where data owners specify how their information are shared and under what circumstances. Subsequently, the *Gateway* sends the corresponding access policy to the *ABE Service*. This entity encrypts the recent established symmetric key by using the CP-ABE scheme with such policy and then, it stores this encrypted key on the *Symmetric Key Storage Service*. After that, the *Gateway* encrypts data by using the AES algorithm with the symmetric key, and publishes such protected information on the *Publish/Subscribe Service*. It should be pointed that this service is instantiated through the *Orion Context Broker*[8], which is one of the enablers provided by the FIWARE platform. Finally, the group of interested data-driven *Services* receives the protected data, which only can be accessible to those entities whose CP-ABE private key satisfies the access policy employed to encrypt the corresponding symmetric key. To achieve this, such services must have been previously subscribed to receive notification about these data, as well as be in possession of their corresponding CP-ABE private key.

In brief, the previous subsections are focused on specifying the different data-centric security solutions integrating the architecture presented in this thesis. On the one hand, the *Data Source* and the *Gateway* implement the LO-CoAP-EAP and EDHOC-based security approaches, with the aim of establishing security associations that allows to protect their information exchanges. On the other hand, the *Gateway*, the *IoT Platform* and the interested data-driven *Service* deploy the SymCpABE approach, which aims to protect group data communications. Accordingly, the combination of such solutions enables protection of the shared data during their entire lifecycle in IoT scenarios.

3.4. Lessons Learned

The IoT paradigm envisages a hyper-connected world where a plenty of heterogeneous devices are continually shared data about their surrounding environments. Under this perspective, the integration of the IoT in our society is enabling the development of innovative data-driven services, which are aimed to improve people's life quality. In order to fulfil with their functionality, these services are usually based on processing of large amounts of information obtained from different devices, and infer additional knowledge to make more effective decisions accordingly. However, the realization of this data-driven society vision is still challenging due to new security and privacy issues related to the treatment of exchanged information. This aspect is particularly crucial in case of sensitive information, such as personal health data, since an inadequate use of them could even harm people themselves. Therefore, there is a need to consider security solutions that allow to ensure protection of data during its whole lifecycle in IoT scenarios.

In this direction, important standardization bodies, such as the IETF and ETSI, have offered different proposals to overcome security and privacy concerns in IoT scenarios. This fact proves that security and privacy in the IoT context are currently one of the main hot research topics getting rising attention from the academia. Nevertheless, the application of these proposals is not trivial due to the particularities inherent to these scenarios (i.e., technological heterogeneity, devices' resource constraints, presence of proxies and group communications). Therefore, while they are considered as a

[8] `https://fiware-orion.readthedocs.io/en/master/index.html`

good starting point to address security aspects, ensuring end-to-end data protection in IoT scenarios is still challenging.

Accordingly, this thesis has provided a security architecture based on the adaptation and integration of recent and complementary data-centric security solutions. Throughout its realisation, we have achieved the following results:

- Design and development of two lightweight key exchange solutions based on EDHOC, which enable the establishment and updating of end-to-end security associations in IoT scenarios, even in the presence of intermediate entities.
- Design and development of extensions to the LO-CoAP-EAP bootstrapping service, in order to derive and establish the authentication credentials required by the implemented EDHOC-based approaches.
- Design and development of a lightweight, flexible and scalable attribute-based encryption solution combining the CP-ABE scheme and the symmetric key cryptography, in order to enable secure group data sharing.
- Instantiation of the developed security solutions on real resource-constrained devices and the FIWARE platform, with the aim of carrying out an exhaustive evaluation to demonstrate their adequate suitability for IoT scenarios.
- Presentation of the obtained results in different journals and conference publications, and as part of three European research projects: ARMOUR[9], SocIoTal[10] and CHIST-ERA Use-IT[11].

All in all, security and privacy are currently considered as the main barriers to be overcome for increasing people's trust and fostering the deployment of IoT scenarios on a broad scale. Thereby, the data-centric security architecture presented in this thesis represents an excellent starting point to address the main security and privacy concerns in the IoT context, specially for the integration of resource-constrained devices. Eventually, it should be noted that this architecture could be still extended by integrating other complementary approaches, such as OSCORE or authorisation models designed for constrained scenarios, thus achieving secure, flexible and efficient IoT data sharing ecosystems.

[9] `https://www.armour-project.eu/`
[10] `https://cordis.europa.eu/project/id/609112`
[11] `http://useit.eu.org/`

Chapter 4

Publications composing the PhD Thesis

4.1. Protecting Personal Data in IoT Platform Scenarios Through Encryption-Based Selective Disclosure

Title	Protecting Personal Data in IoT Platform Scenarios Through Encryption-Based Selective Disclosure
Authors	José L. Hernández-Ramos, Salvador Pérez, Christine Hennebert, Jorge Bernal Bernabé, Benoit Denis, Alexandre Macabies and Antonio Skarmeta
Type	Journal
Journal	Computer Communications
Impact factor (2018)	2.766
Rank	Q2
Publisher	Elsevier
Volume	130
Pages	20-37
Year	2018
Month	October
ISNN	0140-3664
DOI	10.1016/j.comcom.2018.08.010
URL	https://www.sciencedirect.com/science/article/pii/S0140366418302123
State	Published
Author's contribution	The PhD student, Salvador Pérez Franco, contributed to the architecture design, implementation, results and writing the paper

Abstract

As the Internet of Things evolves, citizens are starting to change the way they share information and communicate with their surrounding environment, enabling a constant, invisible and sometimes unintended information exchange. This trend raises new challenges regarding user's privacy and personal consent about the disclosure of personal data that must be addressed by flexible and scalable mechanisms. Towards this end, this work introduces the concept of bubble, as a coalition or group of smart objects that can be created according to the relationship between their owners. The proposed approach is based on the use of attribute-based encryption to protect the associated data according to users' preferences, and FI-WARE components for deployment purposes. As a scenario example, the solution is integrated with a radio localization system, in order to protect location data in the context of smart buildings. Finally, this work provides implementation details about the required components, as well as their evaluation on real smart environment scenarios.

4.2. A Lightweight and Flexible Encryption Scheme to Protect Sensitive Data in Smart Building Scenarios

Title	A Lightweight and Flexible Encryption Scheme to Protect Sensitive Data in Smart Building Scenarios
Authors	Salvador Pérez, José L. Hernández-Ramos, Sara N. Matheu-García, Domenico Rotondi, Antonio Skarmeta, Leonardo Straniero and Diego Pedone
Type	Journal
Journal	IEEE Access
Impact factor (2018)	4.098
Rank	Q1
Publisher	IEEE
Volume	6
Pages	11738-11750
Year	2018
Month	February
ISNN	2169-3536
DOI	10.1109/ACCESS.2018.2801383
URL	https://ieeexplore.ieee.org/abstract/document/8279412
State	Published
Author's contribution	The PhD student, Salvador Pérez Franco, is the main author of the paper

Abstract

Smart buildings represent key environments to encourage the growth of more sustainable and efficient cities. With the strong development of the Internet of Things (IoT), the integration of heterogeneous physical devices fosters the emergence of data-driven services to make more effective decisions accordingly. However, the need for sharing large amounts of data could help to infer users' sensitive information, such as their daily habits, thus harming their privacy. Under these premises, this paper introduces an encryption scheme based on the lightness of the symmetric cryptography, and the expressiveness of attribute-based encryption. Our proposal aims to ensure only authorised services will be able to access specific pieces of data, so that users' privacy is not compromised, while scalability and efficiency are provided. The resulting scheme has been deployed on a real smart building scenario, and validation results demonstrate its suitability to protect large amounts of sensitive data on IoT-enabled buildings.

4.3. Application Layer Key Establishment for End-to-End Security in IoT

Title	Application Layer Key Establishment for End-to-End Security in IoT
Authors	Salvador Pérez, José L. Hernández-Ramos, Shahid Raza and Antonio Skarmeta
Type	Journal
Journal	IEEE Internet of Things Journal
Impact factor (2020)	9.515
Rank	Q1
Publisher	IEEE
Volume	7
Pages	2117-2128
Year	2019
Month	December
ISNN	2327-4662
DOI	10.1109/JIOT.2019.2959428
URL	https://ieeexplore.ieee.org/abstract/document/8932424
State	Published
Author's contribution	The PhD student, Salvador Pérez Franco, is the main author of the paper

Abstract

In most IoT deployments, intermediate entities are usually employed for efficiency and scalability reasons. These intermediate proxies break end-to-end security when using even the state-of-the-art transport layer security (TLS) solutions. In this direction, the recent Object Security for Constrained RESTful Environments (OSCORE) has been standardized to enable end-to-end security even in the presence of malicious proxies. In this work, we focus on the key establishment process based on application layer techniques. In particular, we evaluate the Ephemeral Diffie-Hellman over COSE (EDHOC), the *de facto* key establishment protocol for OSCORE. Based on EDHOC, we propose CompactEDHOC, as a lightweight alternative, in which negotiation of security parameters is extracted from the core protocol. In addition to providing end-to-end security properties, we perform extensive evaluation using real IoT hardware and simulation tools. Our evaluation results prove EDHOC-based proposals as an effective and efficient approach for the establishment of a security association in IoT constrained scenarios.

4.4. Architecture of Security Association Establishment Based on Bootstrapping Technologies for Enabling Secure IoT Infrastructures

Title	Architecture of Security Association Establishment Based on Bootstrapping Technologies for Enabling Secure IoT Infrastructures
Authors	Salvador Pérez, Dan Garcia-Carrillo, Rafael Marín-López, José L. Hernández-Ramos, Rafael Marín-Pérez and Antonio Skarmeta
Type	Journal
Journal	Future Generation Computer Systems
Impact factor (2019)	5.768
Rank	Q1
Publisher	Elsevier
Volume	95
Pages	570-585
Year	2019
Month	June
ISNN	0167-739X
DOI	10.1016/j.future.2019.01.038
URL	https://www.sciencedirect.com/science/article/pii/S0167739X18325573
State	Published
Author's contribution	The PhD student, Salvador Pérez Franco, is the main author of the paper

Abstract

The next generation of IoT scenarios must consider security aspects as a first class component. As a core aspect, key management is crucial for the establishment of security associations between endpoints. According to it, in this work we propose a novel architecture of security association establishment based on bootstrapping technologies in order to manage the life-cycle of cryptographic keys in IoT. Based on our previous work, we propose a key derivation process by using a lightweight bootstrapping mechanism specifically designed for IoT. Then, the derived cryptographic material is used as an authentication credential of the EDHOC protocol, which represents a standardization effort for key agreement in IoT. EDHOC is an application layer alternative to the DTLS handshake, in order to provide end-to-end security properties even in the presence of intermediate entities, such as proxies. Evaluation results prove the feasibility of our approach, which represents one of the first efforts to consider application layer security approaches for the IoT.

Chapter 5

Bibliography

5.1. References

[1] Moreno Ambrosin, Arman Anzanpour, Mauro Conti, Tooska Dargahi, Sanaz Rahimi Moosavi, Amir M Rahmani, and Pasi Liljeberg. On the Feasibility of Attribute-Based Encryption on Internet of Things Devices. *IEEE Micro*, 36(6):25–35, 2016.

[2] Kevin Ashton et al. That 'Internet of Things' thing. *RFID journal*, 22(7):97–114, 2009.

[3] Nuttapong Attrapadung, Javier Herranz, Fabien Laguillaumie, Benoît Libert, Elie De Panafieu, and Carla Ràfols. Attribute-Based Encryption Schemes with Constant-Size Ciphertexts. *Theoretical computer science*, 422:15–38, 2012.

[4] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The Internet of Things: A Survey. *Computer networks*, 54(15):2787–2805, 2010.

[5] Behcet Sarikaya, Mohit Sethi, and Dan Garcia Carillo. Secure IoT Bootstrapping: A Survey. Internet-Draft draft-sarikaya-t2trg-sbootstrapping-07, Internet Engineering Task Force, July 2019.

[6] Olaf Bergmann, Stefanie Gerdes, Silke Schäfer, Florian Junge, and Carsten Bormann. Secure Bootstrapping of Nodes in a CoAP Network. In *2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pages 220–225. IEEE, 2012.

[7] Gil Bernabeu, Eddie Jaffuel, Bruno Legeard, and Fabien Peureux. MBT for Global Platform Compliance Testing: Experience Report and Lessons Learned. In *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, pages 66–70. IEEE, 2014.

[8] J. Bethencourt, A. Sahai, and B. Waters. CPABE Toolkit, 2011.

[9] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-Policy Attribute-Based Encryption. In *2007 IEEE symposium on security and privacy (SP'07)*, pages 321–334. IEEE, 2007.

[10] Bodo Moeller, Nelson Bolyard, Vipul Gupta, Simon Blake Wilson, and Chris Hawk. Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS). RFC 4492, May 2006.

[11] Carsten Bormann, Mehmet Ersue, and Ari Keranen. Terminology for Constrained-Node Networks. *Internet Engineering Task Force (IETF): Fremont, CA, USA*, pages 2070–1721, 2014.

[12] Carsten Bormann, Mehmet Ersue, and Ari Keränen. Terminology for Constrained-Node Networks. RFC 7228, May 2014.

[13] Carsten Bormann and Paul E. Hoffman. Concise Binary Object Representation (CBOR). RFC 7049, October 2013.

[14] Min Chen, Shiwen Mao, and Yunhao Liu. Big Data: A Survey. *Mobile networks and applications*, 19(2):171–209, 2014.

[15] Timothy Claeys, Franck Rousseau, and Bernard Tourancheau. Securing Complex IoT Platforms with Token Based Access Control and Authenticated Key Establishment. In *2017 International Workshop on Secure Internet of Things (SIoT)*, pages 1–9. IEEE, 2017.

[16] Dan Forsberg, Basavaraj Patil, Alper E. Yegin, Yoshihiro Ohba, and Hannes Tschofenig. Protocol for Carrying Authentication for Network Access (PANA). RFC 5191, May 2008.

[17] Daniel Simon, Dr. Bernard D. Aboba Ph.D., and Pasi Eronen. Extensible Authentication Protocol (EAP) Key Management Framework. RFC 5247, August 2008.

[18] S Das and Y Ohba. Provisioning Credentials for CoAP Applications using EAP, 2012.

[19] Eric Rescorla and Nagendra Modadugu. Datagram Transport Layer Security Version 1.2. RFC 6347, January 2012.

[20] Dan Garcia Carrillo and Rafael Marin Lopez. Lightweight CoAP-Based Bootstrapping Service for the Internet of Things. *Sensors*, 16(3):358, 2016.

[21] Dan Garcia Carrillo, Rafael Marin Lopez, Arunprabhu Kandasamy, and Alexander Pelov. A CoAP-Based Network Access Authentication Service for Low-Power Wide Area Networks: LO-CoAP-EAP. *Sensors*, 17(11):2646, 2017.

[22] Oscar Garcia Morchon, Sye Loong Keoh, Sandeep Kumar, Pedro Moreno Sanchez, Francisco Vidal Meca, and Jan Henrik Ziegeldorf. Securing the IP-Based Internet of Things with HIP and DTLS. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pages 119–124, 2013.

[23] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98, 2006.

[24] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. Application-Layer Security for the WoT: Extending CoAP to Support End-To-End Message Security for Internet-Integrated Sensing Applications. In *International Conference on Wired/Wireless Internet Communication*, pages 140–153. Springer, 2013.

[25] Fuchun Guo, Yi Mu, Willy Susilo, Duncan S Wong, and Vijay Varadharajan. CP-ABE with Constant-Size Keys for Lightweight Devices. *IEEE transactions on information forensics and security*, 9(5):763–771, 2014.

[26] Göran Selander, Francesca Palombini, and Klaus Hartke. Requirements for CoAP End-To-End Security. Internet-Draft draft-hartke-core-e2e-security-reqs-03, Internet Engineering Task Force, July 2017. Work in Progress.

[27] Göran Selander, John Mattsson, and Francesca Palombini. Ephemeral Diffie-Hellman Over COSE (EDHOC). Internet-Draft draft-selander-lake-edhoc-01, Internet Engineering Task Force, March 2020. Work in Progress.

[28] Göran Selander, John Mattsson, Francesca Palombini, and Ludwig Seitz. Object Security for Constrained RESTful Environments (OSCORE). RFC 8613, July 2019.

[29] Göran Selander, John Mattsson, Mališa Vučinić, Michael Richardson, and Aurelio Schellenbaum. Lightweight Authorization for Authenticated Key Exchange. Internet-Draft draft-selander-ace-ake-authz-01, Internet Engineering Task Force, March 2020. Work in Progress.

[30] Darrel Hankerson, Alfred J Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Springer Science & Business Media, 2006.

[31] Dick Hardt et al. The OAuth 2.0 Authorization Framework. Technical report, RFC 6749, October, 2012.

[32] José L Hernández Ramos, Jorge Bernal Bernabé, and Antonio Skarmeta. Army: Architecture for a Secure and Privacy-Aware Lifecycle of Smart Objects in the Internet of Things. *IEEE Communications Magazine*, 54(9):28–35, 2016.

[33] Florian Hess. Efficient Identity Based Signature Schemes based on Pairings. In *International Workshop on Selected Areas in Cryptography*, pages 310–324. Springer, 2002.

[34] René Hummen, Jan H Ziegeldorf, Hossein Shafagh, Shahid Raza, and Klaus Wehrle. Towards Viable Certificate-Based Authentication for the Internet of Things. In *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy*, pages 37–42, 2013.

[35] IoT Analytics. Global number of Connected Devices, 2018.

[36] Jim Schaad. CBOR Object Signing and Encryption (COSE). RFC 8152, July 2017.

[37] Neal Koblitz and Alfred Menezes. Pairing-Based Cryptography at High Security Levels. In *IMA International Conference on Cryptography and Coding*, pages 13–36. Springer, 2005.

[38] Jouni Korhonen. Applying Generic Bootstrapping Architecture for use with Constrained Devices. In *Workshop on Smart Object Security*. Citeseer, 2012.

[39] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brünig, and Georg Carle. DTLS Based Security and Two-Way Authentication for the Internet of Things. *Ad Hoc Networks*, 11(8):2710–2723, 2013.

[40] Alexandros Krontiris. Evaluation of Certificate Enrollment over Application Layer Security, 2018.

[41] Sandeep Kumar, Sye Keoh, and Oscar Garcia Morchon. DTLS Relay for Constrained Environments. *IETF draft, April*, 2014.

[42] Meglena Kuneva. Roundtable on online Data Collection, Targeting and Profiling. *European EC Rapid Press Release, SPEECH/09/156*, 2009.

[43] Marc Langheinrich. Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems. In *International conference on Ubiquitous Computing*, pages 273–291. Springer, 2001.

[44] Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah, and Yacine Challal. Secure and Scalable Cloud-Based Architecture for E-health Wireless Sensor Networks. In *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, pages 1–7. IEEE, 2012.

[45] Huadong Ma, Dong Zhao, and Peiyan Yuan. Opportunities in Mobile Crowd Sensing. *IEEE Communications Magazine*, 52(8):29–35, 2014.

[46] Poonam S. Makeshwar and Govinda Borse. Improving Security in Group Based Data Sharing Using Multicast Key Agreement. *International Journal of Engineering Science and Computing*, 7(02), 2017.

[47] Mališa Vučinić, Göran Selander, John Mattsson, and Dan Garcia Carillo. Requirements for a Lightweight AKE for OSCORE. Internet-Draft draft-ietf-lake-reqs-01, Internet Engineering Task Force, February 2020. Work in Progress.

[48] D McGrew, K Igoe, and Margaret Salter. Fundamental Elliptic Curve Cryptography Algorithms. *Internet Engineering Task Force RFC*, 6090:1–34, 2011.

[49] Kais Mekki, Eddy Bajic, Frederic Chaxel, and Fernand Meyer. A Comparative Study of LPWAN Technologies for Large-Scale IoT Deployment. *ICT express*, 5(1):1–7, 2019.

[50] Michael Jones. JSON Web Algorithms (JWA). RFC 7518, May 2015.

[51] Michael Jones. JSON Web Key (JWK). RFC 7517, May 2015.

[52] Daniel Minoli, Kazem Sohraby, and Benedict Occhiogrosso. IoT Considerations, Requirements, and Architectures for Smart Buildings—Energy Optimization and Next-Generation Building Management Systems. *IEEE Internet of Things Journal*, 4(1):269–283, 2017.

[53] Mobile Ecosystem Forum. The Impact of Trust on IoT, 2016.

[54] Andreas F Molisch, Kannan Balakrishnan, Chia-Chin Chong, Shahriar Emami, Andrew Fort, Johan Karedal, Juergen Kunisch, Hans Schantz, Ulrich Schuster, and Kai Siwiak. IEEE 802.15. 4a Channel Model-Final Report. *IEEE P802*, 15(04):0662, 2004.

[55] Miguel Morales Sandoval and Arturo Diaz Perez. DET-ABE: A Java API for Data Confidentiality and Fine-Grained Access Control from Attribute Based Encryption. In *IFIP International Conference on Information Security Theory and Practice*, pages 104–119. Springer, 2015.

[56] Geoff Mulligan. The 6LoWPAN Architecture. In *Proceedings of the 4th workshop on Embedded networked sensors*, pages 78–82, 2007.

[57] Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, and Mischa Dohler. Standardized Protocol Stack for the Internet of (Important) Things. *IEEE communications surveys & tutorials*, 15(3):1389–1406, 2012.

[58] ETSI Partnership Project oneM2M. Analysis of Security Solutions for oneM2M System. Technical Report, European Telecommunications Standards Institute (NIST), July 2014.

[59] Pablo Picazo Sanchez, Juan E Tapiador, Pedro Peris Lopez, and Guillermo Suarez Tangil. Secure Publish-Subscribe Protocols for Heterogeneous Medical Wireless Body Area Networks. *Sensors*, 14(12):22619–22642, 2014.

[60] Sandro Rafaeli and David Hutchison. A Survey of Key Management for Secure Group Communication. *ACM Computing Surveys (CSUR)*, 35(3):309–329, 2003.

[61] Jose Luis Hernandez Ramos, Dimitrios Geneiatakis, Ioannis Kounelis, Gary Steri, and Igor Nai Fovino. Toward a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data Protection Policies. *IEEE Security & Privacy*, 18:28–38, 2019.

[62] Shahid Raza, Tómas Helgason, Panos Papadimitratos, and Thiemo Voigt. SecureSense: End-to-end Secure Communication Architecture for the Cloud-Connected Internet of Things. *Future Generation Computer Systems*, 77:40–51, 2017.

[63] Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, and Thiemo Voigt. Lithe: Lightweight Secure CoAP for the Internet of Things. *IEEE Sensors Journal*, 13(10):3711–3720, 2013.

[64] Amit Sahai and Brent Waters. Fuzzy Identity-Based Encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 457–473. Springer, 2005.

[65] B Sarikaya. Secure Bootstrapping Solution for Resource-Constrained Devices.

[66] B Sarikaya, Y Ohba, Z Cao, R Cragie, et al. Security Bootstrapping of Resource-Constrained Devices. *Security Bootstrapping of Resource-Constrained Devices*, 2011.

[67] B Sarikaya, Y Ohba, R Moskowitz, Z Cao, and R Cragie. Security Bootstrapping Solution for Resource-Constrained Devices. *RFC*, 2012.

[68] Meena Singh, MA Rajan, VL Shivraj, and P Balamuralidhar. Secure MQTT for Internet of Ihings (IoT). In *2015 Fifth International Conference on Communication Systems and Network Technologies*, pages 746–751. IEEE, 2015.

[69] Nicolas Sornin, Miguel Luis, Thomas Eirich, Thorsten Kramp, and Olivier Hersent. Lorawan Specification Version 1.0. *LoRa Alliance*, 2015.

[70] OASIS Standard. OASIS Advanced Message Queuing Protocol (AMQP) version 1.0. *International Journal of Aerospace Engineering Hindawi www. hindawi. com*, 2018, 2012.

[71] OASIS Standard. MQTT version 3.1. 1. *URL http://docs. oasis-open. org/mqtt/mqtt/v3*, 1, 2014.

[72] Jorg Swetina, Guang Lu, Philip Jacobs, Francois Ennesser, and JaeSeung Song. Toward a Standardized Common M2M Service Layer Platform: Introduction to oneM2M. *IEEE Wireless Communications*, 21(3):20–26, 2014.

[73] Dirk Thatmann, Sebastian Zickau, Alexander Förster, and Axel Küpper. Applying Attribute-Based Encryption on Publish Subscribe Messaging Patterns for the Internet of Things. In *2015 IEEE International Conference on Data Science and Data Intensive Systems*, pages 556–563. IEEE, 2015.

[74] Lyes Touati, Yacine Challal, and Abdelmadjid Bouabdallah. C-Cp-Abe: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things. In *2014 International Conference on Advanced Networking Distributed Systems and Applications*, pages 64–69. IEEE, 2014.

[75] Chun-Wei Tsai, Chin-Feng Lai, Ming-Chao Chiang, and Laurence T Yang. Data Mining for Internet of Things: A Survey. *IEEE Communications Surveys & Tutorials*, 16(1):77–97, 2013.

[76] Mališa Vučinić, Bernard Tourancheau, Franck Rousseau, Andrzej Duda, Laurent Damon, and Roberto Guizzetti. OSCAR: Object Security Architecture for the Internet of Things. *Ad Hoc Networks*, 32:3–16, 2015.

[77] Xinlei Wang, Jianqing Zhang, Eve M Schooler, and Mihaela Ion. Performance Evaluation of Attribute-Based Encryption: Toward Data Privacy in the IoT. In *2014 IEEE International Conference on Communications (ICC)*, pages 725–730. IEEE, 2014.

[78] Rolf H Weber. Internet of Things: New Security and Privacy Challenges. *Computer law & security review*, 26(1):23–30, 2010.

[79] Jie Xu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin. Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing. *IEEE transactions on parallel and distributed systems*, 27(1):119–129, 2015.

[80] Xuanxia Yao, Zhi Chen, and Ye Tian. A Lightweight Attribute-Based Encryption Scheme for the Internet of Things. *Future Generation Computer Systems*, 49:104–112, 2015.

[81] Zach Shelby, Klaus Hartke, and Carsten Bormann. The Constrained Application Protocol (CoAP). RFC 7252, June 2014.

[82] Zach Shelby, Michael Koster, Carsten Bormann, Peter Van der Stok, and Christian Amsüss. CoRE Resource Directory. Internet-Draft draft-ietf-core-resource-directory-23, Internet Engineering Task Force, July 2019.

[83] Zhibin Zhou and Dijiang Huang. An Optimal Key Distribution Scheme for Secure Multicast Group Communication. In *2010 Proceedings IEEE INFOCOM*, pages 1–5. IEEE, 2010.

5.2. Publications

[84] José L Hernández Ramos, Salvador Pérez, Christine Hennebert, Jorge Bernal Bernabé, Benoit Denis, Alexandre Macabies, and Antonio F Skarmeta. Protecting Personal Data in IoT Platform Scenarios Through Encryption-based Selective Disclosure. *Computer Communications*, 130:20–37, 2018.

[85] Sara N Matheu, Salvador Pérez, José L Hernández Ramos, and Antonio Skarmeta. On the Automation of Security Testing for IoT Constrained Scenarios. In *International Workshop on Information Security Applications*, pages 286–298. Springer, 2019.

[86] Sara Nieves Matheu, José Luis Hernández Ramos, Salvador Pérez, and Antonio F Skarmeta. Extending MUD Profiles Through an Automated IoT Security Testing Methodology. *IEEE Access*, 7:149444–149463, 2019.

[87] Salvador Pérez, Dan Garcia Carrillo, Rafael Marín López, José L Hernández Ramos, Rafael Marín Pérez, and Antonio F Skarmeta. Architecture of Security Association Establishment based on Bootstrapping Technologies for Enabling Secure IoT Infrastructures. *Future Generation Computer Systems*, 95:570–585, 2019.

[88] Salvador Pérez, José L Hernández Ramos, Sara N Matheu García, Domenico Rotondi, Antonio F Skarmeta, Leonardo Straniero, and Diego Pedone. A Lightweight and Flexible Encryption Scheme to Protect Sensitive Data in Smart Building Scenarios. *IEEE Access*, 6:11738–11750, 2018.

[89] Salvador Pérez, José L Hernández Ramos, Diego Pedone, Domenico Rotondi, Leonardo Straniero, and Antonio F Skarmeta. A Digital Envelope Approach Using Attribute-Based Encryption for Secure Data Exchange in IoT Scenarios. In *2017 Global Internet of Things Summit (GIoTS)*, pages 1–6. IEEE, 2017.

[90] Salvador Pérez, José L Hernández Ramos, Shahid Raza, and Antonio Skarmeta. Application Layer Key Establishment for End-to-End Security in IoT. *IEEE Internet of Things Journal*, 7(3):2117–2128, 2019.

[91] Salvador Pérez, Juan A Martínez, Antonio F Skarmeta, Márcio Mateus, Bruno Almeida, and Pedro Maló. ARMOUR: Large-scale Experiments for IoT Security & Trust. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 553–558. IEEE, 2016.

[92] Salvador Pérez, Domenico Rotondi, Diego Pedone, Leonardo Straniero, María José Núñez, and Fernando Gigante. Towards the CP-ABE Application for Privacy-Preserving Secure Data Sharing in IoT Contexts. In *International conference on innovative mobile and internet services in ubiquitous computing*, pages 917–926. Springer, 2017.

[93] Ramon Sanchez Iborra, Jesús Sánchez Gómez, Salvador Pérez, Pedro J Fernández, José Santa, José L Hernández Ramos, and Antonio F Skarmeta. Enhancing LoRaWAN Security Through a Lightweight and Authenticated Key Management Approach. *Sensors*, 18(6):1833, 2018.

[94] Ramon Sanchez Iborra, Jesús Sánchez Gómez, Salvador Pérez, Pedro J Fernández, José Santa, José L Hernández Ramos, and Antonio F Skarmeta. Internet Access for LoRaWAN Devices Considering Security Issues. In *2018 Global Internet of Things Summit (GIoTS)*, pages 1–6. IEEE, 2018.