Atenea Lab: Un laboratorio de IoT basado en software para formación, investigación y transferencia de conocimiento

Marta Fuentes-García
COSCYBER, Fidesol
Granada, España
mfuentes@fidesol.org

Celia Fernández
COSCYBER, Fidesol
Granada, España
cfernandez@fidesol.org

Marina Torres
Fever
Granada, España

Luis El-Moga-Sarria
COSCYBER, Fidesol
Granada, España
lmoga@fidesol.org

Francisco L. Benítez-Martínez
COSCYBER, Fidesol
Granada, España
flbenitez@fidesol.org

***Resumen*—La cuarta Revolución Industrial ha tenido una fuerte explosión durante los últimos años. Muchas organizaciones invierten cada vez más dinero en la Transformación Digital. Una de las principales tendencias es el uso de sensores para mejorar los procesos industriales, como parte del llamado internet de las cosas (IoT) industrial. La formación y experimentación en este tipo de tecnologías es cada vez más una necesidad, ya que permite abordar las particularidades de estos entornos desde una perspectiva más realista y práctica. Disponer de una plataforma intermedia para realizar pruebas o experimentos antes del despliegue del ecosistema IoT completo sería interesante tanto a nivel empresarial como académico.**

Atenea Lab es una plataforma basada en software que permite simular un amplio rango de escenarios IoT realistas, facilitando tanto la formación como la transferencia de conocimiento al tejido productivo.

***Index Terms*—IoT, laboratorio, investigación, formación, testbed, transferencia de conocimiento**

Tipo de contribución: *Formación e innovación educativa (límite 8 páginas)*

I. Introducción

La Industria 4.0 ha dejado de ser futuro para ser una realidad durante los últimos años. Cada vez más organizaciones abrazan la revolución y desean aplicar nuevas tecnologías a su ciclo de proceso de producción. Incluso las pequeñas y medianas empresas (pymes) han comenzado a adoptar nuevas soluciones como el internet de las cosas (IoT, del inglés, *Internet of Things*) para optimizar y mejorar sus productos. Hay un amplio rango de áreas en los que se aplica el IoT (p. Ej. agricultura, fabricación o salud). En el caso particular de España (en concreto, en Andalucía), una de las principales bases para reactivar la economía después de la crisis que estamos sufriendo apunta hacia la optimización de técnicas de cultivo [1]. Por esta razón, desplegar sensores en zonas agrarias y utilizar IoT como mecanismo de monitorización podría implicar un enorme avance en este sector [2], [3]. Esto es solo un ejemplo sobre cómo la Cuarta Revolución Industrial está alcanzando todos los ámbitos de nuestra sociedad.

Sin embargo, a veces la inversión en el diseño y despliegue de un sistema IoT podría no identificarse desde en un primer vistazo como un beneficio potencial a medio-largo plazo. Además, es necesario tener en cuenta la necesidad de expertos que pongan en valor los datos recopilados y los interpreten de manera adecuada.

Esta revolución se ha visto acelerada debido a las situaciones derivadas del COVID y la guerra de Ucrania. Adicionalmente, la rápida evolución de las técnicas de inteligencia artificial (IA) ha propiciado que, en ocasiones, la ciberseguridad no avance al mismo ritmo que lo hacen la tecnología o los cibercriminales. Esto afecta particularmente al contexto del IoT, debido a que los dispositivos tienen recursos restringidos y a su naturaleza dinámica. La mayoría de las soluciones existentes fueron diseñadas para redes tradicionales y necesitan ser adaptadas a los entornos actuales [4]. Además, estas soluciones suelen ser caras y difíciles de costear para las pymes.

Por otra parte, la creciente demanda de soluciones basadas en IoT pone de manifiesto la necesidad de disponer de personal cualificado, formado en este tipo de tecnologías [5]. Esta formación debería ser fundamentalmente práctica, lo cual puede llegar a ser costoso. Si además está relacionada con ciberseguridad para ecosistemas IoT, el escenario es aún más complejo, ya que la experimentación es un factor clave y no puede llevarse a cabo en entornos productivos.

I-A. Motivación

En Fidesol existe una gran variedad de proyectos, algunos de ellos relacionados con el IoT. En este tipo de proyectos, es interesante tener la posibilidad de llevar a cabo un primer despliegue que permita tener una idea de cómo funcionará el trabajo. Nosotros creemos que esto debería ser algo similar a un boceto o maqueta. ***EGIDA "primera Red Cervera para la protección de la privacidad"***[1] fue un tipo de proyecto particular donde era necesario desarrollar distintos sub-proyectos y prototipos, que podían ser desplegados en distintos sectores (p. Ej. industria o alimentación).

Por otra parte, hay una estrecha relación con varios grupos de investigación en distintas universidades y centros tecnológicos, permitiendo conocer de primera mano las necesidades formativas y experimentales que se presentan en estos entornos (tanto a nivel universitario como de investigación).

Todo esto nos motivó a diseñar un laboratorio de IoT que fuera capaz de simular distintos casos de uso y nos permitiera probar nuestras soluciones, así como llevar a cabo la propia experimentación que forma parte esencial de la investigación, facilitando al mismo tiempo la formación práctica en el contexto del IoT. Como resultado de EGIDA, se desarrolló ***Atenea Lab***, una primera versión de este laboratorio en forma

[1] https://egidacybersecurity.com/

de prototipo. En la actualidad, gracias al proyecto ***CICERO "Contramedidas inteligentes de ciberseguridad para la red del futuro"***, está previsto evolucionar y mejorar Atenea Lab para que sea accesible y permita colaborar activamente con el resto de centros que forman esta nueva red.

En este artículo se presenta Atenea Lab como herramienta de formación y testbed, describiendo sus principales características actuales, así como la propuesta de evolución enmarcada en CICERO.

I-B. Propuesta y puntos clave

La idea fundamental consiste en crear un laboratorio de IoT que permita desarrollar diferentes entornos de IoT. El principal objetivo es ser capaces de simular distintos dispositivos y protocolos de comunicación para reproducir escenarios de la vida real de forma controlada. En la Tabla I se resumen las funcionalidades deseadas, el estado actual y el estado previsto tras la finalización de CICERO.

I-C. Contribución

Así, los objetivos y necesidades de Atenea Lab son:

- Ser un **puente** entre investigación básica (experimentos teórico-prácticos) y prototipos (algunos de ellos desplegados en el mundo real).
  - Favorecer la **formación práctica** en entornos IoT controlados y seguros.
  - Proporcionar un **testbed multi-escenario** que permita realizar pruebas y experimentación de forma segura, así como la generación de conjuntos de datos basados en ecosistemas IoT.
- Proporcionar una **abstracción** de los dispositivos que solo tiene en cuenta sus características más relevantes, como, por ejemplo: consumo de energía, vida de la batería o comportamiento. Esto implica que no es necesario simular el hardware ni los componentes específicos (p. Ej. Marcas o procesadores concretos).
- Tener una especie de **Lego®**[2] donde sea posible construir escenario que sea necesario de forma realista. Además, con este enfoque se gana flexibilidad y versatilidad para construir casos de uso de cualquier forma.
- Ser capaces de **implementar soluciones propias** una vez simulado el caso de uso. Se podrán lanzar experimentos (previamente diseñados) y evaluar su rendimiento.

El resto del artículo se organiza como sigue. En la Sección II se revisa el estado del arte y el trabajo relacionado con la propuesta. En la Sección III se presenta Atenea Lab, describiendo el concepto, definición y arquitectura de alto nivel. En la Sección V se exponen las líneas de trabajo futuro y las acciones previstas como parte de CICERO. Finalmente, en la Sección VI se presentan las principales conclusiones de este artículo.

II. Estado del arte

El uso de dispositivos IoT ha crecido exponencialmente durante los últimos años. Este incremento ha sido particularmente relevante para aquellas industrias que pretendían optimizar su producción y monitorizar sus actividades. Sin embargo, antes de desplegar un ecosistema IoT, sería recomendable probar el diseño propuesto. Para hacerlo, hay diferentes opciones. Una de estas opciones consiste en contratar compañías externas, que suelen estar limitadas por el estándar IO-link [6]. Otra alternativa es probar los sensores en un entorno físico controlado, bajo condiciones simuladas, como es el caso de *IoT Lab*[3], que fue desarrollado como resultado de un proyecto europeo, Urbana IoT Lab[4], o *Laboratorio de internet de las cosas (IoT)*[5]. Sin embargo, este tipo de soluciones suelen ser caras y complejas de adoptar. Por esta razón, ha habido numerosas propuestas con el objetivo de simular condiciones real utilizando software en lugar de entornos físicos [7]–[10].

Así, por ejemplo, *IoT Device Simulator* permite conectar un gran número de dispositivos y proporciona una solución flexible y escalable que simula la arquitectura IoT utilizando software[6]. Es necesario pagar para utilizar esta solución en función de la cantidad de horas al día que se ejecuta la simulación y el número de dispositivos simulados. Otras soluciones se centran en la simulación de datos, para generar tanto valores de sensores como emular posibles problemas durante la conexión[7]. Por otra parte, *OMNeT++* es un software de simulación para IoT masivo, desarrollado utilizando C++ y siguiendo una arquitectura basada en componentes. Uno de los principales usos de esta solución es estudiar problemas de la red [7]. *FLoRaSaT* es una solución basada en OMNeT++ que se utiliza para simular entornos IoT utilizando el protocolo estándar LoRaWAN Low-Power Wide Area (LPWAN) [8]. Ambas soluciones están restringidas a protocolos de comunicación específicos y el escenario permite una cantidad reducida de dispositivos [7], [8]. Otros autores proponen soluciones que pretenden generar una gran cantidad de datos 5G [9] o simular el código que se ejecutará en las capas reales de la arquitectura IoT [10]. La primera puede generar un gran número de dispositivos IoT y permite interactuar con el mundo real. La segunda se centra en características de bajo nivel, como los detalles de la red de comunicaciones. Por último, *VIoLET* es un entorno para simulación IoT a gran escala que utiliza máquinas virtuales [11].

Desde el punto de vista de la formación y la experimentación en investigación, además de algunas de las herramientas anteriores, también existen algunas soluciones que podrían ser útiles para simular escenarios IoT. Por ejemplo, AWS[8] permite simular múltiples dispositivos y realizar pruebas escalables mediante una interfaz de usuario. Las simulaciones tienen un coste en función del servicio y las horas de uso[9], por lo que realmente no es una solución práctica para formación o investigación. MQTT Labs[10] permite simular varios entornos IoT empleando como protocolo de comunicación MQTT. Entre otras, proporcionan funcionalidades de prototipado rápido o monitorización de IoT. Disponen de una versión de

[2]https://bit.ly/3YX6u4r, https://en.wikipedia.org/wiki/Lego

[3]https://iotlab.com/es/

[4]https://urbanasmart.com/iot-lab/

[5]https://bit.ly/3Nzsf7U

[6]https://go.aws/3XdfdzO

[7]https://bit.ly/3NALApi

[8]https://aws.amazon.com/es/solutions/implementations/iot-device-simulator/

[9]https://docs.aws.amazon.com/solutions/latest/iot-device-simulator/cost.html

[10]https://mqttlab.iotsim.io/

Tabla I
FUNCIONALIDADES DE ATENEA LAB. ESTADO ACTUAL Y PREVISTO (2025)

Funcionalidad/ Objetivo	Estado actual	Estado previsto (2025)
Formación e investigación experimental en entornos IoT	X	✓
Generación de conjuntos de datos realistas para investigación	✓	✓
Transferencia de conocimiento desde investigación base hasta industria	✓	✓
Diseño y prueba de soluciones IoT para clientes, permitiendo reducir costes	X	✓
Diseño y prueba de soluciones de ciberseguridad IoT en entornos controlados y aislados (testbed)	✓	✓
Acceso multiusuario para poder trabajar de forma colaborativa	X	✓
Integración e interoperabilidad con herramientas externas	X	✓

prueba y otra de pago[11]. IoT Lab[12] es un testbed de libre acceso que permite construir escenarios IoT utilizando el protocolo de comunicación MQTT y que soporta varios tipos de dispositivos[13] y redes de comunicación por radio reales.

La mayoría de las soluciones mencionadas tienen al menos una de las siguientes limitaciones: carecen de una interfaz gráfica de usuario usable (GUI, del inglés, *Graphical User Interface*), presentan altos costes (especialmente para propósitos de investigación o pymes) y/o tienen posibilidades limitadas de investigación.

III. NUESTRA PROPUESTA: ATENEA LAB

Existen diferentes arquitecturas para entornos IoT [12]–[15]. Atenea Lab se alinea con la última, que propone las siguientes capas y se representa en la Figura 1:

- **Capa física** (p. Ej. Sensores). También se conoce por otros autores como capa de ”percepción”. En esta capa es donde se generan los datos, que son capturados por los sensores.
- **Capa de comunicaciones**. En esta capa es donde se produce el intercambio de datos, es decir, se envían desde el dispositivo/sensor que los genera hasta donde serán procesados para convertirlos en información. Además del transporte de datos, también se llevan a cabo otras tareas como la unificación del formato.
- **Capa de gestión**. Esta capa permite a los dispositivos unirse al entorno o almacenar valores en una base de datos.
- **Capa de aplicación y analítica**. En esta capa se llevan a cabo tareas como el procesamiento de datos para extraer conocimiento (p. Ej. visualización de datos, construcción de modelos de aprendizaje automático o realización de análisis e informes).

Construir un laboratorio de IoT no es un procedimiento fácil, más aún si se quiere tener una abstracción que permita implementar cualquier caso de uso. Por esta razón, se planteó un diseño y desarrollo incremental del laboratorio. Para ello, comenzamos con un caso de uso simplificado basado en el sector agroalimentario. De esta forma, identificamos cuáles eran los elementos mínimos que necesitaban ser cubiertos para construir un escenario completo. Así: un entorno IoT se compone de **dispositivos**, que se conectan mediante un **protocolo de comunicación** que les permite enviar sus valores a un centro de procesamiento. Además, cada dispositivo IoT debería tener al menos un **sensor**, que se encarga de detectar y medir los valores de interés. El escenario más

[11]https://www.gambitcomm.com/site/mqttsimulator.php
[12]https://iot-lab.github.io/
[13]https://iot-lab.github.io/docs/boards/overview/

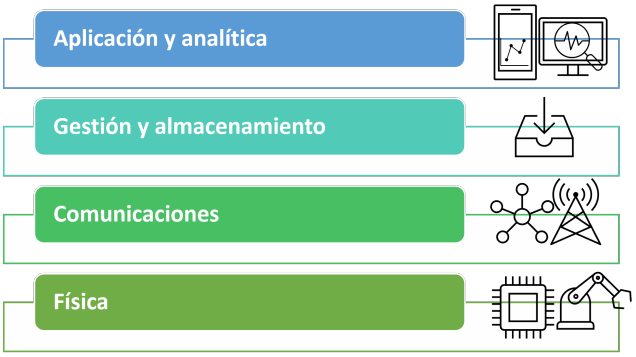

Figura 1. Capas IoT cubiertas por Atenea Lab

reducido de IoT podría ser un dispositivo con un sensor (p. Ej. Sensor de temperatura) que envía los valores medidos a un dispositivo final (p. Ej. Servidor o teléfono inteligente) para su procesamiento. Para enviar los valores, es necesario implementar un protocolo de comunicación. Finalmente, los valores deberían ser almacenados en un **medio persistente**.

De acuerdo con este primer caso de uso, diseñamos y desarrollamos la primera versión del Atenea Lab. Este prototipo funcional tiene las siguientes características:

- **Capa física**. Permite añadir dispositivos, que se componen de al menos un sensor y tienen una función de simulación de comportamiento asignada.
- **Capa de comunicaciones**. Actualmente implementa el protocolo MQTT, que es uno de los protocolos de comunicación más extendidos en entornos IoT. Es posible implementar protocolos de comunicación distintos (actualmente requiere intervención del equipo de desarrollo).
- **Capa de gestión y almacenamiento**. Actualmente dispone de una instancia de Mongo DB ejecutándose para el almacenamiento persistente de los datos recibidos. Es posible conectar con otras bases de datos (actualmente requiere intervención del equipo de desarrollo).
- **Capa de aplicación y analítica**. Implementa una GUI intuitiva, usable y centrada en el usuario que permite construir y editar escenarios IoT, así como visualizar los resultados de simulación tras ejecutar los escenarios.

Los siguientes párrafos describen la forma en que se ha construido el Atenea Lab.

III-A. Arquitectura

Atenea Lab fue pensado y diseñado con un único objetivo en mente: alcanzar una abstracción de los dispositivos IoT que pudiera ser personalizada y/o configurada para simular el

comportamiento y principales recursos de estos dispositivos. Para lograrlo, se propuso seguir un enfoque **Lego®** en el que se tienen diferentes ”piezas” que, no siendo una representación fiel al mundo real, proporcionan un escenario **realístico**. Además, estas ”piezas” permiten construir distintos casos de uso, que abarcan desde el sector agroalimentario hasta la industria (IIoT), incluyendo además otras posibilidades como e-salud o domótica. Otro elemento clave de la solución consiste en tener un conjunto de protocolos disponible para utilizar junto con los dispositivos, como una especie de ”pegamento” que permite la comunicación entre dispositivos y ordenadores de borde (p. Ej. Servidores u ordenadores personales).

La arquitectura de la solución fue diseñada y desarrollada siguiendo un enfoque basado en componentes para proporcionar independencia a lo largo de las capas. Por eso, está construida utilizando contenedores, donde cada elemento se ejecuta de forma aislada con respecto al resto. Esto permite al sistema crecer horizontalmente y desplegar redes IoT complejas de una forma sencilla. Además, proporciona **independencia**, **flexibilidad** y **escalabilidad** al laboratorio, haciendo posible incluir de forma fácil diferentes protocolos de comunicación y nuevas bases de datos en el futuro.

Así, la arquitectura de la solución permite a los usuarios generar una amplia variedad de entornos IoT simulados, donde su principal estructura se describe como sigue:

- **Entorno**. Un entorno es un escenario donde el usuario puede definir las ejecuciones durante un tiempo dado. Esta configuración incluye una descripción, el protocolo de comunicación empleado y el tipo de base de datos. En esta versión, solo es posible seleccionar el protocolo MQTT y la base de datos Mongo DB. En el futuro se incluirán nuevos protocolos y bases de datos a demanda.
- **Dispositivo**. Los dispositivos pertenecen a un entorno. Se pueden configurar uno o más dispositivos con ciertas propiedades, como nombre, descripción y lista de sensores adjuntos. Cada dispositivo se compone al menos de un sensor.
- **Sensor**. Los sensores son la unidad mínima de funcionamiento del Atenea Lab. Un sensor se define como una entidad con varias propiedades, incluyendo un nombre y una descripción significativos, tipos de datos, unidades, valores e intervalo de generación de datos. También se asigna una función de generación de comportamiento a cada sensor, que envía los datos generados utilizando paquetes binarios muy pequeños para simular condiciones de tiempo reales.

Mediante la creación y combinación de los elementos indicados, se pueden simular una gran variedad de escenarios. Para definir un escenario se requiere al menos un elemento de cada tipo.

III-B. Diseño centrado en el usuario

Uno de las principales causas de la falta de aceptación del software es la carencia de un enfoque centrado en el usuario y el descuido de la experiencia de usuario [16]. Por esta razón, Atenea Lab fue diseñado e implementado siguiendo ***scrum***[14] como metodología ágil, y teniendo en cuenta lo siguiente [17]–[19]:

- **Necesidades** del usuario. Al comienzo del proyecto, se elaboró una lista con las necesidades y funcionalidades del laboratorio. Para ello, se contó con la colaboración de investigadores relacionados con el ámbito de IoT e inteligencia artificial. El listado se elaboró teniendo en cuenta tanto la perspectiva de investigación como la de formación. También al inicio del proyecto se priorizaron las funcionalidades más relevantes para los investigadores (usuario) con el propósito de acotar el alcance.
- **Usabilidad y experiencia de usuario**. Estos aspectos son clave en el diseño centrado en el usuario y por eso los investigadores participaron también en la definición del flujo de trabajo, diseño y validación de la GUI. En concreto, la interfaz de usuario se diseñó siguiendo una filosofía minimalista y altamente funcional, fruto de la colaboración entre diseñador de producto, investigadores y desarrolladores.
- **Validación y pruebas** por parte del usuario. Durante todo el proyecto se llevó a cabo un seguimiento continuo de la evolución del laboratorio, así como realización de pruebas periódicas en el contexto de *sprint review/demo*[15] por parte uno de los investigadores participantes en la definición de necesidades (requisitos) del usuario.

Como resultado de lo anterior, se obtuvo un laboratorio funcional, diseñado por y para el usuario con un cuadro de mandos interactivo que permite configurar un escenario IoT personalizado de forma simple y fácil.

III-C. Uso

Para utilizar Atenea Lab, es necesario crear un escenario, incluyendo: nombre, descripción, protocolo de comunicación y base de datos. Una vez se ha creado el entorno, es posible construir un conjunto de sensores y dispositivos de forma fácil mediante un asistente de instalación interactivo. Durante el proceso, se solicita al usuario que proporcione un nombre y descripción para cada dispositivo y sensor. Para los sensores es necesario completar información adicional, incluyendo: tipo de medición, unidades, rango de mediciones y tipo de funciones de generación de comportamiento. En esta versión de Atenea Lab las funciones de comportamiento son:

- **Constante**. Devuelve el mismo valor durante toda la ejecución.
- **Función lineal**. Requiere un valor inicial y un incremento.
- **Valores aleatorios**. Se genera un valor completamente aleatorio en un intervalo dado en cada medición.
- **Valores basados en trigonometría**. Calcula un valor utilizando funciones trigonométricas (seno, coseno, seno exponencial, coseno exponencial). Este tipo de funciones son útiles para simular comportamientos más complejos, como degradación de temperatura u consumo de combustible.

Las funciones disponibles pueden ser fácilmente ampliadas para definir otro tipo de comportamientos, tanto sencillos como complejos (requiere intervención del equipo de desarrollo).

[14]https://www.scrum.org/

[15]https://www.scrum.org/resources/blog/sprint-review-much-more-just-demo

Después de que todos los dispositivos y sensores sean configurados de forma adecuada, el entorno puede ser iniciado. El sistema despliega automáticamente un conjunto de contenedores en la infraestructura y comienza la generación de datos. Después del periodo de tiempo fijado en el entorno, la ejecución se detiene automáticamente. También puede ser detenida o pausada de forma manual.

En la Figura 2 se muestra el flujo de ejecución tras desplegar un entorno, tomando como ejemplo de protocolo MQTT y de base de datos MongoDB. Este flujo, de forma general, es el que sigue: *1)* para cada sensor de un dispositivo, se crea un hilo de ejecución donde, periódicamente (siguiendo la frecuencia fijada), se lee un valor según la función matemática configurada para el comportamiento; *2)* cada medición se envía utilizando el protocolo de comunicación seleccionado, *3)* el protocolo desempaqueta los datos y envía la información a la base de datos a través de la API y *4)* los datos recogidos pueden analizarse posteriormente consultando esta base de datos mediante la interfaz proporcionada o bien ser descargados para utilizarlos fuera del laboratorio. Se puede encontrar una demostración práctica en https://bit.ly/AteneaLabDemo.

IV. Atenea Lab en acción

Con el objetivo de validar el funcionamiento de esta primera versión de Atenea Lab, se realizaron pruebas de dos tipos: *i)* rendimiento y *ii)* uso. El propósito era comprobar no solo si el laboratorio funcionaba adecuadamente sino también encontrar posibles limitaciones y puntos de mejora, ayudando a definir los próximos pasos y líneas de acción para futuras versiones. En los próximos párrafos se resumen estas pruebas y los resultados obtenidos.

IV-A. Pruebas de rendimiento

Para comprobar el rendimiento, Atenea Lab fue probado bajo diferentes condiciones de estrés: incrementando la frecuencia de envío de datos y definiendo un alto número de sensores y dispositivos para verificar su precisión y rendimiento. Estas condiciones se definieron teniendo en cuenta qué aspectos podrían afectar a la efectividad de las comunicaciones por distintas causas. Algunas de las principales limitaciones encontradas fueron las siguientes:

- **Pérdida de datos**. Al definir una alta frecuencia de envío de datos (1 segundo), un número mediano de dispositivos (9 dispositivos) y un alto número de sensores (18 sensores/dispositivo), es posible que se pierdan algunos datos. Esto se debe a que el *broker* MQTT no puede gestionar tal cantidad de datos a un alto ritmo. Sin embargo, esto podría no ser realista, ya que la mayoría de las veces no es necesario enviar la información de manera tan frecuente ni tal cantidad de sensores.
- **Reducción del ancho de banda**. Cuando hay un alto número de sensores y dispositivos definido y la frecuencia de envío de datos es elevada, la recepción de mensajes por los suscriptores podría verse retrasada. En cualquier caso, los mensajes se reciben y almacenan de forma ordenada en la base de datos.

Como conclusión preliminar, se puede comprobar que el laboratorio presenta una buena respuesta a las pruebas de estrés realizadas y tolerancia a fallos aceptable. Sin embargo, sería conveniente realizar una mayor cantidad de tests que permitieran obtener el punto exacto en el que comienza a degradarse el rendimiento (pérdida de datos y reducción de ancho de banda significativos).

IV-B. Pruebas de uso: testbed para investigación en ciberseguridad

Además de las pruebas de validación y demostraciones periódicas con el investigador (usuario de prueba), se implementó el caso de uso básico que sirvió de punto de referencia para el diseño conceptual de Atenea Lab. De esta forma, fue posible comprobar de forma controlada que, efectivamente, el laboratorio funciona. Para ello, se seleccionó un escenario relacionado con el sector agroalimentario. La razón es que el sector primario es uno de los más relevantes en Andalucía, siendo una de las áreas más importantes en este sector la agricultura.

El escenario propuesto disponía de dos dispositivos: uno para mediciones en el ambiente (*DA*) y otro para el suelo (*DS*). Cada dispositivo contaba con un sensor de temperatura (*STA* y *STS*, respectivamente) y otro de humedad (*SHA* y *SHS*, respectivamente), cuyos valores eran simulados mediante una función de comportamiento que generaba valores en un rango dado. Para las comunicaciones y el almacenamiento se utilizaron las opciones disponibles: MQTT y MongoDB. Por cada dispositivo existía un publicador MQTT que enviaba los datos generados por los sensores al *broker* MQTT. Un suscriptor leía los datos recopilados y los almacenaba en la base de datos. El escenario se ejecutó durante varios periodos de tiempo (p. Ej. 1 hora, 1 día, 1 semana...) para verificar que funcionaba adecuadamente, esto es, que los datos eran generados, enviados y almacenados correctamente. En la Figura 3 se muestra parte del contenido de la base de datos tras realizar una de las simulaciones. Se puede observar que se capturaron valores para todos los sensores de los dos dispositivos mediante los *topics* de MQTT *ATENEA/DA/STA* (sensor de temperatura dentro del dispositivo de medición del ambiente), *ATENEA/DA/SHA* (sensor de humedad dentro del dispositivo de medición del ambiente), *ATENEA/DS/SHS* (sensor de temperatura dentro del dispositivo de medición del suelo) y *ATENEA/DS/STS* (sensor de humedad dentro del dispositivo de medición del suelo). Además del valor y el *topic* correspondiente, también se almacenó el sello temporal, para saber en qué momento se generó cada valor, permitiendo así trabajar con series temporales y tener trazabilidad de la simulación.

Por otra parte, en el contexto del proyecto EGIDA[16], y en colaboración con la Universidad de Granada (UGR), se desarrolló un prototipo para la detección de anomalías en el tráfico de red para el sector agroalimentario. De esta forma, fue posible aplicar por primera vez el sensor MSNM (MSNM-S)[17] en un escenario basado en IoT [20], [21], demostrando además la efectividad del laboratorio como testbed para investigación y formación en ciberseguridad.

Para probar el funcionamiento de este prototipo, se inició la simulación del escenario completo, incluyendo el MSNM-S y capturando datos bajo condiciones de operación normales. Finalmente, se lanzaron ataques controlados de denegación

[16]https://egidacybersecurity.com/

[17]https://github.com/nesg-ugr/msnm-sensor

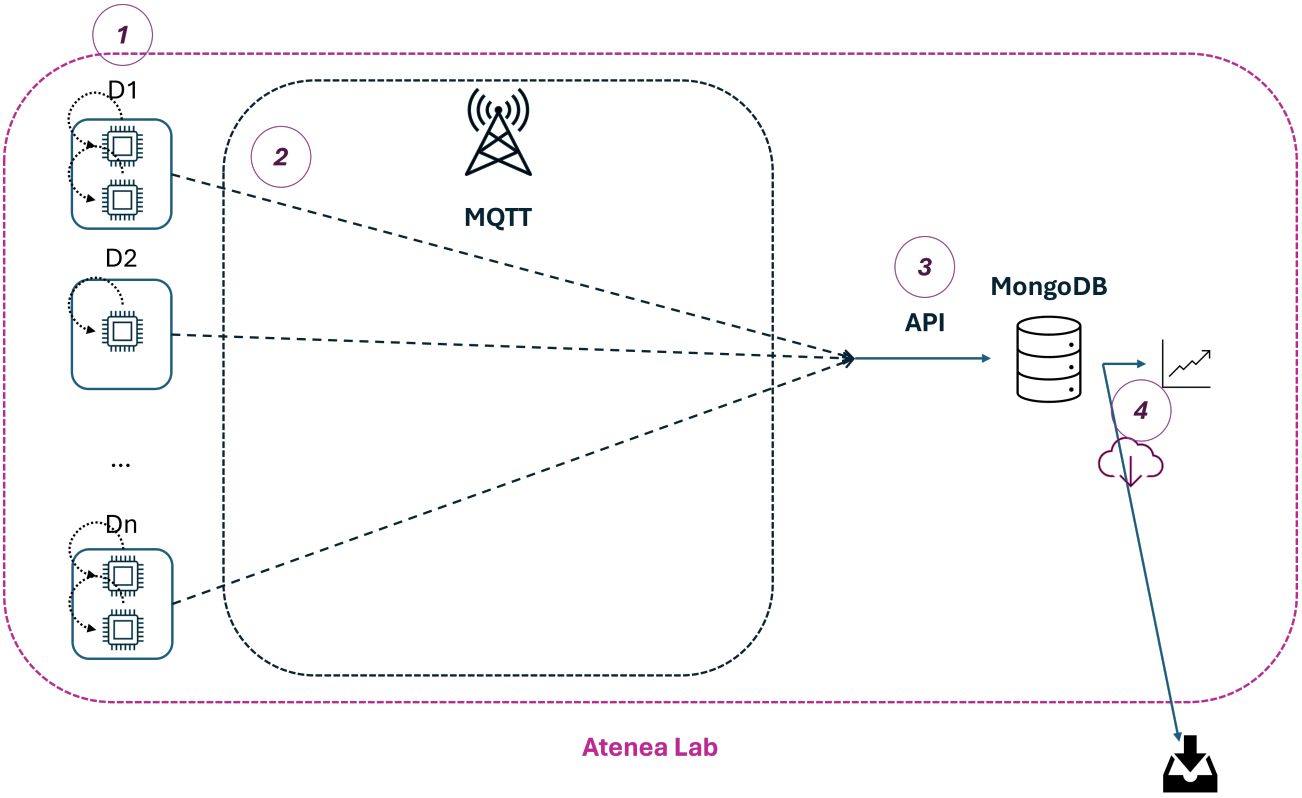

Figura 2. Flujo de ejecución de Atenea Lab: *1)* Generación de valor (medición), *2)* Envío de la medición utilizando el protocolo de comunicación seleccionado, *3)* Envío a la base de datos a través de la API y *4)* Explotación de los datos recogidos

de servicio [20] y de exfiltración de datos [21] para probar la capacidad de detectar anomalías del MSNM-S en este nuevo contexto. Gracias a este prototipo, se probó que: *i)* los ataques eran correctamente detectados y *ii)* que el laboratorio es apto para investigación y/o formación, ya que permite simular tanto condiciones de operación normales como ataques en un entorno controlado. Se puede encontrar más información y resultados de estos experimentos en los artículos [20], [21].

Al igual que con las pruebas de rendimiento, se encontraron fundamentalmente dos limitaciones:

- **Complejidad de integración de la herramienta MSNM-S**. La integración de MSNM-S tuvo que ser realizada *ad-hoc* debido a que aún no existe una funcionalidad específica que permita conectar herramientas de terceros.
- **Imposibilidad de acceso externo a Fidesol**. El despliegue y pruebas tuvieron que ser llevados a cabo de forma desagregada e independiente por parte de Fidesol y la UGR, ya que el acceso al Atenea Lab está limitado a personal de Fidesol.

Como conclusión preliminar, se puede comprobar que el laboratorio es capaz de simular casos de uso realistas de manera efectiva, siendo válido para generar datos y como entorno de pruebas tanto para investigación como para formación. Aunque es posible integrar software de terceros, esto se hace de forma costosa y presenta algunas limitaciones. Por tanto, sería conveniente añadir una funcionalidad que permita conectar de forma sencilla software no nativo de Atenea Lab, así como implementar el acceso a usuarios externos a Fidesol para facilitar la colaboración.

V. Trabajo futuro: próximos pasos

Teniendo en cuenta las funcionalidades actuales del laboratorio y las conclusiones de las pruebas realizadas, las líneas de trabajo y acciones previstas son las que se proponen en los siguientes párrafos.

V-A. Extensión y mejora de funcionalidades

Reutilización:

- Incluir la posibilidad de reutilizar sensores, tanto en entornos propios como por otros usuarios.
- Incluir la posibilidad de reutilizar funciones de comportamiento, tanto en entornos propios como por otros usuarios.

Infraestructura:

- Incluir la posibilidad de simular y configurar redes de comunicaciones más complejas con el objetivo de obtener resultados más realistas.

Usuarios:

- Incluir la posibilidad de registrar múltiples usuarios para que cada uno disponga de su propio espacio y entornos en Atenea Lab.
- Implementar el acceso seguro a personal externo de Fidesol para facilitar la colaboración con otros centros.

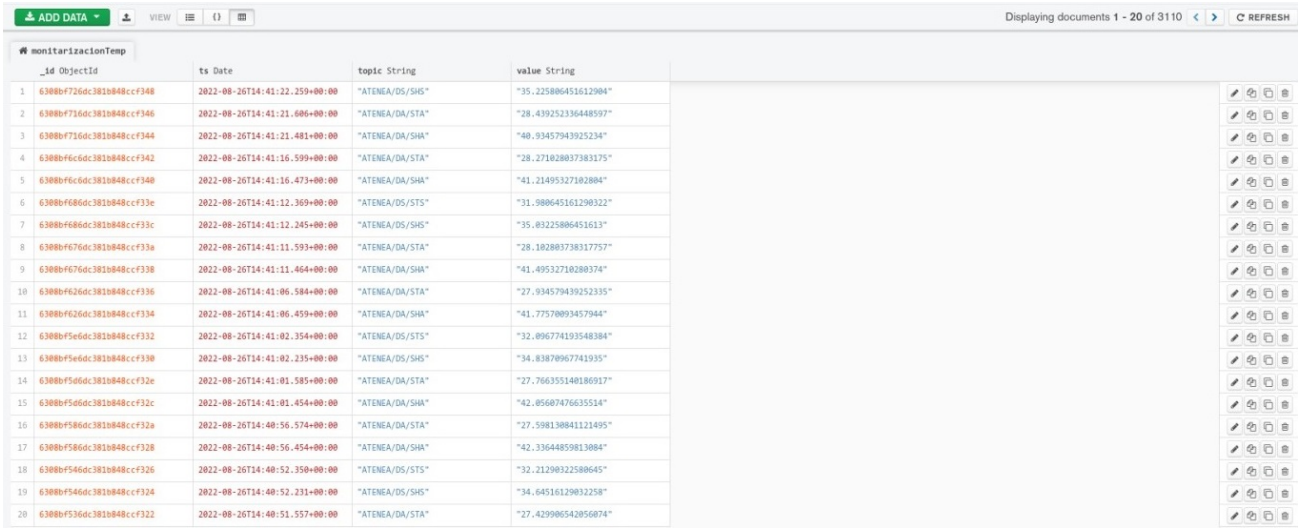

Figura 3. Comprobación de almacenamiento en la base de datos tras la generación y envío

Integración:

- Implementar los mecanismos necesarios para facilitar la integración de otras herramientas, haciendo así que el laboratorio sea más completo y facilitando también la realización de pruebas de desarrollos no realizados dentro del propio laboratorio.

V-B. Prioridades y puntos clave

En CICERO está previsto evolucionar el Atenea Lab abordando los siguientes puntos:

Utilidad y rendimiento:

- Definir y probar **casos de uso más complejos y variados** para obtener una mejor evaluación del rendimiento y los límites del laboratorio.
- Realizar **pruebas de estrés adicionales** para identificar de manera más exhaustiva las limitaciones, llevando a cabo un diseño de experimentos que permita obtener los puntos de saturación (pérdida de datos y reducción de ancho de banda) con diferencias estadísticamente significativas.
- Mejorar la **interoperabilidad**. Trabajar en la implementación de los mecanismos necesarios para facilitar la integración con otras herramientas.

Usuarios:

- Permitir el registro y acceso de **distintos usuarios** para facilitar la independencia de escenarios y entornos.
- Hacer posible el **acceso de personal externo a Fidesol** de forma segura, con el objetivo de favorecer la colaboración (al menos) con el resto de centros.
- **Evaluar y mejorar la usabilidad y experiencia de usuario** con distintos grupos de usuarios.

En concreto, se pretende incrementar el nivel de madurez actual de la Tecnología (punto de partida: TRL3-4) para disponer de un laboratorio funcional y usable que permita la colaboración con otros centros, tanto para experimentación como formación de los investigadores. Todo ello tendrá como principales objetivos la simulación de escenarios IoT y la mejora de la accesibilidad del laboratorio, con el propósito final de favorecer tanto la formación como la disponibilidad de testbed para el desarrollo de sistemas de recomendación automáticos y la automatización de respuestas frente a vulnerabilidades y anomalías detectadas.

VI. Conclusiones

En este trabajo, se presenta Atenea Lab, un laboratorio de IoT que permite construir múltiples escenarios de manera sencilla. Esta plataforma fue diseñada y construida con el objetivo de reducir el hueco existente entre la academia y las empresas (especialmente las pymes), propiciando la transferencia de conocimiento y la transformación digital. Además, pretende ser de utilidad tanto en formación como en investigación, facilitando la experimentación asequible en entornos IoT, gracias a que ayuda a realizar experimentos en entornos realísticos y controlados, obtener conjuntos de datos IoT y evolucionar prototipos IoT hasta TRL 5 o 6.

La primera versión de Atenea Lab es un prototipo funcional que permite: *i)* construir un escenario IoT completo (sensores, dispositivos, protocolos de comunicación y bases de datos), *ii)* simular un escenario IoT completo (el comportamiento de los sensores puede ser simulado, la comunicación y el almacenamiento funcionan correctamente) y *iii)* interactuar con Atenea Lab de forma gráfica e intuitiva gracias a su diseño centrado en el usuario. Las pruebas de estrés y de uso efectuadas revelaron algunas limitaciones que pueden ser fácilmente resueltas. Además, se implementó un primer caso de uso utilizando el Atenea Lab. Se trata de un prototipo de ciberseguridad para la detección de anomalías. Este prototipo se probó bajo diferentes ataques, siendo todos ellos detectados adecuadamente.

Como trabajo futuro, está previsto evolucionar el Atenea Lab al menos en los siguientes puntos: *i)* permitir el registro de distintos usuarios, *ii)* hacer posible el acceso de personal externo a Fidesol, *iii)* definir y probar casos de uso más complejos, *iv)* realizar pruebas de estrés adicionales para definir mejor las limitaciones y *v)* evaluar la usabilidad y experiencia de usuario con distintos grupos de usuarios. Todo ello se abordará en el marco del proyecto CICERO.

AGRADECIMIENTOS

Este trabajo ha sido realizado en el contexto de la Red de Excelencia Contramedidas Inteligentes de Ciberseguirdad para la Red del Futuro CICERO, CER-20231019, financiado por el Ministerio de Ciencia, Innovación y Universidades, a través de CDTI.

REFERENCIAS

[1] PWC, "How fake news has exploited COVID-19," https://cutt.ly/6geEVST, 2020, [Online, accessed on 07/10/2020].

[2] P. P. Ray, "Internet of Things for Smart Agriculture: Technologies, Practices and Future Direction," *IOS Press*, vol. 9, pp. 395–420, 2017.

[3] A. Tzounis, N. Katsoulas, T. Bartzanas, and C. Kittas, "Internet of Things in agriculture, recent advances and future challenges," *Biosystems Engineering*, vol. 164, pp. 31–48, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1537511017302544

[4] M. Fuentes-García, J. Camacho, and G. Maciá-Fernández, "Present and future of network security monitoring," *IEEE Access*, vol. 9, pp. 112 744–112 760, 2021.

[5] B. Boshra. Building University IoT Labs for Professional IoT Applications Development training utilizing IoT Educational and Innovation Labs. [Online, accessed on 27/03/2024]. [Online]. Available: https://www.linkedin.com/pulse/building-university-iot-labs-professional-development-bassem-boshra

[6] IFM. Moneo: la plataforma IIoT para industria y fabricación. [Online]. Available: https://www.ifm.com/es/es/shared/moneo?

[7] K. Josifović, S. Boljević, V. Ninković, and N. Turćinović, "Simulating massive iot environmental monitoring scenario using omnet++," in *2019 27th Telecommunications Forum (TELFOR)*, 2019, pp. 1–4.

[8] J. A. Fraire, P. Madoery, M. A. Mesbah, O. Iova, and F. Valois, "Simulating lora-based direct-to-satellite iot networks with florasat," in *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2022, pp. 464–470.

[9] U. K. Dayalan, R. A. K. Fezeu, T. J. Salo, and Z.-L. Zhang, "Kaala," in *Proceedings of the ACM SIGCOMM Workshop on Networked Sensing Systems for a Sustainable Society*. ACM, 2022.

[10] J. A. Barriga and P. J. Clemente, "Designing and simulating IoT environments by using a model-driven approach," in *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2022.

[11] S. Baheti, S. Badiger, and Y. Simmhan, "VIoLET," *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 3, pp. 1–39, 2022.

[12] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," *Sensors (Special Issue: Sensing and Data Analysis Techniques for Intelligent Healthcare)*, vol. 20, no. 13, 2020.

[13] Altexsoft. IoT Architecture: the Pathway from Physical Signals to Business Decisions. [Online]. Available: https://www.altexsoft.com/blog/iot-architecture-layers-components/

[14] A. Simmons. Internet of Things (IoT) Architecture: Layers Explained. [Online]. Available: https://bit.ly/43YcdK5

[15] R. Agar. IoT Architecture Guide. Major and additional layers of IoT system. [Online]. Available: https://www.helpwire.app/blog/iot-architecture/

[16] N. Einhorn. Why Users Stop Using Your Software: Common Reasons and Solutions. [Online, accessed on 27/03/2024]. [Online]. Available: https://bit.ly/49czzxx

[17] Y. Hassan-Montero and S. Ortega-Santamaría, *Informe APEI sobre Usabilidad*, [Online, accessed on 27/03/2024]. [Online]. Available: https://www.nosolousabilidad.com/manual/3.htm

[18] P. Canal. ¿Qué es el diseño centrado en el usuario? [Online, accessed on 27/03/2024]. [Online]. Available: https://bit.ly/498FXG5

[19] S. Pursell. Diseño centrado en el usuario: qué es, etapas y ejemplos. [Online, accessed on 27/03/2024]. [Online]. Available: https://blog.hubspot.es/website/diseno-centrado-usuario

[20] M. Fuentes-García, R. Magán-Carrión, C. Fernández, D. Álvarez, and M. Torres, "SIMAGRO: Un prototipo para la detección de anomalías en entornos IoT para el sector agroalimentario," in *Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad*, Y. Blanco-Fernández, M. F. Veiga, A. F. Vilas, and J. M. de Fuentes-García-Romero de Tejada, Eds.

[21] R. Magán-Carrión, M. Fuentes-García, C. Fernández-Rosales, and P. Maldonado-Mancilla, "SIMAGRO: A prototype for network anomaly detection in agrifood IoT environments," in *Special Session on Cybersecurity Issues of IoT in Ambient Intelligence (AMI) Environment (2nd Edition). IEEE World Forum on Internet of Things.*