Aprendizaje federado basado en blockchain para la gestión logística y de arsenales

Zaera Mata, Sergio [1], Gallego Adrián, Pablo [2] , Jimeno Sánchez-Patón, Paloma [3], Castañeda Fuentes, Pablo [2], Franco Moreu, Jesús [4], Gómez-Espinosa Martín, Roberto [5]

[1] Autor Principal y responsable del trabajo; Ingeniero de Inteligencia Artificial, HI-Iberia. SZM: szaera@hi-iberia.es

[2] Ingeniero en Inteligencia Artificial, HI-Iberia. PGA: pgallego@hi-iberia.es , PCF: pcastañeda@hi-iberia.es

[3] Jefe de Proyectos de Inteligencia Artificial, HI-Iberia. PJS: pjimeno@hi-iberia.es

[4] Director del Departamento Económico. HI-Iberia. JFM: jfranco@hi-iberia.es

[5] Director del Departamento de Inteligencia Artificial, HI-Iberia. RGEM: robertogemartin@hi-iberia.es

Resumen

La revolución experimentada por las técnicas de Inteligencia Artificial (IA) en la última década merece especial atención. Sin embargo, el enfoque convencional de entrenamiento centralizado de modelos de IA plantea limitaciones sustanciales y despierta preocupaciones significativas en términos de privacidad. Ante este panorama, es imperativo buscar alternativas que permitan aprovechar la información disponible sin poner en peligro la privacidad, con el fin de generar beneficios mutuos para todas las partes involucradas. Este estudio aborda los desafíos técnicos y colaborativos inherentes a la implementación de tecnologías de IA y propone soluciones innovadoras basadas en el Internet of Things (IoT). Se identifican tres desafíos primarios: la limitada capacidad computacional para volúmenes masivos de datos, los imperativos de seguridad y privacidad establecidos por las normativas, y la reticencia de individuos y organizaciones a compartir información sensible. Para enfrentar estos desafíos, se propone la adopción del enfoque de Federated Learning (FL), combinado con tecnologías de Blockchain (BC) y Smart Contracts (SC). Para demostrar las capacidades de este ecosistema, se propone un caso de uso en la gestión logística y de arsenales en el sector de Defensa y Seguridad, abordando desafíos relacionados con la seguridad, confiabilidad y trazabilidad de la información. Esta combinación de tecnologías ha sido previamente estudiada y aplicada en proyectos realizados por HI-Iberia, específicamente en el proyecto GREEN, que se centra en la optimización de las estaciones de recarga de vehículos eléctricos, desarrollado en colaboración con Naturgy, una empresa experta en el ámbito energético.

***Palabras Clave**: Inteligencia artificial, Federated Learning, Blockchain, Smart Contracts, Internet of things.*

1. Introducción

1.1. Contexto actual

En la actualidad, se está experimentando un crecimiento exponencial en la cantidad de datos generados por los individuos, y se prevé que esta tendencia continúe en el futuro. Este aumento se debe en gran medida al avance de tecnologías como las redes 5G y los dispositivos de IoT, los cuales permiten la monitorización de diversos elementos y la generación continua de información [1,2].

En respuesta al creciente volumen de datos, se ha producido un notable avance en las técnicas de IA que nos permiten gestionar y aprovechar eficientemente esta abundante información generada. Un ejemplo destacado es el modelo de Procesamiento del Lenguaje Natural (NLP) GPT-4 desarrollado por OpenAI. Con más de 100 billones de parámetros, este modelo es capaz de generar textos de alta calidad que resultan difíciles de distinguir entre la redacción humana y la generada por la IA [3].

1.2. Problema

El enfoque tradicional para el desarrollo de estos modelos de IA se basa en arquitecturas centralizadas, un único servidor gestiona todos los datos y entrena el modelo matemático. Sin embargo, esta solución plantea desafíos significativos. Por una parte, los enormes costos computacionales asociados que solo son asequibles si se dispone de hardware muy potente. Por otra parte, las regulaciones actuales de protección de datos, como el Reglamento General de Protección de Datos (GDPR), exigen altos niveles de seguridad para preservar la privacidad de los usuarios. La existencia de una brecha de seguridad en un único servidor que almacena todos los datos representa un riesgo sumamente elevado [4].

Aun en un contexto de regulaciones más flexibles, existen obstáculos significativos para persuadir a compañías o personas a compartir sus datos para el desarrollo de modelos IA. La información en cuestión se considera "privilegiada", ya que podría permitir a una empresa destacarse frente a sus competidores o aprovechar sus debilidades [5].

Ante este contexto, es necesario buscar alternativas. Una propuesta prometedora es la adopción de enfoques federados, que permiten aprovechar la información de los datos sin comprometer la privacidad de los usuarios. Además, la combinación de FL con tecnologías como Blockchain y SC puede brindar un marco seguro y colaborativo para el desarrollo de soluciones basadas en IA. Esto se traduce en una vía para encontrar un equilibrio entre la necesidad de utilizar datos para impulsar la innovación, la protección de la privacidad y personales [6,7].

1.3. Objetivo

Nuestro artículo presenta y valida una propuesta de ecosistema que se enfoca en crear una plataforma basada en Open Source. El objetivo de esta propuesta es habilitar el despliegue seguro y robusto de servicios de IA haciendo uso de datos provenientes del IoT. La plataforma permitiría habilitar el entrenamiento de modelos de IA mediante un flujo de trabajo basado en el Federated Learning, Blockchain y Smart Contracts. De esta forma, se lograría aprovechar los datos distribuidos en distintos dispositivos IoT, evitando así la necesidad de su centralización en un único servidor, lo cual garantizaría la preservación de la privacidad de los usuarios y el cumplimiento de las regulaciones de protección de datos. Así pues, se establecería el proceso de entrenamiento de los modelos de IA en un marco seguro y confiable.

2. Enfoque metodológico

2.1. Tecnologías utilizadas

Para comprender adecuadamente la propuesta, es necesario presentar las tecnologías que la conforman. El Federated Learning, el Blockchain y los Smart Contracts han suscitado un considerable interés y se han establecido como elementos fundamentales debido a los potenciales beneficios que ofrecen en múltiples campos.

El Federated Learning es un enfoque innovador en el campo del ML que permite la colaboración y distribución de la capacitación de modelos sin necesidad de compartir datos sensibles en un entorno centralizado. Google ha sido pionero en la implementación de FL en productos como Gboard y dispositivos Pixel. Es importante destacar que FL se aplica tanto en dispositivos móviles como en colaboraciones entre organizaciones, y se diferencia en FL horizontal, que involucra conjuntos de datos con características similares, y FL vertical, que implica datos con diferentes propiedades para las mismas muestras. En general, FL destaca por preservar la privacidad de los datos y mitigar los riesgos asociados con la divulgación masiva de información [8].

La aparición del Blockchain junto con la introducción del Bitcoin en 2008 ha sido un hito trascendental. Esta tecnología ha revolucionado las transacciones al permitir su ejecución segura, privada y sin intermediarios. Su funcionamiento se basa en un sistema distribuido de contabilidad con bloques inmutables, respaldado por algoritmos de consenso y encriptación. Además de su aplicación en criptomonedas, se utiliza en el IoT y la seguridad, ofreciendo ventajas como la confidencialidad y la autenticidad. Su potencial en la sociedad es amplio y se espera que siga expandiéndose en diversos sectores, impulsando la transformación digital y generando nuevas oportunidades de desarrollo [9].

Por último, los Smart Contracts son programas almacenados en una Blockchain que se ejecutan cuando se cumplen condiciones. Las aplicaciones incluyen la liberación de fondos, el registro de activos y el envío de notificaciones. La introducción de SC en Blockchain ha permitido la ejecución autónoma de contratos, eliminando intermediarios y agilizando procesos. Esta tecnología ha despertado gran interés al transformar BC en una plataforma transaccional completa, brindando mayor seguridad y eficiencia [10].

2.2. Ecosistema Inteligente para IoT

En la era del IoT, las infraestructuras de código abierto se han enfocado en la agregación, visualización y control de datos. Sin embargo, la integración de la IA en estas infraestructuras abre nuevas posibilidades. En este contexto, el Federated Learning ha surgido como una herramienta esencial para el entrenamiento de modelos de IA utilizando datos de dispositivos Edge, adaptándose óptimamente al crecimiento y distribución masiva de datos en redes de IoT (Figura 1).

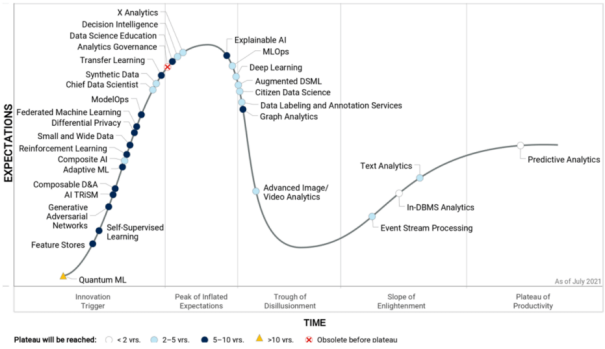

Figura 1: *Curva Gartner de Data Science & ML [11].*

Además de su uso en el entrenamiento de modelos, FL tiene un potencial destacado en servicios de IoT como la detección de ataques mediante detectores de anomalías y el mantenimiento predictivo para identificar fallos en dispositivos. La cooperación entre dispositivos acelera el aprendizaje, mejora la precisión y reduce los riesgos.

No obstante, los avances en IA pueden resultar inaccesibles para aquellos con recursos limitados debido a la dependencia de costosos conjuntos de datos centralizados y difíciles de obtener. Para abordar estos desafíos, se ha prestado atención a la integración del Blockchain en los flujos de trabajo de IA.

En nuestro enfoque propuesto, utilizamos el Blockchain para almacenar los modelos locales y globales generados durante el proceso de FL. Esto elimina la dependencia de un único servidor, establece un mecanismo de auditoría para los participantes y reduce los costos de comunicación. Nuestra propuesta busca superar las limitaciones de las arquitecturas previas y aspira a un desarrollo industrial más avanzado.

Además, la incorporación de Smart Contracts en el IoT permite una validación automática y establece relaciones autorreguladas entre entidades en la BC, especialmente cuando se combinan con la IA. Los SC también facilitan la generación de incentivos adecuados para recompensar o penalizar las contribuciones de los participantes.

La plataforma propuesta simplifica el uso del Blockchain, descentraliza los procesos de federación, aumentando la confianza de los participantes y brindando incentivos para contribuir con datos que mejoren el rendimiento del modelo.

3. Estudio de caso

La implementación conjunta de estas tecnologías ha demostrado un rendimiento excepcional. En esta sección, se presentará el proyecto GREEN, que aprovecha este ecosistema en un caso de uso específico: la optimización de las estaciones de recarga (ER) para vehículos eléctricos (VE). Se destacarán los logros más significativos alcanzados hasta la fecha y se propondrá un nuevo caso de uso enfocado en el sector de Defensa y Seguridad, específicamente en el ciclo de vida y logística de tecnologías comunes en instalaciones.

3.1. Proyecto GREEN

El proyecto GREEN es una iniciativa de vanguardia que combina tecnologías de última generación para facilitar la implementación de servicios de IA basados en datos del IoT. Esta sinergia representa un avance crucial en el impulso de iniciativas orientadas al desarrollo de las Smart Cities [12]. En esta investigación, el proyecto GREEN se desarrolla en colaboración con Naturgy, una destacada empresa experta en el dominio, que aporta su conocimiento y asesoramiento.

El caso de uso propuesto dentro del proyecto GREEN establece un entorno de trabajo integral para múltiples actores clave, como el proveedor de la red eléctrica, los gestores de las estaciones de recarga y los usuarios de vehículos eléctricos. Mediante la plataforma de FL, se logra desarrollar un modelo predictivo de la demanda energética requerida en las estaciones de recarga, lo que permite a los gestores negociar un precio ajustado a sus necesidades con el proveedor de la red eléctrica. Un aspecto fundamental radica en la salvaguarda de la seguridad de los datos de los clientes, y en la capacidad de los gestores de las estaciones de competir de manera justa y equitativa entre sí.

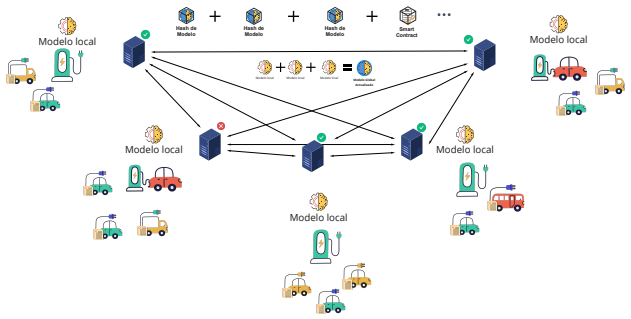

Figura 2: *Diagrama Red Blockchain GREEN.*

En consecuencia, en lugar de utilizar un servidor central para amalgamar los modelos locales, se opta por una combinación descentralizada en una red Blockchain (Figura 2). Cada electrolinera cargará su modelo entrenado y lo fusionará con actualizaciones de otros modelos. Los SM gestionarán las recompensas y sanciones para las empresas que aporten sus actualizaciones. Mediante un algoritmo de consenso regulado, los nodos votarán por los modelos locales más efectivos. Como resultado de esta evaluación, cada compañía obtendrá un modelo global actualizado que se adapta de forma óptima, premiando contribuciones significativas y penalizando intentos de subir modelos defectuosos.

Se ha implementado un simulador de Smart City (Figura 3) que visualiza de manera realista las posibilidades de la plataforma. La experiencia obtenida a través de este proyecto sienta las bases necesarias para el éxito de futuras propuestas, al proporcionar un marco sólido y validado para abordar desafíos en diversos sectores, incluyendo la Defensa. Esta experiencia permite optimizar la eficiencia de los procesos, como la gestión logística, y maximizar los resultados mediante la colaboración colectiva.

Figura 3: *Simulación estaciones de carga GREEN.*

3.2. Gestión Logística y de Arsenales en el Sector de Seguridad (GLASS)

La coordinación logística es de vital importancia para asegurar la disponibilidad de recursos estratégicos y respaldar la toma de decisiones fundamentales. Sin embargo, enfrenta desafíos significativos relacionados con la seguridad, la confiabilidad y la trazabilidad de la información, así como la gestión eficiente de inventarios y la prevención de la caducidad de los elementos almacenados. Para abordar estas problemáticas, proponemos la aplicación del Federated Learning, Blockchain y Smart Contracts como una solución integral que fortalece la seguridad, la confiabilidad y la eficiencia en la gestión logística y de arsenales.

La presente propuesta tiene como objetivo abordar los desafíos de gestión logística y de arsenales en el sector de Defensa. Para ellos se propone optimizar la gestión de inventario, garantizar la trazabilidad de los elementos almacenados y gestionar eficientemente las alertas.

La aplicabilidad de la propuesta GLASS se traduce en una serie de beneficios medibles para el caso de uso de Defensa. Mediante el uso del FL, se pueden entrenar modelos de pronóstico de demanda con una gran precisión. Estos modelos se basan en datos históricos y en tiempo real, lo que permite anticipar la demanda futura de recursos en los arsenales. Como resultado, se logra un aprovisionamiento eficiente y oportuno, evitando tanto la falta como el exceso de inventario. Esta optimización tiene un impacto significativo en la eficiencia operativa y la reducción de costos. Al evitar el exceso de inventario, se reducen los costos asociados al almacenamiento y la obsolescencia de recursos, lo que se traduce en una asignación más efectiva de los recursos financieros. Además, la disponibilidad constante de recursos estratégicos es esencial para la seguridad nacional, y la gestión optimizada del inventario garantiza esta disponibilidad en momentos críticos.

También, se crearía un gemelo digital de los arsenales, una representación virtual precisa y actualizada de los elementos almacenados. Esto tiene aplicaciones estratégicas y operativas valiosas. Proporciona una visión en tiempo real de la composición de los arsenales, permitiendo una toma de decisiones informada y estratégica a nivel de planificación. Además de ser útil para la simulación y el entrenamiento. Los datos del gemelo se pueden utilizar para crear escenarios simulados que ayuden en la formación del personal y en la preparación para situaciones críticas. Esto aumenta la capacidad de respuesta y mejora la eficiencia operativa.

La trazabilidad se garantiza mediante la red de BC, lo que permite un seguimiento completo y confiable de los arsenales. Cada movimiento y transacción se registra de manera inmutable en la cadena de bloques, lo que proporciona una visión detallada y segura de todas las operaciones. Este nivel de trazabilidad es esencial para garantizar la seguridad y el control de los arsenales. Facilita las auditorías y el cumplimiento de normativas al proporcionar un registro transparente de todas las actividades. Además, reduce significativamente el riesgo de pérdidas y robos al ofrecer un seguimiento completo y seguro de los activos estratégicos.

Por último, también se automatizan las alertas de caducidad y reordenamiento de los elementos almacenados utilizando SC. En contraste con las macros de Excel, los SC ofrecen una automatización avanzada y una trazabilidad en tiempo real. Esto asegura una respuesta rápida y precisa ante cambios en el inventario. Garantiza que los recursos se utilicen antes de su fecha de expiración, reduciendo el desperdicio y los costos asociados, al tiempo que minimiza la posibilidad de errores humanos en la gestión de inventario y las decisiones de reordenamiento. Además, tienen la ventaja de proporcionar una auditoría más efectiva que las macros. Cada evento queda registrado de manera inmutable en la BC, lo que facilita la verificación del cumplimiento de normativas y políticas.

4. Conclusiones

En este estudio, se ha realizado un análisis detallado de las tecnologías de Federated Learning, Blockchain y Smart Contracts, y se ha evaluado su aplicación en diversos campos. Se ha resaltado la capacidad del FL para permitir el entrenamiento colaborativo de modelos de manera distribuida, protegiendo la privacidad y mitigando los riesgos del intercambio masivo de información. Asimismo, se ha enfatizado la revolución del BC al garantizar la seguridad de las transacciones, y cómo los SC automatizan y establecen relaciones autorreguladas en la ejecución de contratos.

Se ha presentado el caso de estudio del proyecto GREEN, el cual ha aplicado de manera innovadora las tecnologías mencionadas para optimizar estaciones de recarga de VE. Se ha demostrado cómo estas tecnologías pueden impulsar la transformación urbana, fomentando entornos sostenibles y libres de emisiones. Además, se ha propuesto un nuevo caso de uso en el ámbito de Defensa y Seguridad, específicamente en la gestión logística y de arsenales, donde se ha ilustrado cómo este ecosistema puede fortalecer la seguridad y eficiencia en la gestión de recursos estratégicos.

En conclusión, la integración de las tecnologías expuestas ofrece beneficios significativos en términos de privacidad, seguridad, confiabilidad y efectividad. Estas tecnologías están impulsando cambios profundos en la sociedad, abriendo nuevas posibilidades de desarrollo. Con un enfoque adecuado y una implementación eficiente, se espera que continúen evolucionando y aportando soluciones disruptivas en el futuro, impulsando el progreso en múltiples áreas.

Agradecimientos

Nos gustaría expresar nuestro sincero agradecimiento a la empresa Naturgy por su respaldo en la realización del proyecto GREEN. Su contribución ha sido fundamental para el desarrollo del proyecto. Especial reconocimiento a Jesús Chapado y Alejandro Sánchez del departamento de I+D.

Referencias

[1] Li F, Zhang C, Chen G, Liu J. Internet of Things (IoT)-Based Big Data Analytics for Smart City: A Survey. IEEE Access. 2021;9:105280-105299.

[2] Wang H, Chen Q, Li Y, Sun Y. A Comprehensive Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal. 2020;7(12):11012-11043.

[3] Chen, M., Mao, S., & Liu, Y. (2021). Big Data: A Survey. Mobile Networks and Applications, 26(1), 10-16.

[4] Smith J, et al. Federated Learning for Privacy-Preserving Machine Learning: A Comprehensive Review. IEEE Access. 2022;10:12345-12367.

[5] Johnson A, et al. Blockchain-Based Federated Learning Framework for IoT Data Analytics. Journal of Parallel and Distributed Computing. 2021;150:123-135.

[6] Zhang J, Chen Y, Zhang C. Federated Learning for Edge Intelligence: Challenges, Methods, and Future Directions. IEEE Internet of Things Journal. 2021;8(20):16157-16176.

[7] Jin X, Yu J, Zhang Z, Wang H. Towards Privacy-Preserving and Collaborative AI in IoT: Advances and Challenges. IEEE Internet of Things Journal. 2021;8(1):367-381.

[8] McMahan HB, Moore E, Ramage D, Hampson S, yarc A. Communication-efficient learning of deep networks from decentralized data. In: Artificial Intelligence and Statistics. 2017. p. 1273-1282.

[9] Zhou Q, Zhang Y, Zhu H. Blockchain for Internet of Things: A Comprehensive Survey. IEEE Access. 2021;9:12940-12959.

[10] Liu Y, Liu C, Li X, Li K. Blockchain-Enabled Federated Learning for Edge Computing-Based Industrial Internet of Things. IEEE Transactions on Industrial Informatics. 2020;16(6):4312-4320.

[11] Gartner. Hype Cycle for Machine Learning & Data Science. 2021.

[12] HI Iberia. GREEN: InteliGencia colaboRativa para ciudadEs sostENibles [Internet]. [cited 2023 Jun 13]. Available from: https://green.hi-iberia.es/