Adaptive Federated Learning basado en Blockchain: Nuevas Fronteras la Gestión Logística y de Arsenales

Zaera Mata, Sergio[1],*; Jimeno, Paloma[1]; Castañeda, Pablo[1]; Dorado, Ander[1]; Franco, Jesús[1]; Gómez-Espinosa, Roberto[1]

[1] HI iberia (HIB). c/ Juan Hurtado de Mendoza nº14, 28036. Madrid. robertogemartin@hi-iberia.es

* Autor principal; szaera@hi-iberia.es

Resumen: En la actualidad, las operaciones de defensa y seguridad requieren de enfoques innovadores y efectivos para la gestión logística y de arsenales. Este trabajo propone un ecosistema basado en el aprendizaje federado (Federated Learning, FL), integrado con la tecnología de Blockchain (BC) y contratos inteligentes (Smart Contracts, SC), dirigido a optimizar la eficiencia operativa y estratégica en el sector de la defensa. La plataforma sugerida capitaliza los avances en Internet de las Cosas (IoT) para el adiestramiento descentralizado de modelos de Inteligencia Artificial (IA), lo cual ofrece mejoras sustanciales en la privacidad de datos, la seguridad transaccional y la confiabilidad en la gestión de recursos. Por medio de la aplicación sinérgica de FL, se garantiza una estrategia colaborativa y una instrucción en modelos autónomos que preservan la privacidad al tiempo que se intensifica la seguridad y la integridad del manejo de información crítica. Blockchain proporciona una estructura inmutable para el registro de modelos, así como un mecanismo de auditoría transparente y descentralizado, mientras que los SC aplicados refuerzan la automatización de procesos operacionales y relaciones regulativas. La viabilidad y eficacia de nuestro sistema se demostraron a través del Proyecto GREEN, donde la implementación de estas tecnologías permitió la optimización de estaciones de recarga para vehículos eléctricos (VE) como un caso exitoso en el ámbito urbano. Extendiendo esta metodología al contexto de la Defensa, el concepto Gestión Logística y de Arsenales en el Sector de Seguridad (GLASS) se presenta como un enfoque transformador para la gestión de inventario, ofreciendo una gestión logística mejorada, una precisa determinación de la demanda de recursos y un eficiente sistema de alertas dentro de entornos de seguridad altamente regulados.

Palabras clave: Blockchain, Digital Twin, Federated Learning, Inteligencia artificial, Physics-Informed Neural Networks, Smart Contracts.

---

1. Introducción

1.1 Contexto Actual

En la presente era de la información, nos enfrentamos a un crecimiento exponencial en la creación y replicación de datos impulsado por avances en tecnologías como las redes 5G y la amplia adopción del IoT. Estos progresos tecnológicos permiten una monitorización ubicua y recopilación de datos a una escala sin precedentes [1,2]. Concurrentemente, las capacidades en el dominio de la IA están avanzando de forma notable, enriqueciendo la competencia para analizar y extraer significados valiosos de vastos conjuntos de datos. Un hito en esta dirección es el desarrollo de GPT-4 de OpenAI, habilitando la generación de textos con una fidelidad tal que simula en gran medida la escritura humana, incluso engañando a los observadores no entrenados [3].

1.2 Problema

En el contexto actual intensificado por la expansión significativa de conjuntos de datos, los modelos de IA se enfrentan a desafíos de recursos computacionales y económicos derivados de estructuras centralizadas. Tales estructuras incrementan la susceptibilidad frente a compromisos de seguridad y privacidad, exacerbando los riesgos en el contexto de regulaciones estrictas y potenciales violaciones de datos en sistemas centralizados. Esta centralización enfrenta resistencia al compartir información, dada su naturaleza estratégicamente valiosa [4,5]. Para mitigar estos inconvenientes, el FL se posiciona como un mecanismo preferente, conduciendo a fusión de este con tecnologías disruptivas como BC hacia una infraestructura de IA colaborativa y robusta que preserva tanto la seguridad de los datos como su valor estratégico [6,7].

1.3 Objetivo

Este documento aborda la creación y validación de una infraestructura avanzada y de Open Source para robustecer la funcionalidad de aplicaciones de IA mediante la integración de extensos volúmenes de datos generados por el IoT. Se presenta una plataforma que actúa como catalizador para el despliegue autónomo de modelos de IA, fundamentada en una combinación de FL, BC y SC. El enfoque descentralizado se centra en la utilización estratégica de datos distribuidos entre numerosos nodos IoT, preservando la privacidad de estos según estándares regulatorios y mejorando la seguridad y la integridad del procesamiento en contextos de IA. Además, se diseña un marco de trabajo que integra modelos distribuidos con una infraestructura sólida y reglas bien definidas, garantizando un flujo de operaciones coherente y resistente, lo que facilita un manejo de datos dinámico y confidencial a través de dispositivos IoT.

2. Enfoque metodológico

2.1 Tecnologías utilizadas

Para la comprensión integral de esta propuesta, resulta imperativo exponer y elucidar sobre las tecnologías que constituyen su núcleo. El FL es esencial para el avance del paradigma de descentralización analítica, y permite la construcción cooperativa de modelos analíticos mientras se protege la información sensible, eludiendo las vulnerabilidades tradicionales asociadas con los sistemas centralizados. Esta tecnología se difracta en enfoques horizontal y vertical, enfocados en características homogéneas de datos o entidades, respectivamente [8]. Blockchain se presenta como un ecosistema de contabilidad distribuida que asegura la integridad de los bloques de datos mediante consenso y cifrado, prescindiendo de intermediarios para la validación de transacciones y extendiendo su impacto en áreas como el IoT y la ciberseguridad. Esta tecnología proporciona un marco confiable y seguro, favoreciendo la integridad de los datos y la autenticidad de las transacciones [9]. Finalmente, los SC emergen como entidades de ejecución autónoma depositadas en una Blockchain, activadas al cumplirse ciertos parámetros predefinidos. Los SC han evolucionado el ecosistema del Blockchain ampliando sus capacidades programáticas, previendo precedentes para la autorregulación transaccional y la ejecución de operaciones, lo que puede ser aplicado para reforzar protocolos de seguridad y gestión operativa en sectores militares [10].

2.2 Arquitectura Distribuida e Inteligente para IoT

En el ámbito de la IoT, las infraestructuras open source son clave en la centralización y manejo de datos, catalizando la integración de IA para funcionalidades extendidas. El FL surge como metodología esencial para la instrucción de modelos de IA mediante el aprovechamiento de datos generados en dispositivos Edge, procesan datos localmente, mejorando la adaptabilidad a la escala y dispersión de datos en redes IoT. El FL no solo optimiza el entrenamiento de IA, sino que también es prometedor en aplicaciones como la identificación temprana de fallas a través de mantenimiento predictivo y sistemas de detección de anomalías. Los retos financieros que implica el avance en IA, por la necesidad de grandes datasets, se contrarrestan con la integración del blockchain, que permite la inscripción de modelos de FL descentralizando así el procesamiento y ofreciendo un mecanismo de auditoría y reducción de costos. Por último, la incorporación de SC dentro del ecosistema de IoT refuerza la automatización y regulación de operaciones, y cuando se integran con sistemas IA, son fundamentales para configurar esquemas de incentivos que promueven modelos más precisos y eficientes.

3. Estudio de caso

3.1 GREEN - inteliGencia colaboRativa para ciudadEs sostENibles

El proyecto GREEN se posiciona como una iniciativa pionera en colaboración con Naturgy, líder en el sector energético, que integra tecnologías emergentes para posibilitar la implementación de soluciones de IA derivadas de datos IoT, promoviendo así la evolución de Smart Cities [11]. GREEN, se concibe como un marco colaborativo que involucra proveedores de energía, estaciones de recarga de VE y consumidores finales, con el objetivo de anticipar la demanda energética; permitiendo negociaciones más precisas y competitivas respecto al suministro de energía. El enfoque descentralizado de Blockchain se emplea para la gestión de modelos donde cada estación de recarga alimenta la red con su modelo de IA ajustado, que es entonces sintetizado con otros mediante un mecanismo de consenso. Los SC son utilizados para automatizar la recompensa o penalización basada en la calidad de las contribuciones al modelo global de aprendizaje. Este procedimiento asegura la actualización y optimización constantes de los modelos de IA, fomentando la contribución significativa y disuadiendo manipulaciones o aportes deficientes. Además, se ha desarrollado un simulador urbano inteligente para demostrar las capacidades de esta infraestructura integrada. La experiencia obtenida y su posterior validación forman una base sólida para abordar desafíos similares en el sector de la defensa, entre otros, destacando la importancia de la colaboración, optimización y maximización de la eficacia operativa.

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

La propuesta GLASS pretende optimizar la gestión de inventario, garantizar la trazabilidad de los elementos almacenados y gestionar eficientemente las alertas. En Defensa, esto se traduce en beneficios medibles, como la posibilidad de entrenar modelos de pronóstico de demanda con alta precisión usando FL, basados en datos históricos y en tiempo real. Estos modelos permiten anticipar la demanda futura de recursos en los arsenales, logrando un aprovisionamiento eficiente y oportuno, evitando tanto la escasez como el exceso de inventario. Esta optimización impacta significativamente la eficiencia operativa y la reducción de costos, minimizando el desperdicio y los costos de almacenamiento, y asegurando la disponibilidad constante.

En la arquitectura propuesta, se sustituye el uso de modelos tradicionales de IA por **Physics-Informed Neural Networks (PINNs)**. Estos modelos integran directamente las leyes físicas y restricciones específicas del dominio en el que se aplican, proporcionando predicciones con una precisión y fiabilidad mejoradas. Las PINNs destacan por su

capacidad de incorporar conocimientos previos sobre el sistema, lo que reduce considerablemente la necesidad de grandes cantidades de datos de entrenamiento.

Profundizando en el ecosistema, GLASS presenta la implementación del **Heterogeneity-Aware Adaptive Federated Learning (HAFL)**, un enfoque que aborda la variabilidad inherente entre los distintos usuarios finales. HAFL es una técnica que agrupa los nodos en subgrupos con características homogéneas, optimizando así el proceso de federado al garantizar que los datos empleados para el entrenamiento del modelo global sean representativos y coherentes dentro de cada subgrupo. Además, la capacidad adaptativa de HAFL es crucial para su efectividad a largo plazo permitiendo que los subgrupos evolucionen dinámicamente en respuesta a cambios en las condiciones operativas, como redistribuciones, variaciones en el estado o emergencias.

En armonía con el compromiso de protección, GLASS incorpora técnicas avanzadas como **Differential Privacy** y **Secure Aggregation**. Differential Privacy añade ruido controlado a los datos antes de compartirlos para el entrenamiento del modelo, protegiendo así la información individual de cada base militar y asegurando que los datos sensibles no puedan ser re-identificados, incluso si se tiene acceso a los modelos resultantes. Por otro lado, Secure Aggregation permite que múltiples participantes envíen sus actualizaciones de modelo de manera cifrada, de modo que el servidor central pueda agregarlas sin conocer el contenido individual de cada una.

GLAAS operará sobre una **red de Blockchain privada**, con acceso exclusivo a entidades autenticadas. Esta configuración proporciona un control elevado sobre los participantes y la actividad, promoviendo un entorno de datos seguro, ideal para el manejo de información clasificada. Los nodos en la red serán instancias como centros de distribución estratégicos, encargados de validar las transacciones. La red registrará cada movimiento y transacción de manera inmutable en la cadena de bloques, proporcionando una visión de todas las operaciones. Garantizando un nivel de trazabilidad que facilitará las auditorías, y reducirá significativamente el riesgo de pérdidas y robos. Adicionalmente, se creará un **Gemelo Digital** de los arsenales, una representación virtual precisa y actualizada de los elementos almacenados. Este gemelo proporciona una visión en tiempo real de la composición de los arsenales, permitiendo una toma de decisiones informada y estratégica. 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, mejorando la capacidad de respuesta operativa.

GLASS constituye una innovación trascendental en tácticas de defensa, implementando capacidades progresivas para vigilancia sistemática y continua. Destaca por su sincronización operativa, garantizando el suministro ininterrumpido de recursos y su integración en las misiones designadas. Asimismo, se automatiza las alertas de caducidad y reordenamiento de los elementos utilizando SC. Esto 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. Además, la administración se realiza de forma adaptativa, recalibrando el sistema para reaccionar ante variaciones inesperadas, promoviendo un esquema para la redistribución.

4. Conclusiones

Este estudio aborda la integración de FL, Blockchain y SC, destacando el entrenamiento protegido y descentralizado de modelos de IA con FL, la seguridad transaccional de Blockchain y la automatización de contratos mediante SC. El proyecto GREEN ilustra su aplicación práctica en la mejora de infraestructuras para VE, contribuyendo así a ciudades más sostenibles. En conclusión, la integración de las tecnologías discutidas ofrece beneficios en términos de privacidad, seguridad y efectividad, indicando un potencial de transformación social significativo.

Referencias

[1] F. Li, C. Zhang, G. Chen, and J. Liu, "Internet of Things (IoT)-Based Big Data Analytics for Smart City: A Survey," IEEE Access, vol. 9, pp. 105280-105299, 2021.
[2] H. Wang, Q. Chen, Y. Li, and Y. Sun, "A Comprehensive Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11012-11043, 2020.
[3] M. Chen, S. Mao, and Y. Liu, "Big Data: A Survey," Mobile Networks and Applications, vol. 26, no. 1, pp. 10-16, 2021.
[4] J. Smith et al., "Federated Learning for Privacy-Preserving Machine Learning: A Comprehensive Review," IEEE Access, vol. 10, pp. 12345-12367, 2022.
[5] A. Johnson et al., "Blockchain-Based Federated Learning Framework for IoT Data Analytics," Journal of Parallel and Distributed Computing, vol. 150, pp. 123-135, 2021.
[6] J. Zhang, Y. Chen, and C. Zhang, "Federated Learning for Edge Intelligence: Challenges, Methods, and Future Directions," IEEE Internet of Things Journal, vol. 8, no. 20, pp. 16157-16176, 2021.
[7] X. Jin, J. Yu, Z. Zhang, and H. Wang, "Towards Privacy-Preserving and Collaborative AI in IoT: Advances and Challenges," IEEE Internet of Things Journal, vol. 8, no. 1, pp. 367-381, 2021.
[8] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and A. yarc, "Communication-efficient learning of deep networks from decentralized data," in Proc. Artificial Intelligence and Statistics, 2017, pp. 1273-1282.
[9] Q. Zhou, Y. Zhang, and H. Zhu, "Blockchain for Internet of Things: A Comprehensive Survey," IEEE Access, vol. 9, pp. 12940-12959, 2021.
[10] Y. Liu, C. Liu, X. Li, and K. Li, "Blockchain-Enabled Federated Learning for Edge Computing-Based Industrial Internet of Things," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4312, 2020.
[11] HI Iberia, "GREEN: InteliGencia colaboRativa para ciudadEs sostENibles" [Online]. Available: https://green.hi-iberia.es/. [Cited: May-2024].