Comunicados

Anuncio de IBM z16: IA en tiempo real para el procesamiento de transacciones a escala y el primer sistema con seguridad cuántica de la industria

IBM z16 integra el procesador IBM Telum para que los clientes puedan emplear inferencias de inteligencia artificial para obtener información en tiempo real.

IBM z16 es el primer sistema con seguridad cuántica de la industria



ARMONK, N.Y.,5 de abril de 2022 – Hoy, IBM presentó IBM® z16™, el sistema de última generación con un acelerador de IA integrado en el chip, que ofrece inferencia de latencia optimizada. Esta innovación está diseñada para permitir a los clientes analizar transacciones en tiempo real, a escala, para cargas de trabajo de misión crítica como tarjetas de crédito, salud y transacciones financieras. Desarrollado sobre la historia de liderazgo en seguridad de la compañía, IBM z16 está específicamente diseñado para ayudar a proteger contra las amenazas del futuro cercano que podrían utilizarse para desencriptar las tecnologías de cifrado actuales.

Las innovaciones de IBM, incluido el IBM z16, han formado la columna vertebral tecnológica de la economía global durante décadas. El mainframe moderno de IBM es central para los entornos de nube híbrida, valorado como una plataforma altamente segura para ejecutar las cargas de trabajo más críticas por dos tercios de Fortune 100 -45 de los 50 principales bancos del mundo, 8 de las 10 principales aseguradoras, 7 de los 10 principales retailers y 8 de las 10 principales empresas de telecomunicaciones-. Por ejemplo, según un estudio reciente de Celent para IBM “Operacionalización de la prevención del fraude en IBM Z”, IBM zSystems ejecuta el 70% de las transacciones globales, sobre una base de valor[1].

“IBM es el estándar de referencia para el procesamiento de transacciones de alta seguridad. Ahora, con las innovaciones de IBM z16, nuestros clientes pueden aumentar la velocidad de decisión con la inferencia justo donde residen sus datos de misión crítica”, dijo Ric Lewis, SVP, IBM Systems. “Esto abre enormes oportunidades para cambiar el juego en sus respectivas industrias, para que puedan posicionarse para ofrecer mejores experiencias al cliente y resultados comerciales más poderosos.”

IA empresarial en tiempo real para revolucionar las industrias con nuevos casos de uso y aplicaciones

Las instituciones financieras de todo el mundo luchan con los impactos de las actividades fraudulentas en sus ingresos y en las interacciones de los consumidores. Según un nuevo estudio de IBM y Morning Consult "2022 IBM Global Financial Fraud Impact Report", el fraude con tarjeta de crédito es el tipo más común entre los consumidores de los siete países encuestados. Además, los participantes creen que los bancos y las redes de pago deberían ser las más responsables de prevenir el fraude. Pero la ejecución de modelos de *deep learning* a escala en tiempo real no ha sido posible debido a problemas de latencia, lo que significa que los modelos de detecciones de fraude sólo se ejecutan en menos del 10% de las transacciones de alto volumen, entonces una cantidad significativa de fraude no se detecta.

IBM z16 reúne de forma única la inferencia de IA, a través de su IBM Telum, con el procesamiento de transacciones de gran volumen altamente seguro y confiable por el que la empresa es reconocida. Por primera vez, los bancos pueden analizar el fraude durante las transacciones a gran escala: IBM z16 puede procesar 300 mil millones de operaciones de inferencia por día con sólo un milisegundo de latencia[2]. Para los consumidores, esto significaría reducir el tiempo y la energía necesarios para manejar transacciones fraudulentas en su tarjeta de crédito. Tanto para los comerciantes como para los emisores de tarjetas, permitiría una reducción en la pérdida de ingresos, ya que los consumidores evitarían la frustración asociada con falsos rechazos en los que podrían recurrir a otras tarjetas para futuras transacciones.

Otras amenazas, incluido el fraude fiscal y el robo minorista organizado, están surgiendo como desafíos que los gobiernos y las empresas deben controlar. Los pagos en tiempo real y los métodos de pago alternativos, como las criptomonedas, están empujando los límites de las técnicas tradicionales de detección de fraude. La aplicación de las capacidades de IBM z16 a otras industrias puede ayudar a crear una clase completamente nueva de casos de uso, que incluyen:

- Aprobación de préstamos: para acelerar la aprobación de préstamos comerciales o de consumo.
- Compensación y liquidación: para determinar qué operaciones y/o transacciones pueden tener una exposición de alto riesgo antes de la liquidación.
- Aprendizaje federado para el comercio minorista: para modelar mejor el riesgo contra el fraude y el robo.

Proteger los datos con el primer sistema con seguridad cuántica de la industria

En un entorno de nube híbrida, que incluye recursos locales y de nube pública, es crítico protegerse contra las amenazas actuales y tomar una postura ante los ciberdelincuentes que pueden estar robando datos ahora para descifrarlos más tarde. Basándose en las tecnologías de IBM como el Cifrado Generalizado y la Computación Confidencial, IBM z16 lleva la resiliencia cibernética un paso más allá para proteger los datos contra futuras amenazas que podrían evolucionar con los avances de la computación cuántica.

Como el primer sistema con seguridad cuántica de la industria[3], IBM z16 está respaldado por la criptografía basada en celosía, un enfoque para construir primitivas de seguridad que ayudan a proteger los datos y los sistemas contra amenazas actuales y futuras. Con la criptografía con seguridad cuántica de IBM z16, las empresas pueden preparar hoy sus aplicaciones y datos para el futuro.

Con un *secure boot* (lo que significa que los malos actores no pueden inyectar malware en el proceso de arranque para hacerse cargo del sistema durante el inicio), los clientes de IBM z16 pueden fortalecer su resiliencia cibernética y mantener el control de su sistema. Además, con el módulo de seguridad de hardware

Crypto Express 8S (CEX8S), ofrecerá tecnología criptográfica tanto clásica como cuántica para ayudar a abordar los casos de uso que requieren confidencialidad, integridad y no repudio de la información. El *secure boot* y la criptografía con seguridad cuántica de IBM z16 pueden ayudar a los clientes a abordar futuras amenazas relacionadas con la computación cuántica, incluidos los ataques de "recolección ahora, descifrado posterior" que pueden conducir a la extorsión, la pérdida de propiedad intelectual y la divulgación de otros datos confidenciales.

Modernización para la nube híbrida

IBM ha pasado los últimos tres años realizando importantes inversiones al servicio de su compromiso con la adopción de tecnología de código abierto en la plataforma IBM zSystems y para establecer una experiencia de desarrollador común a través de la nube híbrida. Estas soluciones están diseñadas para ayudar a los clientes a aprovechar sus inversiones y las fortalezas de su infraestructura de TI, nubes y aplicaciones existentes sin fricciones, mientras brinda la flexibilidad de ejecutar, construir, gestionar y modernizar las cargas de trabajo nativas de la nube en la arquitectura de su elección.

Los anuncios recientes como parte de este esfuerzo incluyen:

- **IBM Z y Cloud Modernization Stack**: para ayudar a los clientes a aumentar la agilidad y acelerar su transformación, incluido el soporte para proyectos populares de código abierto.
- **IBM Z y Cloud Modernization Center**: una puerta frontal digital a una amplia gama de herramientas, entrenamientos, recursos, socios de ecosistema y conocimiento específico de la industria a través de IBM Consulting, para ayudar a los clientes de IBM zSystems a acelerar la modernización de sus aplicaciones, datos y procesos en una arquitectura de nube híbrida abierta.
- **Fijación de Precios Adaptada:** un enfoque integral que permite a nuestros clientes responder rápidamente a los cambios en las cargas de trabajo dinámicas y las necesidades del negocio con precios similares a los de la nube.
- **Anaconda a Linux en Z:** un ejemplo de la incorporación de *libraries* y *frameworks* de trabajo populares en ciencia de datos a estas plataformas empresariales, proporcionando una experiencia de usuario de ciencia de datos coherente en la nube híbrida.
- **Soporte optimizado:** IBM Technology Support Services ofrece a los clientes de IBM z16 soporte llave en mano para predecir y prevenir interrupciones no planificadas, y servicios técnicos que agilizan la forma en que las empresas aprovechan la oportunidad de los entornos de tecnología híbrida.

Con IBM z16, IBM utilizó un enfoque altamente colaborativo y centrado en el cliente que involucró profundamente a cientos de personas de más de 70 clientes, una práctica que ya está en marcha para los futuros sistemas mainframe de la compañía. El IBM z16 estará disponible desde el 31 de mayo de 2022.

---

[1] *"Operationalizing Fraud Prevention on IBM Z," an IBM commissioned report by Celent. March 2022.*

[2] *Disclaimer: el resultado del rendimiento se extrapola de las pruebas internas de IBM que ejecutan operaciones de inferencia local en un z16 LPAR con 48 IFL y 128 GB de memoria en Ubuntu 20.04 (SMT mode) utilizando un modelo sintético de detección de fraude con tarjeta de crédito (https://github.com/IBM%20/ai-on-z-fraud-detection) explotando el Acelerador Integrado para IA. El punto de referencia se ejecutaba con 8*

subprocesos paralelos, cada uno anclado al primer núcleo de un chip diferente. El lscpucommand se usó para identificar la topología de chip de núcleo. Se utilizó un tamaño de lote de 128 operaciones de inferencia. Los resultados pueden variar.

[3] *Disclaimer: citado por un analista externo. IBM z16 con Crypto Express 8S card proporciona API con seguridad cuántica que brindan acceso a algoritmos cuánticos seguros que han sido seleccionados como finalistas durante el proceso de estandarización PQC realizado por NIST. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions. La criptografía cuántica segura se refiere a los esfuerzos para identificar algoritmos que sean resistentes a los ataques de computadoras clásicas y cuánticas, para mantener seguros los activos de información incluso después de que se haya construido una computadora cuántica a gran escala. Fuente: https://www.etsi.org/technologies/quantum-safecryptography. Estos algoritmos se utilizan para ayudar a garantizar la integridad de varios procesos de arranque y firmware. IBM z16 es el primer sistema de la industria protegido por tecnología de seguridad cuántica en varias capas de firmware.*
