Published on *BSC-CNS* (https://www.bsc.es)

El investigador del BSC Antonio J. Peña, premiado con una ERC Consolidator Grant por el proyecto ?HomE?

HomE tiene como objetivo permitir la viabilidad del aprendizaje automático con preservación de la privacidad en entornos no confiables, como los servicios en la nube.

Su principal desafío es desarrollar una metodología capaz de superar las limitaciones de software y hardware existentes.

El Consejo Europeo de Investigación (ERC) ha premiado con una ERC Consolidator Grant, al investigador senior del Barcelona Supercomputing Center-Centro Nacional de Supercomputación (BSC), Antonio J. Peña, líder del equipo Accelerators and Communications for HPC . Peña será el investigador principal de la propuesta premiada con una ERC, HomE (Enabling Homomorphic Encryption of Deep Neural Network Models and Datasets in Production Environments), que tiene como objetivo hacer posible la viabilidad del *machine learning* (aprendizaje automático) que preserve la privacidad en entornos no confiables, como los servicios en la nube. Hasta ahora, las técnicas de cifrado homomórfico (aquellas que permiten realizar cálculos directamente sobre datos cifrados) han supuesto una gran sobrecarga computacional y de datos. HomE unirá técnicas de optimización de software de HPC y diseños de hardware novedosos, además de tecnología de memoria persistente, para permitir escenarios de tamaño de producción de aprendizaje profundo cifrado homomórficamente.

Antonio J. Peña asegura que “este proyecto ERC brindará a los usuarios de *Deep learning* (aprendizaje profundo) la posibilidad de enviar sus trabajos con confianza a un proveedor en la nube, incluso cuando existan políticas de protección de datos (por ejemplo, GDPR). Imagino un hospital capaz de descargar procesos avanzados de detección de cáncer basados en redes neuronales profundas sin preocuparse por la privacidad de los registros médicos. Va a ser simplemente increíble".

El reto de HomE: desarrollar una metodología capaz de superar las limitaciones existentes de software y hardware

El aprendizaje profundo (*Deep learning*, DL, por sus siglas en inglés) se usa para resolver problemas de clasificación que antes no se cuestionaban, como el reconocimiento facial, y presenta casos de uso claros con requisitos de privacidad. El cifrado homomórfico (HE) permite operaciones sobre datos cifrados, pero implica un gran aumento del tamaño de los datos. Los tamaños de RAM actualmente limitan el uso de HE en DL a casos de uso muy reducidos. La tecnología de memoria persistente (PMEM) de reciente aparición ofrece espacios de RAM más grandes que nunca, pero su rendimiento está lejos del de las tecnologías DRAM habituales.

El proyecto HomE tiene como objetivo generar una nueva clase de arquitecturas de sistemas para cargas de trabajo de DL encriptadas, al eliminar o reducir drásticamente los movimientos de datos a través de las jerarquías de memoria/almacenamiento y la red, con el respaldo de la tecnología PMEM, superando sus severas limitaciones de rendimiento actuales.

HomE tiene la intención de habilitar por primera vez la ejecución encriptada en aceleradores locales de modelos grandes que no caben en DRAM, ejecutar cientos de modelos DL simultáneamente y soportar grandes conjuntos de datos para proporcionar alta resolución y precisión.

Con estos objetivos innovadores, HomE entra en un campo inexplorado resultante de la convergencia innovadora de varias disciplinas, donde se requiere una investigación de amplio alcance para evaluar la viabilidad actual y futura. Su principal desafío es desarrollar una metodología capaz de superar las limitaciones de software y hardware existentes. HomE propone un enfoque holístico que producirá resultados de gran impacto que incluyen una novedosa caracterización integral del rendimiento, optimizaciones innovadoras sobre la tecnología actual y propuestas de hardware pioneras. HomE puede generar un cambio de paradigma que revolucionará la convergencia de las disciplinas de *machine learning* y criptografía, llenando un vacío de conocimiento y abriendo nuevos horizontes, como el entrenamiento DL en HE, actualmente demasiado exigente incluso para DRAM. HomE, basado en evidencia sólida, revelará la gran incógnita de si PMEM es un habilitador práctico para las cargas de trabajo de DL cifradas.

Sobre Antonio J. Peña

Antonio J. Peña es Investigador Sénior en el Barcelona Supercomputing Center, donde lidera el equipo de Accelerators and Communications for HPC . Es un futuro becario Ramón y Cajal y ha disfrutado anteriormente de otras becas como la prestigiosa Marie Sklodowska-Curie Individual Fellowship. Entre otros, recibió el premio IEEE TCHPC Award for Excellence for Early Career Researchers in HPC de 2017 y es miembro sénior de IEEE y ACM. Está involucrado en la organización y comités directivos de varios congresos como SC o IEEE Cluster. Sus intereses de investigación en el área de sistemas en tiempo de ejecución y modelos de programación para computación de alto rendimiento incluyen la heterogeneidad de recursos y las comunicaciones.

Barcelona Supercomputing Center - Centro Nacional de Supercomputación

Source URL (retrieved on *23 Abr 2024 - 19:27*): https://www.bsc.es/es/noticias/noticias-del-bsc/el-investigador-del-bsc-antonio-j-pe%C3%B1a-premiado-con-una-erc-consolidator-grant-por-el-proyecto-%E2%80%9Chome