L'investigador del BSC Antonio J. Peña, premiat amb una ERC Consolidator Grant pel projecte ?HomE?

HomE té com a objectiu permetre la viabilitat de l'aprenentatge automàtic amb preservació de la privadesa en entorns no fiables, com els serveis al núvol.



El seu desafiament principal és desenvolupar una metodologia capaç de superar les limitacions de software i hardware existents.

El Consell Europeu de Recerca (ERC) ha premiat amb una ERC Consolidator Grant, l'investigador sènior del Barcelona Supercomputing Center-Centro Nacional de Supercomputación (BSC), Antonio J. Peña, líder de l'equip Accelerators and Communications for HPC. Peña serà l'investigador principal de la proposta premiada amb una ERC, HomE (Enabling Homomorphic Encryption of Deep Neural Network Models and Datasets in Production Environments), que té com a objectiu fer possible la viabilitat del *machine learning* (aprenentatge automàtic) que preservi la privadesa en entorns no fiables, com els serveis al núvol. Fins ara, les tècniques de xifratge homomòrfic (aquelles que permeten fer càlculs directament sobre dades xifrades) han suposat una gran sobrecàrrega computacional i de dades. HomE unirà tècniques d'optimització de software de HPC i dissenys de harware nous, a més de tecnologia de memòria persistent, per permetre escenaris de mida de producció d'aprenentatge profund xifrat homomòrficament.

Antonio J. Peña assegura que “aquest projecte ERC brindarà als usuaris de *Deep learning* (aprenentatge profund) la possibilitat d'enviar els seus treballs amb confiança a un proveïdor al núvol, fins i tot quan hi hagi polítiques de protecció de dades (per exemple, GDPR) . Imagino un hospital capaç de descarregar processos avançats de detecció de càncer basats en xarxes neuronals profundes sense preocupar-se per la privadesa dels registres mèdics. Serà simplement increïble”.

El repte de HomE: desenvolupar una metodologia capaç de superar les limitacions existents de software i hardware

L'aprenentatge profund (*Deep learning*, DL, per les sigles en anglès) es fa servir per resoldre problemes de classificació que abans no es qüestionaven, com el reconeixement facial, i presenta casos d'ús clars amb requisits de privadesa. El xifratge homomòrfic (HE) permet operacions sobre dades xifrades, però implica un gran augment de la mida de les dades. Les mides de RAM actualment limiten l'ús de HE en DL a casos molt reduïts. La tecnologia de memòria persistent (PMEM) de recent aparició ofereix espais de RAM més grans que mai, però el seu rendiment és lluny del de les tecnologies DRAM habituals.

El projecte HomE té com a objectiu generar una nova classe d'arquitectures de sistemes per a càrregues de treball de DL encriptades, en eliminar o reduir dràsticament els moviments de dades a través de les jerarquies de memòria/emmagatzematge i la xarxa, amb el suport de la tecnologia PMEM, superant les seves severes limitacions de rendiment actuals.

HomE té la intenció d'habilitar per primera vegada l'execució encriptada en acceleradors locals de models grans que no caben a DRAM, executar centenars de models DL simultàniament i suportar grans conjunts de dades per proporcionar alta resolució i precisió.

Amb aquests objectius innovadors, HomE entra en un camp inexplorat resultant de la convergència innovadora de diverses disciplines, on cal una investigació d'ampli abast per avaluar la viabilitat actual i futura. El seu principal desafiament és desenvolupar una metodologia capaç de superar les limitacions de software i hardware existents. HomE proposa un enfocament holístic que produirà resultats de gran impacte que inclouen una nova caracterització integral del rendiment, optimitzacions innovadores sobre la tecnologia actual i propostes de hardware pioneres. HomE pot generar un canvi de paradigma que revolucionarà la convergència de les disciplines de *machine learning* i criptografia, omplint un buit de coneixement i obrint nous horitzons, com l'entrenament DL a HE, actualment massa exigent fins i tot per a DRAM. HomE, basat en evidència sòlida, revelarà la gran incògnita de si PMEM és un habilitador pràctic per a les càrregues de treball de DL xifrades.

Sobre Antonio J. Peña

Antonio J. Peña és Investigador Sènior al Barcelona Supercomputing Center, on lidera l'equip d' Accelerators and Communications for HPC. És un futur becari Ramon i Cajal i ha gaudit anteriorment d'altres beques com la prestigiosa Marie Sklodowska-Curie Individual Fellowship. Entre altres, va rebre el premi IEEE TCHPC Award for Excellence per Early Career Researchers in HPC de 2017 i és membre sènior de IEEE i ACM. Està involucrat en l'organització i els comitès directius de diversos congressos com SC o IEEE Cluster. Els seus interessos de recerca en l’àrea de sistemes en temps d’execució i models de programació per a computació dalt rendiment inclouen la heterogeneïtat de recursos i les comunicacions.

Barcelona Supercomputing Center - Centro Nacional de Supercomputación

---

Source URL (retrieved on *29 Mar 2024 - 12:53*): https://www.bsc.es/ca/noticies/noticies-del-bsc/linvestigador-del-bsc-antonio-j-pe%C3%B1a-premiat-amb-una-erc-consolidator-grant-pel-projecte-%E2%80%9Chome%E2%80%9D