Offre n°2023-06854

PhD Position F/M Reliability and Security of Large Foundation Models

Le descriptif de l'offre ci-dessous est en Anglais

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

The Inria Rennes - Bretagne Atlantique Centre is one of Inria's eight centres and has more than thirty research teams. The Inria Center is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institute, etc.

Mission confiée

Large Foundation Models (LFMs) are cutting-edge technology for natural language processing, object detection and segmentation, and audio and multimodal processing, outperforming any available machine learning technique. LFMs, such as OpenAI GPT-4, Google ViT, and Meta LLaMA, have gained public attention with their unprecedented accuracy. Given the superior performance of LFMs, they are being deployed in safety-critical and mission-critical applications, including space exploration and self-driving cars. Improving LFMs' security and reliability is crucial to enable dependable real-time safety-critical systems.

Large and complex accelerators like Graphics Processing Units (GPUs) are ideal for deploying LFMs in safety-critical applications. However, GPUs integrated into safety-critical systems must meet specific constraints, including real-time execution and high classification/detection accuracy, even in harsh environments. It is imperative to evaluate whether these critical requirements are met when undesirable events, such as radiation-induced faults and electromagnetic hardware attacks, disrupt correct hardware execution and modify the expected results of the LFMs.

This Ph.D. aims to identify hardware and software vulnerabilities in LFM-based systems and propose error mitigation techniques.

Principales activités

The Ph.D. student will characterize the impact of radiation-induced faults and electromagnetic hardware attacks on system reliability and security on GPUs for vision, language processing, and multimodal LFMs. The results will be combined with software simulation data to identify effective hardening solutions. The Ph.D. student will work on developing new fault tolerance approaches tailored for LFMs. Standard fault tolerance techniques may introduce unacceptable overhead. We will conduct a comprehensive fault propagation analysis to propose efficient and effective hardening methods.

The Ph.D. student will participate in international experiments and internships at laboratories like Rutherford Appleton Laboratory in the UK and Los Alamos National Laboratory in the USA. In addition, the student will participate in conferences and international projects. This can help them to develop their research skills and network with other professionals in their field.

Compétences

Required technical skills:

- Good knowledge of computer architectures and embedded systems
- Good programming knowledge (C/C++, python)
- Basics of Machine Learning (pytorch/tensorflow)
- Experience in fault tolerant architectures is a plus
- Experience with hardware design is a plus

Candidates must have a Master's degree (or equivalent) in Computer Science, Computer Engineering, or

Electrical Engineering.

Languages: proficiency in written English and fluency in spoken English is required.

Relational skills: the candidate will work in a research team, where regular meetings will be set up. The candidate has to be able to present the progress of their work in a clear and detailed manner.

Other valued appreciated: Open-mindedness, strong integration skills and team spirit.

Most importantly, we seek highly motivated candidates.

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Possibility of teleworking (90 days per year) and flexible organization of working hours
- Partial payment of insurance costs

Rémunération

monthly gross salary amounting to 2082 euros for the first and second years and 2190 euros for the third year

Informations générales

- **Thème/Domaine :** Architecture, langages et compilation
  Système & réseaux (BAP E)
- **Ville :** Rennes
- **Centre Inria :** Centre Inria de l'Université de Rennes
- **Date de prise de fonction souhaitée :**2024-06-01
- **Durée de contrat :**3 ans
- **Date limite pour postuler :**2024-05-24

Contacts

- **Équipe Inria :** TARAN
- **Directeur de thèse :**
  Kritikakou Angeliki / angeliki.kritikakou@irisa.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Please submit online : your resume, cover letter and letters of recommendation eventually

For more information, please contactangeliki.kritikakou@irisa.fr

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.