Offre n°2020-02890

Une infrastructure de vérification pour l'apprentissage machine sécurisé

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Ingénieur scientifique contractuel

Mission confiée

L'apprentissage machine utilise massivement des données utilisateurs (incluant des données personelles) pour produire des modèles analytiques, qui sont ensuite utilisés pour faire des décisions de classification sur des nouvelles données sans intervention humaine. Alors que les applications de l'apprentissage machine deviennent de plus en plus sophistiquées, la sécurité et la confidentialité des données dans ce contexte ont reçues moins d'attention. Avec l'apprentissage machine préservant la vie privée (Privacy Preserving Machine Learning, PPML), un tel classifieur (sur un serveur) doit traiter les requêtes de l'utilisateur de manière opaque, et ne rien apprendre sur la requête ni sur la réponse. Un client doit seulement apprendre la réponse associée à sa requête, et ne doit rien apprendre sur le modèle.
Atteindre ces objectifs, aussi simples qu'ils paraissent, se trouvent être difficiles et coûteux en pratique, et sont un domaine actif de recherche.

Principales activités

Notre but dans ce projet est de faire une implémentation vérifiée de SPDZ2k, un protocole de calcul multi-parti sécurisé, dans le but de l'appliquer au PPML.
L'implémentation et la vérification se fait en F*, un langage fonctionnel type ML avec un système de type incluant polymorphisme, types dépendants, effets monadiques, sous-typage. Ce langage a pour but la vérification via un solveur SMT, et peut ensuite être compilé en OCaml, F#, C ou même WebAssembly.

Une spécification haut-niveau et bas-niveau du protocole étant déjà écrites, nous avons les objectifs suivants :
— Preuve de sécurité de la spécification bas-niveau

— Écriture et preuve de l'implémentation bas-niveau

— Application au PPML

Avantages

- Restauration subventionnée
- Transports publics remboursés partiellement
- Congés: 7 semaines de congés annuels + 10 jours de RTT (base temps plein) + possibilité d'autorisations d'absence exceptionnelle (ex : enfants malades, déménagement)
- Possibilité de télétravail (après 6 mois d'ancienneté) et aménagement du temps de travail
- Équipements professionnels à disposition (visioconférence, prêts de matériels informatiques, etc.)
- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)
- Accès à la formation professionnelle
- Sécurité sociale

Informations générales

- **Thème/Domaine :** Sécurité et confidentialité
  Système & réseaux (BAP E)
- **Ville :** Paris
- **Centre Inria :** Centre Inria de Paris
- **Date de prise de fonction souhaitée :** 2020-09-01
- **Durée de contrat :** 7 mois
- **Date limite pour postuler :** 2020-09-24

Contacts

- **Équipe Inria :** PROSECCO
- **Recruteur :**
  Mourey Mathieu / mathieu.mourey@inria.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

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.