Offre n°2022-05366

Post-Doctoral Research Visit F/M Private and Secure Computation on Personal Data

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

Type de contrat : CDD

Contrat renouvelable : Oui

Niveau de diplôme exigé : Thèse ou équivalent

Fonction : Post-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.

Contexte et atouts du poste

The selected applicant will work within the WIDE research team at Inria of the University of Rennes (https://team.inria.fr/wide/). WIDE focuses on large-scale distributed systems and applications, as well as on privacy, and distributed machine learning.

This postdoctoral position is funded by the SOTERIA H2020 project (https://www.soteria-h2020.eu/) which aims to develop a user-centric, citizen-driven tool to help European citizens to manage their personal data. The project therefore involves close collaboration with French international partners such as AriadNext by IDNow, Idiap Switzerland, COSIC Team @ KU Leuven, a complete list is available at https://www.soteria-h2020.eu/partners/.

The successful applicant will have the opportunity to travel and collaborate with such international partners. All travel expenses will be covered by Inria within the limits set by French regulations.

Mission confiée

The recruited postdoctoral researcher is expected to work on the design of a distributed data vault that can (i) store personal data while keeping it safe from third parties, (ii) support computation on encrypted or otherwise protected personal data to obtain aggregate statistics while respecting the privacy of the individual data items, (iii) provide means to remunerate users that enable computation on their personal data.

In particular, we aim to address this challenge by relying on a byzantine-fault tolerant [1,2] decentralized storage platform that can store data reliably in encrypted form. We plan to combine techniques like multiparty computation [3] and homomorphic encryption [4] with technologies like trusted execution environments [5] to enable computation on such encrypted data. This will allow us to address a variety of use cases, such as decentralized [6] and federated machine learning algorithms [7]. The system should also keep track of the usage of personal data to support remuneration schemes. To this end, we plan to leverage our recent theoretical work on lightweight distributed ledgers [8, 9].

The postdoctoral researcher will contribute by performing original research on these topics, and will also participate in the supervision of Masters and PhD students. In doing so, he or she will collaborate with Davide Frey and other members of the WIDE team, as well as with international partners within the SOTERIA project and other related projects. Although teaching is not a requirement, the candidate can also choose to teach relevant courses at the University of Rennes 1 and affiliated institutions.

References

[1] Leslie Lamport, Robert Shostak, and Marshall Pease. 1982. The Byzantine Generals Problem. ACM Trans. Program. Lang. Syst. 4, 3 (July 1982), 382–401. https://doi.org/10.1145/357172.357176

[2] Miguel Castro and Barbara Liskov. 1999. Practical Byzantine fault tolerance. In Proceedings of the third symposium on Operating systems design and implementation (OSDI '99). USENIX Association, USA, 173–186.

[3] Ran Canetti, Uri Feige, Oded Goldreich, and Moni Naor. 1996. Adaptively secure multi-party computation. In Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing (STOC '96). Association for Computing Machinery, New York, NY, USA, 639–648. https://doi.org/10.1145/237814.238015

[4] Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., Jäschke, A., Reuter, C. A. & Strand, M. (2015). A Guide to Fully Homomorphic Encryption.. *IACR Cryptology ePrint Archive*, 2015, 1192.

[5] PieterMaene, Johannes Götzfried, Ruan de Clercq, TiloMüller, Felix Freiling, and Ingrid Verbauwhede. 2018. Hardware-Based Trusted Computing Architectures for Isolation and Attestation. IEEE transactions on computers.

[6] Valentina Zantedeschi, Aurélien Bellet, Marc Tommasi:
Fully Decentralized Joint Learning of Personalized Models and Collaboration Graphs. AISTATS 2020

[7] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. 2017. Practical Secure Aggregation for Privacy-Preserving Machine Learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). Association for Computing Machinery, New York, NY, USA, 1175–1191. https://doi.org/10.1145/3133956.3133982

[8] Davide Frey, Lucie Guillou, Michel Raynal, François Taïani:
Consensus-Free Ledgers When Operations of Distinct Processes are Commutative. PaCT 2021: 359-370

[9] Timothé Albouy, Davide Frey, Michel Raynal and Francois Taiani.
Good-case Early-Stopping Latency of Synchronous Byzantine Reliable Broadcast: The Deterministic Case. DISC 2022.

Principales activités

Main Activities

- Carry out theoretical or practical research on privacy preserving decentralized computation
- Implement solutions into research prototypes
- Write papers or research reports
- Present their work to team members, project partners and at International conferences
- Attend project meetings and project review meetings

Additional activities:

- Teach courses at the University of Rennes
- Co-Supervise research students

Compétences

- Good collaborative and networking skills, excellent written and oral communication in English
- Good programming skills
- Strong analytical skills
- Interest and ability to learn new topics in distributed computing, privacy, security, and machine learning.
- Prior knowledge on at least some of the following areas:
    - Secure Multiparty Computation
    - Trusted Execution Environments (SGX, Trustzone, others)
    - Machine Learning
    - Federated Learning
    - Distributed Systems
    - Privacy

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 2746 euros

Informations générales

- **Thème/Domaine :** Sécurité et confidentialité
  Système & réseaux (BAP E)
- **Ville :** Rennes
- **Centre Inria :** Centre Inria de l'Université de Rennes
- **Date de prise de fonction souhaitée :** 2023-01-01
- **Durée de contrat :** 12 mois
- **Date limite pour postuler :** 2022-12-31

Contacts

- **Équipe Inria :** WIDE
- **Recruteur :**
  Frey Davide / davide.frey@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.

L'essentiel pour réussir

You should hold a PhD in computer science and have a strong background in at least one of the following topics: multiparty computation, trusted execution environment, machine learning, distributed systems and algorithms. You should be interested in learning about the others, and in producing original research that combines the above variety of topics.

You should submit an academic CV comprising a research statement that covers at least partially the areas outlined in this offer.

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 contactdavide.frey@inria.fr Or francois.taiani@inria.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.