Offer #2022-05222

PhD Position F/M Access control for P2P without central authority

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Context

This PhD thesis will be in the context of a collaboration between HIVE and Coast and Wide Inria teams. The Ph.D student will be located at Inria Nancy-Grand Est and will be visiting Wide team at Inria Center of the University of Rennes and the Hive offices in Cannes.

About Hive:

Hive intends to play the role of a next generation cloud provider in the context of Web 3.0. Hive aims to exploit the unused capacity of computers to offer the general public a greener and more sovereign alternative to the existing clouds where the true power lies in the hands of the users. It relies both on distributed peer-to-peer networks, on the encryption of end-to-end data and on blockchain technology.

About Inria Nancy - Grand Est:

The Inria Nancy - Grand Est center is one of Inria's eight centers and has twenty project teams, located in Nancy, Strasbourg and Saarbrücken. Its activities occupy over 400 people, scientists and research and innovation support staff, including 45 different nationalities. 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 institutes, etc.

About Inria Center of the University of Rennes:

The Inria Center of the University of Rennes is one of Inria's eight centers 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 institutes, etc.

Assignment

An access control mechanism is needed to deal with user access rights over the shared documents. The main challenge in the context of a P2P storage lies in the need of the access-control mechanism that does not rely on a central authority to manage the rights of data belonging to different clients and companies. Such an access-control mechanism should be distributed and each client or company should be able to master the access rights associated with their data. The lack of a central authority raises issues of group management such as joining and leaving the group as well as rights revocation.

In this PhD thesis, we aim to propose a security mechanism adapted for distributed collaborative systems without a central authority. The security mechanism has to deal with user access rights to the shared documents as well as with end-to-end encryption of data and with key management suitable for dynamic user groups.

A possible solution for managing access-rights in a decentralized system lies in the use of Self-Sovereign Identity systems (SSI). An SSI makes it possible to assign users credentials and verify them in completely decentralized manner, without a trusted third party. However, existing SSI implementations rely on system-wide synchronization, generally implemented through the use of blockchain solutions.

Our intuition, that we will further explore in this PhD thesis, is that neither SSI nor access-control systems require the level of synchrony provided by the blockchain model. Rather, the lower level of consistency provided by CRDTs (Conflict-Replicated Data Types) [1, 2] and broadcast primitives are likely to be sufficient for most operation. But this leaves open the challenge of how to compose CRDTs for data with CRDTs for access control while preserving causality between these two types of data [3]. Our conjecture in this context is that synchrony may be required at a smaller scale for some specific tasks. For example, some amount of synchrony is probably required to make sure that the access right of users have not been revoked after being initially granted.

Unfortunately, if algorithms for Byzantine reliable broadcast have been known for a while [4], existing CRDTs cannot, apart from a few exceptions [5], withstand attacks or malicious behaviors. This PhD topic will design Byzantine tolerant CRDTs that can support scalable decentralised access-control systems. Such Byzantine Tolerant CRDTs will play a key role in the design of scalable tools for the management of access rights in decentralized systems.

In addition, we plan to investigate suitable end-to-end encryption techniques for collaboration over mutable data where messages sent between participants are end-to-end encrypted and servers do not need to access non encrypted data. Synchronisation algorithms based on Byzantine-Tolerant CRDT are suitable for end-to-end encryption in a peer-to-peer environment where data will be decrypted only at the receiver side and conflicts can be resolved locally.

We plan to evaluate existing group key management solutions such as [6] and their suitability for large dynamic groups where several users join and leave very often the group. Group key generation and revocation can be done in concurrency with modifications on the shared document. The challenge is to compose Byzantine-Tolerant CRDTs for access rights and data synchronisation with group key management operations.

References:

[1] M. Shapiro, N. M. Preguic□a, C. Baquero, and M. Zawirski. “Conflict-Free Replicated Data Types”. In: 13th International Symposium on Stabilization, Safety, and Security of Distributed Systems, SSS 2011. Oct. 2011, pp. 386–400. doi: 10.1007/978-3-642-24550-3_29.

[2] L. Andre□, S. Martin, G. Oster, and C.-L. Ignat. “Supporting adaptable granularity of changes for massive-scale collaborative editing”. In: Proceedings of the International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2013). Austin, Texas, USA, Oct. 2013

[3] P.-A. Rault, C.-L. Ignat, and O. Perrin. “ Distributed Access Control for Collaborative Applications using CRDTs”. In: Proceedings of 9th Workshop on Principles and Practice of Consistency for Distributed Data. Rennes, France, Apr. 2022.

[4] G. Bracha. “Asynchronous Byzantine Agreement Protocols”. In: Information and Computation 75.2 (1987), pp. 130–143. issn: 0890-5401. doi: 10.1016/0890-5401(87)90054-X.

[5] M. Kleppmann. “Making CRDTs Byzantine Fault Tolerant”. In: Proceedings of the 9th Workshop on Principles and Practice of Consistency for Distributed Data. PaPoC ’22. Rennes, France: Association for Computing Machinery, 2022, pp. 8–15. isbn: 9781450392563. doi: 10.1145/ 3517209.3524042.

[6] M. Burmester and Y. Desmedt. “A secure and efficient conference key distribution system”. In: Advances in Cryptology — EUROCRYPT’94. Ed. by A. De Santis. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 275–286. isbn: 978-3-540-44717-7. doi: 10.1007/BFb0053443.

Main activities

Programme

— A study of existing security mechanisms for collaborative systems, SSI, BFT protocols, as well as group encryption mechanisms

— Establishment of the requirements for the envisaged security mechanism through case studies

— Proposal of a group encryption mechanism that satisfies the requirements

— Study of CRDTs

— Proposal for a Byzantine-Tolerant CRDT for access rights

— Composition of the Byzantine-Tolerant CRDT for access rights with a CRDT for the content of shared data in the presence of encrypted data

Skills

- Engineering and/or Master 2 degree in Computer science / Applied mathematics with an experience in computer networks.
- Theoretical expertise: distributed systems, P2P networks, security
- Good collaborative and networking skills, excellent written and oral communication in English
- Good programming skills
- Strong analytical skills

Remuneration

1982,00€ brut mensuel les deux premières années (1594,00€ net)

2085,00€ brut mensuel la 3ème année (1677,00€ net)

1982,00€ gross monthly for the first two years (1594,00€ net)

2085,00€ gross monthly the 3rd year (1677,00€ net)

General Information

- **Town/city :** Villers lès Nancy
- **Inria Center :** Centre Inria de l'Université de Lorraine
- **Starting date :** 2022-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2022-09-30

Contacts

- **Inria Team :** COAST
- **PhD Supervisor :**
  Ignat Claudia-lavinia / claudia.ignat@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.