Offer #2024-07411

PhD Position F/M Security mechanisms for distributed collaborative systems

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Context

This PhD thesis will take place in team COAST and will be supervised by Claudia-Lavinia Ignat, HDR, CRCN Inria, Inria center of Lorraine University and Olivier Perrin, Professor, Lorraine University.

Assignment

We want 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 with **key management** suitable for dynamic user groups. The mechanism has to be **easy to use** and will be tested with users.

Existing access control mechanisms mainly based on a central authority feature several difficulties in the context of collaborative systems. In the case of a federation of organizations, agreeing on an authority that manages access rights is almost impossible. Lack of a central authority raises issues of group management such as joining and leaving the group as well as rights revocation. Indeed, it should be possible for a partner to revoke granted rights without contacting an external authority. Moreover, current access control mechanisms feature performance issues that are critical for real-time collaboration where the number of updates is high. Indeed, delays are too high for sending at each user action an access request and waiting for its answer from a trusted central authority which maintains the security policies.

In order to provide high data availability in collaborative systems, data is typically replicated and users are allowed to concurrently modify replicated data. In order to avoid the use of a central server that stores access rights, we propose that in addition to the replication of data, access rights are also replicated. CRDTs (Commutative Replicated Data Types) [1, 2] were proposed as suitable replicated data structures where parallel modifications are conflict free by construction. We want to propose **CRDTs for managing replicated data and replicated access control**.

In the face of concurrent edits on the access rights and the document, conflicts are likely to occur. For instance, users might execute operations on the document while their rights of executing these operations are concurrently revoked. An important feature of collaborative applications is to allow multiple dynamic administrators that can modify users access rights (e.g. read or write) to the shared documents. Existing solutions that replicate access rights rely either on a single administrator per document [3, 4] or on centralised coordination mechanisms to avoid conflicts introduced by multiple administrators [5]. Considering multiple administrators generates more conflictual cases to deal with than in the case of a single administrator [6,7]. For instance, an administrator might assign an access right to a user, while concurrently this administrator right is removed. We want to propose a replicated access control mechanism that manages a collaborative document with multiple, dynamic administrators. Besides maintaining consistency over the replicated document state and access rights, the proposed CRDT solution should preserve document integrity and prevent unauthorized modifications. An a posteriori enforcement should be provided in order to correct the document state by compensating the effect of unauthorized modifications.

Group key generation and revocation can be done in concurrency with modifications on the shared document and its access rights. The challenge is to **compose CRDTs for access rights and data synchronisation with group key management operations**.

As mentioned above, **end-to-end encryption** is very important for ensuring the security of mutable data in the collaboration. Large collaborative service providers such as Dropbox, iCloud and GoogleDrive adopted encryption solutions in order to store only the encrypted version of shared documents. However, for facilitating the usage of their services, encryption keys are stored by the service providers which gives them the possibility of accessing the non encrypted data and being subject to different attacks. 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. Synchronization algorithms based on 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.

The access control mechanism proposed in this thesis will be implemented on a peer-to-peer collaborative real-time editor such as MUTE (https://github.com/coast-team/mute). Its feasibility will be tested for Matrix (https://matrix.org/), a protocol for secure, decentralised communication, and compared to its current access control mechanism [8]. The proposed solution will be tested by means of user studies.

Bibliography:

[1] Ge□rald Oster, Pascal Urso, Pascal Molli, and Abdessamad Imine. “Data Consistency for P2P Collaborative Editing”. In: Proceedings of the ACM Conference on Computer-Supported Cooperative Work - CSCW 2006. Banff, AB, Canada, 2006, pp. 259–267. isbn: 1-59593-249-6. doi: 10.1145/1180875.1180916.

[2] Marc Shapiro, Nuno M. Preguic□a, Carlos Baquero, and Marek 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.

[3] Ted Wobber, Thomas L. Rodeheffer, and Douglas B. Terry. “Policy-Based Access Control for Weakly Consistent Replication”. In: Proceedings of the 5th European Conference on Computer Systems. EuroSys ’10. Association for Computing Machinery, Apr. 2010, pp. 293–306. isbn: 978-1-60558-577-2. doi: 10.1145/1755913.1755943. (Visited on 04/01/2021).

[4] Asma Cherif, Abdessamad Imine, and Michae□l Rusinowitch. “Practical Access Control Management for Distributed Collaborative Editors”. Pervasive and Mobile Computing. Special Issue on Information Management in Mobile Applications 15 (Dec. 2014), pp. 62–86. issn: 1574-1192. doi: 10.1016/j.pmcj.2013.09.004.

[5] Mathias Weber, Annette Bieniusa, and Arnd Poetzsch-Heffter. “Access Control for Weakly Consistent Replicated Information Systems”. In: Proceedings of International Workshop on Security and Trust Management. STM 2016. Springer International Publishing, Sept. 2016, pp. 82–97. isbn: 978-3-319-46598-2. doi: 10.1007/978-3-319-46598-2_6.

[6] Pierre-Antoine Rault, Claudia-Lavinia Ignat, and Olivier 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. doi: 10.1145/3517209.3524826. hal: hal-03584553.

[7] Pierre-Antoine Rault, Claudia-Lavinia Ignat, and Olivier Perrin. “Access control based on CRDTs for Collaborative Dis- tributed Applications”. In: The International Symposium on Intelligent and Trustworthy Computing, Communications, and Networking (ITCCN-2023), Proceedings of the 22nd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2023). Exeter, UK, Nov. 2023. hal: hal-04224855.

[8] Florian Jacob, Luca Becker, Jan Grashöfer, Hannes Hartenstein. Matrix Decomposition: Analysis of an Access Control Approach on Transaction-based DAGs without Finality. SACMAT 2020: 81-92. doi:10.1145/3381991.3395399

Main activities

- Study of existing access control mechanisms for collaborative systems
- Elicitation of requirements for the envisaged security mechanism through case studies
- Proposal of a group key management that satisfies the requirements
- Study of CRDTs
- Proposal of a composed CRDT that combines a CRDT for shared data with a CRDT for access rights with and that considers group key management operations
- Implementation of the proposed security mechanism in MUTE
- User studies on the proposed security mechanism

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

Benefits package

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours

- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Remuneration

2100€ gross/month the 1st year

General Information

- **Theme/Domain :** Distributed Systems and middleware
  Information system (BAP E)
- **Town/city :** Villers lès Nancy
- **Inria Center :** Centre Inria de l'Université de Lorraine
- **Starting date :** 2024-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2024-07-12

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.