



Offre n°2024-07944

## PhD Position F/M Improving security and performance of IPFS's DHT

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

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Doctorant

### Contexte et atouts du poste

The PhD student will be hosted by Coast team. Collaborative work between COAST and RESIST teams and HIVE. Funding granted by France 2030, project PEPR Cloud, subproject TrustInCloudS.

### Mission confiée

#### Scientific Context

The InterPlanetary File System (IPFS) is a modern fully distributed system for storing and accessing files with the goal to decentralize content storage and distribution over Internet from a few big actors (GAFAM, Content Delivery Networks) to the edge. It brings together a well-known underlying P2P network architecture (based on the Kademlia Distributed Hash Table [1]) on top of which additional data structures are used to manage content addressing and versioning (Content Identifiers (CIDs), Merkle DAGs, Mutable File System (MFS)).

However, recent studies [2,3] have shown that the IPFS's DHT implementation was left defenseless for years against legacy Sybil attacks that could easily prevent access to shared content. Some mitigation has been proposed but may induce overhead on the DHT usage, which is already critical because Hive uses the DHT beyond the simple indexing of files and sources, so a security vs performance trade-off must be carefully considered.

#### Objectives

The goal of this PhD thesis is to improve the security and performance of IPFS's DHT to support current and future Hive operations. The PhD student will design and evaluate new attack strategies against IPFS with active attacker models, confront them against defense mechanisms from the state of the art such as [4], combine them, and propose new ones if needed. In particular, the impact on performance will be considered to define a curated selection of the best defense mechanisms.

This PhD thesis will be in the context of the collaboration with Hive (<https://www.hivenet.com/>). Hive's goal is to propose a new cloud compute and storage service leveraging a fully distributed and collaborative P2P infrastructure instead of traditional data-center solutions. It is partly based on the IPFS source code and in particular on the libP2P that implements the DHT, but it adds service-level guarantees thanks to additional mechanisms to circumvent the unreliable nature of peers.

Once basic DHT operations in IPFS are secured and optimized, this PhD thesis will consider the security and the performance of Hive's additional services such as data replication, collaborative edition and retrieval.

#### Bibliography

1. Kademlia: A Peer-to-Peer Information System Based on the XOR Metric, Petar Maymounkov and David Mazières. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS '01)*, 2002. Springer-Verlag, Berlin, Heidelberg, 53-65. doi:[1007/3-540-45748-8\\_5](https://doi.org/10.1007/3-540-45748-8_5)
2. Content Censorship in the InterPlanetary File System, Srivatsan Sridhar, Onur Ascigil, Navin Keizer, François Genon, Sébastien Pierre, Yiannis Psaras, Etienne Rivière, and Michał Król. 2024. In *31st Annual Network and Distributed System Security Symposium, NDSS 2024*. The Internet Society, 1-17. doi: [10.14722/ndss.2024.23153](https://doi.org/10.14722/ndss.2024.23153)
3. Sybil Attack Strikes Again: Denying Content Access in IPFS with a Single Computer, Thibault Cholez, Claudia-Lavinia Ignat, *The 19th International Conference on Availability, Reliability and Security (ARES'24)*, August 2024, Vienna, Austria
4. S/Kademlia: A practicable approach towards secure key-based routing, I. Baumgart and S. Mies, *2007 International Conference on Parallel and Distributed Systems Hsinchu, Taiwan, 2007*, pp. 1-8,

## Principales activités

- gain knowledge from the academic state of the art on DHT security and performance considerations, and on IPFS and Hive source code (6 months);
- define and evaluate active attacker scenarios against IPFS (6 months);
- define and evaluate an efficient mitigation mechanism (6 months);
- define and evaluate active attacker scenarios against Hive's services (6 months);
- define and evaluate an efficient mitigation mechanism (6 months);
- write the PhD thesis manuscript (6 months).

## Compétences

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

## Avantages

- 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

## Rémunération

2100€ gross/month (the 1st year)

## Informations générales

- **Thème/Domaine** : Systèmes distribués et intergiciels  
Système & réseaux (BAP E)
- **Ville** : Villers lès Nancy
- **Centre Inria** : [Centre Inria de l'Université de Lorraine](#)
- **Date de prise de fonction souhaitée** : 2025-01-01
- **Durée de contrat** : 3 ans
- **Date limite pour postuler** : 2024-08-08

## Contacts

- **Équipe Inria** : [COAST](#)
- **Directeur de thèse** :  
Ignat Claudia-lavinia / [claudia.ignat@inria.fr](mailto:claudia.ignat@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.