Proposition de stage M2/ PFE Ingénieur (6 mois)
Anonymisation des données IoT dans les systèmes Blockchain

Un des freins principaux au déploiement à très large échelle de services IoT en tout genre aujourd'hui réside dans les risques de dévoiler des informations personnelles lorsque l'on partage des données issues des objets connectés. Ce risque est à la fois présent lorsque les objets appartiennent à des particuliers que lorsqu'ils appartiennent à des entreprises ou à des collectivités locales. Ainsi, toute entreprise ou collectivité qui déploierait des objets connectés au sein de son espace, publique ou privé, doit veiller à ce que les informations personnelles de ses utilisateurs, lesquels qui fréquentent son espace, ne peuvent être dévoilées, au risque de se retrouver en infraction vis-à-vis de la nouvelle réglementation européenne sur la protection des données personnelles (RGPD).

Par ailleurs, aussi bien les utilisateurs individuels que les organisations publiques ou privées, rechignent aujourd'hui à faire confiance à des organismes qui centraliserait toute la connaissance (des tiers de confiances centralisés). En effet, la puissance de l'IoT et les perspectives de déploiement massif d'objets connectés que ce paradigme promet, mettraient une responsabilité, et une puissance, énorme entre les « mains » de ces tiers de confiance. Une solution complétement distribuée, de type pair-à-pair, serait donc plus adéquate à condition d'être renforcée au niveau de l'anonymisation des données personnelles des fournisseurs de données IoT. Il est largement admis aujourd'hui que la Blockchain peut représenter cette solution distribuée et ne dépendant d'aucune entité centralisée.

Afin d'assurer l'anonymisation des données personnelles des utilisateurs IoT, les systèmes « Blockchain » utilisent la notion de pseudonyme. Il a cependant été démontré dans la littérature qu'il existe plusieurs techniques de dés-anonymisation possibles dans les systèmes Blockchain. Ainsi, par exemple, lorsqu'un utilisateur émet une transaction avec plusieurs pseudonymes en entrée, il révèle posséder tous ces pseudonymes. Il suffit donc de les lier entre eux [1, 2, 3] pour pouvoir attribuer tous ces pseudonymes à un même utilisateur et ainsi le suivre avec précision. Il est donc clair qu'il est nécessaire de repenser complétement le système de pseudonymes utilisé actuellement dans les systèmes Blockchain. Cet objectif ambitieux serait l'objectif à terme d'une thèse de Doctorat laquelle ferait suite à ce stage. Ainsi, dans un premier temps, le stage s'intéressera surtout à proposer une première version d'algorithme de garantie d'anonymat compatible avec les systèmes Blockhain en termes de fonctionnalité et robustesse. Les tâches du stagiaire se diviseront en trois étapes :

- Etude de l'état de l'art autour de l'anonymisation dans les Blockchains ;
- Comparaison des techniques d'anonymisation existantes ;
- Conception et implémentation d'un algorithme d'anonymisation des données IoT, pour les systèmes Blockchain.

Mots clés : Blockchain, RGPD, Anonymisation, données IoT

Références

[1] M. Spagnuolo, F. Maggi, and S. Zanero, "BitIodine: Extracting Intel- ligence from the Bitcoin Network," in Financial Cryptography, ser. Lecture Notes in Computer Science, vol. 8437. Springer, 2014, pp. 457–468.

[2] J. Herrera-Joancomarti, "Research and Challenges on Bitcoin Anony- mity," in DPM/SETOP/QASA, ser. Lecture Notes in Computer Science, vol. 8872. Springer, 2014, pp. 3–16.

[3] M. Moser, R. Bohme, and D. Breuker, "An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem." [Online]. Available: https://maltemoeser.de/paper/money- laundering.pdf

Profil recherché :

Etudiant(e) en Master 2 ou 3ème année Ingénieur, Informatique, avec des connaissances en sécurité système et réseaux, en système et programmation, et ayant un esprit collaboratif, et motivé pour un travail de recherche.

Durée et période :

6 mois, à partir de mi-janvier/début février 2019.

Contact :

Rim Ben Messaoud, Post-doctorante, L3i/Université de La Rochelle, rim.ben_messaoud@univ-lr.fr.

Yacine Ghamri-Doudane, Professeur, L3i/Université de La Rochelle, yacine.ghamri@univ-lr.fr.

Lieu du stage :

Laboratoire Informatique, Image et Interaction (L3i) - https://l3i.univ-larochelle.fr

Facultés des Sciences et Technologies – Université de La Rochelle

Avenue Michel Crépeau, 17042 La Rochelle Cedex 1 - France

Rémunération : gratification réglementaire des stages en France (cf. https://www.service-public.fr/professionnels-entreprises/vosdroits/F32131).