Offre de stage en laboratoire entre mars et août 2023 :

Mise en œuvre scalable de solutions d'apprentissage fédéré sur des réseaux orientés contenu : application à la détection d'attaque dans les clouds publics

Contexte du stage

L'apprentissage fédéré est un paradigme qui permet à différents clients d'échanger leurs modèles sans révéler les données qui ont permis son élaboration. Fondé initialement sur un composant central d'agrégation et de diffusion des modèles, différentes solutions architecturales de l'état de l'art visent à améliorer la performance globale de cette architecture par des solutions de décentralisation, ou d'identification et clusterisation de clients selon des critères de proximité des données ou de réputation, par exemple. Dans ce contexte, le paradigme des réseaux orientés contenu apparaît comme une solution prometteuse pour assurer le facteur d'échelle des approches d'apprentissage fédéré, de par l'abstraction de la localisation des données pour leur publication et accès, la mise en cache des données au plus proche de leur accès et enfin la possibilité d'effectuer des calculs d'agrégats directement dans le réseau.

Objectif du stage

Dans un contexte de détection d'attaques par déni de service distribuée opérée dans un environnement de cloud public multi-tenants, il sera question ici d'évaluer la performance d'un algorithme d'apprentissage fédéré, sélectionné dans la littérature pour sa capacité à détecter des attaques multi-tenants, mis en œuvre sur un réseau orienté contenu tel que Named Data Networking.

Travail attendu

Les différentes étapes du stage sont les suivantes :

1. Étude bibliographique sur (1) l'apprentissage fédéré pour la détection d'intrusion à grande échelle, (2) les réseaux orientés contenu et (3) les premiers travaux scientifiques qui couplent de ces deux paradigmes. A l'issue de cette étape, on sélectionnera les approches mises en œuvre par la suite.
2. Implémentation d'une méthode de détection d'attaque de type DoS dans un environnement multi-tenant sur un substrat de réseau orienté contenu. On s'intéressera notamment au nommage des données échangées et leur cachabilité.
3. Mise en œuvre d'une campagne d'évaluation de performance de la solution développée. On identifiera ici des scénarios de tests mettant notamment en exergue le facteur d'échelle et on sélectionnera les métriques qui permettront de caractériser la performance de l'approche.
4. Collecte des données, traitement et analyse des résultats.

Compétences nécessaires

Idéalement, les candidats doivent connaitre les outils mathématiques d'apprentissage automatique (y compris profond) et un framework d'implémentation (eg. Tensorflow, PyTorch…). Des connaissances en sécurité et détection d'intrusion en particulier seront appréciées. Au-delà, des compétences générales en informatique sont requises (au niveau réseau, système et programmation/scripting).

Conditions du stage

Le stage se déroule à IMT Atlantique (site de Rennes) au sein l'axe Cybersécurité de l'équipe OCIF de l'IRISA. Un bureau, partagé par plusieurs étudiants en stage, sera alloué au stagiaire avec un ordinateur fixe pour le travail.
La rémunération de stage se situe autour de 530€ par mois.

Contacts

Léo Lavaur : leo.lavaur@imt-atlantique.fr
Guillaume Doyen : guillaume.doyen@imt-atlantique.fr

Références

[1] S., Manolis, B. Kohler, C. Scherb, and C. Tschudin. « An information centric network for computing the distribution of computations ». In Proceedings of the 1st ACM Conference on Information-Centric Networking, 137-46. ACM-ICN '14. New York, NY, USA: Association for Computing Machinery, 2014. https://doi.org/10.1145/2660129.2660150.
[2] L. Lavaur, M. -O. Pahl, Y. Busnel and F. Autrel, "The Evolution of Federated Learning-based Intrusion Detection and Mitigation: a Survey," in IEEE Transactions on Network and Service Management (TNSM), 2022, doi: 10.1109/TNSM.2022.3177512
[3] Amadeo, Marica, Claudia Campolo, Antonio Iera, Antonella Molinaro, et Giuseppe Ruggeri. « Client Discovery and Data Exchange in Edge-based Federated Learning via Named Data Networking ». In ICC 2022 - IEEE International Conference on Communications, 2990-95, 2022. https://doi.org/10.1109/ICC45855.2022.9839172..