



Intelligence distribuée et sécurisée pour les environnements contraints

23 juin 2021, 02:00

Nicolás González-Deleito

Les développements récents en intelligence artificielle distribuée en périphérie (edge) donnent lieu à de nouvelles approches en matière d'analyse distribuée sécurisée et ciblée. Dans le cadre de plusieurs projets de recherche, Sirris étudie une mise à l'échelle efficace en termes d'énergie et de ressources des applications reposant sur l'intelligence artificielle dans l'infrastructure périphérique existante, tout en préservant les données sensibles.

Les entreprises tirent parti de l'avènement des nœuds périphériques dotés de capacités accrues de calcul et de stockage en exécutant un large éventail d'applications de plus en plus gourmandes en ressources à travers un nombre croissant de dispositifs hautement instrumentés. Dans le cas des applications de surveillance et de contrôle industriels, cela se traduit par d'énormes quantités de données, réparties sur une multitude d'appareils sur le terrain. Actuellement, toutes ces données sont généralement transférées vers un emplacement central (p. ex. cloud) pour être exploitées par l'apprentissage automatique intelligent et l'IA.

Limites du cloud computing centralisé

Toutefois, ce modèle traditionnel de centralisation de la création et de l'analyse de grands ensembles de données ne représente pas une solution viable pour l'analyse distribuée ciblée. Le déchargement des capacités de traitement dans le cloud implique les limitations et contraintes suivantes :

- > **disponibilité** des canaux de communication sous-jacents et de l'infrastructure cloud
- > mécanismes nécessaires pour **sécuriser les données** en transit et au repos (en particulier lorsque des **données sensibles** sont en jeu)
- > **coûts** liés à la transmission des données et à l'utilisation de l'infrastructure cloud dorsale
- > **latence inacceptable** des canaux de communication sous-jacents pour de nombreuses applications de contrôle industriel et applications soumises à des contraintes en temps réel

En outre, en fonction de l'application et de l'infrastructure sous-jacente, seule une **fraction des données** est transférée vers la dorsale pour analyse, en raison des limitations de la bande passante ou des contraintes de coût, tandis que les données restantes sont ignorées à un stade très précoce.

Informatique en périphérie (edge computing)

En alternative au modèle traditionnel, qui amène les données aux algorithmes intelligents, on peut amener ces algorithmes aux données tout en continuant d'exploiter les informations de nombreux utilisateurs. C'est l'intelligence artificielle distribuée en périphérie.

Le calcul en périphérie peut réduire le volume de données à déplacer et le trafic global grâce à des **architectures massivement parallèles et distribuées**. Il réduit la distance que les données doivent parcourir, diminuant donc la latence des communications et les coûts de transmission. La répartition des tâches de calcul intensif sur les ressources locales augmente l'extensibilité et permet d'améliorer considérablement les temps de réponse des applications critiques en temps réel. En outre, l'instance centralisée n'est plus un point de défaillance unique et les appareils peuvent fonctionner indépendamment pendant un certain temps.

Intelligence distribuée et sécurisée dans le cadre de 3 projets européens

Dans le cadre des trois projets européens de R&D présentés ci-dessous, Sirris explore des approches efficaces en termes d'énergie et de ressources pour mettre à l'échelle des applications de calcul en périphérie basées sur l'IA, en les orchestrant et en les distribuant aux infrastructures en périphérie existantes, tout en préservant la vie privée des utilisateurs. Les modèles et techniques d'apprentissage automatique distribué et composable, qui se déploient horizontalement entre les appareils périphériques (ainsi que verticalement vers le cloud), permettent également aux applications d'assurer une prise de décision performante.

L'informatique en périphérie pourra ainsi apporter des capacités de traitement et d'analyse en temps réel à proximité du point d'utilisation et de la source des données. Elle réduira considérablement la nécessité d'une connexion coûteuse et relativement lente au cloud, qui

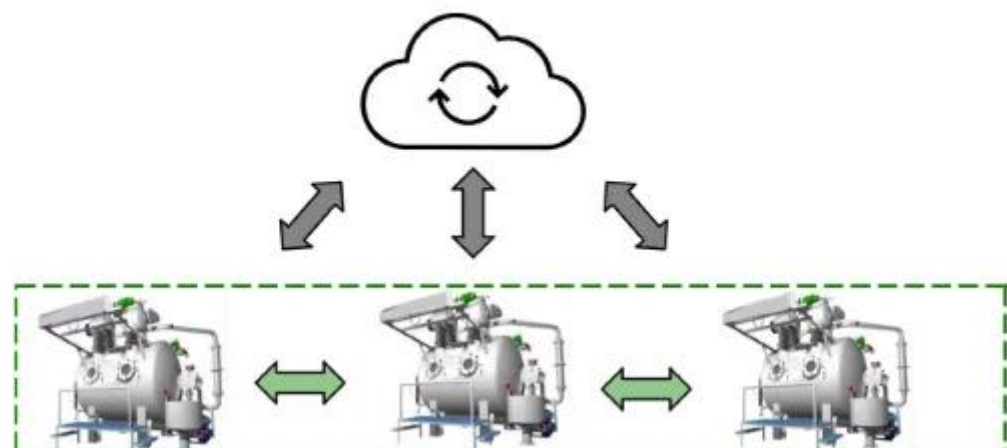
constitue un goulot d'étranglement pour l'analyse. Par ailleurs, aucune information personnelle n'est stockée dans un emplacement centralisé. Les tâches de collecte des données, d'apprentissage automatique et d'inférence des applications d'IA peuvent être distribuées dans une architecture fédérée. Une telle solution est robuste, car les tâches peuvent migrer en cas de défaillance d'un composant.



DAIS (ECSEL, mai 2021 - avril 2024) - ce projet vise à rechercher et à fournir des systèmes d'intelligence artificielle distribuée en résolvant les problèmes d'exécution des algorithmes existants sur des appareils périphériques largement distribués. Les actions de recherche et d'innovation du projet DAIS s'articulent autour de huit chaînes logistiques. Cinq d'entre elles se concentrent sur la fourniture du matériel et des logiciels nécessaires pour faire fonctionner une IA de niveau industriel sur différents types de topologies de réseau. Les autres chaînes logistiques montrent comment cette initiative paneuropéenne relève des défis connus en matière d'IA dans différents domaines fonctionnels.

Fourni par Sentigrate, le cas d'utilisation belge porte sur un moteur de **positionnement** en périphérie.

MIRAI (ITEA3, décembre 2020 - novembre 2023) - ce projet entend développer les blocs de construction du cadre MIRAI (MIRAI Framework Building Blocks – MFBB) en s'appuyant sur des techniques d'IA pour permettre une planification et une exploitation intelligentes et durables des applications IoT et d'informatique en périphérie. Ceux-ci compléteront l'approche traditionnelle de mise à l'échelle au cloud par une mise à l'échelle horizontale des applications IoT et d'informatique en périphérie entre les appareils périphériques. Fournis par 3E, Macq et Shayp, les cas d'utilisation belges portent





SunRISE (PENTA, septembre 2019 - août 2022) - ce projet a pour objectif de développer une solution de sécurité partagée portant sur : (i) l'apprentissage automatique en périphérie facilitant l'analyse de la sécurité IoT pour se protéger contre les intrusions et détecter les anomalies et mauvaises configurations, (ii) le partage de données de sécurité pertinentes entre différents intervenants et l'application de l'apprentissage automatique aux données et modèles combinés, et (iii) l'évaluation du chiffrement homomorphe comme technologie d'amélioration de la confidentialité et l'application de l'apprentissage automatique aux ensembles de données chiffrées combinés. Les partenaires belges (Engie Laborelec, NXP et Sirris) feront la démonstration des résultats de SunRISE dans le contexte d'un cas d'utilisation des **communautés d'énergie** (réseau intelligent).

Pour soutenir ces activités et d'autres à venir, le Data and AI Competence Lab et le groupe Software Engineering de Sirris se sont associés pour conjuguer leur savoir-faire en matière d'approches d'IA distribuée pour les dispositifs à ressources limitées et la sécurité et la confidentialité des données (analyse) en périphérie, dans le fog, dans le cloud et en transit.

AGENTSCHAP
INNOVEREN &
ONDERNEMEN



Vlaanderen
is ondernemen

innoviris
.brussels
we fund your future

]]>

Auteurs



Nicolás González-Deleito