



Beveiligde en gedistribueerde intelligentie voor omgevingen met resourcebeperkingen

23 juni 2021, 02:00

Nicolás González-Deleito

De recente ontwikkelingen in gedistribueerde AI aan de rand resulteren in nieuwe benaderingen voor beveiligde en gerichte gedistribueerde analyses. In het kader van verschillende onderzoeksprojecten bestudeert Sirris de energie- en resource-efficiënte schaling van AI-gebaseerde toepassingen binnen de bestaande randinfrastructuur, mét bescherming van de privacygevoelige gegevens.

Bedrijven maken gebruik van de opkomst van edge nodes met verhoogde reken- en opslagcapaciteiten door een brede waaier van resource-intensieve toepassingen uit te voeren via een toenemend aantal sterk geïntegreerde apparaten. In het geval van, bijvoorbeeld, industriële bewakings- en controletoepassingen resulteert dit in enorme datahoeveelheden, verspreid over een groot aantal apparaten op het terrein. Momenteel worden al deze data doorgaans overgedragen naar een centrale locatie (bijv. de cloud) om daar door intelligent machinelere en AI te worden geëxploiteerd.

Beperkingen van gecentraliseerde cloud computing

Dit traditionele model van gecentraliseerd creëren en analyseren van grote dataverzamelingen is echter geen levensvatbare oplossing voor gerichte gedistribueerde analyses. Het overdragen van verwerkingscapaciteit naar de cloud vereist het omgaan met de volgende beperkingen en grenzen:

- > de **beschikbaarheid** van de onderliggende communicatiekanalen en van de cloudinfrastructuur
- > de noodzakelijke mechanismen om de **gegevens** tijdens de overdracht en in rust te **beveiligen** (vooral bij **privacygevoelige** gegevens)
- > de **kosten** die voortvloeien uit de data-overdracht en uit het gebruik van de backend cloudinfrastructuur
- > de **onaanvaardbare latentie** van de onderliggende communicatiekanalen voor vele industriële besturingstoepassingen en toepassingen met realtimebeperkingen

Afhankelijk van de toepassing en de onderliggende infrastructuur wordt bovendien slechts een **fractie van de gegevens** naar de backend doorgestuurd voor analyse, als gevolg van bandbreedte- of kostenbeperkingen, terwijl de resterende data in een zeer vroeg stadium worden genegeerd.

Edge computing

Een alternatief voor het traditionele model, waarbij de data naar de intelligente algoritmen worden gebracht, is deze algoritmen naar de data te brengen, mét benutting van de informatie van vele gebruikers: gedistribueerde AI aan de rand.

Edge computing heeft het potentieel om het te verplaatsen datavolume en het totale verkeer terug te dringen, dankzij **massale parallelle en gedistribueerde architecturen**. Dit verkort de afstand die de data moeten afleggen, wat de communicatielatentie en de transmissiekosten doet dalen. De distributie van rekenintensieve taken over lokale resources verhoogt de schaalbaarheid en leidt tot een aanzienlijke verbetering van de responstijden voor realtime kritische toepassingen. Daarnaast is de gecentraliseerde instantie niet langer een single point of failure, maar kunnen de apparaten een tijdlang onafhankelijk werken.

Beveiligde en gedistribueerde intelligentie in het kader van 3 Europese projecten

In het kader van de 3 onderstaande Europese R&D-projecten bestudeert Sirris energie- en resource-efficiënte benaderingen om AI-gebaseerde edge computing toepassingen te schalen, door ze te organiseren en te distribueren over de bestaande randinfrastructuur, mét behoud van de privacy van de gebruikers. Gedistribueerde en samenstelbare modellen en technieken van machinelereen die horizontaal schalen tussen randapparaten (en verticaal naar de cloud), laten het de toepassingen ook toe om een kwalitatieve besluitvorming te garanderen.

Hierdoor zal edge computing realtime verwerkings- en analysemogelijkheden kunnen bieden nabij de plaats van gebruik en de bron van gegevens. Er zal fors minder nood zijn aan een dure en relatief trage verbinding met de cloud (een knelpunt voor de analyse) en tegelijk wordt geen enkele persoonlijke informatie op een gecentraliseerde plaats opgeslagen. Gegevensverzameling, machineleren en inferentietaken van AI-toepassingen kunnen in een federatieve architectuur worden gedistribueerd. Een dergelijke oplossing is robuust omdat, in geval van defecte componenten, deze taken kunnen migreren.

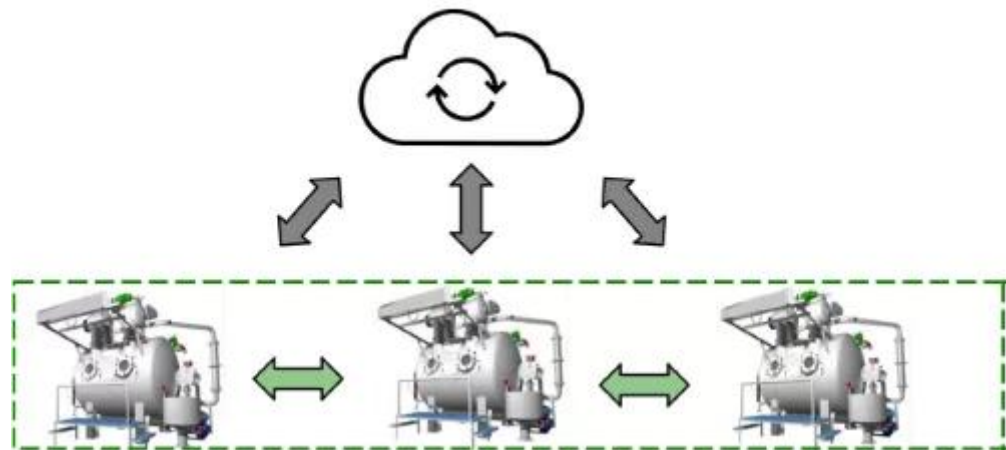


DAIS (ECSEL, mei 2021 - april 2024) - is bedoeld om gedistribueerde AI-systemen te onderzoeken en te leveren, door het oplossen van problemen bij het uitvoeren van bestaande algoritmen op breedscalig gedistribueerde randapparatuur. De onderzoeks- en innovatieacties in het DAIS-project zijn toegespitst op acht verschillende toeleveringsketens. Vijf ervan zijn gericht op het aanleveren van de nodige hard- en software om industriële AI te laten draaien op verschillende types van netwerktopologieën. De overige toeleveringsketens laten zien hoe deze pan-Europese inspanning gekende AI-uitdagingen, uit verschillende functionele domeinen aanpakt.

Het Belgische gebruiksscenario van Sentigrade is toegespitst op een **positioneringsmachine** aan de rand.

MIRAI (ITEA3, december 2020 - november 2023) - richt zich op de ontwikkeling van de MIRAI Framework Building Blocks (MFBB), op basis van AI-technieken, om een slimme en duurzame planning en werking van IoT- en edge computing-toepassingen mogelijk te maken. Deze zullen de traditionele schaalbenadering van de cloud aanvullen met een horizontale schaling van IoT- en edge computing-toepassingen tussen randapparaten.

De Belgische gebruiksscenario's van 3E, Macq en Shayp richten zich



SunRISE (PENTA, september 2019 - augustus 2022) - beoogt de ontwikkeling van een gezamenlijke beveiligingsoplossing om het volgende aan te pakken: (i) de implementatie van machinelere aan de edge nodes mogelijk maken, wat IoT-beveiligingsanalyses vergemakkelijkt om zich te beschermen tegen aanvallen van hackers, anomalieën en onjuiste configuraties; (ii) het delen van pertinente veiligheidsgegevens tussen verschillende belanghebbenden mogelijk maken en machinelere toepassen op de gecombineerde data en modellen; (III) de homomorphe encryptie evalueren als een technologie voor het verbeteren van de privacy en machinelere toepassen op de gecombineerde versleutelde datasets.

De Belgische partners (Engie Laborelec, NXP en Sirris) zullen de resultaten van SunRISE demonstreren in de context van een gebruiksscenario voor **energiegemeenschappen** (slim netwerk).



Om deze en toekomstige activiteiten te steunen, hebben het Data and AI Competence Lab en de Software Engineering groep van Sirris de handen in elkaar geslagen, door het bundelen van hun knowhow over zowel gedistribueerde AI-benaderingen voor apparaten met resourcebeperkingen als veiligheid en privacy van data(analyse) in een edge-/fog-infrastructuur, in de cloud en tijdens de overdracht.



]]>

Auteurs



Nicolás González-Deleito