Offre n°2024-07086

Privacy on-demand and Security preserving Federated Generative Networks or Models

Type de contrat : Fixed-term contract

Contrat renouvelable : Oui

Niveau de diplôme exigé : Master's or equivalent

Fonction : Internship Research

A propos du centre ou de la direction fonctionnelle

The Inria centre at Université Côte d'Azur includes 37 research teams and 8 support services. The centre's staff (about 500 people) is made up of scientists of different nationalities, engineers, technicians and administrative staff. The teams are mainly located on the university campuses of Sophia Antipolis and Nice as well as Montpellier, in close collaboration with research and higher education laboratories and establishments (Université Côte d'Azur, CNRS, INRAE, INSERM ...), but also with the regiona economic players.

With a presence in the fields of computational neuroscience and biology, data science and modeling, software engineering and certification, as well as collaborative robotics, the Inria Centre at Université Côte d'Azur is a major player in terms of scientific excellence through its results and collaborations at both European and international levels.

Contexte et atouts du poste

Teams and supervision

· INRIA : COATI (Frédéric Giroire, Chuan Xu), EPIONE (Marco Lorenzi)

· NOKIA: Bell Labs Core Research

Mission confiée

Future sixth-generation (6G) networks will be highly heterogeneous, with the massive development of mobile edge computing inside networks. Furthermore, 6G is expected to support dynamic network environments and provide diversified intelligent services with stringent Quality of Service (QoS) requirements. Various new intelligent applications and services will emerge (including augmented reality (AR), wireless machine interaction, smart city, etc) and will enable tactile communications and In- ternet of everything (IoE). This will challenge wireless networks in the dimensions of delay, energy consumption, interaction, reliability, and degree of intelligence and knowledge, but also in the dimension of information and data sharing. In turn, 6G networks will be expected about leveraging data at the next step of the new communication system generation. First of all, they will generate large amounts of data much more data than 5G networks: multiple sources as Core, Radio Access Network, OAM, User Equipments (UEs) but also as private and/or personal devices/machines massively con- nected, data-generator applications as sensing, localization, context-awareness services etc. Besides, unlike today's networks where traffic is almost entirely centralized, most 6G traffic will remain localized and highly distributed. The communication system will not only provide the bits reliably, but more importantly will provide the intelligent data processing through connectivity and resources computing in the devices, the edge, and the cloud in the network. For this, with Artificial Intelligence (AI) and Machine Learning (ML), machines will bring to networks the necessary intelligence very close to the place of action and decision-making and will also make data sharing possible.

Reliable and efficient transmission, data privacy and security are great challenges in data sharing. Specially for 5G advanced and 6G networks data is distributed with the wide deployment of various connected Internet of Thing (IoT) devices, and are generated from many distributed network nodes, e.g., end users, small Base Stations or Distributed Units and the network edge. Also, how to col- lect/share efficiently data from multiple sources (e.g., sensors or device) up to AI/ML-based Network applications/services of Orchestration and Automation Layer (network management system) in Edge? The models shall be trained, updated regularly and operate in real-time.

Recently, generative models have been demonstrated playing a key role in data sharing while pre-serving privacy and security. They are able to generate synthetic data which distribution is similar to the original data one. So, instead of sending original data, many applications (medical or financial) use them to transfer data. Generative models are shown be useful in many scenarios such as health and financial applications [VSV+22]. However, the highly distributed architecture in 5G advanced/6G motivates the

need for distributed, multi-agent learning for building generative models located at given anchor points of data collection (Edge server or Central Units) inside the RAN/Edge.

Challenges and objectives

We aim to design a communication-efficient and privacy-preserving on demand framework such that the local agents inside RAN/Edge cooperatively generate a synthetic dataset which represents well the global data distribution for model utility. To this end, one can train a generative adversarial network in a federated way [AMR+20], where the agents and the server alternatively minimize the loss function of the discriminator and the generator. However, deep generative models have a tendency to memorize the training examples which may leak private information [HMDC19, CYZF20]. While, applying the traditional privacy-preserving defense such as differential privacy mechanism [Dwo06] will degrade the generative model's utility and thus influences the synthetic data quality. Moreover, the training requires 500-10000 communication rounds in practice for convergence (see [KMA+21, Table 2]) which is expensive for communication cost. Recently, there is another work [ZCL+22] where the server makes uses of all the local trained models to train a generator, which minimizes the communication cost to only one round. However, transferring these local models are extremely dangerous as they can be used to infer the private information on the dataset of devices [FJR15, YGFJ18]. Alternatively, instead of transferring the models as the previous work proposed, the devices can transfer directly the distilled synthetic data which are computed locally [ZPM+20]. However, the quality of the assembled synthetic dataset degrades especially when some agents have just few training samples.

We will first compare the above-mentioned existing methods for synthetic dataset generation, in terms of their trade-offs on model accuracy, data similarity, communication cost, model compression and privacy. Then, to expose their privacy vulnerability, we will design computational-efficient attacks, for both passive and active adversary cases. Finally, we will design a framework with better trade-off for the task.

The project is part of a larger collaborative project with Nokia Bell labs (Défi LearnNet). A PhD grant is funded as part of the global project as well as this internship. This internship can thus be followed by a PhD for a motivated student.

Principales activités

Research

Compétences

The candidate should have a solid mathematical background, good programming skills and previous experience with PyTorch or TensorFlow. He/She should also be knowledgeable on machine learning, especially generative neural networks, and have good analytical skills. We expect the candidate to be fluent in English.

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

Informations générales

- **Thème/Domaine** : Networks and Telecommunications
  System & Networks (BAP E)
- **Ville** : Sophia Antipolis
- **Centre Inria** : Centre Inria d'Université Côte d'Azur
- **Date de prise de fonction souhaitée** : 2024-03-01
- **Durée de contrat** : 6 months
- **Date limite pour postuler** : 2024-06-26

Contacts

- **Équipe Inria** : COATI
- **Recruteur** :
  Xu Chuan / chuan.xu@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.

L'essentiel pour réussir

There you can provide a "broad outline" of the collaborator you are looking for what you consider to be necessary and sufficient, and which may combine :

- tastes and appetencies,
- area of excellence,
- personality or character traits,
- cross-disciplinary knowledge and expertise...

This section enables the more formal list of skills to be completed and 'lightened' (reduced) :

- "Essential qualities in order to fulfil this assignment are feeling at ease in an environment of scientific dynamics and wanting to learn and listen."
- " Passionate about innovation, with expertise in Ruby on Rails development and strong influencing skills. A thesis in the field of **** is a real asset."

> **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.