Memorandum

From: USC-Amazon Center for Secure and Trusted Machine Learning
To: USC Viterbi Faculty
Subject: Call for Proposals
Date: 2 February 2021

Description of Opportunity

USC and Amazon have created a joint research center focused on development of new approaches to machine learning (ML) privacy, security, and trustworthiness. The Center for Secure and Trusted Machine Learning (in short, Trusted AI), which will be housed at the USC Viterbi School of Engineering, will support USC and Amazon researchers in the development of novel approaches to privacy-preserving ML solutions.

Each year, through a competition process, the Center will provide support for several research projects focused on the development of new methodologies for secure and privacy-preserving machine learning solutions. The Center will also provide annual fellowships to doctoral students working in this research area, enabling them to advance research frontiers. Fellowship recipients will be named as Amazon ML Fellows in recognition of their promise and achievements. In addition to funded research projects and annual fellowships for doctoral students, the collaborators will host an annual joint public research symposium to share their knowledge with the machine learning and AI communities.

We hereby invite USC faculty to submit proposals for the first round of funding via the USC-Amazon Center for Secure and Trusted Machine Learning.

Topics of Interest

The topics solicited for this round of Trusted AI proposals include:

- Federated Learning, in particular the challenges of security, privacy, robustness, heterogeneous datasets, personalization, fairness, lack of labels (unsupervised learning), resource constraints, aggregation/bandwidth bottleneck, adversarial attacks, and scalability.
- Application domains and benchmarks for Federated Learning, in particular applications in image processing, natural language processing, computer vision, healthcare, IoT, and data sciences.
- New information theoretic and cryptographic approaches for secure and privacy-preserving learning and inference.
- Fairness, Bias, and Trust in decentralized and privacy-preserving machine learning, in particular the challenges of establishing trust in federated learning domains, in which the users and the servers can behave autonomously and can be malicious.
Timeline

1. Release of CFP: 2 February, 2021
2. A 1-hour webinar (including time for Q&A) will be held on Wednesday February 10th, 2021 at 4-5 pm PT, via zoom: https://usc.zoom.us/j/98065228950
3. Full proposals due: 22 March, 2021
4. Announcement of selected projects: 30 April, 2021
5. New projects start date: 16 May, 2021

Scope, approximate funding level, eligibility, evaluation process, and expectations

- Performance period will be one year, with the possibility of extending for another year.
- The per-project available funding is approximately $75k (with reduced indirect cost rate of 37.5%).
- It is anticipated that about 4 projects will be selected for funding.
- All USC faculty who can serve as a PI on federally-funded research projects are eligible.
- All proposals will be evaluated by an advisory committee composed of USC faculty and researchers from Amazon.
- The PIs of the selected projects are expected to
  a. provide quarterly reports as well as a final report of their research accomplishments in the project;
  b. participate and present at a technical USC-Amazon workshop on Trusted AI (planned for Fall 2021);
  c. participate and present at an annual Research Symposium on Trusted AI (planned for Spring 2022).

Proposal submission instructions

The proposal format is single-spaced, 11-point font or larger, with no less than 0.5-inch page margins. The proposal should include the following content:

1. Project description (3 pages max), including the title, PI(s), an executive summary, technical description of the project, expected deliverables/outcomes, and milestones
2. List any USC background Intellectual Property (unlimited)
3. References (unlimited)
4. Requested budget, assuming **reduced indirect cost rate of 37.5%**.
5. Bio(s) of the PI(s) (upto 2 pages per PI in NSF format)

Full proposals (compiled in a single-file PDF format) should be sent via email to Center Director, Salman Avestimehr (avestime@usc.edu), by 5 pm Pacific time on 3/22/2021.