IET Information Security

Hindawi

Special Issue on
Usable Security and Privacy for Large Model Systems

CALL FOR PAPERS

Security and privacy concerns surrounding large models, such as GPT-4, are central in today's digital landscape. These large language model (LLM) driven system, while powerful and versatile, raise issues related to data privacy, such as the potential for inadvertently generating or revealing sensitive information from the data they were trained on. Additionally, there are concerns about their misuse for malicious purposes, like generating fake content, and potential vulnerabilities that could be exploited by bad actors. Balancing the benefits of these models with the need to address these privacy concerns is a critical challenge in the field of artificial intelligence.

Research in security and privacy on LLM systems faces a complex array of challenges. The first critical issue is data privacy, as LLMs can inadvertently expose sensitive information from the inference and training data. Additionally, the vulnerability of LLMs to adversarial attacks poses a significant concern, demanding the development of robust defenses. Ethical considerations are paramount, as these models can be harnessed for harmful purposes such as misinformation and hate speech. Researchers must also grapple with the persistence of biases within LLM systems and work to enhance fairness. Transparency and explainability are essential for trust and accountability, necessitating research into methods for understanding model decisions. The regulatory landscape is evolving, and finding the right balance between innovation and responsible use requires interdisciplinary collaborations. Ensuring user control, addressing scalability challenges, identifying and mitigating security vulnerabilities, and navigating the intricate web of regulations all form part of the dynamic landscape that this research field seeks to navigate, shaping the responsible deployment of LLM systems.

In this Special Issue, we cordially invite the submission of high-quality original papers and review articles from leading researchers actively contributing to the emerging field of security and privacy in the context of LLM systems.

Potential topics include but are not limited to the following:

- Adversary example attacks and defenses on LLM systems
- Backdoor attacks and defenses on LLM systems
- Data poisoning attacks and their mitigation on the training data of LLMs
- Fairness issues and solutions for LLM-driven applications
- Certified robustness and explainable theory and practice for LLM systems
- Regulation compliance inspection on LLMs' inputs and outputs
- Ownership and intelligence property protection for LLMs
- Trusted hardware execution environment for LLM-driven appellations
- Traceable and accountable LLM system deployment using Blockchain
- Using LLMs to enhance the security and privacy for real-world applications
- Practical and privacy-preserving inference on LLMs
- Privacy-preserving training for LLMs
- Identity anonymity and privacy for LLM system users
- Fine-grained access control for LLM-driven applications
- Privacy-preserving LLMs fine-tuning

Authors can submit their manuscripts through the Manuscript Tracking System at https://review.wiley.com/submit?specialIssue=387822.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Editor
Guowen Xu, City University of Hong Kong, Hong Kong, Hong Kong
guowenxu@cityu.edu.hk

Guest Editors
Hongwei Li, University of Electronic Science and Technology of China, China
hongweili@uestc.edu.cn

Rongxing Lu, University of New Brunswick, Canada
rlu1@unb.ca

Robert H. Deng, Singapore Management University, Singapore
robertdeng@smu.edu.sg

Submission Deadline
Friday, 2 August 2024

Publication Date
December 2024