پژوهشگاه دانش‌های بنیادی
پژوهشکده علوم کامپیوتر

سخنرانی علمی

Dynamic Mask-Based Federated Learning with Homomorphic Encryption

احسان تن‌قطاری
دکتری دانشگاه تهران

Abstract

In federated learning (FL), multiple parties can collaboratively train a machine learning model without directly sharing their private data. Instead of sending raw data, they only share model updates with a central server. However, these model updates can still leak sensitive information about the local data they were trained on. To solve this, researchers often use techniques like homomorphic encryption (HE), which allows the server to compute on encrypted updates. The problem is that encrypting the entire model is very slow and creates significant communication and computational overhead, making it impractical for many real-world scenarios. In this talk, I will discuss our proposed framework, DMFL-HE, which is designed to find a better balance between privacy, accuracy, and efficiency. Rather than taking a brute-force approach to encryption, our method introduces a more strategic way to protect the model updates. This allows us to significantly reduce the overhead associated with full encryption while still providing strong privacy guarantees.
I will show how this approach not only improves efficiency but also leads to faster model convergence and higher accuracy compared to standard methods. We'll also see that it offers enhanced protection against common privacy attacks.

Biography

Ehsan Tanghatari received his bachelor’s degree in Electrical Engineering from Shahid Beheshti University, Tehran, Iran, in 2014. In 2016, he awarded his M.Sc. degree in Digital Electronics Engineering from Sharif University of Technology and he is currently working toward the Ph.D. degree in Electrical Engineering in University of Tehran. His current research interests inlcude edge computing, security and privacy in distributed systems, with a focus on privacy-preserving machine learning, federated learning.

زمان : چهارشنبه ۱۴۰۱/۴/۱۵ – ساعت ۱۵:۰۰

ارائه به صورت مجازی انجام خواهد شد.

https://vmeeting.ipm.ir/b/com-uwd-qpp

***** شرکت برای عموم علاقه مندان آزاد است*****