SEMINAR ANNOUNCEMENT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
COLLEGE OF DESIGN AND ENGINEERING
Website: https://cde.nus.edu.sg/ece

Area: Communications and Networks (CN)

Host: Prof Biplab Sikdar

TOPIC	:	**Machine Unlearning**
SPEAKER	:	**Ms Feng Xijia** **Graduate Student, ECE Dept, NUS**
DATE	:	**Friday, 20 December 2024**
TIME	:	**10:00AM-11:00AM**
VENUE	:	**Join Zoom Meeting** **https://nus-sg.zoom.us/j/8092137897?pwd=eXFwV0s2SW14VFBzYW5GVXJtdUtvQT09** **Meeting ID: 809 213 7897** **Passcode: 405792**

ABSTRACT

The "right to be forgotten" under modern privacy regulations poses significant challenges for machine learning systems, as models trained on sensitive data often retain information about the training data, making it difficult to erase. In this paper, the authors propose SISA training (Sharded, Isolated, Sliced, and Aggregated training), a framework that strategically limits the influence of individual data points during training. SISA training partitions the dataset into disjoint shards, isolates the training of models on these shards, and introduces incremental slicing, enabling efficient unlearning by retraining only the affected shard and slice. This approach reduces computational overhead while maintaining model accuracy. Evaluations on diverse datasets demonstrate SISA training's potential to uphold privacy requirements while balancing computational efficiency and accuracy. This work provides a practical and scalable mechanism for implementing data governance in ML systems.

BIOGRAPHY

Ms. Feng is currently pursuing her Ph.D. under Prof. Biplab Sikdar. Ms. Feng's current research focuses on security and privacy issues in IoT systems.