Frontier of Artificial Network

Department of Data Science
香港城市大學
City University of Hong Kong

The Audio Auditor: User-level Membership Inference in Internet of Things Voice Services

Invited Speaker
Yuantian Miao
University of Newcastle

Date: May 7, 2026 (Thu)
Time: 14:00 (HKT) | 16:00 (AEST)
Zoom Meeting: 801 137 0362

Biography

Yuantian Miao is currently a Lecturer at the computing and information technology, the University of Newcastle, Australia. She received her PhD degree from the Swinburne University of Technology, Australia in 2021. Her current research interests mainly focus on Security and Privacy in Machine Learning/Artificial Intelligence.

Abstract

With the rapid development of deep learning techniques, the popularity of voice services implemented on various Internet of Things (IoT) devices is ever increasing. In this paper, we examine user-level membership inference in the problem space of voice services, by designing an audio auditor to verify whether a specific user had unwillingly contributed audio used to train an automatic speech recognition (ASR) model under strict black-box access. With user representation of the input audio data and their corresponding translated text, our trained auditor is effective in user-level audit. We also observe that the auditor trained on specific data can be generalized well regardless of the ASR model architecture. We validate the auditor on ASR models trained with LSTM, RNNs, and GRU algorithms on two state-of-the-art pipelines, the hybrid ASR system and the end-to-end ASR system. Finally, we conduct a real-world trial of our auditor on iPhone Siri, achieving an overall accuracy exceeding 80\%. We hope the methodology developed in this paper and findings can inform privacy advocates to overhaul IoT privacy.