Title

Addressing Data Leakage in Split Learning: Attacks and Defence Strategies

Speaker

Professor Naveen Chilamkurti Fellow IET(UK)
La Trobe University, Melbourne

Abstract

Split Learning (SL) has emerged as an innovative framework designed to enable deep learning applications on resource-constrained devices such as IoT or mobiles. Its core concept involves dividing a deep model into multiple parts and distributing them between data owners and a central cloud computing server. During the training process, only processed data is transmitted from the client to the server, safeguarding user data privacy. However, SL encounters several challenges, including (i) the high computational burden on low-end devices, (ii) potential privacy risks arising from the exposed intermediate data, and (iii) susceptibility to model inversion attacks capable of reconstructing raw input data.

In this presentation, we will first delve into recent research addressing privacy attacks and defence mechanisms within the context of SL that could potentially lead to the leakage of users' private data. Subsequently, we will introduce our ongoing work aimed at enhancing the learning performance and privacy preservation of SL. This includes (i) the exploration of binarization in SL's local layers to expedite computation and reduce memory usage on the client side; (ii) an investigation into SL without local weight sharing to strengthen client-side data privacy, especially in environments with semi-trusted participants; and (iii) an examination of the integration of Differential Privacy into SL to further fortify user data privacy. We will identify potential accuracy degradation when training multiple clients with varying privacy requirements and present an approach to mitigate this challenge.

By the end of this presentation, you will gain insights into the latest trends in the development of attacks and defences aimed at enhancing the privacy preservation of SL, which plays a crucial role in extending AI to pervasive devices while addressing data privacy concerns.

Biography

Professor Naveen Chilamkurti is the Head of the Cybersecurity discipline and Associate Dean (International Partnerships) at La Trobe University, Melbourne, Australia. Naveen played a critical role in designing and developing the Master's and Bachelor of Cybersecurity courses at La Trobe. He was a team member in securing a 2.3 million Cybersecurity upskill grant from the Australian government in 2021. He also received the Australia-India Cybersecurity Infrastructure Grant, jointly funded by DFAT and the Indian government. He is a keynote speaker at various international conferences and has been recently elected as an IET (UK) fellow. He has an extensive research record in cybersecurity and published 350 journals/conference articles in Cybersecurity, IoT, Anomaly detection in IoT, the Internet of

Medical Things, Wireless Security, Federated Learning in IoT, wireless multimedia, wireless sensor networks, and Software Defined Networks. He is active in editing and authoring 9 books with Elsevier, Springer, IGI-Global and NOVA publishers. He has successfully attracted 20 research grants since 2000 to support PhD Scholarships, fellowships, and travel grants for research collaboration. Prof. Chilamkurti secured 24 competitive grants from various sources, including SMART SAT CRC, Data61/CSIRO, Defence Science Institute, Australian Academy of Science, and OPTUS telecommunications. He was instrumental in designing and developing cybersecurity micro-credentials and other short courses now delivered online. He has taught networking, security, and cyber areas for 26 years and has supervised 51 research students to complete their master's and PhD programs. He is also the director of La Trobe Cybersecurity Innovation Node, which is primarily focused on research, upskilling, and certification in cybersecurity programs.