Safeguarding Privacy and Security in Mobile Systems with Personalised Decentralised Machine Learning

Qilei Li, Ahmed M. Abdelmoniem

School of Electronic Engineering and Computer Science,
Queen Mary University of London

May 11, 2024

Abstract

Ensuring the privacy and security of user data is critical for mobile technology. Personalised machine learning offer promising avenues for enhancing user experience, yet they also raise concerns regarding data privacy and security. This work explores the intersection of personalised machine learning and mobile systems, with a focus on leveraging decentralised learning approaches to mitigate privacy and security risks. Decentralised learning paradigms distribute the training process across multiple devices or nodes, thereby minimising the need for centralised data repositories. By enabling devices to learn from local data while sharing only aggregated insights, decentralised learning preserves user privacy by design. Furthermore, this approach reduces the vulnerability of centralised data repositories to security breaches. This work investigates various decentralised learning techniques, such as federated learning and differential privacy, and evaluates their efficacy in the context of mobile systems. Federated learning facilitates model training across distributed devices while preserving data privacy, making it particularly suitable for mobile environments where data residency and privacy are critical concerns. Differential privacy techniques add an additional layer of protection by introducing noise to aggregated insights, preventing the inference of sensitive information from individual contributions. Additionally, this work discusses the implementation challenges and considerations associated with deploying decentralised learning in mobile systems. It examines factors such as communication overhead, device heterogeneity, and model aggregation strategies, offering insights into optimising performance and scalability while upholding privacy and security standards. Through a comprehensive analysis of decentralised learning methodologies and their application in mobile systems, this work provides valuable insights for researchers, developers, and policymakers seeking to harness the potential of personalised machine learning while safeguarding user privacy and security in the mobile ecosystem.

Author keywords: Privacy and Security, Mobile Systems, Personalised Machine Learning, Decentralised Machine Learning, Differential Privacy Techniques