




Federated learning for 6G-enabled secure communication systems: a comprehensive survey

Deepika Sirohi¹ · Neeraj Kumar^{1,2,3,7}  · Prashant Singh Rana¹ · Sudeep Tanwar⁴ · Rahat Iqbal⁵ · Mohammad Hijjii⁶

Accepted: 31 January 2023 / Published online: 12 March 2023
© The Author(s), under exclusive licence to Springer Nature B.V. 2023

Abstract

Machine learning (ML) and Deep learning (DL) models are popular in many areas, from business, medicine, industries, healthcare, transportation, smart cities, and many more. However, the conventional centralized training techniques may not apply to upcoming distributed applications, which require high accuracy and quick response time. It is mainly due to limited storage and performance bottleneck problems on the centralized servers during the execution of various ML and DL-based models. However, federated learning (FL) is a developing approach to training ML models in a collaborative and distributed manner. It allows the full potential exploitation of these models with unlimited data and distributed computing power. In FL, edge computing devices collaborate to train a global model on their private data and computational power without sharing their private data on the network, thereby offering privacy preservation by default. But the distributed nature of FL faces various challenges related to data heterogeneity, client mobility, scalability, and seamless data aggregation. Moreover, the communication channels, clients, and central servers are also vulnerable to attacks which may give various security threats. Thus, a structured vulnerability and risk assessment are needed to deploy FL successfully in real-life scenarios. Furthermore, the scope of FL is expanding in terms of its application areas, with each area facing different threats. In this paper, we analyze various vulnerabilities present in the FL environment and design a literature survey of possible threats from the perspective of different application areas. Also, we review the most recent defensive algorithms and strategies used to guard against security and privacy threats in those areas. For a systematic coverage of the topic, we considered various applications under four main categories: space, air, ground, and underwater communications. We also compared the proposed methodologies regarding the underlying approach, base model, datasets, evaluation matrices, and achievements. Lastly, various approaches' future directions and existing drawbacks are discussed in detail.

Keywords Blockchains · Distributed computing · Encryption · Federated learning · Machine learning · Privacy · Security

✉ Neeraj Kumar
neeraj.kumar@thapar.edu

Extended author information available on the last page of the article