World Academy of Science, Engineering and Technology
International Journal of Cognitive and Language Sciences
Vol:17, No:02, 2023

FLEX: A Backdoor Detection and Elimination Method in Federated Scenario

Authors : Shuqi Zhang

Abstract : Federated learning allows users to participate in collaborative model training without sending data to third-party servers, reducing the risk of user data privacy leakage, and is widely used in smart finance and smart healthcare. However, the distributed architecture design of federation learning itself and the existence of secure aggregation protocols make it inherently vulnerable to backdoor attacks. To solve this problem, the federated learning backdoor defense framework FLEX based on group aggregation, cluster analysis, and neuron pruning is proposed, and inter-compatibility with secure aggregation protocols is achieved. The good performance of FLEX is verified by building a horizontal federated learning framework on the CIFAR-10 dataset for experiments, which achieves 98% success rate of backdoor detection and reduces the success rate of backdoor tasks to 0% ~ 10%.

Keywords : federated learning, secure aggregation, backdoor attack, cluster analysis, neuron pruning
Conference Title : ICSLP 2023 : International Conference on Speech and Language Processing
Conference Location : Manila, Philippines
Conference Dates : February 20-21, 2023

Open Science Index, Cognitive and Language Sciences Vol:17, No:02, 2023 publications.waset.org/abstracts/158139.pdf