World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:16, No:01, 2022

Data Poisoning Attacks on Federated Learning and Preventive Measures

Authors : Beulah Rani Inbanathan

Abstract : In the present era, it is vivid from the numerous outcomes that data privacy is being compromised in various ways. Machine learning is one technology that uses the centralized server, and then data is given as input which is being analyzed by the algorithms present on this mentioned server, and hence outputs are predicted. However, each time the data must be sent by the user as the algorithm will analyze the input data in order to predict the output, which is prone to threats. The solution to overcome this issue is federated learning, where the models alone get updated while the data resides on the local machine and does not get exchanged with the other local models. Nevertheless, even on these local models, there are chances of data poisoning, and it is crystal clear from various experiments done by many people. This paper delves into many ways where data poisoning occurs and the many methods through which it is prevalent that data poisoning still exists. It includes the poisoning attacks on IoT devices, Edge devices, Autoregressive model, and also, on Industrial IoT systems and also, few points on how these could be evadible in order to protect our data which is personal, or sensitive, or harmful when exposed.

Keywords : data poisoning, federated learning, Internet of Things, edge computing
Conference Title : ICCAA 2022 : International Conference on Cybernetic Algorithms and Applications
Conference Location : Paris, France
Conference Dates : January 21-22, 2022