PDF Report

Name:Habiba Mahrin
ID:20301339
Paper:Data Poison Detection Schemes for Distributed Machine Learning
https://ieeexplore.ieee.org/abstract/document/8943404

1 Summary

This paper discusses data poison detection schemes for Distributed Machine Learning (DML) and classifies DML into basic-DML and semi-DML. In basic-DML, a novel data poison detection scheme is proposed using a cross-learning mechanism to identify poisoned data, with the optimal number of training loops determined mathematically. In semi-DML, an improved data poison detection scheme is presented to enhance learning protection with central resource support, including an optimal resource allocation approach for efficient resource utilization. Simulation results indicate significant accuracy improvements in basic-DML (up to 20% for support vector machine and 60% for logistic regression) and resource savings in semi-DML (20-100% reduction in wasted resources).

1.1 Motivation

Introduction of a data poison detection scheme for basic-DML, utilizing a cross-learning mechanism to generate training loops and establish a mathematical model for optimal security.
Presentation of a practical method for identifying abnormal training results, aiding in the detection of poisoned datasets

1.2 Contribution

This research contributes to the field of distributed machine learning by developing novel data poisoning detection schemes. These algorithms are designed to identify and mitigate malicious data injection attempts in decentralized environments, ensuring the integrity and security of machine learning models

1.3 Methodology

DATA POISON DETECTION SCHEME IN BASIC-DML
DATA POISON DETECTION SCHEME IN semi-DML

2 Limitations

1.Data Distribution Variability: One limitation is the challenge of handling diverse and evolving data distributions across distributed sources. Detection schemes may struggle to adapt to dynamic changes, leading to potential false positives or false negatives, reducing their effectiveness in real-world scenarios.

2.Privacy Concerns: Privacy-preserving techniques to detect data poisoning may introduce their own limitations, such as added computational overhead and complexity. Striking a balance between effective detection and preserving individual data source privacy remains a significant challenge.

3.Conclusion and future work

This paper examines data poison detection in both basic-DML and semi-DML scenarios. It employs parameter thresholds to detect poisoned sub-datasets and presents a mathematical model for threat probability analysis. The improved detection scheme boosts model accuracy by up to 20% (SVM) and 60% (logistic regression) in basic-DML. In semi-DML, the enhanced scheme with optimal resource allocation reduces resource wastage by 20-100%. Future work should consider dynamic patterns for evolving application environments and balance between security and resource cost.