RESEARCH OF PROBLEMATIC ISSUES IN FEDERATED LEARNING OF NEURAL NETWORKS

Zuikov A.V., Ruzhentsev V.I.
Kharkiv National University of Radio Electronics, Ukraine

With the rapid growth of cloud computing, as it becomes increasingly ubiquitous, security threats and vulnerabilities in cloud services have become a major concern for organizations and individuals alike. Previously, security solutions often relied on rule-based systems or manual analysis, which was time-consuming and ineffective in detecting new and complex security threats. Machine learning (ML) techniques, including neural networks (NN), have shown promise in improving the accuracy and efficiency of security analysis in cloud environments [1]. Combining different data sources to train NNs can improve the accuracy of predictions, as full range of datasets provides a more comprehensive list of threat signatures. According to market research, Distributed learning (DL) and Federated learning (FL) are used to train models for Internet of Things (IoT), healthcare industry, banking services [2]. However, all these cloud-edge collaborative architectures have central cloud servers to keep global aggregation and to provide NN model for all participants of the learning process. Also, there are FL related challenges, such as statistical heterogeneity, system heterogeneity, model heterogeneity and secure management [2].

The purpose of this work is to investigate the mechanisms of FL for NNs that analyzes security threats and vulnerabilities in cloud services. The problem is that cloud providers use complex proprietary models that have different architecture and high heterogeneity. Also privacy and security of the learning process must be taken into an account. This work analyzes the impact of model size and heterogeneity on quantitative measures of the FL process. A described system, consisting of a neural network and a blockchain network, was built. In the course of the research the work is being carried out to collect metrics for learning speed and network traffic, corresponding to different variants of FL. These metrics will be further used to get optimization for the system architecture. The full version of the report will present the models, the dependencies obtained, and recommendations for system optimization.

Conclusions. The process of large model training can be optimized. With incremental learning, when new threats appear, the percentage of new data is insignificant compared to the total database size. FL of a large model while changing a small portion of the training data results in an increased network traffic and in a longer model training time. Partitioning a large model into an aggregation of specialized feature-models can improve the considered metrics.

References

1. Naveed Ahmed and others. Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction, 2022, Sensors.

2. Guanming Bao, Ping Guo. Federated learning in cloud-edge collaborative architecture: key technologies, applications and challenges. Journal of Cloud Computing. URL – https://doi.org/10.1186/s13677-022-00377-4.