ABSTRACT

This research is focused on comparing the performance of Deep Neural Network (DNN) in Centralized Learning (CL) and Federated Learning (FL) concepts on simulating coordinated attack detection, such as Benign (normal activity), PortScan, DDoS, and Bot using the cicids2017 dataset for model training. The data preprocessing used is the Adaptive Synthetic Sampling (ADASYN) method for unbalanced data balancing. This research aims to advance the concept of network attack detection in an effort to keep each device's data safe, without the need to send datasets to a central device to update the attack classification model, i.e. the data is trained in a decentralized way using the FL concept. In the simulation of coordinated attack detection, the result of FL is higher than that of CL. To achieve good attack classification results, the FL concept only required 20.45 seconds per epoch, which is shorter than the time required by the CL concept to train the attack classification model. Some of the advantages of the FL concept allow for smarter modeling, low latency, and less power consumption, while Aulia Arif Wardana Doctoral School Wrocław University of Science and Technology Wroclaw, Poland aulia.wardana@pwr.edu.pl This research proposes deep learning to detect coordinated attacks using the concept of federated learning (FL), FL is a distributed machine learning concept where data can be trained in a decentralized manner without having to send data to the center, this concept allows building smarter models, lower latency, and less power consumption while ensuring data privacy[2][7]. Before FL concept, machine learning or deep learning training is performed in a centralized or traditional way. So this research focuses on simulating the deep neural network model as a learning model and learning federation as one of the solution ideas in the coordinated attack detection problem to maintain data privacy on each device. The concepts of federated learning, coordinated attacks and CIDS are similar, which are distributed in each network node and client. ensuring the privacy of each device's data.

Keywords—Cicids2017, Coordinated Attacks, Deep Neural Network, Dataset Balancing Method, Federated Learning, Centralized Learning.