Abstract

The rising complexity of cyber threats in Industry 5.0-driven healthcare environments necessitates robust, privacy-preserving intrusion detection mechanisms. In this paper, we propose a Federated Learning-Based Ensemble Convolutional Neural Network (FLE-CNN) for Network Intrusion Detection in smart healthcare systems. Unlike traditional centralized models, our approach leverages federated learning to preserve data privacy by enabling collaborative model training across multiple decentralized healthcare systems without exposing sensitive patient data. The FLE-CNN integrates multiple models like CNN, SVM, DT and KNN into an ensemble, enhancing the detection accuracy of diverse intrusion types while mitigating overfitting. We utilize the NSL-KDD dataset to assess the model's performance. Experimental results demonstrate that the proposed FLE-CNN framework outperforms existing intrusion detection schemes in terms of accuracy, recall, precision, and F1-score, while also addressing key security concerns related to data sharing and system scalability. This work presents a significant advancement toward secure, intelligent, and privacy-preserving intrusion detection in next-generation healthcare infrastructures.