Graduate School of Science and Technology Master’s Thesis Abstract

Laboratory name (Supervisor)	Cyber Resilience (Youki Kadobayashi （Professor))		
Student ID	2211420	Submission date	2024 / 7 / 20
Name	TONGIAM PACHARAWAN		
Thesis title	Enhancing Android Malware Detection: Integrated Neural Networks with Federated Learning and Explainable AI Analysis		

Abstract

The proliferation of Android malware presents significant challenges, necessitating robust, scalable, and privacy-preserving detection mechanisms. Traditional machine learning methods struggle with the dynamic and sophisticated nature of such threats, particularly when dealing with heterogeneous data sources across distributed environments. This research explores the integration of Neural Networks model on Federated Learning (FL) and Explainable Artificial Intelligence (XAI) to address these challenges. Our methodology leverages a federated learning framework employing an integration of neural network models—Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM)—trained across three distinct datasets: Drebin, Kronodroid, and CCCS-CIC-AndMal-2020. We investigate the framework’s effectiveness, scalability, and robustness in handling heterogeneous data while ensuring privacy through decentralized data processing. Additionally, we employ XAI techniques to enhance the interpretability of our models, providing insights into feature importance and the decision-making processes of the models. Our results indicate that the proposed approach achieves high accuracy in detection and maintains consistent performance across varied client configurations, illustrating the potential of FL and XAI in enhancing cybersecurity measures.