報告番号	※甲　　第　　号

主　論　文　の　要　旨

論文題目　Effective Application of Artificial Intelligence Technology in Malware Detection and Classification

(マルウェアの検知と分類に対する人工知能技術の効果的な適用)

氏　　名　　高　云

論 文 内 容 の 要 旨

Modern society relies more and more on computer system and network technology, and the threat of malicious software is becoming more and more serious. In the field of information security, malware detection has been a key problem that academia and industry are committed to solving.

With the large-scale development of Artificial Intelligence(AI) technology, more and more information security personnel try to learn the feature of malware and normal software by machine learning, so that malware detection can get rid of threat intelligence and expert knowledge, and can calmly deal with large-scale malware attacks. This thesis proposes using different AI methods to detect and classify malicious software.

Traditional Machine Learning We investigated the malware detection results based on LightGBM in static malware detection methods, and reduced the false alarms by a custom log loss function, which controls the learning process of model through installing coefficient α to a loss function of the false-negative side and coefficient β to the false-positive side.

Graph Representation Learning We propose a Control-Flow Graph (CFG)- and Graph Isomorphism Network (GIN)-based malware classification system. The feature vectors of CFG basic blocks are generated using the large-scale pre-trained language model MiniLM, which is beneficial for the GIN to further learn and compress the CFG-based representation, and classified with multi-layer perceptron.

Graph Contrastive Learning We propose a malware classification framework based on Graph Contrastive Learning (GraphCL) with data augmentation.

According to my experimental evaluation, the unsupervised learning approach outperformed the self-supervised learning approach in Graph Neural Networks based on malware classification.

This thesis has found that generally AI-based methods can effectively improve the detection and classification results of large-scale malware, and with the continuous improvement of AI technology, more and more AI technologies can be applied to the field of information security to help solve difficult security problems.