Abstract

In recent years, malware has issued a very serious threat and continues to make malware detection a major concern. Prevention and prevention of malware can be done through detection of signatures and protection of these malware. Malicious software that can be used for the signature matching process using dynamic software, making it difficult for the system to defend itself against malware. By being able to restore malware, there is some information obtained, one of which is the API call feature. Several related studies have been conducted to deal with malware attacks, and have good accuracy. However, the evaluation is broader than the evaluation of superficial architecture. The deep learning method used, Autoencoder is a method that is very rarely used. Autoencoder is an architecture in deep learning that is used to reduce data. Therefore, in this final project, Convolutional Neural Network Autoencoder (CNN-AE) is used as a malware detection learning method. The detection accuracy that was achieved by the CNN-AE model was 97.14%.

Keywords: deep learning, malware, API call, autoencoder, convolutional neural network