ABSTRACT

The development of digital technology brings both positive impacts and threats in the form of cybercrime, one of which is malware. Malware spreads through emails, websites, and USB devices with various types such as trojans and ransomware. Commonly used cloud-based analysis methods are considered to have limitations such as internet dependence, risk of spread, and high costs. This research addresses the high risk and cost of using cloud-based malware analysis systems, especially in airgap environments that require full isolation.

As a solution, a machine learning-based malware analysis system is developed with the Bidirectional Long Short-Term Memory (Bi-LSTM) algorithm that runs locally on a mini-PC device. The system is designed without an internet connection and features a user interface using PyQt5 and automated reports through ReportLab. The approach used is based on dynamic analysis to observe malware behavior directly.

The test results show that the system is able to classify malware with an accuracy of 91% and classify malware families with 80%. The system also proved to be safe and stable in an isolated environment and provided faster analysis time than conventional methods. In conclusion, this system is an effective and efficient solution for malware analysis needs in restricted environments such as airgap.

Keywords*: malware, machine learning, airgap, sandbox, mini-PC*