ABSTRACT

Threats from cyber attacks such as malware, phishing, and DDoS are serious problems. These attacks are growing rapidly and continuing to evolve, creating new variants that are more complex and difficult for security systems to detect. This requires greater attention to maintaining and securing systems in order to protect data that is considered vital.

Cyber attack prevention systems have been implemented

from time to time, such as Intrusion Prevention Systems (IPS), but these systems tend to have vulnerabilities, such as a lack of prevention from the system to check network logs. By using Machine Learning, new attack patterns can be learned, thereby making the use of IPS more robust. Real-time security aspects are necessary for monitoring, and Security Information and Event Management (SIEM) is a security system that can be used for network monitoring. The purpose of using this system is to alert device owners to take action against attacks that occur.

The testing was conducted by measuring detection performance using parameters such as Accuracy, Precision, Recall, and F1-Score. Neural Network and XGBoost recorded an accuracy of 77%, K-Means 44%, and Naïve Bayes 33%, with good generalisation capabilities against minority attacks. A comparison between rule-based and machine learning systems shows that ML is capable of detecting attacks that are not detected by rules. In IP Sweep attacks, the rule system did not produce any detections, while the Neural Network successfully detected 6 flows. For Full Port Scan, Naïve Bayes detected 436 out of 3,372 flows. In DoS attacks, the Neural Network detected 90,947 out of 90,982 flows and Naïve Bayes detected 81,770 out of 93,759 flows in SYN Flood; and 45,053 out of 68,530 flows and 47,556 out of 62,157 flows in UDP Flood. In the FTP Brute Force (R2L) attack, only rules-based detection successfully detected 400 flows, while ML failed. For the U2R Exploit, Naïve Bayes detected 10 out of 14 flows, compared to only 1 flow by rules.

keywords: *Cyber Security*, *Intrusion Detection System, Intrusion Prevention System, Security Information and Event Management, Machine Learning*