Cyber Attack Detection and Mitigation on Multi-Websites Using Machine Learning dan Multi-Layer Security

Hartono

Abstract

During 2019 to 2021, there is significant increase in cyber attack data, both on an Indonesia and international scale. The number of cyber attacks has increased in the past three years. In fact, in 2020, the National Cyber and Crypto Agency of the Republic of Indonesia detected 495 million of cyber attacks. This trend is not only happening in Indonesia, but also in almost every country. Cases of data breach, account takeovers, and more, are increased in the middle of excessive consumption of information technology. The increase number of cyber attacks must be the concern of various relevant parties, both by technology practitioners, cyber security, academics and non-academics society. Based on those problems, this study aims to implement and test methods of detecting and mitigating cyber attacks on multi-websites using machine learning and multi-layer security. In this case, there are two methods used in this study, they are detection and mitigation methods. These two methods are used to detect and mitigate three types of cyber attack techniques: Cross Site Scripting, SQL Injection, and Remote Code Execution. In relation to the detection method, the indicator to be achieved is the level of accuracy. Meanwhile, in the mitigation method, the indicator to be achieved is the level of effectiveness. Based on the research that has been done, Support Vector Machine becomes the algorithm that gets the highest level of detection accuracy compared to Naïve Bayes, Logistic Regression, Gradient Boosting, and K-Nearest Neigbor. The accuracy level of Support Vector Maching in detecting Cross Site Scripting attacks reaches 0.996546, SQL Injection reaches 0.997713, and Remote Code Execution reaches 0.987495. In relation to the mitigation method, the effectiveness of the multi-layer security method reaches 100%, because it is able to mitigate 269 Arachni attacks and 63 ZAP attacks.

Keywords**:** *cyber attacks, detection methods, mitigation methods, support vector machine, cross site scripting, SQL injection, remote code execution*