Pengembangan Model Pemolisian Berbasis Machine Learning untuk Pendeteksian Serangan Siber pada Jaringan Wi-Fi dan Internet of Things = The Development of Machine Learning-Based Policing Models for Detecting Cyber Attacks on Wi-Fi Networks and Internet of Things

Achmad Eriza Aminanto, author

Abstrak

Pandemi COVID-19 sejak tahun 2020 menyebabkan transofrmasi digital secara masif yang terjadi, Tantangan keamanan yang perlu diatasi berasal dari sifat keterbukaan media nirkabel yang menjadi media komunikasi utama di IoT. Hal tersebut menyebabkan besarnya kerugian yang disebabkan kejahatan siber. Kepolisian Republik Indonesia lewat Direktorat Tindak Pidana Siber diharapkan memiliki peran pencegahan dalam melakukan giat pengawasan terhadap serangan-serangan ini, dimana Dittipidsiber belum memiliki fungsi pencegahan serangan siber. Sistem Pendeteksi Intrusi (Intrusion Detection System) atau lebih dikenal sebagai IDS, merupakan salah satu sistem yang dapat memantau serang siber ini, di mana memanfaatkan kecerdasan buatan untuk dapat memisahkan antara serangan siber dan bukan serangan. Pada penelitian ini, akan dihasilkan model pemolisian berbasis machine learning untuk pendeteksian serangan siber pada jaringan Wi-fi dan IoT. Model tersebut melakukan perekaman data jaringan, kemudian data tersebut dilakukan analisa IDS sehingga dapat ditampilkan di command room, yang kemudian ketika adanya indikasi serangan dapat dilakukan penindakan dengan cepat. Dilakukan simulasi dan analisis terhadap berbagai metode seleksi fitur dan model klasifikasi untuk menghasilkan IDS yang baik. Penelitian ini menggunakan dataset publik berisi serangan siber terhadap jaringan Wi-Fi. Dari hasil eksperimen, didapatkan bahwa metode terbaik untuk pengurangan fitur adalah mutual information dengan fitur berjumlah 20, dan metode untuk klasifikasi serangan adalah Neural Network, menghasilkan F-Score sebesar 94% dengan waktu yang dibuthkan 95 detik. Hasil ini menunjukkan IDS yang diusulkan memiliki kemampuan untuk mendeteksi serangan dengan cepat dan hasil deteksi yang sama bagus dengan penelitian sebelumnya.

.....Since 2020, the Covid-19 pandemic has caused massive digital transformation. Security challenges needed to be overcome is based on the nature of wireless media which is the main communication medium in IoT (Internet of Things). Such condition generates huge loss caused by cybercrime attacks. Indonesian National Police through Directorate of Cyber Crime (Dittipidsiber) is expected to have preventive roles in supervising these attacks, where Dittipidsiber has not had a cyber-attack prevention function. The Intrusion Detection System (IDS) is a system that can identify these cyber-attacks, utilizing artificial intelligence to be able to separate between cyber-attacks and non-attacks. In this study, a machine learning-based policing model will be generated for detecting cyber-attacks on Wi-Fi and IoT networks. The model records network data that will be analysed by IDS so that it can be displayed in the command room. After that, any indications of attacks can be identified quickly. The author performs the simulations and analyses various feature selection methods and classification models in order to produce a good IDS. The study employs a public dataset containing cyber-attacks against Wi-Fi networks. Based the experimental results, it is found that the best method for reducing features is mutual information using twenty features and the method for classifying attacks is Neural Network, resulting F-Score of 94% with a time required of 95 seconds. These

results indicate that the proposed IDS have the ability to detect attacks quickly and the detection results are the same as previous studies.