ABSTRAK

Deteksi intrusi merupakan salah satu bagian yang mendasar dari sebuah alat keamanan, seperti peralatan keamanan adaptif, sistem deteksi intrusi, sistem pencegahan intrusi serta firewall. Ada berbagai macam teknik deteksi intrusi yang digunakan, masalah utama dari teknik intrusi ini dihadapkan dengan masalah kinerja. Keakurasian teknik pendeteksian intrusi sangat mempengaruhi kinerjanya, yang perlu ditingkatkan untuk mengurangi tingkat alarm palsu dan meningkatkan tingkat deteksi. Dalam mengatasi masalah pada kinerja, multilayer perceptron, support vector machine (SVM), dan teknik lainnya telah digunakan baru-baru ini. Teknik ini menunjukkan adanya keterbatasan dan tidak efisien untuk digunakan dalam kumpulan data yang besar, seperti sistem dan data jaringan. Sistem deteksi intrusi digunakan dalam menganalisis sebuah lalu lintas data yang sangat besar; dengan demikian, efisien teknik klasifikasi diperlukan untuk mengatasi masalah tersebut. Masalah ini dipertimbangkan dalam makalah ini. Teknik pembelajaran mesin yang terkenal, yaitu, SVM, hutan acak, dan mesin pembelajaran ekstrim akan diterapkan. Teknik-teknik ini terkenal karena kemampuannya dalam pengklasifikasian. Penemuan pengetahuan NSL dan dataset penambangan data digunakan, yang dianggap sebagai tolok ukur dalam evaluasi deteksi intrusi mekanisme. Hasilnya menunjukkan bahwa ELM mengungguli pendekatan lainnya. Pemanfaatan Firebase Cloud Messenging dikarenakan dapat bekerja dengan multi-platform di samping tersedianya filestore yang dapat menyimpan semua log yang di buat oleh aplikasi JALA.

Kata Kunci: Serangan, Deteksi Intrusi, Firebase, Jaringan, Kemanan

ABSTRACT

Intrusion detection is one of the fundamental parts of a security tool, such as adaptive security tools, intrusion detection systems, intrusion prevention systems and firewalls. There are various kinds of intrusion detection techniques used, the main problem of this intrusion technique is the performance problem. The accuracy of the intrusion detection technique greatly affects its performance, which needs to be improved to reduce the false alarm rate and increase the detection rate. In solving performance problems, multilayer perceptron, support vector machine (SVM), and other techniques have been used recently. This technique shows limitations and is inefficient for use in large data sets, such as system and network data. Intrusion detection systems are used in analyzing a very large data traffic; thus, an efficient classification technique is needed to overcome these problems. This issue is considered in this paper. The well-known machine learning techniques, namely, SVM, random forest, and extreme machine learning will be applied. These techniques are well known for their ability to classify. NSL knowledge discovery and data mining datasets were used, which were considered as benchmarks in the evaluation of intrusion detection mechanisms. The results show that ELM outperforms other approaches. Utilization of Firebase Cloud Messaging because it can work with multiple platforms in addition to the availability of a file store that can store all logs created by the JALA application.

Keywords: *Attack, Intrusion Detection, Firebase, Network, Security*