

INTISARI

PERBANDINGAN PERFORMA: LINEAR REGRESSION DAN LOGISTIC REGRESSION SEBAGAI DETEKTOR INTRUSI JARINGAN

Hanun Fadhil Ilyasa Sugiharto
18/423107/PA/18190

Seiring kemajuan teknologi, jenis-jenis ancaman dan serangan baru pun akan muncul juga. Keamanan dan privasi selalu menjadi perhatian utama dalam teknologi. Dalam perangkat yang saling terhubung seperti IoT, di mana perangkat terhubung satu sama lain dalam jaringan yang besar dan kompleks, sangat penting untuk menerapkan keamanan jaringan yang baik. *Network Intrusion Detection System* (NIDS) adalah salah satu metode untuk memperkuat keamanan jaringan dengan mengklasifikasikan apakah lalu lintas jaringan dianggap normal atau berbahaya. Namun, penerapan NIDS konvensional terbukti tidak mampu mengimbangi serangan yang terus berkembang. Untuk mencegah hal ini, NIDS perlu menjadi lebih adaptif terhadap jangkauan serangan yang lebih luas. Salah satu metode yang dapat dilakukan adalah dengan membiarkan sistem mempelajari pola serangan yang dapat dilakukan dengan mengimplementasikannya dengan pembelajaran mesin.

Dalam penelitian ini, perbandingan antara dua metode regresi pembelajaran mesin, yaitu regresi linear dan regresi logistik dilakukan untuk menentukan model mana yang berkinerja lebih baik ketika diterapkan sebagai detektor intrusi jaringan. Model dirancang untuk mengklasifikasikan apakah lalu lintas jaringan tertentu diklasifikasikan sebagai lalu lintas normal atau anomali dari perilakunya.

Empat metrik yaitu skor akurasi, tingkat presisi rata-rata, tingkat ingatan rata-rata, dan skor F1 digunakan untuk mengukur dan membandingkan kinerja kedua model. Hasil keseluruhan menunjukkan bahwa regresi logistik memberikan keamanan yang lebih tinggi daripada regresi linier, namun regresi linier memberikan aksesibilitas yang lebih tinggi.

Kata kunci: deteksi intrusi jaringan, lalu lintas jaringan, pembelajaran mesin, regresi linear, regresi logistik

ABSTRACT

PERFORMANCE COMPARISON: LINEAR REGRESSION & LOGISTIC REGRESSION AS NETWORK INTRUSION DETECTOR

Hanun Fadhil Ilyasa Sugiharto
18/423107/PA/18190

As the advancement of technology goes on, more advanced and a variety of attacks will also follow. Security and privacy are always a top concern in technology. In interconnected devices such as in IoT, where devices are connected with one another in a large and complex network, it is crucial to implement a good network security. A network intrusion detection system (NIDS) is one of the methods to strengthen network security by classifying if a network traffic is considered normal or malicious. However, implementation of traditional NIDS are proven to not be able to keep up with more sophisticated attacks. To prevent this, NIDS needs to become more adaptive to a wider range of attacks. One of the methods that can be done is by allowing the system to learn the pattern of the attacks, which can be done by implementing it with machine learning.

In this paper, a comparison between the two machine learning regression methods, which are linear regression and logistic regression is conducted to determine which model performs better when applied as a network intrusion detector. The model is designed to classify whether a certain network traffic is classified as a normal or anomalous traffic from the behaviour inspected.

Four metrics which are accuracy score, average precision rate, average recall rate, and F1 score are used to measure and compare the two models' performance. The overall result shows that the logistic regression provides higher security than the linear regression, however linear regression is able to provide higher accessibility.

Keywords: network intrusion detection, network traffic, machine learning, linear Regression, logistic Regression