

ABSTRAK

Keamanan *otentikasi* pengguna merupakan komponen penting dalam pengelolaan jaringan, terutama pada perangkat MikroTik yang umum digunakan di berbagai institusi. Salah satu ancaman serius yang sering muncul adalah serangan *brute force*, yaitu usaha *login* berulang dengan berbagai kombinasi *username* dan *password* hingga mendapatkan akses. Namun sebagian besar mekanisme perlindungan yang tersedia saat ini masih bersifat pasif dan belum mampu mengenali pola serangan sejak dini. Penelitian ini menawarkan pendekatan berbasis *machine learning* dengan memanfaatkan algoritma *Random Forest* untuk mendeteksi serangan *brute force* secara *real-time*. Keunggulan dari metode ini terletak pada kemampuannya membaca pola dari data *log autentikasi* berdasarkan fitur-fitur seperti alamat IP, *username*, protokol *login*, frekuensi login gagal, dan daftar *username* umum yang sering digunakan dalam serangan. Data *log* diolah melalui beberapa tahapan, mulai dari konversi format file, pembersihan data, ekstraksi fitur, pelabelan manual, label *encoder*, normalisasi hingga pelatihan model. Hasil pengujian menunjukkan bahwa model dengan parameter $n_estimators = 10$ dan $max_depth = 5$ mampu menghasilkan akurasi prediksi sebesar 100% pada data uji. Selain akurat, sistem ini juga terintegrasi langsung dengan perangkat MikroTik untuk melakukan pemblokiran otomatis terhadap IP yang terprediksi sebagai penyerang, sehingga memberikan perlindungan aktif terhadap sistem jaringan.

Kata Kunci: Keamanan Jaringan, *Brute force*, *Mikrotik*, *Machine learning*, *Log Autentikasi*, *Random Forest*.

ABSTRACT

User authentication security is a crucial component in network management, especially on MikroTik devices that are widely used across various institutions. One of the most common and serious threats is brute force attacks, which involve repeated login attempts using various combinations of usernames and passwords to gain access. However, most existing protection mechanisms are still passive and unable to recognize attack patterns early on. This study proposes a machine learning-based approach using the Random Forest algorithm to detect brute force attacks in real-time. The advantage of this method lies in its ability to learn patterns from authentication log data based on features such as IP address, username, login protocol, failed login frequency, and commonly used attack usernames. The log data undergoes several processing stages, including file format conversion, data cleaning, feature extraction, manual labeling, label encoding, normalization, and model training. The test results show that the model with parameters $n_estimators = 10$ and $max_depth = 5$ achieves a prediction accuracy of 100% on the test dataset. In addition to its high accuracy, the system is also directly integrated with MikroTik devices to automatically block IP addresses predicted as attackers, thus providing active protection for the network system.

Keywords: Network Security, Brute Force, MikroTik, Machine Learning, Authentication Logs, Random Forest.