Analisis Kinerja Algoritma *Long Short-Term Memory* dalam Deteksi Intrusi Jaringan Berbasis Log Honeypot Cowrie SSH

Rendy Sahrasad

ABSTRAK

Peningkatan aktivitas jaringan komputer menuntut adanya sistem deteksi intrusi yang mampu mengenali pola aktivitas mencurigakan secara terstruktur. Penelitian ini bertujuan mengimplementasikan model *Network Intrusion Detection System* (NIDS) berbasis *Long Short-Term Memory* (LSTM) untuk mengklasifikasikan aktivitas pada log *honeypot* Cowrie SSH. Data log diproses melalui seleksi data Cowrie SSH, pembersihan data, pembentukan *event sequence* berdasarkan *session*, pembentukan label *multiclass*, *feature engineering*, penghapusan fitur yang berpotensi menyebabkan *data leakage* dan *proxy label*, *tokenization*, *padding*, serta pembagian data latih, validasi, dan uji. Kelas klasifikasi yang digunakan terdiri dari *normal*, *scan_probe*, dan *brute_force*. Model LSTM dievaluasi menggunakan metrik *accuracy*, *precision*, *recall*, *F1-score*, dan *confusion matrix*. Hasil evaluasi menunjukkan bahwa model memperoleh *accuracy* sebesar 99,30%, dengan *macro average* dan *weighted average precision*, *recall*, serta *F1-score* sebesar 99,30%. Selain evaluasi model, penelitian ini mengintegrasikan model ke dalam prototipe *dashboard* NIDS berbasis Flask, MongoDB, dan Docker. Hasil pengujian menunjukkan bahwa sistem mampu membaca log Cowrie SSH, membentuk token *session*, melakukan prediksi, menyimpan hasil, dan menampilkan klasifikasi dengan status pencatatan *LOGGED*. Sistem yang dikembangkan bersifat *detection-only* tanpa pemblokiran otomatis.

Kata Kunci: Cowrie SSH, *Honeypot*, *Long Short-Term Memory* (LSTM), *Multiclass*, *Network Intrusion Detection System* (NIDS).

Performance Analysis of Long Short-Term Memory for Network Intrusion Detection Based on Cowrie SSH Honeypot Logs

Rendy Sahrasad

ABSTRACT

The increasing use of computer networks requires an intrusion detection system capable of identifying suspicious activity patterns in a structured manner. This study aims to implement a Long Short-Term Memory (LSTM)-based Network Intrusion Detection System (NIDS) model to classify activities in Cowrie SSH honeypot logs. The log data were processed through Cowrie SSH data selection, data cleaning, session-based event sequence formation, multiclass label construction, feature engineering, removal of features causing data leakage and proxy labels, tokenization, padding, and data splitting into training, validation, and testing sets. The target classification categories consist of normal, scan_probe, and brute_force. The LSTM model was evaluated using accuracy, precision, recall, F1-score, and a confusion matrix. The evaluation results show that the model achieved an accuracy of 99.30%, with macro average and weighted average precision, recall, and F1-score values of 99.30%. In addition, the model was integrated into a NIDS dashboard prototype using Flask, MongoDB, and Docker. The testing results demonstrate that the system can read Cowrie SSH logs, generate session tokens, perform predictions, store results, and display classifications with a LOGGED status. The developed system operates as a detection-only mechanism and does not perform automatic blocking.

Keywords: *Cowrie SSH, Honeypot, Long Short-Term Memory (LSTM), Multiclass, Network Intrusion Detection System (NIDS).*