UNIVERSITAS
GADJAH MADA
Deep Learning-based Intrusion Detection System using LSTM
Teuku Aldi Fadhlur Rahman, I Gede Mujiyatna, S.Kom.,M.Kom
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

The increasing sophistication of cyber-attacks has necessitated the development of more robust intrusion detection systems (IDS) capable of identifying both known and zero-day threats. While traditional signature-based and anomaly-based detection methods have limitations in accuracy and false positive rates, deep learning approaches have demonstrated significant improvements in intrusion detection performance. This study developed a Long Short-Term Memory (LSTM)-based intrusion detection system using the UNSW-NB15 dataset to investigate the impact of network depth on detection performance. Unlike previous research that has primarily focused on demonstrating the viability of LSTM for intrusion detection, this study specifically examined how varying the number of hidden layers, from one to five, affects model accuracy, computational efficiency, and the risk of overfitting. Each configuration was trained with 128 hidden units per layer and evaluated across three independent trials to account for training variability. The dataset was preprocessed through an independent XGBoost-based feature selection process, Z-score normalization, and Synthetic Minority Over-sampling Technique (SMOTE) to address class imbalance. Results showed that all five configurations achieved comparable overall accuracy (97.48%–97.61%) and weighted F1-scores (0.9781–0.9790), indicating that increasing LSTM depth alone provides negligible improvement in aggregate classification performance. However, the macro-average F1-score, which weights all classes equally, peaked at the 2-layer and 3-layer configurations (0.5044 and 0.5030) before declining at greater depth, while minority attack classes such as Worms, Backdoor, and Analysis remained poorly detected across all configurations. Computational cost, in contrast, rose consistently and substantially with depth, with training time increasing by approximately 293% from the 1-layer to the 5-layer configuration. These findings indicate that model depth beyond two to three layers is not justified by the resulting performance gains, and that class imbalance, rather than architectural depth, remains the primary limiting factor for intrusion detection performance on the UNSW-NB15 dataset.

Keywords: Intrusion Detection System, Deep Learning, LSTM, UNSW-NB15, Network Security, Hidden Layers, Cyber-attack