Pengembangan Model Deteksi Intrusi Cerdas untuk Mengatasi Serangan Denial of Service Berbasis Hybrid Autoencoder, Long Short-Term Memory, dan Convolutional Neural Network = Development of Intelligence Intrusion Detection Model against Denial of Service Based on Hybrid Autoencoder, Long Short-Term Memory, and Convolutional Neural Network

Bambang Susilo, author

Abstrak

Perkembangan pesat perangkat Internet of Things (IoT) telah secara signifikan meningkatkan konektivitas dan otomatisasi dalam sistem modern, namun juga membuka jaringan ini terhadap ancaman siber yang semakin canggih. Salah satu ancaman yang paling krusial adalah serangan Distributed Denial of Service (DDoS), yang dapat melumpuhkan layanan IoT penting dan menyebabkan gangguan luas. Sistem deteksi intrusi (IDS) yang ada sering menghadapi tantangan dalam mengidentifikasi dan memitigasi serangan semacam itu karena tingginya dimensi data jaringan, sifat dinamis pola lalu lintas IoT, dan ketidakseimbangan bawaan dalam dataset yang tersedia. Pendekatan berbasis pembelajaran mesin tradisional, meskipun cukup efektif, sering kali kesulitan beradaptasi dengan kompleksitas dan skala jaringan IoT modern yang terus berkembang.

Penelitian ini mengatasi tantangan tersebut dengan mengusulkan kerangka kerja pembelajaran mendalam (deep learning) hibrid yang mengintegrasikan arsitektur Autoencoder (AE), Long Short-Term Memory (LSTM), dan Convolutional Neural Network (CNN). AE digunakan untuk ekstraksi fitur, mengurangi gangguan, dan fokus pada atribut yang paling relevan, sementara LSTM digunakan untuk menangkap ketergantungan temporal dan pola dalam data lalu lintas jaringan IoT yang bersifat sekuensial. Komponen CNN diintegrasikan untuk kekuatannya dalam ekstraksi fitur spasial, memungkinkan klasifikasi yang andal terhadap berbagai jenis serangan. Untuk mengatasi masalah krusial ketidakseimbangan dataset, model yang diusulkan memanfaatkan Synthetic Minority Oversampling Technique (SMOTE) untuk meningkatkan representasi kelas serangan yang kurang terwakili, sehingga memastikan pelatihan dan evaluasi yang lebih andal. Model ini dirancang untuk mengatasi tantangan kompleksitas dan skala jaringan IoT, serta memastikan deteksi yang akurat terhadap berbagai jenis serangan.

Metodologi penelitian ini mencakup pra-pemrosesan terhadap dataset intrusi IoT standar, termasuk penskalaan dan transformasi fitur untuk mengoptimalkan kinerja model. Model hibrid AE-LSTM+CNN kemudian dilatih dan divalidasi menggunakan dataset CICIoT2023 untuk mengevaluasi kemampuannya dalam mendeteksi dan mengklasifikasikan berbagai jenis serangan, termasuk serangan DoS.

Hasil eksperimen menunjukkan keunggulan pendekatan yang diusulkan dibandingkan metode mutakhir lainnya, dengan mencapai akurasi klasifikasi sebesar 99,15% dan presisi sebesar 99,39%. Dengan menggabungkan rekayasa fitur tingkat lanjut, analisis temporal dan spasial, serta teknik pembelajaran mendalam yang andal, penelitian ini menyediakan solusi yang terukur dan efektif untuk meningkatkan

keamanan jaringan IoT terhadap ancaman siber yang terus berkembang.

Hasil studi ini menegaskan model pembelajaran mendalam hibrid dalam mengatasi keterbatasan kerangka kerja IDS saat ini. Dengan mengintegrasikan fitur temporal, spasial, dan hasil rekayasa fitur ke dalam arsitektur yang terpadu, model yang diusulkan merepresentasikan langkah maju dalam melindungi ekosistem IoT dari vektor serangan yang semakin canggih dan beragam.
.....The rapid proliferation of Internet of Things (IoT) devices has significantly enhanced connectivity and automation in modern systems but has also exposed these networks to sophisticated cyber threats. Among these, Distributed Denial of Service (DDoS) attacks remain a critical concern, capable of crippling essential IoT services and causing widespread disruption. Existing intrusion detection systems (IDS) often face challenges in identifying and mitigating such attacks due to the high dimensionality of network data, the dynamic nature of IoT traffic patterns, and the inherent imbalance in available datasets. Traditional machine learning-based approaches, while effective to an extent, struggle to adapt to the growing complexity and scale of modern IoT networks.

This study addresses these challenges by proposing a hybrid deep learning framework that integrates Autoencoder (AE), Long Short-Term Memory (LSTM), and Convolutional Neural Network (CNN) architectures. The AE is utilized for feature extraction, reducing noise and focusing on the most relevant attributes, while the LSTM is employed to capture temporal dependencies and patterns in sequential IoT network traffic data. The CNN component is incorporated for its strength in spatial feature extraction, enabling robust classification of diverse attack types. To address the critical issue of dataset imbalance, the proposed model leverages the Synthetic Minority Oversampling Technique (SMOTE) to enhance the representation of underrepresented attack classes, ensuring more reliable training and evaluation. The model is designed to tackle the challenges of IoT network complexity and scale while ensuring accurate detection of diverse attack types.

The methodology involves preprocessing of benchmark IoT intrusion datasets, including feature scaling and transformation to optimize model performance. The hybrid AE-LSTM+CNN model is then trained and validated using the CICIoT2023 dataset to evaluate its ability to detect and classify various types of attacks, including DoS and DDoS attacks. The model’s architecture is fine-tuned to balance computational efficiency with detection accuracy.

Experimental results demonstrate the superiority of the proposed approach over existing state-of-the-art methods, achieving a classification accuracy of 99.15% and precision of 99.39%. By combining advanced feature engineering, temporal and spatial analysis, and robust deep learning techniques, this research provides a scalable and effective solution to enhance the security of IoT networks against evolving cyber threats.

The result of this study underscores the potential of hybrid deep learning models in addressing the limitations of current IDS frameworks. By integrating temporal, spatial, and engineered features into a unified architecture, the proposed model represents a step forward in protecting IoT ecosystems from increasingly sophisticated and diverse attack vectors.