

BAB II

TINJAUAN PUSTAKA

Pendekatan *deep learning* telah menjadi salah satu strategi utama dalam pengembangan sistem keamanan siber modern. Menurut Pradani (2024) dalam karyanya yang berjudul “Pendekatan *Deep Learning* untuk Deteksi Anomali dalam Keamanan Siber”, *deep learning* didefinisikan sebagai teknologi yang mampu mempelajari pola-pola kompleks dari data berskala besar dan beragam, guna mendeteksi anomali dengan tingkat akurasi yang tinggi [1]. Model yang digunakan dalam pendekatan ini antara lain *autoencoders*, *convolutional neural networks* (CNN), dan *generative networks*, yang mampu mengenali pola tidak biasa atau mencurigakan dalam data lalu lintas jaringan. Model-model tersebut memanfaatkan pembelajaran berlapis (*multi-layer*) layaknya kerja sistem saraf otak manusia, sehingga memungkinkan sistem untuk belajar dan mengenali ancaman siber yang bersifat dinamis dan terus berkembang.

Sementara itu, Maulani et al. (2023) dalam penelitiannya yang berjudul “Sistem Deteksi Intrusi Cerdas: Studi Perbandingan Algoritma Pembelajaran Mesin untuk Keamanan Siber” mengemukakan bahwa IDS cerdas merupakan pendekatan berbasis teknologi yang memanfaatkan algoritma pembelajaran mesin untuk meningkatkan efektivitas sistem keamanan jaringan [2]. Sistem ini dirancang agar mampu memproses data dalam skala besar secara real-time, menganalisis pola perilaku lalu lintas jaringan, serta mendeteksi aktivitas anomali yang tidak dapat diidentifikasi secara akurat oleh metode tradisional seperti rule-based atau analisis statistik sederhana. Penelitian ini memfokuskan perbandingan pada sejumlah algoritma pembelajaran mesin, dengan mengkaji aspek akurasi deteksi serangan, jumlah kesalahan deteksi (*false positives* dan *false negatives*), serta tingkat respons sistem terhadap berbagai bentuk ancaman. Hasil penelitian menunjukkan bahwa pembelajaran mesin unggul dalam kemampuan adaptasi terhadap pola serangan baru, meskipun masih menghadapi tantangan teknis seperti kebutuhan komputasi yang tinggi dan kesulitan dalam pemeliharaan sistem dalam jangka panjang. Oleh

karena itu, pemilihan algoritma yang tepat sangat penting agar sistem dapat diimplementasikan secara optimal sesuai kebutuhan masing-masing organisasi.

Lebih lanjut, penguatan landasan konseptual mengenai keamanan siber dijelaskan oleh Santoso (2023) dalam bukunya “Teknologi Keamanan Siber (*Cyber Security*)”. Dalam pandangannya, keamanan siber merupakan praktik perlindungan sistem komputer, jaringan, perangkat, dan data dari berbagai ancaman dunia maya [3]. Keamanan siber sendiri mencakup tiga aspek fundamental, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Kerahasiaan bertujuan untuk mencegah akses yang tidak sah terhadap informasi sensitif, integritas menjamin bahwa data tetap akurat dan tidak mengalami perubahan tanpa izin, sedangkan ketersediaan memastikan bahwa layanan dan data dapat diakses oleh pihak yang berhak kapan pun dibutuhkan. Tantangan keamanan siber yang dihadapi saat ini semakin kompleks, mulai dari serangan *malware*, *phishing*, *ransomware*, serangan *Denial of Service* (DoS), hingga eksploitasi perangkat *Internet of Things* (IoT). Oleh karena itu, integrasi antara pendekatan pembelajaran mesin dan *deep learning* dengan prinsip-prinsip dasar keamanan siber menjadi suatu keharusan untuk menciptakan sistem pertahanan digital yang adaptif dan tangguh dalam menghadapi lanskap ancaman siber yang terus berkembang.

Tabel 2.1. Perbandingan dari Penelitian Terdahulu Mengenai *Intrusion Detection System* Berbasis *Deep Learning*

No	Judul Penelitian	Tahun	Algoritma <i>Deep Learning</i>	Dataset yang Digunakan	Metrik Evaluasi Utama	Hasil Kinerja Kunci (Contoh)	Kelebihan Utama	Kekurangan/ Tantangan	Referensi
1.	Pendekatan <i>Deep Learning</i> Untuk Deteksi Anomali dalam Keamanan Siber	2024	Autoencoder, CNN, Generative Networks	Data lalu lintas jaringan berskala besar dan beragam	Akurasi Deteksi Anomali	Akurasi Tinggi (Misal: 97%)	Mampu mempelajari pola kompleks dari data berskala besar dan beragam untuk mendeteksi anomali dengan akurasi tinggi. Fleksibel dalam mengidentifikasi pola tidak biasa	Implementasi memerlukan sumber daya komputasi yang intensif, serta kompleksitas dalam interpretasi hasil model yang mendalam.	[1]

No	Judul Penelitian	Tahun	Algoritma Deep Learning	Dataset yang Digunakan	Metrik Evaluasi Utama	Hasil Kinerja Kunci (Contoh)	Kelebihan Utama	Kekurangan/ Tantangan	Referensi
							dalam lalu lintas jaringan.		
2.	Sistem Deteksi Intrusi Cerdas: Studi Perbandingan Algoritma Pembelajaran Mesin Untuk Keamanan Siber	2023	Algoritma Pembelajaran Mesin (umum) (misal: SVM, Random Forest, ANN)	Data skala besar, lalu lintas jaringan	Akurasi deteksi serangan, <i>False Positives/Negatives</i> , Respons Sistem	Algoritma B optimal (keseimbangan akurasi dan kebocoran rendah)	Unggul dalam adaptasi terhadap pola serangan baru dan mampu memproses data dalam skala besar secara <i>real-time</i> . Menawarkan keseimbangan baik antara akurasi deteksi dan tingkat	Menghadapi tantangan teknis seperti kebutuhan komputasi yang tinggi dan kesulitan dalam pemeliharaan serta kalibrasi sistem dalam jangka panjang.	[2]

No	Judul Penelitian	Tahun	Algoritma <i>Deep Learning</i>	Dataset yang Digunakan	Metrik Evaluasi Utama	Hasil Kinerja Kunci (Contoh)	Kelebihan Utama	Kekurangan/ Tantangan	Referensi
							kebocoran (<i>false positives/negatives</i>).		
3.	Pengembangan <i>Intrusion Detection System</i> (IDS) Berbasis <i>Machine Learning</i>	2023	J48 (Decision Tree), Naïve Bayes, AdaBoost M1	UNSW-NB15 dan CICIDS2017	Akurasi, Presisi, <i>Recall</i>	Algoritma J48 menghasilkan akurasi tertinggi sebesar 99.839%.	Mencapai akurasi deteksi serangan yang sangat tinggi (99.839% dengan J48) dan Menggunakan metode seleksi fitur yang efisien (CFs-Greedy stepwise)	Studi ini berfokus pada algoritma <i>Machine Learning</i> tradisional (J48, Naïve Bayes, AdaBoostM1) daripada arsitektur <i>Deep Learning</i> yang sering digunakan untuk	[4]

No	Judul Penelitian	Tahun	Algoritma Deep Learning	Dataset yang Digunakan	Metrik Evaluasi Utama	Hasil Kinerja Kunci (Contoh)	Kelebihan Utama	Kekurangan/ Tantangan	Referensi
							untuk optimasi kinerja deteksi	pola anomali lebih kompleks	
4.	Implementasi Long Short-Term Memory dalam Deteksi Serangan DDoS pada Virtual Private Server	2024	Long Short-Term Memory (LSTM)	Data serangan DDoS pada VPS: Total 70.343 dan Dataset IDS 2018	F1-Score, Presisi, Recall	Presisi, Recall, F1-Score	Mengatasi masalah <i>vanishing gradient</i> pada RNN dan mampu mempertahankan informasi jangka panjang, penting untuk pola serangan DDoS.	Performa model LSTM sangat bervariasi tergantung pada dataset yang digunakan (akurasi turun drastis dari 96,35% ke 50,42% pada dataset yang berbeda)	[5]

No	Judul Penelitian	Tahun	Algoritma Deep Learning	Dataset yang Digunakan	Metrik Evaluasi Utama	Hasil Kinerja Kunci (Contoh)	Kelebihan Utama	Kekurangan/ Tantangan	Referensi
5.	<i>Intrusion Detection System</i> Berbasis <i>Deep Learning</i> Untuk Peningkatan Mitigasi SQL <i>Injection</i> dan <i>Syn Flood Attack</i>	2024 (Nove mber)	Arsitektur CNN: VGG-16, ResNet50, InceptionV3	CICDDoS2 019 (untuk Syn Flood): 5416 data latih, 1354 data uji. CSE-CIC-IDS2018 (untuk SQL <i>Injection</i>): 3160 data	Akurasi, Presisi, <i>Recall</i> , F1- <i>Score</i> , <i>True Positive Rate</i> (TPR), <i>True Negative Rate</i> (TNR).	Syn Flood Attack: - VGG-16: 99.9261% (Loss: 0.018590) - ResNet50: 99.9263% (Loss: 0.024910) - Inception	Mengusulkan dan membandingkan tiga arsitektur CNN <i>Deep Learning</i> yang canggih (VGG-16, ResNet50, InceptionV3) untuk deteksi intrusi.	Meskipun akurasi InceptionV3 tinggi, kinerja presisi dan recall-nya lebih rendah dibandingkan VGG-16 dan ResNet50 untuk kedua serangan siber, menunjukkan lebih banyak kesalahan dalam deteksi	[6]

No	Judul Penelitian	Tahun	Algoritma <i>Deep Learning</i>	Dataset yang Digunakan	Metrik Evaluasi Utama	Hasil Kinerja Kunci (Contoh)	Kelebihan Utama	Kekurangan/ Tantangan	Referensi
				latih, 790 data uji.		V3: 99.7784% (Loss: 0.015571) SQL Injection: - VGG-16: 99.9983% (Loss: 0.001294) - ResNet50: 99.9962%		positif/negatif palsu.	

No	Judul Penelitian	Tahun	Algoritma <i>Deep Learning</i>	Dataset yang Digunakan	Metrik Evaluasi Utama	Hasil Kinerja Kunci (Contoh)	Kelebihan Utama	Kekurangan/ Tantangan	Referensi
						(Loss: 0.001749) - Inception V3: 99.9872% (Loss: 0.000392)			