BAB II

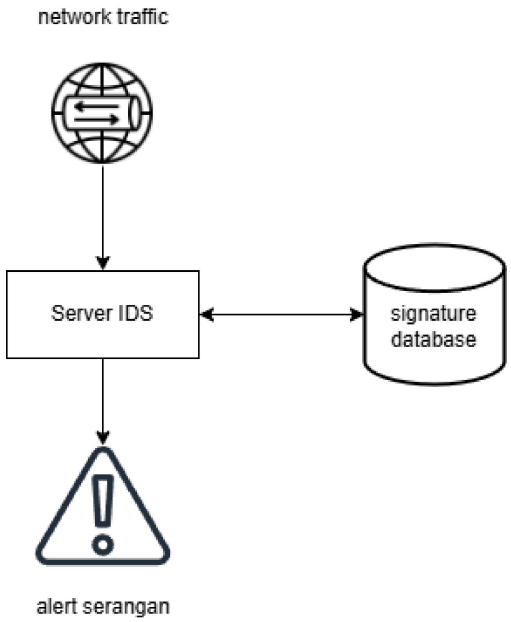
Landasan Teori

2.1 *Intrusion Detection System*

Intrusion Detection System (IDS) merupakan sistem yang digunakan untuk mendeteksi aktivitas mencurigakan dalam sebuah sistem atau jaringan (Ananda Febian dkk., 2024). IDS terbagi menjadi dua jenis, yaitu *Network-Based Intrusion Detection System* (NIDS) dan *Host-Based Intrusion Detection System* (HIDS). NIDS merupakan perangkat lunak yang bekerja dengan cara memantau paket pada trafik dalam suatu jaringan. Paket pada trafik jaringan ini nantinya akan dianalisis untuk mengidentifikasi percobaan serangan pada jaringan. Sementara itu, HIDS merupakan jenis IDS yang bekerja pada *host* individual atau perangkat tertentu pada sistem jaringan komputer secara *real-time.* HIDS akan memantau paket-paket data ketika sedang terjadi penyusupan saja (Purba & Efendi, 2021). Berdasarkan cara deteksinya, IDS memiliki dua pendekatan, yaitu *Signature-based detection* dan *Anomaly-based Detection*.

2.1.1 Signature-based Detection

Signature-based detection merupakan salah satu pendekatan yang sering digunakan untuk mendeteksi serangan siber. Pendekatan ini menggunakan ciri khas pola atau *signature* untuk mengidentifikasi serangan. Pendekatan berbasis *signature* sangat efektif dan jarang menghasilkan kesalahan dalam mendeteksi serangan yang polanya sudah diketahui (Fikri dkk., 2024). Adapun cara kerja deteksi berbasis *signature* terdapat pada Gambar 2.1.



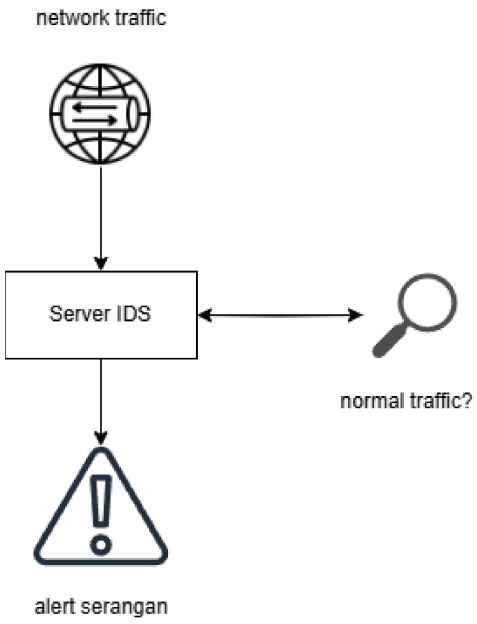
Gambar 2. 1 Cara kerja IDS berbasis *signature*

IDS berbasis *signature* bekerja dengan cara menangkap data pada trafik jaringan, yang kemudian akan dibandingkan dengan *database* yang berisi pola-pola serangan. Jika terdapat kecocokan antara pola data yang ada pada trafik jaringan dengan *database*, maka paket data tersebut akan dianggap sebagai serangan. Pendekatan berbasis *signature* ini sangat cocok digunakan untuk mendeteksi ancaman yang polanya sudah diketahui.

2.1.2 Anomaly-Based Detection

Anomaly-based detection merupakan pendekatan yang berfokus pada pemetaan perilaku normal sistem yang dilindungi. Pendekatan ini bekerja seperti pengawas yang selalu mengamati pola normal pada sistem. Pendekatan ini sangat efektif dalam mendeteksi serangan baru, tetapi memiliki potensi *false positive* yang tinggi

(Fikri dkk., 2024). Cara kerja deteksi berbasis *anomaly* dapat dilihat pada Gambar 2.2.



Gambar 2. 2 Cara kerja IDS berbasis *anomaly*

IDS berbasis *anomaly* bekerja dengan cara menangkap data pada trafik jaringan, yang kemudian akan dibandingkan dengan profil normal yang sebelumnya telah dibuat. Profil normal biasanya dibentuk dari trafik jaringan yang diperoleh melalui observasi atau analisis dari penggunaan jaringan dalam kondisi wajar.

2.2 *Machine Learning*

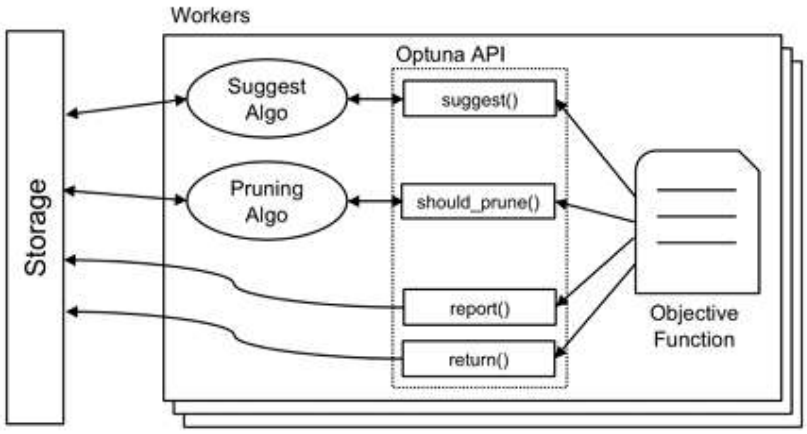
Pembelajaran mesin atau *machine learning* merupakan sebuah keilmuan atau bidang yang mempelajari teknik dan algoritma untuk melakukan otomatisasi terhadap berbagai permasalahan kompleks yang sulit diselesaikan oleh manusia (Rebala Gopinath dkk., 2019). Secara umum, *machine learning* terbagi menjadi

supervised learning, *unsupervised learning*, dan *reinforcement learning. Supervised learning* merupakan suatu pendekatan dalam *machine learning* yang menggunakan data berlabel untuk melakukan klasifikasi atau prediksi. Selanjutnya, *unsupervised learning* merupakan pendekatan yang berkebalikan dengan *supervised learning,* di mana klasifikasi atau prediksi dilakukan tanpa data berlabel. Terakhir, *reinforcement learning* merupakan pendekatan di mana model belajar untuk membuat keputusan dengan cara berinteraksi dengan lingkungannya melalui *trial and error* (Nurhalizah dkk., 2024).

Model *machine learning* yang akan diterapkan pada penelitian ini adalah model *unsupervised learning* dengan nama *Isolation Forest.* Model ini dipilih karena efisiensi komputasinya, seperti kebutuhan memori yang rendah serta waktu eksekusi yang relatif singkat. Dengan kemampuan tersebut, *Isolation Forest* mampu menangani *dataset* besar (Cao dkk., 2024; Chabchoub dkk., 2022; Liu dkk., 2008). Selain efisiensi komputasi, model *Isolation Forest* juga cukup baik dalam membedakan antara data *anomaly* dan data normal (Soenen dkk., 2021).

Machine learning memiliki parameter yang dapat diatur untuk memengaruhi performa model. Pada penelitian ini, model *machine learning* akan dioptimasi menggunakan Optuna untuk menentukan nilai *hyperparameter* (parameter yang dapat diatur). Optuna digunakan karena kemampuannya untuk melakukan *pruning* ketika kombinasi *hyperparameter* tidak menghasilkan peningkatan yang signifikan. *Pruning* pada Optuna membuat pencarian *hyperparameter* terbaik lebih cepat dan efisien jika dibandingkan dengan metode tradisional seperti GridSearch dan

RandomSearch (Lim, 2022; Tikaningsih dkk., 2024). Adapun cara kerja dari Optuna dapat dilihat pada Gambar 2.3.



Gambar 2. 3 Cara kerja Optuna (Akiba dkk., 2019)

Setiap *worker* bertanggung jawab menjalankan bagian dari *objective function. Objective function* memanfaatkan API Optuna untuk melaksanakan *trial*. Selain itu, *objective function* juga menggunakan *storage* untuk memperoleh informasi terkait studi yang telah dilakukan sebelumnya. Meskipun setiap *worker* beroperasi secara independen dalam menjalankan *objective function*, *worker* tetap berbagi perkembangan studi yang sedang berlangsung melalui *storage (Akiba dkk., 2019).*

2.3 *State Of The Art*

Tabel 2. 1 *State Of The Art*

No	Nama Peneliti	Judul	Dataset	Ruang Lingkup	Metode	Hasil	kekurangan
1	(Pinontoan & Sembiring, 2022)	Implementasi dan Analisis Deteksi Serangan Jaringan Pada Web Server NFT Menggunakan Suricata	-	Menguji kehandalan IDS berbasis *signature* Suricata dalam mendeteksi serangan siber seperti *port scanning* dan DDoS	Signature-Based IDS Suricata	Efektif dalam mendeteksi serangan yang sudah diketahui polanya.	Bergantung pada data yang sudah ada dan tidak mampu mendeteksi serangan baru
2	(Ananda Febian dkk., 2024)	Analisis Perbandingan Teknik Signature-Based dan Anomaly-Based Detection Pada Snort dan Zeek Dalam Mencegah Intrusi Jaringan	-	Membandingkan pendekatan signature dan *anomaly* pada open IDS	Signature dan anomaly based (Snort dan Zeek)	Zeek lebih fleksibel dalam anomaly detection, sementara Snort lebih stabil untuk signature-based detection.	Zeek lebih sulit dikonfigurasi dibanding Snort.
3	(Suci Sekar Sari & Agus	Analisis Efektivitas Rule	-	Menganalisis efektivitas dari rule	Pengembangan Rule pada Snort	Pengembangan rule baru	Efektivitas bergantung

No	Nama Peneliti	Judul	Dataset	Ruang Lingkup	Metode	Hasil	kekurangan
	Tedyyana, 2024)	Snort dalam Mendeteksi Serangan Jaringan		snort terhadap serangan siber seperti DdoS		meningkatkan deteksi serangan seperti DDoS.	pada kualitas rule yang diperbarui dan butuh update berkala agar tetap efektif.
4	(Fikri dkk., 2024)	Analisis Perbandingan Metode dan Performa Antara Suricata dan Snort	-	Membandingkan efektivitas dari dua open source IDS dalam mendeteksi serangan.	Signature-Based IDS	Membandingkan dua open source ids dalam mendeteksi serangan. Suricata mendapatkan akurasi sebesar 61% dan snort mendapatkan akurasi sebesar 31%	Snort lebih cepat dalam deteksi serangan tetapi kurang akurat, Suricata lebih akurat tetapi sedikit lebih lambat
5	(Ernawati dkk., 2019)	Analysis of Intrusion Detection System Performance for the Port Scan Attack Detector,	-	Menguji perbedaan 3 signature based ids dalam mendeteksi seragan	Signature based (Suricata, Portsentry, dan PSAD)	Suricata dan psad memiliki performa yang lebih baik saat digunakan sebagai network IDS. Suricata memiliki kemampuan	Signature based ids tidak bisa medeteksi pola serangan *unknown*. Pengujian juga hanya dilakukan

No	Nama Peneliti	Judul	Dataset	Ruang Lingkup	Metode	Hasil	kekurangan
		Portsentry, and Suricata				superior pada penggunaan sumber daya komputer.	terhadap 3 jenis serangan dan masing-masing 10 sampel serangan.
6	(Guide dkk., 2024)	Characterizing the Modification Space of Signature IDS Rules	-	Menunjukan bahwa modifikasi pada rule IDS dapat melonggarkan beeberapa kendala	Modified Signature based IDS	Dengan memodifikasi aturan dan konten, space atau ruang kinerja berhasil diperluas sebesar 11,3%	Masih bergantung pada pembaruan manual rule.
7	(Xu & Liu, 2025)	Robust Anomaly Detection in Network Traffic: Evaluating Machine Learning Models on CICIDS2017	CICIDS2017	Membandingkan penggunaan model supervised dan unsupervised dalam mendeteksi known dan unknown attack	Supervised dan unsupervised model	Supervised model sangat bagus dan hampir sempurna dalam mendeteksi serangan pada skenario known attack. Namun pada skenario unknown attack, unsupervised model lebih unggul.	Meskipun unsupervised model unggul dalam mendeteksi unknown attack, namun kemampuan itu diperoleh dengan pertukaran nilai false alarm yang cukup tinggi.

No	Nama Peneliti	Judul	Dataset	Ruang Lingkup	Metode	Hasil	kekurangan
							hal ini ditunjukan dari tingginya recall unsupervised model seperti *local outlier factor* dengan rendahnya nilai precision.
8	(Wolsing dkk., 2024)	One IDS is not Enough! Exploring Ensemble Learning for Industrial Intrusion Detection	SWAT dan WADI	Melakukan ensemble dengan 7 model IDS berbasis *signature*	Ensemble IDS	Keputusan dari beberapa IDS berhasil menekan tingkat alarm palsu hingga mendekati nilai 0	Semakin ketat *gating* yang digunakan semakin rendah *false positive* tapi semakin rendah juga *recall* atau serangan yang terdeteksi.
9	(Alabdulatif & Rizvi, 2023)	Network intrusion detection system using an optimized machine	Kitsune Dataset	Menganalisis pengaruh hyperparameter terhadap algoritma berbasis tree.	Fine Tree, Medium Tree, Coarse Tree, Linear SVM, Quadratic SVM, Cubic SVM,	Pada pengujian yang dilakukan terhadap 8 tipe serangan, semuanya mendapat nilai	Pengukuran hanya dilakukan terhadap serangan yang sudah

No	Nama Peneliti	Judul	Dataset	Ruang Lingkup	Metode	Hasil	kekurangan
		learning algorithm			Fine Gaussian SVM, Medium Gaussian SVM, Coarse Gaussian SVM, Boosted Tree, Bagged Tree, Subspace Discriminant, RUSBoosted Tree, Logistic Regression, and Gaussian Naïve Bayes, Bayesian, Grid Search, Random Search	akurasi sebesar 100%. Berdasarkan percobaan, Grid Search menunjukkan hasil terbaik dalam mendeteksi serangan dan menghasilkan error klasifikasi yang paling rendah.	diketahui. Selain itu, tidak dilakukan pengecekan apakah model overfitting.
10	(Ouiazzane dkk., 2022)	A Suricata and Machine Learning Based Hybrid Network Intrusion Detection System	CIC-IDS2017	Mengintegrasikan open source IDS SURICATA (SNIDS) dengan model Decision Tree (ADNIDS)	Hibrida SNIDS dan ADNIDS	Akurasi yang sangat tinggi dalam mendeteksi traffic normal. Nilai akurasi yang diperoleh mencapai 99,9%	Pengujian hanya dilakukan terhadap traffic normal. Keandalan model dalam mendeteksi traffic

No	Nama Peneliti	Judul	Dataset	Ruang Lingkup	Metode	Hasil	kekurangan
							malicious belum terukur
11	(Bampoe, 2025)	The Advantages of Hybrid Intrusion Detection Systems: A Comparative Study of Anomaly-Based and Signature-Based Approaches	NSL-KDD dan UNSW-NB15	Mengukur performa model hibrida *signature* dan *anomaly* dalam mendeteksi serangan	Hibrida signature dan anomaly ids	IDS Hibrida berhasil mengungguli model signature dan *anomaly* yang berdiri sendiri pada nilai akurasi, false positive rate, dan penggunaan resource.	Pengukuran model hibrida terhadap serangan known attack dan unknown attack tidak dijelaskan secara terperinci, seperti bagaimana kekuatan model ketika menghadapi skenario known attack dan bagaimana kekuatan model dalam menghadapi skenario

No	Nama Peneliti	Judul	Dataset	Ruang Lingkup	Metode	Hasil	kekurangan
							unknown attack.
12	(Elmubarak dkk., 2019)	Implementation Hybrid (NIDS) System using Anomaly Holtwinter Algorithm and Signature based Scheme	Darapa	Menggabungkan konsep IDS berbasis *signature* dengan algoritma holt-winter	Hibrida snort IDS berbasis *signature* dan holt winter	Model hibrida berhasil meningkatkan tingkat false negative sebanyak 29,30% dan menurunkan false negative sebesar 35,7%.	Pada penelitian ini metode signature dan *anomaly* digabungkan secara mentah, sehingga meningkatkan *false positive rate* sebesar 20,61% yang dimana menyebabkan banyak alarm serangan palsu.
13	(Alnasser dkk., 2025)	Signature and anomaly based intrusion detection system for secure IoTs and V2G communication	CSE-CIC-IDS 2018, CIC-DDoS 2019	Menggabungkan konsep signature dan *anomaly* pada keamanan iot dan komunikasi V2G	Metode hibrida dari *signature* dan *anomaly*	Performa model yang diusulkan menunjukkan hasil yang baik dibandingkan dengan penelitian sebelumnya yang menggunakan	Meskipun rasio deteksi yang ditemukan lebih baik dari penelitian sebelumnya, namun pertukaran nilai

No	Nama Peneliti	Judul	Dataset	Ruang Lingkup	Metode	Hasil	kekurangan
						Support Vector Machine (SVM) yang menjalankan SPARK. Rasio deteksi ditemukan lebih dari 96%, dibandingkan dengan penelitian terbaru pada sistem IDS hibrida.	antara performa yang diperoleh dengan resource yang digunakan belum terukur. Selain itu, *gating* menggunakan 1^1 membuat *unknown attack* tidak memberi *alert* namun hanya memberi data untuk dianalisis lebih lanjut.
14	(Díaz-Verdejo dkk., 2022)	On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks	Fwaf-bad, Fwaf-2200, ataques-800, ataques-1100, rdb, osvdb, A-420	Mengukur kemampuan ids menggunakan default ruleset (kumpulan signature)	*Signature based*	Penggabungan kemampuan 3 model ids dalam melakukan keputusan meningkatkan recall hingga mencapai 96,7%. Penyesuaian	Kemampuan model signature yang berdiri sendiri kurang kuat dan ketika ketiga model digabungkan, resource yang

No	Nama Peneliti	Judul	Dataset	Ruang Lingkup	Metode	Hasil	kekurangan
						ruleset default juga dapat menekan *false positive* hingga 0.	digunakan juga meningkat.
15	(Kalavadekar & Sane, 2019)	Building an Effective Intrusion Detection System using combined Signature and Anomaly Detection Techniques	DARPA Lincoln Lab, KDD Cup 99, NSLKDD, UGR16, dan KyotoAugust2009	Mengkombinasikan pendekatan berbasis *signature* dengan pendekatan berbasis *anomaly*	Hibrida *Signature* dan *anomaly*	Metode hibrida berhasil mendapatkan rata-rata akurasi sebesar 99,87%	Dalam pembahasan dijelaskan bahwa model bisa mendeteksi *known* dan *unknown,* tapi pengukuran terhadap masing-masing skenario pengujian tersebut tidak ada.

Berdasarkan kajian pada Tabel 2.1, diketahui bahwa IDS berbasis *signature* bergantung pada pola serangan yang sudah diketahui dan mengalami kesulitan dalam mendeteksi serangan yang tidak diketahui. Sebaliknya, pendekatan *anomaly* berbasis *machine learning* lebih efektif dalam mengidentifikasi serangan yang tidak diketahui, tetapi memiliki kelemahan berupa tingginya tingkat *false positive* yang dapat menimbulkan beban berlebih pada sistem. Sejumlah penelitian mencoba menggabungkan kedua pendekatan tersebut dalam

bentuk IDS hibrida, dengan harapan mampu mengombinasikan keunggulan *signature* dan *anomaly* secara bersamaan. Meskipun demikian, beberapa penelitian juga menunjukkan bahwa kombinasi antar model yang dirancang secara tidak hati-hati justru dapat menambah beban kerja pada model akibat banyaknya alarm palsu. Berdasarkan kondisi tersebut, penelitian ini mengusulkan penggunaan *gating* dengan mekanisme *watchlist* untuk membatasi alarm palsu pada keputusan akhir sistem. Selain itu, penelitian ini juga menerapkan skenario pengujian *known attack* dan *unknown attack* untuk mengukur kemampuan model hibrida. Kedua skenario pengujian ini digunakan untuk mengukur *trade-off* yang terjadi pada model hibrida dalam dua kondisi yang berbeda.

2.4 Matriks Penelitian

Tabel 2. 2 Matriks penelitian

No	Peneliti	Judul Penelitian	Signature Based Detection	Anomaly Based Detection	Machine Learning	Hybrid Detection	Computional Resource Measurement	Unknown attack Scheme	Hyperparameter Optimization
1	(Pinontoan & Sembiring, 2022)	Implementasi dan Analisis Deteksi Serangan Jaringan Pada Web Server NFT Menggunakan Suricata	✓	-	-	-	-	-	-
2	(Ananda Febian dkk., 2024)	Analisis Perbandingan Teknik Signature-Based dan Anomaly-Based Detection Pada Snort dan Zeek Dalam Mencegah Intrusi Jaringan	✓	✓	-	-	-	-	-
3	(Suci Sekar Sari & Agus Tedyyana, 2024)	Analisis Efektivitas Rule Snort dalam Mendeteksi Serangan Jaringan	-	✓	-	-	-	-	-
4	(Fikri dkk., 2024)	Analisis Perbandingan Metode dan Performa Antara Suricata dan Snort	✓	✓	-	-	-	-	-
5	(Ernawati dkk., 2019)	Analysis of Intrusion Detection System Performance for the Port Scan Attack Detector, Portsentry, and Suricata	✓	✓	-	-	✓	-	-
6	(Xu & Liu, 2025)	Robust Anomaly Detection in Network Traffic: Evaluating Machine Learning Models on CICIDS2017	-	✓	✓	-	-	✓	-

No	Peneliti	Judul Penelitian	Signature Based Detection	Anomaly Based Detection	Machine Learning	Hybrid Detection	Computional Resource Measurement	Unknown attack Scheme	Hyperparamete r Optimization
7	(Wolsing dkk., 2024)	One IDS Is Not Enough! Exploring Ensemble Learning for Industrial Intrusion Detection	-	✓	✓	-	-	-	-
8	(Alabdulatif & Rizvi, 2023)	Network intrusion detection system using an optimized machine learning algorithm	-	✓	✓	-	✓	-	✓
9	(Ouiazzane dkk., 2022)	A Suricata and Machine Learning Based Hybrid Network Intrusion Detection System	✓	✓	✓	✓	-	-	-
10	(Bampoe, 2025)	The Advantages of Hybrid Intrusion Detection Systems: A Comparative Study of Anomaly-Based and Signature-Based Approaches	✓	✓	✓	✓	✓	-	-
11	(Elmubarak dkk., 2019)	Implementation Hybrid (NIDS) System using Anomaly Holtwinter Algorithm and Signature based Scheme	✓	✓	-	✓	-	-	-
12	(Alnasser dkk., 2025)	Signature and anomaly based intrusion detection system for secure IoTs and V2G communication	✓	✓	✓	✓	-	✓	✓
13	(Díaz-Verdejo dkk., 2022)	On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks	✓	-	-	-	-	-	-
14	(Kalavadekar & Sane, 2019)	Building an Effective Intrusion Detection System using combined Signature and Anomaly Detection Techniques	✓	✓	✓	✓	-	-	-
15	(Guide dkk., 2024)	Characterizing the Modification Space of Signature IDS Rules	✓	-	-	-	-	-	-

Berdasarkan metrik pada Tabel 2.2, dapat dilihat bahwa sebagian besar penelitian IDS hibrida belum secara bersamaan membandingkan kinerja model dalam skenario berbeda, yaitu *known attack* dan *unknown attack*. Selain itu, penelitian hibrida yang ada cenderung berfokus pada peningkatan deteksi serangan, namun belum banyak yang mengevaluasi sejauh mana model hibrida mampu mengendalikan dampak *false positive* yang dihasilkan oleh komponen deteksi *anomaly* pada masing-masing skenario. Beberapa penelitian juga jarang menyinggung aspek penggunaan memori, padahal hal ini penting untuk menilai *trade-off* antara performa deteksi dengan sumber daya komputasi yang digunakan. Namun demikian, fokus penelitian ini tetap pada pengukuran efektivitas IDS hibrida dalam skenario *known attack* dan *unknown attack*, sekaligus menganalisis kontribusinya dalam membatasi *false positive* yang dihasilkan oleh model deteksi *anomaly* berbasis *machine learning* pada *output* sistem.