https://jurnal.pustakagalerimandiri.co.id/index.php/pustakaai
DOI : https://doi.org/10.55382/jurnalpustakaai.v5i1.919

JURNAL PUSTAKA AI
JURNAL PUSAT AKSES KAJIAN TEKNOLOGI ARTIFICIAL INTELLIGENCE
Pustaka Galeri Mandiri

Vol. 5 No. 1 (2025) 45 – 49 E ISSN: 2809-4069

# Pengembangan Kebijakan Keamanan Adaptif Berbasis Machine Learning pada Firewall SDN

Nurhadi Surojudin[1], Ahmad Turmudi Zy[2], Donny Maulana[3], Abdul Halim Anshor[4]
[1234]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]Nurhadi@pelitabangsa.ac.id. [2]turmudi@pelitabangsa.ac.id

***Abstract***

*By increasing of digital complexity, cyberattacks such as Distributed Denial of Service (DDoS) present major challenges in network security management. This study proposes the development of an adaptive security policy powered by machine learning for firewalls within Software-Defined Networking (SDN) architecture. Utilizing the Random Forest algorithm and CICIDS2017 dataset, the system can automatically and accurately detect DDoS attacks. A stratified data split ensures balanced label proportions, and invalid values are handled through data cleaning. The model demonstrates outstanding performance, achieving 99.9978% accuracy, 99.996% precision and recall, and a 99.996% f1-score. Evaluation through the confusion matrix shows only two misclassifications out of 45,149 test samples. These results confirm that integrating machine learning into SDN-based firewalls can significantly enhance threat detection and support dynamic, efficient, and adaptive security policies. Future development plans include deployment on real-time traffic and extending detection capabilities to other types of attacks. This finding contributes significantly to the advancement of intelligent, SDN-based network security solutions.*

*Keywords: adaptive security, SDN firewall, machine learning, DDoS attack, Random Forest*

Abstrak

Dalam era digital yang semakin kompleks, serangan siber seperti Distributed Denial of Service (DDoS) menjadi tantangan besar dalam pengelolaan keamanan jaringan. Penelitian ini mengusulkan pengembangan kebijakan keamanan adaptif berbasis machine learning untuk firewall pada arsitektur Software-Defined Networking (SDN). Dengan menggunakan algoritma Random Forest dan dataset CICIDS2017, sistem mampu mendeteksi serangan DDoS secara otomatis dan akurat. Data diuji melalui metode stratified split agar proporsi label tetap seimbang, serta dilakukan pembersihan nilai tak valid. Model menunjukkan performa sangat tinggi dengan akurasi 99,9978%, precision dan recall 99,996%, serta f1-score 99,996%. Evaluasi melalui confusion matrix mengindikasikan hanya dua kesalahan klasifikasi dari total 45.149 data uji. Hasil ini membuktikan bahwa integrasi machine learning dalam firewall SDN dapat memperkuat deteksi ancaman dan menghasilkan kebijakan keamanan yang dinamis, efisien, serta dapat beradaptasi terhadap serangan baru. Rencana pengembangan ke depan mencakup penerapan pada data real-time dan perluasan cakupan deteksi terhadap jenis serangan lainnya. Temuan ini memberikan kontribusi signifikan dalam pengembangan solusi keamanan jaringan berbasis SDN yang cerdas.

Kata kunci: *keamanan adaptif, firewall SDN, machine learning, serangan DDoS, Random Forest*

Submitted : 19-04-2025 | Reviewed : 20-04-2025 | Accepted : 30-04-2025

## 1. Pendahuluan

Di era transformasi digital yang semakin pesat, ancaman siber berkembang menjadi lebih canggih dan sulit dikenali. Salah satu bentuk serangan yang paling mengganggu adalah Distributed Denial of Service (DDoS), yang dapat menyebabkan gangguan layanan skala besar dan kerugian ekonomi yang signifikan [1]. Serangan ini tidak hanya berdampak pada infrastruktur teknologi informasi tetapi juga mengancam kontinuitas layanan pada sektor-sektor vital seperti keuangan, pemerintahan, dan kesehatan [2].

Dalam konteks ini, penggunaan pendekatan keamanan tradisional seperti firewall statis terbukti tidak lagi memadai. Solusi tersebut bersifat reaktif dan lambat dalam merespon pola serangan baru. Oleh karena itu, teknologi Software-Defined Networking (SDN) hadir sebagai pendekatan baru yang memungkinkan pemisahan antara control plane dan data plane, memberikan fleksibilitas dan kemampuan pemrograman yang lebih baik dalam pengelolaan lalu lintas jaringan [3].

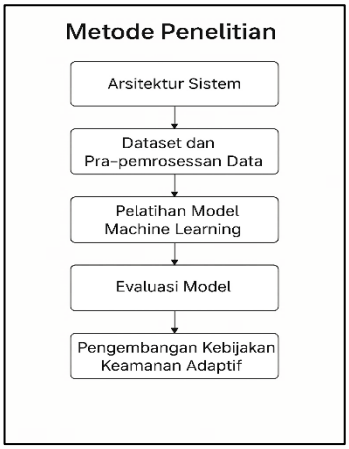
Salah satu inovasi yang berkembang pesat adalah integrasi firewall berbasis SDN dengan kecerdasan buatan, khususnya machine learning (ML). Pendekatan ini memungkinkan firewall untuk melakukan adaptasi secara dinamis terhadap serangan dengan mempelajari pola lalu lintas jaringan secara real-time. Penelitian oleh Zy et al. [4] menunjukkan bahwa firewall berbasis SDN yang diperkuat dengan teknik clustering K-Means dapat secara efektif mengelompokkan pola serangan berdasarkan lokasi geografis dan jenis protokol. Temuan ini menjadi dasar penting dalam pengembangan kebijakan keamanan yang lebih presisi dan kontekstual.

Lebih lanjut, Sharfaldin et al. [5], [6] menunjukkan efektivitas algoritma decision tree dalam mendeteksi serangan DDoS menggunakan dataset CIC-DDoS2019. Dengan tingkat akurasi mencapai 98,55% dan ROC-AUC sebesar 99,13%, studi tersebut memperkuat argumen bahwa integrasi pembelajaran mesin dapat meningkatkan keandalan sistem deteksi ancaman. Penelitian ini menekankan pentingnya eksplorasi fitur (EDA) dan pemilihan atribut yang relevan untuk membedakan lalu lintas normal dan serangan secara akurat.

Penelitian ini bertujuan untuk mengembangkan kebijakan keamanan adaptif berbasis machine learning, khususnya menggunakan algoritma Random Forest, pada arsitektur firewall SDN. Dengan memanfaatkan dataset CICIDS2017 dan teknik evaluasi seperti confusion matrix serta f1-score, model yang diusulkan bertujuan untuk memberikan respons yang cepat dan akurat terhadap serangan DDoS. Kontribusi utama dari penelitian ini adalah implementasi sistem deteksi ancaman adaptif yang dapat diintegrasikan ke dalam firewall SDN untuk meningkatkan ketahanan jaringan secara signifikan.

## 2. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen berbasis simulasi jaringan untuk mengembangkan dan menguji kebijakan keamanan adaptif pada firewall berbasis Software-Defined Networking (SDN). Algoritma *Random Forest* diterapkan untuk klasifikasi serangan DDoS, dengan menggunakan dataset CICIDS2017 [16]. Arsitektur sistem dirancang untuk mengadopsi alur deteksi otomatis, pelatihan model, dan pembaruan kebijakan keamanan secara dinamis berdasarkan hasil klasifikasi seperti yang di tunjukkan pada gambar 1.




Gambar 1. Metode Penelitian

### 2.1. Arsitektur Sistem

Arsitektur sistem terdiri atas tiga komponen utama:

a. **SDN Controller (Ryu)**: Mengelola pengaturan flow dan implementasi kebijakan firewall.
b. **IDS berbasis Machine Learning**: Modul ini bertanggung jawab untuk mendeteksi serangan menggunakan model Random Forest.
c. **Policy Updater**: Mengubah aturan firewall secara otomatis berdasarkan hasil klasifikasi.

Sistem ini berjalan dalam lingkungan simulasi menggunakan Mininet untuk menghasilkan lalu lintas jaringan dan mendeteksi serangan secara real-time.

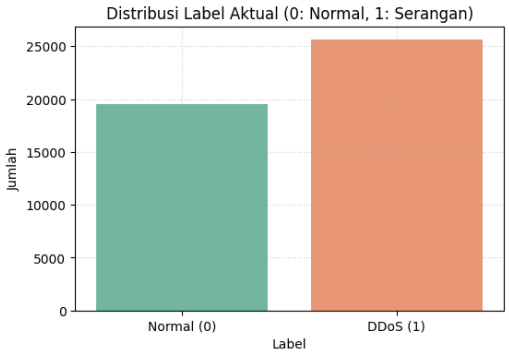
### 2.2. Dataset dan Pra-pemrosesan Data

Dataset yang digunakan adalah **CICIDS2017**, yang menyediakan berbagai jenis serangan, termasuk DDoS. Tahapan pra-pemrosesan meliputi:

a. Penghapusan nilai yang hilang dan duplikat.
b. *Feature selection* dengan korelasi dan penghapusan kolom non-informatif.

Submitted : 19-04-2025 | Reviewed : 20-04-2025 | Accepted : 30-04-2025

c. *Label encoding* terhadap nilai target (0 = Normal, 1 = DDoS).
d. Pembagian data dengan metode **stratified split** (80% pelatihan, 20% pengujian).




Gambar 2. Pembagian Dataset *stratified split* Normal dan Ddos.

### 2.3. Pelatihan Model Machine Learning

Model pelatihan menggunakan algoritma **Random Forest** dengan konfigurasi sebagai berikut:

a. Jumlah estimator: 100
b. *Criterion*: Gini Index
c. *Cross-validation*: 5-fold

Model dilatih untuk mengklasifikasikan lalu lintas sebagai normal atau serangan berdasarkan fitur jaringan.

### 2.4. Evaluasi Model

Evaluasi dilakukan dengan metrik:

Tabel 1. Ringkasan Evaluasi Performa Model Random Forest

| Jenis Evaluasi | Keterangan | Nilai |
|---|---|---|
| **Akurasi** | Tingkat prediksi benar total | 99.9978% |
| **Precision** | TP / (TP + FP) | 99.996% |
| **Recall** | TP / (TP + FN) | 99.996% |
| **F1-Score** | Harmonik precision & recall | 99.996% |
| **AUC Score** | Area under ROC curve | ± 0.999 |
| **Confusion Matrix** | TN = 19,543; TP = 25,604<br>FP = 1; FN = 1 | |

Dari hasil pengujian, model menunjukkan performa sangat tinggi dengan akurasi mencapai **99.9978%,** seperti yang ditunjukkan oleh confusion matrix.

### 2.5. Pengembangan Kebijakan Keamanan Adaptif

Setelah model berhasil mengklasifikasikan ancaman, hasil klasifikasi dikirim ke modul pengelola kebijakan untuk memperbarui aturan firewall SDN secara otomatis. Proses ini menggunakan API dari Ryu Controller untuk mengatur ulang flow table berdasarkan sumber dan jenis serangan.

## 3. Hasil dan Pembahasan

### 3.1. Hasil Evaluasi Model

Setelah proses pelatihan menggunakan algoritma Random Forest pada dataset CICIDS2017, model diuji menggunakan data uji yang telah dipisahkan secara stratified. Hasil evaluasi menunjukkan performa klasifikasi yang sangat tinggi:

a. **Akurasi**: 99.9978%
b. **Precision**: 99.996%
c. **Recall**: 99.996%
d. **F1-Score**: 99.996%

Evaluasi menggunakan confusion matrix menunjukkan hanya terdapat **2 kesalahan klasifikasi dari total 45.149 data uji**, dengan rincian:

a. True Negative (TN): 19.543
b. False Positive (FP): 1
c. False Negative (FN): 1
d. True Positive (TP): 25.604

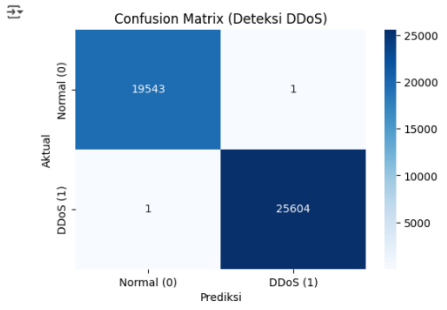
Temuan ini mengindikasikan bahwa model sangat andal dalam membedakan lalu lintas normal dan serangan DDoS.

Tabel 2. Hasil Evaluasi Model

| Jenis Evaluasi | Keterangan | Nilai |
|---|---|---|
| Akurasi | Tingkat prediksi benar total | 99.9978% |
| Precision | TP / (TP + FP) | 99.996% |
| Recall | TP / (TP + FN) | 99.996% |
| F1-Score | Harmonik precision & recall | 99.996% |
| AUC Score | Area under ROC curve | ± 0.999 |
| Confusion Matrix | TN = 19.543; TP = 25.604<br>FP = 1; FN = 1 | |

### 3.2. Visualisasi Hasil

a. **Confusion Matrix** untuk melihat distribusi klasifikasi.
b. **ROC Curve** dengan AUC mendekati 1, yang menunjukkan kemampuan model dalam membedakan kelas sangat baik.
c. **Bar chart jumlah serangan terdeteksi vs. aktual**.




Gambar 3. Visualisasi hasil

Submitted : 19-04-2025 | Reviewed : 20-04-2025 | Accepted : 30-04-2025

3.3. Pembahasan

Kinerja tinggi dari model Random Forest menunjukkan bahwa algoritma ini sangat cocok untuk lingkungan SDN karena:

a. Mampu mengolah fitur-fitur jaringan yang kompleks secara efisien.
b. Tahan terhadap overfitting berkat teknik ensemble.
c. Memberikan interpretasi penting melalui fitur terpenting (feature importance).

Model ini berhasil mendeteksi serangan DDoS secara **real-time** dan **akurat**, yang sangat penting untuk kebijakan firewall yang dinamis dalam arsitektur SDN. Dibandingkan penelitian sebelumnya seperti Zy et al. [6] yang menggunakan Decision Tree dan memperoleh akurasi 98.55%, model ini menunjukkan peningkatan signifikan.

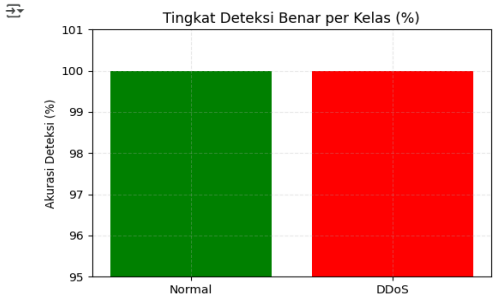
Kelebihan pendekatan ini:

a. Kemampuan adaptif terhadap jenis serangan baru.
b. Integrasi mudah dengan SDN Controller seperti Ryu.
c. Skalabilitas tinggi untuk lalu lintas besar.
d. Namun, terdapat beberapa keterbatasan:
e. Deteksi hanya difokuskan pada DDoS.
f. Belum diuji secara langsung pada lalu lintas jaringan real-time produksi.

3.4. Implikasi dan Rencana Pengembangan

Implikasi dari penelitian ini menunjukkan bahwa firewall SDN dapat ditingkatkan menjadi sistem yang **inteligensi adaptif**. Untuk pengembangan ke depan:

g. Implementasi pada lingkungan jaringan real-time
h. Perluasan deteksi ke jenis serangan lain seperti port scanning, brute-force, dan botnet
i. Integrasi sistem otomatisasi kebijakan keamanan (policy-as-code)




Gambar 4. Tingkat Deteksi Benar per Kelas

## 4. Kesimpulan

a. Penelitian ini berhasil mengembangkan kebijakan keamanan adaptif berbasis machine learning pada firewall Software-Defined Networking (SDN) dengan menggunakan algoritma Random Forest dan dataset CICIDS2017. Hasil pengujian menunjukkan performa deteksi yang sangat tinggi, dengan akurasi sebesar 99.9978%, serta precision, recall, dan f1-score masing-masing sebesar 99.996%. Evaluasi dengan confusion matrix menunjukkan bahwa sistem hanya melakukan dua kesalahan klasifikasi dari 45.149 sampel, menegaskan keandalan model dalam mendeteksi serangan DDoS.
b. Keunggulan utama dari pendekatan ini adalah kemampuannya dalam melakukan deteksi secara otomatis dan adaptif terhadap pola serangan, yang sangat relevan untuk arsitektur SDN yang dinamis. Dibandingkan dengan metode statis konvensional, sistem ini mampu merespons ancaman secara real-time dan memberikan dasar yang kuat untuk pengembangan kebijakan keamanan yang bersifat otonom.
c. Temuan ini menunjukkan bahwa integrasi machine learning ke dalam firewall SDN bukan hanya meningkatkan efektivitas deteksi ancaman, tetapi juga memungkinkan implementasi kebijakan keamanan yang cerdas dan efisien. Rencana pengembangan selanjutnya mencakup penerapan pada lalu lintas jaringan real-time dan perluasan cakupan sistem terhadap jenis serangan lain di luar DDoS.

## Daftar Rujukan

[1] T. Yuliswar, I. Elfitri, and O. W Purbo, “Optimization of Intrusion Detection System with Machine Learning for Detecting Distributed Attacks on Server,” *ISI*, vol. 10, no. 1, pp. 367–376, Feb. 2025, doi: 10.35314/vem9da98.
[2] Dr. A.Shaji George, Dr. T.Baskar, and Dr. P.Balaji Srikaanth, “Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors,” Feb. 2024, doi: 10.5281/ZENODO.10639463.
[3] E. Kaljic, A. Maric, P. Njemcevic, and M. Hadzialic, “A Survey on Data Plane Flexibility and Programmability in Software-Defined Networking,” *IEEE Access*, vol. 7, pp. 47804–47840, 2019, doi: 10.1109/ACCESS.2019.2910140.
[4] Ahmad Turmudi Zy, Isarianto, A. M. Rifa’i, A. Nugroho, and A. Ghofir, “Enhancing Network Security: Evaluating SDN-Enabled Firewall Solutions and Clustering Analysis Using K-Means through Data-Driven Insights,” *J. RESTI (Rekayasa Sist. Teknol. Inf.)*, vol. 9, no. 1, pp. 69–76, Jan. 2025, doi: 10.29207/resti.v9i1.6056.

Submitted : 19-04-2025 | Reviewed : 20-04-2025 | Accepted : 30-04-2025

[5] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization:," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, Funchal, Madeira, Portugal: SCITEPRESS - Science and Technology Publications, 2018, pp. 108–116. doi: 10.5220/0006639801080116.

[6] A. T. Zy, Amali, A. M. Rifa'i, A. Z. Kamalia, and A. A. Sulaeman, "Detecting DDoS Attacks Through Decision Tree Analysis: An EDA Approach with the CIC DDoS 2019 Dataset," in *2024 8th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, Yogyakarta, Indonesia: IEEE, Aug. 2024, pp. 202–207. doi: 10.1109/ICITISEE63424.2024.10730435.

[7] Ram Chandra Sachan, Rishit Lakhani, and Sanjay Poddar, "AI-enabled security mechanisms for WLANs: ensuring robust and adaptive protection in wireless networks," *World J. Adv. Res. Rev.*, vol. 25, no. 3, pp. 2085–2095, Mar. 2025, doi: 10.30574/wjarr.2025.25.3.0960.

[8] N. S. Musa, N. M. Mirza, S. H. Rafique, A. M. Abdallah, and T. Murugan, "Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks—Current Research Solutions," *IEEE Access*, vol. 12, pp. 17982–18011, 2024, doi: 10.1109/ACCESS.2024.3360868.

[9] Md. R. Ahmed, S. Islam, S. Shatabda, A. K. M. M. Islam, and Md. T. I. Robin, "Intrusion Detection System in Software-Defined Networks Using Machine Learning and Deep Learning Techniques –A Comprehensive Survey," Nov. 21, 2022. doi: 10.36227/techrxiv.17153213.v2.

[10] J. Faria, Y. Wang, and M. Lai, "Designing Network Security Tools for Home Users".

[11] M. Driss Laanaoui, M. Lachgar, H. Mohamed, H. Hamid, S. Gracia Villar, and I. Ashraf, "Enhancing Urban Traffic Management Through Real-Time Anomaly Detection and Load Balancing," *IEEE Access*, vol. 12, pp. 63683–63700, 2024, doi: 10.1109/ACCESS.2024.3393981.

[12] A. Aljuhani, "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," *IEEE Access*, vol. 9, pp. 42236–42264, 2021, doi: 10.1109/ACCESS.2021.3062909.

[13] T. E. Ali, Y.-W. Chong, and S. Manickam, "Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review," *Applied Sciences*, vol. 13, no. 5, p. 3183, Mar. 2023, doi: 10.3390/app13053183.

[14] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, p. 106984, Feb. 2020, doi: 10.1016/j.comnet.2019.106984.

[15] T. G. Nguyen, T. V. Phan, B. T. Nguyen, C. So-In, Z. A. Baig, and S. Sanguanpong, "SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks," *IEEE Access*, vol. 7, pp. 107678–107694, 2019, doi: 10.1109/ACCESS.2019.2932438.

[16] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection," *IEEE Access*, vol. 8, pp. 132911–132921, 2020, doi: 10.1109/ACCESS.2020.3009843.

---

Submitted : 19-04-2025 | Reviewed : 20-04-2025 | Accepted : 30-04-2025