

Daftar Pustaka

- Akiba, T., Sano, S., Yanase, T., Ohta, T., & Koyama, M. (2019). *Optuna: A Next-generation Hyperparameter Optimization Framework*.
<https://doi.org/10.1145/3292500.3330701>
- Alabdulatif, A., & Rizvi, S. (2023). Network intrusion detection system using an optimized machine learning algorithm. *Mehran University Research Journal of Engineering and Technology*, 42, 153.
<https://doi.org/10.22581/muet1982.2301.14>
- Alinda Rahmi, N., & Defit, S. (2024). *The Use of Hyperparameter Tuning in Model Classification: A Scientific Work Area Identification*.
<https://doi.org/10.62527/joiv.8.4.3092>
- Alnasser, O., Al Muhtadi, J., Saleem, K., & Shrestha, S. (2025). Signature and anomaly based intrusion detection system for secure IoTs and V2G communication. *Alexandria Engineering Journal*, 125, 424–440.
<https://doi.org/10.1016/j.aej.2025.03.068>
- Ananda Febian, F., Nur Alimyaningtias, W., & History, A. (2024). ANALISIS PERBANDINGAN TEKNIK SIGNATURE-BASED DAN ANOMALY-BASED DETECTION PADA SNORT DAN ZEEK DALAM MENCEGAH INTRUSI JARINGAN. *FORBIS: Forensics Business Information System Journal*, 2, 8–12. <https://journal.universitasmulia.ac.id/index.php/forbis>
- Bampoe, D. K. O. (2025). The Advantages of Hybrid Intrusion Detection Systems: A Comparative Study of Anomaly-Based and Signature-Based Approaches.

NRID - JOURNAL OF NOVEL RESEARCH AND INNOVATIVE DEVELOPMENT (www.JNRID.org), 3(1), a159–a162.

Cao, Y., Xiang, H., Zhang, H., Zhu, Y., & Ting, K. M. (2024). *Anomaly Detection Based on Isolation Mechanisms: A Survey*. <https://doi.org/10.1007/s11633-025-1554-4>

Chabchoub, Y., Togbe, M., Boly, A., & Chiky, R. (2022). An In-Depth Study and Improvement of Isolation Forest. *IEEE Access*, *PP*, 1. <https://doi.org/10.1109/ACCESS.2022.3144425>

Chiba, Z., Abghour, N., Moussaid, K., Omri, A., & Rida, M. (2019). *Newest collaborative and hybrid network intrusion detection framework based on suricata and isolation forest algorithm*. <https://doi.org/10.1145/3368756.3369061>

Díaz-Verdejo, J., Muñoz-Calle, J., Estepa Alonso, A., Estepa Alonso, R., & Madinabeitia, G. (2022). On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks. *Applied Sciences*, *12*(2). <https://doi.org/10.3390/app12020852>

Elmubarak, M., Karrar, A., & Hassan, N. (2019). Implementation Hybrid (NIDS) System using Anomaly Holtwinter Algorithm and Signature based Scheme. *International Journal of Advances in Scientific Research and Engineering*, *5*, 141–148. <https://doi.org/10.31695/IJASRE.2019.33278>

Ernawati, T., Fachrozi, F., & Syaputri, D. (2019). Analysis of Intrusion Detection System Performance for the Port Scan Attack Detector, Portsentry, and

- Suricata. *IOP Conference Series: Materials Science and Engineering*, 662, 052013. <https://doi.org/10.1088/1757-899X/662/5/052013>
- Ficke, E., Schweitzer, K. M., Bateman, R. M., & Xu, S. (2019). Analyzing Root Causes of Intrusion Detection False-Negatives: Methodology and Case Study. *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, 1–6. <https://doi.org/10.1109/MILCOM47813.2019.9020860>
- Fikri, F. F., Ardiansyah, F., Malays, E., & Sakti, S. (2024). Analisis Perbandingan Metode dan Performa Antara Suricata dan Snort. *TEKINFO*, 25(2), 63–72. <https://doi.org/10.37817/tekinfo.v25i2>
- Guide, R., Pauley, E., Beugin, Y., Sheatsley, R., & McDaniel, P. (2024). *Characterizing the Modification Space of Signature IDS Rules*. <https://doi.org/10.1109/MILCOM58377.2023.10356225>
- Kalavadekar, P., & Sane, D. (2019). Building an Effective Intrusion Detection System using combined Signature and Anomaly Detection Techniques. *International Journal of Innovative Technology and Exploring Engineering*, 8, 429–435. <https://doi.org/10.35940/ijitee.I8469.0881019>
- Lim, Y. (2022, Maret 31). *State-of-the-Art Machine Learning Hyperparameter Optimization with Optuna*. [towardsdatascience.com/](https://towardsdatascience.com/state-of-the-art-machine-learning-hyperparameter-optimization-with-optuna-a315d8564de1/). <https://towardsdatascience.com/state-of-the-art-machine-learning-hyperparameter-optimization-with-optuna-a315d8564de1/>

- Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. *Proceedings - IEEE International Conference on Data Mining, ICDM*, 413–422.
<https://doi.org/10.1109/ICDM.2008.17>
- Nawaal, B., Haider, U., Khan, I., & Fayaz, M. (2023). *Signature-Based Intrusion Detection System for IoT* (hlm. 141–158).
<https://doi.org/10.1201/9781003404361-8>
- Nurchahyo, J., & Sasongko, T. (2023). Hyperparameter Tuning Algoritma Supervised Learning untuk Klasifikasi Keluarga Penerima Bantuan Pangan Beras. *Indonesian Journal of Computer Science*, 12.
<https://doi.org/10.33022/ijcs.v12i3.3254>
- Nurhalizah, R. S., Ardianto, R., & Purwono, P. (2024). Analisis Supervised dan Unsupervised Learning pada Machine Learning: Systematic Literature Review. *Jurnal Ilmu Komputer dan Informatika*, 4(1), 61–72.
<https://doi.org/10.54082/jiki.168>
- Ogwara, N. O., Petrova, K., Yang, M. L. (Bobby), & MacDonell, S. G. (2025). MINDPRES: A Hybrid Prototype System for Comprehensive Data Protection in the User Layer of the Mobile Cloud. *Sensors*, 25(3).
<https://doi.org/10.3390/s25030670>
- Ouiazzane, S., Addou, M., & Barramou, F. (2022). *A Suricata and Machine Learning Based Hybrid Network Intrusion Detection System* (hlm. 474–485).
https://doi.org/10.1007/978-3-030-91738-8_43

- Pedregosa, F., Varoquaux, G., Gramfort, A., Michel V. and Thirion, B., Grisel, O., Blondel, M., Prettenhofer P. and Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, E. (2011). Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*, 12, 2825–2830.
- Pinontoan, P. Y., & Sembiring, I. (2022). IMPLEMENTASI DAN ANALISIS DETEKSI SERANGAN JARINGAN PADA WEB SERVER NFT MENGGUNAKAN SURICATA. *Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, 4(1), 65–78. <https://doi.org/10.53682/edutik.v4i1.9428>
- Purba, W., & Efendi, R. (2021). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI*, 17, 143–158. <https://doi.org/10.24246/aiti.v17i2.143-158>
- Rebala Gopinath, Ajay Ravi, & Churiwala Sanjay. (2019). Machine Learning Definition and Basics. Dalam *An Introduction to Machine Learning* (hlm. 1–17). Springer International Publishing. https://doi.org/10.1007/978-3-030-15729-6_1
- Soenen, J., Leuven, K., Wolputte, E. Van, Perini, L., Vercruyssen, V., Meert, W., Davis, J., & Blockeel, H. (2021). *The Effect of Hyperparameter Tuning on the Comparative Evaluation of Unsupervised Anomaly Detection Methods*. <https://api.semanticscholar.org/CorpusID:237108719>
- Sontan, A., & Samuel, S. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced*

Research and Reviews, 21, 1720–1736.
<https://doi.org/10.30574/wjarr.2024.21.2.0607>

Suci Sekar Sari, & Agus Tedyyana. (2024). Analisis Efektivitas Rule Snort dalam Mendeteksi Serangan Jaringan. *Repeater: Publikasi Teknik Informatika dan Jaringan*, 2(4), 01–15. <https://doi.org/10.62951/repeater.v2i4.194>

Tamara Saad Mohamed, & Saad Mohammed Khalifah. (2024). Intrusion Detection Systems: A Revisit of Performance Evaluation Parameters. *Academic International Journal of Engineering Science*, 2(01), 15–21.
<https://doi.org/10.59675/E212>

Tikaningsih, A., Lestari, P., Nurhopipah, A., Tahyudin, I., Winarto, E., & Hassa, N. (2024). Optuna Based Hyperparameter Tuning for Improving the Performance Prediction Mortality and Hospital Length of Stay for Stroke Patients. *Telematika*, 17(1), 1–16. <https://doi.org/10.35671/telematika.v17i1.2816>

Uddin, M. A., Aryal, S., Bouadjenek, M. R., Al-Hawawreh, M., & Talukder, M. A. (2024). usfAD based effective unknown attack detection focused IDS framework. *Scientific Reports*, 14(1). <https://doi.org/10.1038/s41598-024-80021-0>

Ulrich, A., Krňávek, J., Šenkeřík, R., Oplatková, Z. K., & Vala, R. (2025). *Isolation Forest in Novelty Detection Scenario*. <http://arxiv.org/abs/2505.08489>

Wolsing, K., Kus, D., Wagner, E., Pennekamp, J., Wehrle, K., & Henze, M. (2024). One IDS Is Not Enough! Exploring Ensemble Learning for Industrial Intrusion Detection. Dalam G. Tsudik, M. Conti, K. Liang, & G. Smaragdakis (Ed.),

Computer Security – ESORICS 2023 (hlm. 102–122). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-51476-0_6

Xu, Z., & Liu, Y. (2025). Robust Anomaly Detection in Network Traffic: Evaluating Machine Learning Models on CICIDS2017. *2025 10th International Conference on Electronic Technology and Information Science (ICETIS)*, 475–482. <https://doi.org/10.1109/ICETIS66286.2025.11144025>