Deteksi Serangan Ddos Pada Jaringan Internet of Things Menggunakan Deep Learning Sebagai Sistem
Deteksi Intrusi
Daley Devlin Nugraha, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR PUSTAKA

[1] Transforma Insights, "Current IoT Forecast Highlights (IoT Connections Forecast 2023–2034)," Transforma Insights, Aug. 2025. [Online]. Available: https://transformainsights.com/research/forecast/highlights. [Accessed: Jun. 13, 2026].

[2] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and Solutions Survey," Sensors, vol. 22, no. 19, Art. no. 7433, 2022, doi: 10.3390/s22197433.

[3] A. Kaur, C. R. Krishna, and N. V. Patil, "A comprehensive review on Software-Defined Networking (SDN) and DDoS attacks: Ecosystem, taxonomy, traffic engineering, challenges and research directions," Computer Science Review, vol. 55, Art. no. 100692, 2025, doi: 10.1016/j.cosrev.2024.100692.

[4] Z. Lv, L. Qiao, A. K. Singh, and Q. Wang, "AI-empowered IoT security for smart cities," ACM Transactions on Internet Technology, vol. 21, no. 4, pp. 1–21, 2021, doi: 10.1145/3406115.

[5] O. Yoachimik and J. Pacheco, "DDoS Threat Report for 2024 Q2," Cloudflare Blog, Jul. 2024. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-for-2024-q2. [Accessed: Jun. 13, 2026].

[6] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in Proc. IEEE Int. Carnahan Conf. Security Technology (ICCST), 2019, pp. 1–8, doi: 10.1109/CCST.2019.8888419.

[7] Z. Chen, J. Liu, Y. Shen, M. Simsek, B. Kantarci, H. T. Mouftah, and P. Djukic, "Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats," ACM Computing Surveys, vol. 55, no. 14s, pp. 1–37, 2023, doi: 10.1145/3530812.

[8] U. Ahmed et al., "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," Scientific Reports, vol. 15, no. 1, Art. no. 1726, 2025, doi: 10.1038/s41598-025-85866-7.

[9] M. K. U. Ahamed and A. Karim, "Cascaded intrusion detection system using machine learning," Systems and Soft Computing, vol. 7, Art. no. 200182, 2025, doi: 10.1016/j.sasc.2024.200182.

[10] H. C. Altunay and Z. Albayrak, "A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks," Engineering Science and Technology, an International Journal, vol. 38, Art. no. 101322, 2023, doi: 10.1016/j.jestch.2022.101322.

[11] S. Hizal, U. Cavusoglu, and D. Akgun, "A novel deep learning-based intrusion detection system for IoT DDoS security," Internet of Things, vol. 28, Art. no. 101336, 2024, doi: 10.1016/j.iot.2024.101336.

[12] [12] Y. Safitri, D. Dahlan, and M. M. J. Samodro, "Strategi dan Efektivitas Deep Learning untuk Mitigasi Ancaman Keamanan Jaringan di Era IoT," Scientific: Journal

UNIVERSITAS GADJAH MADA
Deteksi Serangan Ddos Pada Jaringan Internet of Things Menggunakan Deep Learning Sebagai Sistem Deteksi Intrusi
Daley Devlin Nugraha, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

of Computer Sciences and Informatics, vol. 2, no. 1, 2025, doi: 10.34304/scientific.v2i1.338.

[13] [13] S. Munawarah, Kurniabudi, and E. A. Winanto, "Deteksi Serangan DDoS SYN Flood Pada Jaringan Internet of Things (IoT) Menggunakan Metode Deep Neural Network (DNN)," Jurnal Informatika dan Rekayasa Komputer (JAKAKOM), vol. 4, no. 1, pp. 982–990, Apr. 2024, doi: 10.33998/jakakom.v4i1.

[14] [14] R. Baidar, S. Maric, and R. Abbas, "Hybrid Deep Learning-Federated Learning Powered Intrusion Detection System for IoT/5G Advanced Edge Computing Network," arXiv preprint, 2025. [Online]. Available: https://arxiv.org/abs/2509.15555.

[15] M. Nasereddin, M. Nakip, and E. Gelenbe, "Deep Learning Intrusion Detection and Mitigation of DoS Attacks," in Proc. 32nd Int. Conf. Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), 2024, doi: 10.1109/MASCOTS64422.2024.10786560.

[16] National Institute of Standards and Technology, "Internet of Things," NIST Computer Security Resource Center Glossary, 2026. [Online]. Available: https://csrc.nist.gov/glossary/term/internet_of_things. [Accessed: Jun. 13, 2026].

[17] Telkom University, "Apa itu Internet of Things? Pengertian, Cara Kerja, dan Contohnya," Telkom University, 2024. [Online]. Available: https://docif.telkomuniversity.ac.id/apa-itu-iot/. [Accessed: Jun. 13, 2026].

[18] K. Kim, I. M. Alshenaifi, S. Ramachandran, J. Kim, T. Zia, and A. Almorjan, "Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey," Sensors, vol. 23, no. 7, Art. no. 3681, 2023, doi: 10.3390/s23073681.

[19] E. Dritsas and M. Trigka, "A Survey on Cybersecurity in IoT," Future Internet, vol. 17, no. 1, Art. no. 30, 2025, doi: 10.3390/fi17010030.

[20] Kementerian Komunikasi dan Digital Republik Indonesia, "Komdigi Siapkan Pranata Humas Pemerintah Hadapi Era AI dan Big Data" Komdigi, 2026. [Online]. Available: https://www.komdigi.go.id/berita/berita-komdigi/detail/komdigi-siapkan-pranata-humas-pemerintah-hadapi-era-ai-dan-big-data. [Accessed: Jun. 13, 2026].

[21] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, "Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey," IEEE Access, vol. 12, pp. 25469–25490, 2024, doi: 10.1109/ACCESS.2024.3365634.

[22] A. Pakmehr, A. Aßmuth, N. Taheri, and A. Ghaffari, "DDoS attack detection techniques in IoT networks: A survey," Cluster Computing, vol. 27, no. 10, pp. 14637–14668, 2024, doi: 10.1007/s10586-024-04662-6.

[23] Cloudflare, "What is a DDoS attack?," Cloudflare Learning Center, 2026. [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [Accessed: Jun. 13, 2026].

[24] Telkom University Jakarta, "DDoS: Definisi, Contoh, Cara Kerja, serta Penanganan Serangan Siber," Telkom University Jakarta, 2024. [Online]. Available:

UNIVERSITAS GADJAH MADA
Deteksi Serangan Ddos Pada Jaringan Internet of Things Menggunakan Deep Learning Sebagai Sistem Deteksi Intrusi
Daley Devlin Nugraha, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

https://jakarta.telkomuniversity.ac.id/distributed-denial-of-service-ddos-definisi-contoh-cara-kerja-penanganan-serangan-siber/. [Accessed: Jun. 13, 2026].

[25] Q. A. Al-Haija and A. Droos, "A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT)," Expert Systems, vol. 42, no. 2, Art. no. e13726, 2025, doi: 10.1111/exsy.13726.

[26] T. Al-Shurbaji, M. Anbar, S. Manickam, I. H. Hasbullah, N. Alfriehat, B. A. Alabsi, A. R. Alzighaibi, and H. Hashim, "Deep Learning-Based Intrusion Detection System for Detecting IoT Botnet Attacks: A Review," IEEE Access, vol. 13, pp. 11792–11822, 2025, doi: 10.1109/ACCESS.2025.3526711.

[27] [27] Canadian Institute for Cybersecurity, University of New Brunswick, "DDoS evaluation dataset (CIC-DDoS2019)," 2026. [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html. [Accessed: Feb. 24, 2026].

[28] S. Satpathy, U. Tripathy, and P. K. Swain, "Cloud-based DDoS detection using hybrid feature selection with deep reinforcement learning (DRL)," Scientific Reports, vol. 15, Art. no. 36546, 2025, doi: 10.1038/s41598-025-18857-3.

[29] Digital Skola, "Data Preprocessing: Definisi, Tahapan, dan Implementasinya," Digital Skola Blog, Mar. 24, 2025. [Online]. Available: https://digitalskola.com/blog/data-science/data-preprocessing. [Accessed: Jul. 9, 2026].

[30] Digital Skola, "Feature Engineering: Definisi, Teknik, dan Praktik Baiknya," Digital Skola Blog, Mar. 24, 2025. [Online]. Available: https://digitalskola.com/blog/data-engineer/feature-engineering. [Accessed: Jul. 9, 2026].

[31] M. N. Puji, "Imbalanced Data – Data yang Tidak Seimbang pada Machine Learning," BINUS ASO School of Engineering (BASE), Oct. 7, 2024. [Online]. Available: https://base.binus.ac.id/automotive-robotics-engineering/2024/10/07/imbalanced-data-data-yang-tidak-seimbang-pada-machine-learning/ . [Accessed: Jul. 9, 2026]

[32] A. Awajan, "A Novel Deep Learning-Based Intrusion Detection System for IoT Networks," Computers, vol. 12, no. 2, Art. no. 34, 2023, doi: 10.3390/computers12020034.

[33] S. Yaras and M. Dener, "IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm," Electronics, vol. 13, no. 6, Art. no. 1053, 2024, doi: 10.3390/electronics13061053.

[34] K. Cho et al., "Learning phrase representations using RNN encoder-decoder for statistical machine translation," in Proc. Conf. Empirical Methods in Natural Language Processing (EMNLP), 2014, pp. 1724–1734.

[35] Y. Song, N. Luktarhan, Z. Shi, and H. Wu, "TGA: A Novel Network Intrusion Detection Method Based on TCN, BiGRU and Attention Mechanism," Electronics, vol. 12, no. 13, Art. no. 2849, 2023, doi: 10.3390/electronics12132849.

[36] S. Bai, J. Z. Kolter, and V. Koltun, "An empirical evaluation of generic convolutional and recurrent networks for sequence modeling," arXiv preprint, 2018. [Online]. Available: https://arxiv.org/abs/1803.01271.

[37] Scikit-learn Developers, "Confusion Matrix," Scikit-learn Documentation, 2026. [Online]. Available: https://scikit-

UNIVERSITAS GADJAH MADA
Deteksi Serangan Ddos Pada Jaringan Internet of Things Menggunakan Deep Learning Sebagai Sistem Deteksi Intrusi
Daley Devlin Nugraha, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

learn.org/stable/modules/generated/sklearn.metrics.confusion_matrix. [Accessed: Jun. 13, 2026].

[38] Scikit-learn Developers, "Metrics and Scoring: Quantifying the Quality of Predictions," Scikit-learn Documentation, 2026. [Online]. Available: https://scikit-learn.org/stable/modules/model_evaluation.html. [Accessed: Jun. 13, 2026].

[39] D. Chicco, N. Tötsch, and G. Jurman, "The Matthews correlation coefficient (MCC) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation," BioData Mining, vol. 14, no. 1, Art. no. 13, 2021, doi: 10.1186/s13040-021-00244-z.

[40] Scikit-learn Developers, "Validation Curves: Plotting Scores to Evaluate Models," Scikit-learn Documentation, 2026. [Online]. Available: https://scikit-learn.org/stable/modules/learning_curve.html. [Accessed: Jun. 13, 2026].

[41] Scikit-learn Developers, "Underfitting vs. Overfitting," Scikit-learn Documentation, 2026. [Online]. Available: https://scikit-learn.org/stable/auto_examples/model_selection/plot_underfitting_overfitting.html. [Accessed: Jun. 13, 2026].

[42] Telegram, "Telegram Bot API," Telegram Core Documentation, 2026. [Online]. Available: https://core.telegram.org/bots/api. [Accessed: Jun. 13, 2026].

[43] Telegram, "From BotFather to 'Hello World'," Telegram Core Documentation, 2026. [Online]. Available: https://core.telegram.org/bots/tutorial. [Accessed: Jun. 13, 2026].

[44] Telegram, "Telegram Web," Telegram, 2026. [Online]. Available: https://web.telegram.org/. [Accessed: Jun. 13, 2026].

[45] OWASP Foundation, "Secrets Management Cheat Sheet," OWASP Cheat Sheet Series, 2026. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Secrets_Management_Cheat_Sheet.html. [Accessed: Jun. 13, 2026].

[46] S. Berríos, S. Garcia, P. Hermosilla, and H. Allende-Cid, "A Machine-Learning-Based Approach for the Detection and Mitigation of Distributed Denial-of-Service Attacks in Internet of Things Environments," Applied Sciences, vol. 15, no. 11, Art. no. 6012, 2025, doi: 10.3390/app15116012.

[47] R. Gunawan, H. A. Ghani, N. Khamis, and H. F. Amran, "Imbalanced data handling in multiclass distributed denial of service attack detection using deep learning," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 22, no. 6, pp. 1396–1404, Dec. 2024, doi: 10.12928/TELKOMNIKA.v22i6.26005.

[48] Scikit-learn Developers, "Common pitfalls and recommended practices," Scikit-learn Documentation, 2026. [Online]. Available: https://scikit-learn.org/stable/common_pitfalls.html. [Accessed: Jun. 15, 2026].

[49] H. Zouhri, A. Idri, and A. Ratnani, "Evaluating the impact of filter-based feature selection in intrusion detection systems," International Journal of Information Security, vol. 23, pp. 759–785, 2024, doi: 10.1007/s10207-023-00767-y.

[50] Scikit-learn Developers, "RobustScaler," Scikit-learn Documentation, 2026. [Online]. Available: https://scikit-

UNIVERSITAS GADJAH MADA
Deteksi Serangan Ddos Pada Jaringan Internet of Things Menggunakan Deep Learning Sebagai Sistem Deteksi Intrusi
Daley Devlin Nugraha, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

learn.org/stable/modules/generated/sklearn.preprocessing.RobustScaler.html. [Accessed: Jun. 15, 2026].

[51] V. Shanmugam, R. Razavi-Far, and E. Hallaji, "Addressing Class Imbalance in Intrusion Detection: A Comprehensive Evaluation of Machine Learning Approaches," Electronics, vol. 14, no. 1, Art. no. 69, 2025, doi: 10.3390/electronics14010069.

[52] imbalanced-learn Developers, "SMOTEENN," imbalanced-learn Documentation, 2026. [Online]. Available: https://imbalanced-learn.org/stable/references/generated/imblearn.combine.SMOTEENN.html. [Accessed: Jun. 15, 2026].

[53] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002, doi: 10.1613/jair.953.

[54] Scikit-learn Developers, "compute_class_weight," Scikit-learn Documentation, 2026. [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.utils.class_weight.compute_class_weight.html. [Accessed: Jun. 15, 2026].

[55] N. Allassak, S. Trichni, and F. Omary, "Federated Intrusion Detection Using TabTransformer-TCN-BiGRU-Attention: A High-Accuracy Hybrid Deep Learning Approach," Engineering, Technology & Applied Science Research, vol. 15, no. 6, pp. 29647–29654, Dec. 2025, doi: 10.48084/etasr.13566.

[56] S. K. Balasubramanian and S. Perumal, "Comparative Study of BiGRU with Multi-Head Attention and CNN for Network Intrusion Detection Using a Cleaned and Balanced CSE-CIC-IDS 2018 Dataset," Turkish Journal of Engineering, vol. 9, no. 4, pp. 725–737, 2025, doi: 10.31127/tuje.1695208.

[57] J. Chung, C. Gulcehre, K. Cho, and Y. Bengio, "Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling," in Proc. NIPS Deep Learning Workshop, 2014. [Online]. Available: https://arxiv.org/abs/1412.3555.

[58] S. Cai, H. Xu, M. Liu, Z. Chen, and G. Zhang, "A malicious network traffic detection model based on bidirectional temporal convolutional network with multi-head self-attention mechanism," Computers & Security, vol. 136, Art. no. 103580, 2024, doi: 10.1016/j.cose.2023.103580.

[59] A. van den Oord et al., "WaveNet: A Generative Model for Raw Audio," arXiv preprint, 2016. [Online]. Available: https://arxiv.org/abs/1609.03499.

[60] M. Mulyanto, M. Faisal, S. W. Prakosa, and J.-S. Leu, "Effectiveness of Focal Loss for Minority Classification in Network Intrusion Detection Systems," Symmetry, vol. 13, no. 1, Art. no. 4, 2021, doi: 10.3390/sym13010004.

[61] D. P. Kingma and J. Ba, "Adam: A Method for Stochastic Optimization," in Proc. International Conference on Learning Representations (ICLR), 2015.

[62] Scikit-learn Developers, "f1_*score*," Scikit-learn Documentation, 2026. [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.metrics.f1_*score*.html. [Accessed: Jun. 15, 2026].

UNIVERSITAS
GADJAH MADA
**Deteksi Serangan Ddos Pada Jaringan Internet of Things Menggunakan Deep Learning Sebagai Sistem
Deteksi Intrusi**
Daley Devlin Nugraha, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

[63] Scikit-learn Developers, "matthews_corrcoef," Scikit-learn Documentation, 2026. [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.metrics.matthews_corrcoef.html. [Accessed: Jun. 15, 2026].

[64] K. M. Ting, "Confusion Matrix," in Encyclopedia of Machine Learning, Boston, MA, USA: Springer, 2011, doi: 10.1007/978-0-387-30164-8_157.

[65] TensorFlow Developers, "Save and load models," TensorFlow Core Documentation, 2026. [Online]. Available: https://www.tensorflow.org/tutorials/keras/save_and_load. [Accessed: Jun. 15, 2026].

[66] Joblib Developers, "Persistence," Joblib Documentation, 2026. [Online]. Available: https://joblib.readthedocs.io/en/stable/persistence.html. [Accessed: Jun. 15, 2026].

[67] python-telegram-bot Developers, "Bot," python-telegram-bot Documentation, 2026. [Online]. Available: https://docs.python-telegram-bot.org/en/stable/telegram.bot.html. [Accessed: Jun. 15, 2026].

[68] A. Hozouri, A. Mirzaei, and M. Effatparvar, "A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges," Discover Artificial Intelligence, vol. 5, Art. no. 314, 2025, doi: 10.1007/s44163-025-00578-1.

[69] A. Seifousadati, S. Ghasemshirazi, and M. Fathian, "A Machine Learning Approach for DDoS Detection on IoT Devices," arXiv preprint, 2021. [Online]. Available: https://arxiv.org/abs/2110.14911.

[70] T. Khempetch and P. Wuttidittachotti, "DDoS attack detection using deep learning," IAES International Journal of Artificial Intelligence, vol. 10, no. 2, pp. 382–388, 2021, doi: 10.11591/ijai.v10.i2.pp382-388.

[71] R. Nazre, R. Budke, O. Oak, S. Sawant, and A. Joshi, "A Temporal Convolutional Network-Based Approach for Network Intrusion Detection," in Proc. 2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS), 2024, pp. 1–6, doi: 10.1109/ICIICS63763.2024.10860234.

[72] A. Hekmati, N. Jethwa, E. Grippo, and B. Krishnamachari, "Correlation-Aware Neural Networks for DDoS Attack Detection in IoT Systems," arXiv preprint, 2023. [Online]. Available: https://arxiv.org/abs/2302.07982.