Jurnal Teknologi dan Sains Modern
E-ISSN: 3062-7966
DOI: https://doi.org/10.69930/jtsm.v2i2.348
Review Article

ScienceTech. Group

Vol. 2 (2), 2025
Hal. 89-96

Kecerdasan Buatan untuk Keberlanjutan: Menavigasi Aplikasi dan Tantangan Etis dalam Mengelola Lingkungan

Agus Salim Ramli [1], Syaiful Bachri M [2,*], Nurhikmah Fajar [1], Nurul Hidayatullah [3], Muhammad Atnang [2]

[1] Program Studi Teknik Komputer, Fakultas Teknik, Universitas Muhammadiyah Kolaka Utara, Indonesia
[2] Program studi Teknologi Informasi, Fakultas Sains Teknologi dan Kesehatan,Institut Sains Teknologi dan Kesehatan 'Aisyiyah Kendari, Indonesia
[3] Program Studi Fisika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Halu Oleo, Indonesia
*Email (corresponding author): syaifulbachrimustamin@gmail.com

Abstrak. *Kecerdasan Buatan (AI) berperan penting dalam mengatasi tantangan lingkungan melalui pemantauan iklim, optimasi sumber daya, dan konservasi alam. Studi ini menggunakan tinjauan sistematis terhadap lima sumber utama untuk mengeksplorasi penerapan AI, seperti analisis citra satelit, pembelajaran mesin, dan integrasi IoT. Hasil menunjukkan peningkatan akurasi prediksi iklim, efisiensi penggunaan air dan energi, serta konservasi keanekaragaman hayati. Namun, tantangan seperti konsumsi energi AI, isu etika, dan kesenjangan akses teknologi masih perlu diatasi. Kesimpulannya, AI memiliki potensi besar untuk mendukung keberlanjutan jika diimbangi dengan pendekatan etis dan kolaboratif.*

Kata kunci: *Kecerdasan buatan, keberlanjutan, mitigasi perubahan iklim, konservasi lingkungan, optimasi sumber daya.*

Abstract. *Artificial Intelligence (AI) plays an important role in addressing environmental challenges through climate monitoring, resource optimization, and nature conservation. This study uses a systematic review of five key sources to explore AI applications, such as satellite image analysis, machine learning, and IoT integration. Results show improvements in climate prediction accuracy, water and energy use efficiency, and biodiversity conservation. However, challenges such as AI energy consumption, ethical issues, and technology access gaps still need to be addressed. In conclusion, AI has great potential to support sustainability if balanced with ethical and collaborative approaches.*

Keywords: *Artificial intelligence, sustainability, climate change mitigation, environmental conservation, resource optimization*

1. Pendahuluan

Keamanan siber semakin menjadi prioritas utama di berbagai sektor, terutama dengan semakin terhubungnya teknologi. Infrastruktur kritis seperti sistem energi, perangkat *Internet of Things* (IoT), dan jaringan *Unmanned Aerial Vehicles* (UAV) menjadi sangat rentan terhadap serangan yang dapat menyebabkan kerugian besar (Yigit et al., 2024). Oleh karena itu, pengembangan sistem pertahanan yang efektif untuk melindungi data dan operasi sangat penting (Axon et al., 2022; Wang et al., 2023).

Studi (Hu et al., 2021) membahas mengenai tantangan keamanan siber pada sistem energi ditemukan dalam *Egyptian Informatics Journal*. Artikel ini membahas sistem energi dan

energy hubs yang terintegrasi dengan *Distributed Energy Resources* (DERs). Penelitian ini menyoroti dampak signifikan dari serangan siber, khususnya serangan *Distributed Denial of Service* (DDoS) dan *False Data Injection* (FDI), terhadap kestabilan sistem energi. Untuk mengatasi tantangan ini, sebuah kerangka kerja baru diperkenalkan untuk meningkatkan ketahanan *energy hubs* terhadap serangan siber, dengan memanfaatkan algoritma *machine learning* untuk mendeteksi dan mencegah serangan yang dapat mengganggu operasi ekonomi dan menyebabkan pemadaman listrik (Pazouki et al., 2021). Lain halnya dengan studi yang dilakukan oleh Zhukabayeva et al., yang diterbitkan dalam *Procedia Computer Science*, yang fokus pada ancaman botnet dalam *Wireless Sensor Networks* (WSNs). Dalam penelitian ini, penggunaan algoritma *Random Forest* dan XGBoost terbukti efektif dalam mendeteksi aktivitas botnet dengan akurasi yang sangat tinggi. Hasil dari penelitian ini menunjukkan potensi *machine learning* sebagai solusi yang kuat untuk mengidentifikasi ancaman botnet yang dapat merusak integritas dan keandalan sistem IoT (Faysal et al., 2022; Pazouki et al., 2021).

Sebuah artikel lain yang diterbitkan dalam *Procedia Computer Science* oleh Kikissagbe et al. juga membahas deteksi serangan *Denial of Service* (DoS) (Laiq et al., 2024; Ramesh et al., 2021) dalam sistem IoT. Studi ini menguji beberapa teknik machine learning, termasuk *Synthetic Minority Over-sampling Technique* (SMOTE) untuk penyeimbangan kelas dan *Deep Neural Networks* (DNN) untuk pemilihan fitur, guna meningkatkan akurasi dalam mendeteksi serangan. Kombinasi teknik-teknik ini menghasilkan performa terbaik dalam mendeteksi serangan DoS, yang dapat mengganggu layanan dan operasi dalam sistem IoT (Din et al., 2024).

Selain itu, dua jurnal dari *Results in Control and Optimization* membahas keamanan siber pada jaringan *Unmanned Aerial Vehicles* (UAV), dengan fokus pada deteksi serangan DoS (Coscia et al., 2024; Valikhanli, 2024a). Penelitian ini mengusulkan pendekatan berbasis *machine learning* dengan menggunakan *Decision Tree* (DT) untuk klasifikasi serangan. Metode yang diusulkan dalam kedua jurnal ini mencapai akurasi hingga 99,51% dalam mendeteksi serangan DoS dengan menggunakan dataset 5G-NIDD. Kedua jurnal ini juga menyoroti pentingnya penanganan ketidakseimbangan data serta pemilihan fitur yang relevan untuk meningkatkan kinerja model deteksi pada jaringan UAV(Valikhanli, 2024a).

Secara keseluruhan, berbagai studi yang dibahas dalam artikel ini menekankan peran penting *machine learning* dalam mengatasi berbagai ancaman siber pada sistem yang berbeda, seperti sistem energi, perangkat IoT, dan jaringan UAV. Setiap studi menunjukkan bagaimana pemilihan algoritma yang tepat, pengolahan data yang sesuai, dan evaluasi yang cermat dapat menghasilkan model yang efektif dalam mendeteksi dan mencegah serangan siber yang semakin canggih.

2. Metode

Dalam menyusun *literature review* ini, kami melakukan pencarian literatur yang sistematis dan seleksi artikel yang relevan mengenai penggunaan *machine learning* untuk deteksi dan pencegahan serangan siber di berbagai sistem, termasuk *energy hubs*, perangkat IoT, dan jaringan UAV (Valikhanli, 2024b). Pendekatan yang digunakan dalam proses ini adalah sebagai berikut:

2.1. Pencarian Literatur

Pencarian artikel dilakukan menggunakan database terkemuka seperti *Scopus, Google Scholar,* dan *IEEE Xplore*. Kata kunci yang digunakan mencakup "*cybersecurity*," "*machine learning*," "DDoS attack," "DoS attack," "IoT security," dan "UAV security." Kami juga mengadopsi kerangka kerja PRISMA untuk mengidentifikasi dan memilih artikel yang relevan (Achuthan et al., 2024; Tatiya et al., 2024).

2.2. Kriteria Inklusi dan Eksklusi

Artikel yang termasuk dalam studi literatur ini harus memenuhi kriteria berikut: (a) dipublikasikan dalam lima tahun terakhir, (b) fokus pada keamanan siber dengan menggunakan teknik machine learning, dan (c) relevansi dengan sistem energi, IoT, atau UAV. Artikel yang tidak relevan atau berfokus pada teknologi selain *machine learning* atau serangan siber dikecualikan (Naveeda & Fathima, 2024; Sun et al., 2024).

2.3. Analisis Literatur

Setelah artikel dipilih, kami menganalisis metodologi yang digunakan dalam setiap studi, termasuk jenis algoritma *machine learning* yang diterapkan, teknik pemrosesan data, serta matrik evaluasi yang digunakan untuk mengukur kinerja model (Ahmad & Alsmadi, 2021). Kami juga menilai kualitas setiap penelitian berdasarkan kriteria seperti jumlah data yang digunakan, metode validasi, dan ketepatan hasil.

2.4. Sintesis Temuan

Kami merangkum temuan-temuan utama dari setiap artikel yang dibahas, serta mengidentifikasi tren umum dan perbedaan dalam pendekatan yang diambil oleh masing-masing studi (Ayub et al., 2023). Temuan ini mencakup efektivitas berbagai algoritma *machine learning* dalam mendeteksi dan mencegah serangan siber, serta tantangan dan peluang yang ada dalam implementasi teknik-teknik ini dalam sistem yang berbeda (Qureshi et al., n.d.).

3. Hasil dan Pembahasan

Berbagai penelitian menunjukkan bahwa *machine learning* (ML) sangat efektif dalam mendeteksi dan mengatasi serangan siber di sistem energi, IoT, dan jaringan UAV. Pada *energy hubs*, serangan seperti *False Data Injection* (FDI) dan DDoS dapat meningkatkan biaya operasional secara signifikan, dan algoritma seperti *Decision Tree, Gradient Boosting*, dan SVM terbukti mampu mendeteksinya dengan baik. Dalam konteks IoT, algoritma *Random Forest* dan XGBoost berhasil mendeteksi serangan botnet dengan akurasi lebih dari 99%. Untuk deteksi serangan DoS, kombinasi teknik seperti SMOTE, pemilihan fitur dengan DNN dan PCA, serta klasifikasi dengan neural network memberikan hasil yang seimbang dan akurat. Penelitian pada jaringan UAV menekankan pentingnya efisiensi dan akurasi, dengan pendekatan seperti RFI dan *Decision Tree* yang mencapai akurasi hingga 99.51%. Semua studi ini menegaskan pentingnya pemilihan algoritma, pra-pemprosesan data, dan evaluasi model yang menyeluruh untuk menghadapi ancaman siber secara efektif.

Berikut adalah rangkuman umum dari penelitian masing-masing sumber, disajikan dalam bentuk tabel untuk memudahkan pemahaman, dengan sumber diganti dengan judul penelitian:

Tabel 1. Rangkuman dari beberapa penelitian

Judul Penelitian	Fokus Penelitian	Metode Utama	Hasil Utama
Cybersecurity of Energy hubs Based on IoT Devices Using Machine learning Algorithms (Sakr et al., 2024)	Keamanan siber *energy hubs* (EH) yang terintegrasi dengan *Distributed Energy Resources* (DERs), dengan fokus pada deteksi serangan DDoS melalui perangkat IoT.	Evaluasi berbagai algoritma *machine learning* yang diawasi seperti *Decision Tree* (DT), *Gaussian Process*, *Gradient Boosting*, *K-Nearest Neighbors* (KNN), *Support Vector Machine* (SVM), dan *Random Forest*. Simulasi serangan *False Data Injection* (FDI) juga dilakukan.	Perbandingan kinerja algoritma *machine learning* dalam memprediksi serangan DDoS, menunjukkan bahwa beberapa algoritma lebih efektif dalam kondisi tertentu. Serangan FDI berdampak signifikan pada operasi ekonomi dan pemadaman listrik.
Enhancing IoT Security: Effective Botnet Attack Detection Through Machine learning (Khaleefah & Al-Mashhadi, 2023)	Deteksi serangan *botnet* pada *Wireless Sensor Networks* (WSNs) menggunakan algoritma *machine learning*.	Implementasi dan perbandingan algoritma *Random Forest* dan *XGBoost* untuk mengidentifikasi aktivitas *botnet*. Strategi pencarian literatur menggunakan kerangka kerja PRISMA.	*Random Forest* dan XGBoost terbukti efektif dalam mendeteksi serangan *botnet* dengan akurasi tinggi, menunjukkan potensi *machine learning* sebagai alat pertahanan yang kuat di lingkungan IoT.
Machine learning for DoS Attack Detection in IoT Systems (Bajaj et al., 2023)	Peningkatan deteksi serangan *Denial of Service* (DoS) dalam sistem IoT dengan mengkombinasikan berbagai teknik *machine learning*.	Kombinasi teknik penyeimbangan kelas (SMOTE, *Random Undersampling*), pemilihan fitur (DNN, *Random Forest*, PCA), dan klasifikasi (SVM, DNN, XGBoost, *Random Forest*).	Kombinasi SMOTE + DNN + pengklasifikasi DNN memberikan kinerja terbaik dalam mendeteksi serangan DoS, dengan keseimbangan *precision*, *recall*, dan *F1-score* yang optimal.
A Machine Learning-Based Approach for Detection of DoS Attacks Targeting UAV Networks (dua jurnal dengan konten identik) (Alsumayt et al., 2024; Valikhanli, 2024c)	Deteksi serangan DoS pada jaringan *Unmanned Aerial Vehicles* (UAVs) atau drone menggunakan pendekatan berbasis *machine learning*.	Pemilihan fitur menggunakan uji chi-square (chi2), ANOVA F-value, dan *Random Forest Importance* (RFI), diikuti dengan pelatihan model *Decision Tree* (DT). Penambahan bobot kelas untuk mengatasi ketidakseimbangan data.	Kombinasi RFI + DT mencapai akurasi tinggi (99.51%) dalam mendeteksi serangan DoS pada jaringan UAV, dengan waktu pelatihan dan prediksi yang efisien.

Keamanan siber kini menjadi bagian integral dari berbagai sistem, mulai dari *energy hubs* (EH) hingga perangkat *Internet of Things* (IoT) dan jaringan Unmanned Aerial Vehicles (UAV). Keamanan tidak bisa lagi dipandang sebagai masalah terpisah; ia harus menjadi elemen yang menyatu dalam seluruh infrastruktur. Hal ini disebabkan oleh semakin kompleksnya sistem yang saling terhubung, di mana data mengalir antara berbagai platform,

yang meningkatkan potensi ancaman siber. Oleh karena itu, *machine learning* (ML) memiliki peran penting dalam mengatasi tantangan ini dengan membantu mengidentifikasi ancaman, mendeteksi pola serangan, dan merespons dengan cepat terhadap potensi risiko.

Walaupun karakteristik setiap sistem yang ditinjau, seperti sistem energi, IoT, dan jaringan UAV, berbeda, ketiganya rentan terhadap serangan yang serupa, seperti *Denial of Service* (DoS), *Distributed Denial of Service* (DDoS), dan *False Data Injection* (FDI) (Khedr et al., 2023). Dampak dari serangan ini dapat bervariasi tergantung pada sistem yang diserang. Misalnya, serangan DDoS pada *energy hubs* dapat mengganggu distribusi energi secara luas dan menyebabkan pemadaman listrik, sementara serangan DoS pada IoT mungkin hanya menonaktifkan sensor-sensor penting dalam jaringan tersebut. Berbagai dampak yang ditimbulkan menegaskan perlunya pendekatan keamanan yang komprehensif dan adaptif untuk melindungi semua jenis sistem ini. ML dapat membantu dengan memberikan deteksi serangan yang lebih cepat dan lebih efisien, baik itu dalam sistem energi, perangkat IoT, atau jaringan UAV (Dayarathne et al., 2025).

Dalam hal algoritma *machine learning* yang digunakan, penelitian menunjukkan bahwa berbagai algoritma memiliki kelebihan dan kekurangan masing-masing, tergantung pada jenis serangan dan sistem yang dianalisis. Misalnya, *Gradient Boosting* terbukti efektif dalam mendeteksi DDoS pada sistem energi berkat kemampuannya dalam menangani data besar dan dinamis. Untuk deteksi botnet di IoT, *Random Forest* dan *XGBoost* menunjukkan hasil yang baik dalam klasifikasi dan identifikasi serangan. Sedangkan *Deep Neural Networks* (DNN) memberikan hasil terbaik dalam deteksi serangan DoS pada sistem IoT, terutama ketika digabungkan dengan teknik penyeimbangan kelas seperti SMOTE. Untuk jaringan UAV, *Decision Tree* (DT) yang didukung dengan teknik *Random Forest Importance* (RFI) memberikan kinerja terbaik dalam deteksi serangan DoS. Masing-masing algoritma ini memiliki keunggulan tergantung pada karakteristik serangan dan sistem yang diamati.

Berdasarkan pada tabel 1 menjelaskan bahwa penelitian ini juga menekankan pentingnya pra-pemrosesan data untuk meningkatkan akurasi model ML. Teknik seperti feature selection dan class balancing sangat krusial untuk meningkatkan performa model. Misalnya, RFI digunakan untuk memilih fitur yang paling relevan dalam model, sementara SMOTE dan Random Undersampling membantu menyeimbangkan distribusi kelas dalam dataset. Selain itu, penggunaan matrik evaluasi yang lebih komprehensif, seperti precision, recall, dan F1-score, lebih disarankan dibandingkan hanya mengandalkan akurasi, terutama ketika dataset yang digunakan tidak seimbang. Ini penting untuk menghindari kesalahan pengukuran, terutama dalam mendeteksi serangan yang jarang terjadi.

Seiring berkembangnya ancaman siber yang semakin canggih, penting untuk memastikan bahwa model ML terus diperbarui dan diadaptasi agar tetap efektif dalam mendeteksi ancaman baru. Penyerang terus mengembangkan teknik-teknik baru untuk menghindari deteksi, sehingga model yang ada harus mampu beradaptasi dengan perubahan tersebut. Selain itu, banyak penelitian yang menggunakan dataset spesifik, yang mungkin tidak sepenuhnya mencerminkan kondisi dunia nyata. Oleh karena itu, perlu ada pengembangan model yang lebih umum yang dapat beradaptasi dengan berbagai jenis data dan skenario serangan yang lebih beragam. Pengembangan model yang mampu bekerja dalam kondisi dunia nyata, yang melibatkan berbagai jenis serangan dan data yang lebih kompleks, sangat penting untuk meningkatkan ketahanan sistem terhadap ancaman yang lebih kompleks.

Implementasi model ML dalam lingkungan yang memiliki keterbatasan sumber daya, seperti perangkat IoT dan UAV, juga menjadi tantangan tersendiri. Perangkat-perangkat ini seringkali memiliki kapasitas pemrosesan dan memori yang terbatas, yang membatasi kemampuan untuk menjalankan algoritma ML yang kompleks dalam waktu nyata. Oleh karena itu, penelitian lebih lanjut diperlukan untuk mengembangkan algoritma yang lebih efisien, yang dapat berjalan dalam lingkungan dengan sumber daya terbatas sambil tetap memberikan perlindungan yang efektif terhadap serangan siber. Fokus pada efisiensi pemrosesan dan pengurangan penggunaan sumber daya akan menjadi kunci untuk mengimplementasikan model ML yang dapat beroperasi dalam sistem nyata yang memiliki keterbatasan.

Secara keseluruhan, berbagai penelitian menunjukkan bahwa *machine learning* memiliki potensi besar dalam meningkatkan keamanan siber di berbagai sistem. Implementasi teknik-teknik ML yang tepat dapat memperkuat deteksi serangan dan mitigasi risiko pada sistem energi, perangkat IoT, dan UAV. Keberhasilan penggunaan ML dalam aplikasi ini sangat bergantung pada pemilihan algoritma yang sesuai, pengolahan data yang efektif, dan evaluasi yang cermat untuk memastikan model yang dihasilkan dapat diandalkan dalam mendeteksi dan mengatasi ancaman siber yang terus berkembang.

Kesimpulan

Berdasarkan penelitian-penelitian yang telah dijelaskan diatas bahwa studi ini menegaskan pentingnya peran *machine learning* (ML) dalam meningkatkan keamanan siber pada berbagai sistem, termasuk *energy hubs*, IoT, dan UAV. Berbagai penelitian menunjukkan bahwa algoritma seperti Gradient Boosting, SVM, XGBoost, *Random Forest*, dan *Deep Neural Network* (DNN) efektif dalam mendeteksi serangan seperti DDoS, DoS, dan botnet. Keberhasilan deteksi bergantung pada pemilihan algoritma yang sesuai, seleksi fitur yang tepat, dan penyeimbangan data. Evaluasi model tidak hanya didasarkan pada akurasi, tetapi juga pada metrik precision, recall, dan F1-score. Penelitian juga menyoroti pentingnya pendekatan keamanan yang adaptif serta perlunya riset lanjutan untuk menghadapi ancaman siber yang terus berkembang.

Ucapan Terima Kasih

Kami mengucapkan terima kasih yang mendalam kepada semua pihak yang telah memberikan dukungan dalam penelitian ini. Secara khusus, kami sangat menghargai kontribusi para penulis dan peneliti yang telah menyediakan literatur yang sangat berguna dalam menyusun dasar penelitian ini. Kami juga mengucapkan terima kasih kepada pihak-pihak yang memberikan bantuan administratif dan teknis yang sangat berarti selama proses penelitian.

Daftar Pustaka

Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. *Frontiers in Big Data*, *7*. https://doi.org/10.3389/FDATA.2024.1497535

Ahmad, R., & Alsmadi, I. (2021). *Machine learning* approaches to IoT security: A systematic literature review. *Internet Things*, *14*. https://doi.org/10.1016/J.IOT.2021.100365

Alsumayt, A., Nagy, N., Alsharyofi, S., Al Ibrahim, N., Al-Rabie, R., Alahmadi, R., Alesse, R. A., & Alahmadi, A. A. (2024). *Detecting Denial of Service Attacks (DoS) over the Internet of Drones (IoD) Based on Machine Learning*. *Sci*, *6*(3). https://doi.org/10.3390/SCI6030056

Axon, L., Fletcher, K., Scott, A. S., Stolz, M., Hannigan, R., Kaafarani, A. El, Goldsmith, M., & Creese, S. (2022). Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda. *Digital Threats: Research and Practice*, *3*(4), 1–27. https://doi.org/10.1145/3503920

Ayub, M., Lajam, O., Alnajim, A., & Niazi, M. (2023). Use of *Machine learning* for Web Denial-of-Service Attacks: A Multivocal Literature Review. *Arabian Journal for Science and Engineering*, *48*(8), 9559–9574. https://doi.org/10.1007/S13369-022-07517-7

Bajaj, P., Mishra, S., & Paul, A. (2023). Comparative Analysis of Stack-Ensemble-Based Intrusion Detection System for Single-Layer and Cross-layer DoS Attack Detection in IoT. *SN Computer Science*, *4*(5), 1–11. https://doi.org/10.1007/S42979-023-02105-4

Coscia, A., Dentamaro, V., Galantucci, S., Maci, A., & Pirlo, G. (2024). Automatic decision tree-based NIDPS ruleset generation for DoS/DDoS attacks. *J. Inf. Secur. Appl.*, *82*. https://doi.org/10.1016/J.JISA.2024.103736

Dayarathne, M. A. S. P., Jayathilaka, M. S. M., Bandara, R. M. V. A., Logeeshan, V., Kumarawadu, S., & Wanigasekara, C. (2025). Mitigating Cyber Risks in Smart Cyber-Physical Power Systems Through Deep Learning and Hybrid Security Models. *IEEE Access*, *13*, 37474–37492. https://doi.org/10.1109/ACCESS.2025.3545637

din, S. M. ud, Sharma, R., Rizvi, F., & Sharma, N. (2024). Detection of botnet in IoT network through *machine learning* based optimized feature importance via ensemble models. *International Journal of Information Technology*, *16*(2), 1–9. https://doi.org/10.1007/S41870-023-01603-1

Faysal, J. Al, Mostafa, S. T., Tamanna, J. S., Mumenin, K. M., Arifin, M. M., Awal, M. A., Shome, A., & Mostafa, S. S. (2022). XGB-RF: A Hybrid *Machine learning* Approach for IoT Intrusion Detection. *Telecom*, *3*(1), 52–69. https://doi.org/10.3390/TELECOM3010003

Hu, J., Liu, X., Shahidehpour, M., & Xia, S. (2021). *Optimal Operation of Energy hubs With Large-Scale Distributed Energy Resources for Distribution Network Congestion Management*. *IEEE Transactions on Sustainable Energy*, *12*(3), 1755–1765. https://doi.org/10.1109/TSTE.2021.3064375

Khaleefah, A. D., & Al-Mashhadi, H. M. (2023). Detection of IoT Botnet Cyber Attacks using Machine Learning. *Informatica (Slovenia)*, *47*(6), 55–64. https://doi.org/10.31449/INF.V47I6.4668

Khedr, W. I., Gouda, A. E., & Mohamed, E. R. (2023). FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using *Machine learning* for Stateful SDN-Based IoT Networks. *IEEE Access*, *11*, 28934–28954. https://doi.org/10.1109/ACCESS.2023.3260256

Laiq, F., Al-Obeidat, F. N., Amin, A., & Moreira, F. (2024). DDoS Attack Detection in Edge-IIoT Network Using Ensemble Learning. *Journal of Physics: Complexity*. https://doi.org/10.1088/2632-072X/AD506B

Naveeda, K., & Fathima, S. M. H. S. S. (2024). Real-time implementation of IoT-enabled cyberattack detection system in advanced metering infrastructure using *machine learning* technique. *Electrical Engineering*. https://doi.org/10.1007/S00202-024-02552-Z

Pazouki, S., Naderi, E., & Asrari, A. (2021). A remedial action framework against cyberattacks targeting *energy hubs* integrated with distributed energy resources. *Applied Energy*, *304*. https://doi.org/10.1016/J.APENERGY.2021.117895

Qureshi, S. U., He, J., Tunio, S., Zhu, N., Nazir, A., Wajahat, A., Ullah, F., & Wadud, A. (n.d.). Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. *J. King Saud Univ. Comput. Inf. Sci.*, *36*. https://doi.org/10.1016/J.JKSUCI.2024.102164

Ramesh, S., Yaashuwanth, C., Prathibanandhi, K., Basha, A. R., & Jayasankar, T. (2021). An optimized deep neural network based DoS attack detection in wireless video sensor network. *Journal of Ambient Intelligence and Humanized Computing*, 1–14. https://doi.org/10.1007/S12652-020-02763-9

Sakr, H. A., Fouda, M. M., Ashour, A. F., Abdelhafeez, A., El-Afifi, M. I., & Refaat Abdellah, M. (2024). Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems. *Egyptian Informatics Journal*, *28*. https://doi.org/10.1016/J.EIJ.2024.100540

Sun, C., Fontanesi, G., Canberk, B., Mohajerzadeh, A., Chatzinotas, S., Grace, D., & Ahmadi, H. (2024). Advancing UAV Communications: A Comprehensive Survey of Cutting-Edge *Machine learning* Techniques. *IEEE Open Journal of Vehicular Technology*, *5*, 825–854. https://doi.org/10.1109/OJVT.2024.3401024

Tatiya, Dr. M., Verma, Dr. A., Talekar, Dr. S., Kumar, S., Kiran, Dr. V., Bhosale, & Kumar, S. (2024). Cybersecurity in IoT-Based Smart Grids: A Comprehensive Survey. *Computer Fraud and Security*, 73–81. https://doi.org/10.52710/CFS.51

Valikhanli, O. (2024a). UAV networks DoS attacks detection using artificial intelligence based on weighted machine learning. *Results in Control and Optimization*, *16*. https://doi.org/10.1016/J.RICO.2024.100457

Wang, Z., Li, Y., Wu, S., Zhou, Y., Yang, L., Xu, Y., Zhang, T., & Pan, Q. (2023). A survey on cybersecurity attacks and defenses for unmanned aerial systems. *J. Syst. Archit.*, *138*.

Yigit, Y., Ferrag, M., Ghanem, M. C., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., Tihanyi, N., & Janicke, H. (2024). Generative AI and LLMs for Critical Infrastructure Protection: Evaluation Benchmarks, Agentic AI, Challenges, and Opportunities. *Sensors*. https://doi.org/10.3390/S25061666