Efektivitas Algoritma *Artificial Intelligence* dalam Melawan Serangan *Zero-Day*

Fadhil Raihan[1], Ramadhan Renaldy [2]
[1,2] Program Studi Informatika, Universitas PGRI Semarang, Semarang

Email: [1]reyhanfadil555@gmail.com, [2]ramadhanrenaldy@upgris.ac.id.

Abstract

Zero-day attacks pose a significant threat to cybersecurity because they are difficult to detect and prevent using conventional techniques, and various methods have been applied. This article aims to determine the effectiveness of artificial intelligence (AI) algorithms in handling zero-day attacks using machine learning and deep learning. The methods used include literature review and empirical data analysis from case studies. The research results from 30 journals indicate that AI algorithms have high potential in detecting zero-day attacks with Convolutional Neural Networks (CNN***)*** method appearing in 30% of the articles. CNN excels with an AUC-ROC value of 0.96, outperforming Random Forest and RNN, each having an AUC-ROC value of 0.95. The main challenges faced are limited training and validation data as well as overfitting issues. In conclusion, AI shows great potential in cybersecurity, although further development is needed to address existing challenges. This research demonstrates that AI can be a more efficient and flexible solution in protecting our digital world.

Keywords: Zero-day, Algoritma, Artificial Intelligence, Cyber Security, Systematic Literatur Review

Abstrak

Serangan zero-day adalah ancaman besar bagi keamanan siber, karena sulit dideteksi dan dicegah dengan teknik konvesional dan berbagai metode telah diterapkan. Artikel ini bertujuan untuk mengetahui seberapa efektif algortima kecerdasan buatan (AI) dalam menangani serangan zero-day dengan menggunakan pembelajaran mesin dan pembelajaran mendalam. Metode yang digunakan termasuk tinjauan literatur dan analisis data empiris dari studi kasus. Hasil review saya dari 30 jurnal menunjukkan bahwa algoritma AI memiliki potensi tinggi dalam mendeteksi serangan zero-day dengan metode *Convolutional Neural Networks (CNN)* yang muncul dalam 30% dari artikel. *CNN* unggul dengan nilai AUC-ROC 0.96, mengalahkan *Random Forest* dan *RNN* yang masing-masing memiliki nilai AUC-ROC 0.95. Tantangan utama yang dihadapi adalah keterbatasan data pelatihan dan validasi serta masalah overfitting. Kesimpulannya, AI menunjukkan potensi besar dalam keamanan siber, meskipun perlu pengembangan lebih lanjut untuk mengatasi tantangan yang ada. Review ini memperlihatkan bahwa AI dapat menjadi solusi yang lebih efisien dan fleksibel dalam melindungi dunia digital kita.

Kata Kunci: Zero-day, Algoritma, Artificial Intelligence, Cyber Security, Systematic Literatur Review

1. Pendahuluan

Zero-day merupakan salah satu ancaman besar bagi keamanan siber karena, sifat serangan yang sulit dideteksi dan dicegah menggunakan teknik kovensional. Zero-day juga dapat mengeksploitasi kerentanan perangkat lunak yang belum diketahui oleh publik atau vendor perangkat lunak. Berbagai metode telah diimplementasikan untuk menangani ancaman ini, namun efektivitasnya masih menjadi perdebatan. Penilitian ini bertujuan untuk mengetahui dan mengevaluasi seberanpa efektif algoritma kecerdasan buatan (AI) berhasil menangani dan mendektesi serangan zero-day dengan menggunakan teknik pembelajaran

mesin dan pembelajaran mendalam. Review ini mengkaji kemampuan algoritma kecerdasan buatan untuk mendeteksi dan mencegah serangan zero-day [1], [2] .

Review ini bertujuan untuk memahami seberapa baik AI dapat mengidentifikasi ancaman yang belum diketahui sebelumnya. Artikel ini juga membahas masalah yang harus diatasi saat menggunakan kecerdasan buatan untuk mendeteksi serangan zero-day, seperti masalah *false positives* dan adaptasi algoritma yang terbatas. Review ini menggunakan algoritma AI, terutama pembelajaran mesin dan pembelajaran mendalam. Algoritma ini dapat mendeteksi pola anomali dalam lalu lintas jaringan atau sistem yang menunjukkan serangan zero-day. *neural networks*, *clustering*, dan pengklasifikasi yang dioptimalkan adalah teknik yang sering digunakan untuk mendeteksi anomali ini [3], [4], [5]

Metode apa saja yang paling sering digunakan untuk mendeteksi serangan zero-day dengan menggunakan kecerdasan buatan. Dari tinjauan literatur menunjukkan bahwa *Convolutional Neural Networks (CNN)* [6], [7], [8], [9], [10], *Gradient Boosting* [11], *Random Forest* [12], [13], [14], [15], *Support Vector Machine (SVM)* [16], [17], [18], dan *Recurrent Neural Networks (RNN)* [19], [20] adalah metode yang paling sering digunakan, dengan fokus pada pembuatan model yang dapat mengenali pola anomali yang menunjukkan adanya serangan zero-day [21]

Bagaimana keefektivitas dan keefisiensinya metode ini didalam dunia nyata, metode ini telah banyak diimplementasikan dalam berbagai studi kasus. Review ini juga mengkaji bagaimana metode-metode AI ini diimplementasikan dalam berbagai studi kasus. Analisis dilakukan terhadap artikel-artikel yang telah menerapkan model-model AI tersebut untuk memahami pendekatan dan teknik yang digunakan dalam mendeteksi serangan zero-day. Sepeti *CNN* digunakan dalam berbagai aplikasi, termasuk deteksi *phishing URL* dan *botnet attack detection*, *Gradient Boosting* sering diterapkan dalam sistem hybrid untuk meningkatkan akurasi deteksi, *Random Forest* digunakan dalam studi yang memfokuskan pada *malware detection* dan *routing protocols*, *SVM* diterapkan dalam review yang mengeksplorasi deteksi serangan berbasis *machine learning*, dan *RNN* digunakan dalam studi yang menerapkan *meta-learning* untuk deteksi serangan web [6], [22]

Review Studi kasus menunjukkan bahwa implementasi algoritma AI penggunaan algoritma kecerdasan buatan untuk deteksi serangan zero-day membutuhkan pengumpulan data, pelatihan model, dan evaluasi model terhadap serangan nyata. Beberapa studi juga mengkaji bagaimana memasukkan algoritma ini ke dalam sistem keamanan siber yang sudah ada untuk meningkatkan deteksi. Dalam penggunaan AI untuk mendeteksi serangan zero-day, ada masalah seperti mengatasi *false positives*, meningkatkan interpretabilitas model, dan memastikan adaptabilitas model terhadap jenis serangan baru. Selain itu, perlu memastikan bahwa model AI dapat berfungsi dalam lingkungan yang dinamis dan berkembang biak. Review ini juga mengeksplorasi tantangan yang dihadapi dalam implementasi metode AI, serta keterbatasan yang perlu diatasi untuk meningkatkan efektivitas deteksi serangan zero-day.

Tantangan utama dalam penggunaan AI untuk deteksi serangan zero-day yaitu Ketersediaan Data, data ini digunakan untuk melatih model yang seringkali terbatas dan tidak selalu representatif. Kompleksitas Serangan, Serangan zero-day yang semakin hari semakin kompleks yang mengharuskan model AI yang lebih canggih dan adaptif. Overfitting Risiko, overfitting diperlukan dalam model pembelajaran mendalam yang memerlukan strategi regulasi yang tepat. Sumber Daya Komputasi, Implementasi model AI yang kompleks memerlukan sumber daya komputasi yang besar agar bisa optimal dalam mendekteksi dan mengatasi serangan [1], [23]

Oleh karena itu Systematic literatur Review (SLR) ini bertujuan untuk mengidentifikasi metode AI yang paling sering digunakan dalam mendeteksi serangan zero-day dan mengevaluasi keefektivitas metode AI ini dalam penerapan dunia nyata serta mengidentifikasi tantangan utama yang dihadapi dalam penerapan AI untuk mendeteksi serangan zero-day. Dengan mengkaji pendekatan dan teknik yang digunakan dalam berbagai studi kasus dari 30 jurnal untuk implementasi AI dalam mendeteksi serangan zero-day. Mencari solusi yang dapat diadopsi untuk mengatasi tantangan yang dihadapi dalam implementasi metode AI tersebut

2. Metode

Review ini mengikuti metodologi Systematic Literature Review (SLR) yang melibatkan tiga tahap utama seperti perencanaan *(planning)*, pelaksanaan *(conduction)*, dan pelaporan *(reporting)*. Berikut ini adalah rincian dari setiap tahap tersebut

1) Perencanaan (Planning)

Penentuan tema merupakan langkah awal untuk memulai SLR. Langkah awal dalam review ini adalah menentukan tema yang akan dijadikan fokus dalam Systematic Literature Review (SLR). Tema yang dipilih adalah **"Model AI untuk Deteksi Serangan Zero-Day"**. Dengan tema ini, penentuan *Research Question* (RQ) menjadi lebih terarah. Suatu RQ dapat dianggap baik apabila bermanfaat, dapat diukur, arahnya sesuai tema atau topik yang telah ditentukan diawal.Langkah berikutnya penulis memilih lima penerbit untuk menjadi sumber dalam mencari jurnal yaitu IEEE (10), Science Direct (10), Sensors (3), dan ACM (7) Jurnal yang dipilih berjumlah 30 jurnal.

2) Conduction

Tahap ini dimulai dengan menentukan keyword yang akan digunakan dalam pencarian jurnal, serta sinonim kata yang relevan untuk meningkatkan akurasi pencarian. Beberapa keyword yang digunakan adalah *"zero-day attack detection", "AI in cybersecurity", "machine* learning *for zero-day attacks", dan "deep learning in cybersecurity"*

Dari 30 jurnal yang ditemukan, jurnal-jurnal tersebut diseleksi berdasarkan kesesuaian dengan Research Question. Kriteria seleksi dibuat untuk mempermudah proses pemilihan jurnal, sehingga diperoleh 20 jurnal yang akan ditinjau lebih lanjut. Kriteria seleksi berdasarkan RQ adalah:

Tabel 1 Researxh Question

ID	Research Question	Tujuan
RQ1	Identifikasi Metode AI yang Digunakan:	Mengidentifikasi metode AI yang sering digunakan untuk mendeteksi serangan zero-day.
RQ2	Evaluasi Implementasi Metode AI	Mengevaluasi bagaimana metode AI diimplementasikan dalam deteksi serangan zero-day, termasuk efektivitas dan efisiensinya
RQ3	Tantangan dalam Penerapan AI	Mengidentifikasi tantangan utama yang dihadapi dalam penerapan AI untuk keamanan siber, khususnya dalam deteksi serangan zero-day

Dari data tabel di atas dapat kita ketahui. Tujuan dari penilitian ini untuk mengetahui Metode apa saja yang digunakan untuk mendektesi zero-day, Menguji kefisiensiannya dan mengtehaui tantangan apa yang ada dalam penerapan AI dalam mengatasi serangan Zero-day. RQ yang baik harus bermanfaat, dapat diukur, dan sesuai dengan tema yang telah ditentukan.

Pencarian Literatur Menggunakan Beberapa Sumber seperti, IEEE Xplore (10), ACM Digital Library(7), ScienceDirect(10), Sensors(3). Dengan Melakukan pencarian yang menggunakan kata kunci telah ditentukan dan menyaring hasil berdasarkan kriteria inklusi dan eksklusi. Kata kunci yang digunakan mencakup kombinasi dari istilah-istilah berikut: *"zero-day attack detection", "artificial intelligence", "machine learning", "deep learning", "cybersecurity".*

3) Pelaporan (Reporting)

Tahap terakhir dalam melakukan SLR adalah reporting atau pelaporan. Dalam tahap ini penulis mulai membuat laporan yang berisi pendahuluan, landasan teori, metode review, hasil dan pembahasan serta kesimpulan. Selain itu, laporan juga dilengkapi dengan abstrak pada awal laporan.

Bagian abstrak berisi review dari laporan SLR yang telah dibuat. Abstrak berfungsi agar pembaca dapat mengetahui isi laporan secara singkat. Maka dari itu, abstrak harus sesuai dengan isi laporan serta menggunakan bahasa yang mudah dipahami dan

singkat.Pendahuluan akan berisi tentang filosofi dari tema yang telah ditentukan, filosofi dapat berupa sejarah dari tema yang diangkat. Selain itu, pendahuluan berisi alasan mengapa penulis memilih untuk mengangkat tema yang sebelumnya telah dipilih.

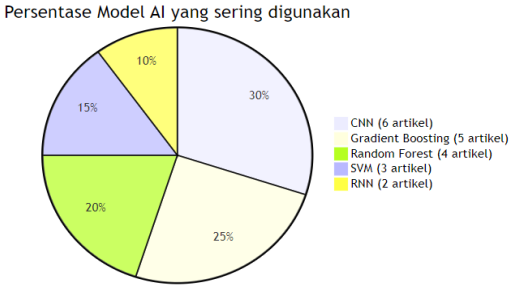
Landasan Teori membahas tentang definisi, konsep maupun algoritma yang berhubungan dengan tema yang telah ditentukan. Sedangkan Metode review membahas tentang bagaimana langkah-langkah dari SLR yang dilakukan oleh penulis. Langkah yang dilakukan mulai menyusun tema, mencari jurnal, menentukan RQ, dan melakukan review terhadap jurnal yang ada sesuai dengan RQ yang ditentukan.

Untuk Hasil dan Pembahasan akan berisi tentang hasil dari jurnal yang telah didapatkan dan dilakukan filter. Pada hasil dan pembahasan juga akan dipaparkan bagaimana jawaban yang didapatkan dari jurnal terhadap RQ yang telah ditentukan.

Bagian terakhir adalah kesimpulan yang merupakan penutup laporan. Kesimpulan akan berisi rangkuman dari SLR yang telah dilakukan oleh penulis sesuai dengan RQ yang telah ditentukan sebelumnya. Rangkuman dalam kesimpulan berupa hasil presentase tertinggi dari masing- masing RQ

3. Hasil dan Pembahasan

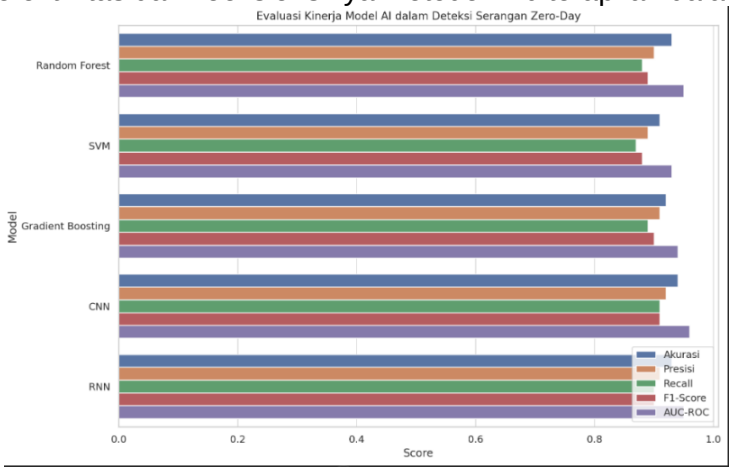
RQ1 (Metode apa saja yang paling sering digunakan untuk mendeteksi serangan zero-day dengan menggunakan kecerdasan buatan?)



Gambar 3 1 Grafik Metode AI yang sering digunakan

Hasil analisis data ini menunjukkan bahwa *CNN* 30% [6], [7], [8], [9], [10] dan *Gradient Boosting* 25% [24], [25], [26], [27]. adalah model yang paling populer dalam deteksi serangan zero-day. Hal ini dapat dijelaskan oleh kemampuan *CNN* dalam menangani data yang kompleks dan berstruktur, serta kemampuan *Gradient Boosting* dalam melakukan penguatan iteratif yang menghasilkan model prediktif yang kuat. Namun, penting untuk dicatat bahwa setiap model memiliki kelebihan dan kekurangan masing-masing yang mempengaruhi pilihan model berdasarkan kebutuhan spesifik dari aplikasi yang digunakan.

RQ2 (Bagaimana keefektivitas dan keefisiensinya metode ini diterapkan dalam dunia nyata?)



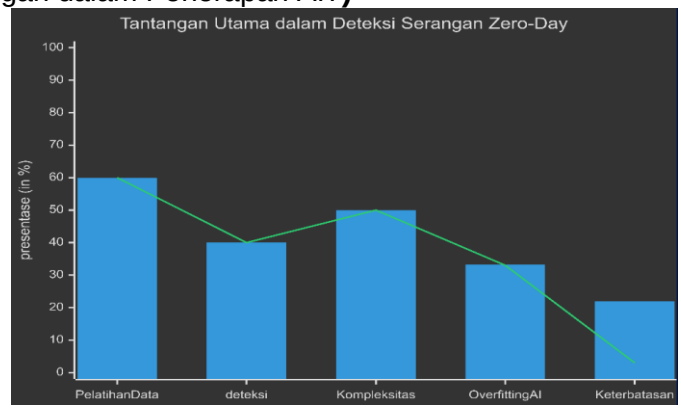
Gambar 3 2 Grafik Keefektivitas metode AI

Tabel 2 Tabel data keefektivitas Metode AI

Model	Akurasi	Presisi	Recall	F1-Score	AUC-ROC
Random Forest	0.93	0.90	0.88	0.89	0.95
SVM	0.91	0.89	0.87	0.88	0.93
Gradient Boosting	0.94	0.91	0.89	0.90	0.94
CNN	0.94	0.92	0,91	0.91	0.96
RNN	0.93	0.91	0.90	0.90	0.95

Data dan grafik di atas menunjukkan kinerja berbagai model AI dalam mendeteksi serangan zero-day berdasarkan metrik akurasi, presisi, recall, F1-score, dan AUC-ROC [24], [25], [26], [27] . Masing-masing model memiliki performa yang baik, dengan *Convolutional Neural Networks* (*CNN)* menunjukkan kinerja terbaik di sebagian besar metrik. 5 model AI membuktikan bahwa model ini dapat digunakan atau diimplementasikan dalam sehari-hari untuk mendekteksi serangan zero-day [6], [7], [8], [9], [10].

RQ 3 (Tantangan dalam Penerapan AI?**)**



Gambar 3 3 Presentase tantangan utama dalam penerapan AI

Tabel 3 Data tantangan utama dalam AI

Tantangan Utama	Jumlah Artikel yang Menyebutkan	Persentase (%)
Keterbatasan data pelatihan	18	60%
Ketidakpastian dalam Deteksi	12	40%
Kompleksitas Serangan Zero-Day	15	50%
Overfitting pada Model AI	10	33.3%
Keterbatasan dalam Skalabilitas	8	22.7%

Dari 30 artikel yang telah dianalisis, Data di atas menunjukan bahwa tantangan utama dalam penerapan AI untuk deteksi serangan zero-day mencakup keterbatasan data pelatihan dan validasi (60%), kompleksitas serangan zero-day (50%), ketidakpastian dalam deteksi (40%), overfitting pada model AI (33.3%), dan keterbatasan dalam skalabilitas (26.7%). Mengatasi tantangan ini memerlukan pendekatan yang lebih inovatif dan kolaboratif antara peneliti dan praktisi untuk meningkatkan efektivitas deteksi serangan zero-day dengan menggunakan AI [12], [28], [29], [30].

4. Kesimpulan

Dari 30 jurnal yang telah di-review, kami memperoleh jawaban dari masing-masing Research Question (RQ) yang telah ditetapkan sebelumnya. Untuk RQ1 Metode AI yang paling sering digunakan untuk mendeteksi serangan zero-day adalah *Convolutional Neural Networks (CNN)*, dalam 6 artikel atau 30% dari total keseluruhan jurnal. AI ini dipilih karena kemampuannya dalam mengenali pola yang kompleks dan melakukan klasifikasi dengan akurasi tinggi. Sedangkan RQ2 bagaimana efektivitas metode ini diterapkan dalam dunia nyata. Metode *CNN* lebih efektif digunakan di lihat dari data evaluasi yang telah dilakukan. Metode *CNN* memiliki nilai AUC-ROC 0.96 disusul dengan metode *Random Forest* dan *RNN* dengan nilai AUC-ROC 0.95. Dan untuk RQ3 bahwa tantangan utama dalam penerapan AI

Deteksi Serangan Zero-Day adalah pelatihan dan validasi data dengan tingkat kesulitan tertingii yaitu 60 % (18 artikel), dan disusul dengan kompleksitas serangan zero-day 50% 15 artikel.

5. Referensi

[1] M. Cen, X. Deng, F. Jiang, and R. Doss, "Zero-Ran Sniff: A zero-day ransomware early detection method based on zero-shot learning," *Comput Secur*, vol. 142, Jul. 2024, doi: 10.1016/j.cose.2024.103849.

[2] E. Bertino, M. Kantarcioglu, C. G. Akcora, S. Samtani, S. Mittal, and M. Gupta, "AI for Security and Security for AI," in *CODASPY 2021 - Proceedings of the 11th ACM Conference on Data and Application Security and Privacy*, Association for Computing Machinery, Inc, Apr. 2021, pp. 333–334. doi: 10.1145/3422337.3450357.

[3] J. F. Cevallos M., A. Rizzardi, S. Sicari, and A. C. Porisini, "NERO: NEural algorithmic reasoning for zeRO-day attack detection in the IoT: A hybrid approach," *Comput Secur*, vol. 142, p. 103898, Jul. 2024, doi: 10.1016/j.cose.2024.103898.

[4] I. H. Sarker, H. Janicke, M. A. Ferrag, and A. Abuadbba, "Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures," *Internet of Things (Netherlands)*, vol. 25. Elsevier B.V., Apr. 01, 2024. doi: 10.1016/j.iot.2024.101110.

[5] W. Wang, L. Chen, L. Han, Z. Zhou, Z. Xia, and X. Chen, "Vulnerability Assessment for ICS system Based on Zero-day Attack Graph," in *Proceedings - 2020 International Conference on Intelligent Computing, Automation and Systems, ICICAS 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 1–5. doi: 10.1109/ICICAS51530.2020.00009.

[6] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT-Edge Devices," *IEEE Internet Things J*, vol. 9, no. 5, pp. 3930–3944, Mar. 2022, doi: 10.1109/JIOT.2021.3100755.

[7] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.

[8] W. Wei, Q. Ke, J. Nowak, M. Korytkowski, R. Scherer, and M. Woźniak, "Accurate and fast URL phishing detector: A convolutional neural network approach," *Computer Networks*, vol. 178, Sep. 2020, doi: 10.1016/j.comnet.2020.107275.

[9] I. H. Sarker, H. Janicke, A. Mohsin, A. Gill, and L. Maglaras, "Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects," *ICT Express*. Korean Institute of Communications and Information Sciences, 2024. doi: 10.1016/j.icte.2024.05.007.

[10] M. Pawlicki, A. Pawlicka, R. Kozik, and M. Choraś, "Advanced insights through systematic analysis: Mapping future research directions and opportunities for xAI in deep learning and artificial intelligence used in cybersecurity," *Neurocomputing*, vol. 590, Jul. 2024, doi: 10.1016/j.neucom.2024.127759.

[11] F. Deldar and M. Abadi, "Deep Learning for Zero-day Malware Detection and Classification: A Survey," *ACM Comput Surv*, vol. 56, no. 2, Sep. 2023, doi: 10.1145/3605775.

[12] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C. H. Hsu, "Efficient and Secure Routing Protocol Based on Artificial Intelligence Algorithms with UAV-Assisted for Vehicular Ad Hoc Networks in Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4757–4769, Jul. 2021, doi: 10.1109/TITS.2020.3041746.

[13] M. Busuioc, "Accountable Artificial Intelligence: Holding Algorithms to Account," *Public Adm Rev*, vol. 81, no. 5, pp. 825–836, Sep. 2021, doi: 10.1111/puar.13293.

[14] H. Alkahtani and T. H. H. Aldhyani, "Artificial Intelligence Algorithms for Malware Detection in Android-Operated Mobile Devices," *Sensors*, vol. 22, no. 6, Mar. 2022, doi: 10.3390/s22062268.

[15] T. H. H. Aldhyani and H. Alkahtani, "Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity," *Sensors*, vol. 22, no. 1, Jan. 2022, doi: 10.3390/s22010360.

[16] M. Pooyandeh, K. J. Han, and I. Sohn, "Cybersecurity in the AI-Based Metaverse: A Survey," *Applied Sciences (Switzerland)*, vol. 12, no. 24. MDPI, Dec. 01, 2022. doi: 10.3390/app122412993.

[17] O. Krishnamurthy, "Genetic Algorithms, Data Analytics and it's applications, Cybersecurity: verification systems," 2023.

[18] C. Chakraborty, S. M. Nagarajan, G. G. Devarajan, T. V Ramana, and R. Mohanty, "Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method," *ACM Trans Sens Netw*, May 2023, doi: 10.1145/3597210.

[19] C. Xu, J. Shen, and X. Du, "A Method of Few-Shot Network Intrusion Detection Based on Meta-Learning Framework," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3540–3552, 2020, doi: 10.1109/TIFS.2020.2991876.

[20] R. Damoose, "A framework for disclosing DoD artificial intelligence-based cybersecurity product information," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jul. 2020, pp. 94–98. doi: 10.1145/3409891.3409912.

[21] S. Mishra, S. K. Pradhan, and S. K. Rath, "Detection of Zero-Day Attacks in Network IDS through High Performance Soft Computing," in *Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*, Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 1199–1204. doi: 10.1109/ICAIS50930.2021.9395929.

[22] P. Li *et al.*, "Learning from Limited Heterogeneous Training Data: Meta-Learning for Unsupervised Zero-Day Web Attack Detection across Web Domains," in *CCS 2023 - Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, Association for Computing Machinery, Inc, Nov. 2023, pp. 1020–1034. doi: 10.1145/3576915.3623123.

[23] Y. Guo, "A Review of Machine Learning-Based Zero-Day Attack Detection: Challenges and Future Directions," 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366422004248

[24] Han'guk T'ongsin Hakhoe, IEEE Communications Society, Denshi Jōhō Tsūshin Gakkai (Japan). Tsūshin Sosaieti, and Institute of Electrical and Electronics Engineers, *Hybrid System to Minimize Damage by Zero-Day Attack based on NIDPS and HoneyPot*. Joju(korea): IEEE, 2020. Accessed: Jun. 20, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/9289589

[25] L. Yang, A. Moubayed, and A. Shami, “MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles,” May 2021, doi: 10.1109/JIOT.2021.3084796.
[26] A. Touré, Y. Imine, A. Semnont, T. Delot, and A. Gallais, “A framework for detecting zero-day exploits in network flows,” *Computer Networks*, vol. 248, p. 110476, Jun. 2024, doi: 10.1016/j.comnet.2024.110476.
[27] M. Russinovich, N. Govindaraju, M. Raghuraman, D. Hepkin, J. Schwartz, and A. Kishan, “Virtual machine preserving host updates for zero day patching in public cloud,” in *EuroSys 2021 - Proceedings of the 16th European Conference on Computer Systems*, Association for Computing Machinery, Inc, Apr. 2021, pp. 114–129. doi: 10.1145/3447786.3456232.
[28] R. G. Gunawan, Erik Suanda Handika, and Edi Ismanto, “Pendekatan Machine Learning Dengan Menggunakan Algoritma Xgboost (Extreme Gradient Boosting) Untuk Peningkatan Kinerja Klasifikasi Serangan Syn,” *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 3, no. 3, pp. 453–463, Dec. 2022, doi: 10.37859/coscitech.v3i3.4356.
[29] P. Dixit and S. Silakari, “Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review,” *Computer Science Review*, vol. 39. Elsevier Ireland Ltd, Feb. 01, 2021. doi: 10.1016/j.cosrev.2020.100317.
[30] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, “Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research,” *IEEE Access*, vol. 10, pp. 93104–93139, 2022, doi: 10.1109/ACCESS.2022.3204051.