PENERAPAN MACHINE LEARNING UNTUK MENDETEKSI SERANGAN ANOMALI DALAM JARINGAN KOMPUTER : SYSTEMATIC LITERATURE REVIEW

Aprilian Gevindo, Billy Hendrik
Teknik Informatika, Universitas Putra Indonesia "YPTK" Padang
Padang, Indonesia
liando1801@gmail.com

ABSTRAK

Jaringan komputer berperan krusial dalam berbagai aspek kehidupan di era digital. Serangan siber dengan sifat anomali mengancam stabilitas sistem, baik dalam dunia bisnis maupun bagi individu. Teknik deteksi anomali diperlukan untuk mengidentifikasi aktivitas mencurigakan yang berpotensi mengganggu operasional sistem. Penelitian ini merupakan kajian literatur sistematis yang membahas penerapan machine learning dalam mendeteksi serangan anomali pada jaringan komputer. Fokus kajian ini berangkat dari meningkatnya kebutuhan keamanan siber di berbagai sektor, termasuk kesehatan, keuangan, pendidikan, dan pemerintahan. *Machine learning* dipilih karena kemampuannya mengenali pola dari data historis, sehingga meningkatkan akurasi dalam deteksi anomali secara adaptif. Hasil tinjauan terhadap penelitian sebelumnya membuktikan bahwa *machine learning* efektif dalam mengidentifikasi serangan anomali. Beragam algoritma yang telah diterapkan menunjukkan kemampuan dalam menghadapi ancaman keamanan jaringan yang tidak terduga.

Kata kunci : *Jaringan Komputer, Serangan Anomali, Machine Learning*

1. PENDAHULUAN

Jaringan komputer memainkan peran fundamental dalam mendukung berbagai aspek kehidupan manusia di era yang semakin terhubung dan bergantung pada teknologi [1]. Kemajuan era komunikasi berbasis *internet* menjadikan keamanan jaringan komputer sebagai perhatian utama [2]. Berkat kemajuan tersebut banyak kebutuhan serta pekerjaan dengan mudah dapat dikerjakan dan secara tidak langsung, hal ini telah menjadi fondasi yang sangat berpengaruh bagi kelangsungan berbagai sektor kehidupan manusia terutama pada sistem yang digunakan dapat terkena serangan dari pihak yang tidak bertanggung jawab [3].

Serangan siber sebagai anomali pada sistem dapat merusak sistem yang digunakan baik pada bisnis maupun pada individu [4]. Ancaman siber yang semakin meningkat serta kompleksitas infrastruktur jaringan menuntut teknik deteksi anomali yang lebih efektif. Teknik ini berperan dalam mengidentifikasi aktivitas mencurigakan atau berbahaya yang dapat mengganggu operasi sistem. Penerapan metode deteksi yang tepat mampu meningkatkan keamanan jaringan, mencegah serangan, serta menjaga kelangsungan layanan dan perlindungan data [5]. Ancaman siber terhadap sistem kontrol industri dapat mengakibatkan kerusakan peralatan, penurunan produktivitas, dan bahkan membahayakan keselamatan manusia hingga dibutuhkannya suatu sistem yang dapat mendeteksi seranga anomali pada keamanan jaringan komputer [6].

Keamanan jaringan menjadi aspek krusial yang harus diperhatikan oleh berbagai institusi dan perusahaan, termasuk yang bergerak dalam bidang teknologi [7]. Pendekatan yang lebih cerdas dan responsif menjadi kebutuhan dalam menghadapi ancaman ini. Sistem keamanan harus mampu secara aktif memantau pola lalu lintas yang tidak biasa serta mengidentifikasi aktivitas mencurigakan, bahkan tanpa adanya tanda-tanda klasik dari serangan. Kemampuan ini memungkinkan deteksi dini dan respons yang lebih cepat untuk melindungi jaringan dari potensi ancaman [8]. Memahami distribusi probabilitas dari perilaku normal jaringan, kita dapat mengidentifikasi perbedaan signifikan yang mungkin menunjukkan serangan atau aktivitas yang mencurigakan hingga perlunya suatu algoritma dalam mendeteksi serangan yang tak terduga atau tak dikenali pada saat serangan dilakukan [9].

Algoritma deteksi anomali tradisional kerap mengalami kesulitan dalam menangani volume data yang besar serta keragaman data jaringan. Tantangan ini dapat memengaruhi efektivitas deteksi dan meningkatkan risiko terlewatnya ancaman yang tersembunyi di dalam lalu lintas jaringan. [5]. Metode yang efektif untuk mencapai hal ini adalah menggabungkan teori probabilitas dan pembelajaran mesin [9]. Teknik kecerdasan buatan (AI), terutama dalam bentuk machine learning dapat dimanfaatkan untuk merancang sistem deteksi intrusi yang cerdas berbasis data [10].

2. TINJAUAN PUSTAKA

Tinjauan pustaka disusun berdasarkan berbagai literatur yang mendukung landasan teori dalam penelitian ini. Literatur yang dikaji berasal dari berbagai sumber penelitian terdahulu, yang memberikan wawasan lebih mendalam mengenai konsep, metode, serta pendekatan yang telah digunakan dalam deteksi serangan anomali pada jaringan komputer. Dengan adanya tinjauan ini, peneliti dapat mengidentifikasi keterbatasan studi sebelumnya, menemukan peluang pengembangan, serta memperkuat dasar teori yang digunakan dalam

penelitian ini. Selain itu kajian pustaka juga membantu dalam memahami tren terbaru dalam penerapan machine learning untuk deteksi anomali, sehingga penelitian ini dapat memberikan kontribusi yang lebih signifikan. Berikut adalah landasan teori yang digunakan dalam penelitian ini.

2.1. Jaringan Komputer

Jaringan komputer terdiri dari dua atau lebih komputer yang saling terhubung untuk berkomunikasi dan bertukar data. Koneksi antar komputer ini dapat dilakukan menggunakan media kabel atau teknologi nirkabel [11]. Jaringan komputer memungkinkan perangkat yang terhubung untuk saling berkomunikasi melalui media komunikasi, sehingga dapat berbagi data, informasi, program, dan perangkat keras [12]. Perangkat yang menghubungkan komputer dalam sebuah jaringan berperan penting dalam komunikasi data. Para ahli telah mengklasifikasikan jaringan komputer berdasarkan area cakupan atau skala, jenis media penghantar, dan fungsinya untuk mempermudah pemahaman [13].

2.2. Keamanan Jaringan

Keamanan jaringan bertujuan untuk mencegah dan mengidentifikasi akses tidak sah atau penyusup dalam suatu jaringan [14]. Potensi ancaman terhadap keamanan jaringan dapat berasal dari pengguna internal maupun eksternal. Target ancaman pun beragam, tergantung pada tujuan dan metode yang digunakan [15]. Menerapkan sistem keamanan berlapis dapat meningkatkan perlindungan jaringan, tetapi juga berisiko menurunkan performa. Kepadatan data dalam lalu lintas jaringan meningkat karena banyaknya data yang harus difilter pada proses pengiriman dan penerimaan paket [16].

2.3. Serangan Anomali

Serangan anomali menjadi ancaman serius bagi keamanan informasi dan infrastruktur teknologi karena metode penyerangannya yang tidak biasa dan di luar ekspektasi [17]. Penyerang semakin terampil dalam menerapkan berbagai metode dan taktik yang terus berkembang, sehingga membuat deteksi serangan menjadi semakin rumit [18]. Serangan anomali merugikan karena mengancam keamanan data serta privasi pengguna maupun instansi. Serangan ini dapat muncul dalam berbagai bentuk, seperti *malware*, serangan DDoS, *phishing*, dan metode tak terduga lainnya [19].

2.4. Deteksi Anomali

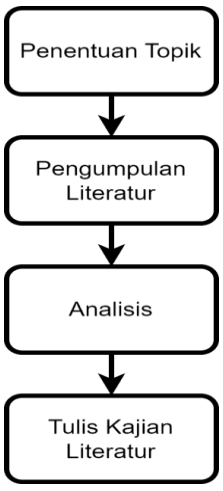
Deteksi serangan anomali merupakan aspek krusial dalam menjaga keamanan jaringan komputer [17]. Penyerang terus mengembangkan strategi mereka seiring waktu, meninggalkan pola yang sulit diprediksi [18]. Deteksi anomali dapat digunakan untuk mengenali serangan dengan memanfaatkan pengalaman sebelumnya dalam mengidentifikasi perilaku pengguna yang tidak normal [20].

2.5. Mechine Lerning

Machine learning merupakan cabang dari kecerdasan buatan yang menggunakan metode statistika untuk menganalisis data. Teknologi ini memungkinkan komputer mengenali pola dalam data tanpa harus diprogram secara eksplisit [21]. Teknologi *machine learning* digunakan untuk mengembangkan sistem cerdas dengan melatih mesin agar mampu membuat keputusan secara mandiri [22]. Metode dan vektor serangan siber semakin kompleks dan beragam, menuntut pendekatan deteksi yang lebih canggih. *Machine learning* digunakan sebagai metode deteksi untuk mengidentifikasi pola serangan dengan lebih akurat dan adaptif [23].

3. METODE PENELITIAN

Studi literatur diawali dengan mengidentifikasi dan mengakses berbagai artikel penelitian melalui platform pencarian akademis. Proses ini dilakukan secara daring dengan menelusuri sumber-sumber terpercaya, terutama artikel yang dipublikasikan di Indonesia, guna memperoleh referensi yang relevan dan mendukung penelitian. Tahapan dalam kajian literatur ini meliputi penentuan topik penelitian, pengumpulan literatur yang relevan, analisis literatur dengan membaca secara menyeluruh, pengelompokkan berdasarkan metode dan kriteria yang digunakan dalam penelitian sebelumnya, hingga penyusunan tinjauan literatur. Model dari langkah-langkah kajian literatur yang dilakukan dapat dilihat pada Gambar 1. dibawah ini:



Gambar 1. Langkah-langkah Literatur

Gambar 1. diatas menunjukan prosedur dari tahapan langkah-langkah kajian literatur. Penggunaan konsep tersebut digunakan agar tahapan kajian literatur dapat dilakukan secara sistematis. Berdasarkan hal tersebut dapatlah peneliti melakukan sebuah kajian literatur dengan baik dan jelas. Berikut penjelasan terhadap langkah-langkah tersebut berdasarkan tahapannya sebagai berkiut ini.

3.1. Penentuan Topik

Penelitian ini berfokus pada penerapan *machine learning* untuk deteksi serangan anomali pada jaringan komputer. Pemilihan topik ini didasarkan pada urgensi deteksi serangan anomali di berbagai sektor, seperti kesehatan, keuangan, pendidikan, pemerintahan, dan lainnya. *Machine learning* dipilih karena kemampuannya dalam mempelajari pola dari data historis, sehingga dapat meningkatkan keakuratan dalam mendeteksi serangan anomali secara lebih efektif.

3.2. Pengumpulan Literatur

Proses ini mencakup pengumpulan artikel ilmiah yang membahas penerapan *machine learning* dalam mendeteksi serangan anomali pada jaringan komputer. Literatur yang dikumpulkan berfokus pada implementasi machine learning dalam deteksi serangan anomali. Selain itu, studi kasus mengenai serangan anomali di berbagai bidang juga dianalisis, termasuk deteksi serangan pada jaringan komputer.

3.3. Analisis

Peneliti melakukan evaluasi kritis terhadap metode dan hasil penelitian terdahulu mengenai penerapan machine learning dalam mendeteksi serangan anomali pada jaringan komputer. Analisis ini mencakup beberapa aspek utama yang berkaitan dengan efisiensi, efektivitas, dan kriteria evaluasi dalam deteksi serangan anomali. Aspek-aspek tersebut meliputi:

a. Efisiensi penerapan algoritma *machine learning* dalam deteksi serangan anomali pada jaringan komputer.
b. Efektivitas implementasi diuji melalui berbagai studi kasus praktis untuk menilai kinerjanya dalam situasi nyata.
c. Kriteria evaluasi seperti variabel faktor-faktor dari serangan tak terterduga dan dikenali pada sebuah jaringan komputer.

3.4. Tulis Kajian Literatur

Tahap akhir penelitian ini berfokus pada penyusunan temuan dari tinjauan pustaka secara sistematis. Peneliti menguraikan mekanisme kerja algoritma machine learning serta manfaatnya dalam mendeteksi serangan anomali pada jaringan komputer. Aspek-aspek yang dicakup dalam algoritma *machine learning* meliputi:

a. Permasalahan, Serangan anomali mengancam keamanan jaringan komputer..
b. Implementasi, Metode deteksi telah diterapkan dalam berbagai kasus dengan hasil beragam..
c. Metodologi, Algoritma machine learning digunakan untuk mendeteksi anomali..
d. Studi Kasus, Evaluasi performa metode dilakukan dalam berbagai skenario..
e. Keterbatasan dan Pengembangan, Analisis dilakukan untuk meningkatkan efektivitas deteksi.

4. HASIL DAN PEMBAHASAN

Penelusuran menghasilkan lima belas artikel ilmiah yang dianalisis secara naratif berdasarkan kriteria inklusi yang telah ditentukan. Rincian artikel disajikan dalam bentuk tabel. Hasil analisis artikel ilmiah terkait deteksi serangan anomali pada jaringan komputer seperti dapat dilihat pada Tabel 1. dibawah ini:

Tabel 1. Analisa Artikel Ilmiah

Penelitian	Hasil	Metodologi
Klasifikasi Deteksi Anomali Menggunakan Metode Machine Learning [10]	Penerapan metode klasifikasi tree bahwa proses pre-processing data ini dapat mempengaruhi hasil perfoma dari sebuah metode klasifikasi.	Deceision Tree
Deteksi Anomali Dan Serangan Low Rate Ddos Dalam Lalu Lintas Jaringan [24]	Model GaussianNB mencapai akurasi tertinggi sebesar 83,45%, lebih tinggi dibandingkan model BernoulliNB yang hanya mencapai 76,21%. Precision dan F1 Score pada model GaussianNB masing-masing sebesar 61,573% dan 55,546%	Naive Bayes
Model Deteksi Anomali Jaringan Komputer Menggunakan Teknik Machine Learning [25]	Tingkat akurasi model untuk label 0 anomaly sebesar Accuracy 60%,Precision 60%,F1-Score 75%,Support 100%, dan Recall 100%. untuk label 1 = normal sebesar Accuracy 33%,Precision 33%,F1-Score 100%,Support 50%, dan Recall 100%.	Support Vector Machine
Analisis Perbandingan Metode Seleksi Fitur untuk Mendeteksi Anomali pada Dataset CIC-IDS-2018 [26]	Algoritma classifier yang diimplementasikan pada metode filter menggunakan Information Gain bekerja dengan baik, Random Forest memiliki akurasi 99%.	Random Forest
Implementasi Deep Learning Dalam Deteksi Anomali: Meningkatkan Keamanan Sistem Informasi [27]	Arsitektur jaringan saraf tiruan yang dalam, seperti CNN dan RNN, memungkinkan sistem mengenali pola kompleks dalam data, sehingga meningkatkan kemampuan deteksi terhadap serangan yang belum diketahui sebelumnya.	CNNs dan RNNs
Model Machine Learning SVM (Support Vector Machine) untuk Deteksi Anomali pada Sistem	Hasil penelitian menunjukkan Akurasi (seberapa sering model membuat prediksi yang benar terhadap semua data yang diuji) sebesar 96,5 %. Presisi 94.8% (dari semua data yang diklasifikasikan sebagai anomali oleh model, sebanyak 94.8%	Support Vector Machine

Penelitian	Hasil	Metodologi
Kelistrikan Perusahaan Kerajinan Kayu GS4 [28]	benar-benar anomali). Recall 92.3% (dari semua kasus anomali yang ada, model berhasil mendeteksi 92.3%).	
Deteksi Serangan Siber Pada Jaringan Komputer [29]	Model Random Forest efektif untuk deteksi serangan dan berpotensi meningkatkan keamanan siber, meskipun pemahaman kelas serangan masih perlu diperluas.	Random Forest
Implementasi Machine Learning untuk Deteksi Intrusi pada Jaringan Komputer [30]	Seluruh model machine learning yang diuji menunjukkan kinerja optimal dalam mendeteksi intrusi. Namun, Random Forest mencapai akurasi, presisi, recall, dan F1-score tertinggi dibandingkan Decision Tree dan SVM, menjadikannya metode yang lebih efektif untuk deteksi serangan siber.	Decision Tree, Random Forest, dan Support Vector Machine.
Perbandingan Support Vector Machine, Random Forest Classifier, dan K-Nearest Neighbour dalam Pendeteksian Anomali pada Jaringan Ddos [31]	Hasil penelitian penerapan algoritma Random Forest Classifier (RFC) menunjukkan performa terbaik dengan akurasi 99,99%, precision 99,98%, recall 100%, dan MCC 99,98%. SVM dan KNN juga menunjukkan performa tinggi dengan akurasi masing-masing 99,91% dan 99,98%. Namun, RFC memiliki keunggulan utama pada recall sempurna (100%) dan tingkat kesalahan (FPR) yang paling rendah (0,02%). Hal ini menjadikan RFC sebagai algoritma yang paling efektif dalam mendeteksi anomali jaringan DDoS.	Support Vector Machine, Random Forest Classifier, dan K-Nearest Neighbour
Deteksi Anomali Jaringan Menggunakan Isolation Forest pada Log Wazuh dengan Pemberitahuan WhatsApp di PT XYZ [32]	Berdasarkan hasil evaluasi, algoritma ini menunjukkan kinerja yang sangat baik dalam mendeteksi anomali dengan akurasi 100% pada sampel data log sebanyak 2000 data. Sistem ini juga berhasil mengirimkan notifikasi melalui pesan WhatsApp dengan waktu pengiriman rata-rata hanya 5 detik, dan mendeteksi 17 anomali yang teridentifikasi sebagai true positives.	Isolation Forest
Mengoptimalkan Kinerja Naïve Bayes Pada Ancaman Modern Dengan Menggunakan PCA Pada Data Intrusion Detection System (IDS) [33]	Penggunaan PCA mendapati Akurasi 96.65%, recall kelas positif sangat tinggi (1.00) sedangankan Tanpa PCA Akurasi lebih rendah (92.73%) dengan presisi kelas positif lebih buruk (0.31)	Naïve Bayes
Analisis Perbandingan Kinerja Algoritma Machine Learning Berbasis Feature Selection Dalam Deteksi Serangan Botnet [34]	Hasil penelitian ini SVM menunjukkan performa terbaik dalam mendeteksi serangan botnet dengan akurasi 84% dan F1-Score 80%, serta diikuti oleh KNN dengan akurasi 79% dan F1-Score 73%. NB memiliki performa terendah dengan akurasi 75% dan F1- Score 66%.	SVM dan KNN
Efektivitas Algoritma Artificial Intelligence dalam Melawan Serangan Zero-Day [35]	Deteksi Serangan Zero-Day menggunakan pelatihan dan validasi data dengan tingkat kesulitan tertingii yaitu 60 %, dan disusul dengan kompleksitas serangan zero-day 50%.	Convolutional Neural Networks
Klasifikasi Serangan Pada Jaringan Internet of Thing (IoT): Tinjauan Literatur Komparatif [36]	Hasil penelitian menunjukkan bahwa metode yang diterapkan memiliki akurasi di atas rata-rata, dengan RF mencapai 97%, KNN 80%, dan NB 92%	RF, KNN, dan NB
Deteksi Anomali Dan Serangan Low Rate Ddos Dalam Lalu Lintas Jaringan [37]	Model GaussianNB mencapai akurasi tertinggi sebesar 83,45%, lebih tinggi dibandingkan BernoulliNB yang hanya mencapai 76,21%. Precision dan F1 Score pada GaussianNB masing-masing sebesar 61,573% dan 55,546%	Naïve Bayes

Tabel 1. diatas menunjukan hasil dari analisis artikel ilmiah dalam deteksi serangan anomali pada sebuah jaringan komputer. Deteksi dilakukan dengan menggunakan penerapan dari berbagai algoritma *Machine Learning*. Penerapan yang dilakukan menujukan hasil yang signifikan dalam mendeteksi serangan anomali pada sebuah jaringan komputer hingga menjadikannya sebuah evaluasi dalam upaya meningkatkan keamanan jaringan komputer.

5. KESIMPULAN

Penerapan *machine learning* terbukti menjadi solusi efektif dalam mendeteksi serangan anomali pada jaringan komputer. Berbagai algoritma yang digunakan dalam penelitian terdahulu menunjukkan kemampuan dalam mengatasi permasalahan keamanan jaringan dari ancaman serangan yang tidak terduga. Temuan ini diharapkan menjadi referensi penting bagi penelitian mendatang dalam pengembangan metode deteksi serangan anomali yang lebih akurat dan reliabel.

DAFTAR PUSTAKA

[1] G. M. G. Bororing, “Pengembangan Algoritma Machine Learning Untuk Mendeteksi Anomali Dalam Jaringan Komputer,” *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, vol. 7, no. 1, pp. 1361–1368, 2024.

[2] D. Suprihadi and I. Magfira, "FORENSIK PADA JARINGAN KOMPUTER LOKAL DENGAN KLASIFIKASI SVM BERBASIS FRAMEWORK TAARA," *Jurnal Review Pendidikan dan Pengajaran (JRPP)*, vol. 7, no. 1, pp. 666–673, 2024.

[3] G. S. W. Prabuningrat, D. P. Hostiadi, and N. L. P. Srinadi, "Klasifikasi deteksi anomali menggunakan metode machine learning," in *Seminar Hasil Penelitian Informatika dan Komputer (SPINTER)| Institut Teknologi dan Bisnis STIKOM Bali*, 2024, pp. 845–850.

[4] T. G. Laksana and S. Mulyani, "Pengetahuan dasar identifikasi dini deteksi serangan kejahatan siber untuk mencegah pembobolan data perusahaan," *Jurnal Ilmiah Multidisiplin*, vol. 3, no. 01, pp. 109–122, 2024.

[5] O. Triana, "Deteksi Anomali Jaringan Menggunakan Algoritma Isolation Forest," *Jurnal Dunia Data*, vol. 1, no. 5, 2024.

[6] R. M. Imam, P. Sukarno, and M. A. Nugroho, "Deteksi Anomali Jaringan Menggunakan Hybrid Algorithm," in *e-Proceeding of Engineering*, 2019, pp. 8766–8787.

[7] P. Y. Pinontoan and I. Sembiring, "Implementasi dan Analisis Deteksi Serangan Jaringan pada Web Server NFT Menggunakan Suricata," *Edutik: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, vol. 4, no. 1, pp. 65–78, 2024.

[8] G. M. G. Bororing, "Pengembangan Algoritma Machine Learning Untuk Mendeteksi Anomali Dalam Jaringan Komputer," *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, vol. 7, no. 1, pp. 1361–1368, 2024.

[9] A. Maharani, "Pengembangan Model Prediktif untuk Deteksi Anomali dalam Keamanan Jaringan menggunakan Teori Peluang dan Pembelajaran Mesin," *Jurnal Dunia Ilmu*, vol. 3, no. 8, 2023.

[10] G. S. W. Prabuningrat, D. P. Hostiadi, and N. L. P. Srinadi, "Klasifikasi deteksi anomali menggunakan metode machine learning," in *Seminar Hasil Penelitian Informatika dan Komputer (SPINTER)| Institut Teknologi dan Bisnis STIKOM Bali*, 2024, pp. 845–850.

[11] D. D. Papaceda, A. Mewengkang, and S. Pratasik, "Analisis dan Pengembangan Jaringan Komputer di SMK Negeri 8 Weda Halmahera Tengah," *Edutik: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, vol. 3, no. 1, pp. 1–13, 2023.

[12] A. V. Mananggel, A. Mewengkang, and A. C. Djamen, "Perancangan jaringan komputer di SMK menggunakan cisco packet tracer," *Edutik: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, vol. 1, no. 2, pp. 119–131, 2021.

[13] R. Refina and T. D. Purwanto, "Manajemen Bandwidth Menggunakan Metode Simple Queue Dan Queue Tree Pada Dinas Kominfo Kota Prabumulih," in *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)*, 2022, pp. 50–59.

[14] O. Rivaldi and N. L. Marpaung, "Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata," *Jurnal Inovtek Polbeng Seri Informatika*, vol. 8, no. 1, pp. 141–153, 2023.

[15] S. Sartomo and W. Sulistyo, "Model Keamanan Jaringan Menggunakan Firewall Port Blocking," *Krea-TIF: Jurnal Teknik Informatika*, vol. 10, no. 1, pp. 10–18, 2022.

[16] G. B. Guntoro, M. K. Hidayat, and F. Ajismanto, "Pemanfaatan Firewall Rule Base dan SSL dalam Penerapan Sistem Keamanan Jaringan," *Teknomatika*, vol. 12, no. 02, pp. 131–140, 2022.

[17] L. I. Uzlah, R. A. Saputra, and I. Isnawaty, "DETEKSI SERANGAN SIBER PADA JARINGAN KOMPUTER MENGGUNAKAN METODE RANDOM FOREST," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 3, pp. 2787–2793, 2024.

[18] G. M. G. Bororing, "Pengembangan Algoritma Machine Learning Untuk Mendeteksi Anomali Dalam Jaringan Komputer," *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, vol. 7, no. 1, pp. 1361–1368, 2024.

[19] A. Z. Hermawan, M. N. Anggoro, D. Lozera, and A. Faroqi, "Studi Literatur: Ancaman Serangan Siber Artificial Intelligence (AI) Terhadap Keamanan Data di Indonesia," in *Prosiding Seminar Nasional Teknologi dan Sistem Informasi*, 2023, pp. 581–591.

[20] M. R. R. Islami, "DETEKSI DINI SERANGAN PADA WEBSITE MENGGUNAKAN METODE ANOMALI BASED," *JIKO (Jurnal Informatika dan Komputer)*, vol. 5, no. 3, pp. 224–229, 2022.

[21] M. Pandia, "Kajian Literatur Multimedia Retrieval: Machine Learning Untuk Pengenalan Wajah," *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, vol. 7, no. 1, pp. 161–166, 2024.

[22] F. Febriansyah, Z. A. Dwiyanti, and D. Firdaus, "Deteksi Serangan Low Rate Ddos Pada Jaringan Tradisional Menggunakan Machine Learning Dengan Algoritma Decision Tree," *Cyber Security Dan Forensik Digital*, vol. 6, no. 1, pp. 6–11, 2023.

[23] H. Hartono, K. Khotimah, and A. Wibowo, "DETEKSI SERANGAN REMOTE CODE EXECUTION DAN CROSS SITE SCRIPTING MENGGUNAKAN MACHINE LEARNING," *Jurnal Informatika*, vol. 23, no. 2, pp. 229–242, 2023.

[24] D. Firdaus, F. Fahira, and R. Rianti, "DETEKSI ANOMALI DAN SERANGAN LOW RATE DDOS DALAM LALU LINTAS JARINGAN MENGGUNAKAN NAIVE BAYES," *Naratif: Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika*, vol. 5, no. 2, pp. 140–148, 2023.

[25] D. Subuhanto and L. Tanti, "Model Deteksi Anomali Jaringan Komputer Menggunakan Teknik Machine Learning," in *PROSIDING SEMINAR NASIONAL MULTI DISIPLIN ILMU (SENADIMU)*, 2024, pp. 239–259.

[26] A. Devia and B. Soewito, "Analisis Perbandingan Metode Seleksi Fitur untuk Mendeteksi Anomali pada Dataset CIC-IDS-2018," *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 5, no. 4, pp. 572–578, 2023.

[27] J. Kurniawan, "IMPLEMENTASI DEEP LEARNING DALAM DETEKSI ANOMALI: MENINGKATKAN KEAMANAN SISTEM INFORMASI," *Jurnal Teknologi Pintar*, vol. 3, no. 12, 2023.

[28] B. M. Basuki and D. Cahyono, "Model Machine Learning SVM (Support Vector Machine) untuk Deteksi Anomali pada Sistem Kelistrikan Perusahaan Kerajinan Kayu GS4," *Jurnal Teknik Mesin, Industri, Elektro dan Informatika*, vol. 4, no. 1, pp. 310–320, 2025.

[29] L. I. Uzlah, R. A. Saputra, and I. Isnawaty, "DETEKSI SERANGAN SIBER PADA JARINGAN KOMPUTER MENGGUNAKAN METODE RANDOM FOREST," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 3, pp. 2787–2793, 2024.

[30] D. P. Sari, Z. Halim, I. Irlon, B. Waseso, and S. Saromah, "Implementasi Machine Learning untuk Deteksi Intrusi pada Jaringan Komputer," *Jurnal Minfo Polgan*, vol. 13, no. 2, pp. 1389–1394, 2024.

[31] H. Haeruddin, E. Erick, and H. W. Aripradono, "Perbandingan Support Vector Machine, Random Forest Classifier, dan K-Nearest Neighbour dalam Pendeteksian Anomali pada Jaringan DDos," *JTIM: Jurnal Teknologi Informasi dan Multimedia*, vol. 7, no. 1, pp. 23–33, 2025.

[32] R. P. Dewa and W. Windarto, "Deteksi Anomali Jaringan Menggunakan Isolation Forest pada Log Wazuh dengan Pemberitahuan WhatsApp di PT XYZ," *KRESNA: Jurnal Riset dan Pengabdian Masyarakat*, vol. 4, no. 2, pp. 208–216, 2024.

[33] K. S. Arlandy, A. Faqih, and A. R. Rinaldi, "Mengoptimalkan Kinerja Naïve Bayes Pada Ancaman Modern Dengan Menggunakan PCA Pada Data Intrusion Detection System (IDS)," *Jurnal Ilmiah ILKOMINFO-Ilmu Komputer & Informatika*, vol. 8, no. 1, pp. 25–37, 2025.

[34] R. Khoo and K. Handoko, "ANALISIS PERBANDINGAN KINERJA ALGORITMA MACHINE LEARNING BERBASIS FEATURE SELECTION DALAM DETEKSI SERANGAN BOTNET," *Computer and Science Industrial Engineering (COMASIE)*, vol. 12, no. 2, pp. 139–148, 2025.

[35] F. Raihan, "Efektivitas Algoritma Artificial Intelligence dalam Melawan Serangan Zero-Day," in *Prosiding Seminar Nasional Informatika*, 2024, pp. 658–665.

[36] R. A. Khairulah, R. Herdianto, and M. A. Setiawan, "Klasifikasi Serangan Pada Jaringan Internet of Thing (IoT): Tinjauan Literatur Komparatif," *Jurnal Inovasi Teknologi Dan Edukasi Teknik*, vol. 3, no. 1, pp. 47–53, 2023.

[37] D. Firdaus, F. Fahira, and R. Rianti, "DETEKSI ANOMALI DAN SERANGAN LOW RATE DDOS DALAM LALU LINTAS JARINGAN MENGGUNAKAN NAIVE BAYES," *Naratif: Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika*, vol. 5, no. 2, pp. 140–148, 2023.