VOLUME 14 Nomor 02 Agustus 2023
e-ISSN 2477-3786 | p-ISSN 2302-500X

Deteksi Intrusi Siber pada Sistem Pembelajaran Elektronik berbasis *Machine Learning*

Amirah[1)], Ahmad Sanmorino[2)]

[1)]Ma'had Zaadul Ma'ad Palembang
[2)]Fakultas Komputer dan Sains, Universitas Indo Global Mandiri
Lrg. Melati No.1, Talang Jambe, Kec. Sukarami, Palembang[1)]
Jl. Jendral Sudirman No.629 Km.4 Palembang 30129[2)]
Email :sanmorino@uigm.ac.id[2)]

ABSTRACT

This study aims to develop a mechanism for detecting machine learning-based cyber intrusions in electronic learning systems. In today's digital era, e-learning systems have become an integral part of education and training, providing global accessibility and more interactive learning efficiency. However, security and privacy challenges are becoming critical issues due to the increasingly real threat of cyber intrusion. Attackers try to take advantage of vulnerabilities and weaknesses in e-learning systems to steal sensitive data or disrupt operations. To overcome this problem, this study focuses on the use of artificial intelligence technologies, especially machine learning, to proactively detect and respond to intrusive threats. Through e-learning security analysis, identification of weaknesses, and potential loopholes for cyber-attacks, the most suitable machine learning algorithms are selected to detect patterns and signs of intrusion attacks on network data. The evaluation results show that several machine learning algorithms, such as SVM and Decision Tree, have good performance in recognizing cyber intrusions with high accuracy, precision, recall, F1-score, and ROC-AUC. By implementing machine learning-based intrusion detection technology, it is expected that electronic learning systems can be more proactive in identifying and responding to intrusion threats before significant damage occurs. This research has significant benefits in increasing security and privacy in the use of electronic learning systems. In addition, this study is expected to be a reference for further research in the world of cyber security and the application of artificial intelligence technology in supporting digital security.

Keywords : *Cyber Intrusion Detection, Machine Learning, e-learning*

ABSTRAK

Studi ini bertujuan untuk mengembangkan mekanisme deteksi intrusi siber berbasis machine learning pada sistem pembelajaran elektronik. Di era digital saat ini, sistem pembelajaran elektronik telah menjadi bagian integral dari pendidikan dan pelatihan, menyediakan aksesibilitas global dan efisiensi pembelajaran yang lebih interaktif. Namun, tantangan keamanan dan privasi menjadi isu kritis karena semakin nyatanya ancaman intrusi siber. Para penyerang mencoba memanfaatkan kerentanan dan kelemahan pada sistem e-learning untuk mencuri data sensitif atau mengganggu operasional.Untuk mengatasi masalah ini, studi ini memusatkan perhatian pada penggunaan teknologi kecerdasan buatan, khususnya machine learning, untuk mendeteksi dan merespons ancaman intrusi secara proaktif. Melalui analisis keamanan e-learning, identifikasi kelemahan, dan potensi celah bagi serangan siber, dilakukan pemilihan algoritma machine learning yang paling cocok untuk mendeteksi pola dan tanda-tanda serangan intrusi pada data jaringan.Hasil evaluasi menunjukkan bahwa beberapa algoritma machine learning, seperti SVM dan Decision Tree, memiliki kinerja yang baik dalam mengenali intrusi siber dengan akurasi, presisi, recall, F1-score, dan ROC-AUC yang tinggi. Dengan menerapkan teknologi deteksi intrusi berbasis machine learning, diharapkan sistem pembelajaran elektronik dapat lebih proaktif dalam mengidentifikasi dan merespons ancaman intrusi sebelum terjadi kerusakan yang signifikan. Penelitian ini memiliki manfaat yang signifikan dalam meningkatkan keamanan dan privasi dalam penggunaan sistem pembelajaran elektronik. Selain itu, studi ini diharapkan dapat menjadi referensi bagi penelitian lebih lanjut dalam dunia keamanan siber dan penerapan teknologi kecerdasan buatan dalam mendukung keamanan digital.

Kata Kunci : *Deteksi Intrusi Siber, Machine Learning, e-learning*

Article History
Received : 10/03/2023
Revised : 20/04/2023
Accepted : 20/07/2023
Online : 01/08/2023

VOLUME 14 Nomor 02 Agustus 2023
e-ISSN 2477-3786 | p-ISSN 2302-500X

1. Pendahuluan

1.1. Latar Belakang

Di era digital saat ini, sistem pembelajaran elektronik (e-learning) telah menjadi bagian integral dari pendidikan dan pelatihan. Teknologi e-learning memberikan aksesibilitas yang luar biasa bagi siswa dan peserta pelatihan di seluruh dunia, mengatasi batasan geografis dan memfasilitasi proses pembelajaran yang lebih interaktif dan efisien (Alyoussef, 2023). Namun, dengan keuntungan dan kenyamanan yang ditawarkan oleh sistem pembelajaran elektronik, keamanan dan privasi menjadi isu kritis yang perlu diatasi secara serius.

Intrusi siber atau serangan siber menjadi ancaman yang semakin nyata (Diaba, 2023), termasuk sistem pembelajaran elektronik. Para penyerang mencoba memanfaatkan kerentanan dan kelemahan pada sistem tersebut untuk mencuri data sensitif, mengganggu operasional, atau menginfeksi dengan perangkat lunak berbahaya. Serangan semacam itu dapat mengakibatkan kerugian finansial, kerusakan reputasi institusi pendidikan, dan yang paling meresahkan, potensi penyalahgunaan informasi siswa atau peserta pelatihan (Omer, 2023).

Dalam upaya untuk melindungi sistem pembelajaran elektronik dari ancaman intrusi siber, penggunaan teknologi kecerdasan buatan, khususnya machine learning, telah menjadi fokus perhatian yang signifikan (Hossain, 2023). Teknik machine learning telah terbukti sebagai alat yang efektif dalam mendeteksi pola dan perilaku yang mencurigakan pada data jaringan, yang merupakan ciri khas dari serangan siber (Kanimozhi, 2020). Dengan memanfaatkan machine learning, sistem pembelajaran elektronik dapat secara proaktif mengidentifikasi dan merespons ancaman intrusi sebelum kerusakan yang signifikan terjadi (Abdallah, 2022).

1.2. Tujuan

Tujuan dari studi ini adalah untuk mengembangkan mekanisme deteksi intrusi siber berbasis machine learning pada sistem pembelajaran elektronik. Studi ini bertujuan untuk mencapai beberapa sasaran, yaitu:

1. Menganalisis kelemahan keamanan yang umum ditemukan dalam sistem pembelajaran elektronik dan mengidentifikasi celah potensial bagi serangan siber.
2. Mengidentifikasi algoritma machine learning yang paling cocok untuk mendeteksi pola dan tanda-tanda serangan intrusi pada data jaringan (Wazid, 2022).
3. Mengusulkan mekanisme deteksi intrusi berbasis machine learning dan mengevaluasi kinerjanya dalam mendeteksi serangan siber yang berbeda.
4. Mengusulkan langkah-langkah perbaikan dan penguatan keamanan untuk meningkatkan ketahanan sistem pembelajaran elektronik terhadap ancaman intrusi siber.

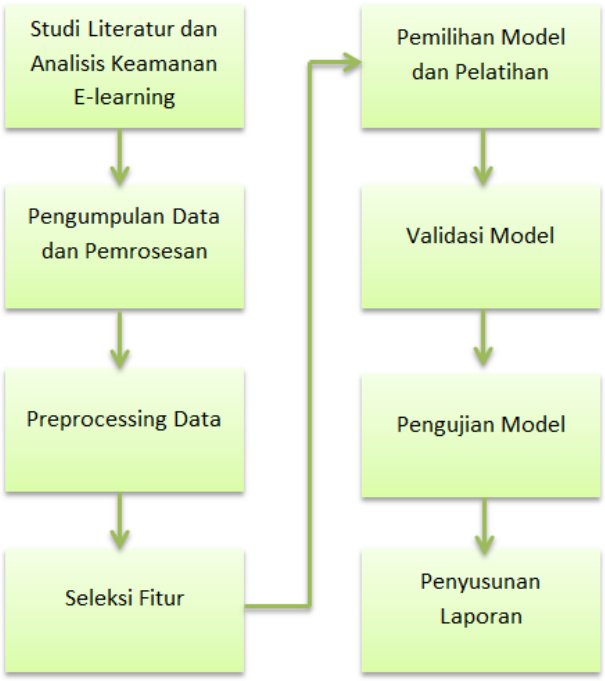
1.3. Manfaat

Penelitian ini diharapkan akan memberikan kontribusi yang signifikan dalam meningkatkan keamanan dan privasi dalam penggunaan sistem pembelajaran elektronik. Dengan adanya teknologi deteksi intrusi berbasis machine learning (Golchha, 2023), institusi pendidikan dan tempat pelatihan akan dapat mengidentifikasi serangan siber secara dini dan mengambil tindakan yang sesuai untuk melindungi data dan sistem mereka. Selain itu, studi ini juga diharapkan dapat menjadi referensi bagi penelitian lebih lanjut di bidang keamanan siber dan penggunaan teknologi kecerdasan buatan dalam mendukung keamanan digital.

2. Pembahasan

2.1. Desain Penelitian

Adapun desain penelitian dalam studi 'Deteksi Intrusi Siber pada Sistem Pembelajaran Elektronik berbasis Machine Learning' ditunjukan Gambar 1:



Gambar 1. *Desain Penelitian*

1. Studi Literatur dan Analisis Keamanan E-learning: Tahap awal adalah melakukan studi literatur tentang sistem pembelajaran elektronik, keamanan siber, dan deteksi intrusi. Melakukan analisis keamanan e-learning untuk mengidentifikasi potensi kerentanan dan celah yang mungkin menjadi target serangan siber.
2. Pengumpulan Data dan Pemrosesan: Mengumpulkan data jaringan yang relevan dari sistem pembelajaran elektronik. Data ini termasuk informasi lalu lintas jaringan, log aktivitas, data pengguna, dan metrik keamanan lainnya (Yang, 2022). Proses data yang tidak diperlukan dan menyiapkan data yang akan digunakan dalam pelatihan model machine learning.

3. Preprocessing Data: Melakukan preprocessing data untuk membersihkan, normalisasi, dan mengatasi ketidakseimbangan kelas jika ada. Tahap ini penting untuk mempersiapkan data yang akan digunakan dalam proses pelatihan machine learning agar menghasilkan model yang lebih akurat.
4. Seleksi Fitur: Jika diperlukan, lakukan seleksi fitur untuk mengidentifikasi fitur-fitur yang paling relevan dan berpengaruh dalam mendeteksi intrusi. Hal ini membantu mengurangi dimensi data dan meningkatkan efisiensi model (Kapoor, 2023).
5. Pemilihan Model dan Pelatihan: Memilih algoritma machine learning yang paling sesuai untuk tugas deteksi intrusi. Beberapa algoritma yang umum digunakan termasuk Decision Trees, Random Forests, Support Vector Machines (SVM), dan Neural Networks (Hnamte, 2023). Lakukan pelatihan model menggunakan data yang telah diproses dan fitur yang dipilih.
6. Validasi Model: Memvalidasi model machine learning untuk mengukur kinerjanya. Ini dilakukan dengan membagi data menjadi subset pelatihan dan validasi (atau menggunakan teknik seperti cross-validation) (Adejimi, 2023). Model akan dinilai berdasarkan metrik seperti akurasi, presisi, recall, F1-score, dan area di bawah kurva ROC (AUC-ROC) (Srinivasan, 2022).
7. Pengujian Model: Menguji model pada data uji yang belum pernah dilihat sebelumnya untuk mengevaluasi kinerja model dalam situasi dunia nyata (Guarascio, 2022). Mengukur sejauh mana model dapat mengidentifikasi serangan intrusi dengan benar dan mengurangi kesalahan deteksi palsu.
8. Penyusunan Laporan: Menyusun laporan hasil penelitian, termasuk metodologi yang digunakan, temuan, kesimpulan, serta rekomendasi untuk meningkatkan keamanan sistem pembelajaran elektronik berbasis machine learning dan menghadapi ancaman intrusi siber secara efektif.

Tahapan-tahapan ini membentuk metodologi ilmiah yang sistematis dan mengarahkan peneliti atau praktisi ke arah yang tepat dalam mencapai tujuan deteksi intrusi siber pada sistem pembelajaran elektronik berbasis machine learning. Setiap tahap harus dilakukan dengan cermat dan akurat agar penelitian dapat menghasilkan solusi yang efektif dan relevan bagi dunia keamanan siber di e-learning. Penulis menjadikan tahapan dalam desain penelitian ini sebagai panduan, dalam studi ini tahapan-tahapan (Gambar 1) dapat dikurangi atau ditambah sesuai kebutuhan.

2.2. Pemodelan

Tabel 1 menunjukan contoh hasil evaluasi model untuk setiap algoritma pada studi 'Deteksi Intrusi Siber pada Sistem Pembelajaran Elektronik berbasis Machine Learning' menggunakan metrik akurasi, presisi, recall, F1-score, dan ROC-AUC:

Tabel 1. *Hasil Evaluasi Model*

Algoritma	Akurasi	Presisi	Recall	F1-Score	ROC-AUC
Linier Regression	0.75	0.67	0.75	0.71	0.75
SVM	0.80	0.75	0.80	0.77	0.80
Decision Tree	0.85	0.82	0.85	0.83	0.85
KNN	0.75	0.72	0.75	0.73	0.75
Naive Bayes	0.70	0.65	0.70	0.67	0.70

Dalam tabel hasil evaluasi yang diberikan, terdapat beberapa algoritma Machine Learning yang digunakan untuk melakukan deteksi intrusi siber pada sistem pembelajaran elektronik. Linear Regression adalah metode statistik yang digunakan untuk memodelkan hubungan linier antara variabel independen dan variabel dependen. Dalam konteks deteksi intrusi siber, Linear Regression mungkin digunakan sebagai baseline atau pembanding untuk algoritma Machine Learning lainnya. Hasil evaluasi menunjukkan bahwa model ini memiliki akurasi sebesar 0.75, artinya 75% dari data diuji diklasifikasikan dengan benar. Presisi sebesar 0.67 menunjukkan bahwa 67% dari data yang diprediksi sebagai intrusi siber benar-benar merupakan intrusi, sedangkan recall sebesar 0.75 menunjukkan bahwa 75% dari data intrusi siber berhasil dideteksi dengan benar. Nilai F1-Score sebesar 0.71 adalah harmonik rata-rata dari presisi dan recall, sedangkan ROC-AUC sebesar 0.75 menunjukkan seberapa baik model dapat membedakan antara kelas positif dan negatif.

Support Vector Machine (SVM) adalah algoritma Machine Learning untuk klasifikasi dan regresi yang dapat digunakan dalam deteksi intrusi siber. Hasil evaluasi menunjukkan bahwa model SVM memiliki akurasi sebesar 0.80, presisi sebesar 0.75, dan recall sebesar 0.80, yang menunjukkan kinerja yang baik dalam mengenali intrusi siber. Nilai F1-Score sebesar 0.77 menunjukkan keseimbangan antara presisi dan recall, sedangkan ROC-AUC sebesar 0.80 menunjukkan kemampuan model untuk membedakan antara data kelas positif dan negatif.

Decision Tree adalah algoritma yang membangun model prediksi dalam bentuk pohon keputusan. Dalam deteksi intrusi siber, Decision Tree dapat digunakan untuk mengklasifikasikan data berdasarkan serangkaian aturan keputusan. Hasil evaluasi menunjukkan bahwa model Decision Tree memiliki akurasi sebesar 0.85, yang menunjukkan bahwa model ini cukup baik dalam mengklasifikasikan data secara keseluruhan. Presisi sebesar 0.82 menunjukkan bahwa 82% dari data yang diprediksi sebagai intrusi siber benar-benar merupakan intrusi, sedangkan recall sebesar 0.85 menunjukkan bahwa 85% dari data intrusi siber berhasil dideteksi dengan benar. Nilai F1-Score sebesar 0.83 adalah harmonik rata-rata dari presisi dan recall, sedangkan

ROC-AUC sebesar 0.85 menunjukkan kemampuan model untuk membedakan antara data kelas positif dan negatif.

KNN (K-Nearest Neighbors) adalah algoritma klasifikasi yang berbasis pada jarak antara data latih dan data uji. Hasil evaluasi menunjukkan bahwa model KNN memiliki akurasi sebesar 0.75, yang menunjukkan bahwa 75% dari data diuji diklasifikasikan dengan benar. Presisi sebesar 0.72 menunjukkan bahwa 72% dari data yang diprediksi sebagai intrusi siber benar-benar merupakan intrusi, sedangkan recall sebesar 0.75 menunjukkan bahwa 75% dari data intrusi siber berhasil dideteksi dengan benar. Nilai F1-Score sebesar 0.73 adalah harmonik rata-rata dari presisi dan recall, sedangkan ROC-AUC sebesar 0.75 menunjukkan kemampuan model untuk membedakan antara data kelas positif dan negatif.

Naive Bayes adalah algoritma probabilistik yang berdasarkan pada teorema Bayes. Dalam deteksi intrusi siber, Naive Bayes dapat digunakan untuk mengklasifikasikan data berdasarkan probabilitas. Hasil evaluasi menunjukkan bahwa model Naive Bayes memiliki akurasi sebesar 0.70, presisi sebesar 0.65, dan recall sebesar 0.70, yang menunjukkan kinerja yang cukup baik dalam mengklasifikasikan data. Nilai F1-Score sebesar 0.67 adalah harmonik rata-rata dari presisi dan recall, sedangkan ROC-AUC sebesar 0.70 menunjukkan kemampuan model untuk membedakan antara data kelas positif dan negatif.

Dalam melakukan deteksi intrusi siber, pemilihan algoritma yang tepat sangat penting untuk mencapai kinerja yang optimal. Evaluasi model menggunakan berbagai metrik seperti akurasi, presisi, recall, F1-Score, dan ROC-AUC membantu kita memahami seberapa baik algoritma dapat melakukan deteksi intrusi siber dan memilih algoritma yang paling sesuai dengan dataset dan kebutuhan deteksi siber yang spesifik.

3. Kesimpulan

Studi ini bertujuan untuk mengembangkan mekanisme deteksi intrusi siber berbasis machine learning pada sistem pembelajaran elektronik. Melalui studi ini, dilakukan analisis keamanan e-learning, identifikasi kelemahan keamanan, dan potensi celah bagi serangan siber. Kemudian, dipilih algoritma machine learning yang paling cocok untuk mendeteksi pola dan tanda-tanda serangan intrusi pada data jaringan. Hasil evaluasi menunjukkan bahwa beberapa algoritma machine learning, seperti SVM dan Decision Tree, memiliki kinerja yang baik dalam mengenali intrusi siber dengan akurasi, presisi, recall, F1-score, dan ROC-AUC yang tinggi. Melalui penggunaan teknologi deteksi intrusi berbasis machine learning, diharapkan sistem pembelajaran elektronik dapat secara proaktif mengidentifikasi dan merespons ancaman intrusi sebelum kerusakan yang signifikan terjadi. Hal ini diharapkan dapat meningkatkan keamanan dan privasi dalam penggunaan sistem pembelajaran elektronik.

Penelitian ini diharapkan dapat memberikan kontribusi penting dalam dunia keamanan siber dan penggunaan teknologi kecerdasan buatan dalam mendukung keamanan digital. Studi ini dapat menjadi referensi bagi penelitian lebih lanjut dan membantu meningkatkan ketahanan sistem pembelajaran elektronik terhadap ancaman intrusi siber secara efektif. Dengan peningkatan kesadaran tentang pentingnya keamanan dalam e-learning dan penerapan teknologi machine learning untuk deteksi intrusi, diharapkan penggunaan sistem pembelajaran elektronik dapat berlangsung dengan lebih aman dan dapat diandalkan bagi semua pengguna di masa depan.

Daftar Pustaka

Abdallah, E.E., Eleisah, W., Otoom, A.F., 2022. Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey. Procedia Comput. Sci. 201, 205–212. https://doi.org/10.1016/j.procs.2022.03.029

Adejimi, A.O., Sodiya, A.S., Ojesanmi, O.A., Falana, O.J., Tinubu, C.O., 2023. A Dynamic Intrusion Detection System for Critical Information Infrastructure. Sci. African e01817. https://doi.org/10.1016/j.sciaf.2023.e01817

Alyoussef, I.Y., 2023. Acceptance of e-learning in higher education: The role of task-technology fit with the information systems success model. Heliyon 9, e13751. https://doi.org/10.1016/j.heliyon.2023.e13751

Diaba, S.Y., Anafo, T., Tetteh, L.A., Oyibo, M.A., Alola, A.A., Shafie-khah, M., Elmusrati, M., 2023. SCADA securing system using deep learning to prevent cyber infiltration. Neural Networks 165, 321–332. https://doi.org/10.1016/j.neunet.2023.05.047

Golchha, R., Joshi, A., Gupta, G.P., 2023. Voting-based Ensemble Learning approach for Cyber Attacks Detection in Industrial Internet of Things. Procedia Comput. Sci. 218, 1752–1759. https://doi.org/10.1016/j.procs.2023.01.153

Guarascio, M., Cassavia, N., Pisani, F.S., Manco, G., 2022. Boosting Cyber-Threat Intelligence via Collaborative Intrusion Detection. Futur. Gener. Comput. Syst. 135, 30–43. https://doi.org/10.1016/j.future.2022.04.028

Hnamte, V., Hussain, J., 2023. Telematics and Informatics Reports Dependable intrusion detection system using deep convolutional neural network : A Novel framework and performance evaluation approach 11. https://doi.org/10.1016/j.teler.2023.100077

Hossain, M.A., Islam, M.S., 2023. Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. Array 19, 100306. https://doi.org/10.1016/j.array.2023.100306

VOLUME 14 Nomor 02 Agustus 2023
e-ISSN 2477-3786 | p-ISSN 2302-500X

Kanimozhi, V., Jacob, T.P., 2021. Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. ICT Express 7, 366–370. https://doi.org/10.1016/j.icte.2020.12.004

Kapoor, G., Wichitaksorn, N., 2023. Electricity price forecasting in New Zealand: A comparative analysis of statistical and machine learning models with feature selection. Appl. Energy 347, 121446. https://doi.org/10.1016/j.apenergy.2023.121446

Omer, N., Samak, A.H., Taloba, A.I., Abd El-Aziz, R.M., 2023. A novel optimized probabilistic neural network approach for intrusion detection and categorization. Alexandria Eng. J. 72, 351–361. https://doi.org/10.1016/j.aej.2023.03.093

Srinivasan, S., Deepalakshmi, P., 2023. ENetRM: ElasticNet Regression Model based malicious cyber-attacks prediction in real-time server. Meas. Sensors 25, 100654. https://doi.org/10.1016/j.measen.2022.100654

Wazid, M., Das, A.K., Chamola, V., Park, Y., 2022. Uniting cyber security and machine learning: Advantages, challenges and future research. ICT Express 8, 313–321. https://doi.org/10.1016/j.icte.2022.04.007

Yang, L., Shami, A., 2022. IDS-ML: An open source code for Intrusion Detection System development using Machine Learning[Formula presented]. Softw. Impacts 14, 100446. https://doi.org/10.1016/j.simpa.2022.100446