Full Paper

PENERAPAN MODEL PEMBELAJARAN MESIN DALAM SISTEM CYBERSECURITY

Alfannisa Annurrallah Fajrin[1] Andi Maslan[2]
[1]Program Studi Teknik Informatika, Universitas Putera Batam, Indonesia
[1]Program Studi Teknik Informatika, Universitas Putera Batam, Indonesia

Informasi Artikel

Terbit: Juli 2025

Kata Kunci:

Cybersecurity
Malware
Jaringan
Machine Learning

ABSTRAK

Keamanan jaringan atau cybersecurity sangat penting dalam dunia digital,karena seseorang yang melakukan penyerangan bisa megirim kode jahat seperti malware ke berbagai file yang bisa merugikan orang lain. Ada berbagai jenis malware atau program yang cukup berbahaya bisa ditemukan di internet. Banyak hal yang harus diperhatikan dalam perlindungan system, seperti jaringan dan keamanan lainnya yang merupakan fakrot penting karena berkaitan dengan pengoperasian sistem informasi agar bisa mencegah ancaman terhadap kerusakan sistem. Malware merupakan program software yang berbahaya pagi pengguna komputer. Serangan kerusakan yang sering terjadi seperti Ping of Death, UDP Flood, Smurf Attack dan lainnya. Model pembelajaran mesin atau biasnaya disebut dengan Machine Learning akan melakukan pendekatan untuk mendeteksi serangan malware ini yang dianalisis secara statistik menggunakan algoritma genetika. Dari pembelajaran mesin ini akan dilakukan secara kategori untuk serangan malware yang terjadi dengan cara eksplorasi data,training dan testing, maka akan terlihat tingkat akurasi dari *neural networknya.*

Corresponding Author:

Alfannisa Annurrallah Fajrin,
Email: asykharit1302@gmail.com

1. PENDAHULUAN

Malware telah menjadi risiko yang sangat besar di dunia saat ini. Ada berbagai jenis malware atau program berbahaya yang ditemukan di internet. Malware adalah program atau perangkat lunak berbahaya yang terbukti sangat berbahaya bagi komputer pengguna. Sistem pengguna dapat terpengaruh dalam beberapa cara. Solusi yang diusulkan menggunakan berbagai teknik pembelajaran mesin untuk mendeteksi apakah file yang diunduh dari internet mengandung malware atau tidak. Jenis-jenis malware yang tersedia saat ini seperti Adware, Trojan, Backdoors, Unknown, Multidrop, Rbot, Spam, dan Ransomware [1]. Selain itu malware sangat membahayakan system keamanan data komputer dan menurunkan performa jaringan dengan menyerang masuk ke sistem komputer melalui port-port terbuka yang tidak digunakan dalam sistem jaringan [2].

Trojan dan spyware akan menginfeksi komputer melalui banyak cara seperti email, menyamar seolah software yang baik, berupa link atau file lainnya. Malware ini dapat melihat data dan file penting bahkan aktivitas pada perangkat pengguna di platform Android serta menyusup lewat layanan distribusi aplikasi (app store), baik resmi (Google Play Store) maupun milik pihak ketiga, dengan menyamar menjadi aplikasi sah seperti pemutar video, permainan dan utilitas system. Dan baru-baru ini juga ditemukan file yang dianggap malware yang menyamarkan file PDF menjadi Pdf, jika pengguna tidak jeli pada kedua jenis file tersebut maka besar kemungkinan jenis malware ini akan mencuri data-data mobile banking, dan akibatnya merugikan nasabah bank.

Dalam mendeteksi serangan Malware banyak algoritma yang dapat digunakan seperti decision tree, random forest, support vector machine dan algoritma ini sangat baik untuk klasifikasi cyber-threat actor (CTA) [3]. Berdasarkan analisis yang dilakukan terhadap fitur-fitur ini, file akan diklasifikasikan sebagai berbahaya atau tidak berbahaya. Model dilatih tentang berbagai fitur yang memungkinkan mereka mempelajari cara mengklasifikasikan file. Model-model setelah pelatihan yang tepat akan dibandingkan satu sama lain berdasarkan berbagai kriteria. Perbandingan ini dilakukan dengan bantuan kumpulan data Validasi dan Pengujian. Terakhir, model dengan akurasi terbaik akan dipilih. Proses ini membantu mengidentifikasi semua jenis malware yang dapat berdampak buruk pada sistem pengguna setelah terinfeksi. Pendekatan yang digunakan disini akan mampu mendeteksi malware seperti Adware, Trojan, Backdoors, Unknown, Multidrop, Rbot, Spam, dan Ransomware.

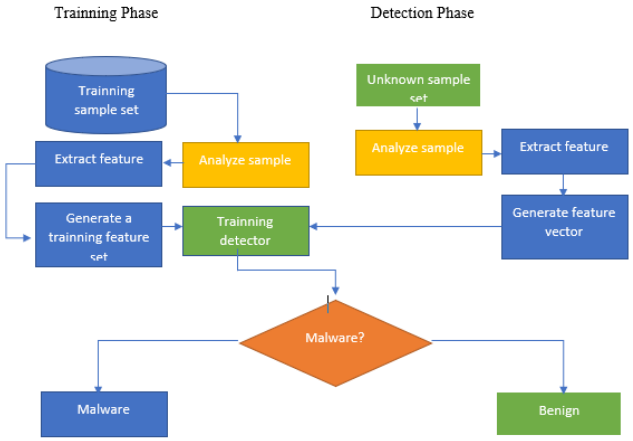
Penelitian yang dilakukan [4] berfokus pada deteksi malware dinamis. Malware semakin berubah, sehingga mengarah pada penggunaan teknik pendeteksian malware dinamis dalam studi penelitian ini. Setiap hari muncul gelombang baru program perangkat lunak berbahaya yang mengancam keamanan online dengan mengeksploitasi kerentanan di Internet. Proliferasi perangkat lunak berbahaya telah membuat pemeriksaan heuristik manual terhadap analisis malware menjadi tidak efektif.

Deteksi malware berbasis Automatic behaviour-based malware menggunakan algoritma pembelajaran mesin dianggap sebagai inovasi yang mengubah keadaan. Ancaman secara otomatis dievaluasi berdasarkan perilakunya dalam lingkungan simulasi, dan laporan dibuat [5]. Catatan ini diubah menjadi sparse vector models untuk digunakan dalam upaya pembelajaran mesin lebih lanjut. Pengklasifikasi yang digunakan untuk mensintesis hasil penelitian ini antara lain kNN, DT, RF, AdaBoost, SGD, pohon ekstra dan pengklasifikasi Gaussian NB.

2. METODE PENELITIAN

2.1 Desain Penelitian

Agar bisa mendapatkan hasil yang hierarki, maka perlu dilakukan dalam penelitian ini harus menggunakan tahapan yang sesuai dengan metodenya. Dalam pembelajaran mesin memerlukan pemahaman yang lengkap agar bisa memproses dari awal hingga akhir, seperti berikut :



Gambar 2.1 Desain Penelitian

1. Proses yang pertama dilakukan adalah mengolah data yang disimpan menggunakan kode biner lalu menggunakan software khusus untuk mengelola executable.
2. Membangun serangkaian fitur yang lebih kecil dari serangkaian fitur yang lebih besar; teknik ini biasanya digunakan untuk mempertahankan tingkat akurasi yang sama dengan menggunakan fitur yang lebih sedikit agar menyempurnakan kumpulan data fitur yang paling digunakan agar meningkatkan akurasi.
3. Pemilihan fitur merupakan proses penting untuk meningkatkan akurasi, menyederhanakan model, dan mengurangi overfitting. Strategi klasifikasi fitur digunakan mengidentifikasi kode berbahaya dalam perangkat lunak. Karena teknik pemeringkatan fitur sangat efektif dalam memilih fitur yang tepat untuk membangun model deteksi malware.

2.2 Variabel Penelitian

Metode pembelajaran terawasi merupakan teknik yang memanfaatkan contoh data yang sudah dilabeli untuk melatih sebuah model atau pengklasifikasi. Model ini kemudian mampu mengenali pola pada data baru dan mengelompokkan data tersebut ke dalam dua kategori yang sudah ditentukan sebelumnya. Biasanya, model ini dapat dijelaskan dalam bentuk kumpulan aturan [7]. Dalam konteks sistem deteksi intrusi, teknik pembelajaran terawasi memungkinkan pembuatan aturan yang dapat menyaring data berdasarkan fitur-fitur tertentu. Dengan demikian, sistem dapat mengklasifikasikan data baru, misalnya, sebagai 'aman' atau 'serangan'.

Klasifikasi merupakan proses untuk menentukan atau menetapkan suatu objek ke dalam salah satu kategori yang telah ditetapkan sebelumnya. Algoritma klasifikasi digunakan untuk mengotomatisasi dan memperluas gagasan metode berbasis heuristik [8]. Proses pembelajaran di sini bertujuan untuk membentuk suatu fungsi atau model klasifikasi, yang dapat memetakan setiap kombinasi atribut (input) ke dalam kelas tertentu (output) yang sudah ditentukan sebelumnya. Data input terdiri dari sekumpulan data (training set), di mana setiap data memiliki sejumlah atribut, dan salah satunya berperan sebagai penanda kelas. Tujuan utama dari proses ini adalah membangun sebuah model yang mampu memprediksi kelas berdasarkan nilai-nilai atribut lainnya. Model klasifikasi ini kemudian dapat digunakan untuk berbagai keperluan, seperti:

(i) Pemodelan deskriptif adalah perangkat menggambar untuk membedakan objek dari kelas yang berbeda.
(ii) Pemodelan prediktif digunakan untuk memprediksi label kelas untuk catatan yang tidak dikenal atau tidak dikenal.

Matriks kebingungan membantu menganalisis seberapa baik pengklasifikasi mengenali tupel dari kelas yang berbeda [9]. Nilai True-Positive dan True-Negative memberikan informasi ketika pengklasifikasi mengklasifikasikan data dengan benar. Sebaliknya, False-Positive dan False-Negative memberikan informasi ketika pengklasifikasi salah dalam mengklasifikasikan data [10]. Lalu lintas jaringan yang normal ditandai dengan nilai positif, sedangkan lalu lintas yang terindikasi malware ditandai dengan nilai negatif. Informasi terkait klasifikasi ini disajikan dalam bentuk tabel matriks yang diperlihatkan pada Tabel berikut :

Tabel 2.1 Confusion matrix

Prediction / Actual	DDoS	Normal
DDoS	TP	FN
Normal	FP	TN

Dari confusion matrix, akurasi, presisi, recall, dan F-measure dapat diukur untuk menganalisis kinerja algoritma machine learning dalam mengklasifikasikan untuk mendeteksi serangan malware dengan persamaan dibawah ini :

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$\text{Precession} = \frac{TP}{TP+FN} \quad (2)$$

$$\text{Recall} = \frac{TN}{TN+FN} \quad (3)$$

F-Measure = 2 * (Precision * Recall) / (Precision + Recall)

Algoritma ini bekerja dengan membentuk fungsi atau model klasifikasi yang sesuai berdasarkan data contoh yang diberikan. Reinforcement Learning merupakan metode pembelajaran yang mempelajari strategi atau kebijakan untuk menentukan tindakan terbaik dengan mengamati kondisi lingkungan. Setiap tindakan yang diambil akan memengaruhi lingkungan, dan sebagai gantinya, lingkungan memberikan umpan balik yang membantu algoritma dalam proses belajar.

Transduksi merupakan metode yang memprediksi hasil baru dengan memanfaatkan data pelatihan (baik input maupun output) serta data pengujian yang tersedia selama proses pembelajaran. Terakhir, pada pendekatan learning to learn, algoritma berusaha mempelajari kemampuan induktifnya melalui pengalaman sebelumnya. Subbagian ini membahas beberapa teknik pembelajaran mesin yang paling umum digunakan dalam mendeteksi serangan atau anomali pada lalu lintas jaringan

3. HASIL DAN ANALISIS

Dari total fitur yang telah didapatkan maka selanjutnya dilakukan pengelompokan fitur utama dari kumpulan dataset malware.

3.1. Extract Feature

Pengelompokkan fitur utama dengan tujuan agar lebih mudah untuk melakukan klasifikasi, seperti tabel dibawah ini :

Tabel 3.1 Category Feature

No	Feature Utama	Feature Dataset	Jumlah Feature
1	DDoS Feature	e_cblp, e_maxalloc, e_sp, e_lfanew, SizeOfCode, AddressOfEntryPoint, BaseOfCode, BaseOfData, SizeOfStackReserve, SizeOfHeapCommit, E_text	10
2	File Feature	FH_char0, FH_char1, FH_char2, FH_char3, FH_char4, FH_char5, FH_char6, FH_char7, FH_char8, OH_DLLchar0, OH_DLLchar1, OH_DLLchar2, OH_DLLchar3,	13
3	Optional Feature	e_cp, e_cparhdr, MajorLinkerVersion, MinorLinkerVersion, SizeOfUninitializedData, ImageBase, SectionAlignment, FileAlignment, MajorOperatingSystemVersion MinorOperatingSystemVersion, MajorImageVersion, MinorImageVersion, SizeOfImage, SizeOfHeaders,	14

3.2. Feature Selection

Hasil seleksi fitur pada penelitian ini menggunakan metode Weight By Correlation, dan menghasilkan nilai kolerasi data. Berikut urutan nilai kolerasi yang telah didapatkan :

Tabel 3.2 Nilai Kolerasi

No	Nilai Correlation	Feature
1	0.6081	FH_char12
2	0.5428	OH_DLLchar2
3	0.5189	OH_DLLchar0
4	0.5140	Fileinfo
5	0.5119	FH_char0
6	0.3526	FH_char3
7	0.3476	FH_char2
8	0.3400	MinorSubsystemVersion
9	0.3321	MajorSubsystemVersion

Berdasarkan grafik dan hasil dar tabel diatas maka feature terbaik dalam menggunakan pembelajaran mesin untuk keamanan data dari virus atau malware adalah *FH_char12, OH_DLLchar2, OH_DLLchar0* dengan nilai *weight correlation* masing-masing adalah 0.6081, 0.5428 dan 0.5189.

Evaluasi performace model Machine Learning dalam mendeteksi serangan Malware adalah sebagai berikut :

Tabel 3.5 : DDOS Feature

	true Normal	true Benign	class precision
pred. Normal	2176	578	79.01%
pred. Benign	312	2144	87.30%
class recall	87.46%	78.77%	

Dari tabel diatas dijelaskan bahwa paket data normal untuk DDoS Feature dengan jumlah feature sebanyak 18 yang terdeteksi sebagai paket normal sebanyak 2176 paket dan paket malware sebanyak 2144 paket, dan paket data normal terdeteksi sebagai malware sebanyak 312 dan paket malware terdeteksi sebagai paket normal sebanyak 578 dengan Tingkat akurasi mencapai 82.92%. Algoritma yang digunakan untuk mendeteksi paket data apakah normal atau tidak menggunakan algoritma SVM.

Hasil evaluasi performace model Pembelajaran Mesin dalam memprediksi serangan Malware adalah sebagai berikut:

Tabel 3.5 Hasil Compare

Algoritma	**Category Atribut**	**Number of Feature**	**Accuracy**	**Recall**	**Precision**
KNN	DDoS Feature	18	91.17	91.37	91.71
	File Feature	26	63.19	30.20	97.93
	Optional Feature	24	86.07	76.31	96.25
	All Feature	68	91.21	91.29	91.85
SVM	DDoS Feature	18	82.92	78.76	87.28
	File Feature	26	87.75	85.32	94.60
	Optional Feature	24	78.56	78.77	79.93
	All Feature	68	88.12	99.63	81.70
Neural Network	DDoS Feature	18	91.96	92.17	92.48
	File Feature	26	93.36	95.52	92.11
	Optional Feature	24	87.41	88.87	87.76
	All Feature	68	96.91	97.35	96.78

3.2. Pembahasan

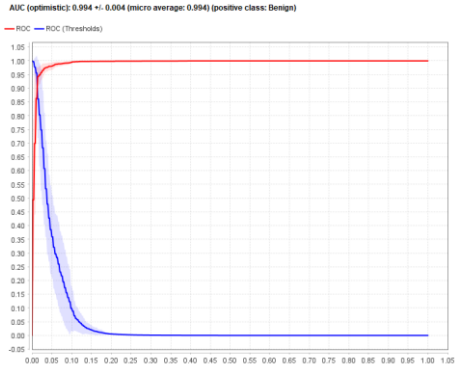
Klasifikasi pada dataset malware maka diperlukan proses Machine Learning, dengan langsung awal melakukan pengcategorian atribut pada semua feature dataset. Kategori feature yang terbentuk yaitu DdoS Feature, File Feature, Optimal Feature dan kombinasi feature. Hasil pemisahan feature-fature pada penelitian ini dengan rincian sebagai berikut:

Tabel 3.7 Atribut

Algoritma	**Category Atribut**	**Number of Feature**
KNN	DDoS Feature	18
	File Feature	26
	Optional Feature	24
	All Feature	68
SVM	DDoS Feature	18
	File Feature	26
	Optional Feature	24

	All Feature	68
Neural Network	DDoS Feature	18
	File Feature	26
	Optional Feature	24
	All Feature	68

Hasil klasifikasi menggambarkan bahwa algoritma *Neural Network* menjadi algoritma klasifikasi terbaik dengan tingkat akurasi mencapai 96.91, dengan nlai ROC seperti pada gambar berikut ini:



Gambar 3.1 ROC NN

Berdasarkan tabel diatas, algoritma terbaik dalam mendeteksi suatu paket malware atau tidak adalah *Neural Network* untuk category kombinasi feature dengan tingkat akurasi 96.91%, Recall 97.35% dan Precision 96.78%.

4. KESIMPULAN

Dari uraian dan penjelasan dari bab-bab sebelumnya, maka dapat disimpulkan bahwa Penerapan Model Pembelajaran Mesin Dalam Sistem Cybersecurity bisa dilihat dari jumlah paket data pada dataset ini sebanyak 5212 dengan total atribut sebanyak 69 dan satu class. Tahap penelitian dilakukan mulai dari persiapan dataset, extract feature, Explorasi Data, trainning dan testing serta pembuatan model. Model ini dibuat menggunakan tiga algoritma machine learning. Berdasarkan hasil pencarian pun Algoritma terbaik dalam mendeteksi suatu paket malware atau tidak adalah *Neural Network* untuk category kombinasi feature dengan tingkat akurasi 96.91%, Recall 97.35% dan Precision 96.78%.

DAFTAR PUSTAKA

[1] Akhtar, M. S., & Feng, T. (2022). Malware Analysis and Detection Using Machine Learning Algorithms. *Symmetry*, *14*(11). https://doi.org/10.3390/sym14112304

[2] Aldwairi, M., Mardini, W., & Alhowaide, A. (2018). Anomaly payload signature generation system based on efficient tokenization methodology. *International Journal on Communications Antenna and Propagation*, *8*(5), 421–429. https://doi.org/10.15866/irecap.v8i5.12794

[3] Alkasassbeh, M. (2017). An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods. *Journal of Theoretical and Applied Information Technology*, *95*(22), 5962–5976.

[4] Arelakis, A. (2015). *MSc THESIS Efficient Pre-filtering Techniques for Packet Inspection*. *September*.

[5] Damanik, A. R., Seta, H. B., & Theresiawati, T. (2023). Analisis Trojan Dan Spyware Menggunakan Metode Hybrid Analysis. *Jurnal Ilmiah Matrik*, *25*(1), 89–97. https://doi.org/10.33557/jurnalmatrik.v25i1.2327

[6] Dieta Wahyu Asry, Eko Siswanto, Dendy Kurniawan, & Haris Ihsanil Huda. (2023). Deteksi Malware Statis Menggunakan Deep *Neural Network*s Pada Portable Executable. *Teknik: Jurnal Ilmu Teknik Dan Informatika*, *3*(1), 19–34. https://doi.org/10.51903/teknik.v3i1.325

[7] Farhana, N., Firdaus, A., Darmawan, M. F., & Ab Razak, M. F. (2023). Evaluation of Boruta algorithm in

DDoS detection. *Egyptian Informatics Journal*, *24*(1), 27–42. https://doi.org/10.1016/j.eij.2022.10.005

[8] Arora, R., Singh, A., Pareek, H., & Edara, U. R. (2013). A heuristics-based static analysis approach for detecting packed PE binaries. *International Journal of Security and Its Applications*, *7*(5), 257–268. https://doi.org/10.14257/ijsia.2013.7.5.24

[9] Bouchlaghem, Y., Akhiat, Y., & Amjad, S. (2022). Feature Selection: A Review and Comparative Study. *E3S Web of Conferences*, *351*(May). https://doi.org/10.1051/e3sconf/202235101046

[10] Hairani, T. (2018). *Botnet Detection Using K-Nearest Neighbor Algorithm*.