Tersedia online di www.sciencedirect.com

Sains Langsung

Procedia Ilmu Komputer 218 (2023) 57–66

Procedia Computer Science

www.elsevier.com/locate/procedia

Konferensi Internasional tentang Pembelajaran Mesin dan Rekayasa Data

Deteksi Serangan Jaringan menggunakan Machine Learning dan Deep Learning Model Pembelajaran

Dhanya KA[A] Sulakshan Vajipayajula[B] Kartik Srinivasan[C] Anjali Tibrewal[,C], T. Sentil Kumar[D], T. Gireesh Kumar[D]

[A] *TIFAC-CORE dalam Keamanan Siber, Sekolah Teknik Amrita, Coimbatore, Amrita Vishwa Vidyapeetham, India.*

[B] *Arsitek STSM, IBM Security, IBM.*

[C] *Arsitek Senior, IBM Security, IBM India Pvt Ltd*

[D] *Departemen Ilmu Komputer dan Teknik, Sekolah Komputasi Amrita, Coimbatore, Amrita Vishwa Vidyapeetham, India.*

Abstrak

Sistem deteksi intrusi jaringan berbasis anomali sangat penting dalam mendeteksi serangan jaringan. Model pembelajaran mesin dan pembelajaran mendalam yang kuat untuk mengidentifikasi jenis intrusi dan serangan jaringan diusulkan dalam makalah ini. Model yang diusulkan telah bereksperimen dengan dataset UNSW-NB15 yang terdiri dari 49 fitur untuk sembilan ditidaksampel serangan yang berbeda. Pengklasifikasi Pohon Keputusan menghasilkan akurasi terbaik sebesar 99,05% dibandingkan dengan model ensemble - Hutan acak (98,96%), Adaboost (97,87%), dan XGBoost (98,08%). Pengklasifikasi K-Nearest Neighbour dilatih untuk berbagai nilai K dan kinerja terbaik diperoleh untuk K=7 dengan akurasi 95,58%. Model Pembelajaran Mendalam dengan dua lapisan padat dengan aktivasi ReLU dan lapisan padat ketiga dengan fungsi aktivasi Sigmoid dirancang untuk klasifikasi biner dan menghasilkan akurasi yang baik sebesar 98,44% dengan pengoptimal ADAM, Rasio Pemisahan Pelatihan-Uji 80:20. Eksploitasi serangan jaringan dideteksi dengan akurasi 95% oleh XGBoost, serangan Fuzzers dengan akurasi 90% oleh Hutan Acak, serangan Umum dengan akurasi 99% oleh Hutan Acak, dan serangan Pengintaian dengan 79% oleh Pohon Keputusan. Semua fitur relevan dan kuat dalam deteksi serangan jaringan, yang menghilangkan persyaratan pemilihan fitur.

Kata kunci: Keamanan jaringan; Hutan Acak; Deep Multi-Layer Perceptron; Adaboost; XGBoost

*Penulis korespondensi.Telp.: +91-894-332-0379

Alamat email: alamat email tgireeshkumar@cb.amrita.edu

1877-0509
10.1016/j.procs.2022.12.401

1. Pendahuluan

Peningkatan pesat dalam jaringan data disebabkan oleh Internet of Things (IoT), layanan berbasis cloud, dan perangkat jaringan kolosal [31]. Seiring dengan data jaringan, serangan meningkat secara eksponensial, menjadi ancaman signifikan terhadap keamanan jaringan. Keamanan jaringan dapat ditingkatkan dengan menambahkan lebih banyak perangkat keamanan tetapi tidak dapat memastikan perlindungan lengkap. Keamanan jaringan tidak hanya perlu mengatasi ancaman saat ini tetapi juga ancaman di masa mendatang. Sistem Deteksi Intrusi Jaringan (NIDS) yang ada menyediakan pertahanan keamanan berlapis untuk jaringan di tingkat sistem, jaringan, aplikasi, dan transmisi [12]. Keamanan berlapis menjamin bahwa lapisan selanjutnya akan menghentikan penyerang yang mengalahkan satu lapisan pertahanan. Tantangan signifikan dari NIDS baru-baru ini adalah akurasi yang tidak memadai, perilaku dinamis trafik jaringantidak adac, serangan jaringan frekuensi rendah, kemampuan beradaptasi terhadap jaringan yang ditentukan perangkat lunak, volume besar data yang disimpan dan dikirim, dan berbagai perangkat akses jaringan.

Sebagian besar NIDS yang ada adalah sistem deteksi berbasis tanda tangan atau berbasis anomali. NIDS berbasis tanda tangan hanya menangani daftar ancaman yang diketahui, dan indikator kompriminya [13]. Ia memiliki kecepatan pemrosesan yang tinggi dan akurasi yang tinggi untuk serangan yang diketahui. Namun, ia gagal mengidentifikasi serangan zero-day dan secara tidak perlu memunculkan peringatan apa pun hasilnya, seperti cacing Windows yang mencoba menyerang sistem Linux. Ia tidak praktis untuk serangan internal dan bergantung pada sistem operasi, versi, dan aplikasi [16]. NIDS berbasis anomali dapat mendeteksi perilaku mencurigakan baru yang menyimpang dari perilaku normal. NIDS berbasis anomali bagus dalam mendeteksi serangan zero-day. Namun, peningkatan kemungkinan positif palsu menghasilkan waktu dan sumber daya tambahan untuk menyelidiki semua peringatan terhadap potensi ancaman [31].

NIDS berbasis Pembelajaran Mesin [18] dapat mempelajari model klasifikasi dari data pelatihan. Pelatihan dengan sampel data jaringan yang luas dan beragam membuat model tersebut tangguh untuk mengklasifikasikan serangan ke dalam kategori yang memungkinkan. Model pembelajaran mendalam juga memainkan peran penting dalam NIDS dengan mempelajari perilaku serangan dari fitur jaringan. Model ini juga menghilangkan persyaratan untuk korelasi, pemilihan, dan representasi fitur [29]. Model pembelajaran mendalam etidak ada mempelajari perilaku jaringan tersembunyi secara efisien dantidak adamengidentifikasi serangan secara efisien dengan lebih sedikit alarm palsu [32], [30].Sayangnya, penyerang menggunakan teknik canggih untuk mengeksploitasi kerentanan sumber daya komputasi. Di sisi lain, jumlah infrastruktur komputasi yang disusupi meningkat secara eksponensial. NIDS yang tangguh menggunakan teknik pembelajaran mesin dan pembelajaran mendalam dengan akurasi tinggi dan F-Measure diusulkan dalam makalah ini. Kontribusi signifikan dari karya yang diusulkan dirangkum sebagai berikut.

1. Kami mengevaluasi pentingnya berbagai model pembelajaran mesin klasik dan ensemble dalam mengidentifikasi serangan jaringan yang canggih.
2. Pembelajar malas, model K-Nearest Neighbor dilatih untuk beberapa nilai K, dan hasilnya dibandingkan dan dievaluasi.tidak efektivitas dalam mengidentifikasi serangan jaringan.
3. Arsitektur Perceptron multi-layer yang mendalam diusulkan untuk meningkatkan kinerja klasifikasi sistem deteksi intrusi jaringan, dan hasilnya dibandingkan dengan model pembelajaran mesin.

Makalah yang tersisa disusun sebagai berikut. Bagian II mencakup latar belakang dan literatur. Arsitektur model deteksi serangan diusulkan di Bagian III. Hasil dan pembahasan disertakan di Bagian IV. Terakhir, Bagian V menyimpulkan karya penelitian.

2. Tinjauan Pustaka

2.1. Serangan jaringan

Serangan pada jaringan komputer sangatlah merusak dan dapattidakmengganggu fungsi seluruh sistem dengan membaca, merusak, dan mencuri data [11]. Serangan didahului oleh aktivitas pra-intrusi seperti pemindaian port dan IP Spoofing. Fungsi utama NIDS adalah pemindaian pakettidak adang, mengidentifikasi tanda-tanda serangan, mengidentifikasi serangan, dan melaporkan detail serangan. Serangan diidentifikasi dengan menangkap fitur dari alamat IP sumber dan tujuan, port, detail protokol, detail header, dll. Berdasarkan sifat serangan, serangan dapat diklasifikasikan sebagai pasif dan aktif [12]. Serangan pasif bisa berbasis sistem atau berbasis jaringan, dimana penyerang secara diam-diam memonitor jaringan dan mencoba

mempelajari data rahasia. Serangan pasif sulit dipantau. Penyerang aktif merusak semua langkah keamanan dan masuk ke jaringan dengan memanfaatkan celah keamanan, menyamar sebagai sistem tepercaya, atau mencuri kata sandi.

2.1.1. Serangan Fuzzer

Serangan fuzzer memasukkan sejumlah besar data acak ke sistem untuk membuatnya gagal dan menemukan bug [27]. Dapat mengidentifikasi kerentanan perangkat lunak dan sistem serta celah dalam jaringan dan sistem operasi.

2.1.2. Analisis

Menembus aplikasi web dengan pemindaian port, email spam, dan skrip web [22]. Model pembelajaran mesin dapat mengidentifikasi pemindaian port dengan mengalahkan IP Spoofing, mengubah frekuensi pemindaian port, dan mengubah urutan pemindaian port. Email spam berbahaya karena menyebarkan kode berbahaya, menjalankan penipuan phishing, dan menghasilkan uang. Model pembelajaran mesin menggunakan penyaringan email berbasis konten, yang mengidentifikasi beberapa kata kunci yang dapat menghasilkan varians tinggi antara spam dan email yang sah [6]. Penetrasi kode HTML yang berbahaya memiliki banyak konsekuensi, seperti terungkapnya cookie, sehingga mengubah konten halaman korban.

2.1.3. Pintu Belakang

Serangan backdoor membahayakan mekanisme keamanan dan mengakses komputer dan datanya [22]. Serangan ini menargetkan privasi dan ketersediaan sumber daya komputasi bagi pengguna [25].

2.1.4. Serangan DoS

Serangan DoS membuat sumber daya jaringan tidak tersedia bagi pengguna dengan menangguhkan layanan [22]. Verisign melaporkan peningkatan besar dalam frekuensi dan kompleksitas serangan DoS yang menuntut NID kuat menggunakan pembelajaran mesin dan model pembelajaran mendalam.

2.1.5. Eksploitasi

Penyerang mengeksploitasi kerentanan perangkat lunak atau sistem operasi, mengambil alih sumber daya komputer atau data jaringan, dan mengakibatkan kerusakan atau malfungsi sistem. Eksploitasi zero-day memanfaatkan kerentanan perangkat lunak yang tidak diketahui oleh vendor.

2.1.6. Umum

Serangan generik bekerja terhadap cipher blok tanpa mempertimbangkan struktur internal cipher blok [22]. Karena panjang kunci dan blok terbatas, semua cipher blok berada di bawah ancaman serangan generik. Serangan generik dideteksi dengan memilih parameter eksternal yang sesuai.tidakSerangan generik yang berbeda pada cipher blok adalah pencarian kunci menyeluruh, serangan kamus, serangan tabel pelangi, dll.7].

2.1.7. Pengintaian

Serangan pengintaian mengumpulkan semua informasi yang mungkin tentang sistem target sebelum meluncurkan serangan yang sebenarnya, dan bertindak sebagai alat persiapan untuk serangan yang sebenarnya. Tiga jenis utama serangan pengintaian adalah pengintaian sosial, publik, dan perangkat lunak. Selama serangan ini, informasi dikumpulkan oleh paket snitidak adang, pemindaian port, menyapu ping, dan pertanyaan mengenai informasi internet [28[Bahasa Indonesia]

2.1.8. Kode shell

Shellcode adalah potongan kode kecil yang digunakan sebagai muatan dalam eksploitasi kerentanan perangkat lunak. Shellcode menjalankan penerjemah perintah yang secara interaktif memasukkan perintah yang akan dieksekusi pada sistem yang rentan dan membaca kembali output [3]. Serangan shellcode dapat dideteksi menggunakan heuristik run-time yang mewakili operasi tingkat mesin.

2.1.9. Cacing

Cacing mereplikasi dan menyebar ke sumber daya komputasi lain dengan memanfaatkan kegagalan keamanannya. Peringatan dini dan waktu reaksi yang lebih singkat untuk tindakan pencegahan adalah dua fitur yang diharapkan dari sistem deteksi cacing. Sistem ini mempertimbangkan konten dan format muatan, header paket, lalu lintas jaringan, dan banyak lagi.tidak adac, dan memantau perilaku host untuk mendeteksi cacing [19[Bahasa Indonesia]

2.2. Deteksi berbasis tanda tangan

Almutairi et al., mengusulkan NIDS empat komponen yang terdiri dari Sistem Deteksi Intrusi, database tanda tangan sering, agen pembaruan, dan database tanda tangan pelengkap [1]. IDS mengekstrak tanda tangan dari paket jaringan, membandingkannya dengan basis data tanda tangan, dan memicu peringatan jika terjadi kecocokan. Sistem empat komponen ini memastikan deteksi serangan yang lebih awal dan akurat dengan lebih sedikit positif palsu. Serangan dengan tanda tangan yang jarang juga tertangkap dengan tanda tangan yang disimpan dalam basis data pelengkap. Minimalisasi alarm palsu merupakan masalah utama yang harus diatasi dalam deteksi berbasis tanda tangan dan dapat diselesaikan menggunakan peningkatan tanda tangan, tanda tangan status penuh, dan tanda tangan kerentanan [14].

2.3. NIDS Berbasis Anomali

Moustafa dkk., melakukan analisis statistik terhadap observasi dan fitur menggunakan uji Kolmogorov-Smirnov, Multivariate skewness, dan Multivariate kurtosis. Korelasi fitur terbimbing dengan Gain Ratio dan korelasi tak terbimbing dengan koefisien korelasi Pearson.tidak adaEfisien juga dilakukan untuk mengukur relevansi antar fitur. Akhirnya, kompleksitas dataset UNSW-NB15 dievaluasi dengan pengklasifikasi yang ada dengan metrik akurasi dan tingkat alarm palsu. Pengklasifikasi pohon keputusan bekerja dengan baik dengan akurasi 85,56% dan tingkat alarm palsu 15,78% [23]. Meftah dkk., mengusulkan NIDS berbasis anomali dengan teknik pembelajaran mesin. Hutan acak dengan validasi silang 10 kali lipat untuk menetapkan indeks signifikansi fitur dalam mengurangi ketidakmurnian di seluruh hutan. Fitur utama dari Dataset UNSW-NB15 adalah ct_dst_src ltm, ct srv dst, ct dst sport ltm, ct src dport ltm, ct srv src. Support vector machine dengan akurasi 82,11% mengungguli Logistic Regression dan Gradient Boost Machine dalam model klasifikasi biner untuk deteksi serangan. Untuk mengidentifikasi jenis serangan, model multiklasifikasi dengan Decision Tree C5.0, mengungguli Naive Bayes dan Support vector machine [20].

Peng et al., mengusulkan Deep Neural Network (DNN) dengan lima lapisan tersembunyi untuk mengidentifikasi serangan (Normal, DoS, Probe Categories, R2L, U2R) dengan Dataset NSL-KDD dan membandingkan kinerjanya dengan model Machine Learning (Support Vector Machines, Random Forest, Linear Regression Models). DNN menghasilkan hasil yang memuaskan untuk mengidentifikasi kategori Normal, DoS, dan Prob. SVM bekerja dengan baik dalam mendeteksi serangan Normal dan empat serangan lainnya. Random forest dan linear regression juga bekerja dengan baik dalam mengidentifikasi serangan jaringan [24].

Penelitian sebelumnya pada dataset UNSW-NB15 mencakup pembelajaran model pembelajaran mesin dan pembelajaran mendalam pada fitur-fitur terpilih, yang menurunkan kinerja model karena kardinalitas set fitur hanya 47 yang tidak semuanya besar dan relevansi setiap fitur sangat signifikan. Mengenai jaringan saraf dalam, karya-karya literatur sangat terbatas dan karya-karya tersebut hanya membahas sejumlah serangan yang terbatas. Dalam penelitian ini, empat model pembelajaran mesin klasik, tiga model pembelajaran mesin ensemble, dan model persepsi multi-lapis dalam dirancang untuk mengidentifikasi serangan jaringan.

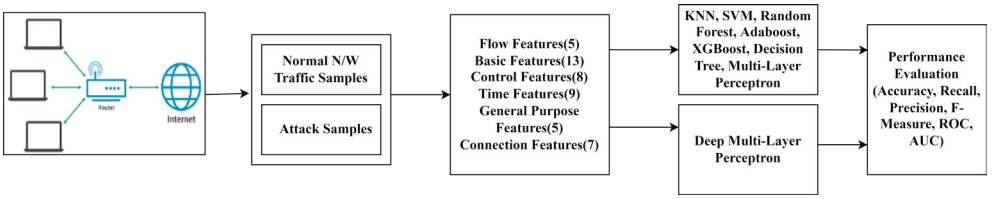
3. Metodologi yang Diusulkan

3.1 Perumusan Masalah

Biarkan dataset (A_1Bahasa Indonesia:A_2,.....A_9Bahasa Indonesia:N) terdiri dari Analisis(A_1), DoS(A_2), Eksploitasi(A_3), Pengacau(A_4), Umum(A_5), Pengintaian(A_6), Cacing(A_7), Pintu Belakang(A_8), Kode Shell(A_9) dan sampel Normal(N). Setiap sampelS_{Saya}terdiri dari 49 Fitur (F_1Bahasa Indonesia:F_2,....F_{47}Bahasa Indonesia:TBahasa Indonesia:C) Di mana$T$adalah jenis serangan Label dan$A$adalah Jaringan Tratidak adac Label. $T\in$ {*Analisa*Bahasa Indonesia:*Serangan DoS*Bahasa Indonesia: *Mengeksploitasi*Bahasa Indonesia:*Pengacau*Bahasa Indonesia:*Umum*Bahasa Indonesia:*Pengintaian*Bahasa Indonesia:*Cacing*Bahasa Indonesia:*Pintu Belakang*Bahasa Indonesia:*Kode neraka S*Bahasa Indonesia:*Normal*}Dan$C\in$ {*Normal*Bahasa Indonesia:*Menyerang*Masalahnya adalah membangun model klasifikasi yang mengidentifikasi sampel jaringan apa pun$S_i$sebagai serangan atau normal. Jika sampel serangan diklasifikasikan lebih lanjutS_iArsitektur yang kuat untuk mendeteksi serangan jaringan digambarkan pada Gambar1.

3.2. Kumpulan data

Metode yang diusulkan telah diujicobakan pada Dataset UNSW-NB15 [22], yang dibuat oleh Pusat Keamanan Siber Australia, terdiri dari sembilan keluarga serangan dan 49 fitur (5 fitur Aliran, 13 fitur dasar,



Gambar 1. Arsitektur yang diusulkan

delapan fitur kontrol, sembilan fitur waktu, lima fitur tujuan umum tambahan yang dihasilkan, tujuh fitur koneksi tambahan yang dihasilkan, dua fitur berlabel). Fitur-fitur ini mewakili trafik jaringan kontemporertidak adapola c dikumpulkan dari header paket, komunikasi klien ke server, dan server ke klien [21]. Dataset terdiri dari 2540044 sampel dengan jaringan Normal (2218761), Fuzzers (24246), Analysis (2677), Backdoors (2329), DoS (16353), Exploits (44525), Generic (215481), Reconnaissance (13987), Shellcode (1511) dan Worms (174).tidak adaC.

3.3 Model Klasifikasi

Model klasifikasi biner yang digunakan untuk mengidentifikasi serangan jaringan adalah Support Vector Machine (SVM), Adaboost, XGBoost, Random Forest, K-Nearest Neighbour (KNN), Decision Tree (DT), Multi-Layer Perceptron (MLP), dan Deep Multi-Layer Perceptron (Deep MLP) [26]. SVM adalah pengklasifikasi pembelajaran statistik yang menggunakan hiper-bidang multidimensi untuk memisahkan pola serangan jaringan dari lintasan normal.tidak adapola c [33]. SVM dengan kernel linear mendukung set fitur yang luas dan pelatihan yang cepat. KNN adalah pengklasifikasi berbasis memori yang memprediksi label kelas dari sampel yang tidak diketahui berdasarkan label kelas mayoritas dari K-tetangga terdekat [5]. Klasifikasi DT adalah model pengambilan keputusan multitahap yang sesuai dengan data numerik dan nominal [2]. Model ini menghasilkan keputusan cepat karena terdiri dari sejumlah pernyataan kondisional sederhana yang bersarang. Pengklasifikasi Random Forest adalah model klasifikasi ensemble yang melatih sekumpulan pohon CART dengan bagging untuk membuat prediksi. Model ini secara acak memilih fitur untuk menetapkan keputusan pada node dan menggunakan estimasi kesalahan out-of-bag dan keputusan kelas akhir dengan merata-ratakan probabilitas penugasan kelas pohon individual [4]. Adaboost membangun model prediktif yang kuat dengan meningkatkan beberapa model yang lebih lemah. Ini adalah pengklasifikasi terbaik yang sudah ada tanpa mengubah parameter dan tidak mudah mengalami over-fitting [9]. Extreme Gradient (XG) adalah pengklasifikasi ensemble yang menerapkan boosting ke pengklasifikasi lemah melalui implementasi paralel. Ia juga mendukung pemangkasan pohon, penanganan data yang hilang, menghindari over-fitting, dan optimasi perangkat keras [10].

Jaringan saraf dalam sangat penting dalam memetakan fitur masukan ke label kelas. Dua model, Multi-Layer Perceptron (MLP) dan Deep MLP, diimplementasikan untuk memprediksi label kelas dengan algoritma penyesuaian bobot propagasi balik. Nilai parameter MLP adalah lbfgs quasi-newton untuk pengoptimal, kekuatan neuron tersembunyi 15, parameter istilah regularisasi penalti alpha dengan nilai 1e-5, dan nilai status acak 1. Deep MLP yang diusulkan terdiri dari 2 lapisan padat dengan aktivasi Relu diikuti oleh lapisan padat dengan fungsi aktivasi sigmoid. Lapisan padat dengan aktivasi Relu menghasilkan campuran masukan yang akurat dari fitur, dan aktivasi sigmoid memprediksi kelas target berdasarkan keluaran dari lapisan sebelumnya [17].

3.4. Metrik Evaluasi

Metrik yang digunakan untuk mengevaluasi sistem yang diusulkan adalah Akurasi, Presisi, Recall, F1-Measure, Receiver Operating Characteristics Curve (ROC), dan Area under ROC (AUC) [8]. Matriks konfusi adalah matriks 2*2 yang terdiri dari nilai True positive (TP), False negative (FN), False positive (FP) dan True negative (TN). True Positive menunjukkan jumlah sampel serangan yang diklasifikasikan sebagai serangan. False Negative menunjukkan jumlah sampel serangan yang salah diklasifikasikan sebagai normal. False Positive menunjukkan jumlah sampel normal yang salah diklasifikasikan, dan true negative menunjukkan jumlah sampel normal yang diklasifikasikan sebagai normal. Accuracy menunjukkan persentase sampel yang diklasifikasikan dengan benar. Recall menunjukkan rasio serangan yang diklasifikasikan dengan benar terhadap jumlah total sampel serangan. Precision menunjukkan sampel serangan aktual dalam serangan yang diklasifikasikan. Metrik kualitatif dan kuantitatif F1-Measure menunjukkan rata-rata harmonik precision dan recall.

4. Hasil dan Pembahasan

Sistem deteksi intrusi jaringan yang diusulkan diimplementasikan pada Ubuntu 20.04.4 dengan dukungan Intel core 11*th*prosesor i7 generasi terbaru, RAM 16 GB, dan HDD 1 TB. Model pembelajaran mesin dan pembelajaran mendalam diimplementasikan dalam bahasa python dengan pustaka Keras 2.3.1 dan TensorFlow 2.2.0.

4.1. Kinerja Model Pembelajaran Mesin

Kinerja berbagai model pembelajaran mesin dalam deteksi serangan jaringan ditunjukkan pada Tabel1dan Gambar2Decision Tree menghasilkan akurasi terbaik sebesar 99,05% dan F1-Measure sebesar 0,99 untuk mengidentifikasi serangan jaringan. Hasil yang dihasilkan oleh SVM dengan akurasi sebesar 95,17% dan F1-Measure 0,94 juga tidak dapat diabaikan. Model KNN dilatih untuk ditidaktetangga K yang berbeda (2,3,4,5,6,7,8,9), dan akurasi terbaik adalah 95,58% yang dihasilkan untuk K = 7. Fitur yang digunakan untuk pelatihan model sangat relevan dan dapat membuat banyak varian antara serangan dan trafik jaringan biasa.tidak adac. Jadi pohon keputusan sederhana berkinerja lebih baik daripada pembelajaran ensemble seperti bagging di random forest dan boosting di Adaboost dan XGBoost. Model hyperplane multidimensi SVM berkinerja dengan recall 0,93, yang menunjukkan ine modeltidak adaefisiensi dalam mengidentifikasi serangan (True Positives). Kinerja KNN ditunjukkan pada Tabel2yang menggambarkan bahwa model tersebut tidak kuat dalam mengidentifikasi serangan dan lebih cenderung mengklasifikasikan serangan biasatidak adac sebagai serangan (positif palsu).

Tabel 1. Hasil: Model Deteksi Serangan Jaringan

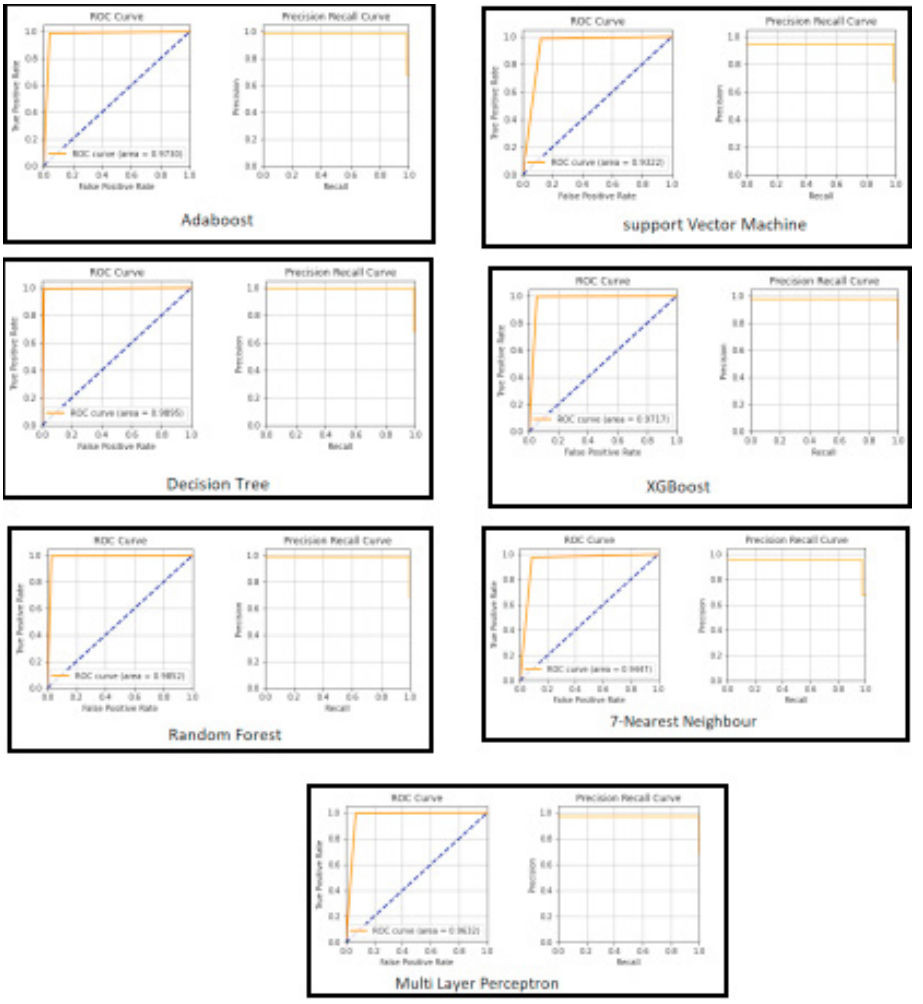
Model	Ketepatan	Presisi	Mengingat	F1-Ukur
Bahasa Indonesia: SVM	95.17	0,96	0,93	0,94
Pohon Keputusan	99.05	0,99	0,99	0,99
Hutan Acak	98.96	0,99	0,99	0,99
Penguat Ada	97.87	0,98	0,97	0,98
XGBoost	98.08	0,98	0,97	0,98
Bahasa Inggris MLP	97.47	0,98	0,96	0,97

Tabel 2. Hasil: Hasil KNN

Model	Ketepatan	Presisi	Mengingat	F1-Ukur
2-NN	94.51	0,93	0,95	0,94
3-NN	95.47	0,95	0,95	0,95
4-NN	Nomor 95.12	0,94	0,95	0,94
5-NN	95.56	0,95	0,95	0,95
6-NN	95.31	0,94	0,95	0,95
7-NN	95.58	0,95	0,94	0,95
8-NN	95.48	0,95	0,95	0,95
9-NN	95.57	0,95	0,94	0,95

4.2. Kinerja Model Pembelajaran Mendalam

Kinerja Deep Multi-Layer Perceptron ditunjukkan pada Tabel3sangat baik dengan akurasi tinggi 98,44% dan F1-Measure 0,98 untuk pengoptimal Adam dan rasio Train-Test 80:20. Kinerja Adam lebih baik daripada pengoptimal Stochastic Gradient Descent. Model Deep MLP dengan pengoptimal Adam menghasilkan hasil terbaik untuk pemisahan Train-Test 80:20 karena mewakili normal sistem alami dan trafik jaringan serangan.tidak adaSistem deteksi anomali jaringan yang diusulkan oleh Moustafa et al., memperoleh akurasi sebesar 85,56% untuk Decision Tree dan 81,34% untuk Artificial Neural Network [23]. Namun sistem yang diusulkan menghasilkan akurasi sebesar 99,05% untuk pengklasifikasi Decision Tree dan 97,47% untuk Multilayer Perceptron. Peningkatan kinerja sistem yang diusulkan menunjukkan bahwa semua fitur dari dataset UNSW-NB15 sangat relevan dan penerapan pemilihan fitur dalam dataset mengurangi akurasi. Meftah dkk. mengusulkan NIDS dengan pemilihan fitur Random Forest dan eliminasi fitur Rekursif [20]. Setelah pemilihan dan eliminasi fitur, klasifikasi dengan SVM menghasilkan akurasi sebesar 82,11%. Sistem yang diusulkan dengan SVM menghasilkan akurasi sebesar 95,17% tanpa pemilihan fitur.



Gambar 2. Kurva ROC dan Precision-Recall (Model ML)

Tabel 3. Hasil Perceptron Multi Layer Dalam

Pengoptimal	Kereta:Uji	Ketepatan	Presisi	Mengingat	F1-Ukur	AUC
SGD	90 : 10	98.19	0,98	0,98	0,98	0,976 tahun
SGD	80 : 20	97.68	0,98	0,97	0,97	0,971 tahun
SGD	70 : 30	97.99	0,98	0,98	0,98	0,975
SGD	60 : 40	97.82	0,98	0,97	0,97	0,972 tahun
ADAM	90 : 10	Nomor 98.11	0,98	0,98	0,98	0,975
ADAM	80 : 20	98.44	0,98	0,98	0,98	0,981
ADAM	70 : 30	98.36	0,98	0,98	0,98	0,98
ADAM	60 : 40	98.35	0,98	0,98	0,98	0,979 tahun

4.3. Kinerja Model Deteksi Serangan

Kinerja model pembelajaran mesin untuk mengidentifikasi sembilan serangan jaringan ditunjukkan pada Tabel4, Meja5, Meja6, Meja7, Meja8, Meja9, Meja10, Meja11dan Tabel12Model pembelajaran mesin lemah dalam mengidentifikasi serangan jaringan seperti analisis (Random Forest 23%), DoS (Random Forest 35%), worm (XGBoost 46%), Backdoor (ADABoost 53%) dan Shellcode (Random Forest 65%) dengan fitur UNSW-NB15. XGBoost adalah model terbaik dengan akurasi 95% dan Recall 0,95 untuk deteksi eksploitasi. Random Forest bagus dalam mengidentifikasi serangan Fuzzers dengan 90%

akurasi dan serangan generik dengan akurasi 99%. Kinerja model pembelajaran mesin untuk serangan Pengintaian memuaskan dengan akurasi 79% untuk Pohon Keputusan. Kinerja Hutan Acak untuk mengidentifikasi serangan Fuzzer lebih baik daripada model yang diusulkan oleh [20[Bahasa Indonesia]15].

Tabel 4. Hasil Analisis Deteksi Serangan

Model	Presisi	Mengingat	F1-Ukur	Ketepatan
Hutan Acak	0.24	0.23	0.23	0.23
XGBoost	0.73	0.19	0.3	0.19
Peningkatan ADA	0,04	0,01	0,01	0,01
Bahasa Inggris MLP	0.63	0.12	0.21	0.12
Pohon Keputusan	0.5	0.12	0.19	0.12
7-NN	0.48	0.16	0.24	0.16

Tabel 5. Hasil Deteksi Serangan DoS

Model	Presisi	Mengingat	F1-Ukur	Ketepatan
Hutan Acak	0.37	0,35	0.36	0,35
XGBoost	0.41	0,03	0,05	0,03
Peningkatan ADA	0,09	0,02	0,04	0,02
Bahasa Inggris MLP	0.39	0,09	0.14	0,09
Pohon Keputusan	0.00	0.00	0.00	0.00
7-NN	0.29	0.29	0.29	0.29

Tabel 6. Hasil Deteksi Serangan Eksploitasi

Model	Presisi	Mengingat	F1-Ukur	Ketepatan
Hutan Acak	0,74	0,79	0.76	0,79
XGBoost	0.61	0,95	0,75	0,95
Peningkatan ADA	0.56	0,35	0.43	0,35
Bahasa Inggris MLP	0.61	0,89	0.72	0,89
Pohon Keputusan	0.53	0.92	0.67	0.92
7-NN	0.62	0.73	0.67	0.73

Tabel 7. Hasil Deteksi Serangan Fuzzer

Model	Presisi	Mengingat	F1-Ukur	Ketepatan
Hutan Acak	0.9	0.9	0.9	0,90
XGBoost	0,93	0,89	0,91	0,89
Peningkatan ADA	0.68	0.6	0.64	0.60
Bahasa Inggris MLP	0.86	0.84	0,85	0.84
Pohon Keputusan	0,94	0.11	0.19	0.11
7-NN	0.76	0.81	0,78	0.82

Tabel 8. Hasil Deteksi Serangan Umum

Model	Presisi	Mengingat	F1-Ukur	Ketepatan
Hutan Acak	0,99	0,98	0,99	0,98
XGBoost	1.00	0,98	0,99	0,98
Peningkatan ADA	0,03	0.00	0.00	0.00
Bahasa Inggris MLP	1.00	0,98	0,99	0,98
Pohon Keputusan	1.00	0,98	0,99	0,98
7-NN	1.00	0,98	0,99	0,98

Tabel 9. Hasil Deteksi Serangan Pengintaian

Model	Presisi	Mengingat	F1-Ukur	Ketepatan
Hutan Acak	0,79	0.76	0,78	0.76
XGBoost	0,90	0,75	0.82	0,75
Peningkatan ADA	0.54	0,45	0.49	0,45
Bahasa Inggris MLP	0.73	0.71	0.72	0.71
Pohon Keputusan	0.41	0,79	0.54	0,79
7-NN	0.66	0.51	0,58	0.51

Tabel 10. Hasil Deteksi Serangan Worms

Model	Presisi	Mengingat	F1-Ukur	Ketepatan
Hutan Acak	0.73	0.21	0.32	0.21
XGBoost	0,90	0.46	0.61	0.46
Peningkatan ADA	0.00	0,08	0.00	0,08
Bahasa Inggris MLP	0.00	0.00	0.00	0.00
Pohon Keputusan	0.00	0.00	0.00	0.00
7-NN	1.00	0,05	0.10	0.00

Tabel 11. Hasil Deteksi Serangan Backdoor

Model	Presisi	Mengingat	F1-Ukur	Ketepatan
Hutan Acak	0.23	0.22	0.23	0.22
XGBoost	0.73	0.23	0,35	0.23
Peningkatan ADA	0,04	0.53	0,07	0.53
Bahasa Inggris MLP	0.00	0.00	0.00	0.00
Pohon Keputusan	0.00	0.00	0.00	0.00
7-NN	0.51	0,04	0,07	0,04

Tabel 12. Hasil Deteksi Serangan Shell Code

Model	Presisi	Mengingat	F1-Ukur	Ketepatan
Hutan Acak	0.69	0,65	0.67	0,65
XGBoost	0.66	0.49	0.56	0.49
Peningkatan ADA	0.71	0.29	0.41	0.29
Bahasa Inggris MLP	0,70	0.20	0.31	0.20
Pohon Keputusan	1.00	0,01	0,02	0,01
7-NN	0.51	0.14	0.22	0.14

5. Kesimpulan

Makalah ini membahas model machine learning dan deep learning untuk NIDS. Decision Tree menghasilkan performa terbaik dengan 99,05% dibandingkan dengan model ensemble Random Forest, Adaboost, dan XGBoost. Fitur dataset UNSW-NB15 sangat relevan dan tangguh dalam mengidentifikasi serangan jaringan. Model machine learning KNN dengan 7 tetangga menghasilkan akurasi 95,58%. Model deep learning dengan ADAM optimizer dan 80:20 Train-Test split menghasilkan akurasi 98,44% dengan True Positives tinggi dan False negatives rendah. Model machine learning jugatidakefektif dalam mengidentifikasi jenis serangan seperti Exploits, Fuzzers, serangan Generic, dan Reconnaissance. Fitur UNSW-NB15 tidak kuat dalam menghasilkan varians untuk serangan DoS, Worms, Backdoors, dan Shellcode. Sebagai arah masa depan, model pembelajaran mendalam seperti jaringan Convolutional Neural (CNN) satu dimensi dapat dilatih secara langsung dengan string yang ada dalam lalu lintas jaringan.tidak adac file pcap untuk mengidentifikasi serangan. CNN menghilangkan persyaratan rekayasa fitur yang kompleks dengan mengekstraksi fitur secara otomatis dari file pcap dengan lapisan konvolusionalnya. Salah satu metode yang muncul untuk serangan jaringan dan deteksi malware adalah menggunakan representasi Visualisasi. Biner file pcap jaringan dapat direpresentasikan dalam skala abu-abu, RGB, atau gambar Markov. Gambar-gambar ini digunakan untuk melatih CNN dua dimensi, yang dapat mendeteksi serangan jaringan dengan banyak kovarians.

Referensi

[1] Almutairi, AH, Abdelmajeed, NT, 2017. Sistem deteksi intrusi berbasis tanda tangan yang inovatif: Pemrosesan paralel dan basis data yang diminimalkan, dalam: Konferensi Internasional 2017 tentang Batasan dan Kemajuan dalam Ilmu Data (FADS), IEEE. hlm. 114–119.

[2] Ammar, A., et al., 2015. Pengklasifikasi pohon keputusan untuk penandaan prioritas deteksi intrusi. Jurnal Komputer dan Komunikasi 3, 52.

[3] Arce, I., 2004. Generasi shellcode. Keamanan & privasi IEEE 2, 72–76.

[4] Belgiu, M., Drăguţ, L., 2016. Hutan acak dalam penginderaan jauh: Tinjauan aplikasi dan arah masa depan. Jurnal fotogrametri dan penginderaan jauh ISPRS 114, 24–31.

[5] Cunningham, P., Delany, SJ, 2021. pengklasifikasi k-tetangga terdekat-tutorial. Survei Komputasi ACM (CSUR) 54, 1–25.

[6] Dada, EG, Bassi, JS, Chiroma, H., Adetunmbi, AO, Ajibuwa, OE, et al., 2019. Pembelajaran mesin untuk penyaringan spam email: tinjauan, pendekatan, dan masalah penelitian terbuka. Heliyon 5, e01802.

[7] De Canniere, C., Biryukov, A., Preneel, B., 2006. Pengantar kriptoanalisis cipher blok. Prosiding IEEE 94, 346–356.

[8] Dhanya, K., Dheesha, O., Gireesh Kumar, T., Vinod, P., 2020. Deteksi malware seluler yang dikaburkan dengan model pembelajaran mesin dan pembelajaran mendalam, dalam: Simposium tentang Algoritma Pembelajaran Mesin dan Metaheuristik, dan Aplikasi, Springer. hlm. 221–231.

[9] Freund, Y., Schapire, RE, 1997. Generalisasi teoritis keputusan pembelajaran daring dan penerapannya pada peningkatan. Jurnal ilmu komputer dan sistem 55, 119–139.

[10] Friedman, JH, 2001. Aproksimasi fungsi Greedy: mesin penguat gradien. Annals of statistics, 1189–1232.

[11] Gandhi, M., Srivatsa, S., 2008. Mendeteksi dan mencegah serangan menggunakan sistem deteksi intrusi jaringan. Jurnal Internasional Ilmu Komputer dan Keamanan 2, 49–60.

[12] Garuba, M., Liu, C., Fraites, D., 2008. Teknik intrusi: Studi perbandingan sistem deteksi intrusi jaringan, dalam: Konferensi Internasional Kelima tentang Teknologi Informasi: Generasi Baru (itng 2008), IEEE. hlm. 592–598.

[13] Gascon, H., Orfila, A., Blasco, J., 2011. Analisis penundaan pembaruan dalam sistem deteksi intrusi jaringan berbasis tanda tangan. Komputer & Keamanan 30, 613–624.

[14] Hubballi, N., Suryanarayanan, V., 2014. Teknik meminimalkan alarm palsu dalam sistem deteksi intrusi berbasis tanda tangan: Sebuah survei. Komunikasi Komputer 49, 1–17.

[15] Jing, D., Chen, HB, 2019. Deteksi intrusi jaringan berbasis Svm untuk dataset unsw-nb15, dalam: konferensi internasional IEEE ke-13 tahun 2019 tentang ASIC (ASICON), IEEE. hlm. 1–4.

[16] Kumar, V., Sangwan, OP, 2012. Sistem deteksi intrusi berbasis tanda tangan menggunakan snort. Jurnal Internasional Aplikasi Komputer & Teknologi Informasi 1, 35–41.

[17] Lee, B., Amaresh, S., Green, C., Engels, D., 2018. Studi perbandingan model pembelajaran mendalam untuk deteksi intrusi jaringan. SMU Data Science Review 1, 8.

[18] Lee, CH, Su, YY, Lin, YC, Lee, SJ, 2017. Deteksi intrusi jaringan berbasis pembelajaran mesin, dalam: konferensi internasional IEEE ke-2 tahun 2017 tentang kecerdasan komputasi dan aplikasi (ICCIA), IEEE. hlm. 79–83.

[19] Li, P., Salour, M., Su, X., 2008. Survei deteksi dan penahanan cacing internet. Survei & Tutorial Komunikasi IEEE 10, 20–35.

[20] Meftah, S., Rachidi, T., Assem, N., 2019. Deteksi intrusi berbasis jaringan menggunakan dataset unsw-nb15. Jurnal Internasional Komputasi dan Sistem Digital 8, 478–487.

[21] Moustafa, N., Slay, J., 2015a. Fitur signifikan dari kumpulan data unsw-nb15 dan kdd99 untuk sistem deteksi intrusi jaringan, dalam: Lokakarya internasional ke-4 tahun 2015 tentang membangun kumpulan data analisis dan mengumpulkan hasil pengalaman untuk keamanan (BADGERS), IEEE. hlm. 25–31.

[22] Moustafa, N., Slay, J., 2015b. Unsw-nb15: kumpulan data komprehensif untuk sistem deteksi intrusi jaringan (kumpulan data jaringan unsw-nb15), dalam: konferensi sistem informasi dan komunikasi militer 2015 (MilCIS), IEEE. hlm. 1–6.

[23] Moustafa, N., Slay, J., 2016. Evaluasi sistem deteksi anomali jaringan: Analisis statistik kumpulan data unsw-nb15 dan perbandingannya dengan kumpulan data kdd99. Jurnal Keamanan Informasi: Perspektif Global 25, 18–31.

[24] Peng, Y., Su, J., Shi, X., Zhao, B., 2019. Mengevaluasi sistem deteksi intrusi jaringan berbasis pembelajaran mendalam di lingkungan yang merugikan, dalam: Konferensi Internasional IEEE ke-9 tahun 2019 tentang Informasi Elektronik dan Komunikasi Darurat (ICEIEC), IEEE. hlm. 61–66.

[25] Rieger, P., Nguyen, TD, Miettinen, M., Sadeghi, AR, 2022. Deepsight: Mitigasi serangan backdoor dalam pembelajaran terfederasi melalui inspeksi model yang mendalam. arXiv pracetak arXiv:2201.00763 .

[26] Sugunan, K., Gireesh Kumar, T., Dhanya, K., 2018. Analisis statis dan dinamis untuk deteksi malware android, dalam: Kemajuan dalam Big Data dan Cloud Computing. Springer, hlm. 147–155.

[27] Thanh, HN, Van Lang, T., 2020. Mengevaluasi etidakefektivitas pengklasifikasi ensemble saat mendeteksi serangan fuzzer pada dataset unsw-nb15. Jurnal Ilmu Komputer dan Sibernetika 36, 173–185.

[28] Uma, M., Padmavathi, G., 2013. Survei mengenai berbagai serangan cyber dan klasifikasinya. Int. J. Netw. Secur. 15, 390–396.

[29] Vinayakumar, R., Alazab, M., Soman, K., Poornachandran, P., Al-Nemrat, A., Venkatraman, S., 2019. Pendekatan pembelajaran mendalam untuk sistem deteksi intrusi cerdas. IEEE Access 7, 41525–41550.

[30] Vinayakumar, R., Soman, K., Poornachandran, P., 2017. Menerapkan jaringan saraf konvolusional untuk deteksi intrusi jaringan, dalam: Konferensi Internasional 2017 tentang Kemajuan dalam Komputasi, Komunikasi dan Informatika (ICACCI), IEEE. hlm. 1222–1228.

[31] Wang, W., Jian, S., Tan, Y., Wu, Q., Huang, C., 2022. Sistem deteksi intrusi jaringan berbasis pembelajaran representasi dengan menangkap interaksi fitur eksplisit dan implisit. Komputer & Keamanan 112, 102537.

[32] Yang, H., Cheng, L., Chuah, MC, 2019. Deteksi intrusi jaringan berbasis pembelajaran mendalam untuk sistem scada, dalam: Konferensi IEEE 2019 tentang Komunikasi dan Keamanan Jaringan (CNS), IEEE. hlm. 1–7.

[33] Yang, Y., Li, J., Yang, Y., 2015. Penelitian metode pengklasifikasi svm cepat, dalam: konferensi komputer internasional ke-12 tahun 2015 tentang teknologi media aktif wavelet dan pemrosesan informasi (ICCWAMTIP), IEEE. hlm. 121–124.