

Analisis Kinerja Algoritma Machine Learning Dalam Deteksi Anomali Jaringan

Sintia Situmorang

Universitas Islam Negeri Sumatera Utara, FITK, Pendidikan Matematika

Email : tumorangsintia@gmail.com

Yahfizham

Universitas Islam Negeri Sumatera Utara, FITK

Email : Yahfizham@uinsu.ac.id

Abstract. Network anomaly detection is a situation that occurs in network traffic that causes conditions to become abnormal. This research aims to analyze the performance of various machine learning algorithms in network anomaly detection and compare the performance of single classifier algorithms with ensemble learning. This ensemble learning technique has advantages such as increased accuracy and performance, can reduce the risk of overfitting and underfitting by using different subsets and features of data, and can turn weak learning into strong learning. However, on the other hand, this ensemble learning technique also has disadvantages in its use, namely that this ensemble method may not work well with high variance models, as the ensemble method may not be optimized for anomaly detection and that this method can be computationally expensive and time consuming due to the need to train and store multiple models. Some of the techniques used are deep learning, eager learning, lazy learning, bagging, feature selection, boosting, and stacking. In addition to this, this machine learning algorithm has weaknesses, including if any of the data used is incomplete, it will result in inaccurate completion data, making the programming process quite time-consuming. This research can help develop a more effective and efficient network anomaly detection system. The results of this research show that using ensemble learning and feature selection techniques can improve anomaly detection performance by reducing the processing time of redundant data and classification, as well as increasing precision values.

Keywords : algorithm, anomaly, machine learning.

Abstrak. Deteksi anomali jaringan adalah suatu keadaan yang terjadi pada suatu lalu lintas jaringan yang menyebabkan kondisi menjadi tidak normal . Penelitian ini bertujuan untuk menganalisis kinerja berbagai algoritma machine learning dalam mendeteksi anomali jaringan dan membandingkan kinerja algoritma single classifier dengan pembelajaran ensemble. Teknik pembelajaran ensemble ini memiliki kelebihan seperti peningkatan akurasi dan kinerja, dapat mengurangi resiko overfitting dan underfitting dengan menggunakan sub kumpulan dan fitur data yang berbeda, serta dapat mengubah pembelajaran yang lemah menjadi pembelajaran yang kuat. Namun disisi lain, teknik pembelajaran ensemble ini juga memiliki kekurangan dalam pemakaiannya yaitu metode ensemble ini mungkin tidak bekerja dengan baik dengan model variansi tinggi, metode ensemble mungkin tidak dioptimalkan untuk deteksi anomaly, dan metode ini bisa mahal secara komputasi dan memakan waktu karena perlunya pelatihan dan penyimpanan beberapa model. Beberapa teknik yang digunakan yaitu deep learning, eager learning, lazy learning, bagging, feature selection, boosting, dan stacking. Disamping itu algoritma machine learning ini memiliki kelemahan, antara lain apabila salah satu dari data yang digunakan tidak lengkap maka akan mengakibatkan tidak akuratnya data penyelesaian, sehingga proses pemrograman membutuhkan waktu yang cukup lama. Penelitian ini dapat membantu untuk mengembangkan system deteksi anomali jaringan yang lebih efisien dan efektif. Hasil penelitian ini menunjukkan bahwa penggunaan teknik ensemble learning dan feature selection dapat meningkatkan kinerja deteksi anomaly dengan mengurangi redundant data dan waktu proses klasifikasi serta peningkatan nilai akurasi.

Kata kunci : algoritma, anomaly, pembelajaran mesin.

Received September 23, 2023; Revised Oktober 30, 2023; Accepted November 10, 2023

* Sintia Situmorang, tumorangsintia@gmail.com

LATAR BELAKANG

Algoritma berasal dari kata *algorism*, yang diambil dari nama seorang penulis terkenal arab ia adalah Abu Ja'far Muhammad Ibnu Musa Al- Khuwarizmi, yang menciptakan sebuah buku yang berjudul kitab aljabar wal-muqabala (buku pemugaran dan pengurangan). Maka Algoritma adalah prosedur komputasi langkah-langkah yang terdefinisi dengan baik yang menggunakan beberapa nilai sebagai masukan dan menghasilkan beberapa nilai yang disebut keluaran atau suatu masalah. Dalam bidang computer, algoritma sering dimanfaatkan sebagai proses pengambilan keputusan untuk menyelesaikan suatu masalah, serta merancang suatu system agar berjalan dengan baik. Sedangkan program adalah suatu kumpulan instruksi-instruksi yang bisa disebut dengan sourc code yang dibuat oleh program. Dalam algortima ada yang disebut dengan algoritma single classifer yaitu metode yang menggunakan model tunggal untuk membuat prediksi atau klasifikasi. Algoritma jenis ini dapat digunakan dengan menggunakan pembelajaran ensemble (ansambel). Pembelajaran ensemble adalah teknik pembelajaran machine yang menggabungkan prediksi beberapa model peningkatan. Pembelajaran ini dapat dicapai dengan beberapa cara, seperti mengadopsi distribusi untuk menghasilkan basis pembelajaran yang berbeda dengan orang lain atau biasa disebut dengan Bagging, menggabungkan beberapa klasifikasi individu untuk membentuk klasifikasi yang baru dengan prediksi yang lebih bagus dan akurat (biasa disebut penumpukan), dan metode boosting dimana pembelajaran berfokus pada penggabungan pengeluaran dasar.

Perkembangan internet dan jaringan yang terjadi di masa sekarang ini memberikan keuntungan dan kemudahan kepada para pengguna computer untuk dapat berbagi sumber daya informasi dalam suatu jaringan local maupun internasional. Namun disisi lain, perkembangan internet yang semakin pesat ini berdampak bahaya pada anak atau peserta didik maupun di kalangan remaja saat ini. Seperti berbagi macam serangan yang berusaha mencari celah dari system keamanan jaringan computer yang sedang digunakan yang dapat mengakibatkan kerusakan data atau bahkan kerusakan pada perangkat hardware. Ada banyak cara yang dapat dilakukan untuk mengatasi masalah keamanan jaringan dan gangguan system, salah satunya dengan menggunakan IDS (intrusion detection system). Salah satu jaringan yang menggunakan IDS ini adalah deteksi anomaly.

Deteksi anomali jaringan adalah suatu keadaan yang terjadi pada suatu lalu lintas jaringan yang menyebabkan kondisi menjadi tidak normal. Beberapa algoritma machine learning yangdigunakan dalam penelitian ini adalah Eager Learning, Ensemble learning, dan lazy learning. Penelitian ini bertujuan untuk menyelidiki dan membandingkan kinerja berbagai

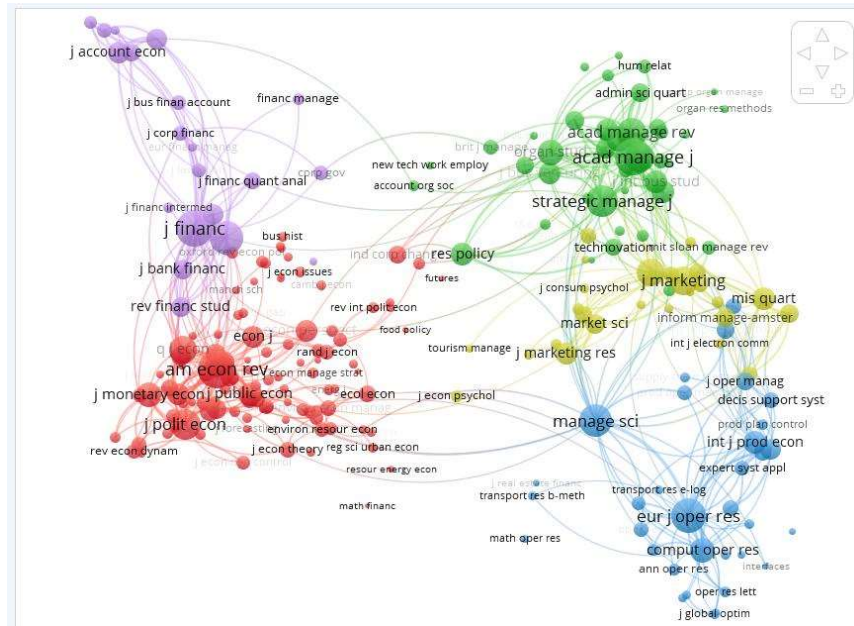
algoritma machine learning. Analisis kinerja algoritma anomaly jaringan ini adalah Intrusion Detection System (IDS) merupakan komponen fundamental organisasi yang mencegah aktivitas kejahatan dunia maya. Karena penggunaan layanan cloud dan internet of things (IoT) yang sangat besar, lalu lintas jaringan juga meningkat setiap hari dalam jumlah yang sangat besar, sehingga sulit bagi IDS untuk membedakan antara perilaku lalu lintas jaringan yang normal dan tidak wajar. Metode pembelajaran mesin (ML) telah menjadi teknik yang mudah untuk mengidentifikasi dan mengkategorikan beberapa serangan jaringan. Intrusion Detection System (IDS) adalah system pertahanan dan keamanan otomatis untuk monitor, mendeteksi, dan menganalisis hostile activities dalam jaringan atau host. Garis pertahanan pertama dalam IDS ini adalah firewall yang juga digunakan ketika ada bukti anomaly atau serangan, yang tidak dapat dihentikan atau dikurangi. Penggunaan perangkat IoT ini semakin meningkat dan bisa mengundang para penjahat untuk berbuat aksi di dunia maya, namun IoT juga bertanggung jawab dalam menghadapi tantangan itu dengan cara meningkatkan pemantauan penggunaan jaringan terutama di sektor-sektor pemerintahan, bank dan lainnya.

Beberapa teknik yang digunakan dalam masalah ini yaitu deep learning, eager learning, lazy learning, bagging, feature selection, boosting, dan stacking. Pertama deep learning yaitu sebuah metode dalam kecerdasan yang mengajarkan computer untuk memproses data dengan cara mempelajari dan mengklasifikasikan sebuah kebiasaan yang terinspirasi dari otak. Dan deep learning ini dapat digunakan sebagai bagian integral dari keamanan jaringan evaluasi untuk meningkatkan tingkat akurasi pada serangan yang tidak aman pada jaringan tersebut. Kedua eager learning adalah metode pembelajaran dimana system mencoba membangun target yang tidak bergantung pada model perhitungan sebelumnya. Ketiga lazy learning adalah metode pembelajaran dimana pelatihan data tertunda secara teori, sehingga membuat sebagian system tertunda dalam bekerja. Keempat bagging adalah penggabungan antara algoritma pembelajaran machine learning dan akurasi dari klasifikasi statistik dan regresi secara terpisah untuk menghasilkan prediksi akhir dari statistik yang dikerjakan sebelumnya. Kelima feature selection adalah suatu metode menganalisis data dimana data atau fitur yang dimiliki digunakan untuk pembelajaran sehingga bertujuan untuk memilih fitur yang lebih berpengaruh dan mengesampingkan fitur yang tidak berpengaruh pada analisis data tersebut. Keenam boosting adalah metode yang digunakan dalam ML untuk mengurangi kesalahan dalam analisis data performa yang sudah diprediksi sebelumnya. Ketujuh stacking adalah tahap awal dalam melakukan pengolahan data dengan cara menggabungkan kombinasi beberapa model dari konsep yang terpisah menjadi satu model atau kesatuan yang utuh.

Secara umum, salah satu solusi dalam machine learning yang memastikan bahwa hasil pada algoritma yang dilakukan akan berhasil 100% adalah pembelajaran yang bersifat soft computing. Soft computing adalah sekumpulan metodologi yang berkembang dan dapat mengolah data secara terus-menerus yang bertujuan untuk menghasilkan mesin IQ yang tinggi dan dapat diimplementasikan dengan biaya yang murah. Contohnya fuzzy logic (pengetahuan yang berkontribusi dalam pemecahan masalah dan dapat mengekspresikan konsep nilai-nilai yang lebih bagus), probabilistic reasoning (pengambilan keputusan atau alasan untuk mengambil informasi yang mengandung unsur ketidakpastian dalam mencari nilai optimal pada kromosom individu) dan neural network (jaringan tiruan dimana neuron-neuron yang di rangkai dapat menentukan bagaimana cara penguatan yang optimal dalam pembuatan mesin). Pada abad ke 21, perkembangan pembelajaran mesin ini semakin berkembang, melalui program google brain yang dapat mendeteksi objek-objek yang ada di dalam internet seperti Youtube. Namun dalam menyelesaikan masalah, pembelajaran ML ini harus menggunakan ruang penyimpana yang sangat besar untuk menyelesaikan semua masalah yang timbul, dan juga dibutuhkan pelabelan yang digunakan untuk pengenalan wajah sekalipun itu dari ribuan penggunanya.

METODE PENELITIAN

Metode penelitian dalam penelitian ini menggunakan metode bibliometrik dengan pendekatan kuantitatif. Pendekatan ini menjelaskan mengenai metode ilmiah yang memiliki focus utama dalam penjelasan konsep dasar yang kemudian digunakan untuk sarana analisis penelitian. Menurut Samsu (2017), penelitian kuantitatif merupakan suatu alat untuk menemukan keterangan mengenai suatu yang akan diketahui dengan melakukan proses analisis data yang berupa angka untuk menumbuhkan suatu pengetahuan. Data dalam penelitian ini didapat dari hasil pendataan data sampel distribusi kelas dalam kumpulan data pelatihan, kumpulan data pengujian, dan subset pelatihan dengan menggunakan perangkat Edge yang dilakukan penganalisisan menggunakan software VOSviewer.



Gambar 1. Software VOSviewer

VOSviewer adalah salah satu software yang digunakan untuk memvisualkan peta bibliometrik, memetakan topic untuk penelitian terbaru, mencari referensi yang paling banyak digunakan pada bidang tertentu. Beberapa langkah yang harus digunakan dalam analisis bibliometrik dengan VOSviewer adalah proses pencarian data, filterisasi bibliografi, pengecekan kembali atribut bibliografi, dan dilakukan analisis secara bibliometrik. .

HASIL DAN PEMBAHASAN

1. Deteksi anomaly

Anomaly berasal dari bahasa inggris yang bearti penyimpangan. Anomali merupakan sebuah penyimpangan yang terjadi pada model lingkungan. Penyimpangan ini dapat diakibatkan oleh factor dari dalam system itu sendiri maupun dari luar. Pendeteksian anomaly yang melibatkan manusia dapat sangat ampuh tetapi memerlukan waktu yang sangat lama dalam penggunaannya.

Dalam ilmu statistic, anomaly atau yang sering disebut outlier adalah data atau sekumpulan data yang memiliki bobot sangat berbeda. Pendeteksian anomaly sangat penting di industry, seperti keuangan, ritel, dan keamanan siber, tetapi setiap bisnis harus mempertimbangkan solusi deteksi anomaly. Algoritma ini menggabungkan eager learning dan lazy learning untuk menghasilkan deteksi anomaly dengan akurasi terbaik.

Dalam penggunaan anomaly ini, pasti ada beberapa masalah yang muncul. Masalah tersebut dapat diatasi atau dicegah yaitu dengan cara di bawah ini :

- a. pemutusan sirkuit data yaitu dengan cara menggunakan logika untuk menghentikan perjalanan data tersebut.
- b. Kontrak data
- c. Wawasan kesehatan data
- d. SLA data
- e. Kepemilikan data
- f. Membuat lapisan semantic
- g. Mempromosikan literasi data
- h. Meningkatkan interval data sebelum peringatan.

Beberapa manfaat dari deteksi anomaly antara lain :

- a. Melokalisasi dan menyelesaikan masalah sebelum mencapai bagian lain dari system. Hal ini menghasilkan penghematan biaya karena hanya menyelesaikan satu area system
- b. Melindungi system anda secara langsung dari instans
- c. Mengidentifikasi aktivitas penipuan dan pola yang tidak konsisten serta melindungi data.

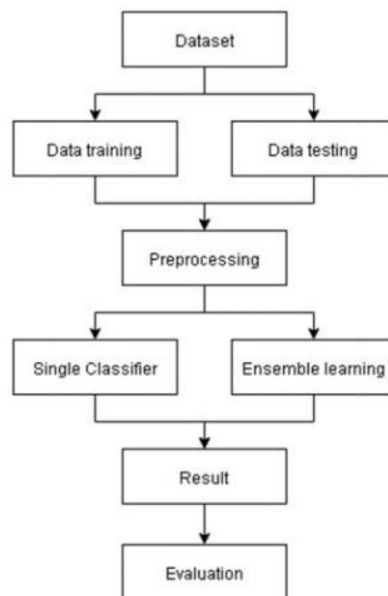
2. Machine learning

Machine learning adalah ilmu yang mempelajari tentang algoritma computer yang bisa mengenali pola-pola di dalam data dengan tujuan untuk mengubah beragam macam data menjadi suatu tindakan yang nyata dengan sedikit mungkin campur tangan manusia. Algoritma ML ini memiliki kemampuan untuk mempelajari data anomaly yang mungkin sangat sulit diatasi dan dapat mempelajari data dari data historis saja. Meskipun ML ini menjanjikan keberhasilan pemrograman namun ada sedemikian tantangan yang perlu diwaspadai dalam penggunaan ML ini. Deteksi intrusi adalah suatu metode yang dapat digunakan sebagai mendeteksi aktivitas yang mencurigakan dalam sebuah system dan dirancang untuk memantau, menganalisis pengguna jaringan agar tidak melanggar kebijakan akses yang berlaku.

Berikut adalah beberapa hal yang perlu dipahami mengenai machine learning yaitu :

- a. Cara kerja : pada dasarnya prinsip cara kerja pembelajaran mesin sama, meliputi pengumpulan data, eksplorasi data, pemilihan model atau teknik, memberikan pelatihan terhadap model yang dipilih, dan mengevaluasi hasil dari machine learning.
- b. Tujuan : Tujuan utama dari ML adalah mencari pola dan insight yang ada dalam data secara otomatis tanpa bantuan manusia
- c. Jenis : Machine learning dapat dibagi menjadi tiga jenis yaitu supervised learning, unsupervised learning, dan reinforcement learning.
- d. Kelebihan : Mampu memproses data yang besar dan kompleks dalam waktu singkat, dapat mempelajari pola dan tren yang tidak dapat dilihat oleh manusia, dan dapat meningkatkan efisiensi yanpa berorientasi pada kesuksesan.
- e. Kekurangan : Membutuhkan data yang valid sebagai bahan ajar, memerlukan waktu dan biaya yang cukup besar untuk pelatihan model, dan dapat menghasilkan output yang tidak akurat jika data yang digunakan tidak representative.
- f. Pemanfaatan : dapat dimanfaatkan dalam berbagai bidang, seperti di dunia perbankan, kesehatan dan bisnis.

Dalam penelitian ini, penulis menerapkan metode Maching Learning (ML), untuk medeteksi anomali dalam jaringan internet of things (IoT) dan metode ini melibatkan beberapa tahap. Terdapat beberapa langkah dalam penelitian untuk mempermudah dalam pengambilan tindakan, seperti ditunjukkan pada gambar di bawah ini.



Gambar 1. Diagram alur penelitian

a. Himpunan data (dataset)

Pertama, data dan jaringan IoT harus dikumpulkan dari lapisan aplikasi yang ditangkap di lingkungan IoT. Bisa termasuk data sensorik, log jaringan, atau atribun lain yang relevan untuk deteksi anomali jaringan. Berikut akan diambil data sampel distribusi kelas dalam kumpulan data pelatihan, kumpulan data pengujian, dan subset pelatihan dengan menggunakan perangkat Edge. Sebelum melakukan himpunan data, lita harus tau dulu apa itu perangkat Edge ?. perangkat Edge adalah proses menghadirkan penyimpanan informasi dan kemampuan komputasi yang lebih dekat ke perangkat yang menghasilkan informasi tersebut dan pengguna yang mengonsumsinya. Komputasi Edge menjasi semakin populer karena memungkinkan korporasi untuk mengumpulkan dan menganalisis data mentah mereka dengan efisien.

Ada beberapa manfaat dari perangkat Edge yaitu

1. mengurangi latensi/ menambah kecepatan.
2. Meningkatkan keamanan data
3. Meningkatkan produktivitas
4. Pengumpulan data jarak jauh
5. Mengurangi biaya
6. Performa andal

Selanjutnya kita akan mengambil data sampel distribusi kelas dalam kumpulan data pelatihan, kumpulan data pengujian, dan subset pelatihan dengan menggunakan perangkat Edge yaitu sebagai berikut :

Himpunan data	Data yang tidak wajar	Data biasa	Total
Kumpulan data asli (DS2OS)	10.017	278.264	375.941
Kumpulan data pelatihan (80%)	8088	278.264	286.352
Kumpulan data pengujian (20%)	1929	69.660	71.589
D1 (1%)	102	2761	2863
D2 (2%)	179	5548	5727
D5 (5%)	410	13.908	14.318
D10 (10%)	842	27.793	28.635

D15 (15%)	1220	41.732	42.952
D20 (20%)	1612	55.658	57.270
D40 (40%)	3224	111.316	114.540
D60 (60%)	4831	166.980	171.811
D80 (80%)	6456	222.625	229.081
D100 (kumpulan data pelatihan)	8088	278.264	286.352

Table 1. distribusi acak kumpulan data DS2OS.

Kumpulan data diatas berisi jejak lalu lintas IoT dari lapisan aplikasi yang ditangkap di lingkungan IoT. Ini mencakup data dari berbagai jenis perangkat, untuk lebih spesifik. Data ini berupa perangkat sumber, perangkat tujuan, kapan dan operasi apa yang dilakukan, serta informasi tingkat normalitas mengenai apakah suatu peristiwa dianggap sebagai anomaly atau tidak. Penentuan subset dimulai dengan pemisahan acak dari dataset asli menjadi dataset pelatihan dan pengujian awal (80-20 %). Dalam dua pendekatan berikutnya, subset yang lebih kecil ditentukan untuk tujuan melakukan komputasi dimana set data pelatihan yang tidak seimbang diubah menjadi subset data yang seimbang. Tujuan utama pendekatan ini adalah mengurangi ukuran kumpulan data dengan memilih beberapa observasi yang paling representatif dan membuang observasi lainnya.

b. Pemrosesan dan pembersihan data

Data yang dikumpulkan mungkin memiliki noise atau outlier yang perlu diatasi. Maka akan dilakukan pemrosesan data atau pembersihan data untuk menghapus nilai yang tidak valid atau mencurigakan dan menjaga kualitas data yang akan digunakan agar tetap relevan. Tujuan utama pendekatan ini adalah mengurangi ukuran kumpulan data dengan memilih beberapa observasi yang paling representatif dan membuang observasi lainnya. Kumpulan data yang tidak seimbang memberikan hasil umum untuk metric evaluasi yang dipilih untuk mengenali kumpulan data terkecil yang dipilih secara acak yang memberikan hasil yang tidak sama sekali ditingkatkan dengan jumlah sampel yang lebih banyak.

Adapun langkah-langkah dalam pembersihan data yaitu sebagai berikut :

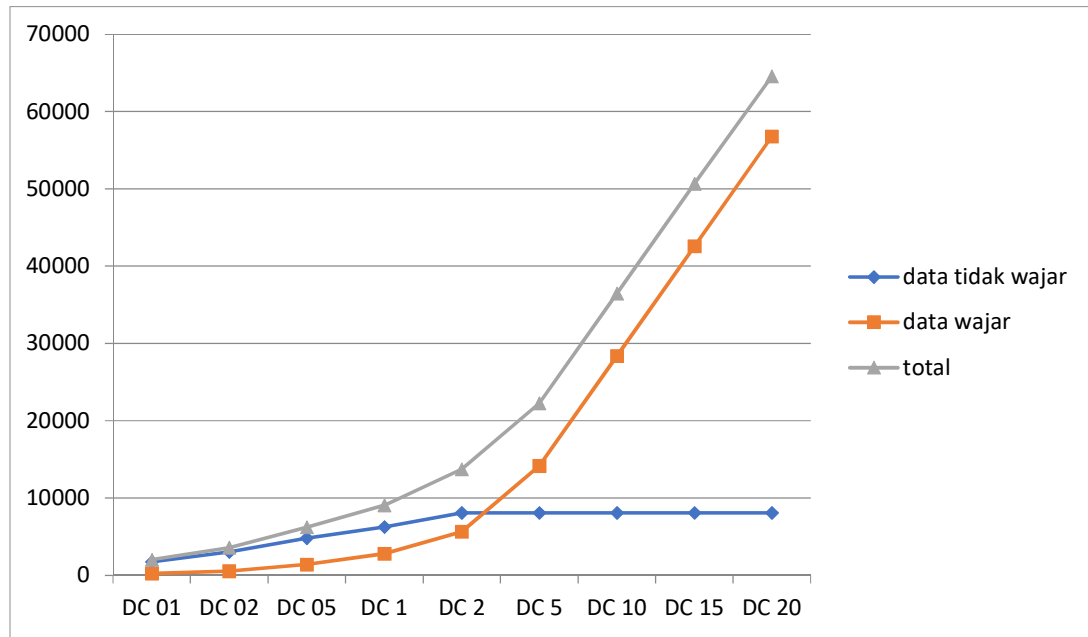
- 1) Membuang data duplikat
- 2) Membuang data yang tidak relevan
- 3) Hubungkan data-data yang hilang yang merupakan data yang dibutuhkan
- 4) Perbaiki kesalahan pengetikan, peletakan angka dan sebagainya

Berikut bagian kelas dengan data anomali dan persentase sampel dengan data normal setelah di bersihkan atau di acak ulang.

Himpunan data	Data yang tidak wajar	Data biasa	Total
DR01 (0,1 %)	8088	278	8366
DR02 (0,2%)	8088	557	8645
DR05 (0,5%)	8088	1391	9479
DR1 (1%)	8088	2783	10.871
DR2 (2%)	8088	5565	13.653
DR5 (5%)	8088	13.913	22.001
DR10 (10%)	8088	27.826	35.914
DR15 (15%)	8088	41.740	49.828
DR20 (20%)	8088	55.653	63.741

c. Pemilihan fitur

Pemilihan fitur yang baik akan membantu meningkatkan kinerja model dan menghindari dimensi data yang tidak perlu. Maka, kita akan memperlihatkan hasil klasifikasi dari data diatas dalam bentuk grafik. Dari data tersebut akan menunjukkan hasil akurasi pelatihan dataset seimbang dan pengujian untuk semua algoritma ML. untuk setiap algoritma ML, program python yang dijalankan menggunakan pelatihan rata-rata dan waktu pengujian untuk kumpulan data sehingga mencapai sampel yang ditentukan. Pada pemilihan fitur ini, ada dua cara yang dilakukan, pertama pencarian yang kurang optimal yaitu menghindari percobaan semua data atau fitur. Kedua pencarian yang berpotensi melelahkan yaitu semua fitur dikombinasi untuk memperoleh kinerja dan nilai yang mungkin layak untuk pengklasifikasian dalam data.



KESIMPULAN DAN SARAN

Algoritma adalah metode efektif yang diekspresikan melalui prosedur komputasi langkah-langkah yang terdefinisi dengan baik yang menggunakan beberapa nilai sebagai masukan dan menghasilkan beberapa nilai yang disebut keluaran atau suatu masalah. Dalam menghadapi kompleksitas dan pertumbuhan jaringan IoT, penggunaan teknik machine learning (ML) telah membuktikan bahwa teknik ini adalah solusi yang kuat untuk mendeteksi jaringan anomaly.

Hasil penyajian evaluasi hasil algoritma pembelajaran mesin (ML) pada data di atas tidak seimbang untuk mengidentifikasi anomaly. Kumpulan data yang lebih kecil akan memberikan hasil yang sebanding dengan kumpulan data yang dibuat. Pendekatan yang diusulkan di awal didasarkan pada semua sampel di kelas anomaly yang pengelompokan sampel representatifnya lebih kecil dan kumpulan data dan sampel dari cluster terkomputasi dari kelas tersebut. Namun, tidak semua jaringan ML bisa diperiksa dan memberikan hasil prediksi yang memuaskan, ada juga yang tidak berhasil. Seperti yang ditunjukkan dalam matriks konfusi, terdapat kesalahan klasifikasi pada kelas anomaly dan kumpulan data. Solusi yang paling menjanjikan dalam masalah komputasi edge ini adalah dengan menggunakan algoritma DT, namun memberi konsumsi sumber daya yang rendah dan proses yang cepat pada pengumpulan data.

Dengan demikian, dapat disimpulkan bahwa komputasi edge (edge computing) dapat menjadi alternative yang cocok untuk solusi ini. Dengan memilih metode evaluasi ML dapat berdampak performa dari hasil yang diinginkan. Pada pembahasan selanjutnya nanti, kami berencana untuk menggunakan metode prapemrosesan, dengan menggunakan data tidak seimbang yang lebih besar, dan mengadopsi beberapa algoritma ML untuk diterapkan beberapa pembelajaran dalam komputasi edge.

DAFTAR REFERENSI

- Anggraini, C. (2023). teknk machine learning untuk deteksi anomali dalam jaringan loT. *jurnal pendidikan* , 1-3.
- B. A. Tama, dkk. (2017) evaluasi empiris ekstenti ensemble untuk deteksi sains. *Jurnal pendidikan*, 149-158.
- dinata, R. k. (2020). *machine learning* . lhokseumawe: unimal press.
- imam, r. m. (2019). deteksi anomaly jaringan menggunakan hybrid algorithm. *jurnal prosiding teknik*, 2-3.
- iriani, s. a. (2023). analisis bibliometrik VOSviewer :study artificial intelegence dalam pendidikan . *jurnal simki pedagogia*, 5-7.
- kusuma, p. d. (2020). *algoritma dan pemrograman*. Yogyakarta: CV BUDI UTANA.
- Munawar, Z. (2020). keamanan loT dengan deep learning dan teknologi big data. *jurnal informasi dan komunikasi* , 162-164.
- perkasa, v. b. (2022). studi bibliometrik dengan VOSviewer terhadap publikasi ilmiah mengenai situs astana gede kawali . *jurnal ilmiah multidisiplin* , 2-4.
- roihan, a. (2020). pemanfaatan machine learning dalam berbagai bidang :review paper. *indonesia journal on computer and information technology*, 77-79.
- saheed, Y. k. (2022). A Machine learning-based intrusion detection for detection internet of things network attacks. *alexandria engineering journal* , 4-6.
- suartana, I. M. (2022). analisis penerapan deep learning untuk klasifikasi serangan terhadap keamanan jaringan. *jurnal ilmu komputer* , 101-103.
- sudiyarno, R. (2020). peningkatan performa pendekatan animaly menggunakan ensembel learning dan feature learing. *citec journal* , 2-3.
- sugiyono, dkk. (2017). *metode penelitian kuantitatif, kualitatif, dan R dan D*. Bandung : PT Alfabet.
- sulastrri, h. (2021). implementasi algoritma machine learning untuk penentuan cluster status gizi balita. *jurnal pekayasa teknologi informasi* , 1-2.
- Tan, T. (2023). study perbandingan deteksi intrusi jaringan menggunakan machine learning . *jurnal teknilogi dan informasi* , 152-155.