SMATIKA : STIKI Informatika Jurnal
Vol. 12, No. 2, Desember 2022, pp. xx~xx
ISSN: 2087-0256, e-ISSN: 2580-6939

Prediksi Kategori Serangan Siber dengan Algoritma Klasifikasi Random Forest Menggunakan Rapidminer

Prediction of Cyber Attack Categories with Random Forest Classification Algorithm Using Rapidminer

Saddam Rabbani[1*]
Diana[2]

[1,2]Teknik Informatika, Universitas Bina Darma, Indonesia
[1]saddamrabbani@gmail.com, [2]diana@binadarma.ac.id

***Penulis Korespondensi:**
Saddam Rabbani
saddamrabbani@gmail.com

Riwayat Artikel:
Diterima :
Direview :
Disetujui :
Terbit :

Abstrak

Serangan siber menjadi ancaman serius bagi organisasi atau lembaga yang menggunakan jaringan komputer dalam operasinya, salah satunya Dinas Komunikasi dan Informatika Kota Palembang. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan algoritma klasifikasi Random Forest pada platform Rapidminer untuk memprediksi kategori serangan siber pada Dinas Komunikasi dan Informatika Kota Palembang. Data yang digunakan dalam penelitian ini adalah data serangan siber dari perangkat firewall selama periode tertentu. Data tersebut diproses menggunakan Rapidminer dengan algoritma Random Forest untuk memprediksi kategori serangan siber. Hasil penelitian ini memberikan nilai akurasi yang tinggi sehingga memungkinkan pihak yang bertanggung jawab untuk segera mengambil tindakan pencegahan atau response terhadap serangan siber yang merugikan Dinas Komunikasi dan Informatika Kota Palembang. Hasil yang didapatkan dari evaluasi menggunakan confusion matrix dan accuracy score, didapatkan nilai akurasi 99.84% dan nilai out of bag error 0.16.
Kata Kunci: Prediksi, Serangan Siber, *Data Mining*, *Random Forest*, *Confusion Matrix*, Rapidminer

Abstract (Cambria, 11, italic, bold)

Cyber attacks are a serious threat to organizations or institutions that use computer networks in their operations, one of which is Communication and Informatics Department of Palembang. Therefore, this study aims to implement the Random Forest classification algorithm on the Rapidminer platform to predict cyber attack categories at the Communication and Informatics Department of Palembang. The data used in this study is cyber attack data from firewall devices for a certain period. The data is processed using Rapidminer with the Random Forest algorithm to predict cyber attack categories. The results of this research provide a high accuracy value, thereby enabling the responsible team to take preventive action or response detrimental cyber to the Communication and Informatics Department of Palembang. After evaluation using the confusion matrix and accuracy score, the results obtained were 99.84% accuracy and out of bag error 0.16.
Keywords: Prediction, Cyber Attack, Data Mining, Random Forest, Confusion Matrix, Rapidminer

1. Pendahuluan

Semakin tingginya ancaman serangan siber yang dihadapi oleh lembaga atau organisasi di seluruh dunia. *International Business Machines* (IBM) memperlihatkan bahwa selama pandemi Covid-19, serangan siber global naik sebesar 6.000% [1]. Interpol menyebutkan bahwa lanskap kejahatan

siber global selama pandemi Covid-19 didominasi oleh beberapa jenis serangan, yaitu *scam* dan *online phising*, *disruptive malware*, *data harvesting malware*, *malicious domain*, dan *misinformation* [2]. Berbagai penyerangan ancaman siber yang maraknya sering terjadi dikarenakan adanya kecerobohan dan lemahnya sistem keamanan teknologi online sehingga menyebabkan dampak yang sangat buruk bagi pemilik akun bahkan platform yang terkait akan merasakan dampaknya pula [3]. Berdasarkan publikasi *The Global Cybersecurity Index* (GCI) 2017 yang dirilis oleh *International Telecommunication Union* (ITU), kondisi keamanan siber Indonesia masih termasuk dalam negara dengan kategori keamanan siber yang lemah berada dalam tahap peningkatan optimal (*maturing stage*). Oleh karena itu, pencegahan dan deteksi serangan siber menjadi sangat penting dalam menjaga keamanan jaringan dan sistem informasi.

Dinas Komunikasi dan Informatika Kota Palembang sebagai salah satu lembaga pemerintah yang memiliki jaringan komputer dan sistem keamanan informasi yang kompleks sehingga sangat rentan untuk menjadi *target* serangan siber. Dinas Komunikasi dan Informatika Kota Palembang perlu mengambil tindakan untuk meningkatkan keamanan dan mencegah serangan siber yang dapat mengancam keberlangsungan operasionalnya. Salah satu cara untuk mengatasi hal ini adalah dengan menggunakan teknologi prediksi serangan siber yang dapat memberikan peringatan dini dan membantu dalam mengambil tindakan pencegahan atau *response* terhadap serangan yang terdeteksi.

Algoritma klasifikasi *Random Forest* dapat menjadi solusi untuk memprediksi serangan siber pada periode yang akan datang. Khariwal & Arora mengusulkan deteksi *malware* pada *android* berdasarkan *permission* dengan menggunakan beberapa algoritma *machine learning* seperti SVM, *Naive Bayes* dan *Random Forest* [4]. Hasil yang didapat *Random Forest* memiliki akurasi paling tinggi dalam deteksi *malware android* berdasarkan *permission* [5]. Pada studi kasus klasifikasi debitur berdasarkan kualitas kredit menyatakan bahwa klasifikasi *Random Forest* merupakan metode klasifikasi yang memiliki tingkat akurasi paling tinggi untuk klasifikasi kualitas kredit yaitu mencapai 98,16% disusul *Naïve Bayes* 95,93% [6].

Peramalan atau prediksi adalah upaya untuk memperkirakan nilai atau peristiwa di masa depan berdasarkan informasi dan data yang tersedia di masa lalu [7]. Sedangkan menurut Orpa, prediksi adalah suatu proses memperkirakan secara sistematis tentang sesuatu yang paling mungkin terjadi di masa depan berdasarkan informasi masa lalu dan sekarang yang dimiliki, agar kesalahannya (selisih antara sesuatu yang terjadi dengan hasil perkiraan) dapat diperkecil [8]. Prediksi tidak harus memberikan jawaban secara pasti kejadian yang akan terjadi, melainkan berusaha untuk mencari jawaban sedekat mungkin yang akan terjadi [8]. Maka prediksi atau peramalan dalam diartikan sebagai proses atau kemampuan untuk membuat perkiraan atau estimasi tentang apa yang mungkin terjadi di masa depan berdasarkan informasi yang tersedia saat ini.

Serangan siber adalah serangan yang dilakukan oleh *network* komputer atau telekomunikasi terhadap *network* komputer atau telekomunikasi yang lain seperti *website*, sistem komputer, dan komputer individu [9]. Berkat teknologi informasi dan Internet, para pelaku ini dapat melakukannya dengan lebih mudah, hemat biaya, dan dengan cara yang lebih hemat sumber daya. Insiden yang terkait dengan serangan dunia maya termasuk spionase industri dan *target* vital pemerintah, seperti pencurian dan penghancuran informasi rahasia penting, yang dapat menimbulkan kekhawatiran dan ketidakamanan karena ancaman kehilangan batas pribadi dan kehilangan harta benda dan aset. Upaya serangan siber ini tidak hanya jika terjadi dapat digunakan untuk kepentingan politik dunia siber, tetapi juga sebagai alat politik, seperti penyebaran berita bohong untuk tujuan provokasi politik bagi perencanaan sektor ekonomi [10].

Ada berbagai jenis serangan siber yang sering terjadi, di antaranya *Malware* adalah sejenis program komputer yang dimaksudkan untuk mencari kelemahan *software* sehingga pada perangkat akan terkena *virus*, *malware* dapat berisi kode berbahaya seperti *Virus*, *Worm*, *Trojan Horse* [11]. DDoS (*Distributed Denial of Service*) adalah jenis serangan terstruktur, serangan DDoS mampu melumpuhkan server dengan membanjiri lalu lintas jaringan dan mengakibatkan down [12]. Serangan DDoS bertujuan untuk mengganggu ketersediaan layanan dengan mengirimkan lalu lintas internet yang sangat tinggi ke sistem *target*, yang membuatnya tidak dapat merespons permintaan pengguna yang sah. *Phishing* adalah suatu taktik penipuan dengan mengelabui *target* untuk mencuri informasi dari akun korban. Istilah ini berasal dari kata *fishing* yang artinya memancing korban agar terperangkap kedalam jebakan pelaku. Pada dasarnya *phishing* didefinisikan sebagai tindak penipuan yang memanfaatkan *email* dari pengguna untuk menggali informasi sensitif milik korban [13]. *Man-in-the-Middle* adalah jenis serangan dimana penyerang diam-diam mengambil alih saluran komunikasi antara dua perangkat atau lebih, penyerang dapat melakukan interupsi, modifikasi atau mengganti trafik komunikasi perangkat korban. *SQL Injection* adalah aksi *hacking* yang dilakukan di aplikasi *client* dengan memodifikasi perintah SQL yang ada di memori aplikasi *client* dan merupakan teknik mengeksploitasi web aplikasi yang didalamnya menggunakan *database* untuk penyimpanan data [14]. *Pharming* adalah aksi penipuan yang dilakukan *cyber crime* dengan cara mengelabui korban dengan mengarahkan ke situs web asli ke situs web palsu. Sehingga korba akan menyangka telah memasuki situs web asli dan tanpa ragu korban akan mengisi data pribadi atau data lainnya yang diminta oleh *cyber crime* melalui situs palsu [15].

Penelitian ini dilakukan dengan tujuan untuk mengimplementasikan algoritma klasifikasi *Random Forest* pada platform Rapidminer untuk memprediksi kategori serangan siber pada Dinas Komunikasi dan Informatika Kota Palembang. Dengan memanfaatkan teknologi prediksi tersebut, diharapkan dapat memberikan hasil akurasi yang tinggi terhadap jenis serangan yang terjadi sehingga akan memungkinkan pihak yang bertanggung jawab untuk segera mengambil tindakan pencegahan atau *response* terhadap serangan siber yang terdeteksi

2. Metode Penelitian

Data Penelitian

Dalam melakukan penelitian ini data yang digunakan adalah *dataset* yang dimiliki oleh Dinas Komunikasi dan Informatika Kota Palembang, diunduh atau *export* dari perangkat *Firewall* yang berupa log IPS (*Intrusion Prevention System*). Dataset yang digunakan adalah dataset dengan jenis CSV (*Comma Separated Values*). Agar dataset tersebut dapat dibaca dengan mudah, maka dilakukan proses *import* ke Microsoft Excel. Jumlah seluruh sampel atau *record* yang terdapat pada *dataset* adalah 9022 sampel atau *record*. Berdasarkan dari waktu atau *time* bulan Februari 2023 hingga Maret 2023.

Random Forest

Random Forest (RF) adalah salah satu metode yang banyak digunakan untuk kegiatan klasifikasi dan deteksi dengan cara membangun banyak pohon (*tree*) klasifikasi. Metode *Random Forest* ini dapat digunakan untuk meningkatkan akurasi karena pada metode ini terdapat pemilihan yang dilakukan secara acak dalam membangkitkan simpul anak untuk setiap *node* (simpul diatasnya) dan kemudian diakumulasikan hasil klasifikasi dari setiap pohon tersebut, kemudian dari hasil tersebut dipilih hasil klasifikasi yang paling banyak muncul. Sedikit banyaknya pohon yang akan dibentuk pada metode ini sangat berpengaruh dengan tingkat akurasi hasil dari klasifikasi. Pada metode ini semakin banyak pohon, maka tingkat akurasi hasil klasifikasinya akan semakin tinggi.

Confusion Matrix atau dalam *Machine Learning* juga dikenal dengan nama *Error Matrix* merupakan tata letak tabel secara khusus yang berfungsi untuk memvisualisasikan kinerja suatu algoritma. Contohnya dalam penelitian ini menggunakan algoritma Random Forest.

Berikut ini adalah beberapa performa yang diukur pada *confusion matrix*:

1. *True Positive* (TP), memiliki nilai prediksi positif dengan kondisi aktual positif.
2. *True Negative* (TN), memiliki nilai prediksi negatif dengan kondisi aktual negatif.
3. *False Positive* (FP), memiliki nilai prediksi positif dengan kondisi aktual negatif.
4. *False Negative* (FN), memiliki nilai prediksi negatif dengan kondisi aktual positif.

Rumus yang bisa digunakan adalah sebagai berikut:

Accuracy

Tingkat kedekatan nilai prediksi dan nilai aktual.

$$Accuracy = (TP+TN) / (TP+FN+FP+TN) \quad (1)$$

Recall

Tingkat keberhasilan sistem dalam menemukan kembali informasi.

$$Recall = TP / (TP+FN) \quad (2)$$

OOB Error

Out of Bag (OOB) *Error* merupakan parameter yang menentukan seberapa baik kinerja algoritma *Random Forest* pada penelitian.

$$OOB\ Error = 1 - Accuracy \quad (3)$$

Tahapan Penelitian

Berikut adalah langkah-langkah penelitian yang akan dilakukan [16]:

1. Analisis *Dataset*

Langkah pertama penelitian ini adalah menganalisis *dataset* yang akan digunakan. Proses ini melihat apakah ada data yang *null* atau tidak lengkap. Sehingga dipastikan dataset sudah siap untuk diolah.

2. Pemilihan Fitur

Setelah diketahui bahwa dataset sudah siap untuk diolah, maka selanjutnya dilakukan pemilihan fitur. Pemilihan fitur atau *features selection*, merupakan langkah yang dilakukan untuk menyeleksi data dimana langkah ini bekerja untuk mengurangi jumlah fitur ataupun menghapus dan menghilangkan data yang tidak dibutuhkan, atau *data noise*, maupun data yang berlebihan terhadap data yang akan digunakan pada proses inti dari penelitian.

3. *Data Split*

Tahap pemisahan data adalah untuk membagi data menjadi dua kategori yaitu *data training* dan *data testing*. Berdasarkan hasil pengujian yang dilakukan Yogiek, semakin banyaknya *data training* yang digunakan, maka nilai *accuracy* akan semakin meningkat [17]. Maka dalam penelitian ini akan dilakukan tiga kali pengujian dengan *data training* diberikan sebesar 60% dari keseluruhan data dan sisanya sebesar 40% dari keseluruhan data diberikan untuk *data testing*, data training diberikan sebesar 70% dari keseluruhan data dan sisanya sebesar 30% dari keseluruhan data diberikan untuk *data testing*, dan terakhir *data training* diberikan sebesar 80%

dari keseluruhan data dan sisanya sebesar 20% dari keseluruhan data diberikan untuk *data testing*.

4. Inisialisasi *Random Forest*

Setelah dilakukannya pemilihan fitur dan pemisahan data, maka selanjutnya dilakukan inisialisasi Algoritma *Random Forest*. Tahap ini dilakukan dengan menerapkan Algoritma *Random Forest* untuk melakukan prediksi kategori serangan siber pada Dinas Komunikasi dan Informatika Kota Palembang, sehingga akan didapatkan nilai akurasi yang dibutuhkan.

5. Hasil Akurasi

Hasil akurasi dari penerapan Algoritma *Random Forest* divisualisasikan dalam berbagai model statistik. Dapat berupa tabel maupun grafik. Sehingga dapat lebih mudah dilihat atau dianalisa.

6. Analisa dan Kesimpulan

Visualisasi tersebut kemudian dianalisa berdasarkan identitas dari server atau sistem yang menjadi *target* dan juga identitas pelaku yang melakukan serangan siber serta dibuatkan kesimpulan. Diharapkan hasil dari penerapan Algoritma *Random Forest* yang telah dilakukan dapat memberikan kesimpulan yang sesuai dengan harapan dari penelitian ini.

3. Hasil dan Pembahasan

Hasil Akurasi

Penelitian ini dilakukan dengan 3 (tiga) kali percobaan. Masing-masing percobaan diberikan perbandingan yang berbeda. Percobaan pertama diberikan perbandingan dengan rasio *data training* sebesar 60% berbanding *data testing* sebesar 40%. Sehingga dari jumlah 6413 sampel akan didapat 3846 sampel pada *data training* dan 2567 sampel pada *data testing*.

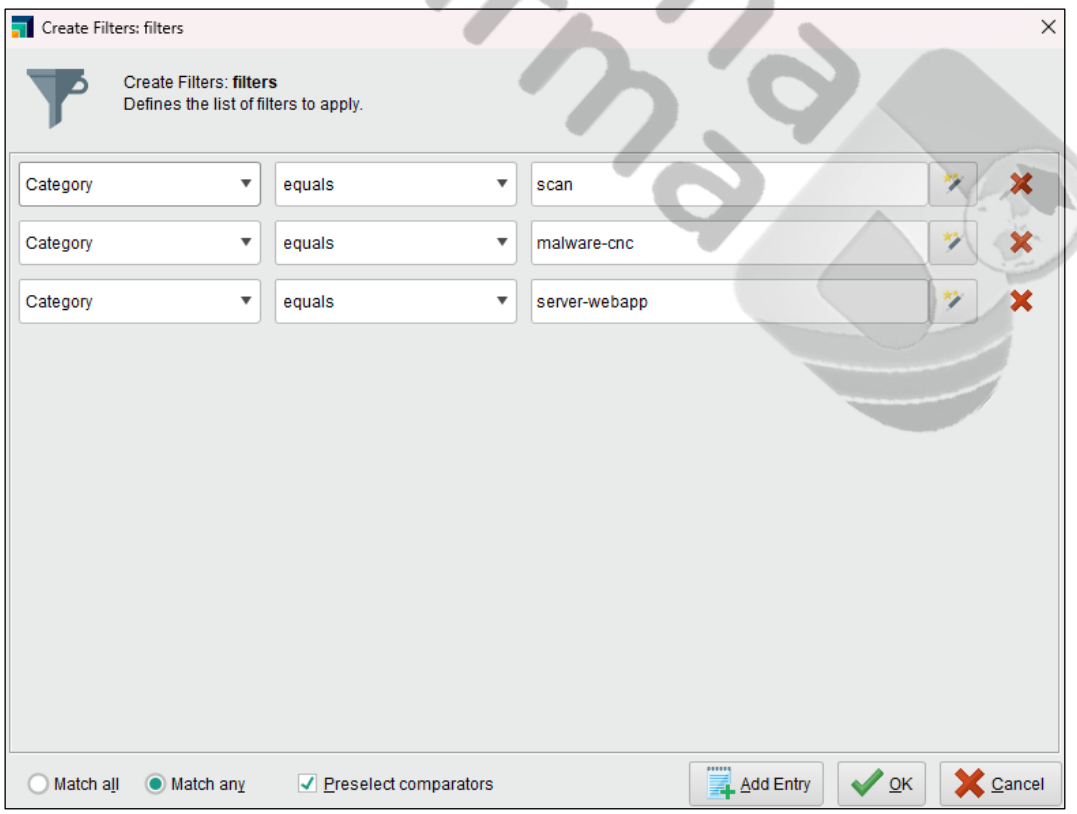
Pada percobaan kedua diberikan perbandingan dengan rasio *data training* sebesar 70% berbanding *data testing* sebesar 30%. Sehingga dari jumlah 6413 sampel akan didapat 4487 sampel pada *data training* dan 1926 sampel pada *data testing*.

Dan pada percobaan yang terakhir diberikan perbandingan dengan rasio *data training* sebesar 80% berbanding *data testing* sebesar 20%. Sehingga dari jumlah 6413 sampel akan didapat 5132 sampel pada *data training* dan 1281 sampel pada *data testing*.

Hasil dari inisialisasi algoritma *Random Forest* pada Tabel 1 dengan 3 (tiga) kali percobaan menggunakan perbandingan yang berbeda, menunjukkan bahwa semakin banyak sampel yang dipakai sebagai *data training* maka hasil akurasi yang didapat juga semakin meningkat. Dikarenakan semakin banyak sampel yang dijadikan sampel latih maka kinerja dari *machine learning* menjadi lebih baik. Terdapat 3 (tiga) kategori serangan siber yang mempunyai nilai *recall* paling tinggi. Sehingga peneliti melakukan penambahan operator *filter examples* dengan melakukan filter terhadap 3 (tiga) kategori serangan siber yang mempunyai nilai *recall* paling tinggi tersebut seperti pada Gambar 1.

Tabel 1. *Perbandingan Hasil Percobaan*

Percobaan ke-	Perbandingan *Data training* : *Data testing*	Kategori serangan										Akurasi
		Scan		*Malware-cnc*		*Server Web-app*		*Server-other*		*Protocol-dns*		
		True	*False*	*True*	*False*	*True*	*False*	*True*	*False*	*True*	*False*	
1	60:40	1510	0	736	0	257	4	7	3	4	25	97,94 %
	Recall	100%		100%		98,47%		70%		13,79%		
2	70:30	1132	0	552	0	194	2	6	1	3	19	97,98 %
	Recall	100%		100%		98,98%		85,71		13,64%		
3	80:20	755	0	368	0	128	2	4	1	3	11	98,20 %
	Recall	100%		100%		98,46		80%		21,43		



Gambar 1. *Penerapan Filter Examples Kategori Serangan Siber*

Percobaan dengan menambahkan *filter examples* (Gambar 1) pada kategori serangan siber yang mempunyai nilai *recall* paling tinggi dilakukan inisialisasi algoritma *Random Forest* dengan rasio perbandingan *data training* dengan *data testing* sebesar 80 berbanding 20. Memperoleh nilai akurasi sebesar 99,84% didapatkan nilai *recall* untuk kategori *scan* sebesar 100% (755), kategori

malware-cnc sebesar 100% (368), kategori *server web-app* sebesar 98,40% (128) dan kategori lainnya 0%. Berdasarkan tabel di atas maka perhitungan manual yang didapatkan adalah sebagai berikut:

Accuracy = (TP+TN) / (TP+FN+FP+TN) = 1251/1253 = 99,84%

Recall "Scan" = TP / (TP+FN) = 755/755 = 100%

Recall "Malware-cnc" = TP / (TP+FN) = 368/368 = 100%

Recall "Server Web-app" = TP / (TP+FN) = 128/130 = 98,46%

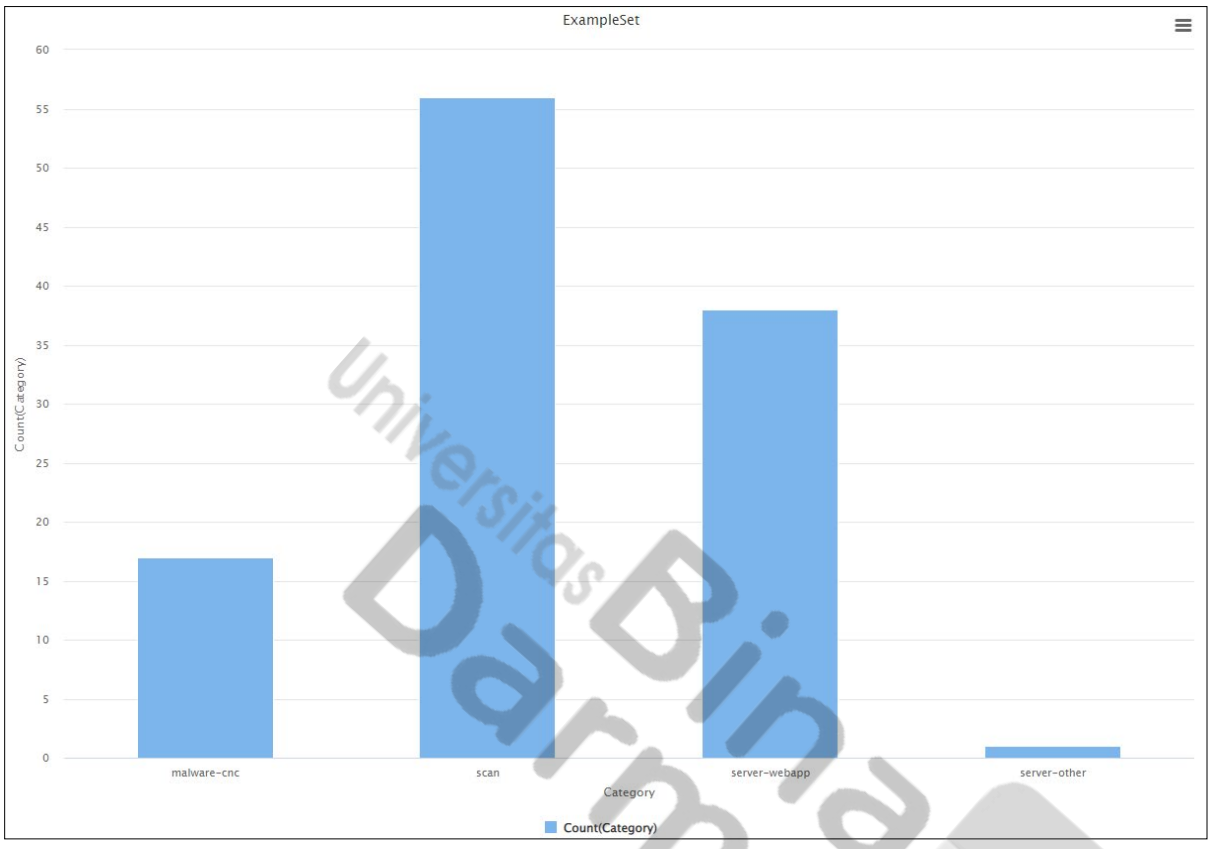
OOB Error = 100-99,84 = 0,16%

Tabel 2. *Perbandingan Hasil Percobaan dengan menerapkan Filter Examples*

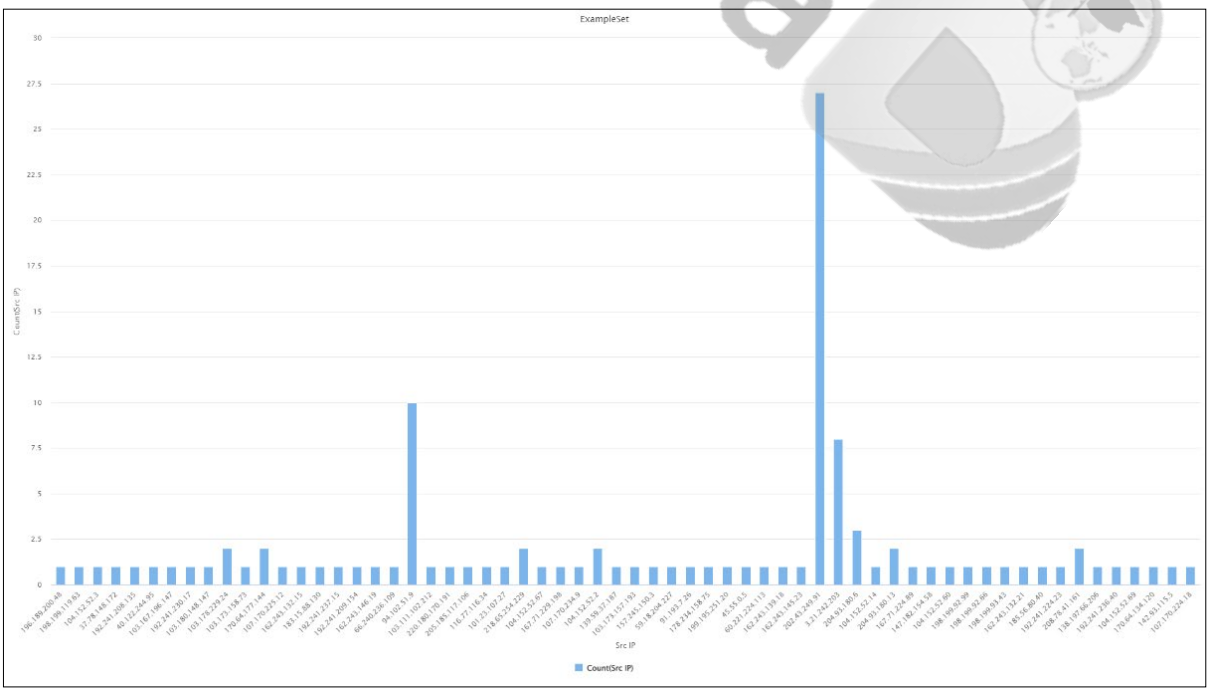
Percobaan ke-	Perbandingan *Data training* : *Data testing*	Kategori serangan										Akurasi
		Scan		*Malware-cnc*		*Server Web-app*		*Server-other*		*Protocol-dns*		
		True	*False*	*True*	*False*	*True*	*False*	*True*	*False*	*True*	*False*	
1	60:40	1510	0	736	0	257	4	7	3	4	25	97,94 %
	Recall	100%		100%		98,47%		70%		13,79%		
2	70:30	1132	0	552	0	194	2	6	1	3	19	97,98 %
	Recall	100%		100%		98,98%		85,71		13,64%		
3	80:20	755	0	368	0	128	2	4	1	3	11	98,20 %
	Recall	100%		100%		98,46		80%		21,43		
4	80:20	755	0	368	0	128	2					99,84 %
	Recall	100%		100%		98,46						

Pembahasan

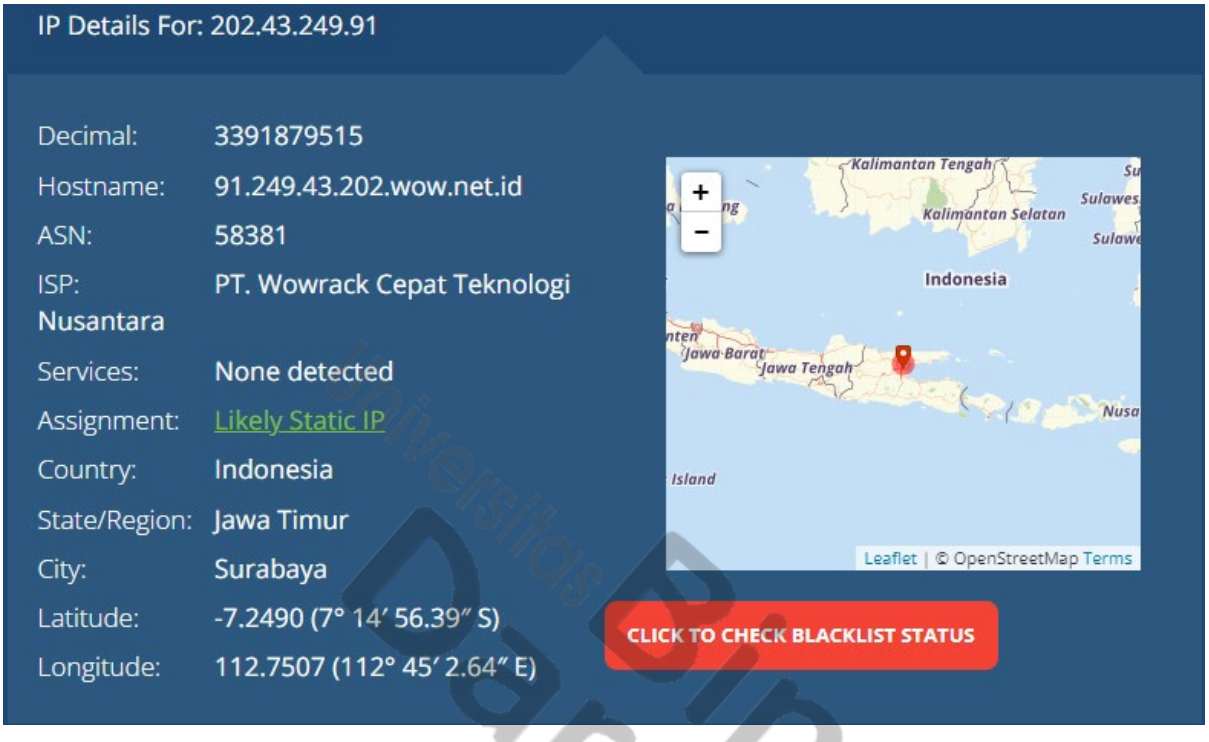
Berdasarkan visualisasi yang dilakukan untuk melihat identitas server atau sistem yang menerima aktivitas serangan siber, terdapat 1 server atau sistem yang mendapatkan jumlah serangan paling tinggi yaitu sebanyak 112 kali. Dari jumlah 112 kali serangan siber yang diterima oleh IP tersebut, terdapat 4 kategori serangan siber, yaitu malware-cnc, scan, server-webapp dan server-other (Gambar 2). Pada sejumlah serangan siber yang diterima oleh IP tersebut, telah terdeteksi 27 kali percobaan serangan siber oleh IP 202.43.249.91 (Gambar 3).



Gambar 2. *Visualisasi Kategori Serangan Siber*



Gambar 3. *Visualisasi Identitas IP dari Pelaku Serangan Siber*



Gambar 4. *IP Details untuk 202.43.249.91*

Pada Gambar 4 hasil penelusuran data pada situs whatismyipaddress.com diketahui bahwa detail identitas dari IP 202.43.249.91 adalah berasal dari negara Indonesia. Namun tidak dapat dipastikan bahwa memang pelaku adalah warga negara Indonesia, dikarenakan setiap pelaku serangan siber tentunya akan selalu berusaha untuk menyembunyikan identitas asli mereka.

4. Penutup

Penerapan algoritma klasifikasi Random Forest untuk memprediksi kategori serangan siber pada platform Rapidminer berhasil dilakukan dengan hasil akurasi yang tinggi yaitu sebesar 99,84%. Untuk mendapatkan akurasi yang baik dalam memprediksi kategori serangan siber pada Platform Rapidminer dengan algoritma Random Forest menggunakan rasio perbandingan 80% sebagai data training dan 20% sebagai data testing, serta menambahkan operator filter examples kepada 3 kategori serangan siber yang mempunyai nilai recall paling tinggi.

5. Referensi

[1] R. Hendra Wicaksana, A. Imam Munandar, P. L. Samputra, J. Salemba, R. No, dan J. Indonesia, "Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic," *Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi*, vol. 22, no. 2, hlm. 143–158, doi: 10.33164/iptekkom.22.2.2020.143-158.

[2] I. G. Secretariat, "Cyber Crime: Covid-19 Impact," *Lyon, France*, 2020.

[3] D. A. Sudarmadi dan A. J. S. Runturambi, "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional*, vol. 2, no. 2, hlm. 157–178, 2019.

[4] K. Khariwal, J. Singh, dan A. Arora, "IPDroid: Android malware detection using intents and permissions," *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, vol. IEEE, hlm. 197–202, 2020.

[5] H. Yang, Y. Zhang, Y. Hu, dan Q. Liu, "Android malware detection method based on permission sequential pattern mining algorithm," *Journal on Communications*, vol. 34, no. Z1, hlm. 107–115, 2013.

[6] M. Ignasius, J. Lamabelawa1, dan B. Sukarto2, "ANALISIS DATA KUNJUNGAN WISATAWAN MANCANEGARAKE NTT DENGAN METODE PREDIKSI TIME SERIES." [Daring]. Tersedia pada: https://ntt.bps.go.id

[7] A. K. Hermawan dan A. Nugroho, "Analisa Data Mining Untuk Prediksi Penyakit Ginjal Kronik Dengan Algoritma Regresi Linier," *Bulletin of Information Technology (BIT)*, vol. 4, no. 1, hlm. 37–48, 2023, doi: 10.47065/bit.v3i1.

[8] E. P. K. Orpa, E. F. Ripanti, dan T. Tursina, "Model Prediksi Awal Masa Studi Mahasiswa Menggunakan Algoritma Decision Tree C4. 5," *JUSTIN (Jurnal Sistem dan Teknologi Informasi)*, vol. 7, no. 4, hlm. 272–278, 2019.

[9] D. Luthfah, "Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia".

[10] T. Vimy, S. Wiranto, R. Rudiyanto, P. Widodo, dan P. Suwarno, "Ancaman Serangan Siber Pada Keamanan Nasional Indonesia," *Jurnal Kewarganegaraan*, vol. 6, no. 1, hlm. 2319–2327, 2022.

[11] Y. Ilhamdi dan Y. N. Kunang, "ANALISIS MALWARE PADA SISTEM OPERASI WINDOWS MENGGUNAKAN TEKNIK FORENSIK," *Bina Darma Conference on Computer Science*.

[12] J. Pendidikan dan D. Konseling, "Optimasi Metode Naïve Bayes dengan Particle Swarm Optimization untuk Sistem Deteksi Serangan D-Dos Universitas Pahlawan Tuanku Tambusai," vol. 4, 2022.

[13] N. B. Putri dan A. W. Wijayanto, "Analisis Komparasi Algoritma Klasifikasi Data Mining Dalam Klasifikasi Website Phishing," *Komputika : Jurnal Sistem Komputer*, vol. 11, no. 1, hlm. 59–66, Jan 2022, doi: 10.34010/komputika.v11i1.4350.

[14] T. Imam *dkk.*, "J I I F K O M (J u r n a l I l m i a h I n f o r m a t JIIFKOM (Jurnal Ilmiah Informatika & Komputer) STTR Cepu Analisis Serangan dan Keamanan pada SQL Injection: Sebuah Review Sistematik."

[15] P. R. Silalahi *dkk.*, "Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online," Jurnal Manajemen, 2022.

[16] F. Rahmat, "DETEKSI MALWARE RANSOMWARE PADA PLATFORM ANDROID MENGGUNAKAN METODE RANDOM FOREST," Universitas Sriwijaya, 2021.

[17] Y. I. Kurniawan, "Perbandingan Algoritma Naive Bayes dan C.45 dalam Klasifikasi Data Mining," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 4, p. 455, Oct. 2018, doi: 10.25126/jtiik.201854803.