IJAI (Indonesian Journal of Applied Informatics)
Vol. 9 No. 2 Tahun 2025 pISSN: 2548-3846, eISSN: 2598-5981

Klasifikasi Ancaman Keamanan Siber Menggunakan Algoritma Naive Bayes

Irwan Budianto[1]*, Nurchim[1], Hanifah Permatasari[1]
[1]Program Studi S1 Teknik Informatika, Universitas Duta Bangsa Surakarta, Indonesia
Email: ir1.budianto@gmail.com

Info Artikel

Kata Kunci :
deteksi ancaman keamanan siber, naive bayes, analisis data

Keywords :
cybersecurity threat detection, naive byaes, data analysis

Tanggal Artikel
Dikirim : 21 Januari 2025
Direvisi : 25 Januari 2025
Diterima : 10 Februari 2025

Abstrak

Saat ini keamanan siber menjadi permasalahan utama di dalam tata kelola keamanan informasi Pemerintah Daerah. Untuk mencegah terjadinya kerugian akibat serangan siber maka perlu dilakukan identifikasi dan klasifikasi terhadap ancaman siber secara cepat dan akurat. Sehingga diperlukan sebuah sistem untuk mengklasifikasikan ancaman siber yang terjadi. Penelitian ini adalah membangun sistem klasifikasi ancaman keamanan siber menggunakan algoritma Naive Bayes sehingga dapat dilakukan analisis data ancaman secara efektif dan mengklasifikasikan jenis ancaman dengan akurasi yang tinggi. Metode yang digunakan adalah pengumpulan dataset terkait log aktifitas serangan yang terekam di aplikasi Wazuh. Selanjutnya dilakukan preprocessing data untuk mendapatkan atribut yang sesuai dengan kebutuhan sistem. Penerapan algoritma Naive Bayes digunakan sebagai metode klasifikasi berdasarkan probabilitas atribut terhadap kategori ancaman. Hasil penelitian menunjukkan bahwa algoritma Naive Bayes mampu mengklasifikasikan ancaman keamanan siber dengan akurasi yang baik, sehingga dari system yang dibangun dapat ditentukan bahwa serangan yang terjadi pada area sistem operasi server atau aplikasi web serta mampu memberikan dukungan pengambilan keputusan yang lebih cepat dalam mitigasi serangan. Hasil pengujian menunjukkan performa yang sangat baik dari model Naive Bayes pada kedua kelas yaitu presisi=0.98, recall=1, f1-score=0.99, support=57.

Abstract

Currently, cybersecurity is a major problem in the governance of regional government information security. To prevent losses due to cyber attacks, it is necessary to identify and classify cyber threats quickly and accurately. So a system is needed to classify cyber threats that occur. This study is to build a cybersecurity threat classification system using the Naive Bayes algorithm so that threat data analysis can be carried out effectively and classify types of threats with a high level of accuracy. The method used is collecting datasets related to attack activity logs recorded in the Wazuh application. Furthermore, data preprocessing is carried out to obtain attributes that match system needs. The Naive Bayes algorithm is implemented as a classification technique that evaluates the probability of attributes relative to threat categories. The findings indicate that this algorithm effectively categorizes cybersecurity threats with high accuracy. Consequently, the developed system can identify whether an attack targets the server operating system or the web application, while also enabling faster decision-making to support attack mitigation. The Naive Bayes model performs exceptionally well in both classes according to the test results, with precision=0.98, recall=1, f1-score=0.99, and support=57.

1. PENDAHULUAN

Akhir-akhir ini, Keamanan siber menjadi salah satu tantangan utama di Indonesia karena ancaman terhadap infrastruktur Teknologi Informasi (TI) terus berkembang, terutama di sektor pemerintahan, perbankan, dan kesehatan.[1]. Ancaman utama dalam keamanan siber meliputi serangan seperti malware, ransomware, DDoS, dan phishing[2]. Pada tahun 2023 Badan Siber dan Sandi Negara (BSSN) melaporkan terjadi lonjakan signifikan dalam jumlah serangan siber, terutama ransomware dan DDoS, yang mengakibatkan kerugian pada sistem TI nasional. Situasi ini menjadikan keamanan siber sebagai salah satu indikator dalam menilai kinerja instansi pemerintah.[3].

Peran keamanan siber sangat penting karena menyangkut stabilitas dan keselamatan sebuah negara. Meningkatnya kejahatan siber di Indonesia disebabkan oleh pertumbuhan jumlah pengguna internet yang terus meningkat. Untuk mengatasi hal tersebut, diperlukan upaya yang efektif guna melindungi pengguna dunia maya dari berbagai potensi ancaman. Keamanan siber tidak hanya melibatkan pengamanan data, tetapi juga menjaga keberlanjutan layanan kritis di berbagai sektor.

Security Information and Event Management (SIEM) menjadi salah satu solusi dalam memperkuat keamanan siber. SIEM membantu petugas keamanan siber dengan memberikan informasi detail terkait serangan yang terjadi pada lingkungan server[4]. Namun, data yang ditampilkan oleh SIEM sering kali sangat banyak dan kompleks, sehingga menyulitkan petugas dalam menganalisis serangan. Oleh karena itu, diperlukan *tool* yang dapat membantu mengidentifikasi serangan guna meningkatkan efisiensi analisis[5].

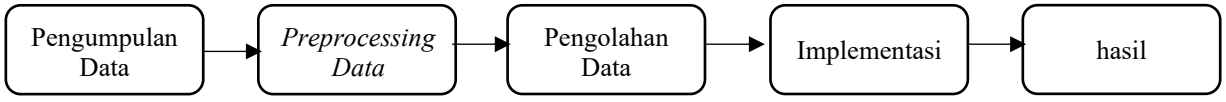
Wazuh adalah salah satu perangkat lunak yang memiliki fitur SIEM dengan visibilitas keamanan yang mendalam[6]. Perangkat ini mampu memantau aktivitas pada host baik di tingkat sistem operasi maupun aplikasi. Saat ini, melalui Wazuh mampu mengidentifkasi setiap insiden yang terjadi berdasarkan periode waktu dan dikategorikan sesuai dengan atribut tertentu [7]. Contoh atribut tersebut meliputi *common web attack, SQL injection attempt, shellshock attack,* hingga *login attack.*

Dengan demikian diperlukan klasifikasi pada data log serangan tersebut. Algoritma Naïve Bayes dapat diterapkan sebagai solusi penentuan klasifikas[8]. Naïve Bayes mengklasifikasikan berdasarkan probabilitas dengan asumsi bahwa setiap data bersifat independen satu sama lain.[9]. Algoritma ini dapat dengan efektif mengidentifikasi jenis serangan apabila didukung oleh jumlah data latih yang memadai.[10]. Jumlah data latih yang lebih banyak akan meningkatkan akurasi prediksi, sehingga administrator server dapat lebih mudah menentukan apakah serangan terjadi pada level sistem operasi atau aplikasi.

Penelitian ini bertujuan untuk menganalisis *event log* serangan dengan pendekatan naïve bayes. Penelitian ini dilakukan dengan mengidentifikasi dan mengklasifikasikan jenis serangan berdasarkan level kejadian, yaitu pada sistem operasi (server) atau aplikasi (web). Dengan hasil klasifikasi ini, maka didapatkan pengetahuan yang lebih jelas mengenai potensi risiko yang dihadapi. Selain itu, penelitian ini juga dapat memberikan solusi konkret dalam meningkatkan efisiensi pengelolaan keamanan siber.

2. METODE PENELITIAN

Pada penelitian ini digunakan metode kualitatif dan implementatif. Kualitatif digunakan untuk menganalisis dan memahami tinjauan literatur yang relevan dengan variabel atau objek yang digunakan dalam pengumpulan data[11]. Penelitian yang bersifat implementatif adalah penelitian yang menerapkan sebuah metode pada perangkat lunak dan perangkat keras, tidak hanya melakukan analisis data saja[12]. Dengan menggabungkan kedua metode diharapkan menambah wawasan mendalam dan solusi yang aplikatif. Metode kualitatif dapat mengidentifikasi kebutuhan dan konteks sesuai dengan atribut yang muncul pada *event log* Wazuh, sedangkan metode implementatif memungkinkan pengujian solusi yang diusulkan. Sehingga penggunaan kedua metode ini dapat memberikan hasil yang lengkap, baik dari aspek teoritis maupun praktis. Diagram alur penelitian ditampilkan pada Gambar 1.



Gambar 1. Tahapan penelitian

2.1 Pengumpulan Data

Langkah pertama dimulai dengan mengumpulkan data log kejadian, di mana peneliti memilih agen yang akan dijadikan objek, kemudian menentukan kategori serangan, serta menetapkan tanggal awal dan akhir periode menggunakan aplikasi

Wazuh. Data dari Wazuh diekspor kedalam bentuk C*omma Separated Values* (csv). Berikutnya melakukan *preprocessesing* data untuk mendapatkan nilai sesuai kebutuhan penelitian.

2.2 *Preprocessing* Data

Preprocessing data adalah tahap untuk membersihkan data, yang meliputi pemeriksaan untuk mendeteksi adanya data duplikat atau data yang hilang. Jika ditemukan data duplikat atau yang hilang, data tersebut dapat diisi menggunakan median, rata-rata, atau dihapus. Data penelitian diperoleh dari SIEM dengan memanfaatkan aplikasi Wazuh, yang mencakup 8 atribut fitur yaitu *Defense Evasion, Privilege Escalation, Discovery, Initial Access, Execution, Impact, Credential Access, Reconnaissance* dan 1 atribut label yaitu *Attact Area* pada periode 1-31 Desember 2024 di Dinas XYZ.

2.4 Pembuatan Model Klasifikasi

Klasifikasi adalah proses pembuatan atau penerapan pola-pola yang memberikan gambaran untuk membedakan kelompok data atau desain untuk mempertimbangkan kategori subjek dengan label kelas yang tidak pasti. Tujuan klasifikasi adalah untuk mengelompokkan data ke dalam kategori berdasarkan karakteristiknya[13]. Teknik Klasifikasi digunakan untuk menetukan jenis ancaman termasuk kedalam kategori yang berada di level server atau level aplikasi.

Klasifikasi dengan metode Naïve Bayes menghitung probabilitas menjadi bagian dari proses klasifikasi. Teorema Bayes menjelaskan cara mengevaluasi probabilitas suatu peristiwa dengan mempertimbangkan pengetahuan yang ada mengenai kemungkinan terjadinya peristiwa tersebut. Berikut adalah rumus untuk menghitung persamaan Teorema Bayes:

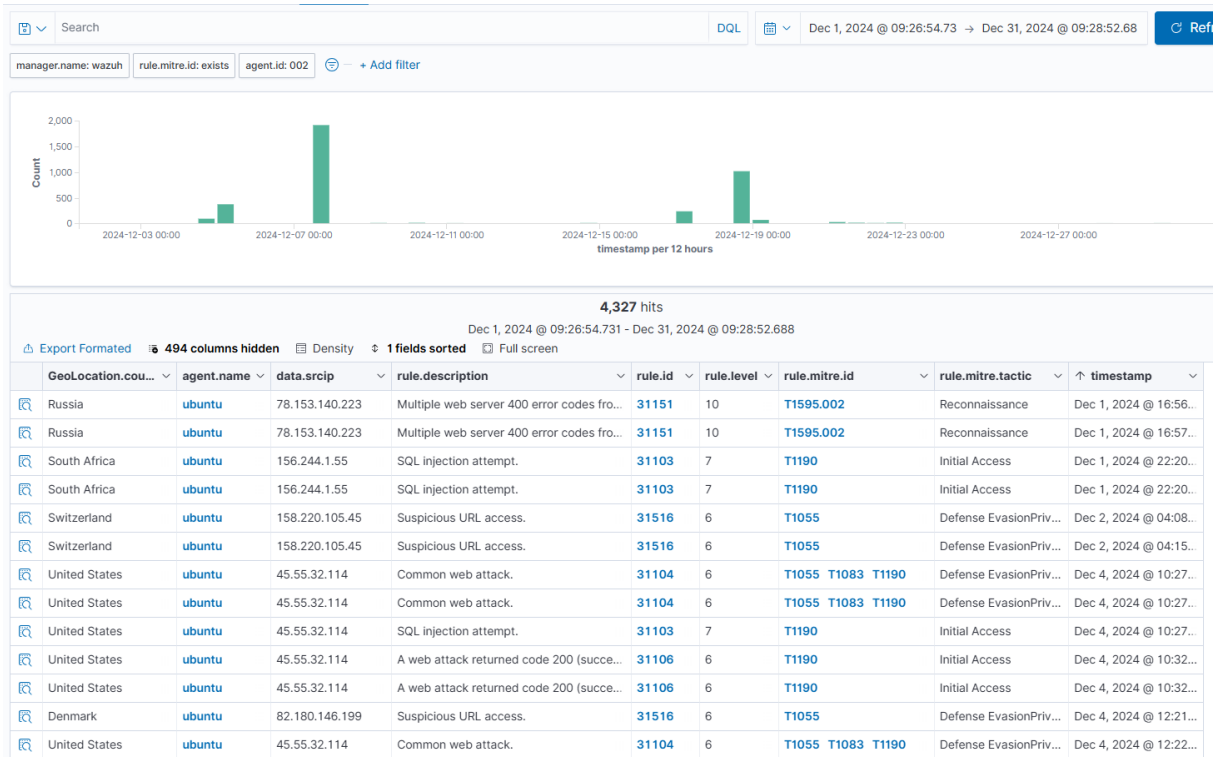
$$P(U|R) = \frac{\mathrm{P(R|U)} \times \mathrm{P(U)}}{\mathrm{P(R)}} \quad (1)$$

Keterangan:
R = Data dari suatu kelas yang belum diketahui.
U = Hipotesis yang berkaitan dengan data dari kelas tertentu.
P(U|R) = Probabilitas hipotesis U, berdasarkan kejadian R
P(R) = Probabilitas terjadinya kejadian R
P(U) = Probabilitas eksistensi hipotesis U
P(R|U) = Probabilitas terjadinya kejadian R untuk hipotesis U tetap

3. HASIL DAN PEMBAHASAN

3.1 Data Training

Penelitian ini memanfaatkan data yang diperoleh dari aplikasi Wazuh dengan mengakses halaman administrasi melalui web *browser*. Selanjutnya memilih *agent* yang menjadi target dan memilih *event* sesuai dengan priode yang diinginkan. Untuk Mendapatkan file dengan format .csv dapat dilakukan dengan menekan tombol *export formated*.



GeoLocation.cou...	agent.name	data.srcip	rule.description	rule.id	rule.level	rule.mitre.id	rule.mitre.tactic	timestamp
Russia	ubuntu	78.153.140.223	Multiple web server 400 error codes fro...	31151	10	T1595.002	Reconnaissance	Dec 1, 2024 @ 16:56..
Russia	ubuntu	78.153.140.223	Multiple web server 400 error codes fro...	31151	10	T1595.002	Reconnaissance	Dec 1, 2024 @ 16:57..
South Africa	ubuntu	156.244.1.55	SQL injection attempt.	31103	7	T1190	Initial Access	Dec 1, 2024 @ 22:20..
South Africa	ubuntu	156.244.1.55	SQL injection attempt.	31103	7	T1190	Initial Access	Dec 1, 2024 @ 22:20..
Switzerland	ubuntu	158.220.105.45	Suspicious URL access.	31516	6	T1055	Defense EvasionPriv...	Dec 2, 2024 @ 04:08..
Switzerland	ubuntu	158.220.105.45	Suspicious URL access.	31516	6	T1055	Defense EvasionPriv...	Dec 2, 2024 @ 04:15..
United States	ubuntu	45.55.32.114	Common web attack.	31104	6	T1055 T1083 T1190	Defense EvasionPriv...	Dec 4, 2024 @ 10:27..
United States	ubuntu	45.55.32.114	Common web attack.	31104	6	T1055 T1083 T1190	Defense EvasionPriv...	Dec 4, 2024 @ 10:27..
United States	ubuntu	45.55.32.114	SQL injection attempt.	31103	7	T1190	Initial Access	Dec 4, 2024 @ 10:27..
United States	ubuntu	45.55.32.114	A web attack returned code 200 (succe...	31106	6	T1190	Initial Access	Dec 4, 2024 @ 10:32...
United States	ubuntu	45.55.32.114	A web attack returned code 200 (succe...	31106	6	T1190	Initial Access	Dec 4, 2024 @ 10:32...
Denmark	ubuntu	82.180.146.199	Suspicious URL access.	31516	6	T1055	Defense EvasionPriv...	Dec 4, 2024 @ 12:21...
United States	ubuntu	45.55.32.114	Common web attack.	31104	6	T1055 T1083 T1190	Defense EvasionPriv...	Dec 4, 2024 @ 12:22...

Gambar 2. Data Tranining

3.2 *Preprocessing* Data

Tahapan *prepocessing* data dilakukan setelah mendapatkan file dataset berupa file .csv untuk kemudian dilakukan normalisasi dengan ketentuan diambil 500 baris serta menghapus kolom yang tidak digunakan. Penggunaan kolom disesuaikan dengan kategorisasi label dan atribut. Data hasil eksport dari aplikasi Wazuh yang masih berupa file dengan format csv dibuka menggunakan Microsoft Excel. Selanjutnya dilakukan pemilihan kolom yang akan digunakan sebagai dataset yaitu kolom *rule description* dan kolom *mitre tactic*.

Proses normalisasi data pada penelitian ini menghilangkan karakter yang tidak digunakan seperti tanda kurung dan petik atas. ([, “,]). Proses penghapusan karakater menggunakan fitur *replace* yang ada di Microsoft Excel. Selain melakukan penghapusan karakter tidak terpakai, proses kali ini juga melakukan kategorisasi serangan yang terjadi dengan ketentuan yang ditunjukkan pada tabel 1.

Tabel 1. Table Kategorisasi

No	Attack	Area
1	A web attack returned code 200 (success).	web
2	Apache: Attempt to access forbidden directory index.	server
3	CMS (WordPress or Joomla) login attempt.	web
4	Common web attack.	web
5	File deleted.	server
6	Integrity checksum changed.	server
7	Multiple common web attacks from same source IP.	web
8	Multiple SQL injection attempts from same source IP.	web
9	Multiple XSS (Cross Site Scripting) attempts from same source IP.	web
10	Shellshock attack detected.	server
11	SQL injection attempt.	web
12	Suspicious URL access.	server
13	URL too long. Higher than allowed on most browsers. Possible attack.	web
14	Wazuh agent stopped.	Server

Data export Wazuh menunjukkan jenis serangan yang dilakukan dengan *tactic* bervariasi sehingga perlu dilakukan normalisasi table. Jenis *tactic* yang muncul dijadikan sebagai atribut untuk perhitungan naive bayes. Atribut yang digunakan antara lain *Defense Evasion, Privilege Escalation, Discovery, Initial Access, Execution, Impact, Credential Access, Reconnaissance.* Berdasarkan tabel kategorisasi dan disesuaikan dengan label dan atribut maka didapatkan tabel hasil normalisasi sebagai berikut:

Tabel 2. Hasil Normalisasi

Attack Area	*Defense Evasion*	*Privilege Escalation*	*Discovery*	*Initial Access*	*Execution*	*Impact*	*Credential Access*	*Reconnaissance*
web	1	1	1	1	0	0	0	0
web	1	1	1	1	0	0	0	0
web	0	0	0	1	0	0	0	0
web	0	0	0	0	1	0	0	0
web	0	0	0	1	0	0	0	0
web	0	0	0	1	0	0	0	0
web	1	1	0	1	0	0	0	0
web	0	0	0	1	0	0	0	0
web	0	0	0	1	0	0	0	0
web	0	0	0	1	0	0	0	0
web	0	0	0	0	1	0	0	0
web	0	0	0	0	1	0	0	0
web	0	0	0	0	1	0	0	0
web	1	1	1	1	0	0	0	0
web	0	0	0	1	0	0	0	0
server	0	0	0	0	0	1	0	0
server	0	0	0	0	0	1	0	0
server	0	0	0	0	0	1	0	0
web	1	1	1	1	0	0	0	0
web	0	0	0	0	0	0	1	0

Keterangan:
0 = Tidak terjadi insiden dengan *tactic* fitur
1 = Terjadi insiden dengan *tactic* fitur

3.3 Penghitungan Naïve Bayes

3.3.1 Probabilitas Prior

Perhitungan probabilitas prior berdasarkan pada distribusi label "Attack Area" di dalam dataset.

Total data n = 500

$$P(web) = \frac{jumlah\ web}{n} \quad (2)$$

$$P(server) = \frac{jumlah\ server}{n} \quad (3)$$

Dihasilkan:
P(web) = 0.566
P(server) = 0.434

- DEFENSE EVASION:
  P(Defense Evasion | Attack Area=web):
  P(1 | web) = 0.34
  P(0 | web) = 0.66
  P(Defense Evasion | Attack Area=server):
  P(1 | server) = 0.18
  P(0 | server) = 0.82

- PRIVILEGE ESCALATION:
  P(Privilege Escalation | Attack Area=web):
  P(1 | web) = 0.41
  P(0 | web) = 0.59
  P(Privilege Escalation | Attack Area=server):
  P(1 | server) = 0.14
  P(0 | server) = 0.86

- DISCOVERY:
  P(Discovery | Attack Area=web):
  P(1 | web) = 0.29
  P(0 | web) = 0.71
  P(Discovery | Attack Area=server):
  P(1 | server) = 0.00
  P(0 | server) = 1.00

- INITIAL ACCESS:
  P(Initial Access | Attack Area=web):
  P(1 | web) = 0.78
  P(0 | web) = 0.22
  P(Initial Access | Attack Area=server):
  P(1 | server) = 0.02
  P(0 | server) = 0.98

- EXECUTION:
  P(Execution | Attack Area=web):
  P(0 | web) = 0.84
  P(1 | web) = 0.16
  P(Execution | Attack Area=server):
  P(0 | server) = 1.00
  P(1 | server) = 0.00

- IMPACT:
  P(Impact | Attack Area=web):
  P(0 | web) = 1.00
  P(1 | web) = 0.00
  P(Impact | Attack Area=server):
  P(0 | server) = 0.89
  P(1 | server) = 0.11

- CREDENTIAL ACCESS:
  P(Credential Access | Attack Area=web):
  P(0 | web) = 0.97
  P(1 | web) = 0.03
  P(Credential Access | Attack Area=server):
  P(0 | server) = 1.00
  P(1 | server) = 0.00

- RECONNAISSANCE:
  P(Reconnaissance | Attack Area=web):
  P(0 | web) = 1.00
  P(1 | web) = 0.00
  P(Reconnaissance | Attack Area=server):
  P(0 | server) = 0.27
  P(1 | server) = 0.73

3.3.2 Pengujian

Sebelum melakukan pengujian perlu di tentukan *convusion matrix* yaitu tabel yang menunjukkan empat kombinasi nilai prediksi dan nilai aktual yang berbeda[14]. Pengujian model dilakukan untuk mngetahui efektiftas metode naive bayes dalam mengklasifikan data. Serta untuk memastikan bahwa algoritma ini memberikan solusi yang tepat dalam konteks analisis dan klasifikasi data sesuai kebutuhan. Pengujian yang dilakukan antara lain:

1. Penghitungan Nilai Akurasi
   Pengukuran model menghasilkan prediksi yang akurat, baik untuk hasil positif maupun negatif.
2. Penghitungan Nilai Presisi
   Pengukuran akurasi prediksi positif yang dihasilkan oleh model.
3. Penghitungan Nilai Recall
   Pengukuran seberapa baik model dalam menemukan semua data positif yang sebenarnya.
4. Penghitungan Nilai F1-score
   Pengukuran rata-rata harmonik dari presisi dan recall, yang digunakan untuk mengukur keseimbangan antara presisi dan recall dalam evaluasi kinerja model.

3.4 Implementasi

Aplikasi penghitungan dibangun menggunakan bahasa pemrograman Python dengan menambahkan *library*, Streamlit, Pandas, Scikit-Learn, NumPy. Aplikasi dijalankan menggunakan *browser* Google Chrome, seperti tampilan dibawah ini

Gambar 3. Tampilan Upload File Log

	Attack Area	Defense Evasion	Privilege Escalation	Discovery	Initial Access	Execution	Impact	Cred
0	web	1	1	1	1	0	0	
1	web	1	1	1	1	0	0	
2	web	0	0	0	1	0	0	
3	web	0	0	0	0	1	0	
4	web	0	0	0	1	0	0	

Gambar 4. Data *Preview*

Gambar 5. Pemilihan Label

Target variable distribution:

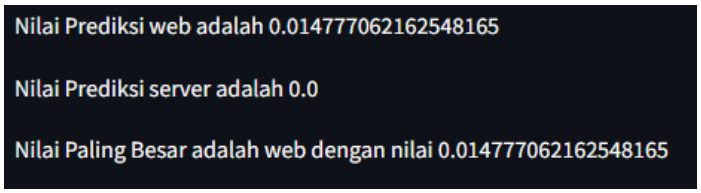
Attack Area	count
web	283
server	217

Accuracy on test set: 0.99

Classification Report on test set:

	precision	recall	f1-score	support
0	1	0.9831	0.9915	59
1	0.9891	1	0.9945	91
accuracy	0.9933	0.9933	0.9933	0.9933
macro avg	0.9946	0.9915	0.993	150
weighted avg	0.9934	0.9933	0.9933	150

Gambar 6. Pengujian Data



Gambar 7. Hasil Perhitungan

4. KESIMPULAN

Hasil pengujian menunjukkan performa yang sangat baik dari model Naive Bayes pada kedua kelas yaitu presisi=0.98, recall=1, f1-score=0.99, support=57. Hal ini mengindikasikan model mampu mengklasifikasikan data dengan akurasi tinggi. Penelitian ini berhasil menganalisis data *event log* yang terdapat pada *Security Information and Event Management* (SIEM) di Dinas XYZ. Melalui dataset yang didapat melalui log *event* pada aplikasi Wazuh didapatkan 8 atribut fitur dan 1 atribut label. Dan dapat dikategorisasikan area serangan menjadi 2 yaitu area web dan server. Metode naive bayes berhasil digunakan untuk mengklasifikasikan data serangan berdasarkan pola *tactic* yang terekam di dalam log. Hasil klasifikasi membantu SIEM dalam memberikan informasi terkait jenis ancaman serangan tersebut mengarah ke area web atau server, sehingga memudahkan analisis dan respon yang lebih cepat.

Melalui analisis yang mendalam terhadap pola serangan, tim keamanan dapat dengan cepat mengidentifikasi jenis ancaman yang sedang terjadi dan menentukan langkah-langkah pencegahan yang strategis serta efektif. SIEM memberikan kontribusi meningkatkan kemampuan Dinas XYZ untuk mendeteksi dan merespons ancaman keamanan siber secara cepat dan efisien. Dengan pengoptimalan lebih lanjut, sistem ini dapat menjadi solusi yang lebih efektif dalam menghadapi perkembangan ancaman siber yang semakin kompleks.

DAFTAR PUSTAKA

[1] Direktorat Operasi Keamanan Siber and B. S. D. S. Negara, "Laporan Tahunan Monitoring Keamanan Siber," *Direktorat Operasi Keamanan Siber Badan Siber Dan Sandi Negara*, 2022.

[2] O. Prasetia, S. Machfud, and G. A. Ibnurhus, "Sosialiasi Pengenalan Pentingnya Cyber Security Guna Menjaga Keamanan Data di Era Digital Pada Siswa/i SMK Bakti Idhata Jakarta," *JIPM J. Inov. Pengabdi. Masy.*, vol. 2, no. 1, 2024, doi: 10.55903/jipm.v2i1.141.

[3] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2022," *Badan Siber dan Sandi Negara*, 2022.

[4] M. Nas, F. Ulfiah, and U. Putri, "Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan," *J. Teknol. Elekterika*, vol. 20, no. 2, p. 92, 2023, doi: 10.31963/elekterika.v20i2.4536.

[5] H. Khotimah, F. Bimantoro, and R. S. Kabanga, "Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat," *J. Begawe Teknol. Inf.*, vol. 3, no. 2, pp. 213–219, 2022, doi: 10.29303/jbegati.v3i2.752.

[6] B. Haryanto and D. W. Chandra, "Implementasi Wazuh Integritas File untuk Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW," *J. Indones. Manaj. Inform. dan Komun.*, vol. 5, no. 1, 2024, doi: 10.35870/jimik.v5i1.447.

[7] N. Firman Pratama, "Perancangan Sistem Deteksi Dini Keamanan Informasi DISKOMINFO Kabupaten Bandung," *J. Tek. Inform. dan Sist. Inf.*, vol. 10, no. 1, 2023.

[8] T. D. Ramadhan, D. Wahiddin, and E. E. Awal, "Klasifikasi Sentimen Terhadap Pinjaman Online (Pinjol) Menggunakan Algoritma Naive Bayes," *Sci. Student J. Information, Technol. Sci.*, vol. IV, no. 1, 2023.

[9] H. Annur, "Klasifikasi Masyarakat Miskin Menggunakan Metode Naive Bayes," *Ilk. J. Ilm.*, vol. 10, no. 2, 2018, doi: 10.33096/ilkom.v10i2.303.160-165.

[10] H. A. Damar Rani and S. Zuhri, "Sistem Prediksi Kondisi Kelahiran Bayi menggunakan Klasifikasi Naïve Bayes," *Joined J. (Journal Informatics Educ.*, vol. 3, no. 2, 2020, doi: 10.31331/joined.v3i2.1432.

[11] S. I. Alfaeni and M. Asbari, "Kurikulum Merdeka: Fleksibilitas Kurikulum bagi Guru dan Siswa," *J. Inf. Syst. Manag.*, vol. 2, no. 5, 2023.

[12] Y. JOKO PRESETYO, R. WIDYAWATI, and M. MARDIANA, "PERENCANAAN PEMBANGUNAN MESS PRAMUKA 2 LANTAI BUMI PERKEMAHAN GANDUS," *Semin. Nas. Ins. Prof.*, vol. 3, no. 2, 2023, doi: 10.23960/snip.v3i2.525.

[13] N. Bayes, A. F. Abadi, N. Alamsyah, F. G. Retnanto, E. Daniati, and A. Ristyawan, "Penerapan Data Mining dalam Mengklasifikasi Penyakit Stroke Menggunakan Algoritma," *Agustus*, vol. 7, pp. 2549–7952, 2024.

[14] Z. P. P. Joy Lawa Rizky, "Analisis Perbandingan Algoritma Pembelajaran Mesin untuk Meningkatkan Akurasi dan Klasifikasi Tumor Otak," 2024, *iJAi (Indonesian Journal of Applied Informatics)*. [Online]. Available: https://jurnal.uns.ac.id/ijai/article/view/90101/pdf