Jurnal Teknik Informatika (JUTIF)
Vol. 5, No. 2, April 2024, pp. 415-427

DOI: https://doi.org/10.52436/1.jutif.2024.5.2.1822
p-ISSN: 2723-3863
e-ISSN: 2723-3871

SURICATA ACCURACY OPTIMIZATION BASED ON LIVE ANALYSIS USING ONE-CLASS SUPPORT VECTOR MACHINE METHOD AND STREAMLIT FRAMEWORK

I Putu Yesha Agus Ariwanta[*1], Kadek Yota Ernanda Aryanto[2], I Gede Aris Gunadi[3]

[1,2,3]Postgraduate Programs, Computer Science Study Program, Universitas Pendidikan Ganesha,
Email: [1]yesha@student.undiksha.ac.id, [2]yota.ernanda@undiksha.ac.id, [3]igedearisgunadi@undiksha.ac.id

(Article received: February 1, 2024; Revision: February 20, 2024; Published: April 04, 2024)

Abstract

Based on data from the Checkpoint website, there are more than 10 million cyber-attacks in a single day, and the top sequence of this cyber-attack is evident in educational institutions. The IT unit of Kartini Bali Health Polytechnic has not yet conducted testing for accuracy and speed to detect suspicious activities on the computer network. The implementation of network security systems that have not undergone testing will undoubtedly have a negative impact on system providers and users. The application of Live Analysis based on a website and the One-Class Support Vector Machine (SVM) is used to optimize the capabilities of the Suricata in detecting suspicious activities on computer networks and providing visual and real-time reports. This research utilizes the Suricata for optimizing the computer network security system, with the researcher using the Streamlit Framework for Live Analysis based on a website and the One-Class Support Vector Machine (SVM) for classifying log data and visual reporting. For testing the computer network security system, tools such as Nmap, Loic, and Brutus are used. The results of the research using the One-Class Support Vector Machine (SVM) in detecting three types of attacks Port Scanning, DDOS Attack, and Brute Force Attack, show an accuracy value of 96%, precision of 95%, recall of 96%, and F1-Score of 95%. In the performance and load testing of the live analysis system using the Streamlit framework, the results show that the developed system is responsive, with CPU usage at 38%, memory usage at 62.3%, and an average system load time of 5 milliseconds.

Keywords: *security computer network, optimization, live analysis, one-class SVM, suricata, streamlit*

OPTIMASI AKURASI SURICATA BERBASIS LIVE ANALYSIS MENGGUNAKAN METODE ONE-CLASS SUPPORT VECTOR MACHINE DAN FRAMEWORK STREAMLIT

Abstrak

Berdasarkan data dari situs *checkpoint* terdapat 10 juta lebih serangan *cyber* dalam satu hari dan urutan teratas serangan *cyber* tersebut ditunjukkan di institusi pendidikan. Unit TIK Politeknik Kesehatan Kartini Bali belum melakukan pengujian nilai akurasi dan kecepatan untuk mendeteksi aktivitas mencurigakan di jaringan komputer Politeknik Kesehatan Kartini Bali. Sistem keamanan jaringan komputer yang belum dilakukan pengujian tentu akan berdampak buruk bagi penyedia dan pengguna sistem. Penerapan *Live Analysis* berbasis *website* dan *Algoritma Machine Learning One-Class Support Vector Machine* (SVM) digunakan untuk mengoptimalkan kemampuan *Intrusion Detection System* (IDS) Suricata dalam mendeteksi aktivitas mencurigakan pada jaringan komputer serta memberikan laporan secara visual dan *real-time*. Penelitian ini menggunakan *Intrusion Detection System* (IDS) Suricata untuk melakukan optimasi sistem keamanan jaringan komputer peneliti menggunakan *Framework* Streamlit sebagai *Live Analysis* berbasis *website* dan *Algoritma Machine Learning One-Class Support Vector Machine* (SVM) untuk klasifikasi *log* data dan pelaporan secara visual sedangkan untuk pengujian sistem keamanan jaringan komputer menggunakan *tools* Nmap, Loic dan Brutus. Hasil dari penelitian menggunakan *Algoritma One-Class Support Vector Machine* (SVM) dalam mendeteksi tiga jenis serangan yaitu *Port Scanning*, *DDOS Attack* dan *Brute Force Attack* didapatkan hasil yaitu nilai akurasi sebesar 96%, *precision* 95%, *recall* 96% dan *F1-Score* 95%. Sedangkan pada pengujian performa dan *load* sistem *live analysis* menggunakan *Framework* Streamlit didapatkan hasil bahwa sistem yang peneliti *develop* bersifat *responsive* dan *CPU Usage* 38%, *Memory Usage* 62.3% dan rata-rata waktu load sistem sebesar 5 (ms).

Kata kunci: *keamanan jaringan komputer, optimasi, live analisis, one-class SVM, suricata, streamlit*

1. PENDAHULUAN

Pasca pandemi COVID-19, saat ini penggunaan dan perkembangan teknologi informasi mengalami percepatan yang sangat signifikan, contohnya di institusi pendidikan yang memanfaatkan teknologi informasi untuk bertukar informasi dan data melalui jaringan komputer atau internet. Semakin meningkatnya penggunaan jaringan komputer atau internet tentu resiko atau ancaman akan muncul terhadap pengguna dan penyedia layanan. Keamanan jaringan komputer telah menjadi masalah besar di institusi pendidikan untuk menjaga integritas dan keberlangsungan operasional institusi tersebut. Berdasarkan data dari situs *checkpoint* terdapat 10 juta lebih serangan *cyber* dalam satu hari dimana jenis serangan *Denial of Service Attack* menjadi 8 besar jenis serangan *cyber* yang digunakan oleh *Cybercriminals* dan urutan teratas serangan *cyber* tersebut ditunjukkan di institusi pendidikan. Dari data tersebut dapat di katakan bahwa setiap menit ada serangan *cyber* yang terjadi di seluruh dunia dan institusi pendidikan merupakan target teratas serangan *cyber* tersebut.

Institusi pendidikan menggunakan jaringan komputer atau internet untuk berbagai keperluan operasional seperti menyimpan data sensitif atau administrasi, memberikan akses ke sumber daya digital, dan melakukan proses pembelajaran[1]. Maka dari itu perlindungan keamanan jaringan komputer menjadi aspek penting dalam institusi pendidikan. Keamanan jaringan komputer di institusi pendidikan melibatkan langkah-langkah untuk melindungi data pribadi dosen dan mahasiswa, mencegah akses tidak sah terhadap sumber daya digital dan melindungi kekayaan intelektual yang dimiliki oleh institusi pendidikan tersebut[2]. Dalam operasionalnya institusi pendidikan perlu melakukan pemantauan serta pemeliharaan sistem jaringan komputer dan mengadopsi kebijakan atau standar sistem keamanan jaringan komputer yang di terbitkan oleh pemerintah.

Menurut Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 tentang Standar Sistem Manjemen Keamanan Informasi (SMKI), bahwa setiap penyelenggara sistem elektronik harus mematuhi SMKI dengan memegang nilai CIA Kerahasian (*Confidentiality*), Keutuhan (*Availability*), dan Ketersediaan (*Integrity*). Oleh karena itu idealnya keamanan jaringan komputer di institusi pendidikan dapat efektif melindungi data sensitif, mencegah ancaman, dan menjaga integritas jaringan. Selain itu, kekurangan keamanan dalam sistem dapat memungkinkan masuknya peretas yang berpotensi menyebabkan kerusakan atau mengubah fungsi sistem yang sudah ada[3]. Untuk memenuhi standar tersebut institusi pendidikan wajib memiliki kebijakan keamanan jaringan yang jelas dan terdokumentasi. Kebijakan tersebut mencakup kebijakan akses yang terbatas, tindakan pencegahan serangan *malware*, dan langkah-langkah lainnya untuk melindungi jaringan komputer. Selain itu Institusi pendidikan juga wajib memiliki sistem pemantauan dan deteksi keamanan yang aktif. Hal ini untuk mendeteksi aktivitas mencurigakan atau serangan, termasuk serangan *DDoS*, serangan *phishing*, atau upaya peretasan[4].

Politeknik Kesehatan Kartini Bali merupakan sebuah institusi pendidikan tinggi di bidang kesehatan. Sebagai lembaga pendidikan, Politeknik Kesehatan Kartini Bali juga menggunakan teknologi informasi dan jaringan komputer untuk mendukung kegiatan operasional dan pembelajaran. Politeknik Kesehatan Kartini Bali menggunakan jaringan komputer untuk mendukung konektivitas, komunikasi, akses informasi di seluruh kampus dan termasuk penyediaan akses internet yang cepat dan stabil bagi mahasiswa, dosen dan staf. Institusi pendidikan ini memiliki tiga buah server yang berfungsi untuk sistem *web server*, sistem informasi terintegrasi (SISTER) perguruan tinggi, dan sistem Neo Feeder PDDikti.

Agar pelayanan dan operasional institusi berjalan dengan baik maka perlu pengamanan atau perlindungan yang baik pula. Politeknik Kesehatan Kartini Bali menggunakan sistem *Intrusion Detection System* (IDS) Snort sebagai pendeteksi aktifitas mencurigakan di jaringan komputer dan sistem *firewall* sederhana yang ada pada router mikrotik sebagai sistem pengamanan jaringan komputer. Snort adalah sebuah arsitektur *singlethread* yang menggunakan tumpukan TCP/IP untuk mendeteksi dan memeriksa isi paket jaringan[5][6]. Berdasarkan penelitian[7] ditemukan bahwa Serangan pada jaringan komputer dapat terdeteksi tergantung pola serangan pada konfigurasi rules pada snort. Oleh sebab itu, rules perlu di update secara rutin. Firewall pada mikrotik digunakan sebagai komponen yang mengatur akses antara jaringan yang dilindungi, dan merupakan solusi untuk mengatasi keamanan dalam sebuah jaringan yang rentan terhadap berbagai ancaman, baik dari dalam maupun luar jaringan[8]. Pada penelitian[9] didapatkan bahwa kelemahan firewall yang disediakan oleh router mikrotik tidak menampilkan peringatan bahwa sebuah *IP Address* yang dicurigai melakukan anomali pada jaringan komputer telah diblok. Sistem snort dan *firewall* pada Politeknik Kesehatan Kartini Bali membantu menentukan paket jaringan komputer yang boleh lewat dan yang diblokir berdasarkan *rule* yang ditentukan oleh administrator jaringan. Jika terdapat aktifitas mencurigakan dan aktifitas tersebut adalah serangan tetapi tidak terdaftar pada rule keamanan yang terdaftar atau terjadi kesalahan dalam mendefinisikan suatu *rule* maka dapat sangat berbahaya bagi jaringan komputer. Dari data dan fakta yang ada dilapangan untuk mengoptimasi sistem keamanan jaringan komputer di Politeknik Kesehatan Kartini Bali peneliti mengusulkan untuk memanfaatkan *Framework* Streamlit sebagai *Live*

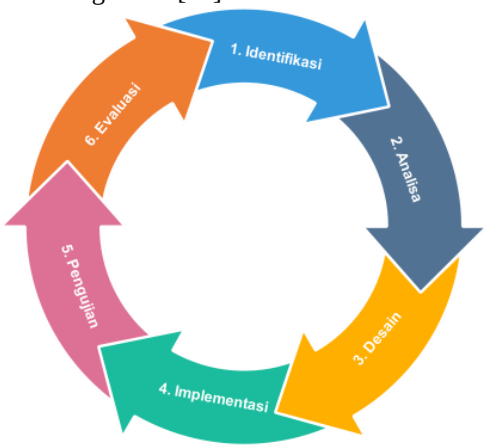
Analysis berbasis *website* untuk memberikan hasil analisa *event* dan *log* paket jaringan komputer. Penggunaan *framework* streamlit cocok untuk membuat visualisasi data dengan antarmuka pengguna yang *responsive*[10]. *One-Class Support Vector Machine* (SVM) merupakan pengembangan dari metode *Support Vector Machine* (SVM) yang digunakan untuk masalah deteksi anomali[11]. Penelitian ini menggunakan *Algoritma One-Class Support Vector Machine* (SVM) pada *Intrusion Detection System* (IDS) untuk melakukan analisa dan menemukan anomali data pada jaringan komputer Politeknik Kesehatan Kartini Bali, penggunaan *algoritma* tersebut didasarkan pada penelitian[12] yang berdasarkan pengujian Nilai akurasi *algoritma One-Class Support Vector Machine* (SVM) sebesar 98.08%. Pada penelitian ini akan mengimplementasikan sistem *Intrusion Detection System* (IDS) Suricata untuk menggantikan sistem lama yaitu Snort. Penggunaan sistem *Intrusion Detection System* (IDS) Suricata didasarkan pada penelitian[13] yang berdasarkan pengujian nilai akurasi suricata didapat 61% dibanding snort yang hanya 31%. Dari segi penggunaan memori, Suricata lebih stabil daripada Snort dikarenakan Suricata menggunakan fitur *multithreading*. Hal ini memungkinkan Suricata untuk memproses banyak tugas secara bersamaan, sehingga dapat mengoptimalkan penggunaan memori dengan lebih efisien daripada Snort yang menggunakan arsitektur singlethread[14][15].

Berdasarkan hal tersebut ditemukan bahwa sistem keamanan jaringan komputer yang ada di Politeknik Kesehatan Kartini Bali saat ini perlu dioptimalkan ke sistem yang baru. Maka penelitian ini akan mengimplementasi dan melakukan analisa penggunaan *Framework* Streamlit sebagai *Live Analysis* berbasis *website*, penerapan *Algoritma Machine Learning One-Class Support Vector Machine* (SVM) pada *Intrusion detection system* (IDS) dan mengimplementasi sistem *Intrusion Detection System* (IDS) Suricata untuk memecahkan masalah yang ada di sistem keamanan jaringan komputer Politeknik Kesehatan Kartini Bali, Maka peneliti akan mengangkat penelitian ini dengan judul "Optimasi Akurasi Suricata Berbasis *Live Analysis* Menggunakan Metode *One-Class Support Vector Machine* (SVM) dan *Framework* Streamlit Studi Kasus Poltekkes Kartini Bali". Dengan dilakukan penelitian ini diharapkan dapat melakukan optimasi keamanan jaringan komputer di Politeknik Kesehatan Kartini Bali.

2. METODE PENELITIAN

2.1. Tahapan Penelitian

Pada penelitian ini memiliki lingkup penelitian yang akan dibahas yaitu keamanan jaringan komputer pada Politeknik Kesehatan Kartini Bali, Tahap penelitian merupakan gambaran umum mengenai alur penelitian yang dikerjakan dalam penelitian ini dari awal hingga akhir. Tahapan yang dilakukan dalam penelitian ini dapat dilihat pada Gambar 1 yang terdapat enam tahapan yaitu Identifikasi, Analisa, Desain, Implementasi, Pengujian, dan Evaluasi menggunakan metode pengembangan sistem *Security Policy Development Life Cycle* (SPDLC) yang memiliki tujuan utama untuk mengembangkan dan memelihara kebijakan keamanan organisasi Lingkup dari metode SPDLC sendiri berkaitan dengan aspek keamanan informasi dan pengaturan kebijakan yang melibatkan tindakan, praktik, dan prosedur untuk melindungi aset informasi organisasi[16].

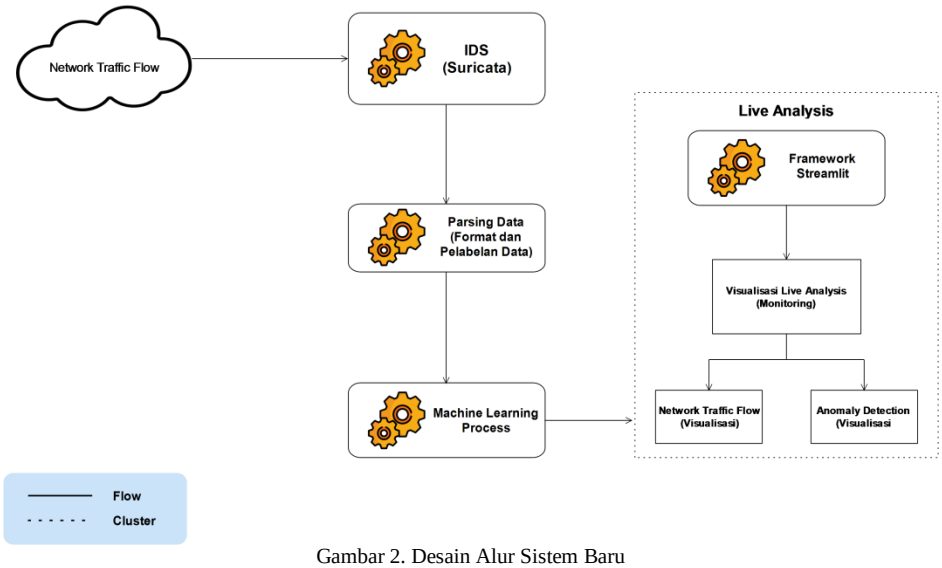


Gambar 1. Tahapan Penelitian

Berikut penjelasan pada gambar 1:

1. Identifikasi, Pada tahap ini peneliti melakukan identifikasi untuk menemukan berbagai macam masalah sistem keamanan yang dihadapi oleh jaringan komputer yang sedang berjalan di Politeknik Kesehatan Kartini Bali. Ditemukan bahwa pada saat ini sistem keamanan jaringan komputer yang sedang berjalan menggunakan sistem *Intrusion Detection System* (IDS) Snort dan *Firewall* dari *router* mikrotik.
2. Analisa, Pada tahap ini peneliti melakukan analisa masalah sistem keamanan yang dihadapi oleh jaringan komputer yang sedang berjalan di Politeknik Kesehatan Kartini Bali. Ditemukan bahwa sistem keamanan jaringan komputer yang sedang berjalan menggunakan sistem *Intrusion Detection System* (IDS) Snort dan *Firewall* dari *router* mikrotik yang belum dilakukan pengujian nilai akurasi dan kecepatan untuk mendeteksi anomali pada jaringan komputer Politeknik Kesehatan Kartini Bali. Selain itu pada sistem keamanan jaringan komputer yang sedang berjalan belum ada sistem pengumpulan dan pelaporan informasi event atau log jaringan komputer secara visual. Sistem *Intrusion Detection System* (IDS) Snort pada penelitian[13] yang berdasarkan hasil pengujian nilai akurasi yang di dapat hanya 31%.

3. Desain, Pada tahap ini peneliti mendesain rancangan sistem keamanan jaringan komputer baru pada Politeknik Kesehatan kartini Bali yang akan dibangun dan membuat alur sistem keamanan jaringan.



Gambar 2. Desain Alur Sistem Baru

Pada Gambar 2 merupakan alur sistem keamanan jaringan komputer Politeknik Kesehatan Kartini Bali pada desain sistem keamanan jaringan komputer yang baru menggunakan *algoritma machine learning One-Class Support Vector Machine* (SVM) pada *Intrusion Detection System* (IDS) Suricata hasil dari analisa tersebut di tampilkan menggunakan *Framework* Streamlit berbasis *website* untuk menampilkan hasil analisa secara visual.

4. Implementasi, Pada tahap ini dilakukan penerapan hasil dari desain atau perancangan yang telah dilakukan pada tahap sebelumnya. Tahap implementasi diawal peneliti melakukan penggantian sistem *Intrusion Detection System* (IDS) Snort ke sistem yang baru menggunakan Suricata, pada penelitian ini dikerjakan menggunakan Bahasa pemrograman *python*. dengan rincian untuk tahapan *preprocessing* hingga pemodelan menggunakan *software jupyter notebook* dan untuk *deployment* dengan *framework* streamlit menggunakan *software* notepad++.
5. Pengujian, Pada tahap ini peneliti akan menguji sistem keamanan jaringan komputer baru yang telah diimplementasi atau diterapkan untuk memastikan bahwa sistem keamanan jaringan komputer yang telah di terapkan sudah sesuai dengan tujuan awal. Pengujian yang dilakukan meliputi pengujian fungsionalitas dasar, pengujian *logging* dan *monitoring*, pengujian *rules* suricata, pengujian performa aplikasi, dan pengujian waktu *load* sistem.
6. Evaluasi, Pada tahap ini peneliti melakukan evaluasi dari hasil pengujian atau testing yang telah dilakukan pada tahap sebelumnya, dan melihat sejauh mana tingkat efektifitas dari penerapan sistem keamanan jaringan komputer baru tersebut. Evaluasi yang dilakukan meliputi evaluasi model *One-Class Support Vector Machine* (SVM) dan evaluasi responsive dan waktu *load* sistem *live analysis*.

2.2. Waktu dan Lokasi Penelitian

Waktu dan tempat penelitian dengan judul Optimasi Akurasi Suricata Berbasis *Live Analysis* Menggunakan Metode *One-Class Support Vector Machine* (SVM) dan *Framework* Streamlit adalah di Politeknik Kesehatan Kartini Bali yang beralamat di Jl. Piranha No 2 Pegok Sesetan dengan estimasi waktu penelitian selama empat bulan mulai minggu pertama bulan September 2023 hingga minggu pertama bulan Desember 2023.

2.3. Data

Data pada penelitian ini merupakan data dari hasil pencatatan atau *Log* Jaringan komputer di Politeknik Kesehatan Kartini Bali saat waktu normal aktivitas kegiatan di tempat studi kasus yang terdiri dari 73.299 rekaman data, data *log* jaringan komputer merupakan data yang diperoleh dari *Intrusion Detection System* (IDS) Suricata. Data *log* jaringan ini terdiri dari 15 indikator menentukan aktivitas normal atau anomali pada jaringan komputer[17]. Berikut merupakan penjelasan dari setiap attribut yang ada pada data dan akan digunakan.

Tabel 1. Attribut Data

Attribut	Keterangan
flow_id	Identitas aliran atau koneksi jaringan yang unik setiap koneksi atau aliran data
pkts_toserver	Jumlah paket yang dikirimkan ke server dalam aliran
pkts_toclient	Jumlah paket yang dikirimkan ke klien dalam aliran
bytes_toserver	Jumlah byte yang dikirimkan ke server dalam aliran
bytes_toclient	Jumlah byte yang dikirimkan ke klien dalam aliran
state	Jenis koneksi atau komunikasi pada aliran data antara server dan client
alerted	Informasi kejadian yang memicu peringatan pada sistem suricata
alert_gid	ID grup aturan yang terkait dengan peringatan
alert_signature_id	ID tanda tangan yang digunakan dalam peringatan
alert_rev	Revisi aturan tanda tangan
alert_severity	Jenis tingkatan peringatan
hour	Jam pencatatan log
minute	Menit pencatatan log
second	Detik pencatatan log
label	Target (Aktivitas jaringan normal atau anomaly)

2.4. Parsing dan Pelabelan Data

Data *log* yang dihasilkan oleh *Intrusion Detection System* (IDS) Suricata masih berformat json untuk memudahkan dalam proses selanjutnya peneliti mengubah format JSON ke CSV. Proses parsing data menggunakan bahasa pemrograman *Python* dengan *library json* untuk membantu menguraikan data berformat JSON[18]. Dalam proses parsing data diambil fitur-fitur atau atribut data yang akan digunakan peneliti untuk proses pelatihan model *One-Class Support Vector Machine* (SVM) dalam mendeteksi anomali data di jaringan komputer Politeknik Kesehatan kartini Bali. Sebelum ke tahap *preprocessing* data, data yang sudah di parsing ke format CSV selanjutnya dilakukan pelabelan data untuk membedakan data jaringan komputer normal dan data jaringan komputer anomali hasil dari proses tersebut menghasilkan data yang akan di gunakan untuk data pelatihan dan data pengujian.

2.5. *Handling Outlier*

Setelah data melewati tahap parsing dan pelabelan, peneliti kemudian melakukan analisis terhadap *outlier*. *Outlier* merujuk pada nilai dari objek pengamatan yang mungkin memiliki nilai yang ekstrem, baik terlalu rendah maupun terlalu tinggi, yang dapat mengakibatkan ketidakakuratan dalam hasil akhir analisis. Dalam penelitian ini, peneliti mengatasi *outlier* dengan menggunakan metode *Z-Score*. Metode *Z-Score* digunakan untuk mengidentifikasi data yang memiliki nilai ekstrem, baik yang terlalu rendah maupun terlalu tinggi, yang kemudian akan dihapus dari analisis[19].

2.6. Pengecekan *Correlation*

Pengecekan korelasi digunakan untuk menilai hubungan antara dua atau lebih variabel. Tujuan dari analisis korelasi adalah untuk mengukur sejauh mana perubahan dalam satu variabel dapat dikaitkan dengan perubahan dalam variabel lainnya. Oleh karena itu, pada tahap *preprocessing*, peneliti melakukan pengecekan korelasi data menggunakan fungsi *corr* dari pustaka pandas. Hasilnya divisualisasikan menggunakan pustaka *plotly* untuk memfasilitasi interpretasi korelasi antar variabel[20]. Pada tahap ini, kriteria hasil perhitungan korelasi digunakan untuk menilai interpretasi hubungan antar variabel.

Tabel 2. Koefisien Korelasi

Koefisien	Keterangan
0	Tidak ada korelasi antara variabel
>0 – 0,25	Korelasi Sangat Lemah
>0,25 – 0,5	Korelasi Cukup
>0,5 – 0,75	Korelasi Kuat
1	Korelasi sempurna positif
-1	Korelasi sempurna negatif

Pada tabel 2 di atas, peneliti akan menghapu koefisien korelasi data yang lemah sehingga menyisakan korelasi data cukup, kuat dan sempurna.

2.7. Klasifikasi dengan *One-Class SVM*

One-Class Support Vector Machine (SVM) merupakan pengembangan dari metode *Support Vector Machine* (SVM) yang digunakan untuk masalah deteksi anomali. Pada penelitian ini dalam hal deteksi anomali tujuan nya adalah untuk mengidentifikasi data aktivitas jaringan komputer yang tidak umum atau tidak sesuai pola dalam dataset pelatihan sehingga algoritma ini hanya memerlukan data mayoritas saat melakukan pelatihan dan membuat pola data aktivitas normal jaringan komputer[11]. Berikut merupakan Langkah-langkah dari klasifikasi dengan *One-Class Support Vector Machine* (SVM) pada *log* yang dihasilkan oleh *Intrusion Detection System* (IDS) Suricata :

1. Membagi *dataset* yang telah melewati proses *preprocessing* menjadi dua bagian, yakni data latih dan data uji, dengan perbandingan persentase 80% untuk data latih dan 20% untuk data uji.
2. Mengoptimalkan parameter pada *One-Class Support Vector Machine* (SVM) melalui proses *tuning* parameter menggunakan metode *GridSearch Cross Validation*. *GridSearchCV*, sebagai bagian dari modul *scikit-learn*, secara otomatis dan sistematis melakukan validasi terhadap beberapa model dan setiap *hyperparameter*. Setelah proses *GridSearchCV* selesai, model yang diperoleh akan dilengkapi dengan skor terbaik yang telah dihasilkan.

2.8. Evaluasi

Tahap ini dimanfaatkan oleh peneliti untuk mengevaluasi kinerja model yang telah dikembangkan. Peneliti menggunakan *confusion matrix* sebagai alat untuk menganalisis kinerja model yang telah dibuat. *Confusion matrix* merupakan tabel yang mencakup 4 kombinasi berbeda antara nilai prediksi dan nilai aktual[21]. Selanjutnya, dari *confusion matrix* tersebut, peneliti dapat menghitung nilai akurasi, *precision*, *recall*, dan *F1 Score* untuk menilai seberapa baik model dapat memprediksi hasil. Selain mengukur peforma model yang dihasilkan, peneliti juga melakukan evaluasi sistem *live analysis* yang di *deploy* peneliti melakukan pengujian pada bagian performa aplikasi dan waktu *load* aplikasi.

2.9. *Deployment*

Setelah melewati tahapan pembuatan model dan evaluasi, langkah berikutnya adalah tahapan *deployment* model atau mengimplementasikan hasil dalam antarmuka aplikasi *live analysis*. Model yang telah dibuat disimpan dalam *format joblib* untuk diintegrasikan ke dalam sistem. *Framework* yang digunakan dalam pembuatan sistem ini adalah Streamlit[22]. berikut merupakan desain sistem *live analysis* berbasis *website*.

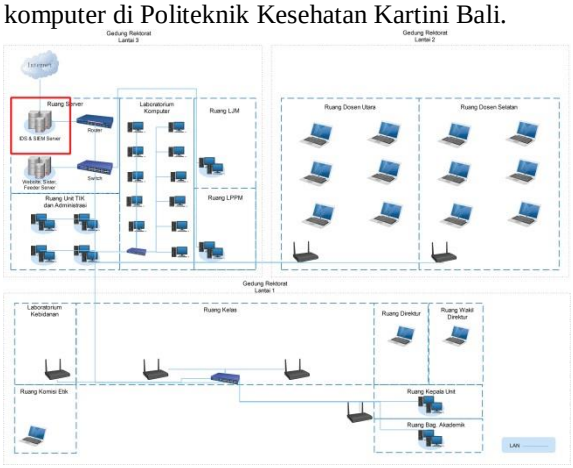
3. HASIL DAN PEMBAHASAN

3.1. Implementasi Sistem

Setelah menganalisis sistem yang sedang berjalan di Politeknik Kesehatan Kartini Bali dan merancang desain sistem baru yang akan diimplementasikan, langkah berikutnya adalah menerapkan sistem keamanan jaringan komputer. Hal ini bertujuan agar sistem baru yang telah dirancang dapat beroperasi sesuai dengan desain yang telah dibuat sebelumnya. Pada tahap implementasi atau penerapan desain sistem keamanan jaringan komputer, detail rancangan atau desain digunakan sebagai petunjuk atau panduan untuk memandu proses implementasi sehingga sistem yang dikembangkan dapat sesuai dengan desain yang telah dirancang. Proses implementasi mencakup instalasi dan konfigurasi untuk memastikan kesesuaian antara sistem yang dibangun dengan desain yang telah direncanakan sebelumnya.

3.2. Implementasi Topologi Jaringan

Dalam implementasi topologi jaringan, peneliti mengumpulkan semua perangkat yang diperlukan, termasuk *hardware* dan *software*. Selanjutnya, peneliti menempatkan perangkat-perangkat tersebut sesuai dengan topologi yang telah dirancang sebelumnya. Pada perangkat *server* Suricata, beberapa konfigurasi penting yang dilakukan mencakup alamat *internet protocol*, *subnet mask*, alamat *IP gateway*, dan alamat *IP DNS*[23]. Setelah semua perangkat terhubung satu sama lain, langkah selanjutnya adalah mengkonfigurasi setiap perangkat agar dapat berkomunikasi dengan perangkat lainnya. Pada Gambar 3 merupakan topologi jaringan komputer di Politeknik Kesehatan Kartini Bali.



Gambar 3. Topologi Jaringan Komputer

3.3. Konfigurasi Komputer *Server* Suricata

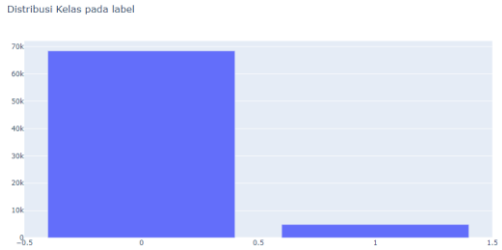
Komponen utama dan pendukung yang peneliti implementasi pada komputer server *Intrusion Detection System* (IDS) adalah sebagai berikut :

1. Implementasi dan Konfigurasi Suricata, sebagai komponen utama komputer *server Intrusion Detection System* (IDS) dengan melakukan instalasi sistem suricata versi 7.0.2 yang lebih stabil saat dirilis selanjutnya peneliti melakukan instalasi sistem tersebut sampai *Intrusion Detection System* (IDS) Suricata terpasang di komputer *server* dan melakukan konfigurasi *file* suricata.yaml peneliti mengedit *file* tersebut menggunakan *software* notepad++.
2. Implementasi dan konfigurasi Npcap, sebagai komponen pendukung fungsi *Intrusion Detection System* (IDS) Suricata. Peneliti menggunakan Npcap versi 1.78, Npcap sendiri memiliki fungsi sebagai *software packet capture* untuk mendukung kinerja suricata. Selanjutnya peneliti melakukan instalasi sistem tersebut sampai Npcap terpasang di komputer *server*.
3. Implementasi dan Konfigurasi *Framework* Streamlit, streamlit sebagai *framework python* pada penelitian ini digunakan untuk menampilkan hasil klasifikasi *algoritma machine learning One-Class Support Vector Machine* (SVM*) log* suricata dalam bentuk *live analysis* agar laporan dapat secara *real-time* diketahui oleh *administrator* jaringan. Setelah pemasangan *framework python* streamlit berhasil selanjutnya dilakukan pengujian untuk memastikan instalasi streamlit telah berhasil dengan cara ketik perintah *streamlit hello* pada tampilan terminal sehingga akan muncul

notifikasi perintah untuk mengakses halaman *demo* streamlit.

3.4. Hasil Parsing dan Pelabelan Data

Pada tahap ini peneliti melakukan pengambilan data di lokasi penelitian dan melakukan pengujian suricata menggunakan tiga metode serangan yaitu, Port Scanning, Ddos Attack, dan *Brute Force Attack*. Hasil rekaman data tersebut disimpan oleh suricata pada *file* eve.json dan selanjutnya peneliti melakukan parsing data json ke csv.



Gambar 4. Perbandingan Jumlah Rekaman

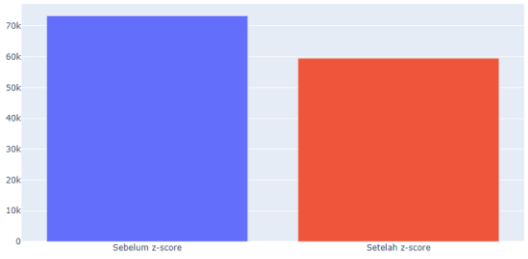
Pada Gambar 4 merupakan perbandingan jumlah rekaman *log* jaringan komputer yang dihasilkan oleh *Intrusion Detection System* (IDS) Suricata. Nilai 0 merupakan aktivitas jaringan komputer yang dianggap normal dan nilai 1 merupakan aktivitas jaringan komputer yang dianggap anomali.

3.5. Hasil *Handling Outlier*

Setelah melalui tahap parsing data untuk mengubah *file log* suricata *format* JSON ke CSV menggunakan bahasa pemrograman Python dengan *library* json untuk membantu menguraikan data berformat JSON. Tahap selanjutnya yaitu melakukan *filter outlier* dengan metode *Z-Score*. Dalam penelitian ini berikut langkah-langkah untuk melakukan *filter outlier* dengan metode *Z-score*.

1. Peneliti memulai dengan menghitung nilai *z-score* pada setiap kolom menggunakan *library numpy* dan fungsi stats pada *library scipy*. Nilai *z-score* di setiap kolom diabsolutkan dan disimpan dalam variabel z.
2. Selanjutnya, peneliti melakukan penyaringan data dengan mengambil nilai yang memiliki nilai absolut kurang dari 3 atau lebih dari 3.
3. Langkah terakhir adalah penghapusan data yang memiliki nilai absolut kurang dari 3 atau lebih dari 3 dari dataset.

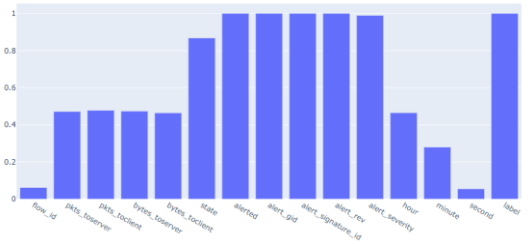
Setelah menjalankan sumber kode pada *software Jupyter Notebook* dengan menggunakan *library numpy* dan fungsi *stats* dari *library scipy*, di mana nilai yang memiliki nilai absolut kurang dari 3 atau lebih dari 3 pada data akan dihapus, ditemukan bahwa jumlah data yang awalnya 73.299 *record* berubah menjadi 59.523 *record*. Hal ini mengindikasikan bahwa terdapat 13.776 *record data* yang dianggap sebagai *outlier* karena melebihi batas atas dan batas bawah yang ditentukan.



Gambar 5. Hasil *Handling Outlier*

3.6. Hasil Pengecekan *Correlation*

Setiap variabel memiliki korelasi positif atau negatif dengan target, namun tidak semua variabel tersebut memiliki korelasi yang signifikan terhadap target. Oleh karena itu, korelasi yang lemah dapat memengaruhi akurasi hasil dari model *machine learning*. Oleh karena itu, peneliti sangat penting untuk melakukan pengecekan korelasi pada tahap ini. Langkah ini digunakan untuk menentukan variabel mana yang memiliki pengaruh signifikan terhadap target dan mana yang tidak. Dalam penelitian ini, peneliti menghapus variabel atau kolom pada *dataset* yang memiliki korelasi lemah terhadap target, dengan parameter korelasi yang digunakan yaitu di atas -0,25 dan 0,25.



Gambar 6. Hasil Pengecekan *Correlation*

Berdasarkan Gambar 6, terlihat bahwa variabel atau kolom *flow_id*, *minute*, dan *second* menunjukkan korelasi yang lemah terhadap target. Nilai koefisien dari variabel atau kolom tersebut berada di atas -0.25 dan di bawah 0.25. Oleh karena itu, peneliti memutuskan untuk menghapus variabel atau kolom tersebut dari *dataset*.

3.7. Analisa dan Hasil dengan *One-Class SVM*

Setelah data melalui tahapan *preprocessing*, selanjutnya adalah data dimasukkan ke tahap pemrosesan sehingga mendapatkan hasil yang diharapkan. *One-Class Support Vector Machine* (SVM) merupakan pengembangan dari metode *Support Vector Machine* (SVM) yang digunakan untuk masalah deteksi anomali. Dalam deteksi anomali, tujuan adalah untuk mengidentifikasi data yang tidak umum atau tidak sesuai dengan pola yang ada dalam dataset pelatihan[24]. Setelah membagi dataset menjadi 80% untuk data latih 20% untuk data uji dan pada proses *hyperparameter tuning* menggunakan *Grid Search Cross Validation* dihasilkan parameter terbaik sebagai berikut.

Tabel 3. Hasil *Hyperparameter Tuning*

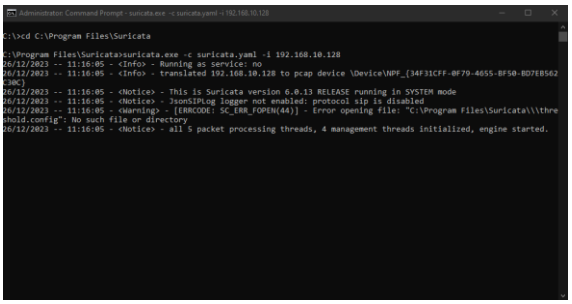
Parameter	Value
gamma	0.001
kernel	Rbf
nu	0.01

Dalam Tabel 3, ditemukan bahwa parameter terbaik yang dihasilkan melalui teknik *Grid Search Cross Validation* adalah *gamma* sebesar 0.001, kernel jenis rbf, dan nilai nu sebesar 0.01. Pada parameter tersebut, skor terbaik yang berhasil dicapai adalah sebesar 90%. Parameter hasil dari Tabel 3 kemudian digunakan untuk melakukan *fitting model* dengan menerapkan *algoritma One-Class Support Vector Machine* (SVM). Hasil dari *fitting model* ini kemudian diuji dan dievaluasi dalam langkah selanjutnya.

3.8. Pengujian dan Evaluasi Suricata

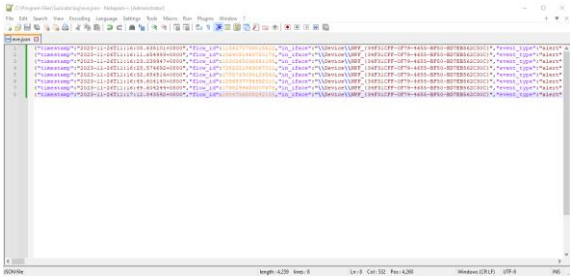
Pengujian *Intrusion Detection System* (IDS) Suricata merupakan tahap untuk memastikan bahwa sistem dapat efektif mendeteksi dan merespons serangan yang berbahaya. Pada tahap ini ada beberapa langkah yang dilakukan untuk memastikan bahwa sistem berfungsi dengan baik seperti pengujian fungsionalitas dasar, dan pengujian *logging* dan *monitoring*.

1. Pengujian fungsionalitas dasar suricata dilakukan pada sensor deteksi, Pada gambar 7 sensor deteksi *Instrusion Detection System* (IDS) Suricata berhasil dijalankan selanjutnya peneliti melakukan pengujian pada sistem pencatatan atau *log* kejadian yang di deteksi oleh Suricata.



Gambar 7. Pengujian Fungsionalitas Suricata

2. Pengujian *logging* dan *monitoring* dilakukan untuk memastikan bahwa fungsionalitas sistem *Instrusion Detection System* (IDS) Suricata berjalan dengan baik. Untuk memastikan bahwa pencatatan *log* yang dilakukan oleh suricata berhasil dilakukan dapat dilihat pada *file* eve.json yang ada pada directory suricata. Pada gambar 8 pengujian *logging* dan *monitoring* suricata berhasil dilakukan dan sistem sensor deteksi suricata berhasil melakukan pembacaan dan pencatatan aktivitas yang dianggap anomali pada jaringan komputer Poltekkes Kartini Bali.

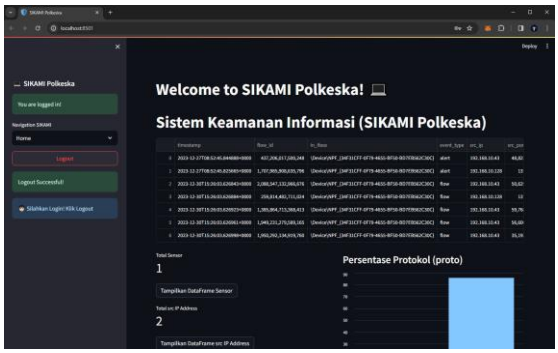


Gambar 8. Pengujian *Logging* dan *Monitoring* Suricata

3.9. Pengujian dan Evaluasi Sistem *Live Analysis*

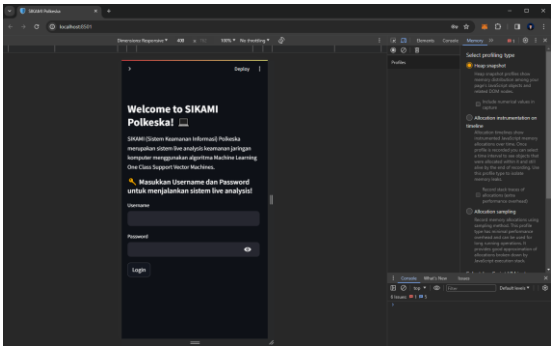
Pengujian Sistem *Live Analysis* yang dibangun menggunakan *Framework* Streamlit merupakan tahap untuk memastikan bahwa sistem dapat efektif melakukan analisa hasil *log* dari *Intrusion Detection System* (IDS) Suricata. Pada tahap ini ada beberapa langkah yang dilakukan untuk memastikan bahwa sistem berfungsi dengan baik seperti pengujian fungsionalitas dasar, pengujian performa aplikasi, dan pengujian waktu *load* sistem[25].

1. Pengujian fungsionalitas dasar sistem *live analysis* yang dibangun menggunakan *framework* streamlit, pengujian ini menggunakan *browser* google chrome untuk memastikan sistem yang peneliti *deploy* dapat berjalan dengan baik. Pada gambar 9 Sistem Keamanan Informasi (SIKAMI) Poltekkes Kartini Bali atau sistem *live analysis* yang dibangun berhasil berjalan dengan baik.



Gambar 9. Pengujian Fungsionalitas Sistem *Live Analysis*

2. Pengujian performa sistem *live analysis* yang dibangun menggunakan *framework* streamlit, pengujian ini menggunakan *browser* google chrome untuk menguji bagaimana performa sistem saat digunakan pengguna. Pada gambar 10 didapat bahwa sistem *live analysis* bersifat *Responsive* yang berarti *administrator* dapat mengakses sistem tersebut dengan berbagai perangkat seperti komputer atau *smartphone*. Didapat juga hasil bahwa sistem *live analysis* menggunakan *CPU Usage:* 38.0% dan *Memory Usage:* 62.3%.

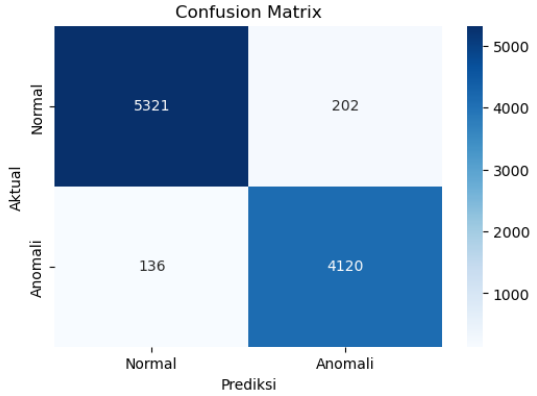


Gambar 10. Pengujian Performa Sistem *Live Analysis*

3. Pengujian waktu *load* sistem *live analysis* yang dibangun menggunakan *framework* streamlit, pengujian ini menggunakan *tools locust* pengujian ini untuk memastikan sistem yang peneliti *deploy* dapat berjalan dengan baik pada saat pengguna melakukan *load* sistem. Pada *request statistics* Jenis metode HTTP yang digunakan adalah *GET* dimana Total *request* sebanyak 450 permintaan HTTP telah dikirimkan selama pengujian didapatkan hasil bahwa *Average* (ms) rata-rata waktu respon adalah 5 (ms), waktu respons minimum adalah 2 (ms) dan waktu respons maksimum adalah 23 (ms). Waktu respons rata-rata yang rendah dan jumlah kegagalan pengujian yang nol menunjukkan bahwa sistem yang diuji mampu menanggapi permintaan dengan baik selama periode pengujian tersebut.

3.10. Hasil Pengujian *Model One-Class SVM*

Sebelum menerapkan model ke Sistem Keamanan Informasi (SIKAMI) Poltekkes Kartini Bali atau sistem *live analysis* yang dibangun, peneliti memaparkan terlebih dahulu hasil evaluasi model untuk mengukur performa model yang dihasilkan. Peneliti menggunakan *confusion matrix* untuk melakukan analisa performa dari model.



Gambar 11. Hasil *Confusion Matrix*

Berdasarkan gambar 11 yang merupakan hasil *confusion matrix*, selanjutnya dapat dilakukan perhitungan *precision*, *recall*, dan *accuracy*. Berikut merupakan rumus beserta perhitungannya[26].

$$Akurasi = \frac{(TP+TN)}{(TP+FN+FP+TN)} * 100\% \quad (1)$$

$$Akurasi = \frac{(4120+5321)}{(4120+136+202+5321)} * 100\%$$

$$Akurasi = \frac{9441}{9779} * 100\%$$

$$Akurasi = 0.965 * 100\%$$

$$Akurasi = 96\%$$

Berdasarkan perhitungan untuk mencari nilai akurasi model didapatkan hasil bahwa model *One-Class Support Vector Machine* (SVM) yang digunakan peneliti untuk mendeteksi anomali jaringan komputer mendapatkan nilai 96% hal ini dapat disimpulkan bahwa model *One-Class Support Vector Machine* (SVM) memiliki akurasi sebesar 96% untuk mengklasifikasikan data dengan benar secara keseluruhan baik itu data normal atau data anomali pada dataset pelatihan. Adanya 4% kesalahan dari model *One-Class Support Vector Machine* (SVM) dikarenakan hasil pengujian terdapat nilai *False Negatif* (FN) dan *False Positif* (FP).

$$Presisi = \frac{\text{TP}}{(TP+FP)} * 100\% \quad (2)$$

$$Presisi = \frac{4120}{(4120+202)} * 100\%$$

$$Presisi = \frac{4120}{4322} * 100\%$$

$$Presisi = 0.95 * 100\%$$

$$Presisi = 95\%$$

Berdasarkan perhitungan untuk mencari nilai presisi model didapatkan hasil bahwa model *One-Class Support Vector Machine* (SVM) yang digunakan peneliti untuk mendeteksi anomali jaringan komputer mendapatkan nilai 95% hal ini dapat disimpulkan bahwa model *One-Class Support Vector Machine* (SVM) 95% prediksi positif yang dibuat oleh model adalah benar-benar positif. Adanya 5% kesalahan dari model *One-Class Support Vector Machine* (SVM) dikarenakan model lebih banyak kesalahan prediksi pada jenis serangan *port scanning* dan *brute force attack* dari pada jenis serangan *Ddos Attack*.

$$Recall = \frac{\text{TP}}{(TP+FN)} * 100\% \quad (3)$$

$$Recall = \frac{4120}{(4120+136)} * 100\%$$

$$Recall = \frac{4120}{4256} * 100\%$$

$$Recall = 0.968 * 100\%$$

$$Recall = 96\%$$

Berdasarkan perhitungan untuk mencari nilai *recall* model didapatkan hasil bahwa model *One-Class Support Vector Machine* (SVM) yang digunakan peneliti untuk mendeteksi anomali jaringan komputer mendapatkan nilai 96% hal ini dapat disimpulkan bahwa model *One-Class Support Vector Machine* (SVM) memiliki sensitivitas sebesar 96% ini berarti model dapat mengidentifikasi data positif atau anomali yang benar merupakan data positif atau anomali. Adanya 4% kesalahan dari model *One-Class Support Vector Machine* (SVM) dikarenakan model salah memprediksi yang seharusnya anomali diprediksi normal. Jumlah 136 data yang salah di prediksi normal merupakan jenis serangan *port scanning* dan *Brute Force Attack*.

$$F1 - Score = \frac{2*\text{Recall}*\text{Presisi}}{Recall+Presisi} * 100\% \quad (4)$$

$$F1 - Score = \frac{2 * 0.95 * 0.968}{0.95 * 0.968} * 100\%$$

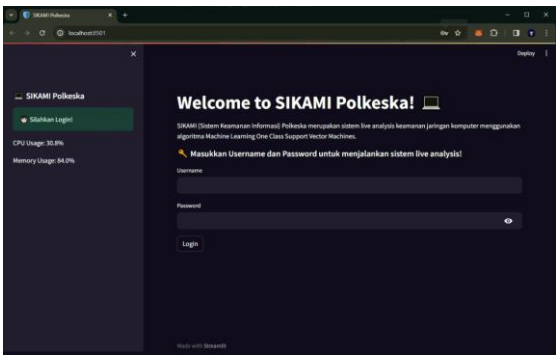
$$F1 - Score = 0.95 * 100\%$$

$$F1 - Score = 95\%$$

Berdasarkan perhitungan untuk mencari nilai *F1-Score* model didapatkan hasil bahwa model *One-Class Support Vector Machine* (SVM) yang digunakan peneliti untuk mendeteksi anomali jaringan komputer mendapatkan nilai 95%. *F1-Score* perbandingan rata-rata dari nilai *precision* dan *recall* menjadi satu nilai. Pada penelitian ini peneliti menghitung *F1-Score* ketidakseimbangan kelas, seperti dalam kasus deteksi anomali jaringan komputer.

3.11. Hasil Deploy Sistem *Live Analysis*

Setelah melalui tahapan pembuatan model dan evaluasi, selanjutnya yaitu tahapan *deployment* model atau menjabarkan hasil *interface* aplikasi *live analysis*. Dimana model disimpan dalam ekstensi *joblib* untuk dimasukkan ke dalam sistem. *Framework* yang digunakan pada pembuatan sistem adalah streamlit. berikut merupakan desain sistem *live analysis* berbasis *web*site.

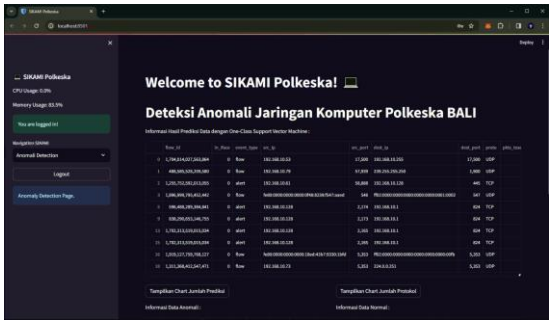


Gambar 12. Halaman *Login* Sistem *Live Analysis*

Pada gambar 12 merupakan tampilan awal saat melakukan akses sistem *live analysis* dimana halaman awal *administrator* jaringan komputer Poltekkes Kartini Bali diminta untuk memasukan *username* dan *password* sebelum ke halaman utama sistem *live analysis*.

Gambar 13. Halaman *Home* Sistem *Live Analysis*

Pada gambar 13 merupakan halaman *home* pada sistem *live analysis* yang peneliti *develop* pada halaman *home* berisi informasi *log* data *Intrusion Detection System* (IDS) Suricata yang belum di proses menggunakan *algoritma One-Class Support Vector Machine* (SVM). Pengguna atau *administrator* jaringan komputer dapat mengakses halaman *Anomali Detection* yang ada pada *navigation pane* yang ada pada tampilan sebelah kiri sistem *live analysis*.



Gambar 14. Halaman *Anomali Detection*

Pada gambar 14 merupakan halaman *anomali detection* yang dimana data *log Intrusion Detection System* (IDS) Suricata yang ada pada halaman *home* dilakukan *parsing data* dan di proses menggunakan *algoritma One-Class Support Vector Machine* (SVM) untuk menghasilkan data yang dianggap anomali pada jaringan komputer Poltekkes Kartini Bali. Pada halaman *anomali detection* berisi data lengkap hasil prediksi dari *algoritma One-Class Support Vector Machine* (SVM) dimana data hasil tersebut peneliti tampilkan di sistem *live analysis* untuk selanjutnya administrator jaringan dapat dengan cepat mengambil keputusan jika terjadi data jaringan komputer yang bersifat anomali.

4. DISKUSI

Pada penelitian ini dataset diambil dari *log* suricata yang ada pada komputer *server* Politeknik Kesehatan Kartini Bali. Pengambilan data dilakukan

saat jam normal aktivitas pengguna dan peneliti melakukan pengujian menggunakan tiga metode serangan yaitu *Port Scanning, Ddos Attack* dan *Brute Force Attack* untuk mengambil data sampel minoritas yang bersifat anomali pada jaringan komputer. *Algoritma* yang digunakan dalam penelitian ini ialah *One-Class Support Vector Machine* (SVM) dimana saat melakukan proses *hyperparameter tuning* menggunakan *Grid Search Cross Validation* dihasilkan parameter terbaik *gamma 0.001*, *kernel RBF*, dan *nu 0.01* dengan skor akurasi yang didapat yaitu 90%. Hasil pengujian model yang didapat berdasarkan *confusion matrix* dihasilkan nilai akurasi sebesar 96%, *precision* 95%, *recall* 96% dan *F1-Score* 95%.

Penelitian ini berhasil melakukan optimasi sistem keamanan jaringan komputer berdasarkan hasil penelitian sebelumnya yang dilakukan oleh peneliti[13] didapat bahwa nilai akurasi suricata hanya 61% dengan menggunakan *Algoritma One-Class Support Vector Machine* (SVM) nilai akurasi yang didapat sebesar 96% dengan tingkat sensitivitas atau *recall* sebesar 96% untuk mendeteksi anomali pada sebuah jaringan komputer selain itu sistem *live analysis* yang peneliti *deploy* juga memudahkan *administrator* jaringan komputer untuk mendapatkan informasi jika terdapat aktivitas jaringan komputer yang bersifat anomali. Sistem *live analysis* yang peneliti *deploy* menggunakan *framework* streamlit berhasil menangani kekurangan dari penelitian[9] yang didapatkan bahwa kelemahan firewall yang disediakan oleh router mikrotik tidak menampilkan peringatan bahwa sebuah *IP Address* yang dicurigai melakukan anomali pada jaringan komputer.

Pada pengujian sistem *live analysis* yang peneliti *deploy* menggunakan *framework* streamlit didapatkan hasil bahwa sistem bersifat *responsive* dan sistem *live analysis* menggunakan *CPU Usage:* 38.0% dan *Memory Usage:* 62.3%. Waktu *load* sistem *live analysis* Pada *request statistics* Jenis metode HTTP yang digunakan adalah *GET* dimana Total *request* sebanyak 450 permintaan HTTP telah dikirimkan selama pengujian didapatkan hasil bahwa *Average* (ms) rata-rata waktu respon adalah 5 (ms), waktu respons minimum adalah 2 (ms) dan waktu respons maksimum adalah 23 (ms). Waktu respons rata-rata yang rendah dan jumlah kegagalan pengujian yang nol menunjukkan bahwa sistem yang diuji mampu menanggapi permintaan dengan baik selama periode pengujian tersebut.

5. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan dalam penelitian ini maka dapat disimpulkan bahwa penelitian ini telah berhasil melakukan implementasi *Intrusion Detection System* (IDS) Suricata pada jaringan komputer Poltekkes Kartini Bali dan seluruh sistem pendukung suricata bekerja sesuai fungsinya, Implementasi sistem *Live Analysis* menggunakan *framework* streamlit telah berhasil melakukan *develop* dan implementasi pada *Intrusion Detection System* (IDS) Suricata sehingga seluruh sistem baru keamanan jaringan komputer Poltekkes kartini Bali berhasil diimplementasikan. Pengujian yang dilakukan didapat bahwa setelah melakukan implementasi sistem dan penerapan *algoritma One-Class Support Vector Machine* (SVM) untuk mendeteksi tiga jenis serangan yaitu *Port Scanning*, *DDOS Attack* dan *Brute Force Attack* didapatkan hasil evaluasi yaitu nilai akurasi sebesar 96%, *precision* 95%, *recall* 96% dan *F1-Score* 95%. Hasil nilai akurasi dan nilai *recall* yang didapat berhasil mengoptimasi *Intrusion Detection System* (IDS) Suricata dimana penelitian yang dilakukan sebelumnya mendapatkan nilai 61%. Sedangkan pada pengujian performa dan *load* sistem *live analysis* didapatkan hasil bahwa sistem yang peneliti *develop* bersifat *responsive* dan *CPU Usage* 38%, *Memory Usage* 62.3% dan rata-rata waktu *load* sistem sebesar 5 (ms).

DAFTAR PUSTAKA

[1] E. P. Silmina, A. Firdonsyah, R. Adhella, and A. Amanda, "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf," no. 3, pp. 83–91, 2022.

[2] R. RASNAL, "Implementasi Keamanan Jaringan Komputer Dengan Menggunakan Model Forensik Pada Kantor Dinas Pendidikan Kota Palopo," vol. 1, no. 1, pp. 35–42, 2022, [Online]. Available: http://repository.uncp.ac.id/id/eprint/1464

[3] F. Fachri, A. Fadlil, and I. Riadi, "Analisis Keamanan Webserver menggunakan Penetration Test," *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.

[4] M. Rijal Kamal and M. Andri Setiawan, "Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII," *Univ. Islam Indones.*, 2021.

[5] E. H. Kalabo, "Analisa Performa Intrusion Detection System (IDS) Snort Dan Suricata Terhadap Serangan TCP SYN Flood," *J. Repos.*, vol. 4, no. 3, pp. 397–406, 2022, doi: 10.22219/repositor.v4i3.1407.

[6] G. Jain and Anubha, "Application of SNORT and Wireshark in Network Traffic Analysis," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1119, no. 1, p. 012007, 2021, doi: 10.1088/1757-899x/1119/1/012007.

[7] D. Yuliandari, B. K. Raja, R. Ningsih, and A. J. Wahidin, "Simulasi Penerapan Sistem Monitoring Jaringan Snort NIDS Pada Web Server Menggunakan Metode SPDLC," vol. 5, no. 2, pp. 133–138, 2023.

[8] Bayu Santosa and Ali Akbar Rismayadi, "Implementasi Keamanan Jaringan Lan Menggunakan Mikrotik Dengan Metode Firewall Filtering," *E-PROSIDING Tek. Inform. Vol. 3, No. 1, Juni 2022*, vol. 3, no. 1, pp. 1–12, 2022.

[9] W. Wildan, A. Romadhona, and S. F. Ramadhani, "Implementasi Firewall Dan Proxy Menggunakan Prangkat Mikrotik Pada Laboratorium Komputer Smk Bina Potensi Palu," *JTIK (Jurnal Tek. Inform. Kaputama)*, vol. 7, no. 1, pp. 136–143, 2023, doi: 10.59697/jtik.v7i1.56.

[10] A. Putranto, N. L. Azizah, I. Ratna, and I. Astutik, "Web-based Heart Disease Prediction System Using SVM Method and Streamlit Framework [Sistem Prediksi Penyakit Jantung Berbasis Web Menggunakan Metode SVM dan Framework Streamlit]," pp. 1–9, 2013.

[11] D. N. Mhawi, A. Aldallal, and S. Hassan, "Advanced Feature-Selection-Based Hybrid Ensemble Learning Algorithms for Network Intrusion Detection Systems," *Symmetry (Basel).*, vol. 14, no. 7, 2022, doi: 10.3390/sym14071461.

[12] B. B. Sudhanshu Sekhar Tripathy, "PERFORMANCE EVALUATION OF MACHINE LEARNING ALGORITHMS FOR INTRUSION DETECTION SYSTEM," *J. Biomech. Sci. Eng.*, no. July, pp. 110–114, 2023, doi: 10.1109/ICISC47916.2020.9171147.

[13] Adam Dwi Ralianto and S. Cahyono, "Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Intrusi Lalu Lintas di Jaringan," *Info Kripto*, vol. 15, no. 2, pp. 69–75, 2021, doi: 10.56706/ik.v15i2.10.

[14] P. Veerasingam, S. Abd Razak, A. Faisal Amri Abidin, M. Afendee Mohamed, and S. Dhalila Mohd Satar, "Intrusion Detection and Prevention System in Sme'S Local Network By Using Suricata," *Malaysian J. Comput. Appl. Math.*, vol. 6, no. 1, pp. 21–30, 2023.

[15] J. Guo, H. Guo, and Z. Zhang, "Research on High Performance Intrusion Prevention System Based on Suricata," *Highlights Sci. Eng. Technol.*, vol. 7, pp. 238–245, 2022, doi: 10.54097/hset.v7i.1077.

[16] Yunanri. W and Yasinta Bella Fitriana, "Analisis Network Security Komputer Tingkat Desa Menggunakan Metode Security Policy Development Life Cycle (SPDLC)," *J. Tek. Juara Aktif Glob. Optimis*, vol. 1, no. 2, pp. 11–21, 2021, doi: 10.53620/jtg.v1i2.28.

[17] S. I. Abudalfa, E. S. Isleem, M. J. E. Khalil, and ..., "Evaluating Performance of Supervised Learning Techniques for Developing Real-Time Intrusion Detection System," *Int. J. Eng. Inf. Syst.*, vol. 6, no. 2, pp. 103–119, 2022.

[18] Y. D. Prabowo, "Deteksi Ujaran Kebencian pada Komentar Instagram dalam Bahasa Indonesia Menggunakan Metode Recurrent Neural Network," *KALBISIANA J. Sains, Bisnis dan Teknol.*, vol. 8, no. 1, pp. 461–468, 2022.

[19] A. Putranto, N. L. Azizah, and I. R. I. Astutik, "Sistem Prediksi Penyakit Jantung Berbasis Web Menggunakan Metode Svm Dan Framework," *J. Penerapan Sist. Inf. (Komputer Manajemen)*, vol. 4, no. 2, pp. 442–452, 2023, doi: 10.30645/kesatria.v4i2.180.

[20] S. Anwar, F. Septian, and R. D. Septiana, "Klasifikasi Anomali Intrusion Detection System (IDS) Menggunakan Algoritma Naïve Bayes Classifier dan Correlation-Based Feature Selection," *J. Teknol. Sist. Inf. dan Apl.*, vol. 2, no. 4, pp. 135–140, 2019, doi: 10.32493/jtsi.v2i4.3453.

[21] A. H. Azizan *et al.*, "A machine learning approach for improving the performance of network intrusion detection systems," *Ann. Emerg. Technol. Comput.*, vol. 5, no. Special issue 5, pp. 201–208, 2021, doi: 10.33166/AETiC.2021.05.025.

[22] ABU THOLIB, *Implementasi Algoritma Machine Learning Berbasis Web dengan Framework Streamlit*. Pustaka Nurja, 2023.

[23] Stephanie P. Adithama, M. Maslim, and J. A. M. Nugraha, "Perancangan Blueprint dan Pembangunan Jaringan Komputer Gereja Brayat Minulya Yogyakarta," *GIAT Teknol. untuk Masy.*, vol. 1, no. 1, pp. 1–11, 2022, doi: 10.24002/giat.v1i1.5844.

[24] M. R. Ayyagari, "Classification of Imbalanced Datasets using One-Class SVM, k-Nearest Neighbors and CART Algorithm," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 11, pp. 1–5, 2020, doi: 10.14569/IJACSA.2020.0111101.

[25] Fiqri Syah Redha, Renny Puspita Sari, and Syahru Rahmayuda, "Perbandingan Performa Web Services Yang Dibangun Menggunakan Arsitektur Monolithic Dan Microservices Pada Sistem Point of Sales," *J. Tek. Inform. dan Sist. Inf. ISSN*, vol. 10, no. 1, pp. 406–420, 2023.

[26] M. K. Suryadewiansyah and T. E. E. Tju, "Naïve Bayes dan Confusion Matrix untuk Efisiensi Analisa Intrusion Detection System Alert," *J. Nas. Teknol. dan Sist. Inf.*, vol. 8, no. 2, pp. 81–88, 2022, doi: 10.25077/teknosi.v8i2.2022.81-88.