Monitoring Performa Jaringan Lokal Menggunakan Protokol SNMP dan Dashboard Grafana

Angelica Barus[1*], Dedy Kiswanto[2], Gus Rosauli Pandiangan[3], Maria Winarni Br. Silitonga[4]
[1,2,3,4)] Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan
[1]angelicabarus99@gmail.com, [2]dedykiswanto@unimed.ac.id, [3]rosapandiangan71@gmail.com,
[4]mariawinarnibrsilitonga@gmail.com
*Penulis Korespondensi
(Gus Rosauli Pandiangan, Universitas Negeri Medan, rosapandiangan71@gmail.com)

ABSTRAK

Pemantauan jaringan berbasis SNMP konvensional umumnya menghasilkan data mentah yang memerlukan interpretasi manual. Kondisi ini menyulitkan deteksi anomali secara waktu nyata karena ambang batas statis gagal beradaptasi dengan dinamika lalu lintas jaringan. Penelitian ini bertujuan mengatasi keterbatasan tersebut dengan mengembangkan sistem pemantauan kinerja jaringan lokal waktu nyata yang mengintegrasikan SNMP dan algoritme *K-Means clustering* berpanduan ambang batas. Sistem ini mengklasifikasikan kondisi kesehatan jaringan secara otonom ke dalam tiga status: SEHAT, WASPADA, dan KRITIS. Penelitian menerapkan metodologi *Design Science Research* (DSRM) menggunakan arsitektur klien-server yang disimulasikan pada *Graphical Network Simulator* (GNS3) dengan *router* Cisco virtual. Data *throughput* diambil melalui basis data deret waktu Prometheus. Algoritme *K-Means* diinisialisasi menggunakan titik pusat berbasis standar teknik, sementara *exporter* berbasis Python menjembatani model pembelajaran mesin dengan tumpukan observabilitas secara langsung. Hasil evaluasi menunjukkan sistem berhasil beroperasi secara waktu nyata. Model pengelompokan memperoleh *Silhouette Score* sebesar 0,9055 melalui validasi silang lima lipatan, serta mencapai akurasi klasifikasi 100% terhadap label ambang batas manual. Capaian ini memvalidasi fungsionalitas artefak pada data simulasi yang bersih dan terpisah secara tegas. Luaran akhir berupa dasbor Grafana dua belas panel yang menyajikan visualisasi metrik secara komprehensif. Integrasi ini terbukti meningkatkan keteramatan jaringan simulasi, mendukung pengelolaan proaktif, dan meminimalkan kebutuhan inspeksi manual, sehingga menjadi rujukan praktis untuk pemantauan jaringan skala kampus maupun perusahaan kecil.

Kata kunci: Grafana; Pengelompokan K-Means; Machine Learning; Pemantauan Jaringan; Protokol Manajemen Jaringan Sederhana

ABSTRACT

Conventional SNMP-based network monitoring typically provides raw data requiring manual interpretation. This condition hinders real-time anomaly detection, as static thresholds fail to adapt to dynamic network traffic patterns. This research aims to address these limitations by developing a real-time local network performance monitoring system that integrates SNMP with a threshold-guided K-Means clustering algorithm. This system autonomously classifies network health status into three categories: HEALTHY, WARNING, and CRITICAL. The study adopts the Design Science Research Methodology (DSRM) utilizing a client-server architecture simulated within Graphical Network Simulator (GNS3) using virtual Cisco routers. Throughput metrics are collected via the Prometheus time-series database. The K-Means algorithm is initialized with centroid positions derived from established engineering standards, while a custom Python-based exporter directly bridges the machine learning model with the observability stack. Evaluation results demonstrate that the integrated system successfully operates in real time. The clustering model achieved a Silhouette Score of 0.9055 via five-fold cross-validation and a 100% classification accuracy against manually defined threshold labels. These findings validate the functional integrity of the artifact on clean, well-separated simulation data. The final output is a twelve-panel Grafana dashboard providing comprehensive metric visualization. Ultimately, this threshold-guided integration enhances network observability in simulated environments, promotes proactive management, and minimizes manual inspection dependencies, offering a practical reference for campus or small enterprise network monitoring.

Keywords: *Grafana; K-Means Clustering; Machine Learning; Network Monitoring; Simple Network Management Protocol*

1. PENDAHULUAN

Jaringan komputer telah menjadi tulang punggung komunikasi fundamental di berbagai sektor, yang menuntut ketersediaan tinggi dan kinerja yang konsisten. Mempertahankan komunikasi yang lancar ini memerlukan pemastian bahwa setiap perangkat dalam jaringan beroperasi secara optimal [1],[2]. Jika gangguan

jaringan tidak terdeteksi sejak dini, dampaknya dapat berjenjang dari penurunan produktivitas hingga pemadaman layanan yang berkepanjangan. Oleh karena itu, pemantauan jaringan yang andal telah menjadi komponen yang sangat diperlukan dalam mengelola infrastruktur teknologi informasi modern [3],[4].

Pemantauan jaringan yang efektif melampaui sekadar memverifikasi apakah suatu perangkat aktif atau daring. Pemantauan harus memberikan gambaran menyeluruh secara waktu nyata tentang kondisi jaringan, termasuk volume lalu lintas data, kecepatan transfer, dan status antarmuka jaringan [5],[6]. Secara historis, Protokol Manajemen Jaringan Sederhana (SNMP) telah terbukti andal untuk pengumpulan data dan penemuan topologi [7],[8],[9]. SNMP beroperasi pada model manajer-agen, di mana seorang manajer pusat secara periodik meminta variabel Basis Informasi Manajemen (MIB) yang disimpan pada setiap perangkat yang dipantau; mekanisme berbasis tarik ini secara signifikan mengurangi beban pemrosesan pusat pada perangkat keras jaringan selama manajemen lalu lintas [10],[11]. Namun, SNMP versi 1 dan 2c, termasuk SNMPv2c yang digunakan pada penelitian ini, hanya mengandalkan community string yang dikirim sebagai teks biasa tanpa enkripsi, sehingga rentan terhadap penyadapan dan akses tidak sah; SNMPv3 menyediakan autentikasi dan enkripsi tetapi memerlukan konfigurasi yang lebih kompleks. Keterbatasan keamanan ini dipertahankan karena pengujian dilakukan pada jaringan simulasi yang terisolasi, dan dibahas lebih lanjut pada Bagian 3.4 dan Kesimpulan.

Meskipun andal, pendekatan pemantauan konvensional yang hanya mengandalkan grafik visual manual memiliki keterbatasan yang signifikan. Administrator jaringan diharuskan untuk terus memantau layar guna mendeteksi kerentanan atau anomali yang tersembunyi, yang tidak efisien dan rentan terhadap kesalahan manusia [12],[13]. Seiring dengan meningkatnya kompleksitas jaringan, pemanfaatan alat visualisasi canggih dan streaming waktu nyata, seperti Grafana dan basis data deret waktu, telah menjadi metode standar untuk mengelola aliran data heterogen secara efektif [14],[15],[16]. Basis data deret waktu seperti Prometheus dirancang khusus untuk menyimpan dan membuat kueri metrik yang berubah secara terus-menerus seiring waktu, sementara Grafana berfungsi sebagai lapisan visualisasi yang merender metrik ini ke dalam dasbor interaktif waktu nyata; bersama-sama, kedua alat ini membentuk tulang punggung tumpukan observabilitas modern. Namun, metrik mentah yang ditampilkan pada dasbor masih memerlukan interpretasi manual oleh administrator untuk menentukan apakah kondisi jaringan normal atau abnormal, karena baik SNMP maupun dasbor konvensional tidak mampu mengklasifikasikan kesehatan jaringan secara otomatis.

Untuk mengatasi keterbatasan pemantauan manual, penelitian ini mengusulkan integrasi kecerdasan buatan melalui penerapan algoritme pengelompokan K-Means. K-Means adalah metode pembelajaran tanpa pengawasan yang mempartisi kumpulan data ke dalam K kelompok dengan mengiterasi minimalisasi varians antara setiap titik data dan pusat massa kelompok terdekatnya, sehingga memungkinkan metrik lalu lintas kontinu dikelompokkan ke dalam kategori kesehatan diskrit tanpa memerlukan data pelatihan berlabel manual [17]. Integrasi pembelajaran mesin memungkinkan sistem melakukan diagnosis mandiri dan deteksi anomali otonom tanpa intervensi manusia yang berkelanjutan [18],[19],[20]. Emulasi lingkungan jaringan ini dilakukan menggunakan Graphical Network Simulator-3 (GNS3), sebuah platform canggih yang mampu menjalankan sistem operasi vendor nyata (termasuk router Cisco virtual yang digunakan dalam penelitian ini) untuk menyimulasikan protokol routing yang kompleks, menguji keamanan jaringan, dan memvalidasi konfigurasi redundansi [21],[22],[23],[24].

Tujuan utama dari penelitian ini adalah membangun sistem pemantauan jaringan lokal waktu nyata yang mengintegrasikan SNMP, basis data deret waktu Prometheus, Grafana, dan modul pengelompokan khusus ke dalam arsitektur klien-server yang terpadu [25]. Dengan menerapkan algoritme pengelompokan berpanduan ambang batas, penelitian ini bertujuan untuk menyediakan klasifikasi kondisi jaringan yang otomatis dan konsisten dengan ambang batas teknik yang ditetapkan [26]. Penelitian ini memberikan tiga kontribusi utama. Kontribusi pertama adalah integrasi tumpukan pemantauan lengkap dari SNMP ke Prometheus ke Grafana dengan pengumpulan data waktu nyata. Kontribusi kedua adalah pengembangan algoritme pengelompokan K-Means berpanduan ambang batas yang memastikan klasifikasi kesehatan jaringan yang konsisten dan dapat diinterpretasikan. Kontribusi ketiga adalah pembuatan eksportir pengelompokan berbasis Python khusus yang menjembatani inferensi pembelajaran mesin dengan observabilitas deret waktu. Diharapkan bahwa sistem yang dihasilkan akan mengurangi ketergantungan administrator jaringan pada inspeksi visual manual yang berkelanjutan, mempercepat respons insiden melalui klasifikasi kesehatan yang otomatis dan dapat diinterpretasikan, serta berfungsi sebagai referensi praktis untuk implementasi pemantauan waktu nyata serupa di lingkungan jaringan kampus atau perusahaan kecil.

2. METODOLOGI PENELITIAN

Penelitian ini disusun berdasarkan kerangka Metodologi Penelitian Ilmu Desain (DSRM), sebuah pendekatan yang banyak digunakan dalam penelitian sistem informasi untuk menghasilkan artefak teknologi. DSRM terdiri dari enam fase yang saling terkait, yaitu identifikasi masalah, tujuan solusi, perancangan dan pengembangan artefak, demonstrasi, evaluasi, dan komunikasi. Penelitian ini mengikuti keenam fase tersebut secara berurutan, dimulai dari identifikasi kelemahan pemantauan berbasis SNMP konvensional dan diakhiri dengan diseminasi artefak yang dihasilkan beserta hasil evaluasinya.

2.1 Identifikasi Masalah

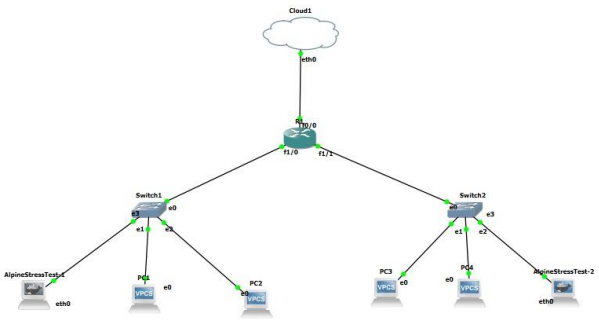
Berdasarkan analisis literatur dan observasi langsung terhadap lingkungan jaringan kampus, terdapat tiga masalah utama yang mendasari penelitian ini. Pertama, sistem pemantauan jaringan konvensional seperti SNMP hanya mampu mengumpulkan data throughput dan latensi mentah yang masih memerlukan interpretasi manual oleh administrator untuk menentukan kesehatan jaringan, menyebabkan keterlambatan dalam respons insiden. Kedua, pendekatan deteksi berbasis ambang batas yang umum digunakan memiliki ambang batas statis, misalnya 80 kB/s untuk peringatan dan 150 kB/s untuk kritis, yang tidak dapat beradaptasi dengan pola lalu lintas dinamis dan sering menghasilkan positif palsu atau negatif palsu. Ketiga, belum ada sistem yang mengintegrasikan protokol SNMP dengan algoritme pembelajaran mesin secara waktu nyata, khususnya untuk lingkungan laboratorium seperti di Universitas Negeri Medan, meninggalkan kesenjangan antara pengumpulan data, penyimpanan, visualisasi, dan analisis cerdas. Ketiga masalah ini memotivasi penelitian ini untuk merancang sistem pemantauan waktu nyata terintegrasi dengan kemampuan klasifikasi otomatis.

2.2 Tujuan Solusi

Untuk mengatasi masalah yang teridentifikasi, penelitian ini menetapkan empat tujuan solusi. Tujuan pertama adalah membangun sistem pemantauan jaringan lokal waktu nyata yang mengintegrasikan empat komponen utama, yaitu Eksportir SNMP untuk mengambil metrik throughput, Prometheus sebagai basis data deret waktu, Grafana sebagai platform visualisasi, dan algoritme pengelompokan K-Means untuk klasifikasi otomatis. Tujuan kedua adalah mengembangkan model pengelompokan K-Means dengan pendekatan inisialisasi berpanduan ambang batas yang mampu mengklasifikasikan kondisi jaringan ke dalam tiga status, yaitu SEHAT, WASPADA, dan KRITIS, memastikan kelompok-kelompok tersebut dapat diinterpretasikan dan selaras dengan standar teknik. Tujuan ketiga adalah membangun jembatan antara model pembelajaran mesin terlatih dan tumpukan observabilitas melalui eksportir khusus berbasis Python yang mengambil data waktu nyata, melakukan pra-pemrosesan, membuat prediksi, dan mengekspos hasil sebagai metrik Prometheus. Tujuan keempat adalah menghasilkan dasbor Grafana yang informatif dengan panel dinamis yang menampilkan metrik waktu nyata, dilengkapi dengan interval penyegaran otomatis 10 detik dan kode warna untuk interpretasi cepat oleh administrator jaringan.

2.3 Perancangan dan Pengembangan Artefak

Artefak yang dihasilkan adalah sistem pemantauan jaringan terintegrasi dengan arsitektur klien-server yang terdiri dari empat lapisan fungsional: simulasi jaringan, pengumpulan data, penyimpanan dan pemrosesan, serta visualisasi dan kecerdasan. Lapisan simulasi jaringan diterapkan menggunakan GNS3 [23],[24] dengan topologi yang terdiri dari satu router Cisco (R1, IP 192.168.56.103) sebagai gateway utama, dua switch, empat PC Virtual, dua instance Alpine Linux sebagai generator lalu lintas, dan sebuah node cloud yang menjembatani ke mesin host yang menjalankan Prometheus, Eksportir SNMP, Eksportir Blackbox, dan Grafana. Kombinasi elemen fisik dan virtual ini memungkinkan emulasi jaringan yang realistis sekaligus mendukung eksperimen terkontrol pada tiga skenario lalu lintas yang digunakan dalam penelitian ini.



Gambar 1. Topologi Jaringan untuk Sistem Pemantauan Jaringan Lokal

Seperti yang diilustrasikan pada Gambar 1, kedua switch diberi label Switch1 dan Switch2, sementara keempat PC Virtual diberi label PC1 hingga PC4, menghubungkan perangkat pengguna akhir ke router melalui tautan Ethernet standar. PC Virtual ini mewakili stasiun kerja pengguna akhir biasa dan tidak menghasilkan lalu lintas tambahan, karena injeksi beban terkontrol ditangani secara terpisah oleh node Alpine Linux yang disebutkan di atas. Memisahkan kedua peran ini memungkinkan skenario demonstrasi pada Bagian 2.4 untuk memvariasikan beban yang diberikan secara sengaja sementara perilaku perangkat pengguna akhir tetap tidak berubah di semua tiga skenario pengujian.

Lapisan pengumpulan data menggunakan Eksportir SNMP pada port 9116 untuk mengambil throughput melalui OID ifHCInOctets dan ifHCOutOctets, dan Eksportir Blackbox pada port 9115 untuk mengukur latensi ICMP, keduanya diambil oleh Prometheus setiap 10 detik. Lapisan penyimpanan dan pemrosesan menggunakan Prometheus sebagai basis data deret waktu, dengan proses pemanenan data selama satu jam menghasilkan 185 sampel valid dari tiga skenario lalu lintas (idle pada 0 hingga 80 kB/s dengan 64 sampel, peringatan pada 80 hingga

150 kB/s dengan 90 sampel, dan kritis di atas 150 kB/s dengan 31 sampel). Jendela pemanenan satu jam ini dipilih untuk memastikan bahwa masing-masing dari tiga kondisi lalu lintas terwakili oleh jumlah sampel yang cukup untuk kemudian melatih dan memvalidasi model pengelompokan yang dijelaskan nanti di bagian ini. Justifikasi ukuran sampel. Sebanyak 185 sampel valid memang relatif kecil untuk ukuran pembelajaran mesin, sehingga kecukupannya dijustifikasi secara terbatas. Pertama, model yang dilatih sangat sederhana, yaitu K-Means satu dimensi dengan tiga parameter pusat massa, sehingga tidak memerlukan data dalam jumlah besar untuk konvergen; kelompok terkecil (KRITIS) tetap memiliki 31 sampel, jauh di atas jumlah parameter yang diestimasi. Kedua, lalu lintas pada setiap skenario dibangkitkan secara terkendali (ukuran paket dan laju pengiriman tetap), sehingga variabilitas di dalam skenario rendah dan ketiga kondisi sudah terwakili dalam satu jendela pengamatan; kestabilan hasil juga didukung oleh validasi silang 5-lipat pada Bagian 3.1. Ketiga, tujuan eksperimen ini adalah memvalidasi fungsionalitas alur pemantauan dari ujung ke ujung, bukan mengestimasi distribusi lalu lintas jaringan produksi. Meskipun demikian, durasi satu jam dan satu sesi pengambilan data tidak dapat mewakili variasi lalu lintas alami (misalnya pola harian atau mingguan, lonjakan tak terduga, dan beragam aplikasi), sehingga jumlah sampel ini diakui sebagai keterbatasan yang dibahas pada Bagian 3.4.

Lapisan visualisasi dan kecerdasan mengintegrasikan pengelompokan K-Means dengan tumpukan observabilitas. Sebelum pelatihan, pra-pemrosesan data melibatkan penguraian nilai throughput mentah yang diekspor dari Grafana (241 sampel) dan membuang sampel dengan throughput nol (justifikasi pada Bagian 2.4), menghasilkan 185 sampel valid yang digunakan untuk pelatihan, diikuti dengan standardisasi menggunakan StandardScaler. Selama inferensi waktu nyata, eksportir pengelompokan juga menerapkan pemulusan median dengan ukuran jendela 3 pada aliran throughput langsung sebelum klasifikasi. Model K-Means menggunakan inisialisasi berpanduan ambang batas dengan tiga kelompok dan pusat massa awal pada 40.000 B/s, 115.000 B/s, dan 200.000 B/s. Parameter model K-Means disajikan pada Tabel 1.

Table 1. K-Means Model Parameters

Parameter	Value
n_clusters	3
init	Custom (threshold guided)
n_init	10
max_iter	300
random_state	42
algorithm	lloyd

Berdasarkan Tabel 1, inisialisasi berpanduan ambang batas yang dikombinasikan dengan algoritme lloyd dan status acak tetap 42 memastikan bahwa hasil pengelompokan tetap stabil dan dapat direproduksi pada beberapa kali pengulangan. Tidak seperti inisialisasi acak penuh yang dapat konvergen ke optimal lokal yang berbeda tergantung pada titik awal yang dipilih, pusat massa berpanduan ambang batas menjangkar algoritme ke rentang throughput yang bermakna secara fisik sejak iterasi pertama [17]. Parameter lainnya, yaitu sepuluh inisialisasi (n_init) dan maksimum 300 iterasi (max_iter), memberikan peluang yang cukup bagi algoritme untuk menyempurnakan batas kelompok tanpa membebani alur pemantauan waktu nyata secara komputasional yang tidak perlu.

Sebuah eksportir Python khusus berjalan sebagai server HTTP, secara periodik melakukan kueri ke Prometheus setiap 5 detik untuk total throughput masuk yang digabungkan di semua antarmuka router R1 (jumlah dari laju ifHCInOctets selama jendela 30 detik), menerapkan pemulusan median, dan mengekspos tiga metrik ke Prometheus, yaitu network_cluster_value, network_throughput_bytes, dan network_health_status. Dengan mengekspos metrik ini langsung ke Prometheus daripada menulis hasil klasifikasi ke basis data terpisah, eksportir menjaga komponen pembelajaran mesin tetap tersinkronisasi penuh dengan alur deret waktu yang sama yang sudah digunakan untuk data SNMP mentah, memungkinkan Grafana untuk melakukan kueri metrik mentah dan terklasifikasi melalui sumber data tunggal yang konsisten. Keluaran akhir adalah dasbor Grafana dua belas panel yang menampilkan metrik jaringan waktu nyata.

Pemilihan fitur tunggal. Vektor fitur model hanya berisi throughput masuk, meskipun latensi ICMP juga diukur oleh Eksportir Blackbox, dengan alasan metodologis berikut. Pertama, ambang batas teknik yang menjadi dasar pelabelan dan inisialisasi pusat massa (80 kB/s dan 150 kB/s) hanya didefinisikan untuk throughput; menambahkan latensi tanpa ambang batas yang setara akan menghilangkan kemampuan inisialisasi berpanduan ambang batas dan pembandingan dengan label acuan. Kedua, Eksportir Blackbox mengirim satu permintaan ICMP per probe sehingga nilai probe_success bersifat biner (berhasil atau gagal); rasio kehilangan paket baru dapat dihitung bila beberapa probe diagregasi dalam suatu jendela waktu, dan jitter memerlukan deret latensi yang lebih rapat daripada interval pengambilan 10 detik. Ketiga, latensi pada lingkungan GNS3 dapat dipengaruhi oleh beban CPU mesin host yang menjalankan emulasi, bukan hanya oleh kepadatan lalu lintas pada tautan, sehingga pemakaiannya sebagai fitur klasterisasi pada tahap awal berisiko memasukkan derau yang tidak berkaitan dengan kondisi jaringan. Pemilihan ini menjadikan masalah klasterisasi satu dimensi sehingga hasilnya hampir setara

dengan pemartisian pada ambang batas; konsekuensi ini dibahas pada Bagian 3.4. Klasterisasi multivariat (throughput dan latensi, kemudian kehilangan paket dan jitter) dengan standardisasi tiap fitur dan pusat massa awal multidimensi diusulkan sebagai pengembangan pada penelitian mendatang.

2.4 Demonstrasi

Demonstrasi dilakukan dengan menjalankan semua komponen sistem secara simultan dan menguji tiga skenario lalu lintas dengan durasi pengamatan efektif sekitar 15 menit untuk masing-masing skenario pada data yang diekspor. Pada skenario pertama (SEHAT), sistem dijalankan tanpa beban eksternal, hanya merekam lalu lintas routing OSPF [9], dan dasbor menunjukkan status hijau dengan throughput berkisar antara 0 hingga 80 kB/s. Pada skenario kedua (WASPADA), generator lalu lintas menghasilkan banjir paket ICMP sedang, dan dasbor menunjukkan status oranye dengan throughput berkisar antara 80 hingga 150 kB/s. Pada skenario ketiga (KRITIS), dua generator lalu lintas secara simultan menghasilkan banjir paket ICMP masif, dan dasbor menunjukkan status merah dengan throughput melebihi 150 kB/s. Hasil demonstrasi mengonfirmasi bahwa dasbor secara konsisten menampilkan warna dan status yang diharapkan untuk setiap skenario, dengan semua target Prometheus tetap dalam status "UP" sepanjang periode pengujian; evaluasi akurasi yang sesuai dari hasil klasifikasi ini disajikan pada Bagian 3.

Justifikasi pembuangan sampel throughput nol. Dari 241 sampel mentah, 56 sampel (23,2 persen) bernilai throughput nol dan dikeluarkan dari data latih. Sampel-sampel ini tidak diperlakukan sebagai kondisi idle, melainkan sebagai kondisi tanpa pengukuran yang bermakna, berdasarkan tiga alasan. Pertama, pola kemunculannya: nilai nol muncul dalam blok berurutan pada awal perekaman (2 sampel), pada dua pergantian skenario (masing-masing 5 sampel, sekitar 75 detik), dan pada akhir perekaman setelah pengujian selesai (44 sampel), bukan tersebar di dalam skenario SEHAT. Pola ini konsisten dengan prosedur eksperimen, yaitu persiapan, pergantian generator lalu lintas, dan penghentian pengujian. Kedua, kondisi idle pada topologi ini tidak bernilai nol: router tetap bertukar paket routing OSPF dan menerima polling SNMP, sehingga throughput kondisi SEHAT yang teramati berada pada kisaran puluhan kB/s (pusat massa sekitar 48,3 kB/s); throughput nol yang bertahan berarti tidak ada kenaikan penghitung oktet pada antarmuka, yang lebih mungkin mencerminkan tautan terputus atau celah pengambilan data. Ketiga, mempertahankan nilai nol akan membentuk konsentrasi data tersendiri di sekitar 0 B/s yang menarik pusat massa kelompok SEHAT ke bawah dan memperlebar sebarannya sehingga tidak lagi mencerminkan lalu lintas idle yang sebenarnya. Pada operasi waktu nyata, pembacaan nol yang berkepanjangan sebaiknya diperlakukan sebagai peringatan ketersediaan data atau status antarmuka (panel Status Koneksi), bukan sebagai status SEHAT. Pembuangan ini tetap mengubah distribusi data dan dicatat sebagai keterbatasan pada Bagian 3.4.

2.5 Evaluasi

Evaluasi dalam penelitian ini dirancang untuk menilai tiga aspek utama sistem. Aspek pertama, kinerja model pengelompokan, dinilai menggunakan Skor Siluet bersama dengan validasi silang 5-lipat, di mana model K-Means dilatih ulang pada setiap lipatan pelatihan menggunakan inisialisasi berpanduan ambang batas yang sama dan dievaluasi pada lipatan uji tahanan yang sesuai, untuk memverifikasi bahwa kelompok yang dihasilkan terpisah dengan baik dan bukan merupakan produk dari overfitting terhadap satu pemisahan pelatihan tunggal. Aspek kedua, kinerja sistem waktu nyata, dinilai dengan memantau stabilitas operasional eksportir pengelompokan, latensi antara pengambilan data dan pembaruan dasbor, serta status ketersediaan semua target pengambilan Prometheus sepanjang periode pengujian. Aspek ketiga, kualitas dasbor, dinilai berdasarkan apakah kedua belas panel Grafana berfungsi dengan benar di bawah interval penyegaran yang dikonfigurasi dan apakah skema kode warna mendukung interpretasi cepat oleh administrator jaringan. Hasil lengkap evaluasi ini disajikan dan dibahas pada Bagian 3.

2.6 Komunikasi

Komunikasi hasil penelitian dilakukan melalui tiga saluran. Pertama, publikasi artikel jurnal ini menyebarluaskan temuan kepada peneliti lain di bidang jaringan komputer dan pembelajaran mesin. Kedua, semua kode sumber dibuat tersedia secara terbuka untuk memungkinkan replikasi dan pengembangan lebih lanjut oleh peneliti lain. Ketiga, dokumentasi teknis yang berisi petunjuk instalasi, konfigurasi, dan pengujian memungkinkan praktisi jaringan untuk mengimplementasikan sistem serupa di lingkungan masing-masing.

3. HASIL DAN PEMBAHASAN

3.1 Kinerja Model Pengelompokan

Model pembelajaran mesin berhasil dilatih pada 185 sampel valid yang diekstraksi dari simulasi jaringan. Evaluasi menghasilkan Skor Siluet sebesar 0,9055, yang mendekati nilai maksimum 1 dan menunjukkan bahwa titik data dalam setiap kelompok dikelompokkan secara ketat dan terpisah dengan jelas dari kelompok tetangga.

Hasil validasi silang selanjutnya mengonfirmasi ketahanan model, dengan Skor Siluet rata-rata sebesar 0,9050 dan deviasi standar kurang lebih 0,025 pada lima lipatan uji tahanan, yang menunjukkan tidak adanya overfitting.

Hasil pengelompokan mengidentifikasi tiga zona lalu lintas yang berbeda. Kelompok sehat memiliki pusat massa sekitar 48,3 kB/s, yang mewakili kondisi idle normal. Kelompok peringatan memiliki pusat massa sekitar 100,8 kB/s, yang berada di bawah rata-rata aritmetika dari 80 dan 150 (115 kB/s), menunjukkan bahwa lalu lintas yang diamati dalam skenario stres sedang mengelompok ke arah bagian tengah bawah dari rentang ambang batas 80-150 kB/s. Kelompok kritis memiliki pusat massa sekitar 205,0 kB/s, yang secara akurat menangkap skenario banjir. Tabel 2 menunjukkan distribusi 185 sampel pelatihan di ketiga kelompok.

Tabel 2. Distribusi Data Pelatihan per Kelompok

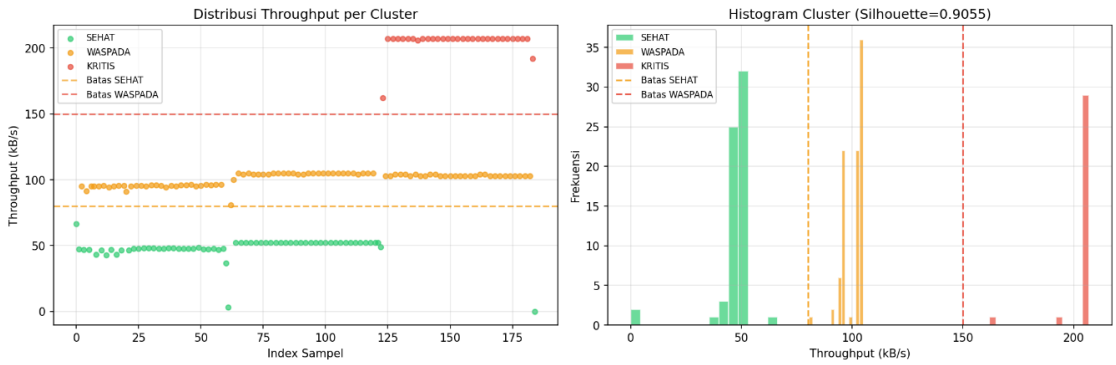
Cluster	Throughput Range	Number of Samples	Percentage
SEHAT	0 to 80 kB/s	64	34,6%
WASPADA	80 to 150 kB/s	90	48,6%
KRITIS	Above 150 kB/s	31	16,8%

Seperti yang ditunjukkan pada Tabel 2, kelompok WASPADA mengandung porsi sampel terbesar yaitu 48,6 persen, diikuti oleh SEHAT sebesar 34,6 persen dan KRITIS sebesar 16,8 persen, distribusi yang ditentukan oleh tingkat throughput terukur menurut ambang batas. Distribusi ini mengikuti tingkat throughput terukur dan tidak berarti skenario WASPADA berlangsung lebih lama: durasi efektif ketiga skenario pada data latih relatif sama (sekitar 61 hingga 62 sampel per skenario), dan sampel berlabel WASPADA berasal dari ketiga skenario (lihat Bagian 3.4). Proporsi sampel KRITIS yang relatif lebih kecil juga konsisten dengan maksud jaringan produksi nyata, di mana kondisi kelebihan beban ekstrem diharapkan terjadi lebih jarang daripada lalu lintas normal atau yang sedikit meningkat.

Letak pusat massa WASPADA (100,8 kB/s) di bawah titik tengah 115 kB/s mencerminkan karakteristik beban uji, bukan kegagalan algoritme. Titik 115 kB/s hanyalah titik awal inisialisasi yang dihitung dari rata-rata kedua batas ambang, sedangkan pusat massa akhir ditentukan oleh data. Pada data latih, sampel kelompok WASPADA terkonsentrasi sangat rapat di sekitar 95 hingga 105 kB/s (simpangan baku sekitar 4,7 kB/s), jauh lebih rapat daripada kelompok SEHAT (sekitar 9,3 kB/s) maupun KRITIS (sekitar 8,4 kB/s). Perilaku ini sesuai dengan sifat generator lalu lintas: paket ICMP berukuran tetap yang dikirim pada laju tetap menghasilkan throughput yang mendekati satu tingkat beban konstan, bukan tersebar merata di seluruh rentang 80 hingga 150 kB/s. Dengan kata lain, batas 80 dan 150 kB/s adalah konvensi teknik, sedangkan tingkat beban yang benar-benar dihasilkan skenario uji ditentukan oleh ukuran paket, laju pengiriman, dan kapasitas node virtual pembangkit. Konsekuensinya, kelompok WASPADA yang terbentuk mencerminkan tingkat beban pada data laboratorium ini, dan ambang batas perlu dikalibrasi ulang pada jaringan nyata. Sebagai pembanding, 100,8 kB/s setara sekitar 0,8 Mbps atau kurang dari 1 persen kapasitas antarmuka FastEthernet 100 Mbps.

Representasi visual dari hasil pengelompokan ini disajikan pada Gambar 2. Panel kiri menunjukkan distribusi sampel throughput per kelompok, dengan SEHAT berwarna hijau, WASPADA oranye, dan KRITIS merah. Garis putus-putus horizontal menunjukkan ambang batas manual pada 80 kB/s dan 150 kB/s. Panel kanan menyajikan histogram dari data yang sama, yang menunjukkan pemisahan yang jelas antar kelompok. Skor Siluet yang dicapai adalah 0,9055, yang menunjukkan pemisahan kelompok yang sangat baik.

Jika dibandingkan dengan ambang batas teknik manual, model mencapai akurasi 100 persen, memvalidasi bahwa inisialisasi berpanduan ambang batas secara efektif menjangkar algoritme ke status jaringan yang bermakna. Matriks kebingungan mengonfirmasi nol kesalahan klasifikasi di ketiga kelompok, dengan semua 64 sampel sehat diklasifikasikan dengan benar sebagai Kelompok 0, semua 90 sampel peringatan sebagai Kelompok 1, dan semua 31 sampel kritis sebagai Kelompok 2, menghasilkan nol positif palsu dan nol negatif palsu. Hasil ini menunjukkan bahwa batas kelompok yang dipelajari oleh model hampir sempurna selaras dengan ambang batas teknik yang ditentukan secara manual yaitu 80 kB/s dan 150 kB/s, menunjukkan bahwa inisialisasi berpanduan ambang batas berhasil mentransfer pengetahuan domain ke dalam proses pembelajaran tanpa pengawasan. Secara keseluruhan, temuan ini secara langsung menjawab tujuan penelitian pertama yang dinyatakan pada Bagian 2.2, yaitu menghasilkan model pengelompokan yang klasifikasinya akurat dan dapat diinterpretasikan oleh administrator jaringan.



Gambar 2. Hasil Pengelompokan K-Means pada Data Throughput Jaringan

3.2 Integrasi Sistem Waktu Nyata

Komponen eksportir pengelompokan khusus yang didedikasikan berhasil diintegrasikan ke dalam alur pemantauan. Alih-alih mengandalkan satu antarmuka yang dikonfigurasi secara manual, eksportir mengambil total throughput masuk yang digabungkan di semua antarmuka router R1 (192.168.56.103) secara langsung melalui kueri agregasi Prometheus, menghilangkan kebutuhan konfigurasi per antarmuka dan meningkatkan kemampuan penerapan di lingkungan jaringan yang berbeda. Eksportir mengambil data throughput waktu nyata setiap 5 detik, menerapkan pemulusan median tiga sampel yang secara efektif menekan lonjakan sementara dari noise pengukuran, dan memproses data melalui model terlatih sebelum mengekspos hasil klasifikasi untuk diambil oleh Prometheus setiap 10 detik.

Kinerja waktu nyata sistem diverifikasi dengan dua cara. Pertama, kontinuitas alur data diperiksa sepanjang jendela pemantauan 60 menit: deret throughput yang diekspor berisi semua 241 stempel waktu yang diharapkan pada resolusi 15 detik tanpa celah, yang menunjukkan tidak ada kegagalan pengambilan atau gangguan layanan yang terjadi sepanjang periode pengujian. Kedua, latensi ujung-ke-ujung antara perubahan throughput mentah dan pencerminannya pada dasbor diperkirakan dengan menjumlahkan waktu konfigurasi setiap tahap alur, yaitu interval polling eksportir 5 detik, interval pengambilan Prometheus 10 detik, dan interval penyegaran otomatis Grafana 10 detik, menghasilkan latensi teoritis mulai dari hampir seketika hingga sekitar 25 detik, dengan rata-rata sekitar 12,5 detik. Ini memenuhi persyaratan waktu nyata yang didefinisikan dalam tujuan solusi kedua (Bagian 2.2), karena dasbor secara andal mencerminkan perubahan status jaringan dalam jangka waktu pemantauan yang dapat dirasakan manusia. Hasil ini juga menunjukkan bahwa agregasi throughput pada tingkat router, daripada per antarmuka, tidak menimbulkan penundaan pemrosesan tambahan, mendukung keputusan desain yang dibahas pada Bagian 2.3 untuk menjaga arsitektur eksportir tetap sederhana dan tidak bergantung pada penerapan.

3.3 Visualisasi dan Analisis Dasbor

Keluaran akhir dari sistem ini adalah dasbor Grafana yang terdiri atas dua belas panel untuk memantau kondisi jaringan secara waktu nyata, dengan interval penyegaran otomatis 10 detik sesuai konfigurasi dasbor. Panel-panel tersebut menampilkan status koneksi, akumulasi data masuk dan keluar, beban maksimum masuk dan keluar, fluktuasi throughput, latensi QoS, ketersediaan layanan QoS, kecepatan unggah dan unduh, status kualitas jaringan, serta klasifikasi kesehatan jaringan berbasis AI. Keluaran klasifikasi divisualisasikan melalui kode warna, yaitu hijau untuk SEHAT, oranye untuk WASPADA, dan merah untuk KRITIS, sehingga administrator dapat mengenali status jaringan tanpa harus menafsirkan seluruh nilai throughput secara manual. Tampilan dashboard yang digunakan dalam penelitian ini disajikan pada Gambar 3.



Gambar 3. Dasbor Grafana Dua Belas Panel untuk Pemantauan Jaringan Lokal

Seperti yang ditunjukkan pada Gambar 3, kedua belas panel disusun untuk memudahkan pembacaan kondisi jaringan secara bertahap. Panel yang menampilkan indikator utama, seperti status koneksi, status kualitas jaringan, dan klasifikasi kesehatan berbasis AI, memberikan gambaran awal mengenai kondisi jaringan. Sementara itu, panel throughput, kecepatan unggah dan unduh, serta latensi QoS menyajikan informasi yang lebih terperinci untuk membantu pemeriksaan lebih lanjut. Susunan tersebut memungkinkan administrator mengamati status jaringan terlebih dahulu, kemudian meninjau metrik terkait apabila diperlukan analisis lanjutan.

Korelasi antara panel latensi QoS dan klasifikasi status AI. Pada Gambar 3, panel QoS: Latensi (Ping), Status Kualitas Jaringan, dan Status Jaringan (AI) ditempatkan berdampingan sehingga perubahan latensi dapat dibandingkan secara visual dengan status klasifikasi. Pada kondisi SEHAT yang tertangkap pada gambar, latensi ICMP berfluktuasi sekitar 4 hingga 42 ms dengan rata-rata 32,2 ms pada panel Status Kualitas Jaringan, ketersediaan layanan 100 persen (tanpa kehilangan paket), dan status AI SEHAT; ketiga panel konsisten menunjukkan jaringan yang sehat. Pada skenario banjir paket, mekanisme yang diharapkan adalah bahwa kenaikan throughput yang mengubah status AI menjadi WASPADA atau KRITIS diikuti kenaikan latensi karena paket probe ICMP bersaing dengan lalu lintas banjir pada antrean router. Namun, karena throughput kelompok KRITIS (sekitar 205 kB/s atau 1,6 Mbps) hanya sekitar 1,6 persen dari kapasitas tautan 100 Mbps, kenaikan latensi akibat antrean tautan diperkirakan kecil, dan perubahan yang teramati lebih mungkin berasal dari beban pemrosesan ICMP pada router virtual dan mesin host. Penelitian ini belum menghitung koefisien korelasi antara latensi dan throughput pada skenario WASPADA dan KRITIS karena deret latensi tidak diekspor bersama data pelatihan; analisis korelasi kuantitatif (misalnya koefisien Pearson atau Spearman per skenario) dijadikan agenda penelitian lanjutan.

Secara keseluruhan, ketiga rangkaian temuan di atas secara langsung menjawab tiga masalah yang diidentifikasi pada awal penelitian ini (Bagian 2.1). Skor Siluet yang tinggi dan akurasi klasifikasi sempurna pada Bagian 3.1 mengindikasikan bahwa pengelompokan berpanduan ambang batas dapat mereproduksi ambang batas teknik secara otomatis; kemampuannya mengatasi keterbatasan ambang batas statis masih perlu diuji pada data nyata (Bagian 3.4). Kontinuitas data tanpa celah dan latensi penyegaran teoritis di bawah 30 detik yang dilaporkan pada Bagian 3.2 mengonfirmasi bahwa inferensi pembelajaran mesin dapat disematkan ke dalam alur observabilitas langsung tanpa mengorbankan responsivitas waktu nyata, menutup kesenjangan integrasi yang dicatat dalam fase identifikasi masalah. Terakhir, dasbor yang dapat diinterpretasikan dengan kode warna pada Bagian 3.3 memenuhi motivasi awal untuk mengurangi ketergantungan administrator pada inspeksi visual manual. Hasil gabungan ini mendukung klaim yang dibuat dalam Pendahuluan bahwa mengintegrasikan SNMP, Prometheus, Grafana, dan pengelompokan K-Means berpanduan ambang batas menyediakan alternatif yang praktis dan ringan untuk pemantauan jaringan manual murni.

3.4 Keterbatasan dan Ancaman terhadap Validitas

Akurasi 100 persen dan Skor Siluet 0,9055 perlu ditafsirkan secara hati-hati. Label acuan dibentuk dari ambang batas 80 dan 150 kB/s, pusat massa awal ditetapkan dari titik tengah ambang batas yang sama, dan evaluasi dilakukan terhadap label yang sama pada data satu dimensi yang tingkat throughput-nya terpisah jelas. Dalam kondisi ini algoritme K-Means hampir pasti konvergen ke pembagian yang berimpit dengan ambang batas, sehingga akurasi sempurna dan Skor Siluet yang tinggi merupakan hasil yang dapat diperkirakan sejak awal dan bersifat sirkuler. Dengan demikian, hasil tersebut hanya membuktikan fungsionalitas artefak, yaitu bahwa model dan alur pemantauan dapat mereproduksi ambang batas teknik secara otomatis pada lingkungan simulasi yang terisolasi, dan bukan membuktikan keunggulan terhadap ambang batas statis, kemampuan mendeteksi anomali,

maupun kemampuan generalisasi pada lalu lintas jaringan produksi. Validasi silang 5-lipat menggunakan data dari distribusi dan sesi pengambilan yang sama sehingga hanya menunjukkan kestabilan internal. Penelitian ini juga belum membandingkan model dengan baseline berupa aturan ambang batas statis, sehingga klaim pengurangan positif palsu dan negatif palsu belum diuji secara empiris.

Ancaman validitas lain berkaitan dengan data dan pengukuran. Pertama, data bersumber dari satu sesi simulasi GNS3 berdurasi satu jam pada satu router dan satu antarmuka, dengan lalu lintas buatan berupa banjir ICMP tanpa pola lalu lintas aplikasi nyata. Kedua, ambang batas 80 dan 150 kB/s merupakan konvensi relatif terhadap lalu lintas dasar laboratorium dan belum dikaitkan dengan kapasitas tautan; pada antarmuka FastEthernet 100 Mbps, 150 kB/s hanya sekitar 1,2 persen kapasitas, sehingga status KRITIS pada penelitian ini berarti lonjakan relatif terhadap kondisi dasar, bukan kejenuhan tautan. Ketiga, pembuangan 56 dari 241 sampel (23,2 persen) bernilai nol dapat menimbulkan bias seleksi walaupun telah dijustifikasi pada Bagian 2.4. Keempat, deret throughput yang diekspor pada resolusi 15 detik memperlihatkan pola dua tingkat yang berselang-seling dengan rasio sekitar 1:2 pada setiap skenario (misalnya sekitar 52 dan 105 kB/s pada skenario WASPADA serta 103 dan 207 kB/s pada skenario KRITIS). Pola ini diduga merupakan artefak ketidakselarasan antara interval pengambilan Prometheus 10 detik dan resolusi ekspor 15 detik, bukan perilaku lalu lintas sebenarnya. Akibatnya, ketiga kelompok lebih mencerminkan tingkat throughput hasil pengukuran daripada skenario beban, dan sampel berlabel WASPADA berasal dari ketiga skenario, sehingga throughput rata-rata sebenarnya per skenario perlu diverifikasi dengan jendela laju yang lebih panjang. Jendela laju 30 detik dan pemulusan median pada eksportir dimaksudkan untuk mengurangi efek ini pada inferensi waktu nyata, namun efektivitasnya belum dievaluasi secara terpisah.

Selain itu, ketergantungan pada satu fitur (Bagian 2.3) menjadikan masalah ini setara dengan pemartisian satu dimensi, dan penggunaan SNMPv2c dengan community string tanpa enkripsi membatasi penerapan pada jaringan yang tidak terisolasi. Meskipun demikian, kontribusi penelitian ini tetap bermakna sebagai arsitektur acuan yang dapat direplikasi: integrasi SNMP, Prometheus, Grafana, dan eksportir pengelompokan yang berjalan secara waktu nyata, serta model yang dapat diinterpretasikan dan dikalibrasi ulang dengan data baru. Implikasi praktisnya, sistem ini layak sebagai prototipe dan landasan pengembangan, sedangkan klaim kinerja klasifikasi perlu dikuatkan dengan data jaringan nyata, fitur multivariat, dan pembanding baseline.

4. KESIMPULAN

Penelitian ini telah berhasil mengembangkan dan mendemonstrasikan sistem pemantauan jaringan lokal waktu nyata yang mengintegrasikan SNMP, Prometheus, Grafana, dan algoritme pengelompokan K-Means berpanduan ambang batas. Model pengelompokan mencapai Skor Siluet sebesar 0,9055 dan akurasi klasifikasi 100 persen terhadap label ambang batas pada status lalu lintas SEHAT, WASPADA, dan KRITIS pada data simulasi (dipahami sebagai validasi fungsionalitas artefak), dengan stabilitas dikonfirmasi melalui validasi silang 5-lipat. Eksportir pengelompokan khusus selanjutnya mempertahankan ketersediaan data berkelanjutan sepanjang periode pengujian tanpa kegagalan pengambilan dan latensi ujung-ke-ujung teoritis rata-rata sekitar 12,5 detik, sementara dasbor Grafana dua belas panel yang dihasilkan berhasil menerjemahkan metrik jaringan mentah menjadi status visual berkode warna yang dapat diinterpretasikan. Dari temuan ini, muncul tiga kontribusi utama: alur pemantauan yang beroperasi penuh yang mengumpulkan data SNMP melalui Prometheus dan memvisualisasikannya di Grafana secara waktu nyata; model K-Means berpanduan ambang batas yang pusat massa awalnya yang kustom menjaga kelompok yang dihasilkan tetap dapat diinterpretasikan dan stabil; dan eksportir berbasis Python khusus yang menjembatani inferensi pembelajaran mesin dengan tumpukan observabilitas dengan menggabungkan throughput di beberapa antarmuka dan menerapkan pemulusan median sebelum klasifikasi.

Temuan ini menunjukkan bahwa pengelompokan berpanduan ambang batas menawarkan alternatif yang ringan dan dapat diinterpretasikan pada lingkungan simulasi untuk pemantauan manual murni atau berbasis ambang batas statis, memberikan administrator jaringan kampus dan usaha kecil hingga menengah dasar yang praktis dan dapat diinterpretasikan untuk pengambilan keputusan proaktif dan respons insiden yang lebih cepat tanpa beban infrastruktur pembelajaran mendalam yang kompleks. Sistem saat ini tetap memiliki beberapa keterbatasan, termasuk ketergantungannya pada satu fitur throughput, penggunaan SNMPv2c yang tidak terenkripsi, dan validasinya hanya pada satu kumpulan data simulasi. Penelitian di masa depan diarahkan pada: (1) migrasi dari SNMPv2c ke SNMPv3 dengan mode autentikasi dan enkripsi (authPriv) untuk keamanan yang lebih kuat; (2) klasterisasi multivariat dengan vektor fitur yang memuat throughput, latensi, jitter, dan kehilangan paket yang distandardisasi, dengan pusat massa awal multidimensi yang diturunkan dari ambang batas tiap metrik; (3) penambahan pemberitahuan otomatis; (4) pembandingan dengan baseline ambang batas statis menggunakan metrik positif palsu dan negatif palsu; serta (5) validasi pada data jaringan produksi nyata dengan pola lalu lintas alami untuk meningkatkan kesiapannya bagi penerapan skala besar di perusahaan.

DAFTAR PUSTAKA

[1] E. K. Silalahi, Y. C. Sitanggang, E. Suryaningsih, and D. Kiswanto, "Implementasi dan Analisis Protokol HSRP dan VRRP dalam Meningkatkan Redundansi Gateway pada Jaringan Virtual," JITET (Jurnal Informatika dan Teknik Elektro Terapan), vol. 13, no. 2, pp. 1431-1444, 2025. DOI: https://doi.org/10.23960/jitet.v13i2.6474

[2] D. Bhamare et al., "IntOpt: In-band Network Telemetry optimization framework to monitor network slices using P4," Computer Networks, vol. 216, p. 109214, 2022. DOI: https://doi.org/10.1016/j.comnet.2022.109214

[3] A. H. Alhilali, A. Al Farawn, and A. Y. Mjhool, "Design And Implement A Real-Time Network Traffic Management System Using Snmp Protocol," Eastern-European Journal of Enterprise Technologies, vol. 5, no. 9 (125), pp. 35-44, 2023. DOI: https://doi.org/10.15587/1729-4061.2023.286528

[4] A. M. T. I. Al-Naib, "Design and Implementation of a Real-Time Monitoring and Protection System," Journal of Positive Sciences, vol. 2023, no. 17, 2023. DOI: https://doi.org/10.52688/17

[5] J. Koumar, K. Hynek, J. Pesek, and T. Cejka, "NetTiSA: Extended IP flow with time-series features for universal bandwidth-constrained high-speed network traffic classification," Computer Networks, vol. 240, p. 110147, 2024. DOI: https://doi.org/10.1016/j.comnet.2023.110147

[6] L. Yu and Y. Bai, "Design of network security monitoring system based on K-means clustering algorithm," Intelligent Decision Technologies, vol. 18, no. 4, pp. 3105-3118, 2024. DOI: https://doi.org/10.3233/IDT-240185

[7] B. C. Pragathi, H. Maddirala, and M. Sneha, "Implementing an Effective Infrastructure Monitoring Solution with Prometheus and Grafana," International Journal of Computer Applications, vol. 186, no. 38, pp. 7–15, Sep. 2024. DOI: https://doi.org/10.5120/ijca2024923873

[8] S. Kamamura, Y. Takei, M. Nishiguchi, Y. Hayashi, and T. Fujiwara, "Network Anomaly Detection Through IP Traffic Analysis With Variable Granularity," IEEE Access, vol. 11, pp. 129818-129828, 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3334212

[9] H. J. Santillan Carranza, J. J. Arellano Riera, B. L. Catota Morocho, and P. M. Wong Wong, "Integration of OSPF and SNMP for Network Monitoring and High Availability: Experimental Evaluation," InGenio Journal, vol. 9, no. 1, pp. 87-112, 2026. DOI: https://doi.org/10.18779/ingenio.v9i1.1102

[10] C. L. Aldea, R. Bocu, and R. N. Solca, "Real-Time Monitoring and Management of Hardware and Software Resources in Heterogeneous Computer Networks through an Integrated System Architecture," Symmetry, vol. 15, no. 6, Art. no. 1134, May 2023. DOI: https://doi.org/10.3390/sym15061134

[11] Q. Naseer Qureshi, G. Jeon, and F. Piccialli, "Anomaly Detection and Trust Authority in Artificial Intelligence and Cloud Computing," Computer Networks, vol. 184, p. 107647, 2021. DOI: https://doi.org/10.1016/j.comnet.2020.107647

[12] N. B. M. Faizu et al., "IoT-based real-time monitoring of agricultural wastewater using Raspberry Pi, Node-RED, and Grafana," Bulletin of Electrical Engineering and Informatics, vol. 14, no. 6, pp. 4665-4677, 2025. DOI: https://doi.org/10.11591/eei.v14i6.10170

[13] M. Zeeshan A., " M. B. Yel, "Analysis of Enterprise Network Performance Using the SNMP (Simple Network Management Protocol) Method," Journal Innovations Computer Science, vol. 4, no. 2, pp. 335–344, Nov. 2025. DOI:Network Monitoring Using Grafana: An Integrated Approach for Enterprise Infrastructure Management," International Journal of Engineering Research and Applications, vol. 15, no. 8, pp. 01–05, Aug. 2025. DOI: https://doi.org/10.9790/9622-15080105

[14] G. Calderon, G. del Campo, E. Saavedra, and A. Santamaria, "Monitoring Framework for the Performance Evaluation of an IoT Platform with Elasticsearch and Apache Kafka," Information Systems Frontiers, vol. 26, pp. 2373-2389, 2024. DOI: https://doi.org/10.1007/s10796-023-10409-2

[15] A. H. Sukma, D. Kiswanto, F. G. Sembiring, and S. Ashillah, "Rancang Bangun Sistem Logging Jaringan Berbasis Web dengan Visualisasi Interaktif Grafana untuk Analisis Aktivitas IP Mencurigakan," JITET (Jurnal Informatika dan Teknik Elektro Terapan), vol. 14, no. 1, 2026. DOI: https://doi.org/10.23960/jitet.v14i1.8200

[16] I. Fosic, D. Zagar, K. Grgic, and V. Krizanovic, "Anomaly detection in NetFlow network traffic using supervised machine learning algorithms," Journal of Industrial Information Integration, vol. 33, p. 100466, 2023. DOI: https://doi.org/10.1016/j.jii.2023.100466

[17] T. Cattai, S. Sardellitti, F. Cuomo, and S. Barbarossa, "Joint Anomaly Detection and Topology Inference for Dynamic Water Distribution Networks Monitoring," Internet of Things, p. 101978, 2026. DOI: https://doi.org/10.1016/j.iot.2026.101978

[18] C. Wang, H. Zhou, Q. Xu, and Y. Zhang, "Network traffic analysis over clustering-based collective anomaly detection," Computer Networks, vol. 205, p. 108760, 2022. DOI: https://doi.org/10.1016/j.comnet.2022.108760

[19] J. J. Peralta Abadia et al., "Self-diagnosis service to support analysis of production performance, monitoring and optimisation activities," Journal of Manufacturing Systems, vol. 83, pp. 800-821, 2025. DOI: https://doi.org/10.1016/j.jmsy.2025.11.010

[20] A. Vargas-Arcila, J. C. Corrales, A. Sanchis, and A. Rendon, "SOFI dataset: Symptom-fault relationship for IP-network," Computer Networks, vol. 216, p. 109233, 2022. DOI: https://doi.org/10.1016/j.comnet.2022.109233

[21] I. Martinez-Yelmo, J. Alvarez-Horcajo, J. A. Carral, and D. Lopez-Pajares, "eHDDP: Enhanced Hybrid Domain Discovery Protocol for network topologies with both wired/wireless and SDN/non-SDN devices," Computer Networks, vol. 191, p. 107983, 2021. DOI: https://doi.org/10.1016/j.comnet.2021.107983

[22] L. Golightly, P. Modesti, and V. Chang, "Deploying Secure Distributed Systems: Comparative Analysis of GNS3 and SEED Internet Emulator," Journal of Cybersecurity and Privacy, vol. 3, pp. 464-492, 2023. DOI: https://doi.org/10.3390/jcp3030024

[23] I. Nedyalkov, "Application of GNS3 to Study the Security of Data Exchange between Power Electronic Devices and Control Center," Computers, vol. 12, p. 101, 2023. DOI: https://doi.org/10.3390/computers12050101

[24] Z. Aziz and R. Bestak, "Insight into Anomaly Detection and Prediction and Mobile Network Security Enhancement Leveraging K-Means Clustering on Call Detail Records," Sensors, vol. 24, no. 6, p. 1716, 2024. DOI: https://doi.org/10.3390/s24061716

[25] F. Graf, T. Watteyne, and M. Villnow, "Monitoring performance metrics in low-power wireless systems," ICT Express, vol. 10, pp. 989-1018, 2024. DOI: https://doi.org/10.1016/j.icte.2024.08.004

[26] I. Vingestin, T. U. Kalsum, and Y. Mardiana, "The Design Of Network Monitoring System Using SNMP Protocol With Telegram Notification," Jurnal Media Computer Science, vol. 2, no. 1, pp. 93-100, 2023. Available: https://jurnal.unived.ac.id/index.php/jmcs/article/view/3441/2842s