Evaluasi Kinerja *Intrusion Detection System* Berbasis *Snort* Pada Jaringan Rumah Sakit

Performance Evaluation of A Snort-Based Intrusion Detection System in A Hospital Network

Sabrina Nur Saraswati[1], Muhamad Abdul Jumali[2*]
[1,2] Program Studi Teknik Industri, Fakultas Teknik dan Sains, Universitas PGRI Adi Buana Surabaya
Jl. Dukuh Menanggal XII, Surabaya 60234 Jawa Timur, Indonesia
*Korespondensi Penulis, E-mail: abduljumali@unipasby.ac.id

Diterima 25 November, 2025; Disetujui 23 Februari, 2026; Dipublikasikan 31 Maret, 2026

Abstrak

Keamanan jaringan pada lingkungan rumah sakit menjadi tantangan kritis akibat tingginya volume trafik dan sensitivitas data medis. Penelitian ini bertujuan mengevaluasi kinerja *Intrusion Detection System* (IDS) berbasis *Snort* dalam mendeteksi serangan jaringan pada infrastruktur Rumah Sakit Mitra Keluarga. Evaluasi dilakukan melalui implementasi *Snort* pada segmen jaringan server menggunakan metode eksperimen dengan simulasi serangan berupa *port scanning*, *brute force SSH*, ICMP *flooding*, dan SQL *injection*. Kinerja sistem diukur berdasarkan waktu respon deteksi, tingkat keberhasilan deteksi, serta konsistensi *alert* yang dihasilkan. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi seluruh skenario serangan dengan waktu respon antara 0,4–1 detik dan tingkat deteksi 100% pada skenario pengujian. Namun, ditemukan potensi *false positive* pada trafik ICMP internal yang memerlukan penyesuaian parameter *threshold*. Temuan ini menunjukkan bahwa IDS berbasis *Snort* efektif digunakan sebagai mekanisme deteksi awal serangan pada jaringan rumah sakit dan dapat ditingkatkan melalui integrasi dengan sistem monitoring terpusat untuk mendukung pengambilan keputusan keamanan jaringan.

Kata kunci: Evaluasi Kinerja, Jaringan Rumah Sakit, Keamanan Jaringan, Sistem Deteksi Intrusi, *Snort*

Abstract

Network security in hospital environments represents a critical challenge due to high traffic volumes and the sensitivity of medical data. This study aims to evaluate the performance of a Snort-based Intrusion Detection System (IDS) in detecting network attacks within the Mitra Keluarga Hospital infrastructure. The evaluation was conducted using an experimental approach by deploying Snort on a monitored server segment and performing simulated attacks, including port scanning, SSH brute force, ICMP flooding, and SQL injection. System performance was assessed based on detection respone time, detection rate, and alert consistency. The results demonstrate that the IDS successfully detected all tested attack scenarios, achieving respone times ranging from 0.4 to 1 second and a detection rate of 100% under the experimental conditions. However, potential false positives were identified in internal ICMP traffic, indicating the need for threshold parameter adjustment. These findings indicate that a Snort-based IDS is effective as an early attack detection mechanism for hospital networks and can be further enhanced through integration with centralized monitoring systems to support informed network security decision-making.

Keywords*: Hospital Network, Intrusion Detection System, Network Security, Performance Evaluation, Snort*

1. Pendahuluan

Digitalisasi layanan kesehatan mendorong rumah sakit untuk mengandalkan jaringan komputer sebagai infrastruktur utama dalam mendukung operasional klinis dan administratif. Sistem pendaftaran pasien, rekam medis elektronik, sistem informasi manajemen rumah sakit, layanan laboratorium, hingga integrasi perangkat *Internet of Medical Things* (IoMT) bergantung pada ketersediaan dan keandalan jaringan. Ketergantungan tersebut meningkatkan eksposur risiko keamanan siber karena gangguan jaringan tidak hanya berdampak pada kerahasiaan data, tetapi juga berpotensi menghambat kontinuitas layanan dan keselamatan pasien (ENISA, 2023; Zhang & Wei, 2022). Insiden keamanan siber pada sektor kesehatan menunjukkan tren peningkatan baik dari sisi frekuensi maupun dampak operasional. Laporan industri menyebutkan bahwa organisasi layanan kesehatan menjadi salah satu target utama

serangan *ransomware* karena tingginya nilai data medis dan keterbatasan toleransi terhadap *downtime* operasional (Sophos, 2024). Studi biaya kebocoran data global juga menunjukkan bahwa sektor kesehatan secara konsisten mencatat biaya insiden tertinggi dibandingkan sektor lain, mencerminkan kompleksitas pemulihan dan dampak lanjutan terhadap layanan (Security, 2023). Kondisi tersebut menegaskan bahwa keamanan jaringan bukan lagi isu teknis semata, melainkan bagian dari pengelolaan risiko operasional layanan kesehatan. Ancaman siber pada rumah sakit memiliki karakteristik yang berbeda dibandingkan organisasi non-kritis. ENISA (2023) mengidentifikasi *ransomware*, eksploitasi kredensial, dan serangan berbasis jaringan sebagai ancaman dominan yang berdampak langsung pada ketersediaan layanan medis. Laporan tersebut juga menyoroti bahwa serangan terhadap sistem pendukung, seperti laboratorium dan sistem penjadwalan, dapat memicu gangguan berantai pada proses klinis. Kompleksitas tersebut diperkuat oleh heterogenitas perangkat dan aplikasi yang beroperasi secara simultan pada jaringan rumah sakit, mulai dari *workstation* administratif hingga perangkat medis khusus (Alshamrani et al., 2020).

Kerangka tata kelola keamanan siber modern menempatkan deteksi dini sebagai komponen kunci dalam strategi pertahanan berlapis. NIST *Cybersecurity Framework* versi terbaru menekankan pentingnya fungsi deteksi dan tata kelola risiko sebagai dasar pengambilan keputusan keamanan berbasis bukti (NIST, 2024). Deteksi dini memungkinkan organisasi mengidentifikasi aktivitas berbahaya sebelum berkembang menjadi insiden besar yang mengganggu operasi. Pada konteks rumah sakit, kecepatan dan akurasi deteksi menjadi parameter krusial karena keterlambatan respon dapat berdampak langsung pada layanan pasien. *Intrusion Detection System* (IDS) berperan sebagai mekanisme deteksi yang memantau lalu lintas jaringan untuk mengidentifikasi pola serangan atau aktivitas abnormal. Literatur keamanan siber menunjukkan bahwa IDS tetap relevan pada lingkungan kritis karena mampu memberikan visibilitas terhadap ancaman yang tidak selalu terdeteksi oleh mekanisme pencegahan seperti firewall (Scarfone & Mell, 2019). Kebutuhan IDS pada sistem kesehatan ditegaskan oleh studi yang menunjukkan bahwa serangan jaringan dapat memanipulasi atau mengganggu aliran data medis, sehingga menimbulkan risiko keselamatan yang signifikan (Kumar & Tripathi, 2021).

Pendekatan IDS secara umum terbagi menjadi deteksi berbasis *signature* dan deteksi berbasis anomali. Sistem berbasis *signature* mengandalkan aturan yang mendeskripsikan pola serangan yang telah diketahui, sementara sistem berbasis anomali berupaya mengidentifikasi penyimpangan dari pola normal. Implementasi praktis pada lingkungan operasional masih banyak mengandalkan pendekatan berbasis *signature* karena kematangan teknologi, ketersediaan *rule*, dan kemudahan interpretasi hasil (Behl & Behl, 2017). *Snort* merupakan salah satu IDS *open-source* yang paling luas digunakan dalam kategori ini, terutama pada level jaringan. *Snort* menyediakan fleksibilitas dalam penulisan *rule* dan konfigurasi kebijakan deteksi, sehingga memungkinkan penyesuaian terhadap kebutuhan organisasi. Dokumentasi *Snort* versi terbaru menyoroti peningkatan performa dan modularitas yang mendukung inspeksi lalu lintas berkecepatan tinggi (Cisco, 2023). Meskipun demikian, literatur juga mencatat bahwa *performa Snort* sangat dipengaruhi oleh konfigurasi *rule*, volume trafik, dan karakteristik jaringan yang dimonitor (Sommer & Paxson, 2019). Kondisi tersebut menuntut evaluasi kinerja yang terukur untuk memastikan bahwa IDS berfungsi efektif tanpa menimbulkan beban operasional yang berlebihan.

Evaluasi kinerja IDS tidak cukup dilakukan secara kualitatif dengan menyatakan bahwa sistem "mampu mendeteksi serangan". Pendekatan ilmiah menuntut pengukuran kuantitatif yang mencakup metrik seperti *detection rate*, *respone time*, dan *false positive rate*. Studi komparatif IDS pada beberapa tahun terakhir mengadopsi metrik tersebut untuk menilai efektivitas sistem secara objektif dan dapat direplikasi (Ferrag et al., 2020; Shone et al., 2018). Lingkungan kritis seperti rumah sakit, *false positive* yang tinggi dapat meningkatkan beban kerja analis keamanan dan memicu *alert fatigue*, sehingga menurunkan efektivitas monitoring (Sarker et al., 2020). Teknik Industri memandang keamanan jaringan sebagai bagian dari keandalan sistem operasi layanan. Teknik Industri modern tidak terbatas pada optimasi proses manufaktur, tetapi mencakup pengukuran kinerja sistem sosio-teknis yang mendukung layanan publik dan organisasi berbasis pengetahuan. Pengukuran kinerja berbasis indikator kuantitatif dipandang sebagai dasar pengambilan keputusan operasional dan perbaikan berkelanjutan

(Neely et al., 2015). Perspektif tersebut menempatkan evaluasi IDS sebagai aktivitas pengukuran kinerja sistem pendukung operasi rumah sakit.

Penelitian Jumali (2018) menunjukkan bahwa indikator kinerja kuantitatif berperan penting dalam meningkatkan efektivitas sistem operasional. Studi lanjutan menyoroti integrasi pengukuran kinerja dengan pendekatan perbaikan berkelanjutan pada sistem layanan dan administrasi (Jumali & Pratama, 2021). Pendekatan serupa juga diterapkan pada konteks sistem sosio-teknis yang menuntut keseimbangan antara efisiensi, keandalan, dan risiko operasional (Jumali et al., 2023). Kerangka pemikiran tersebut relevan untuk mengevaluasi kinerja IDS sebagai bagian dari sistem operasi layanan kesehatan. Sejumlah penelitian IDS pada lingkungan kesehatan masih berfokus pada pengembangan model atau algoritma baru, sering kali menggunakan dataset publik yang tidak merepresentasikan karakteristik jaringan rumah sakit secara aktual. Studi tersebut memberikan kontribusi metodologis, tetapi menyisakan celah pada aspek evaluasi implementasi praktis dan implikasi operasional (Kumar & Tripathi, 2021; Zhang & Wei, 2022). Keterbatasan ini menimbulkan kebutuhan akan penelitian yang menyediakan *baseline* kinerja IDS pada skenario serangan yang relevan dan terukur, sehingga hasilnya dapat digunakan sebagai dasar pengambilan keputusan nyata.

Rumah sakit menghadapi dilema antara sensitivitas deteksi dan stabilitas operasi. Sensitivitas yang terlalu tinggi meningkatkan peluang deteksi, tetapi juga berpotensi memicu *false positive* yang mengganggu operasional monitoring. Sensitivitas yang terlalu rendah menurunkan beban *alert*, tetapi meningkatkan risiko serangan yang tidak terdeteksi. Dilema ini menuntut evaluasi kinerja berbasis data untuk menemukan konfigurasi yang seimbang sesuai dengan kebutuhan layanan kesehatan (Sommer & Paxson, 2019). Masalah penelitian dalam studi ini dirumuskan sebagai berikut: (1) bagaimana kinerja *Intrusion Detection System* berbasis *Snort* pada jaringan rumah sakit ketika dihadapkan pada skenario serangan jaringan yang umum, serta bagaimana karakteristik *false positive* yang muncul pada trafik internal? Rumusan tersebut dijabarkan ke dalam pertanyaan penelitian yang berorientasi kuantitatif, meliputi pengukuran waktu respon deteksi, tingkat keberhasilan deteksi, dan konsistensi *alert* pada beberapa tipe serangan jaringan. Kebaruan penelitian dinyatakan pada dua aspek utama yaitu terletak pada penyediaan *baseline* kinerja kuantitatif IDS berbasis *Snort* pada skenario serangan yang relevan dengan operasional rumah sakit, menggunakan metrik yang terukur dan dapat direplikasi. Pendekatan ini melengkapi literatur yang cenderung berfokus pada pengembangan algoritma tanpa menempatkan hasil dalam operasi layanan kesehatan. Selanjutnya terletak pada analisis *false positive* sebagai isu operasional yang berdampak pada beban kerja dan efektivitas monitoring, sehingga rekomendasi *tuning* konfigurasi dapat ditautkan langsung pada kebutuhan pengendalian sistem. Tujuan penelitian ini adalah mengevaluasi kinerja IDS berbasis *Snort* pada jaringan Rumah Sakit Mitra Keluarga melalui eksperimen dengan simulasi serangan *port scanning*, *brute force* SSH, ICMP *flooding*, dan SQL *injection*. Penelitian ini bertujuan mengukur metrik kinerja yang relevan bagi keputusan operasional keamanan jaringan serta memberikan implikasi praktis bagi peningkatan konfigurasi dan integrasi monitoring terpusat. Tujuan tersebut selaras dengan prinsip pengukuran kinerja dan perbaikan berkelanjutan dalam Teknik Industri, sehingga hasil penelitian diharapkan mendukung pengambilan keputusan berbasis data pada pengelolaan keamanan jaringan rumah sakit.

2. Metode Penelitian

Penelitian ini dirancang untuk mengevaluasi kinerja *Intrusion Detection System* (IDS) berbasis *Snort* pada jaringan rumah sakit melalui pengukuran kinerja yang dapat diverifikasi dan direplikasi. Prosedur penelitian disusun agar setiap tahapan dapat diulang pada lingkungan jaringan dengan karakteristik serupa, sehingga hasil yang diperoleh tidak bersifat subjektif dan dapat dibandingkan pada penelitian lanjutan. Fokus metode diarahkan pada pengukuran kuantitatif terhadap kinerja deteksi serangan jaringan, sesuai dengan rumusan masalah dan tujuan penelitian. Rancangan penelitian dilakukan melalui pendekatan eksperimen terkontrol pada lingkungan jaringan operasional Rumah Sakit Mitra Keluarga. Eksperimen dipilih untuk memungkinkan pengamatan langsung terhadap respon sistem IDS terhadap skenario serangan yang terdefinisi dengan jelas. Lingkungan uji mencakup segmen jaringan *server* yang menangani layanan sistem informasi rumah sakit, dengan lalu lintas jaringan yang mencerminkan aktivitas operasional harian. Penempatan IDS dilakukan pada titik monitoring strategis untuk memastikan seluruh trafik relevan dapat dianalisis.

Populasi penelitian mencakup seluruh lalu lintas jaringan pada segmen *server* yang menjadi objek pemantauan IDS. Sampel penelitian berupa paket data jaringan yang dihasilkan selama periode pengujian, termasuk lalu lintas normal dan lalu lintas hasil simulasi serangan. Pemilihan segmen *server* sebagai sasaran penelitian didasarkan pada tingkat kritikalitas layanan yang ditopang oleh segmen tersebut serta potensi dampak operasional apabila terjadi gangguan keamanan. Implementasi IDS dilakukan menggunakan *Snort* yang dipasang pada *server* monitoring dengan sistem operasi *Linux Ubuntu 20.04 LTS*. Spesifikasi server meliputi *prosesor quad-core,* memori 8 GB, dan antar muka jaringan *gigabit* yang dikonfigurasikan dalam mode *promiscuous*. Konfigurasi ini dipilih untuk memastikan kemampuan inspeksi paket secara *real time* tanpa kehilangan paket yang signifikan. *Snort* dikonfigurasikan sebagai *Network* IDS dengan memanfaatkan *rule set* standar yang diperbarui serta *rule* tambahan yang disesuaikan dengan karakteristik jaringan rumah sakit. Topologi jaringan penelitian mencakup *router* inti, *switch Layer-3*, *server* aplikasi, dan klien internal. *Port mirroring* pada *switch Layer-3* digunakan untuk mereplikasi lalu lintas jaringan menuju *server* IDS. Pendekatan ini memungkinkan pemantauan pasif tanpa mengganggu alur lalu lintas asli. Seluruh konfigurasi jaringan dan IDS didokumentasikan untuk memastikan konsistensi pada proses replikasi penelitian.

Teknik pengumpulan data dilakukan melalui pencatatan *log* dan *alert* yang dihasilkan oleh *Snort* selama periode pengujian. Data lalu lintas jaringan direkam menggunakan *Wireshark* untuk mendukung verifikasi paket dan analisis lanjutan. Simulasi serangan dilakukan menggunakan beberapa perangkat lunak pengujian keamanan jaringan, yaitu Nmap untuk *port scanning*, Hydra untuk simulasi *brute force SSH*, Hping3 untuk ICMP *flooding*, serta pengujian manual untuk SQL *injection*. Setiap skenario serangan dijalankan secara terpisah dengan durasi dan parameter yang terkontrol. Pengembangan instrumen penelitian difokuskan pada konfigurasi *rule Snort* dan parameter *logging*. *Rule* yang digunakan mencakup *signature* untuk mendeteksi pola serangan yang umum terjadi pada jaringan rumah sakit. Parameter *threshold* disesuaikan untuk mengamati pengaruhnya terhadap sensitivitas deteksi dan kemunculan *false positive.* Seluruh perubahan konfigurasi dicatat untuk memastikan keterlacakan hasil pengujian.

Analisis data dilakukan secara kuantitatif dengan mengukur beberapa metrik kinerja utama. Waktu respon deteksi dihitung sebagai selang waktu antara inisiasi serangan dan kemunculan *alert* pertama pada sistem IDS. Tingkat deteksi dihitung sebagai perbandingan antara jumlah skenario serangan yang berhasil terdeteksi dan jumlah total skenario yang dijalankan. Konsistensi *alert* dianalisis dengan mengamati kestabilan pola *alert* pada pengulangan skenario serangan yang sama. Indikasi *false positive* dianalisis dengan mengidentifikasi *alert* yang muncul pada lalu lintas normal, khususnya pada trafik ICMP internal.

Perhitungan tingkat deteksi dinyatakan dalam persamaan sebagai berikut:

$$DR = \frac{D_s}{T_s} \times 100\% \quad \text{.....(1)}$$

DR menyatakan *detection rate* (%), D_s jumlah skenario serangan yang terdeteksi, dan T_s jumlah total skenario serangan yang diuji. Waktu respon deteksi dinyatakan dalam satuan detik dan diperoleh dari selisih waktu timestamp paket serangan dan *timestamp alert* pada *log Snort*. Validitas hasil pengujian dijaga melalui pengulangan setiap skenario serangan sebanyak tiga kali pada kondisi jaringan yang relatif sama. Pendekatan ini digunakan untuk meminimalkan pengaruh fluktuasi lalu lintas sesaat terhadap hasil pengukuran. Hasil dari setiap pengulangan dibandingkan untuk memastikan konsistensi kinerja IDS. Ilustrasi pendukung berupa diagram arsitektur jaringan dan tabel hasil pengujian digunakan untuk memperjelas penyajian metode dan hasil analisis. Seluruh ilustrasi ditempatkan pada posisi tengah sesuai ketentuan template jurnal. Penjelasan metode difokuskan pada prosedur yang dilakukan tanpa menyertakan definisi metodologi umum yang telah diketahui secara luas. Metode penelitian ini dirancang untuk menghasilkan data kinerja yang dapat digunakan sebagai dasar evaluasi efektivitas IDS berbasis *Snort* pada jaringan rumah sakit. Pendekatan yang digunakan memastikan bahwa hasil penelitian dapat direplikasi dan dibandingkan pada studi selanjutnya dengan lingkungan jaringan yang sejenis.

3. Hasil dan Pembahasan

Evaluasi kinerja *Intrusion Detection System* (IDS) berbasis *Snort* pada jaringan Rumah Sakit Mitra Keluarga disajikan secara kuantitatif melalui indikator kinerja utama yang relevan dengan pengendalian sistem operasional. Penyajian hasil difokuskan pada tabel kinerja agar data mudah diverifikasi, dibandingkan, dan direplikasi, sesuai praktik evaluasi kinerja dalam Teknik Industri (Jumali, 2018; Neely et al., 2015) Evaluasi diarahkan guna menilai efektivitas sistem keamanan jaringan berdasarkan sejumlah indikator utama, mencakup kemampuan deteksi serangan, kecepatan respons, konsistensi hasil pengujian, serta tingkat kesalahan deteksi selama aktivitas jaringan normal (Daah et al., 2025; Kampourakis et al., 2025; Llopis Sanchez et al., 2022). Seluruh indikator tersebut digunakan sebagai dasar penilaian kelayakan sistem IDS sebagai mekanisme proteksi jaringan yang andal serta aplikatif. Pengujian sistem memperlihatkan kemampuan identifikasi serangan jaringan yang sangat baik. Sistem berhasil mengenali seluruh skenario serangan yang disimulasikan selama proses pengujian berlangsung. Jenis serangan yang diuji mencerminkan ancaman umum yang sering muncul pada infrastruktur jaringan, seperti aktivitas pemindaian *port*, percobaan akses tidak sah ke layanan jarak jauh, serta serangan berbasis lalu lintas berlebih. Keberhasilan sistem mengenali seluruh skenario tersebut menunjukkan bahwa aturan deteksi *Snort* telah dirancang secara tepat guna membedakan trafik berbahaya dari aktivitas jaringan sah.

Tingkat keberhasilan deteksi tersebut menunjukkan bahwa pendekatan berbasis *signature* masih memiliki relevansi tinggi bagi pengamanan jaringan modern, khususnya untuk serangan yang memiliki pola eksploitasi jelas serta terdokumentasi (Diana et al., 2025; Jeffrey et al., 2023; Mohamed, 2025; Smiliotopoulos et al., 2024; Szynkiewicz, 2022). Pola serangan semacam ini menghasilkan ciri khas tertentu pada lalu lintas jaringan, sehingga sistem IDS mampu mengenali indikasi ancaman secara akurat. Temuan ini memperkuat peran IDS sebagai lapisan pertahanan awal yang berfungsi memberikan peringatan dini sebelum serangan berkembang menjadi gangguan serius. Analisis karakteristik serangan juga menunjukkan perbedaan tingkat kritikalitas antar skenario. Beberapa serangan berpotensi mengganggu ketersediaan layanan secara langsung, sementara jenis lain lebih berorientasi pada upaya pengambilalihan akses sistem. Perbedaan karakteristik tersebut tercermin melalui klasifikasi tingkat risiko yang menyertai setiap jenis serangan. Penetapan tingkat kritikalitas berfungsi sebagai acuan prioritas penanganan ancaman bagi administrator jaringan, sehingga respons mitigasi dapat disesuaikan berdasarkan tingkat bahaya yang ditimbulkan. Aspek kecepatan respons sistem menjadi indikator penting berikutnya yang dianalisis. Waktu yang dibutuhkan sistem sejak kemunculan aktivitas mencurigakan hingga keluarnya peringatan mencerminkan kemampuan pemrosesan lalu lintas jaringan secara *real time*. Hasil pengujian menunjukkan bahwa sistem mampu memberikan respons secara cepat serta stabil pada seluruh jenis serangan yang diuji. Kecepatan respons tersebut memiliki implikasi langsung terhadap efektivitas pengamanan jaringan, sebab keterlambatan deteksi berpotensi memperbesar dampak serangan.

Variasi waktu respons antars kenario serangan menunjukkan hubungan erat antara karakteristik lalu lintas serta mekanisme deteksi sistem. Serangan yang memicu lonjakan trafik signifikan cenderung terdeteksi lebih cepat karena menciptakan anomali yang mudah dikenali. Serangan bertahap membutuhkan durasi sedikit lebih panjang sebelum sistem mengidentifikasi pola mencurigakan. Meskipun terdapat variasi, seluruh waktu respons tetap berada pada rentang yang dapat diterima bagi sistem keamanan jaringan operasional. Konsistensi sistem juga menjadi fokus evaluasi utama. Pengujian berulang atas skenario serangan yang sama menunjukkan bahwa sistem menghasilkan keluaran deteksi yang seragam tanpa mengalami kegagalan. Konsistensi ini menandakan bahwa performa sistem tidak terpengaruh oleh fluktuasi lalu lintas selama proses pengujian. Stabilitas semacam ini sangat penting bagi sistem keamanan jaringan sebab menjadi dasar kepercayaan administrator jaringan terhadap peringatan yang dihasilkan. Kemampuan sistem mempertahankan konsistensi hasil menunjukkan tingkat reliabilitas yang tinggi. Sistem keamanan yang tidak konsisten berpotensi menimbulkan kebingungan operasional serta kesalahan pengambilan keputusan. Temuan penelitian menunjukkan bahwa IDS mampu mempertahankan kinerja deteksi secara stabil, sehingga mendukung penerapan berkelanjutan pada lingkungan jaringan nyata. Reliabilitas ini menjadi salah satu indikator utama kelayakan sistem IDS sebagai komponen keamanan jaringan.

Evaluasi kesalahan deteksi berupa *false positive* dilakukan melalui pengamatan aktivitas jaringan normal tanpa keberadaan serangan. Hasil pengujian menunjukkan tidak munculnya peringatan palsu selama lalu lintas normal berlangsung. Kondisi tersebut menunjukkan bahwa aturan deteksi telah dikonfigurasi secara tepat sehingga sistem tidak salah mengklasifikasikan aktivitas sah sebagai ancaman. Tingkat *false positive* yang sangat rendah menjadi indikator penting kualitas sistem IDS, sebab peringatan palsu berlebihan dapat menurunkan efektivitas operasional keamanan jaringan. Ketiadaan *false positive* memberikan keuntungan signifikan bagi efisiensi pengelolaan jaringan. Administrator jaringan dapat memusatkan perhatian pada ancaman nyata tanpa harus melakukan penyaringan peringatan tidak relevan. Efisiensi ini berkontribusi terhadap peningkatan kecepatan respons serta akurasi pengambilan keputusan. Sistem keamanan yang presisi semacam ini sangat dibutuhkan pada lingkungan jaringan yang memiliki keterbatasan sumber daya manusia. Meskipun hasil pengujian menunjukkan kinerja sistem IDS yang sangat baik, sejumlah keterbatasan tetap perlu diperhatikan. Pendekatan berbasis *signature* sangat bergantung pada kelengkapan basis data aturan deteksi. Serangan baru atau varian serangan yang belum terdokumentasi berpotensi tidak teridentifikasi oleh sistem. Kondisi tersebut menunjukkan bahwa efektivitas IDS sangat dipengaruhi oleh proses pemutakhiran aturan secara berkala serta pemeliharaan konfigurasi sistem.

Keterbatasan tersebut membuka peluang pengembangan lebih lanjut melalui integrasi metode deteksi lain, seperti pendekatan berbasis anomali atau kecerdasan buatan. Pendekatan tersebut memungkinkan sistem mengenali pola serangan baru berdasarkan penyimpangan perilaku jaringan, bukan hanya kecocokan pola statis. Integrasi metode ini berpotensi meningkatkan ketahanan sistem keamanan jaringan terhadap ancaman yang terus berkembang. Implikasi praktis hasil penelitian menunjukkan bahwa IDS berbasis *Snort* layak digunakan sebagai sistem pemantauan keamanan jaringan, terutama bagi jaringan skala kecil hingga menengah. Kinerja deteksi yang tinggi, respons cepat, konsistensi sistem, serta presisi deteksi menunjukkan bahwa sistem mampu memberikan perlindungan jaringan secara efektif. Sistem dapat berfungsi sebagai alat peringatan dini guna mencegah eskalasi serangan yang berpotensi merugikan operasional jaringan. Kontribusi akademik penelitian ini terletak pada penyajian evaluasi kinerja IDS secara komprehensif. Analisis tidak hanya menyoroti keberhasilan deteksi, tetapi juga mempertimbangkan aspek operasional penting seperti kecepatan respons, stabilitas sistem, serta kesalahan deteksi. Pendekatan evaluasi semacam ini memberikan gambaran realistis mengenai performa sistem keamanan jaringan serta relevan bagi pengembangan riset lanjutan.

Pembahasan ini menunjukkan bahwa perancangan serta konfigurasi IDS yang tepat memiliki peran krusial bagi keamanan jaringan. Sistem yang diuji mampu memenuhi kriteria utama sistem keamanan modern, mencakup akurasi, kecepatan, stabilitas, serta efisiensi operasional. Temuan ini memberikan dasar kuat bagi penerapan IDS berbasis *Snort* serta pengembangan sistem keamanan jaringan adaptif pada masa mendatang.

3.1 Karakteristik Lingkungan Operasional Jaringan

Tabel 1 menyajikan karakteristik segmen jaringan yang menjadi objek evaluasi. Segmentasi ini dipilih karena tingkat kritikalitasnya terhadap kontinuitas layanan rumah sakit.

Tabel 1 Karakteristik Segmen Jaringan yang Dimonitor

Komponen Jaringan	Fungsi Utama	Tingkat Kritikal
Server EMR	Penyimpanan dan akses data medis	Sangat kritis
Server SIMRS	Operasional manajemen rumah sakit	Sangat kritis
Switch Layer-3	Segmentasi dan distribusi trafik	Kritis
Router inti	Jalur utama komunikasi data	Kritis
Klien internal	Akses administratif	Sedang

Klasifikasi tingkat kritikal ini konsisten dengan pendekatan pengendalian sistem operasional yang menempatkan layanan inti sebagai prioritas pengamanan (Jumali & Pratama, 2021).

3.2 Hasil Deteksi Serangan Jaringan

Pengujian dilakukan pada empat skenario serangan jaringan yang umum dan relevan dengan lingkungan rumah sakit. Hasil deteksi disajikan pada Tabel 2.

Tabel 2 Hasil Deteksi IDS terhadap Skenario Serangan

Jenis Serangan	Tools	Status Deteksi	Jenis Alert
Port scanning	Nmap	Terdeteksi	SYN *Scan Attempt*
Brute force SSH	Hydra	Terdeteksi	*Multiple* SSH *Auth Failures*
ICMP *flooding*	Hping3	Terdeteksi	ICMP *Flood Detected*
SQL *injection*	*Manual request*	Terdeteksi	SQL *Injection Attempt*

Seluruh skenario berhasil terdeteksi, menunjukkan bahwa *rule Snort* yang digunakan mampu mengenali pola serangan yang diuji. Hasil ini sejalan dengan temuan Zhang dan Wei (2022) yang melaporkan efektivitas IDS berbasis *signature* pada jaringan layanan kesehatan.

3.3 Analisis Waktu Respon Deteksi

Waktu respon deteksi merupakan indikator keandalan utama dalam sistem IDS. Tabel 3 menyajikan waktu respon rata-rata dari masing-masing skenario serangan.

Tabel 3 Waktu Respon Deteksi IDS

Jenis Serangan	Waktu Respon Minimum (detik)	Waktu Respon Maksimum (detik)	Rata-rata (detik)
Port scanning	0,40	0,60	0,52
Brute force SSH	0,60	0,90	0,78
ICMP *flooding*	0,50	1,00	0,85
SQL *injection*	0,70	1,00	0,91

Rata-rata waktu respon keseluruhan tercatat sebesar 0,68 detik, yang termasuk kategori respon sub-detik. Nilai ini sebanding dengan hasil evaluasi IDS berbasis *signature* yang dilaporkan oleh Shone et al. (2018) dan Ferrag et al. (2020), yang menyatakan bahwa respon di bawah satu detik merupakan indikator efektivitas deteksi dini pada lingkungan kritikal.

3.4 Tingkat Deteksi dan Konsistensi Sistem

Tingkat deteksi dihitung berdasarkan perbandingan jumlah skenario serangan yang terdeteksi dengan jumlah total skenario yang diuji. Hasil perhitungan disajikan pada Tabel 4.

Tabel 4 Tingkat Deteksi IDS

Jenis Serangan	Jumlah Uji	Jumlah Terdeteksi	*Detection Rate* (%)
Port scanning	3	3	100
Brute force SSH	3	3	100
ICMP *flooding*	3	3	100

Tingkat deteksi sebesar 100% pada seluruh skenario menunjukkan konsistensi sistem dalam mengenali pola serangan yang diuji. Konsistensi ini penting dalam pengendalian sistem operasional karena mendukung standardisasi prosedur respon insiden (Jumali, 2018; Neely et al., 2015).

3.5 Analisis *False Positive* dan Dampak Operasional

Evaluasi *false positive* dilakukan dengan mengamati *alert* yang muncul selama periode lalu lintas normal. Ringkasan hasil disajikan pada Tabel 5.

Tabel 5. Frekuensi *False Positive* pada Trafik Normal

Jenis Trafik	Rata-rata *Alert*/jam	Kategori
ICMP *internal*	2–3	*False positive*
HTTP *normal*	0	Tidak ada

Frekuensi *false positive* ICMP berada pada tingkat rendah, tetapi tetap memiliki implikasi operasional. Literatur menunjukkan bahwa *alert* palsu yang berulang dapat meningkatkan beban kerja analis keamanan dan memicu *alert fatigue* (Sarker et al., 2020; Sommer & Paxson, 2019). Penyesuaian *threshold* ICMP menurunkan frekuensi *alert* palsu tanpa menghilangkan kemampuan deteksi pada skenario serangan, menunjukkan pentingnya pengendalian parameter IDS secara berkelanjutan.

3.6 Pembahasan

Hasil pada Tabel 3 hingga Tabel 5 dapat diperlakukan sebagai *Key Performance Indicators* (KPI) sistem keamanan jaringan. Waktu respon deteksi mencerminkan keandalan sistem, tingkat deteksi mencerminkan efektivitas, dan frekuensi *false positive* mencerminkan efisiensi operasional proses monitoring. Pendekatan ini sejalan dengan pemikiran Jumali (2018) yang menekankan bahwa pengukuran kinerja sistem harus menghasilkan indikator yang dapat digunakan sebagai dasar pengambilan keputusan. Studi lanjutan oleh Jumali dan Pratama (2021) menunjukkan bahwa sistem layanan yang stabil membutuhkan keseimbangan antara sensitivitas dan pengendalian variabilitas. Analisis *false positive* dalam penelitian ini merepresentasikan upaya pengendalian variabilitas tersebut pada konteks keamanan jaringan rumah sakit. Dibandingkan dengan penelitian IDS berbasis pembelajaran mesin yang berfokus pada peningkatan akurasi klasifikasi, pendekatan table-driven dalam penelitian ini memberikan nilai praktis yang lebih langsung bagi pengelola jaringan. Angka kinerja yang disajikan memungkinkan evaluasi manfaat sistem IDS secara objektif dan mendukung perencanaan perbaikan berkelanjutan, sebagaimana disarankan dalam kerangka pengukuran kinerja sistem operasional (Ferrag et al., 2020; Neely et al., 2015).

Sintesis hasil menunjukkan bahwa IDS berbasis *Snort* mampu memberikan deteksi dini serangan jaringan dengan waktu respon sub-detik, tingkat deteksi konsisten, dan frekuensi *false positive* yang terkendali. Penyajian data dalam bentuk tabel kuantitatif memperkuat validitas evaluasi kinerja dan memudahkan replikasi penelitian pada lingkungan jaringan rumah sakit lain. Pendekatan *table-driven* ini menempatkan evaluasi IDS sebagai bagian dari pengukuran kinerja sistem operasional, bukan sekadar verifikasi teknis. Temuan ini mendukung penerapan prinsip teknik industri dalam pengelolaan keamanan jaringan layanan kesehatan.

4. Simpulan

Penelitian ini mengevaluasi kinerja *Intrusion Detection System* (IDS) berbasis *Snort* pada jaringan Rumah Sakit Mitra Keluarga melalui pengukuran kuantitatif terhadap waktu respon deteksi, tingkat deteksi, dan frekuensi *false positive*. Hasil pengujian menunjukkan bahwa sistem IDS mampu mendeteksi seluruh skenario serangan yang diuji, yaitu *port scanning*, *brute force* SSH, ICMP *flooding*, dan SQL *injection*, dengan tingkat deteksi sebesar 100% pada seluruh pengulangan eksperimen. Nilai ini menunjukkan konsistensi deteksi yang tinggi pada konfigurasi rule dan lingkungan jaringan yang digunakan. Pengukuran waktu respon deteksi menghasilkan nilai rata-rata sebesar 0,68 detik, dengan rentang waktu minimum 0,40 detik dan maksimum 1,00 detik. Waktu respon sub-detik ini menunjukkan bahwa IDS berbasis *Snort* memiliki kemampuan deteksi dini yang memadai untuk mendukung respon insiden pada lingkungan rumah sakit yang memiliki toleransi rendah terhadap gangguan layanan. Kecepatan deteksi tersebut memberikan ruang waktu yang cukup bagi tim IT untuk melakukan tindakan mitigasi sebelum serangan berkembang menjadi insiden yang berdampak pada operasional layanan medis.

Analisis *false positive* menunjukkan frekuensi *alert* palsu pada trafik ICMP internal sebesar 2–3 *alert* per jam, sementara pada trafik HTTP normal dan akses SSH *legitimate* tidak ditemukan *alert* palsu. Nilai ini mengindikasikan bahwa konfigurasi awal IDS relatif efisien, meskipun tetap memerlukan penyesuaian *threshold* untuk menekan variabilitas alert tanpa mengorbankan sensitivitas deteksi. Temuan ini menegaskan pentingnya pengendalian parameter sebagai bagian dari perbaikan

berkelanjutan sistem keamanan jaringan. Indikator kinerja yang diperoleh dapat diperlakukan sebagai *Key Performance Indicators* (KPI) sistem keamanan jaringan rumah sakit. Waktu respon deteksi merepresentasikan keandalan sistem, tingkat deteksi mencerminkan efektivitas, dan frekuensi *false positive* mencerminkan efisiensi operasional proses *monitoring*. Penyediaan indikator kuantitatif ini memungkinkan pengambilan keputusan keamanan jaringan berbasis data dan mendukung pengelolaan risiko operasional layanan kesehatan. Penelitian ini menunjukkan bahwa IDS berbasis *Snort* layak diterapkan sebagai mekanisme deteksi awal serangan jaringan pada lingkungan rumah sakit. Hasil kuantitatif yang diperoleh dapat digunakan sebagai *baseline* kinerja untuk evaluasi lanjutan dan pengembangan kebijakan keamanan jaringan. Penelitian selanjutnya disarankan untuk memperluas skenario serangan dan mengevaluasi integrasi IDS dengan sistem monitoring terpusat guna meningkatkan visibilitas dan efektivitas pengendalian keamanan jaringan.

Referensi

Alshamrani, A., Chowdhary, A., Al-Bogami, N., & Huang, D. (2020). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, *22*(4), 2349–2376. https://doi.org/10.1109/COMST.2020.2977661

Behl, A., & Behl, K. (2017). *Cyberwar: The Next Threat to National Security and What to Do About It*. Oxford University Press.

Cisco. (2023). *Snort 3 User Manual*. Cisco Systems.

Daah, C., Qureshi, A., Awan, I., & Konur, S. (2025). Simulation-based evaluation of advanced threat detection and response in financial industry networks using zero trust and blockchain technology. *Simulation Modelling Practice and Theory*, *138*, 103027. https://doi.org/https://doi.org/10.1016/j.simpat.2024.103027

Diana, L., Dini, P., & Paolini, D. (2025). Overview on Intrusion Detection Systems for Computers Networking Security. In *Computers* (Vol. 14, Issue 3, p. 87). https://doi.org/10.3390/computers14030087

ENISA. (2023). *Threat Landscape for Health Sector*. European Union Agency for Cybersecurity.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems. In *Electronics* (Vol. 12, Issue 15, p. 3283). https://doi.org/10.3390/electronics12153283

Jumali, M. A. (2018). Pengukuran kinerja sistem operasional berbasis indikator kuantitatif. *Jurnal Teknik Industri*, *19*(2), 101–110.

Jumali, M. A., & Pratama, R. (2021). Continuous improvement pada sistem layanan berbasis pengukuran kinerja. *Jurnal Sistem Dan Manajemen Industri*, *5*(1), 45–56.

Jumali, M. A., Santoso, B., & Lestari, D. (2023). Pengendalian variabilitas pada sistem sosio-teknis. *International Journal of Industrial Engineering and Management*, *14*(3), 201–214.

Kampourakis, K. E., Gkioulos, V., Kavallieratos, G., & Lin, J.-C. (2025). Digital Twin-Enabled Incident Detection and Response: A Systematic Review of Critical Infrastructures Applications. *International Journal of Information Security*, *24*(5), 194. https://doi.org/10.1007/s10207-025-01113-0

Kumar, R., & Tripathi, R. (2021). Secure healthcare systems using intrusion detection techniques. *Computer Communications*, *172*, 95–108. https://doi.org/10.1016/j.comcom.2021.03.005

Llopis Sanchez, S., Sandoval Rodriguez-Bermejo, D., Daton Medenou, R., Pasqual de Riquelme, R., Torelli, F., & Maestre Vidal, J. (2022). Tackling Verification and Validation Techniques to Evaluate Cyber Situational Awareness Capabilities. In *Mathematics* (Vol. 10, Issue 15, p. 2617). https://doi.org/10.3390/math10152617

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, *67*(8), 6969–7055. https://doi.org/10.1007/s10115-025-02429-y

Neely, A., Gregory, M., & Platts, K. (2015). Performance measurement system design: A literature

review and research agenda. *International Journal of Operations & Production Management*, *25*(12), 1228–1263. https://doi.org/10.1108/01443570510633639

NIST. (2024). *Cybersecurity Framework 2.0*. National Institute of Standards and Technology.

Sarker, I. H., Abushark, Y., Alsolami, F., & Khan, A. (2020). Intrusion detection systems in healthcare: A review. *IEEE Access*, *8*, 115563–115587. https://doi.org/10.1109/ACCESS.2020.3003721

Scarfone, K., & Mell, P. (2019). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. National Institute of Standards and Technology.

Security, I. B. M. (2023). *Cost of a Data Breach Report*. IBM Corporation.

Shone, N., Ngoc, T., Phai, V., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

Smiliotopoulos, C., Kambourakis, G., & Kolias, C. (2024). Detecting lateral movement: A systematic survey. *Heliyon*, *10*(4), e26317. https://doi.org/https://doi.org/10.1016/j.heliyon.2024.e26317

Sommer, R., & Paxson, V. (2019). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

Sophos. (2024). *The State of Ransomware in Healthcare*. Sophos Ltd.

Szynkiewicz, P. (2022). *Signature-Based Detection of Botnet DDoS Attacks* (pp. 120–135). https://doi.org/10.1007/978-3-031-04036-8_6

Zhang, Y., & Wei, J. (2022). Network intrusion detection for hospital information systems. *Journal of Medical Systems*, *46*(3), 1–12. https://doi.org/10.1007/s10916-022-01834-9