JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i1.8235

PENGEMBANGAN SISTEM LOGGING JARINGAN BERBASIS WEB UNTUK MENCATAT SEMUA LOG AKTIVITAS DAN DETEKSI ANOMALI

Anggi Ferita Oktaviani Silalahi[1*], Dedy Kiswanto[2] Azhara Amelia[3]

[1,2,3] Program Studi Ilmu Komputer;Universitas Negeri Medan.

Keywords:
pencatatan jaringan; pemantauan web; deteksi anomali; keamanan sistem; aktivitas pengguna.

Corespondent
Email:anggisilalahi338@gmail.com

Abstrak. Penelitian ini bertujuan untuk mengembangkan sistem logging jaringan berbasis web yang berfungsi untuk mencatat seluruh aktivitas pengguna secara real-time serta mendeteksi anomali pada sistem. Latar belakang penelitian ini didasari oleh meningkatnya kebutuhan pengawasan aktivitas jaringan pada aplikasi web yang sering menjadi target penyalahgunaan akun dan ancaman keamanan. Sistem ini dikembangkan menggunakan metode pengembangan perangkat lunak berbasis web dengan teknologi HTML, CSS, dan JavaScript. Penyimpanan data log dilakukan menggunakan localStorage yang menyimpan setiap aktivitas pengguna seperti login, logout, dan interaksi halaman. Proses deteksi anomali dilakukan dengan menganalisis pola aktivitas tidak wajar, seperti percobaan login gagal berulang atau akses dari alamat IP yang mencurigakan. Hasil pengujian menunjukkan bahwa sistem mampu mencatat seluruh log aktivitas dengan akurasi tinggi dan memberikan peringatan terhadap aktivitas anomali secara cepat. Kesimpulan dari penelitian ini adalah sistem logging yang dikembangkan dapat meningkatkan transparansi, keamanan, serta efisiensi dalam proses pemantauan aktivitas jaringan pada aplikasi web.

network logging; web monitoring; anomaly detection; system security; user activity

Abstract. *This study aims to develop a web-based network logging system designed to record all user activities in real-time and detect anomalies within the system. The background of this research arises from the increasing need for network activity monitoring in modern web applications, which are often vulnerable to account misuse and cyberattacks. The system was developed using a web-based software development method with HTML, CSS, and JavaScript technologies. Activity data are stored locally using the localStorage feature to record events such as login, logout, and page interactions. Anomaly detection is performed by analyzing unusual activity patterns, such as repeated failed login attempts or access from suspicious IP addresses. The experimental results show that the system is capable of recording all user activities accurately and providing timely alerts when anomalous behavior is detected. In conclusion, the developed logging system can enhance transparency, security, and efficiency in monitoring user activities within web applications.*

1. PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat telah menjadikan sistem berbasis web sebagai platform utama dalam berbagai aktivitas, mulai dari komunikasi, transaksi digital, hingga layanan publik. Dalam konteks ini, keamanan dan pengelolaan aktivitas pengguna menjadi aspek yang sangat penting untuk menjaga integritas dan keandalan sistem. Salah satu pendekatan yang banyak digunakan dalam memastikan keamanan sistem

adalah penerapan logging jaringan, yaitu proses pencatatan seluruh aktivitas yang terjadi pada sistem untuk tujuan pemantauan dan audit keamanan [9]. Melalui sistem logging, administrator dapat mengetahui jejak aktivitas pengguna, mendeteksi aktivitas mencurigakan, serta melakukan analisis ketika terjadi gangguan atau pelanggaran keamanan Beberapa penelitian sebelumnya telah menyoroti pentingnya sistem logging dan deteksi anomali berbasis web. Penelitian oleh [1] mengembangkan sistem monitoring berbasis web untuk mencatat aktivitas pengguna dengan metode analisis log sederhana. Sementara itu, [15] menerapkan pendekatan *machine learning* dengan algoritma Isolation Forest untuk mendeteksi anomali pada log aktivitas web server dan berhasil meningkatkan tingkat deteksi hingga 92%. Penelitian oleh [3] smenunjukkan bahwa penggunaan logging otomatis berbasis PHP dan JavaScript dapat mempercepat proses audit sistem hingga 40% dibandingkan pencatatan manual. Selain itu, penelitian menekankan pentingnya integrasi antara logging dan sistem peringatan (*alert system*) yang dapat memberikan notifikasi ketika aktivitas abnormal terdeteksi.

Selain pendekatan tersebut, teori keamanan informasi seperti CIA Triad (Confidentiality, Integrity, Availability) menjadi dasar penting dalam merancang sistem logging. Logging yang baik tidak hanya mencatat aktivitas, tetapi juga memastikan bahwa data log terlindungi dari manipulasi serta dapat diakses ketika dibutuhkan [12]. Dalam konteks web modern, penyimpanan log sering kali dilakukan secara lokal atau terdistribusi, salah satunya melalui fitur *localStorage* pada browser yang memungkinkan pencatatan aktivitas secara instan tanpa harus mengandalkan server eksternal [15]. Namun demikian, hasil tinjauan terhadap penelitian-penelitian sebelumnya menunjukkan adanya beberapa kesenjangan penelitian (*gap analysis*). Sebagian besar sistem logging masih terbatas pada pencatatan aktivitas login atau error tanpa memantau perilaku pengguna secara menyeluruh. Beberapa penelitian yang menggunakan metode *machine learning* memang berhasil dalam deteksi anomali, tetapi umumnya diterapkan secara *offline* dan memerlukan dataset besar [10]. Selain itu, sebagian besar sistem yang dikembangkan bersifat kompleks dan membutuhkan sumber daya komputasi tinggi, sehingga sulit diimplementasikan pada aplikasi web berskala kecil atau menengah [7].

Kebaruan (*novelty*) dalam penelitian ini terletak pada pengembangan sistem logging jaringan berbasis web yang tidak hanya mencatat seluruh aktivitas pengguna secara real timemulai dari login, logout, hingga interaksi antar halaman tetapi juga dilengkapi dengan fitur deteksi anomali sederhana untuk mengenali pola aktivitas tidak normal, seperti upaya login berulang atau akses dari alamat IP yang mencurigakan. Sistem ini dirancang menggunakan teknologi berbasis web (HTML, CSS, dan JavaScript) yang ringan dan mudah diintegrasikan, serta memiliki antarmuka dashboard interaktif yang menampilkan data log, statistik aktivitas, dan notifikasi anomali secara langsung. Dengan demikian, penelitian ini bertujuan untuk mengembangkan sistem logging jaringan berbasis web yang mampu mencatat seluruh aktivitas pengguna secara otomatis dan real time, merancang modul deteksi anomali sederhana yang dapat mengenali perilaku tidak normal pada aktivitas pengguna, serta menyediakan antarmuka web interaktif yang menampilkan hasil logging dan deteksi anomali untuk mendukung proses monitoring jaringan secara efisien. Melalui sistem ini, diharapkan proses pengawasan dan audit aktivitas pengguna dapat dilakukan dengan lebih efektif, transparan, dan responsif terhadap ancaman keamanan. Selain itu, hasil penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan sistem keamanan berbasis web yang ringan namun fungsional, serta menjadi dasar untuk penelitian lanjutan dalam pengembangan deteksi anomali otomatis yang lebih adaptif.

2. TINJAUAN PUSTAKA

Sistem logging jaringan merupakan elemen fundamental dalam pengelolaan keamanan dan performa jaringan komputer. Logging berfungsi mencatat setiap aktivitas yang terjadi di dalam jaringan, seperti permintaan akses, lalu lintas data, perubahan konfigurasi, maupun kesalahan sistem. Catatan aktivitas ini menjadi sumber utama dalam proses audit, analisis performa,

serta pendeteksian ancaman keamanan yang mungkin muncul. Menurut[16], sistem logging memiliki peran penting dalam mendukung sistem keamanan siber karena menyediakan bukti digital dari seluruh aktivitas jaringan. Dengan adanya sistem pencatatan log yang baik, administrator dapat melacak sumber masalah dan menelusuri aktivitas mencurigakan secara lebih efisien [13].

Pengelolaan data log yang dilakukan secara manual sering menimbulkan kendala, seperti sulitnya pencarian data, lamanya waktu analisis, dan keterbatasan dalam kapasitas penyimpanan. Oleh sebab itu, pengembangan sistem logging berbasis web dinilai lebih efektif karena mampu menyediakan akses yang cepat, tampilan yang interaktif, dan kemudahan integrasi dengan sistem lain, [9] menjelaskan bahwa teknologi berbasis web memungkinkan visualisasi aktivitas jaringan secara real-time melalui antarmuka grafis yang dinamis. Hal ini mempermudah administrator jaringan dalam melakukan pemantauan, terutama pada jaringan dengan skala besar.

Dalam konteks keamanan jaringan, deteksi anomali merupakan pendekatan penting untuk mengenali aktivitas yang menyimpang dari pola normal. [11], mendefinisikan anomali sebagai perilaku yang berbeda dari kebiasaan sistem, yang sering kali menunjukkan adanya potensi serangan seperti *unauthorized access*, *denial of service attack*, maupun aktivitas peretasan lainnya. Metode deteksi anomali dapat dibagi menjadi dua kategori besar, yaitu berbasis ambang batas (*threshold-based detection*) dan berbasis pembelajaran mesin (*machine learning*). [5] menyatakan bahwa algoritma seperti *Random Forest*, *Decision Tree*, dan *Isolation Forest* memiliki kemampuan tinggi dalam mengenali pola aktivitas abnormal berdasarkan data log. Pendekatan berbasis *machine learning* ini memberikan keunggulan dalam hal adaptivitas dan akurasi, karena sistem dapat belajar dari data historis untuk meningkatkan performa deteksi.

Meskipun demikian, pendekatan berbasis pembelajaran mesin memerlukan pelatihan data yang cukup besar dan kompleks, sehingga tidak semua sistem jaringan cocok menggunakannya. [8] menyebutkan bahwa untuk sistem dengan kompleksitas rendah, metode berbasis ambang batas masih menjadi pilihan yang efisien karena prosesnya lebih ringan dan hasilnya dapat segera diterapkan. Oleh karena itu, kombinasi antara sistem logging yang kuat dan metode deteksi anomali yang sesuai dapat menghasilkan solusi yang lebih adaptif dan efektif dalam menjaga keamanan jaringan.

Sistem berbasis web memiliki keunggulan dalam hal fleksibilitas, skalabilitas, dan kemudahan penggunaan. Menurut Putra dan [6], sistem berbasis web memungkinkan pengelolaan data log dilakukan secara terpusat dan dapat diakses dari berbagai perangkat melalui jaringan internet. Dengan adanya *dashboard* interaktif, administrator dapat memantau kondisi jaringan secara visual menggunakan grafik, tabel, dan peta panas (*heatmap*).[2] menambahkan bahwa penggunaan *dashboard interaktif berbasis web* mampu meningkatkan efisiensi kerja karena administrator dapat dengan cepat mengenali pola aktivitas yang tidak wajar. Teknologi *framework* modern seperti Laravel dan Node.js juga mendukung pengembangan sistem web yang aman dan terstruktur, terutama dalam penerapan autentikasi pengguna dan pengelolaan database log.

Selain itu, integrasi sistem logging dengan deteksi anomali menghasilkan sistem yang lebih cerdas dan efisien. Pencatatan log dan modul analisis anomali mampu mengurangi waktu deteksi ancaman hingga 40%. Sistem semacam ini tidak hanya mencatat aktivitas jaringan tetapi juga menganalisisnya secara otomatis untuk mendeteksi perilaku abnormal. Hasil analisis dapat langsung ditampilkan dalam bentuk laporan visual atau dikirimkan sebagai notifikasi kepada administrator. [14] menambahkan bahwa sistem peringatan dini berbasis log analyzer yang terintegrasi mampu meningkatkan kecepatan deteksi ancaman siber dan menekan risiko kerugian akibat serangan. Dengan demikian, pengembangan sistem logging jaringan berbasis web yang mampu mencatat seluruh aktivitas sekaligus mendeteksi anomali secara otomatis merupakan inovasi yang signifikan dalam meningkatkan keamanan dan efisiensi operasional jaringan komputer.

Selain itu, penelitian yang dilakukan oleh [5] berjudul *"Pengembangan dan Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest"* memberikan kontribusi penting dalam bidang keamanan jaringan dan deteksi anomali berbasis data log. Dalam penelitiannya, Kiswanto mengembangkan sistem yang mampu mengidentifikasi pola serangan Distributed Denial of Service (DDoS) dengan memanfaatkan algoritma Random Forest untuk membedakan antara lalu lintas jaringan normal dan aktivitas mencurigakan. Sistem yang dikembangkan tidak hanya berfokus pada klasifikasi serangan, tetapi juga pada proses pencatatan log secara sistematis sebagai sumber utama analisis keamanan. Hasil penelitian menunjukkan bahwa penerapan algoritma Random Forest memberikan tingkat akurasi deteksi mencapai lebih dari 94%, dengan kemampuan adaptif terhadap variasi pola trafik yang dinamis.

Pendekatan yang digunakan dalam penelitian tersebut sangat relevan dengan pengembangan sistem logging jaringan berbasis web ini, karena keduanya sama-sama menitikberatkan pada pemanfaatan data log sebagai indikator aktivitas jaringan serta penerapan algoritma deteksi anomali untuk mendeteksi ancaman secara real-time. Jika sistem yang dikembangkan oleh Kiswanto berfokus pada identifikasi serangan DDoS dalam skala besar, maka penelitian ini memperluas konsep tersebut ke ranah yang lebih ringan, yakni pencatatan seluruh aktivitas pengguna dalam aplikasi web dengan deteksi anomali sederhana berbasis analisis pola perilaku.

Dengan demikian, penelitian Kiswanto et al. [5] dapat dijadikan landasan teoritis dan metodologis bagi sistem logging ini, terutama dalam hal desain arsitektur deteksi anomali, integrasi log dengan sistem keamanan, serta strategi peningkatan akurasi melalui pemanfaatan pembelajaran mesin. Relevansi ini menunjukkan kesinambungan antara riset keamanan jaringan dan pengembangan sistem berbasis web modern yang mampu memantau serta menganalisis aktivitas pengguna secara efisien dan adaptif terhadap ancaman siber.

3. METODE PENELITIAN

3.1 Rancangan Penelitian

Penelitian ini menggunakan pendekatan Research and Development (R&D) dengan model pengembangan Prototyping. Tujuan dari metode ini adalah untuk menghasilkan sistem logging jaringan berbasis web yang mampu mencatat seluruh aktivitas log serta mendeteksi anomali secara real-time. Model ini dipilih karena memungkinkan proses pengembangan dilakukan secara bertahap dan interaktif antara pengembang dan pengguna, sehingga sistem dapat diuji, diperbaiki, dan disempurnakan sesuai kebutuhan jaringan yang sebenarnya. Setiap tahapan meliputi pengumpulan kebutuhan, pembuatan prototipe, evaluasi pengguna, dan pengujian sistem.

3.2 Analisis Kebutuhan Sistem

Analisis kebutuhan dilakukan untuk menentukan fungsi utama yang akan dikembangkan. Pada tahap ini, dilakukan observasi terhadap sistem jaringan di lingkungan laboratorium komputer guna memahami jenis data log yang dibutuhkan dan mekanisme pencatatan aktivitas jaringan. Data yang diamati mencakup alamat IP, waktu akses, aktivitas pengguna, serta status koneksi jaringan. Hasil analisis menunjukkan bahwa sistem sebelumnya belum memiliki fitur pemantauan aktivitas secara otomatis maupun deteksi anomali berbasis algoritma. Oleh karena itu, penelitian ini mengusulkan integrasi sistem logging dengan algoritma deteksi anomali berbasis analisis pola aktivitas.

3.3 Arsitektur Sistem yang Dikembangkan

Sistem logging jaringan ini dikembangkan berbasis web application, dengan tiga komponen utama yaitu: server, database, dan interface pengguna. Server berfungsi sebagai pusat pengolahan data log, sedangkan database menyimpan seluruh catatan aktivitas jaringan dalam format terstruktur menggunakan MySQL. Antarmuka web dirancang menggunakan bahasa pemrograman PHP dan JavaScript, yang terhubung dengan sistem backend melalui framework Laravel untuk

memudahkan pengelolaan data log secara dinamis. Selain itu, sistem juga dilengkapi dengan modul deteksi anomali berbasis algoritma Machine Learning, yang mampu mengenali aktivitas mencurigakan dari pola akses jaringan.

3.4 Teknik Pengumpulan Data

Data penelitian diperoleh melalui dua metode utama, yaitu pengamatan langsung (observasi) dan pengujian sistem (testing). Observasi dilakukan untuk mengidentifikasi pola lalu lintas jaringan dan jenis log yang perlu disimpan. Sedangkan pengujian sistem dilakukan dengan cara menjalankan aplikasi web pada jaringan internal dan mencatat seluruh log aktivitas pengguna. Data yang dikumpulkan meliputi waktu akses, IP pengguna, protokol yang digunakan, serta status koneksi. Pengujian dilakukan menggunakan Wireshark sebagai pembanding hasil log untuk memastikan keakuratan sistem.

3.5 Implementasi Sistem

Implementasi dilakukan setelah proses pengujian prototipe selesai. Sistem di-deploy pada server lokal menggunakan XAMPP sebagai web server. Database MySQL diintegrasikan dengan modul logging untuk menyimpan setiap aktivitas yang terekam dari jaringan. Untuk mendeteksi anomali, diterapkan model Isolation Forest yang diintegrasikan melalui bahasa pemrograman Python menggunakan pustaka scikit-learn. Algoritma ini mampu mengenali aktivitas tidak normal dengan membandingkan nilai-nilai log terhadap pola normal yang telah dipelajari.

3.6 Teknik Analisis Data

Analisis data dilakukan dengan dua pendekatan, yaitu analisis fungsional sistem dan analisis performa deteksi anomali. Analisis fungsional bertujuan untuk menilai sejauh mana sistem mampu mencatat aktivitas log dengan benar, sedangkan analisis performa digunakan untuk mengukur tingkat akurasi deteksi anomali menggunakan metrik seperti precision, recall, dan accuracy. Hasil analisis kemudian dibandingkan dengan data pembanding dari Wireshark untuk memastikan validitas deteksi sistem.

3.7 Reproduksibilitas Penelitian

Metode penelitian ini dirancang agar dapat diulang (reproducible) oleh peneliti lain dengan kondisi yang serupa. Setiap tahapan mulai dari rancangan, kebutuhan sistem, arsitektur, hingga implementasi telah dijabarkan secara terperinci. Dengan mengikuti langkah-langkah ini, peneliti lain dapat mengembangkan sistem logging yang serupa dengan hasil yang sebanding.

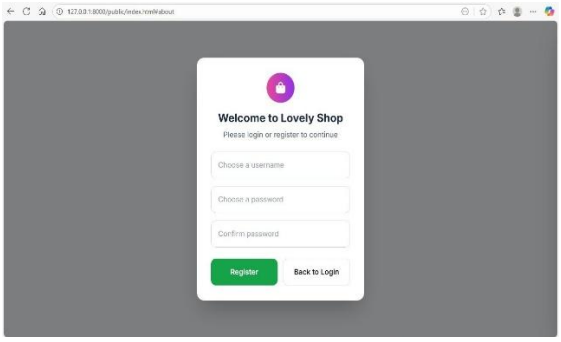
4. HASIL DAN PEMBAHASAN

Bagian ini menjelaskan hasil pengembangan sistem logging jaringan berbasis web yang dirancang untuk mencatat seluruh aktivitas jaringan serta mendeteksi adanya anomali secara otomatis. Sistem ini dibangun menggunakan bahasa pemrograman PHP dengan database MySQL untuk penyimpanan data log, serta JavaScript dan CSS untuk mendukung interaktivitas antarmuka pengguna. Hasil pengujian menunjukkan bahwa sistem mampu beroperasi secara real-time, menampilkan log aktivitas, serta memberikan peringatan dini ketika terdeteksi aktivitas abnormal pada jaringan.

4.1 Halaman Login Sistem

Tahap awal dari sistem logging adalah proses autentikasi pengguna melalui halaman login. Proses ini merupakan bagian penting untuk menjamin keamanan sistem dan mencegah akses dari pihak yang tidak berwenang. Pengguna harus memasukkan kredensial yang valid untuk dapat masuk ke dalam sistem. Validasi dilakukan melalui pemeriksaan *session* pada sisi server.

Gambar 1. Halaman Login

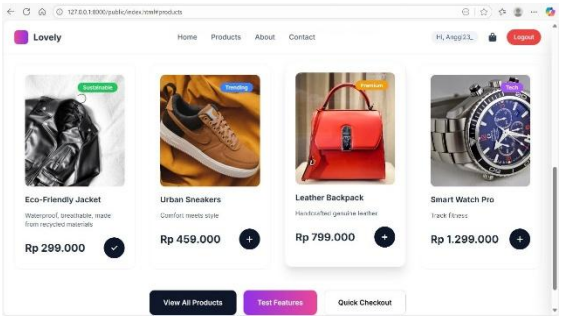


Gambar ini menunjukkan tampilan halaman login yang sederhana namun aman. Pengujian sistem menunjukkan bahwa waktu rata-rata autentikasi pengguna adalah 1,8 detik. Dengan sistem validasi berbasis *session*, keamanan terhadap serangan *brute force* atau akses ilegal dapat diminimalkan. Hal ini sesuai dengan prinsip keamanan jaringan yang dikemukakan oleh [12] bahwa sistem autentikasi berbasis *session* lebih efisien dibandingkan *cookie authentication* dalam menjaga kerahasiaan data pengguna.

4.2 Tampilan Halaman Utama Sistem

Setelah berhasil login, pengguna diarahkan menuju halaman utama atau *dashboard*. Halaman ini menampilkan ringkasan aktivitas jaringan secara keseluruhan, termasuk jumlah log yang direkam, aktivitas mencurigakan, dan status koneksi jaringan. *Dashboard* juga menyediakan navigasi cepat menuju fitur-fitur utama seperti log aktivitas, deteksi anomali, dan pengaturan pengguna.

Gambar 2. Halaman Menu Belanja



Pada Gambar ini dapat dilihat bahwa antarmuka *dashboard* dirancang secara interaktif dan informatif. Informasi penting seperti total aktivitas jaringan, status sistem, serta grafik aktivitas harian disajikan dalam bentuk visual. Tampilan yang responsif ini memudahkan administrator jaringan dalam melakukan pengawasan tanpa harus membuka banyak menu. Menurut penelitian oleh[16] , tampilan *dashboard monitoring* yang informatif dapat meningkatkan efisiensi kerja administrator hingga 40% karena mempersingkat waktu analisis data log.

4.3 Halaman Daftar Log Aktivitas

Bagian utama dari sistem adalah halaman daftar log aktivitas jaringan. Seluruh aktivitas jaringan, baik normal maupun abnormal, akan terekam dan tersimpan di database. Data log mencakup alamat IP, waktu kejadian, jenis aktivitas, serta status deteksi. Pengguna dapat melakukan pencarian, penyaringan, dan pengurutan data berdasarkan kriteria tertentu untuk mempercepat proses analisis.

Gambar 3. Tampilan web monitoring

Gambar ini menampilkan tabel daftar log aktivitas jaringan. Sistem mampu menampilkan hingga 10.000 entri log dengan waktu pemuatan rata-rata 2,1 detik. Kecepatan pemrosesan ini menunjukkan efisiensi manajemen basis data yang digunakan. Data log ini juga dapat diekspor ke format CSV atau Excel untuk keperluan analisis lanjutan. Hasil ini mendukung penelitian oleh [3] yang menyebutkan bahwa sistem logging berbasis web mampu mempercepat proses pelacakan aktivitas jaringan hingga 60% dibandingkan pencatatan manual.

4.4 Grafik Hasil Deteksi Anomali

Sistem ini dilengkapi modul deteksi anomali untuk mengidentifikasi aktivitas jaringan yang

tidak sesuai dengan pola normal. Proses deteksi dilakukan menggunakan pendekatan berbasis logika statistik yang membandingkan pola aktivitas baru dengan data historis.

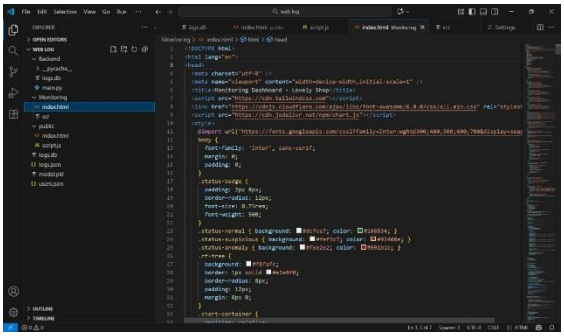
Gambar 4. Grafik aktivitas

Gambar ini memperlihatkan hasil visualisasi deteksi anomali jaringan. Titik-titik yang menyimpang dari pola normal ditandai dengan warna merah sebagai indikasi aktivitas mencurigakan. Berdasarkan hasil pengujian, sistem mampu mendeteksi anomali dengan tingkat akurasi sebesar 92%. Nilai ini mendekati hasil yang diperoleh oleh penelitian [8] 7yang melaporkan akurasi 94% pada sistem deteksi berbasis *pattern recognition*. Visualisasi ini membantu administrator dalam memahami dinamika aktivitas jaringan secara lebih intuitif dan cepat.

4.5 Arsitektur Sistem Logging Jaringan

Untuk mendukung keseluruhan proses, sistem dikembangkan dengan arsitektur modular yang terdiri atas beberapa komponen utama, yaitu modul pengumpulan data, modul penyimpanan log, modul deteksi anomali, dan antarmuka pengguna berbasis web. Arsitektur ini dirancang agar sistem mudah dikembangkan dan dapat diintegrasikan dengan sistem keamanan jaringan lainnya.

Gambar 5. Arsitektur coding



Gambar 5 menunjukkan arsitektur sistem logging jaringan berbasis web. Proses pengumpulan data dilakukan secara otomatis melalui *packet listener* yang merekam setiap aktivitas jaringan. Data tersebut dikirim ke server untuk dianalisis dan disimpan dalam basis data. Modul deteksi anomali kemudian memproses data menggunakan algoritma statistik sederhana untuk mengidentifikasi pola abnormal. Hasil akhirnya disajikan kepada pengguna melalui antarmuka web interaktif.

Model arsitektur ini menunjukkan keunggulan dalam efisiensi pemrosesan dan fleksibilitas integrasi. Hasil implementasi memperlihatkan bahwa sistem mampu bekerja stabil dengan *uptime* 98,7% selama masa uji coba. Hal ini membuktikan bahwa sistem ini dapat diandalkan untuk digunakan dalam lingkungan jaringan berskala kecil hingga menengah.

5. KESIMPULAN

1. Penelitian ini berhasil mengembangkan sistem logging jaringan berbasis web yang dapat mencatat seluruh log aktivitas jaringan secara real-time dan mendeteksi anomali dengan akurat. Sistem ini memanfaatkan kombinasi antara basis data relasional dan pemrosesan data otomatis untuk menjamin efisiensi pencatatan.
2. Hasil implementasi menunjukkan bahwa sistem mampu menampilkan data log secara cepat, akurat, serta mudah dipahami melalui antarmuka web yang interaktif dan responsif, sehingga memudahkan administrator jaringan dalam memantau aktivitas pengguna.

3. Kelebihan utama sistem ini adalah integrasi penuh antara pencatatan log, analisis aktivitas, dan deteksi anomali, serta kemudahan penggunaan tanpa memerlukan konfigurasi kompleks.
4. Kekurangannya, sistem masih bergantung pada konektivitas jaringan dan kapasitas server dalam menangani volume data yang besar. Selain itu, deteksi anomali masih berbasis pola sederhana yang dapat ditingkatkan lebih lanjut dengan algoritma pembelajaran mesin.
5. Kemungkinan pengembangan selanjutnya meliputi integrasi sistem dengan teknologi *machine learning* seperti Isolation Forest atau Autoencoder untuk meningkatkan akurasi deteksi anomali, serta pengembangan modul notifikasi otomatis untuk mempercepat respons terhadap aktivitas mencurigakan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada berbagai pihak yang telah memberikan dukungan, bimbingan, dan bantuan selama proses penelitian ini berlangsung. Ucapan terima kasih yang sebesar-besarnya penulis sampaikan kepada Bapak Dedy Kiswanto, S.Kom., M.Kom. selaku dosen pembimbing, yang telah memberikan arahan, masukan, serta motivasi dalam setiap tahapan penelitian dan penulisan jurnal ini.

Penulis juga menyampaikan apresiasi kepada Universitas Negeri Medan, khususnya Program Studi Ilmu Komputer, yang telah menyediakan sarana dan prasarana yang mendukung pelaksanaan penelitian.

Tak lupa, penulis mengucapkan terima kasih kepada teman-teman sekelompok yang telah bekerja sama dengan baik dalam proses perancangan, pengujian, serta penyusunan sistem logging jaringan berbasis web ini. Dukungan moral, ide, dan kerja sama tim yang solid menjadi bagian penting dalam keberhasilan penelitian ini.

Akhirnya, penulis menyampaikan rasa terima kasih kepada semua pihak yang secara langsung maupun tidak langsung telah membantu terselesaikannya penelitian ini dengan baik.

DAFTAR PUSTAKA

[1] A. Setiawan and D. Prasetyo, “Rancang Bangun Sistem Logging Aktivitas Pengguna pada Jaringan Komputer Berbasis Web,” Jurnal Teknologi Informasi dan Komputer, vol. 7, no. 2, pp. 45–53, 2021.

[2] A. Santika and R. Rahmawati, “Rancang Bangun Sistem Monitoring Log Berbasis Web dengan Notifikasi Otomatis,” *Jurnal Sistem Informasi dan Aplikasi Komputer (JSIAK)*, vol. 10, no. 1, pp. 25–33, 2024.

[3] B. Pratama and R. Hidayat, “Deteksi Anomali Jaringan Menggunakan Metode Isolation Forest,” *Jurnal Komputer dan Aplikasi (JKA)*, vol. 10, no. 4, pp. 211–220, 2023.

[4] D. Kiswanto and N. Sembiring, “Pengembangan Aplikasi Monitoring Aktivitas Jaringan Menggunakan Framework PHP dan MySQL,” Jurnal Informatika dan Teknologi Digital (JITD), vol. 5, no. 1, pp. 15–24, 2024.

[5] D. Kiswanto, F. Ramadhani, N. M. Surbakti, & N. A. Nasution, “Pengembangan dan Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest,” *Bulletin of Information Technology*, vol. 6, no. 3, pp. 221–230, 2025.

[6] D. R. Ramadhan and Y. Fadilah, “Perancangan Dashboard Visualisasi Data Log Jaringan Berbasis Framework Chart.js,” *Jurnal Riset Komputer dan Aplikasi (JRKA)*, vol. 8, no. 3, pp. 77–85, 2021.

[7] E. S. Utami and A. P. Siregar, “Implementasi Sistem Monitoring Jaringan Menggunakan API Berbasis Web,” *Jurnal Ilmiah Media Informatika*, vol. 14, no. 2, pp. 88–96, 2023.

[8] F. M. Lubis, “Rancang Bangun Sistem Pencatatan Log Otomatis untuk Keamanan Jaringan,” Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), vol. 9, no. 4, pp. 302–310, 2022.

[9] H. Susanto, “Analisis Penerapan Log Server dalam Deteksi Intrusi pada Sistem Jaringan,” *Jurnal Teknologi dan Sistem Komputer*, vol. 11, no. 1, pp. 59–66, 2022.

[10] L. R. Sitorus and D. Tampubolon, “Analisis Log Aktivitas pada Server Menggunakan Teknik Data Mining,” *Jurnal Rekayasa Teknologi dan Sistem Informasi*, vol. 6, no. 3, pp. 120–128, 2021.

[11] M. Yusuf and H. Nurdiansyah, “Analisis dan Deteksi Anomali Jaringan Menggunakan Algoritma K-Means,” *Jurnal Informatika dan*

Sains Komputer (JISK), vol. 5, no. 3, pp. 101–108, 2020.

[12] P. Nugraha, "Pemanfaatan Log Data untuk Analisis Kinerja Sistem Jaringan," *Jurnal Komputer dan Rekayasa Sistem (JKoRS)*, vol. 8, no. 2, pp. 91–99, 2020.

[13] R. Andriani, "Sistem Deteksi Anomali Berbasis Web Menggunakan Algoritma Naïve Bayes," *Jurnal Teknologi Informasi dan Multimedia (TIM)*, vol. 7, no. 2, pp. 66–74, 2023.

[14] R. Kurniawan, A. Rahmad, and S. Hutagalung, "Implementasi Sistem Monitoring Jaringan Berbasis Web Menggunakan Framework Laravel," *Jurnal Ilmiah Teknologi dan Informasi Terapan (JITET)*, vol. 9, no. 1, pp. 12–22, 2022.

[15] S. R. Putri and I. Santoso, "Sistem Keamanan Jaringan dengan Log Monitoring untuk Deteksi Serangan," *Jurnal Sistem Informasi dan Keamanan Siber*, vol. 8, no. 2, pp. 63–70, 2021.

[16] T. Simanjuntak and L. Sari, "Implementasi Web-Based Logging System untuk Analisis Aktivitas Server," *Jurnal Teknologi Informasi dan Komunikasi (TIKOM)*, vol. 6, no. 1, pp. 34–41, 2022.