Original Article

e-XXXX-XXXX

Original Article

Implementasi Monitoring Log Sistem Untuk Deteksi Aktivitas Mencurigakan Menggunakan Elk Stack

Anggun Lestari[1], Saharuddin✉[2], Rakhmadi Rahman[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: saharuddins116@gmail.com

Abstrak:

Transformasi digital yang masif di sektor pemerintahan dan pendidikan membawa konsekuensi serius berupa lonjakan risiko keamanan siber yang kian persisten. Celah keamanan seperti serangan brute force, akses tanpa otorisasi, hingga anomali lalu lintas jaringan sering kali luput dari pengamatan administrator akibat pengelolaan catatan aktivitas (log) yang masih bersifat konvensional, terfragmentasi, dan pasif. Studi ini bertujuan untuk merancang dan membangun sebuah mekanisme pengawasan keamanan terpusat yang mampu mengidentifikasi perilaku mencurigakan secara real-time. Dengan mengadopsi metodologi pengembangan Agile, penelitian ini mengintegrasikan arsitektur open source yang tangguh berbasis ELK Stack (Elasticsearch, Logstash, Kibana) dan protokol Syslog di lingkungan sistem operasi Linux. Temuan empiris dari penelitian ini memperlihatkan bahwa infrastruktur yang dibangun berhasil mengagregasi, menormalisasi, dan memvisualisasikan data log dari berbagai sumber secara komprehensif. Sistem terbukti responsif dalam memetakan pola serangan spesifik, seperti kegagalan otentikasi berulang dan akses di luar jam operasional, serta menyajikan visualisasi data interaktif yang krusial bagi administrator dalam pengambilan keputusan mitigasi cepat maupun penelusuran bukti forensik digital pasca-insiden.

Keywords: Deteksi Intruksi, ELK Stack, Forensik Digital, Keamanan Sistem, Monitoring Log

Pendahuluan

Percepatan adopsi teknologi informasi pada berbagai infrastruktur strategis, seperti sektor perbankan, pemerintahan, dan institusi pendidikan, telah membawa peningkatan efisiensi dan efektivitas operasional. Namun, di balik manfaat tersebut, tingkat paparan terhadap ancaman siber juga semakin meningkat dan berkembang menjadi lebih kompleks. Berbagai bentuk serangan, mulai dari eksploitasi kesalahan

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026

konfigurasi sederhana hingga intrusi terorganisir berskala besar, menuntut sistem keamanan yang tidak hanya kuat tetapi juga adaptif. Dalam konteks keamanan siber modern, tantangan utama yang dihadapi oleh administrator sistem bukan lagi sekadar penerapan mekanisme perlindungan seperti firewall, melainkan keterbatasan visibilitas terhadap aktivitas yang terjadi pada server dan infrastruktur jaringan secara real-time.

Dalam keamanan informasi, log sistem berperan sebagai catatan digital yang merekam seluruh aktivitas dan peristiwa penting pada sistem. Chuvakin, Schmidt, dan Phillips (2013) menegaskan bahwa manajemen log merupakan komponen fundamental dalam memahami perilaku sistem secara menyeluruh. Tanpa pengelolaan log yang baik, organisasi berisiko kehilangan kemampuan untuk memantau kondisi sistem secara akurat. Pada praktiknya, data log sering kali hanya disimpan sebagai arsip pasif dan baru dimanfaatkan ketika terjadi insiden besar atau kegagalan sistem. Penelitian oleh Widodo dan Nugroho (2020) menunjukkan bahwa kondisi tersebut menyebabkan proses analisis keamanan menjadi bersifat reaktif dan kurang efektif dalam pencegahan dini. Ketiadaan mekanisme pemantauan log yang proaktif juga berdampak signifikan terhadap kemampuan organisasi dalam melakukan respons insiden. Dalam situasi serangan siber, kecepatan deteksi menjadi faktor penentu dalam meminimalkan dampak kerusakan. Keterlambatan dalam mengidentifikasi aktivitas mencurigakan dapat menyebabkan kebocoran data sensitif, gangguan layanan, hingga kerugian institusional yang lebih besar. Casey (2011) menjelaskan bahwa efektivitas analisis forensik digital sangat bergantung pada ketersediaan data log yang lengkap, terjaga integritasnya, dan mudah diakses untuk merekonstruksi kronologi kejadian secara akurat.

Berdasarkan urgensi tersebut, diperlukan sebuah sistem yang tidak hanya berfungsi untuk mencatat aktivitas sistem, tetapi juga mampu melakukan pemantauan dan analisis secara terpusat dan berkelanjutan. Penelitian ini bertujuan untuk mengimplementasikan sistem monitoring log terpusat di Institut Teknologi Bacharuddin Jusuf Habibie sebagai upaya meningkatkan visibilitas keamanan sistem secara real-time. Melalui sistem ini, setiap anomali atau aktivitas tidak wajar diharapkan dapat terdeteksi lebih dini, sehingga potensi gangguan dan kerusakan sistem dapat dicegah sebelum berkembang menjadi insiden keamanan yang lebih serius.

Metode Penelitian

Kerangka Kerja Pengembangan Agile

Penelitian ini mengadopsi kerangka kerja Agile sebagai pendekatan pengembangan sistem. Agile dipilih karena mampu memberikan fleksibilitas dan adaptabilitas tinggi melalui siklus pengembangan yang bersifat iteratif dan berkelanjutan. Pendekatan ini relevan dengan karakteristik ancaman siber yang dinamis dan terus berkembang, sehingga sistem keamanan yang dibangun harus mampu menyesuaikan diri dengan perubahan tersebut. Alur kerja penelitian dibagi ke dalam beberapa fase utama.

1. Tahap pertama adalah analisis kebutuhan

   Bertujuan untuk mengidentifikasi jenis log krusial sebagai sumber data utama, meliputi log otentikasi (auth.log), log sistem (syslog), serta log aplikasi tertentu. Pada tahap ini juga ditentukan parameter anomali keamanan, seperti ambang batas jumlah kegagalan login dalam satuan waktu tertentu.

2. Perancangan arsitektur sistem

   Difokuskan pada desain topologi pengumpulan data log secara terpusat (centralized logging). Perancangan ini dilakukan untuk meminimalkan beban jaringan

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026

sekaligus memastikan efisiensi pengiriman data. Selain itu, dirancang pula skema pengindeksan data agar proses pencarian dan analisis log dapat dilakukan dengan latensi yang rendah.

3. eksekusi teknis dan konfigurasi

meliputi proses instalasi serta orkestrasi antar-komponen sistem monitoring berbasis ELK Stack pada lingkungan server Linux. Selanjutnya, tahap simulasi dan validasi keamanan dilakukan melalui pengujian terbatas atau simulasi serangan untuk menguji kemampuan sistem dalam mendeteksi aktivitas mencurigakan secara responsif.

4. evaluasi kinerja dan iterasi

yang bertujuan untuk mengukur tingkat akurasi deteksi, kecepatan pemrosesan data, serta kemudahan penggunaan dashboard. Hasil evaluasi ini digunakan sebagai dasar perbaikan dan pengembangan sistem pada siklus berikutnya sesuai prinsip Agile.

Hasil dan Pembahasan

Implementasi Mekanisme Agregasi Log

Tahap implementasi dimulai dengan konfigurasi forwarding Syslog pada server target untuk mengirimkan log otentikasi secara real-time ke server monitoring. Salah satu tantangan utama dalam proses ini adalah karakteristik log mentah yang bersifat tidak terstruktur dan bervariasi antar aplikasi. Untuk mengatasi permasalahan tersebut, pipeline Logstash dikonfigurasikan menggunakan filter grok, yang berfungsi untuk memecah baris log kompleks menjadi beberapa field terstruktur, seperti waktu kejadian (timestamp), alamat IP sumber, akun pengguna, nama proses, dan status peristiwa. Proses normalisasi ini sangat penting karena analisis keamanan berbasis log memerlukan data yang terstruktur agar dapat diproses secara otomatis dan akurat, sebagaimana dijelaskan oleh Owusu et al. (2019).

visabilitas Sistem Melalui Dashboard Interaktif

Hasil pemrosesan log divisualisasikan melalui antarmuka Kibana yang dirancang secara ergonomis untuk memberikan gambaran kondisi sistem secara menyeluruh. Dashboard yang dikembangkan tidak hanya menampilkan data statistik, tetapi juga memberikan kesadaran situasional (situational awareness) bagi administrator sistem. Visualisasi yang disajikan meliputi grafik aktivitas log berdasarkan waktu untuk mendeteksi lonjakan trafik, perbandingan antara login berhasil dan gagal, peta sebaran geografis alamat IP pengakses, serta tabel rincian insiden dengan tingkat prioritas tertentu. Dengan pendekatan ini, administrator tidak perlu lagi membaca ribuan baris log secara manual, melainkan dapat mengenali pola anomali secara cepat melalui tampilan visual.

Analisis Studi Kasus: Deteksi Serangan Brute Force

Pengujian fungsional dilakukan melalui simulasi serangan Brute Force terhadap layanan SSH. Hasil pengujian menunjukkan bahwa sistem monitoring mampu mendeteksi anomali berupa percobaan login gagal yang terjadi secara berulang dalam waktu singkat.

Dashboard Kibana menampilkan lonjakan signifikan pada kategori kegagalan login, sementara Logstash berhasil mengidentifikasi bahwa percobaan tersebut berasal dari satu alamat IP yang sama dengan target akun administratif. Deteksi dini ini memungkinkan administrator melakukan tindakan mitigasi, seperti pemblokiran alamat IP penyerang, sebelum terjadi kompromi sistem. Temuan ini menunjukkan

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026

efektivitas sistem dalam mendukung konsep pertahanan aktif (active defense).

Analisis Anomali Akses dan Implikasi Forensik

Studi kasus berikutnya difokuskan pada deteksi anomali berdasarkan waktu akses. Sistem dikonfigurasikan untuk memberikan penanda khusus terhadap aktivitas login yang terjadi di luar jam operasional normal. Pada pengujian, akses yang terjadi pada dini hari berhasil terdeteksi dan ditampilkan secara mencolok pada dashboard. Anomali semacam ini dapat mengindikasikan adanya akun yang telah dikompromikan atau potensi ancaman dari dalam (insider threat). Kemampuan sistem dalam mendeteksi pola perilaku yang tidak wajar sejalan dengan rekomendasi NIST yang menekankan pentingnya konteks waktu dan perilaku dalam sistem deteksi intrusi.

Selain untuk deteksi dini, arsitektur sistem ini juga mendukung kebutuhan forensik digital pasca-insiden. Penyimpanan log pada Elasticsearch yang bersifat append-only menjaga integritas data dan meminimalkan risiko manipulasi. Hal ini menjadikan data log sebagai bukti digital yang valid dan dapat dipertanggungjawabkan, sesuai dengan standar penanganan insiden keamanan dan prinsip keamanan siber yang baik.

Kesimpulan

Berdasarkan serangkaian perancangan, implementasi, dan pengujian yang telah dilakukan, penelitian ini menyimpulkan bahwa penerapan ELK Stack sebagai solusi monitoring log sistem di Institut Teknologi Bacharuddin Jusuf Habibie memberikan dampak signifikan terhadap peningkatan postur keamanan informasi. Sistem ini berhasil mengonsolidasikan proses pengawasan log yang sebelumnya terfragmentasi menjadi satu pintu visual yang komprehensif. Hasil pengujian empiris menegaskan kemampuan sistem dalam memberikan peringatan dini terhadap aktivitas mencurigakan—seperti serangan brute force dan akses ilegal—sekaligus menyediakan arsip data yang reliabel untuk keperluan audit kepatuhan dan forensik digital.

Saran

Meskipun sistem monitoring yang dikembangkan telah menunjukkan kinerja yang efektif, masih terdapat peluang untuk pengembangan lebih lanjut. Penelitian selanjutnya disarankan untuk mengintegrasikan sistem dengan algoritma Machine Learning atau Artificial Intelligence guna meningkatkan kemampuan deteksi ancaman, khususnya terhadap serangan yang belum memiliki pola serangan yang dikenal (zero-day threats), sekaligus mengurangi tingkat false positive. Selain itu, penambahan mekanisme notifikasi otomatis melalui surat elektronik (email) maupun aplikasi pesan instan seperti Telegram atau WhatsApp dinilai penting untuk membantu administrator merespons insiden keamanan secara lebih cepat tanpa harus melakukan pemantauan

Daftar Pustaka

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

Chuvakin, A., Schmidt, K., & Phillips, C. (2013). Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngress.

Elastic. (2023). Elasticsearch Reference Guide. Elastic Documentation.

Elastic. (2023). Kibana User Guide. Elastic Documentation.

Elastic. (2023). Logstash Reference Guide. Elastic Documentation.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026

Techniques into Incident Response. NIST Special Publication 800-86.
Owusu, E., et al. (2019). "Log-Based Intrusion Detection Systems: A Review." International Journal of Computer Applications, 178(7), 1-7.
Scarfone, K., & Mell, P. (2012). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94.
Stallings, W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley.
Widodo, A., & Nugroho, Y. (2020). "Analisis Keamanan Sistem Informasi Menggunakan Monitoring Log." Jurnal Teknologi Informasi, 14(2), 45-54.

Received: November 15, 2025 – Revised: November 24, 2025 - Accepted: Desember 17, 2025 - Published online: January 10, 2026