Jurnal Ilmu Komputer dan Teknologi Informasi
https://journal.stmiki.ac.id

E-ISSN: 3047-6674 | P-ISSN: 3047-6682
Vol. 2 No. 1 (2025) | Maret

OPEN ACCESS

https://doi.org/10.35870/jikti.v2i1.1341

Perancangan dan Pengembangan Aplikasi Deteksi Anomali pada Jaringan Internet Gedung Disaster Recovery Center Badan Diklat Kejaksaan RI dengan Implementasi Sistem Manajemen Informasi dan Keamanan (SIEM) Berbasis Web

Issenoro [1*], Herlina Trisnawati [2], Sakius Octavianus Tarigan [3] Novianti Madhona Faizah [4] Veranita [5]

[1*,2,3,4,5] Program Studi Sistem Informasi, Universitas Tama Jagakarsa, Kota Jakarta Selatan, Daerah Khusus Ibu kota Jakarta, Indonesia.

Corresponding Email: issenoro@gmail.com [1*] herlina@jagakarsa.ac.id [2] sakiustarigan@jagakarsa.ac.id [3] novianti@jagakarsa.ac.id [4] veranita@jagakarsa.ac.id [5]

Histori Artikel:
Dikirim 06 Februari 2025; *Diterima dalam bentuk revisi* 21 Februari 2025; *Diterima* 20 Maret 2025; *Diterbitkan* 29 Maret 2025.

Abstrak

Penelitian ini mengembangkan aplikasi deteksi anomali pada jaringan internet Gedung Disaster Recovery Center (DRC) Badan Diklat Kejaksaan RI dengan implementasi Security Information and Event Management (SIEM) menggunakan bahasa pemrograman Python. Aplikasi yang dihasilkan bertujuan untuk membantu admin jaringan di Gedung DRC dalam memantau alur komunikasi jaringan serta mendeteksi potensi ancaman terhadap sistem. Pendekatan yang digunakan mencakup pembuatan aplikasi yang meningkatkan keamanan jaringan melalui deteksi anomali dan perangkat monitoring untuk melindungi jaringan. Teknologi SIEM diterapkan untuk mengumpulkan dan menganalisis data log yang berasal dari jaringan, aplikasi, dan perangkat keras. Teknologi ini memungkinkan pengumpulan data log dalam jumlah besar serta menganalisis peristiwa yang terjadi dari berbagai sumber. Dengan penerapan sistem ini, DRC Kejaksaan RI diharapkan memiliki kemampuan untuk memantau lalu lintas jaringan internet dan perangkat keamanan yang diterapkan, serta mengevaluasi efektivitas SIEM dalam melindungi aset informasi. Fokus penelitian ini terletak pada peningkatan keamanan jaringan, pengumpulan log dan event lalu lintas jaringan, serta pengembangan aplikasi dashboard untuk menampilkan hasil monitoring. Sistem ini bertujuan mendeteksi anomali yang berbahaya dan memberikan informasi terkini terkait kondisi jaringan internet, sehingga memudahkan admin jaringan dalam melakukan monitoring dan melaporkan hasilnya kepada pimpinan.

Kata Kunci: Jaringan Internet, SIEM, Aplikasi, Python.

Abstract

This research develops an anomaly detection application for the internet network of the Disaster Recovery Center (DRC) building at the Training Agency of the Indonesian Prosecutor's Office (Badan Diklat Kejaksaan RI), implemented with Security Information and Event Management (SIEM) using the Python programming language. The resulting application aims to assist network administrators at the DRC in monitoring network communication flows and detecting potential threats to the system. The approach involves developing an application that enhances network security through anomaly detection and monitoring devices to protect the network. SIEM technology is used to collect and analyze log data from the network, applications, and hardware. This technology allows for the large-scale collection of log data and the analysis of events from multiple sources. With the implementation of this system, the DRC Kejaksaan RI is expected to gain the ability to monitor internet network traffic and the security devices applied, as well as evaluate the effectiveness of SIEM in protecting information assets. The focus of this research is on improving network security, collecting logs and events related to network traffic, and developing a dashboard application to display monitoring results. The system aims to detect harmful anomalies and provide up-to-date information regarding network conditions, thus facilitating network administrators in performing monitoring tasks and reporting findings to leadership.

Keyword: Internet Network, SIEM, Application, Python.

Jurnal Ilmu Komputer dan Teknologi Informasi
https://journal.stmiki.ac.id
E-ISSN: 3047-6674 | P-ISSN: 3047-6682
Vol. 2 No. 1 (2025) | Maret
OPEN ACCESS
https://doi.org/10.35870/jikti.v2i1.1341

1. Pendahuluan

Perancangan dan pengembangan aplikasi deteksi anomali pada jaringan internet, khususnya di Disaster Recovery Center Badan Diklat Kejaksaan RI, membutuhkan pendekatan yang menyeluruh dalam manajemen informasi dan keamanan. Salah satu metode yang efektif untuk diterapkan dalam sistem ini adalah algoritma K-Means, yang digunakan untuk pengelompokan data. Metode ini telah terbukti efektif dalam berbagai aplikasi deteksi anomali karena kemampuannya untuk mengidentifikasi pola abnormal dalam data. Sebagai contoh, penelitian oleh Aini *et al.* (2018) menunjukkan bahwa K-Means dapat digunakan untuk mendeteksi anomali dalam lalu lintas jaringan, dengan cara mengelompokkan data yang normal dan mencurigakan. Ketika terdapat gangguan atau pola yang tidak biasa, sistem dapat segera memberikan notifikasi kepada administrator untuk mengambil langkah-langkah mitigasi yang diperlukan. Selain itu, Ridho dan Kusuma (2019) juga menekankan pentingnya penerapan K-Means dalam analisis log akses untuk mendeteksi intrusi pada jaringan. Dengan menggunakan metode ini, sistem dapat secara otomatis mengelompokkan dan menganalisis data log yang terkumpul, sehingga lebih cepat dalam mengidentifikasi aktivitas yang mencurigakan. Penerapan K-Means dalam sistem deteksi anomali ini tidak hanya meningkatkan kemampuan deteksi tetapi juga mempermudah pengawasan terhadap lalu lintas jaringan, sehingga memberikan perlindungan yang lebih efektif terhadap potensi ancaman.

Dalam hal keamanan jaringan, Intrusion Detection System (IDS) memegang peranan yang sangat penting. IDS digunakan untuk mendeteksi dan mengidentifikasi serangan dari pihak yang tidak sah serta memberikan notifikasi kepada administrator jaringan untuk mengambil langkah-langkah mitigasi yang diperlukan. Purnama *et al.* (2023) menjelaskan bahwa IDS sangat krusial untuk menjaga integritas dan keamanan sistem jaringan, dengan mendeteksi ancaman yang masuk sebelum dapat menyebabkan kerusakan lebih lanjut. Selain itu, penelitian oleh Syujak (2024) menunjukkan bahwa integrasi Deep Packet Inspection (DPI) dengan IDS dapat meningkatkan kemampuan sistem dalam mendeteksi serangan, khususnya Distributed Denial of Service (DDoS). Teknologi DPI memungkinkan pemantauan yang lebih mendalam terhadap paket data yang mengalir dalam jaringan, sehingga memudahkan identifikasi serangan yang lebih tersembunyi. Temuan ini sejalan dengan penelitian Faiz *et al.* (2022), yang mengungkapkan bahwa penggunaan machine learning untuk mendeteksi serangan DDoS dapat meningkatkan akurasi dan efisiensi deteksi. Dengan penerapan teknik klasifikasi yang lebih canggih, seperti yang digunakan dalam machine learning, sistem IDS dapat lebih efektif dalam mengidentifikasi pola-pola serangan yang kompleks. Hal ini menunjukkan bahwa penerapan teknologi baru seperti DPI dan machine learning dalam IDS sangat penting untuk meningkatkan perlindungan terhadap ancaman yang semakin berkembang.

Penggunaan sistem manajemen informasi berbasis web memiliki peranan yang sangat relevan dalam pengelolaan dan pemantauan data, terutama dalam konteks teknologi informasi. Kurniawan *et al.* (2023) menjelaskan bahwa aplikasi berbasis web memungkinkan pengguna untuk mengakses dan mengelola data dengan lebih mudah dan efisien. Sistem seperti ini menawarkan kemudahan dalam pemantauan informasi yang diperlukan, serta menyediakan antarmuka yang terintegrasi, sehingga mempercepat pengambilan keputusan. Meskipun demikian, referensi ini lebih relevan untuk pengelolaan data umum dan tidak langsung terkait dengan deteksi anomali pada jaringan, sehingga kurang tepat untuk mendukung klaim yang berhubungan dengan keamanan jaringan. Sebaliknya, penelitian oleh Hariyadi *et al.* (2023) menunjukkan bahwa sistem berbasis web juga dapat diterapkan dalam bidang forensik digital, yang sangat relevan untuk investigasi keamanan jaringan. Sistem berbasis web memungkinkan pengumpulan dan analisis data digital yang dapat membantu mendeteksi serangan serta melacak jejak aktivitas yang mencurigakan. Dalam pengembangan aplikasi deteksi anomali pada jaringan internet, seperti yang diterapkan di Disaster Recovery Center, dibutuhkan integrasi berbagai teknologi dan metode. Metode seperti K-Means clustering, Intrusion Detection System (IDS), serta sistem berbasis web akan bekerja secara sinergis untuk menciptakan solusi yang efektif dalam menjaga keamanan informasi. Dengan menggabungkan teknologi-teknologi ini, sistem yang dihasilkan akan lebih efisien dalam mendeteksi ancaman dan memberikan perlindungan terhadap data penting.

Jurnal Ilmu Komputer dan Teknologi Informasi
https://journal.stmiki.ac.id
E-ISSN: 3047-6674 | P-ISSN: 3047-6682
Vol. 2 No. 1 (2025) | Maret
OPEN ACCESS
https://doi.org/10.35870/jikti.v2i1.1341

Sistem Manajemen Informasi dan Keamanan (SIEM) berbasis web merupakan komponen yang sangat penting dalam menjaga keamanan informasi di berbagai organisasi. SIEM berfungsi untuk mengumpulkan, menganalisis, dan mengelola data yang berkaitan dengan aspek keamanan dari berbagai sumber yang ada. Dengan kemampuan untuk memantau sistem secara real-time, SIEM memungkinkan identifikasi ancaman secara cepat serta memberikan respons yang lebih efisien. Penelitian oleh González-Granadillo *et al.* (2021) menunjukkan bahwa SIEM telah banyak diterapkan di berbagai sektor sebagai alat yang efektif dalam mencegah, mendeteksi, dan merespons serangan siber. Selain itu, SIEM juga memberikan cakupan analisis yang lebih luas dalam mengidentifikasi area-area dengan tingkat risiko tinggi, yang memungkinkan organisasi untuk mengoptimalkan upaya mitigasi ancaman. Lebih lanjut, studi oleh Tuyishime *et al.* (2023) menekankan peran penting dari SIEM dalam meningkatkan keamanan sistem berbasis cloud. Pendekatan berbasis SIEM ini memiliki kemampuan untuk secara otomatis memantau dan mendeteksi insiden keamanan, sekaligus memitigasi ancaman yang muncul, sehingga meningkatkan keselamatan data yang tersimpan di cloud. Kemampuan SIEM untuk mengintegrasikan berbagai alat dan sumber data juga memungkinkan organisasi untuk mengelola risiko dengan lebih baik, mengidentifikasi ancaman yang lebih cepat, dan merespons dengan langkah-langkah mitigasi yang tepat. Dengan perkembangan teknologi yang semakin pesat, penerapan SIEM menjadi semakin relevan dalam menghadapi ancaman yang semakin kompleks dan dinamis di dunia maya.

Implementasi Security Information and Event Management (SIEM) dapat dioptimalkan dengan mengadopsi standar keamanan informasi yang diakui secara internasional, seperti ISO 27001. Bakri dan Irmayana (2017) menjelaskan bahwa penerapan sistem manajemen keamanan informasi yang sesuai dengan standar ISO 27001 memberikan kerangka kerja yang jelas untuk merancang dan mengimplementasikan model pengendalian keamanan informasi yang lebih efektif. Dengan mengikuti pedoman ini, organisasi dapat membangun sistem keamanan yang lebih solid dan terstruktur, yang juga membantu dalam pemantauan dan mitigasi ancaman secara lebih sistematis. Penelitian oleh Thoyyibah (2018) juga sejalan dengan temuan tersebut, di mana ia mengevaluasi manajemen keamanan informasi menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO 27001:2013. Hasil penelitian tersebut menunjukkan bahwa evaluasi yang dilakukan dengan pendekatan sistematis dapat memberikan gambaran yang lebih jelas mengenai efektivitas sistem pengendalian yang diterapkan. Selain itu, evaluasi semacam ini berkontribusi signifikan pada peningkatan tingkat keamanan sistem informasi di dalam organisasi. Penerapan standar ISO 27001, yang mengutamakan pengelolaan risiko keamanan informasi secara menyeluruh, memungkinkan organisasi untuk mengidentifikasi kelemahan yang ada dan mengambil langkah-langkah mitigasi yang tepat. Oleh karena itu, integrasi standar ISO 27001 dengan SIEM menjadi solusi yang sangat tepat untuk meningkatkan ketahanan dan keamanan sistem informasi dalam menghadapi ancaman yang terus berkembang.

Selain faktor keamanan, sistem berbasis web juga menawarkan kemudahan akses yang lebih fleksibel dan efisien terhadap data keamanan. Duma dan Pusvita (2023) menjelaskan bahwa sistem informasi berbasis web dapat meningkatkan efisiensi pengelolaan data secara terintegrasi, yang menjadi sangat penting dalam implementasi Security Information and Event Management (SIEM). Dengan sistem berbasis web, pengumpulan, analisis, dan pelaporan data menjadi lebih cepat dan mudah diakses. Hal ini memungkinkan pengelolaan data keamanan yang lebih efektif, sekaligus mempermudah pengambilan keputusan dalam menghadapi potensi ancaman. Pengembangan dan penerapan SIEM berbasis web memberikan manfaat ganda, yaitu tidak hanya memperkuat sistem keamanan informasi tetapi juga meningkatkan efisiensi operasional organisasi. Akses yang lebih terorganisir dan mudah memungkinkan administrator untuk melakukan pemantauan lebih cepat dan lebih tepat waktu. Dengan memanfaatkan teknologi berbasis web, berbagai sumber data dan alat keamanan dapat diintegrasikan dalam satu platform yang mudah digunakan, mengurangi kompleksitas dan mempermudah proses pemantauan. Selain itu, integrasi SIEM berbasis web dengan standar keamanan informasi seperti ISO 27001 menawarkan solusi yang lebih efektif dalam mengelola risiko. Dengan dukungan teknologi modern, pendekatan ini memungkinkan organisasi untuk

Jurnal Ilmu Komputer dan Teknologi Informasi
https://journal.stmiki.ac.id
E-ISSN: 3047-6674 | P-ISSN: 3047-6682
Vol. 2 No. 1 (2025) | Maret
OPEN ACCESS
https://doi.org/10.35870/jikti.v2i1.1341

meningkatkan ketahanan sistem informasi secara signifikan, mendeteksi ancaman lebih cepat, dan memastikan kepatuhan terhadap standar keamanan yang diakui secara global.

2. Metode Penelitian

Penelitian ini berfokus pada analisis sistem jaringan internet di Gedung Disaster Recovery Center (DRC) Kejaksaan RI, yang berlokasi di Jl. Mabes Hankam, Badan Diklat Kejaksaan RI. Penelitian dilaksanakan selama tahun 2023 dengan tujuan untuk memahami, mengevaluasi, dan mengembangkan sistem deteksi anomali pada jaringan yang digunakan di gedung tersebut. Pendekatan yang digunakan dalam penelitian ini melibatkan beberapa metode, yaitu pengumpulan data, observasi, dan wawancara. Pengumpulan data dilakukan melalui berbagai sumber, baik data primer maupun sekunder, untuk mendapatkan pemahaman yang komprehensif mengenai struktur jaringan dan potensi ancaman keamanan. Data primer diperoleh langsung melalui observasi dan wawancara, sedangkan data sekunder berasal dari dokumentasi teknis serta catatan log keamanan jaringan. Metode observasi dilakukan dengan mengamati secara langsung konfigurasi jaringan yang ada, termasuk analisis topologi jaringan dan kebijakan keamanan yang diterapkan. Proses ini melibatkan identifikasi perangkat jaringan yang digunakan, skema pengaturan firewall, serta pola lalu lintas data dalam jaringan. Observasi juga mencakup analisis terhadap anomali yang mungkin terjadi dalam sistem, seperti lonjakan trafik tidak wajar atau akses tidak sah ke jaringan. Selain observasi, dilakukan juga wawancara dengan beberapa pihak terkait. Salah satu narasumber utama dalam wawancara ini adalah Mas Punky, selaku administrator jaringan internet di Gedung DRC Kejaksaan RI. Wawancara bertujuan untuk memahami aspek teknis pengelolaan jaringan, kendala yang dihadapi dalam operasional harian, serta kebijakan keamanan yang diterapkan. Selain itu, wawancara juga dilakukan dengan beberapa staf yang menjadi pengguna jaringan untuk mendapatkan perspektif terkait pengalaman mereka dalam mengakses dan menggunakan jaringan tersebut. Sebagai bagian dari pengumpulan data teknis, analisis log firewall juga dilakukan untuk mengidentifikasi pola serangan atau akses mencurigakan yang dapat menjadi indikasi anomali jaringan. Data dari log firewall dikumpulkan melalui administrator jaringan dan dianalisis menggunakan teknik pemrosesan data untuk mendeteksi aktivitas tidak normal. Dengan menggunakan kombinasi metode ini, penelitian dapat memperoleh gambaran yang lebih jelas mengenai kondisi jaringan, efektivitas sistem keamanan yang diterapkan, serta area yang memerlukan perbaikan atau peningkatan. Hasil dari metode ini menjadi dasar dalam merancang solusi deteksi anomali yang lebih optimal untuk meningkatkan keamanan jaringan di Gedung DRC Kejaksaan RI.

3. Hasil dan Pembahasan

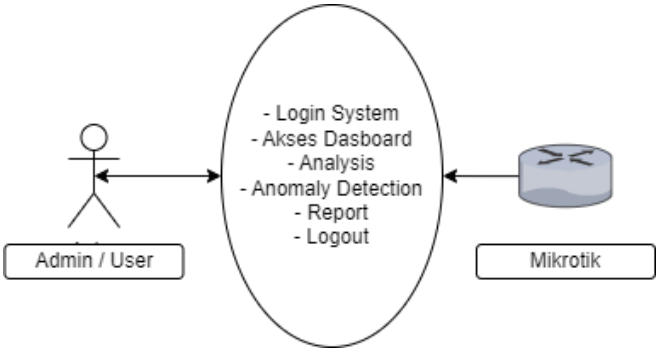
3.1 Hasil

3.1.1 Rancangan UML

Use Case Diagram merupakan bagian dari Unified Modeling Language (UML) yang digunakan untuk menggambarkan interaksi antara pengguna dan sistem yang dikembangkan. Diagram ini menunjukkan bagaimana setiap aktor berperan dalam menjalankan fungsionalitas tertentu yang telah didefinisikan. Fungsionalitas yang ditampilkan dalam Use Case Diagram memberikan gambaran tentang bagaimana sistem bekerja secara keseluruhan. Setiap aktor memiliki peran spesifik dalam menjalankan tugasnya, seperti administrator yang bertanggung jawab atas pemantauan dan analisis data atau pengguna yang mengakses layanan tertentu. Penggunaan diagram ini membantu dalam mengidentifikasi kebutuhan sistem serta memastikan setiap fungsi yang dirancang selaras dengan tujuan pengembangan. Dalam implementasinya, Use Case Diagram membantu pengembang memahami interaksi antara komponen yang ada, sehingga alur kerja sistem dapat dirancang dengan lebih efektif. Pemodelan ini juga menjadi referensi dalam proses pengembangan untuk memastikan setiap fitur yang dibuat sesuai dengan kebutuhan pengguna. Dengan adanya Use Case Diagram,

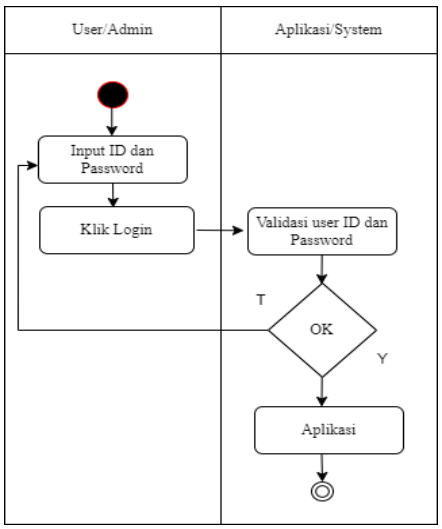
Jurnal Ilmu Komputer dan Teknologi Informasi
https://journal.stmiki.ac.id
E-ISSN: 3047-6674 | P-ISSN: 3047-6682
Vol. 2 No. 1 (2025) | Maret
OPEN ACCESS
https://doi.org/10.35870/jikti.v2i1.1341

rancangan sistem dapat dibuat lebih terstruktur, memudahkan analisis terhadap kebutuhan pengguna, serta mendukung perancangan yang lebih sistematis sebelum masuk ke tahap implementasi teknis.



Gambar 1. Use case diagram

Activity Diagram menggambarkan alur kerja sistem berdasarkan urutan proses yang telah ditetapkan. Setiap tahapan mencerminkan langkah-langkah yang harus dilakukan pengguna dalam menggunakan sistem. Proses diawali dengan User Login, di mana pengguna memasukkan kredensial untuk mendapatkan akses. Setelah berhasil masuk, pengguna diarahkan ke Dashboard, yang berfungsi sebagai pusat navigasi utama. Selanjutnya, sistem menyediakan fitur Analysis yang memungkinkan pemrosesan data untuk mendeteksi anomali. Proses Anomaly Detection bekerja dengan menganalisis data jaringan dan mengidentifikasi pola yang tidak normal. Hasil analisis kemudian disusun dalam bentuk laporan melalui fitur Report, yang dapat diakses oleh administrator atau pengguna dengan hak akses tertentu. Setelah seluruh proses selesai, pengguna dapat keluar dari sistem dengan melakukan Logout untuk memastikan keamanan akses. Pada tahap User Login, sistem memverifikasi informasi pengguna yang dimasukkan sebelum memberikan akses. Jika kredensial yang diberikan sesuai, pengguna dapat masuk dan melanjutkan ke tahapan berikutnya. Diagram aktivitas ini memvisualisasikan bagaimana sistem menangani setiap interaksi pengguna, memastikan proses berjalan sesuai dengan prosedur yang telah ditentukan. Dengan adanya Activity Diagram, rancangan sistem dapat lebih dipahami dan diimplementasikan secara efisien.

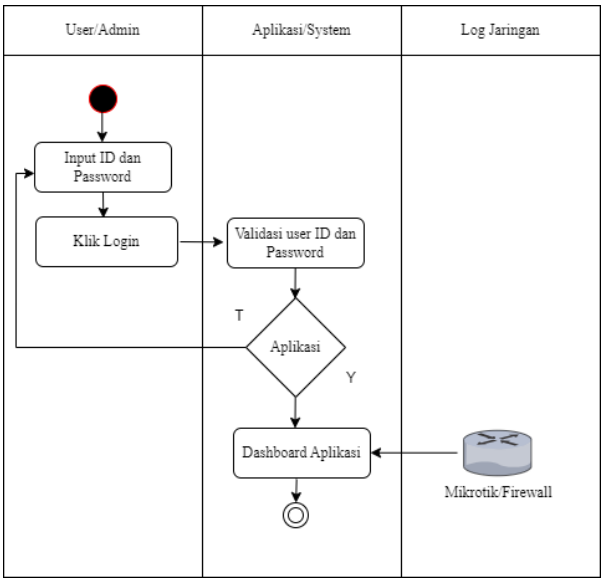


Gambar 2. Activity Diagram User Login

Gambar di atas menggambarkan proses pengguna dalam melakukan login ke dalam sistem menggunakan username dan password. Pengguna harus memasukkan kredensial yang sesuai untuk mendapatkan akses. Jika data yang dimasukkan benar, sistem akan langsung mengarahkan pengguna

Jurnal Ilmu Komputer dan Teknologi Informasi
https://journal.stmiki.ac.id
E-ISSN: 3047-6674 | P-ISSN: 3047-6682
Vol. 2 No. 1 (2025) | Maret
OPEN ACCESS
https://doi.org/10.35870/jikti.v2i1.1341

ke halaman utama. Namun, jika terdapat kesalahan dalam username atau password, sistem akan menampilkan pesan peringatan yang menyatakan bahwa kredensial tidak valid. Proses ini memastikan bahwa hanya pengguna yang memiliki akun yang dapat mengakses sistem, sehingga meningkatkan keamanan data dan mencegah akses tidak sah. Activity Diagram Dashboard menggambarkan alur kerja setelah proses login berhasil dilakukan. Diagram ini menunjukkan bagaimana pengguna diarahkan ke dashboard aplikasi, yang berfungsi sebagai pusat navigasi utama dalam sistem. Pada tahap ini, pengguna dapat mengakses berbagai fitur yang tersedia sesuai dengan hak akses yang dimiliki. Dashboard menampilkan informasi yang relevan serta menyediakan akses ke berbagai modul, termasuk analisis data, deteksi anomali, dan laporan sistem. Dengan adanya dashboard, interaksi pengguna dengan sistem menjadi lebih terstruktur dan efisien.



Gambar 3. ActivityDiagram Dashboard

Pada gambar di atas, dapat dilihat dengan jelas bahwa setelah pengguna berhasil melakukan proses login ke dalam sistem, mereka akan langsung diarahkan menuju tampilan awal yang merupakan dashboard sistem. Dashboard ini memberikan gambaran umum mengenai fitur-fitur yang tersedia, memungkinkan pengguna untuk dengan mudah mengakses informasi dan melakukan interaksi sesuai kebutuhan. Sebagai antarmuka utama, dashboard memainkan peran penting dalam memandu navigasi pengguna dalam sistem.

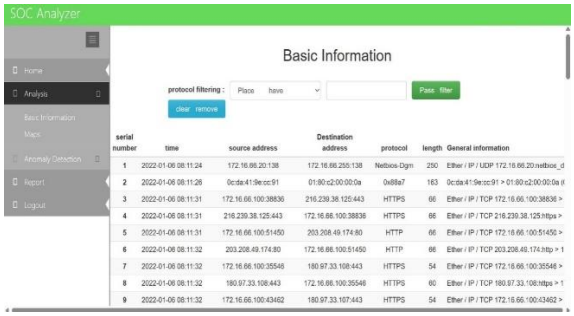
Activity Diagram Analysis dapat dilihat pada diagram berikut. Alur dalam diagram ini menjelaskan proses yang dilakukan setelah pengguna berhasil login ke dalam sistem, di mana pengguna langsung diarahkan ke tampilan berikutnya, yaitu menu Analysis. Diagram ini menggambarkan dengan jelas bagaimana pengguna dapat mengakses dan berinteraksi dengan menu tersebut setelah login berhasil. Activity Diagram Anomaly Detection dapat dilihat pada diagram berikut. Diagram ini menggambarkan alur aktivitas yang terjadi setelah pengguna login ke dalam sistem, yang kemudian mengarahkan pengguna untuk melihat menu Anomaly Detection. Alur ini menunjukkan langkah-langkah yang diambil pengguna dalam mengakses dan menggunakan fitur deteksi anomali setelah login berhasil. Activity Diagram Report dapat dilihat pada diagram berikut. Diagram ini menjelaskan alur aktivitas pengguna setelah login menuju menu Report. Setelah login berhasil, pengguna langsung melihat tampilan menu Report untuk melanjutkan kegiatan mereka dalam sistem. Activity Diagram Logout dapat dilihat pada diagram berikut. Diagram ini menggambarkan alur aktivitas yang terjadi saat pengguna melakukan logout dari sistem. Proses ini memastikan pengguna dapat keluar dari sistem dengan langkah-langkah yang jelas dan aman setelah selesai menggunakan aplikasi.

Jurnal Ilmu Komputer dan Teknologi Informasi
https://journal.stmiki.ac.id
E-ISSN: 3047-6674 | P-ISSN: 3047-6682
Vol. 2 No. 1 (2025) | Maret
OPEN ACCESS
https://doi.org/10.35870/jikti.v2i1.1341

3.1.2 Implementasi Rancangan Aplikasi

Pada tahap implementasi rancangan aplikasi, tampilan sistem yang telah dirancang akan diterapkan dalam aplikasi. Salah satu bagian yang terlihat pertama kali setelah pengguna login adalah tampilan dashboard sistem. Dashboard ini dirancang untuk memberikan gambaran umum dan akses mudah ke fitur utama aplikasi, memungkinkan pengguna untuk dengan cepat mengakses informasi dan fungsi yang mereka butuhkan dalam satu tampilan yang terorganisir dengan baik.

Gambar 4. Tampilan Halaman Sistem



Gambar 5. Tampilan Halaman Dasboard

Tampilan dashboard Analysis memiliki beberapa elemen penting yang memungkinkan pengguna untuk mengakses informasi secara komprehensif. Salah satu bagian utama adalah Basic Information, yang menyajikan data dasar dan informasi penting terkait dengan sistem yang sedang dipantau. Pengguna dapat dengan mudah memperoleh gambaran umum dari kondisi sistem yang sedang dianalisis. Selain itu, terdapat fitur Maps yang memberikan visualisasi geospasial yang interaktif, memudahkan pengguna dalam memahami data melalui peta dan lokasi yang terkait, serta memantau pergerakan atau kejadian di dalam sistem. Selanjutnya, tampilan dashboard Anomaly difokuskan pada deteksi anomali yang dapat membantu pengguna mengidentifikasi pola atau kejadian yang tidak biasa dalam sistem. Hal ini penting untuk menjaga sistem agar tetap aman dan terhindar dari potensi ancaman.

Gambar 6. Tampilan Halaman Anomaly

Gambar 7. Hasil Report

Tampilan Report memungkinkan pengguna untuk mengunduh laporan dalam format PDF, memberikan kemudahan dalam pencetakan atau distribusi hasil analisis dan laporan yang telah dilakukan. Pada tahap testing aplikasi, berbagai uji coba dilakukan untuk memastikan aplikasi berjalan dengan baik. Pengujian login dilakukan untuk memastikan akses pengguna berjalan lancar. Selain itu, menu diuji untuk memverifikasi bahwa hasil preview yang ditampilkan sesuai dengan yang diharapkan, memberikan pengalaman pengguna yang optimal dan bebas dari kesalahan.

3.2 Pembahasan

Berdasarkan hasil penelitian, pengembangan dan penerapan sistem deteksi anomali dalam jaringan menggunakan berbagai teknologi dan pendekatan telah terbukti efektif dalam meningkatkan pengawasan dan keamanan. Salah satu pendekatan yang banyak digunakan adalah Security

Jurnal Ilmu Komputer dan Teknologi Informasi
https://journal.stmiki.ac.id
E-ISSN: 3047-6674 | P-ISSN: 3047-6682
Vol. 2 No. 1 (2025) | Maret
OPEN ACCESS
https://doi.org/10.35870/jikti.v2i1.1341

Information and Event Management (SIEM). Teknologi SIEM memungkinkan untuk memonitorin infrastruktur kritis dengan cara mengumpulkan dan menganalisis event serta log yang berasal dari berbagai sumber dalam jaringan. Sistem ini memberikan kemampuan untuk mendeteksi ancaman secara real-time, yang sangat penting untuk memastikan sistem tetap aman dari potensi serangan. González-Granadillo *et al.* (2021) menjelaskan bahwa SIEM tidak hanya membantu dalam pemantauan, tetapi juga memungkinkan analisis mendalam terhadap data yang dikumpulkan. Dengan cara ini, pola abnormal dalam aliran data dapat segera terdeteksi dan dievaluasi untuk mengidentifikasi potensi ancaman yang membahayakan sistem (González-Granadillo *et al.*, 2021). Hal serupa juga diungkapkan oleh Tuyishime *et al.* (2023) yang menekankan pentingnya penggunaan SIEM dalam meningkatkan keamanan cloud, dengan mendeteksi ancaman secara otomatis dan mengirimkan notifikasi kepada administrator untuk respon lebih cepat (Tuyishime *et al.*, 2023).

Selain SIEM, teknik lain yang digunakan dalam deteksi anomali adalah k-means clustering, sebuah metode pembelajaran mesin yang digunakan untuk mengelompokkan data berdasarkan pola atau kemiripan tertentu. Teknik ini banyak diterapkan dalam analisis log jaringan untuk mendeteksi pola yang tidak biasa, yang mungkin menunjukkan adanya serangan atau intrusi. Aini *et al.* (2018) dalam penelitian mereka menyebutkan bahwa k-means clustering sangat efektif dalam mendeteksi anomali pada lalu lintas jaringan, terutama ketika pola serangan tidak terdeteksi oleh metode tradisional. Teknik ini memungkinkan sistem untuk memisahkan data normal dan mencurigakan, serta memberikan informasi yang lebih akurat mengenai aktivitas yang terjadi dalam jaringan (Aini *et al.*, 2018). Begitu pula, Ridho dan Kusuma (2019) membahas penerapan k-means dalam mendeteksi intrusi pada log akses, yang semakin penting mengingat volume dan kompleksitas data yang semakin besar. Dengan metode ini, sistem dapat secara otomatis mengklasifikasikan log dan mendeteksi potensi serangan tanpa memerlukan pengawasan manual (Ridho & Kusuma, 2019).

Penerapan SIEM yang dikombinasikan dengan teknik seperti k-means clustering diharapkan dapat meningkatkan kemampuan deteksi ancaman dalam jaringan dengan cara yang lebih cepat dan efisien. Sistem seperti ini tidak hanya membantu dalam mendeteksi ancaman dengan lebih akurat tetapi juga mempermudah proses pengawasan secara real-time. Dengan platform yang terintegrasi, administrator dapat mengakses laporan dan analisis dengan lebih mudah, mempercepat respons terhadap ancaman yang teridentifikasi, serta mengurangi resiko kerusakan yang lebih besar akibat serangan siber. Pengembangan lebih lanjut dari sistem ini kemungkinan akan melibatkan integrasi teknologi canggih seperti kecerdasan buatan (AI) dan pembelajaran mendalam (deep learning) untuk meningkatkan kemampuan deteksi dan respons terhadap ancaman yang semakin kompleks. Integrasi teknologi-teknologi ini diharapkan mampu mengatasi tantangan yang lebih besar dalam menjaga keamanan jaringan, terutama dalam menghadapi serangan yang semakin dinamis dan sulit diprediksi. Seiring dengan perkembangan dunia siber, penerapan sistem berbasis SIEM dan teknik analisis data seperti k-means clustering akan terus menjadi alat yang sangat penting dalam menjaga integritas dan keamanan jaringan.

4. Kesimpulan

Berdasarkan uraian yang telah disampaikan, dapat disimpulkan beberapa hal berikut: Gedung Disaster Recovery Center (DRC) Kejaksaan RI memiliki sistem yang menyediakan informasi mengenai lalu lintas jaringan internet serta mendeteksi anomali yang mungkin terjadi. Sistem ini memungkinkan pengguna untuk segera memperoleh informasi apabila ditemukan anomali yang dapat membahayakan kestabilan dan keamanan jaringan. Selain itu, sistem ini juga memberikan laporan mengenai log dan event yang tercatat pada lalu lintas jaringan, yang memudahkan administrator dalam memantau kondisi sistem secara real-time. Dengan demikian, pengawasan terhadap perangkat keamanan jaringan yang digunakan menjadi lebih terkontrol dan cepat dalam merespons potensi ancaman. Pembuatan dashboard berbasis Security Information and Event Management (SIEM) diharapkan dapat menyederhanakan proses pemantauan dengan menampilkan berbagai informasi log dan event dari berbagai perangkat dalam satu tampilan. Dashboard ini memberikan kemudahan bagi

E-ISSN: 3047-6674 | P-ISSN: 3047-6682
Vol. 2 No. 1 (2025) | Maret
OPEN ACCESS
https://doi.org/10.35870/jikti.v2i1.1341

pengelola untuk mengawasi seluruh aspek keamanan dan performa sistem, memudahkan identifikasi ancaman, serta memastikan pengelolaan dan pengawasan jaringan lebih efisien dan terorganisir.

5. Daftar Pustaka

Aini, F., Riadi, I., & Umar, R. (2018). Perancangan deteksi anomali traffic untuk investigasi log menggunakan metode k-means clusters. Prosiding Sains Nasional Dan Teknologi, 1(1). https://doi.org/10.36499/psnst.v1i1.2387

Bakri, M. and Irmayana, N. (2017). Analisis dan penerapan sistem manajemen keamanan informasi simhp bpkp menggunakan standar iso 27001. Jurnal Tekno Kompak, 11(2), 41. https://doi.org/10.33365/jtk.v11i2.162

Duma, A. and Pusvita, E. (2023). Pengembangan sistem informasi data siswa berbasis web pada smpn 09 nabire dengan metode waterfall. Journal of Information System Management (Joism), 5(1), 70-76. https://doi.org/10.24076/joism.2023v5i1.1115

Fahmi, R., Imilda, & Salam, A. (2023). Rancang Bangun Platform Penjualan Domain Dan Hosting Berbantuan Whmcs Berbasis Web. *Jurnal Sistem Komputer (SISKOM)*, *3*(1), 49-55. https://doi.org/10.35870/siskom.v3i1.793

Faiz, M., Somantri, O., & Muhammad, A. (2022). Rekayasa fitur berbasis machine learning untuk mendeteksi serangan ddos. Jurnal Nasional Teknik Elektro Dan Teknologi Informasi (Jnteti), 11(3), 176-182. https://doi.org/10.22146/jnteti.v11i3.3423

González-Granadillo, G., González-Zarzosa, S., & Díaz, R. (2021). Security information and event management (siem): analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759. https://doi.org/10.3390/s21144759

Hariyadi, D., Nugroho, M., Setiawan, C., & Wicaksono, A. (2023). Hybrid acquisition pada forensik digital berbasis iso/iec 27037:2012 menggunakan port mirroring dan single board computer. Journal of Information System Management (Joism), 5(1), 8-13. https://doi.org/10.24076/joism.2023v5i1.1157

Kurniawan, C., Sutiningsih, D., & Martini, M. (2023). Sistem aplikasi berbasis website dalam deteksi dini dan edukasi pneumonia. Jurnal Ilmiah Permas Jurnal Ilmiah Stikes Kendal, 13(2), 507-518. https://doi.org/10.32583/pskm.v13i2.928

Pongoh, B. R., Ahmad, L., & Idwan, H. (2024). Sistem Informasi Infografis Berbasis Web Pada Kantor Dinas Pangan Provinsi Aceh. *Jurnal Ilmu Komputer Dan Teknologi Informasi*, *1*(1), 34-44. https://doi.org/10.35870/jikti.v1i1.736

Purnama, T., Muhyidin, Y., & Singasatia, D. (2023). Implementasi intrusion detection system (ids) snort sebagai sistem keamanan menggunakan whatsapp dan telegram sebagai media notifikasi. Jurnal Teknologi Informasi Dan Komunikasi, 14(2), 358-369. https://doi.org/10.51903/jtikp.v14i2.726

Ridho, F. and Kusuma, A. (2019). Deteksi intrusi jaringan dengan k-means clustering pada akses log dengan teknik pengolahan big data. Jurnal Aplikasi Statistika & Komputasi Statistik, 10(1), 53. https://doi.org/10.34123/jurnalasks.v10i1.202

E-ISSN: 3047-6674 | P-ISSN: 3047-6682
Vol. 2 No. 1 (2025) | Maret
OPEN ACCESS
https://doi.org/10.35870/jikti.v2i1.1341

Riza, M., Ahmad, L., & Imilda. (2024). Perancangan Sistem Informasi Manajemen Produksi Padi Berbasis Web untuk Dinas Pertanian Provinsi Aceh. *Jurnal Ilmu Komputer Dan Teknologi Informasi*, *1*(1), 14-23. https://doi.org/10.35870/jikti.v1i1.733

Syujak, A. (2024). Integrasi deep packet inspection dengan intrusion detection system (ids) untuk identifikasi serangan ddos dalam jaringan skala besar. Jurnal Minfo Polgan, 13(2), 1971-1975. https://doi.org/10.33395/jmp.v13i2.14324

Thoyyibah, T. (2018). Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (kami) berdasarkan iso 27001:2013 pada pusat informasi dan pangkalan data perguruan tinggi x. Jurnal Coreit Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi, 4(2), 72. https://doi.org/10.24014/coreit.v4i2.6292

Tuyishime, E., Bălan, T., Cotfas, P., Cotfas, D., & Rekeraho, A. (2023). Enhancing cloud security—proactive threat monitoring and detection using a siem-based approach. Applied Sciences, 13(22), 12359. https://doi.org/10.3390/app132212359

Zulfinar, D., Nurrisma, & Imilda. (2023). Rancang Bangun Sistem Informasi Pustaka Online Berbasis Web untuk Kampus STMIK Indonesia Banda Aceh. *Jurnal Sistem Komputer (SISKOM)*, *3*(1), 36-48. https://doi.org/10.35870/siskom.v3i1.792