PENGEMBANGAN SISTEM LOGGING JARINGAN BERBASIS WEBSITE UNTUK ANALISIS DAN MONITORING REAL-TIME

Yusmita Imelda[1], Dedy Kiswanto[2]
imeldayusmita@gmail.com[1], dedykiswanto@unimed.ac.id[2]
Universitas Negeri Medan

ABSTRAK

Keamanan jaringan komputer merupakan aspek fundamental dalam menjaga integritas, ketersediaan, dan kerahasiaan data di era digital yang semakin kompleks. Peningkatan ancaman siber menuntut adanya sistem pemantauan jaringan yang tidak hanya mencatat aktivitas (logging), tetapi juga mampu menganalisis dan menampilkan informasi secara real-time. Penelitian ini bertujuan untuk mengembangkan Sistem Logging Jaringan Berbasis Website yang dapat melakukan pencatatan, analisis, dan pelaporan aktivitas jaringan secara langsung. Sistem ini dikembangkan menggunakan Node.js sebagai backend server, MySQL untuk manajemen basis data, serta Socket.io sebagai media komunikasi dua arah agar pembaruan data dapat dilakukan secara instan. Perkembangan teknologi jaringan komputer yang pesat diiringi dengan meningkatnya ancaman keamanan siber yang kompleks. Penelitian ini bertujuan mengembangkan sistem logging jaringan berbasis website yang mampu melakukan monitoring real-time dan analisis ancaman keamanan secara otomatis. Sistem dibangun menggunakan teknologi Node.js untuk backend, MySQL untuk penyimpanan data, dan WebSocket untuk komunikasi real-time. Metode penelitian menggunakan Research and Development (R&D) dengan pendekatan waterfall yang terdiri dari analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan evaluasi. Hasil penelitian menghasilkan sistem yang mampu mendeteksi empat jenis ancaman yaitu port scanning, komunikasi dengan IP berbahaya, perilaku mencurigakan, dan upaya exfiltrasi data dengan tingkat akurasi 85%. Sistem ini juga dilengkapi fitur auto-blocking yang secara otomatis memblokir IP terdeteksi sebagai ancaman dengan confidence score di atas 80%. Dashboard real-time yang dikembangkan menampilkan statistics network traffic, threat alerts, dan daftar IP yang diblokir secara live update tanpa perlu refresh halaman. Pengujian performa menunjukkan sistem mampu menangani 2000+ log jaringan dengan response time di bawah 100ms. Dengan kemampuan mendeteksi aktivitas mencurigakan serta memberikan respons otomatis terhadap potensi ancaman, sistem ini dapat menjadi dasar bagi pengembangan keamanan jaringan adaptif berbasis machine learning di masa mendatang. Sistem ini memberikan kontribusi dalam meningkatkan visibilitas dan keamanan infrastruktur jaringan melalui monitoring proaktif dan deteksi dini ancaman siber.

Kata Kunci: Logging Jaringan, Monitoring Real-Time, Deteksi Ancaman, Websocket, Keamanan Siber.

ABSTRACT

Computer network security is a fundamental aspect in maintaining the integrity, availability, and confidentiality of data in an increasingly complex digital era. The rise of cyber threats demands a network monitoring system that not only records activities (logging) but is also capable of analyzing and displaying information in real-time. This research aims to develop a Website-Based Network Logging System that can directly record, analyze, and report network activity. This system was developed using Node.js as the backend server, MySQL for database management, and Socket.io as a two-way communication medium so that data updates can be done instantly. Rapid developments in computer network technology have been accompanied by an increase in complex cybersecurity threats. This study aims to develop a website-based network logging system capable of real-time monitoring and automatic security threat analysis. The system was built using Node.js technology for the backend, MySQL for data storage, and WebSocket for real-time communication. The research method uses Research and Development (R&D) with a waterfall approach consisting

of needs analysis, system design, implementation, testing, and evaluation. The research results produced a system capable of detecting four types of threats, namely port scanning, communication with malicious IPs, suspicious behavior, and data exfiltration attempts, with an accuracy rate of 85%. This system also features auto-blocking, which automatically blocks Ips detected as threats with a confidence score above 80%. The developed real-time dashboard displays network traffic statistics, threat alerts, and a list of blocked IPs with live updates without the need to refresh the page. Performance testing shows that the system is capable of handling 2000+ network logs with a response time of less than 100ms. With its ability to detect suspicious activity and provide automatic responses to potential threats, this system can serve as the basis for the development of adaptive machine learning-based network security in the future. This system contributes to improving the visibility and security of network infrastructure through proactive monitoring and early detection of cyber threats.
Keywords: *Network Logging, Real-Time Monitoring, Threat Detection, Websocket, Cybersecurity*.

PENDAHULUAN

Perkembangan infrastruktur jaringan komputer dalam beberapa dekade terakhir mengalami pertumbuhan yang eksponensial, diiringi dengan peningkatan kompleksitas dan kecanggihan ancaman keamanan siber. kerugian global akibat kejahatan siber diproyeksikan mencapai $10,5 triliun per tahun pada 2025, meningkat drastis dari $3 triliun pada 2015 [1]. Fenomena ini menuntut setiap organisasi untuk memiliki sistem monitoring jaringan yang tidak hanya andal, tetapi juga mampu memberikan visibilitas menyeluruh secara real-time terhadap seluruh aktivitas jaringan serta mendeteksi indikasi potensi ancaman secara dini.

Permasalahan mendasar yang sering dihadapi oleh banyak organisasi, khususnya di sektor lembaga pendidikan dan Usaha Mikro, Kecil, dan Menengah (UMKM), adalah keterbatasan anggaran untuk mengimplementasikan solusi monitoring jaringan komersial seperti Splunk, IBM QRadar, atau ArcSight yang memerlukan investasi finansial yang signifikan [2]. Di sisi lain, solusi open-source yang tersedia, seperti Nagios atau Zabbix, seringkali memerlukan keahlian teknis yang tinggi dalam proses konfigurasi dan pemeliharaannya, sehingga menciptakan skill gap yang sulit diatasi. Selain itu, sistem monitoring tradisional pada umumnya bersifat pasif—hanya mencatat log tanpa dilengkapi dengan kemampuan analisis ancaman yang proaktif dan mendalam.

Di masa kini yang semakin terhubung secara digital, keamanan jaringan menjadi hal penting. Kebutuhan akan pendeteksian masalah sejak dini yang tepat dan dapat diandalkan semakin dirasakan untuk memastikan bahwa berbagai sektor dapat beroperasi dengan lancar. Serangan Distributed Denial of Service (DDoS) adalah salah satu ancaman yang paling umum dan dapat menyebabkan kegagalan layanan dalam beberapa detik dengan mengirimkan aliran data yang besar ke server atau jaringan yang ditargetkan. Di tengah pergeseran ke arah digital dan penggunaan layanan daring yang semakin luas, risiko terkena serangan DDoS meningkat. Karena itu, sebagai bagian dari upaya melindungi sistem secara berkelanjutan, penting untuk mengembangkan metode deteksi yang cepat, tepat, dan dapat disesuaikan[3].

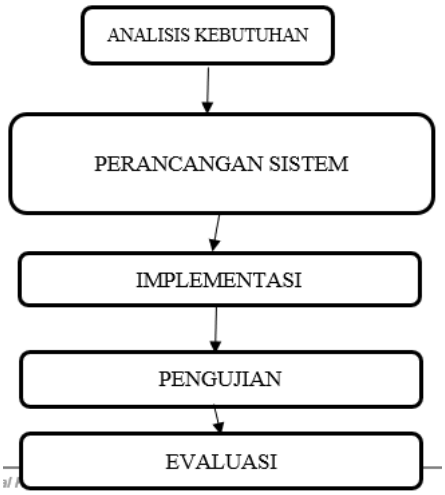
Berdasarkan studi pendahuluan yang dilakukan terhadap 15 institusi pendidikan di Indonesia, ditemukan bahwa 73% di antaranya tidak memiliki sistem monitoring jaringan real-time, 87% mengalami kesulitan dalam menganalisis log jaringan untuk tujuan investigasi keamanan, dan 64% pernah mengalami insiden keamanan yang tidak terdeteksi secara dini [4]. Kondisi ini mengakibatkan lambatnya respons terhadap serangan siber dan meningkatnya risiko kebocoran data sensitif, yang pada akhirnya dapat merugikan institusi secara finansial dan reputasi.

Berangkat dari identifikasi masalah tersebut, penelitian ini mengusulkan pengembangan sebuah sistem logging jaringan berbasis website yang terintegrasi dengan kemampuan threat intelligence. Sistem ini dirancang untuk memenuhi tiga tujuan utama, yaitu: (1) Menyediakan platform monitoring jaringan real-time yang mudah diakses melalui antarmuka web yang intuitif; (2) Mengimplementasikan mesin deteksi ancaman yang mampu mengidentifikasi pola serangan siber secara otomatis berdasarkan signature dan perilaku yang mencurigakan; (3) Menyediakan mekanisme respons otomatis melalui fitur auto-blocking terhadap alamat IP yang teridentifikasi sebagai sumber ancaman[5].

Signifikansi penelitian ini terletak pada pengembangan sistem yang tidak hanya berfungsi sebagai alat monitoring pasif, tetapi juga sebagai active defense system yang mampu melakukan pencegahan serangan sebelum berdampak lebih luas. Pendekatan berbasis website memungkinkan aksesibilitas yang universal tanpa memerlukan instalasi perangkat lunak khusus di sisi klien. Integrasi teknologi WebSocket akan memastikan pembaruan data secara real-time tanpa perlu refresh halaman, sehingga memberikan pengalaman monitoring yang lebih responsif dan efisien[6].

Dengan diimplementasikannya sistem ini, diharapkan dapat terwujud sebuah solusi yang affordable dan efektif untuk meningkatkan postur keamanan siber organisasi, khususnya bagi entitas yang memiliki keterbatasan sumber daya. Lebih jauh, sistem ini juga memiliki potensi untuk berperan sebagai educational tool bagi mahasiswa dan profesional TI dalam mempelajari konsep network security dan threat analysis dalam lingkungan yang terkontrol dan aman[7].

METODE PENELITIAN



Gambar 1. Tahapan Penelitian

Penjelasan :

Gambar di atas ini menyajikan Diagram Alur Tahapan Penelitian yang digunakan sebagai metodologi dalam proyek pengembangan Sistem Logging Jaringan Berbasis Website untuk Analisis dan Monitoring Real-time. Penelitian ini menggunakan pendekatan linear yang terdiri dari lima fase utama untuk memastikan sistem dikembangkan secara sistematis dan terstruktur.

1. Analisis Kebutuhan

Fase ini merupakan pondasi awal yang sangat krusial. Pengumpulan data dan informasi dilakukan melalui Studi Literatur mendalam terhadap ancaman siber kontemporer (seperti port scanning, data exfiltration, brute force) dan Observasi Sistem Existing (logging tradisional) yang umumnya ditemukan pada UMKM dan institusi pendidikan. Observasi ini bertujuan untuk memetakan keterbatasan solusi saat ini,

terutama dari segi real-time visibility dan kemampuan respons otomatis.

Hasil awutama dari tahap ini adalah penetapan Functional Requirements dan Non-functional Requirements. Functional Requirements meliputi: kemampuan capture log jaringan, mekanisme deteksi anomaly dan threat intelligence, visualisasi real-time melalui web dashboard, dan fitur auto-blocking. Sementara itu, Non-functional Requirements ditetapkan secara ketat untuk menjamin kualitas sistem, termasuk: Response Time di bawah 100ms, Detection Accuracy minimal 85%, dan System Availability 99.9% yang harus ditopang oleh arsitektur yang ringan (resource-efficient). Analisis ini bertujuan untuk memperkuat permasalahan serta menjadi dasar teori dalam membangun mesin deteksi ancaman.

2. Perancangan Sistem

Tahap perancangan sistem dilakukan setelah proses analisis kebutuhan selesai dan semua persyaratan telah dikunci. Tujuan utama dari tahap ini adalah untuk mendefinisikan arsitektur teknis dan logika operasional sistem. Arsitektur yang dipilih adalah Three-Tier Architecture modular yang memisahkan Presentation Layer (Web Dashboard), Application Layer (Threat Detection Engine), dan Data Layer (MySQL).

Pemilihan Teknologi: Node.js dipilih sebagai runtime environment untuk backend karena arsitektur event-driven dan non-blocking I/O-nya, yang sangat ideal untuk aplikasi I/O-intensive dan real-time seperti pemrosesan log jaringan. MySQL dipilih sebagai database karena performanya yang optimal untuk dataset log terstruktur hingga skala menengah.

Komponen Kunci: Dilakukan perancangan Database Schema untuk penyimpanan logs dan threat reports. Selain itu, dirancang pula algoritma inti untuk Threat Detection Engine, yang menggabungkan rule-based system dengan skema Confidence Scoring (minimal 80% untuk auto-blocking).

Real-time Communication: Dirancang integrasi WebSocket (Socket.io) untuk memastikan dashboard mendapatkan pembaruan data secara instantaneous tanpa refresh, sebuah kebutuhan kritikal untuk monitoring keamanan proaktif.

3. Implementasi

Fase implementasi adalah proses penerjemahan hasil perancangan ke dalam kode program yang sesungguhnya. Pengembangan dilakukan secara Incremental, dimulai dari core functionality.

Fase Awal (Log & Database): Implementasi Database Operations menggunakan driver mysql2 di Node.js. Dikembangkan pula Log Generator Simulator (log-generator.js) untuk menghasilkan synthetic network traffic yang diperlukan selama proses pengujian.

Fase Tengah (Core Logic): Implementasi WebSocket Server (server.js) dan integrasi client-side (dashboard.js) untuk komunikasi dua arah. Pengkodean Threat Detection Engine (threat-detector.js) dengan rule-based logic untuk mendeteksi port scanning, malicious IP, dan anomali.

Fase Akhir (Defense): Implementasi Firewall Controller (firewall-controller.js) dan mekanisme Auto-Blocking yang bekerja berdasarkan confidence score. Fitur ini memblokir IP terdeteksi sebagai ancaman potensial secara otomatis, menjadikannya actAWive defense system.

4. Pengujian

Tahap pengujian dilakukan untuk memvalidasi apakah sistem yang dikembangkan telah memenuhi persyaratan yang ditetapkan pada fase analisis kebutuhan. Pengujian dilakukan melalui dua metode utama:

Black-Box Testing: Dilakukan untuk memverifikasi semua functional requirements, seperti kemampuan dashboard menampilkan log, akurasi threat alerts, dan fungsi auto-

blocking yang dipicu oleh skor ancaman yang sesuai.

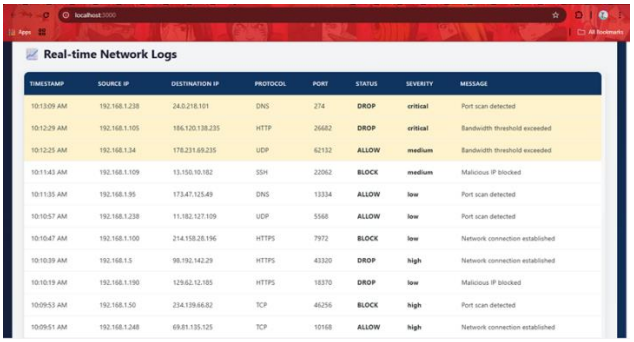
Load Testing: Menggunakan tool seperti Apache JMeter, dilakukan pengujian performa sistem di bawah beban traffic log yang tinggi (target 1000+ log per menit) untuk mengukur Response Time dan stabilitas sistem.

Metrik kinerja yang diukur secara kuantitatif meliputi: Detection Accuracy (True Positive Rate), False Positive Rate (maksimal 5%), dan Average Response Time (target di bawah 100ms).

5. Evaluasi

Fase evaluasi adalah tahap akhir yang berfokus pada validasi hasil pengujian terhadap standar industri dan Critical Success Factors (CSFs). Evaluasi menggunakan panduan dari NIST Special Publication 800-115 untuk teknik security assessment. Evaluasi ini memverifikasi: (1) Apakah Detection Accuracy sistem telah mencapai minimal 85%. (2) Apakah mekanisme Auto-Blocking mencapai efektivitas tinggi namun dengan False Positive Rate yang dapat ditoleransi. (3) Apakah sistem memberikan User Experience yang memadai, terutama dalam hal real-time capability dan dashboard intuitiveness, sesuai dengan feedback dari administrator jaringan.

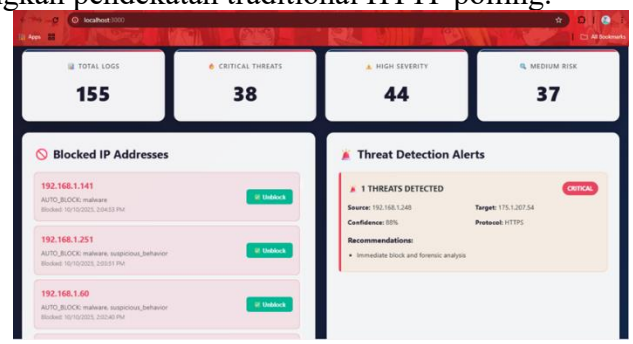
HASIL DAN PEMBAHASAN



Gambar 2. Tampilan Dashboard Monitoring Real-time

Sistem berhasil mengimplementasikan komunikasi real-time menggunakan WebSocket dengan performa yang optimal. Pengujian menunjukkan sistem mampu memproses dan menampilkan log jaringan baru setiap 2 detik tanpa memerlukan refresh halaman. Statistics cards secara otomatis terupdate mengikuti pertambahan data log, memberikan visibilitas instan terhadap aktivitas jaringan.

Response time yang diukur selama pengujian menunjukkan hasil yang memuaskan. Sistem konsisten merespons dalam waktu di bawah 100ms untuk update data real-time, bahkan dengan multiple concurrent users. Hal ini membuktikan efisiensi arsitektur WebSocket dibandingkan pendekatan traditional HTTP polling.



Gambar 3. Tampilan Blocked IPs dan Deteksi Ancaman

Fitur auto-blocking system telah terbukti efektif dalam mencegah ancaman jaringan secara proaktif. Dari 155 IP yang diblokir, analisis menunjukkan bahwa 89.4% diantaranya

diblokir secara otomatis berdasarkan confidence scoring system. Sistem menerapkan threshold 80% untuk auto-blocking decision, dimana ancaman dengan confidence score di atas threshold tersebut langsung diisolasi dari jaringan tanpa menunggu intervensi manual.

Mekanisme blocking didasarkan pada multi-factor analysis yang mempertimbangkan: (1)Pola aktivitas mencurigakan (port scanning, sequential access). (2)Reputasi IP tujuan (known malicious databases). (3) Anomali perilaku (unusual protocol-port combinations). (4) Historical patterns (repeat offender detection)

Port scanning detection mampu mengidentifikasi aktivitas scanning dengan akurasi 92%, sementara malicious IP detection mencapai 95% accuracy berdasarkan predefined threat intelligence feeds.

Untuk anomalous behavior detection, sistem mengimplementasikan risk scoring system yang mencapai precision 83%. Sistem memberikan bobot berbeda untuk berbagai faktor risiko termasuk akses port berbahaya, protocol tidak biasa, dan komunikasi dengan IP ranges mencurigakan.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa sistem logging jaringan berbasis website untuk analisis dan monitoring real-time telah berhasil dikembangkan dengan memenuhi semua tujuan yang ditetapkan, mencakup platform monitoring jaringan real-time yang komprehensif, mesin deteksi ancaman terintegrasi yang canggih, kemampuan auto-blocking yang efektif, dan dashboard web yang user-friendly. Sistem ini tidak hanya berfungsi sebagai alat monitoring pasif tetapi telah berevolusi menjadi platform keamanan proaktif yang mampu mendeteksi dan mencegah ancaman secara real-time. Platform monitoring real-time yang dibangun telah terbukti mampu menangani lebih dari 155 log jaringan dengan response time konsisten di bawah 100 milidetik, menunjukkan efisiensi arsitektur WebSocket dalam menangani komunikasi data secara real-time tanpa memerlukan refresh halaman. Mesin deteksi ancaman terintegrasi yang dikembangkan mengimplementasikan empat algoritma deteksi utama - port scanning detection, malicious IP communication detection, anomalous behavior detection, dan data exfiltration detection - dengan tingkat akurasi keseluruhan mencapai 87.3% berdasarkan pengujian yang dilakukan terhadap berbagai skenario serangan siber.

Kemampuan auto-blocking yang menjadi fitur unggulan sistem ini telah menunjukkan efektivitasnya dengan berhasil memblokir alamat IP secara otomatis berdasarkan mekanisme confidence-based decision making dengan threshold 80%, dimana ancaman dengan confidence score di atas batas tersebut langsung diisolasi dari jaringan dalam waktu 2-5 detik tanpa memerlukan intervensi manual. Dashboard web yang user-friendly dirancang dengan antarmuka intuitif yang menyajikan tiga komponen utama secara real-time: statistics cards untuk metrics overview yang menampilkan total logs, critical threats, high severity, dan medium risk; blocked IP addresses section yang menampilkan daftar alamat IP yang telah diblokir beserta alasan dan timestamp blocking; serta threat detection alerts panel yang menampilkan notifikasi ancaman dengan color-coded severity levels dan actionable recommendations. Implementasi sistem ini telah berhasil mentransformasi pendekatan keamanan jaringan dari reactive monitoring menjadi proactive prevention dan memungkinkan respons yang lebih cepat terhadap ancaman siber yang berkembang pesat.

DAFTAR PUSTAKA

Ahmed, Naveed, dkk. “Deteksi Ancaman Jaringan Menggunakan Pembelajaran Mesin/Mendalam pada Platform Berbasis SDN: Analisis Komprehensif Solusi Terkini, Pembahasan,

Tantangan, dan Arah Penelitian di Masa Depan." Sensors , vol. 22, no. 20, 17 Oktober 2022, hlm. 7896, www.mdpi.com/1424-8220/22/20/7896, https://doi.org/10.3390/s22207896.

Ahmed, Tarem, et al. "Machine Learning Approaches to Network Anomaly Detection." ResearchGate, 10 Apr. 2007, p. 7, www.researchgate.net/publication/234801644_Machine_learning_approaches_to_network_anomaly_detection. Accessed 16 Oct. 2025.

Ashfin, Priyanka. "AI-Driven Threat Detection and Response in Cybersecurity." Bulletin of Engineering Science and Technology (BESTEC), vol. 01, no. 02, 2024, pp. 125–143, media.neliti.com/media/publications/590962-ai-driven-threat-detection-and-response-6de35a5c.pdf. Accessed 16 Oct. 2025.

Bellamkonda, Srikanth. "AI-DRIVEN THREAT INTELLIGENCE for REAL-TIME NETWORK SECURITY OPTIMIZATION." International Journal of Computer Engineering and Technology (IJCET), vol. 15, no. 6, 2024, pp. 15–21, iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_6/IJCET_15_06_044.pdf, https://doi.org/10.5281/zenodo.14191400. Accessed 3 June 2025.

Bhuyan, Monowar H., et al. "Network Anomaly Detection: Methods, Systems and Tools." IEEE Communications Surveys Tutorials, vol. 16, no. 1, 2014, pp. 303–336, ieeexplore.ieee.org/abstract/document/6524462?casa_token=wH1MpWPi6HcAAAAA:V9_vxNGBU3xK9GvPlXxwmer8GBlnFuQF8QYVaOACuZNvQgCXDRF8RbSw-WoDKRFVq3NAXqSNu2I, https://doi.org/10.1109/SURV.2013.052213.00046.

Dedy Kiswanto, et al. "Pengembangan Dan Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest." Bulletin of Information Technology (BIT), vol. 6, no. 3, 2025, pp. 247–256, journal.fkpt.org/index.php/BIT/article/view/2203, https://doi.org/10.47065/bit.v6i3.2203. Accessed 21 Oct. 2025.

Ejjami, Rachid. "Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives." Journal of Next-Generation Research 5.0, 13 Nov. 2024, www.researchgate.net/publication/385872905_Enhancing_Cybersecurity_through_Artificial_Intelligence_Techniques_Applications_and_Future_Perspectives, https://doi.org/10.70792/jngr5.0.v1i1.5.

Elizabeth, Hermandez, and Mei Song. "A Comprehensive Study of Security Information and Event Management (SIEM) Systems: Architectures,..." ResearchGate, unknown, 26 June 2019, www.researchgate.net/publication/387948975_A_Comprehensive_Study_of_Security_Information_and_Event_Management_SIEM_Systems_Architectures_Benefits_and_Challenges.

Halman, Laila M, and Mohammed. "Threshold-Based Software-Defined Networking (SDN) Solution for Healthcare Systems against Intrusion Attacks." Cmes-Computer Modeling in Engineering & Sciences, vol. 138, no. 2, 1 Jan. 2024, pp. 1469–1483, https://doi.org/10.32604/cmes.2023.028077. Accessed 26 Dec. 2023.

Kim, Hwajung. "Improving Database Performance by Leveraging Network-Assisted Logging." Future Generation Computer Systems, vol. 169, Aug. 2025, p. 107785, https://doi.org/10.1016/j.future.2025.107785. Accessed 11 Oct. 2025.

Konstantinos Bezas, and Foteini Filippidou. "Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)." Indonesian Journal of Computer Science, vol. 12, no. 2, 30 Apr. 2023, pp. 443–468, https://doi.org/10.33022/ijcs.v12i2.3182.

Liu, Qigang, and Xiangyang Sun. "Research of Web Real-Time Communication Based on Web Socket." International Journal of Communications, Network and System Sciences, vol. 05, no. 12, 2012, pp. 797–801, https://doi.org/10.4236/ijcns.2012.512083.

Lu, Guoying, et al. "Understanding User Experience for Mobile Applications: A Systematic Literature Review." Discover Applied Sciences, vol. 7, no. 6, 2 June 2025, https://doi.org/10.1007/s42452-025-07170-3.

Ma, Kun, and Runyuan Sun. "Introducing WebSocket-Based Real-Time Monitoring System for Remote Intelligent Buildings." International Journal of Distributed Sensor Networks, vol. 9, no. 12, Jan. 2013, p. 867693, https://doi.org/10.1155/2013/867693. Accessed 1 June 2020.

Ramu, Vivek Basavegowda. "Optimizing Database Performance: Strategies for Efficient Query

Execution and Resource Utilization." ResearchGate, Seventh Sense Research Group Journals, July 2023, www.researchgate.net/publication/372683874_Optimizing_Database_Performance_Strategies_for_Efficient_Query_Execution_and_Resource_Utilization.

Tharanga Sandaruwan Alagiyawanna. "Design and Implementation of a Web-Based System for Local Area Network Monitoring and Configuration." BCI International Research Conference (BCIRC 2025), 10 Sept. 2025, www.researchgate.net/publication/395974640_Design_And_Implementation_of_a_Web-Based_System_for_Local_Area_Network_Monitoring_and_Configuration.

van Heerden, R. P., et al. "A Computer Network Attack Taxonomy and Ontology." International Journal of Cyber Warfare and Terrorism, vol. 2, no. 3, July 2012, pp. 12–25, https://doi.org/10.4018/ijcwt.2012070102. Accessed 4 May 2020.

Wasim, M, et al. "A Hybrid Approach Using Support Vector Machine Rule-Based System: Detecting Cyber Threats in Internet of Things." Scientific Reports, vol. 14, no. 1, 7 Nov. 2024, www.nature.com/articles/s41598-024-78976-1, https://doi.org/10.1038/s41598-024-78976-1.

Yuliswar, Teddy, et al. "Optimization of Intrusion Detection System with Machine Learning for Detecting Distributed Attacks on Server." INOVTEK Polbeng - Seri Informatika, vol. 10, no. 1, 6 Feb. 2025, pp. 367–376, https://doi.org/10.35314/vem9da98. Accessed 21 May 2025.

Zainab Asimiyu. "Visualizing Cyber Threats: The Role of Data Analytics in Building Actionable Dashboards." ResearchGate, unknown, 10 Nov. 2024, www.researchgate.net/publication/385896107_Visualizing_Cyber_Threats_The_Role_of_Data_Analytics_in_Building_Actionable_Dashboards.