KUADRAN
Jurnal Analitika Data dan Ilmu Komputer

Published by PT Yetti Afrida Center Bengkulu
e-ISSN: 3165-3677 | p-ISSN: 3165-3723
Vol. 1 No. 1 Oktober 2026 | Pages 57-70
https://yettiafridacenter.com/kuadran
This Article is licensed under a CC BY-SA 4.0 International License

Pengembangan Sistem Deteksi Anomali Berbasis Artificial Intelligence untuk Meningkatkan Keamanan Informasi dan Ketahanan Sistem Digital

Khairil*
Universitas Dehasen Bengkulu, Indonesia
Email: khairil@unived.ac.id

ABSTRACT

Purpose: *This study develops a conceptual architecture for artificial-intelligence-based anomaly detection to improve information security and the operational resilience of digital systems amid evolving cyber threats.*

Design/Methodology: *A critical methodological review integrates statistical baselines, supervised and unsupervised learning, autoencoders, sequence models, and risk-oriented incident response. Model design, data pipelines, evaluation criteria, governance, and deployment are analyzed without asserting any unperformed experiment.*

Findings: *Anomaly detection can identify deviations not captured by static signatures, but effectiveness depends on representative data, realistic temporal validation, calibrated alerts, adversarial robustness, and responses that do not disrupt essential services.*

Practical Implications: *The proposed layered workflow supports security operations teams in prioritizing alerts, measuring false positives, identifying drift, preserving audit trails, and coordinating detection with recovery and continuity planning.*

Originality/Value: *The synthesis connects predictive anomaly scoring with resilient system operation through a transparent framework encompassing detection, human verification, adaptive response, and continuous model assurance.*

Keywords: *anomaly detection; artificial intelligence; cybersecurity; digital resilience; machine learning; threat monitoring.*

Received: 18/09/2026 Accepted: 25/09/2026 Published: 12/10/2026

A. INTRODUCTION (PENDAHULUAN)

Latar Belakang dan Tujuan Penelitian

Perluasan layanan berbasis komputasi awan, sistem informasi organisasi, perangkat terhubung, dan aplikasi daring membuat keamanan informasi menjadi prasyarat kesinambungan layanan. Infrastruktur digital menghasilkan catatan transaksi, lalu lintas jaringan, aktivitas akun, perubahan konfigurasi, serta peristiwa autentikasi dalam volume besar. Pola aktivitas normal berbeda menurut waktu dan fungsi pengguna. Keadaan tersebut menjadikan pendekatan pemeriksaan manual dan aturan statis semakin sulit diterapkan sebagai satu-satunya mekanisme pengawasan. Anomali dapat muncul sebagai peningkatan permintaan mendadak, pola akses tidak lazim, atau perubahan komunikasi antarperangkat yang tidak sejalan dengan kebiasaan operasional.

Ancaman terhadap sistem digital tidak terbatas pada serangan yang mempunyai tanda tangan dikenal. Penyalahgunaan kredensial sah, pergerakan lateral, percobaan eksploitasi berulang, perubahan hak akses, dan aktivitas otomatis yang tersembunyi dapat menunjukkan kemiripan dengan pekerjaan pengguna normal. Teknologi artificial intelligence menawarkan kemampuan mengenali pola multidimensi pada data telemetri dan memberi skor penyimpangan sebelum tanda tangan eksplisit tersedia. Namun, pemberian skor tidak sama dengan pembuktian adanya insiden. Setiap hasil perlu ditafsirkan berdasarkan konteks bisnis, cakupan sensor, kualitas data, serta potensi konsekuensi tindakan yang menyusul.

Ketahanan sistem digital atau digital resilience melampaui kemampuan mengidentifikasi serangan. Sistem yang tangguh perlu mampu mempertahankan layanan penting, membatasi dampak insiden, memulihkan operasi, dan belajar dari kegagalan. Deteksi anomali yang sangat sensitif dapat berkontribusi pada respons cepat, tetapi juga menghasilkan banyak peringatan salah dan menghabiskan kapasitas petugas keamanan. Sebaliknya, ambang yang terlalu ketat

This Article is licensed under a CC BY-SA 4.0 International License

mungkin melewatkan kegiatan berbahaya. Persoalan desain utamanya adalah menempatkan deteksi dalam rantai keputusan yang mempertimbangkan risiko operasional dan kebutuhan kesinambungan, bukan sekadar meningkatkan jumlah peringatan.

Artikel ini bertujuan mengembangkan kerangka konseptual sistem deteksi anomali berbasis AI yang menggabungkan sumber data, pemodelan, evaluasi, pengawasan manusia, dan respons insiden secara terpadu. Pertanyaan kajian meliputi karakteristik anomali pada lingkungan digital, pilihan metode pembelajaran mesin yang sesuai, prosedur validasi yang mencegah kebocoran data, serta cara menghubungkan skor model dengan tindakan yang proporsional. Penelitian bersifat telaah metodologis dan desain arsitektur konseptual; tidak ada klaim penggunaan data lalu lintas organisasi tertentu ataupun peningkatan akurasi empiris yang belum diukur.

B. LITERATURE REVIEW (KAJIAN PUSTAKA)

Konsep Anomali dan Lanskap Ancaman

Anomali adalah pengamatan atau rangkaian peristiwa yang menyimpang dari pola acuan yang dipelajari atau ditentukan. Penyimpangan titik dapat berupa satu permintaan dengan ukuran sangat besar, sedangkan anomali kontekstual baru tampak setelah memperhatikan jam operasional, perangkat, atau peran pengguna. Anomali kolektif muncul ketika beberapa tindakan yang masing-masing terlihat lazim membentuk urutan mencurigakan. Perbedaan tersebut penting karena algoritma yang menilai setiap peristiwa secara terpisah mungkin gagal mendeteksi serangan bertahap. Kerangka klasifikasi anomali membantu menentukan unit analisis dan kebutuhan fitur.

Keamanan jaringan sering menggunakan log firewall, catatan DNS, aliran paket, data endpoint, informasi identitas, dan audit konfigurasi. Setiap sumber mempunyai cakupan dan keterbatasan. Log jaringan dapat menunjukkan koneksi asing namun tidak selalu menjelaskan proses yang memulainya; catatan endpoint memberi konteks proses tetapi bisa tidak lengkap ketika agen berhenti; audit identitas menjelaskan autentikasi tetapi belum tentu membuktikan maksud pengguna. Penggabungan data lintas sumber dapat meningkatkan pemahaman situasi, tetapi mensyaratkan penyelarasan waktu, identitas entitas, dan kebijakan retensi yang memadai.

Literatur intrusion detection membedakan pendekatan berbasis aturan, tanda tangan, statistik, dan pembelajaran. Sistem berbasis tanda tangan efektif untuk pola serangan yang telah dikenali, sedangkan deteksi anomali mencoba mengenali penyimpangan terhadap kondisi referensi. Kedua pendekatan sebaiknya tidak dipertentangkan sebagai pengganti mutlak. Dalam arsitektur pertahanan berlapis, peringatan tanda tangan dapat memberi bukti spesifik sementara skor anomali menyediakan sinyal tambahan. Penggunaan bersama membutuhkan mekanisme penggabungan dan prioritisasi agar petugas tidak menerima beberapa peringatan terpisah untuk satu peristiwa.

Pola operasional berubah secara alamiah ketika organisasi menerapkan aplikasi baru, terjadi pembaruan sistem, atau jumlah pengguna meningkat. Akibatnya, konsep normal bukan konstanta. Algoritma yang dilatih pada satu periode dapat salah memberi alarm setelah perubahan sistem yang sah. Kesulitan ini sering disebut pergeseran data dan perubahan konsep. Model perlu dinilai bukan hanya pada kumpulan data historis yang sudah dibersihkan, tetapi pada aliran data yang mengandung perubahan konfigurasi, fluktuasi musiman, dan perilaku pengguna yang tidak stabil.

This Article is licensed under a CC BY-SA 4.0 International License

Vol. 1 No. 1, Oktober 2026, hal. 57–70 e-ISSN: 3165-3677 | p-ISSN: 3165-3723

B. LITERATURE REVIEW (KAJIAN PUSTAKA)

Pendekatan Statistik dan Pembelajaran Mesin

Deteksi sederhana menggunakan nilai ambang, skor baku, atau ukuran jarak terhadap pusat sebaran. Metode statistik tersebut murah, mudah diperiksa, dan dapat menjadi baseline penting. Akan tetapi, perilaku jaringan sering mempunyai distribusi miring, kejadian jarang, dan korelasi antarfaktor. Nilai permintaan yang tinggi mungkin normal pada server tertentu tetapi tidak lazim pada endpoint pengguna. Pendekatan statistik perlu mempertimbangkan pengelompokan aset serta perbedaan jendela waktu sebelum menetapkan nilai ambang yang layak.

Metode tanpa label, seperti isolation forest, local outlier factor, dan one-class support vector machine, memanfaatkan struktur data untuk memberi skor keanehan. Isolation forest memisahkan pengamatan menggunakan pemartisian acak dan dapat berguna pada fitur terstruktur; metode kerapatan membandingkan tetangga lokal; one-class classifier berupaya memodelkan daerah data referensi. Keunggulan metode tanpa label adalah tidak selalu membutuhkan katalog serangan yang lengkap. Keterbatasannya, kejadian langka yang sah juga dapat tampak anomali, sehingga skor semata tidak menyediakan bukti bahwa suatu aktivitas melanggar keamanan.

Pembelajaran terawasi memanfaatkan data normal dan serangan yang telah diberi label untuk membangun pemisah kelas. Keluarga pohon keputusan, random forest, dan gradient boosting dapat menjadi kandidat pada fitur tabular, sedangkan jaringan saraf memerlukan pertimbangan kompleksitas dan ukuran sampel. Kinerja tinggi pada kumpulan data pelatihan tidak berarti kemampuan mendeteksi teknik penyerang yang berbeda di masa depan. Label dapat mengandung kesalahan dan serangan yang tidak tampak pada pengamatan kemungkinan dinyatakan normal. Oleh karena itu, model terawasi perlu melaporkan batas cakupan kategori serangan.

Metode pembelajaran representasi, seperti autoencoder, berupaya merekonstruksi pola masukan dan menggunakan galat rekonstruksi sebagai petunjuk penyimpangan. Pada data berurutan, pendekatan temporal dapat memodelkan hubungan aktivitas antarwaktu. Nilai galat yang besar tidak otomatis membuktikan serangan, sebab perubahan format log, hilangnya data, dan kejadian langka yang sah juga dapat mengubah rekonstruksi. Pemilihan arsitektur sebaiknya mengikuti struktur data dan kebutuhan respons, bukan mengikuti kecanggihan nama metode semata.

B. LITERATURE REVIEW (KAJIAN PUSTAKA)

Keamanan Informasi dan Ketahanan Operasional

Keamanan informasi pada umumnya menekankan kerahasiaan, integritas, dan ketersediaan. Deteksi anomali dapat mendukung ketiganya melalui identifikasi akses tidak wajar, perubahan data yang mencurigakan, dan konsumsi sumber daya yang mengganggu layanan. Akan tetapi, satu sistem model tidak dapat menggantikan pengelolaan identitas, pencadangan, segmentasi jaringan, pengujian pemulihan, dan tata kelola kerentanan. Model perlu dipandang sebagai komponen informasi situasional yang memperkuat kontrol organisasi yang telah ada.

Ketahanan operasional membutuhkan toleransi terhadap gangguan dan kemampuan kembali ke keadaan layanan yang dapat diterima. Alarm yang datang lebih awal dapat memperpendek waktu investigasi hanya jika personel, proses eskalasi, dan kewenangan tindakan telah didefinisikan. Alarm tanpa konteks dapat meningkatkan beban dan menunda penanganan. Oleh

This Article is licensed under a CC BY-SA 4.0 International License

karena itu, desain antarmuka harus menampilkan aset terdampak, pola penyimpangan, data pendukung, tingkat keyakinan, serta tindakan aman yang dapat diuji ulang oleh analis.

Pengendalian otomatis berisiko menyebabkan penghentian layanan sah. Menonaktifkan akun berdasarkan skor tunggal dapat menghambat pekerjaan penting, sementara memutus koneksi server dapat memperburuk insiden ketersediaan. Tindakan otomatis layak dipilah berdasarkan dampak dan reversibilitas. Pengayaan log, pemantauan intensif, serta pembatasan sementara yang mudah dibalik sering lebih aman daripada tindakan destruktif. Untuk sistem kritis, persetujuan manusia dan jalur eskalasi yang jelas tetap diperlukan.

Kerangka kerja keamanan siber seperti NIST Cybersecurity Framework menyediakan bahasa organisasi untuk memahami, melindungi, mendeteksi, merespons, dan memulihkan. Penggunaan AI seharusnya membantu berbagai fungsi tersebut tanpa mengaburkan tanggung jawab. Kesuksesan deteksi bukan hanya keluaran teknis berupa skor model, melainkan penurunan dampak insiden, peningkatan keterlacakan, dan pembelajaran dari kejadian. Ukuran manfaat harus terkait dengan operasi nyata dan perlu dipisahkan dari hasil pengujian laboratorium.

C. METHOD (METODE)

Desain Kajian dan Kerangka Pengembangan

Penelitian menggunakan kajian metodologis konseptual yang menelaah literatur deteksi anomali, pembelajaran mesin, pengukuran performa, dan ketahanan digital. Tahapan analisis meliputi identifikasi kebutuhan sistem, pemilihan sumber telemetri, rancangan prapemrosesan, pembandingan kandidat model, serta formulasi tata kelola respons. Referensi dasar digunakan untuk menjelaskan mekanisme algoritma, sedangkan dokumen kerangka keamanan mendukung penempatan deteksi dalam proses organisasi. Kajian ini tidak menggunakan data primer dan tidak melaporkan eksperimen tersamar sebagai temuan empiris.

Unit analisis harus ditentukan sebelum pengumpulan data. Pilihannya mencakup peristiwa tunggal, sesi autentikasi, aliran jaringan, entitas pengguna, perangkat, atau urutan aktivitas per interval waktu. Setiap pilihan memengaruhi interpretasi penyimpangan. Deteksi pada tingkat sesi dapat menemukan pola kegagalan autentikasi berulang, sementara pengawasan entitas berguna untuk menilai akumulasi perubahan perilaku. Penggabungan unit yang tidak sebanding tanpa normalisasi dapat membuat server bertrafik tinggi selalu tampak lebih mencurigakan.

Kerangka desain dimulai dari tujuan risiko: kejadian seperti akses tidak sah, pemindahan data abnormal, atau gangguan ketersediaan. Dari setiap skenario diturunkan sumber log, fitur, unit waktu, toleransi kesalahan, dan batas waktu respons. Prosedur ini memastikan data dikumpulkan untuk menjawab kebutuhan keamanan yang nyata. Penelitian berikutnya perlu merumuskan kriteria keberhasilan sebelum model diuji, sehingga hasil tidak dipilih secara selektif setelah mengetahui skor pengujian.

Pembandingan metode harus menggunakan baseline yang mudah dijelaskan, seperti ambang statistik atau aturan domain, sebelum kandidat AI yang lebih kompleks. Pengaturan hiperparameter dilakukan hanya menggunakan data pelatihan dan validasi. Dataset pengujian final diperlakukan sebagai sumber evaluasi independen, bukan bahan untuk memperbaiki model berkali-kali. Jika catatan berasal dari perangkat yang sama secara berulang, rancangan pembagian berdasarkan entitas atau periode harus digunakan agar independensi penilaian lebih mendekati kondisi penerapan.

This Article is licensed under a CC BY-SA 4.0 International License

Vol. 1 No. 1, Oktober 2026, hal. 57–70 e-ISSN: 3165-3677 | p-ISSN: 3165-3723

C. METHOD (METODE)

Pipeline Data dan Kualitas Telemetri

Data dari berbagai log terlebih dahulu melalui inventarisasi skema, penyeragaman waktu, pemeriksaan duplikasi, dan pemetaan identitas entitas. Penghilangan kolom yang tidak perlu atau bersifat rahasia mengurangi risiko privasi dan kebocoran. Fitur dapat mencakup frekuensi login, perubahan lokasi akses, jumlah tujuan jaringan, interval antarperistiwa, perubahan proses, dan variasi volume komunikasi. Nilai fitur harus dihitung menggunakan informasi yang benar-benar tersedia pada saat prediksi, bukan data yang baru diketahui setelah insiden.

Ketidaklengkapan log tidak boleh diperlakukan sekadar sebagai nilai nol. Hilangnya catatan dapat disebabkan kegagalan agen, gangguan jaringan, perubahan izin, atau kesengajaan penyerang. Setiap penyebab memiliki konsekuensi yang berbeda. Penambahan indikator ketidaktersediaan data serta pengukuran kesehatan sensor membantu membedakan aktivitas abnormal dari masalah observasi. Pipeline harus mendokumentasikan waktu hilang, laju keterlambatan, dan proses penggabungan sumber yang tidak sinkron.

Standardisasi dan transformasi fitur memerlukan perhatian khusus. Nilai count sering berdistribusi menceng dan dapat membutuhkan transformasi yang mempertahankan interpretasi. Variabel kategorikal seperti jenis protokol atau peran akun harus diolah tanpa menciptakan kategori berurutan palsu. Semua parameter transformasi dipelajari hanya dari bagian data pelatihan pada setiap putaran validasi. Jika keseluruhan dataset dipakai menentukan ambang atau pemetaan kategori sebelum pembagian, evaluasi dapat menjadi terlalu optimistis.

Privasi dan keamanan log sama pentingnya dengan keamanan aplikasi yang dipantau. Data autentikasi dapat mengandung identitas personal, alamat internal, dan kebiasaan bekerja. Kebijakan retensi, pembatasan akses berbasis peran, perlindungan enkripsi, serta pencatatan akses analis perlu ditetapkan. Data uji yang dibagikan ke peneliti dapat dianonimkan sesuai tujuan, meskipun anonimisasi tidak selalu menghilangkan risiko pengaitan ulang. Tata kelola tersebut harus terintegrasi sejak rancangan pengumpulan data.

C. METHOD (METODE)

Strategi Validasi dan Metrik Pengukuran

Serangan siber relatif jarang dibanding kegiatan normal, sehingga akurasi klasifikasi total dapat menyesatkan. Model yang selalu menandai normal mungkin memperoleh akurasi tampak tinggi ketika data didominasi aktivitas sah. Evaluasi membutuhkan precision, recall, false positive rate, serta kurva precision-recall untuk kategori yang relevan. Jumlah peringatan per hari per seribu entitas juga penting karena menunjukkan beban operasional yang akan dihadapi petugas, bukan hanya proporsi statistik.

Validasi temporal menguji apakah model yang dilatih pada periode awal dapat bekerja pada periode berikutnya. Pembagian acak antara catatan waktu berdekatan dapat membocorkan kesamaan kejadian dan membuat skor tidak realistis. Bila satu rangkaian serangan menghasilkan ribuan peristiwa, seluruh kejadian yang berhubungan semestinya dijaga berada dalam partisi yang sesuai. Uji lintas perangkat atau lintas lokasi dapat membantu menilai transferabilitas, sedangkan perubahan perangkat lunak perlu dicatat untuk menafsirkan penurunan performa.

Ketepatan skor juga dapat dinilai melalui kalibrasi atau pemetaan ke risiko yang dapat ditafsirkan. Sebuah nilai anomali 0,9 tidak otomatis berarti peluang serangan 90 persen. Probabilitas memerlukan prosedur kalibrasi dan definisi target yang jelas. Ambang keputusan

This Article is licensed under a CC BY-SA 4.0 International License

harus ditetapkan sesuai biaya peringatan salah, konsekuensi kejadian terlewat, dan kapasitas investigasi. Analisis sensitivitas pada beberapa ambang membantu pengambil keputusan memahami trade-off sebelum sistem digunakan.

Kecepatan deteksi merupakan dimensi evaluasi yang berbeda dari ketepatan klasifikasi. Tindakan yang teridentifikasi setelah insiden selesai mungkin bernilai terbatas untuk respons langsung tetapi tetap berguna bagi forensik. Karena itu, penelitian lanjutan perlu melaporkan waktu dari munculnya aktivitas sampai peringatan, waktu pengayaan data, serta keterlambatan eskalasi. Pengukuran ketahanan operasional kemudian menghubungkan deteksi dengan waktu pembatasan dampak dan pemulihan layanan.

D. RESULT AND DISCUSSION (HASIL DAN PEMBAHASAN)

Arsitektur Sistem Deteksi Anomali Berlapis

Analisis konseptual menghasilkan rancangan berlapis yang mencakup pengumpulan telemetri, pengendalian kualitas data, pembentukan fitur, pemberian skor oleh model, korelasi kejadian, verifikasi analis, dan tindakan respons. Lapisan pengumpulan memprioritaskan sumber yang berkaitan dengan aset kritis. Lapisan kualitas memeriksa keterlambatan dan kehilangan catatan. Lapisan analitik menghasilkan skor beserta bukti pendukung. Lapisan operasi menggabungkan kejadian menurut identitas pengguna, perangkat, dan periode agar satu rangkaian perilaku tidak dipecah menjadi puluhan alarm tanpa hubungan.

Arsitektur harus memisahkan model pengukuran dari mesin keputusan. Model hanya menghasilkan penilaian statistik berdasarkan data yang tersedia, sementara mesin keputusan menggabungkan skor dengan klasifikasi aset, sensitivitas layanan, dan aturan organisasi. Akun administratif yang melakukan akses tidak lazim pada server penting mungkin memerlukan prioritas berbeda dari perubahan kecil pada perangkat uji. Pemisahan ini meningkatkan keterjelasan kebijakan: pembaruan model tidak harus secara otomatis mengubah tingkat kewenangan tindakan.

Sistem penyimpanan bukti perlu menjamin bahwa rangkaian kegiatan dapat diperiksa kembali. Setiap peringatan sebaiknya memiliki cap waktu, versi model, rentang fitur, identitas sumber, penjelasan faktor penyimpangan, dan keputusan analis. Pelacakan versi memungkinkan organisasi mengetahui mengapa skor berubah setelah pelatihan ulang. Dokumentasi tersebut mendukung audit keamanan serta analisis kesalahan model. Tanpa jejak, sebuah sistem canggih justru menyulitkan pemeriksaan keputusan ketika terjadi insiden serius.

Keseluruhan rancangan perlu mengantisipasi kegagalan komponen. Saat layanan AI tidak tersedia, pengumpulan log dan kontrol dasar harus tetap berjalan. Mekanisme fallback berupa aturan sederhana dan alarm kesehatan sensor dapat menjaga sebagian fungsi keamanan. Pengujian pemulihan perlu mencakup kegagalan konektivitas, lonjakan trafik, dan gangguan penyimpanan. Prinsip ini memperlihatkan bahwa ketahanan tidak berasal dari algoritma yang selalu aktif, melainkan dari rancangan layanan yang mampu menoleransi degradasi parsial.

D. RESULT AND DISCUSSION (HASIL DAN PEMBAHASAN)

Pemilihan Model dan Penggabungan Bukti

Pilihan model dapat dikelompokkan menurut kebutuhan label dan bentuk data. Pada telemetri tabular yang sedikit label insidennya, model anomali tanpa pengawasan layak dipertimbangkan sebagai alat penyaringan. Jika terdapat label insiden yang dipercaya, klasifikasi terawasi dapat digunakan untuk skenario serangan tertentu. Untuk urutan kegiatan, model temporal menilai hubungan antarevent. Tidak ada satu arsitektur yang tepat untuk

This Article is licensed under a CC BY-SA 4.0 International License

seluruh skenario; perbandingan harus memperhitungkan biaya komputasi, interpretabilitas, dan tingkat kestabilan saat pola normal berubah.

Metode ensemble dapat menggabungkan skor dari baseline statistik, isolasi anomali, dan aturan domain. Penggabungan sebaiknya dilakukan secara hati-hati karena skor mentah dari berbagai algoritma sering tidak sebanding. Normalisasi berdasarkan data pelatihan dan pengujian korelasi keluaran membantu mencegah penghitungan bukti yang sama berulang kali. Model yang hampir identik dapat menghasilkan kesepakatan tinggi tanpa menambah informasi. Nilai penggabungan perlu diuji pada kejadian berbeda, bukan diasumsikan lebih baik hanya karena menggunakan lebih banyak algoritma.

Keterjelasan alasan peringatan penting untuk penyaringan awal. Analis perlu mengetahui fitur mana yang menyimpang dari pola referensi, apakah perubahan terjadi mendadak atau bertahap, dan apakah sensor lain menguatkan dugaan. Teknik interpretasi lokal dapat memberi indikasi kontribusi fitur, tetapi hasil penjelasan tidak selalu bersifat kausal. Model dapat memanfaatkan artefak data yang tidak relevan secara keamanan. Oleh sebab itu, penjelasan yang dihasilkan perlu dibandingkan dengan log mentah serta pengetahuan petugas tentang sistem.

Sebuah ilustrasi konseptual adalah akun yang biasanya mengakses satu aplikasi pada jam kerja kemudian mencoba banyak layanan internal dalam waktu singkat. Baseline frekuensi dapat mengenali peningkatan jumlah tujuan, model urutan dapat membaca perubahan pola interaksi, dan audit identitas dapat memberi konteks autentikasi. Ketiga sinyal memperkuat alasan penyelidikan, tetapi belum membuktikan kompromi akun. Peningkatan hak akses yang sah selama pemeliharaan atau pengujian juga dapat menghasilkan pola serupa. Konfirmasi konteks menjadi bagian esensial sebelum pembatasan dilakukan.

D. RESULT AND DISCUSSION (HASIL DAN PEMBAHASAN)

False Positive, False Negative, dan Pengambilan Keputusan

Peringatan salah positif merupakan masalah operasional karena mengonsumsi waktu, meningkatkan kejenuhan petugas, dan berisiko menurunkan kepercayaan terhadap sistem. Sebaliknya, false negative membiarkan sebagian tindakan berbahaya tidak terdeteksi. Keseimbangan antara keduanya tidak dapat ditentukan dari angka akurasi tunggal. Organisasi perlu mengaitkan ambang model dengan nilai aset, urgensi peristiwa, serta sumber daya investigasi. Ambang dinamis dimungkinkan tetapi harus diaudit agar perubahan kebijakan tidak terjadi tanpa pengawasan.

Prioritisasi dapat memakai pendekatan berlapis: peringatan berisiko rendah masuk pemantauan, peringatan sedang memicu pemeriksaan manual, dan peringatan tinggi yang didukung beberapa sumber dapat mengaktifkan respons terukur. Namun, tinggi rendahnya risiko harus didefinisikan oleh gabungan kemungkinan dan dampak, bukan oleh skor AI semata. Server yang memproses data sensitif dapat memerlukan penanganan berbeda dari komputer laboratorium. Klasifikasi aset yang usang bisa membuat sistem memberi prioritas salah meskipun model statistiknya bekerja dengan baik.

Penyajian peringatan juga memengaruhi mutu keputusan. Daftar alarm yang terlalu panjang tanpa pengelompokan dapat memaksa analis memeriksa peristiwa duplikat. Korelasi kejadian, kronologi interaktif, dan ringkasan bukti dapat mempercepat penilaian. Namun, ringkasan otomatis harus menyertakan tautan ke data sumber agar kesalahan interpretasi dapat dilacak. Petugas perlu dapat menyatakan alarm salah, kejadian sah, insiden belum pasti, atau kompromi yang dikonfirmasi sehingga hasil investigasi menjadi umpan balik yang lebih terstruktur.

This Article is licensed under a CC BY-SA 4.0 International License

Dampak pengendalian salah juga perlu dinilai. Pemutusan sambungan jaringan untuk mengatasi anomali dapat menghentikan proses bisnis yang penting. Karena itu, tindakan respons hendaknya mempertimbangkan kesempatan pembalikan, isolasi terbatas, serta keberadaan proses pengganti. Protokol pengujian sebelum produksi dapat mensimulasikan skenario salah positif dalam lingkungan terkendali untuk memastikan keamanan proses eskalasi. Dengan demikian, model yang baik harus menekan risiko keseluruhan, bukan sekadar menambah penangkapan peristiwa.

D. RESULT AND DISCUSSION (HASIL DAN PEMBAHASAN)

Model Drift, Serangan Adversarial, dan Keandalan

Kinerja model dapat menurun ketika distribusi trafik berubah karena penambahan layanan atau migrasi infrastruktur. Perubahan tersebut dapat memengaruhi fitur yang sebelumnya stabil. Pemantauan drift memerlukan baseline distribusi, pengamatan tingkat alarm, dan pemeriksaan perubahan hubungan skor terhadap insiden yang dikonfirmasi. Peningkatan jumlah alarm tidak selalu berarti serangan meningkat; bisa jadi model sedang mendeteksi konfigurasi baru yang sah. Investigasi perlu membandingkan perubahan telemetri dengan kalender perubahan sistem sebelum memutuskan pelatihan ulang.

Penyerang yang memahami mekanisme deteksi dapat mencoba menyesuaikan perilaku agar tampak normal, memecah aktivitas besar menjadi tindakan kecil, atau memanipulasi data yang masuk model. Risiko adversarial ini menuntut perhatian pada kualitas sumber log, pengamanan integritas pipeline, serta pemeriksaan model terhadap skenario yang tidak terlihat saat pelatihan. Pengujian ketahanan tidak sama dengan memberikan petunjuk serangan; fokusnya ialah mengukur kelemahan sistem secara terkendali dan menetapkan kontrol pertahanan yang sesuai.

Pelatihan ulang otomatis menggunakan data terbaru dapat menimbulkan masalah apabila periode baru mengandung aktivitas berbahaya yang belum dikenali. Pola serangan yang sering muncul dapat dianggap normal oleh sistem dan membuat ambang semakin longgar. Untuk mengurangi risiko, dataset pembaruan perlu diseleksi dan dipisahkan antara aktivitas terverifikasi dengan periode berstatus tidak pasti. Retensi benchmark yang tetap membantu membandingkan versi baru terhadap versi sebelumnya. Setiap pembaruan perlu memiliki jalur rollback bila alarm melonjak atau kasus penting tidak lagi terdeteksi.

Ketahanan AI juga terkait dengan transparansi dependensi perangkat lunak, pengaturan akses model, dan kepastian versi fitur. Pipeline yang menghasilkan nilai fitur berbeda setelah pembaruan dapat menurunkan performa tanpa terlihat sebagai kegagalan model. Kontrak skema, pengujian integrasi, dan pemeriksaan kualitas data perlu dilakukan secara berkala. Ketika sistem digunakan lintas organisasi, perbedaan hak akses atau format telemetri harus dinilai sebelum parameter dari lingkungan lain diterapkan kembali.

D. RESULT AND DISCUSSION (HASIL DAN PEMBAHASAN)

Evaluasi Ketahanan dan Tanggung Jawab Sistem

Keberhasilan deteksi anomali perlu dinilai dengan indikator yang relevan terhadap respons insiden. Waktu rata-rata menemukan kejadian, waktu melakukan triase, waktu membatasi dampak, serta kemampuan mengembalikan layanan dapat memperlihatkan manfaat operasional. Indikator itu dipengaruhi proses manusia dan kontrol sistem lain; peningkatannya tidak boleh otomatis diatribusikan kepada AI tanpa rancangan evaluasi yang memadai. Perbandingan sebelum dan setelah implementasi harus mempertimbangkan perubahan volume insiden, infrastruktur, dan kebijakan pengawasan.

This Article is licensed under a CC BY-SA 4.0 International License

Pengujian kesiapan dapat menggunakan simulasi insiden yang disepakati oleh organisasi, dengan pengamanan agar layanan tidak terganggu. Tujuan simulasi adalah memeriksa apakah data tersedia, alarm muncul tepat waktu, penjelasan cukup membantu, dan prosedur eskalasi berjalan. Keberhasilan skenario tertentu tidak membuktikan cakupan seluruh jenis ancaman. Pengujian perlu dipadukan dengan peninjauan log kejadian nyata yang telah ditangani dan analisis alarm yang tidak terkonfirmasi.

Sistem deteksi harus mempunyai pemilik yang bertanggung jawab atas model, data, dan tindakan. Tim keamanan bertanggung jawab terhadap interpretasi ancaman, tim data mengawasi kualitas pipeline dan model, sedangkan pengelola sistem menentukan tindakan terhadap layanan kritis. Kewenangan yang jelas mencegah keputusan otomatis dijalankan tanpa otorisasi. Kebijakan juga perlu menjelaskan kapan hasil model dapat diabaikan, bagaimana ketidaksepakatan analis dicatat, dan bagaimana masalah keamanan model dilaporkan serta diperbaiki.

Keterlacakan audit mendukung evaluasi ilmiah dan organisasi. Versi model, parameter, tanggal pelatihan, sumber data, perubahan ambang, serta catatan respons harus dapat ditelusuri. Ketika insiden besar terjadi, organisasi perlu membedakan kegagalan observasi, keterbatasan model, kesalahan eskalasi, dan respons yang tidak tepat. Analisis pascainsiden yang transparan memungkinkan perbaikan sistematis dan mencegah ketergantungan berlebihan pada satu teknologi keamanan.

D. RESULT AND DISCUSSION (HASIL DAN PEMBAHASAN)

Penerapan di Organisasi dan Prioritas Riset

Penerapan bertahap dapat dimulai dari inventaris aset penting dan audit ketersediaan log sebelum memilih model AI. Organisasi yang belum mempunyai pencatatan waktu dan identitas konsisten akan kesulitan menafsirkan keluaran algoritma. Pilot pada satu kelompok sistem memungkinkan pengukuran volume alarm, penanganan kasus, dan biaya operasional. Setelah perilaku model dipahami, cakupan dapat diperluas disertai dokumentasi perbedaan data dan risiko pada lingkungan berikutnya. Strategi ini lebih realistis daripada menempatkan satu model pada seluruh jaringan tanpa segmentasi konteks.

Bagi perguruan tinggi dan lembaga layanan publik, ragam akun mahasiswa, pegawai, administrator, dan layanan daring menimbulkan pola akses berbeda. Kalender akademik, periode pendaftaran, serta penyelenggaraan ujian dapat mengubah lonjakan trafik yang dianggap wajar. Detektor yang tidak memperhitungkan jadwal tersebut dapat menghasilkan alarm tinggi pada saat layanan paling dibutuhkan. Penetapan konteks kalender dan tipe aset menjadi bagian desain, sementara perlindungan data pengguna dan hak akses terhadap log harus tetap dijaga.

Agenda penelitian selanjutnya meliputi evaluasi lintas periode dan institusi, pembelajaran pada label terbatas, kemampuan menjelaskan peringatan, serta ketahanan terhadap perubahan skema log. Penerapan edge analytics atau federated learning dapat dipertimbangkan ketika data sensitif tidak boleh dipusatkan, tetapi manfaat dan biayanya harus diuji. Perbandingan dengan metode statistik sederhana tetap diperlukan untuk mengetahui kapan kompleksitas AI benar-benar menghasilkan nilai tambah. Pelaporan harus memuat dataset, periode, label, metrik yang sesuai dengan ketimpangan kelas, serta batas generalisasi.

Penelitian yang lebih matang juga sebaiknya menilai hubungan deteksi dengan pemulihan layanan. Misalnya, apakah peringatan yang lebih awal benar-benar mengurangi waktu gangguan atau hanya menambah pekerjaan triase. Rancangan studi dapat melibatkan observasi

This Article is licensed under a CC BY-SA 4.0 International License

prosedur SOC, latihan insiden berkala, dan evaluasi kualitatif operator. Penggabungan metrik teknis dengan pengalaman pengguna sistem keamanan memungkinkan penilaian yang lebih lengkap terhadap ketahanan digital. Dengan pendekatan tersebut, teknologi AI ditempatkan sebagai pendukung proses yang dapat diaudit dan terus ditingkatkan.

Analisis Risiko Keterandalan Telemetri

Keandalan penilaian anomali sangat dipengaruhi kemampuan sistem membedakan kejadian tidak lazim dari ketidaklengkapan pencatatan. Salah satu persoalan praktis ialah ketidaksinkronan waktu antara mesin yang mempunyai zona waktu, pengaturan jam, dan jadwal sinkronisasi berbeda. Ketika urutan peristiwa berubah akibat perbedaan tersebut, rangkaian aktivitas yang sebenarnya masuk akal bisa terlihat sebagai anomali. Pengembangan model sebaiknya mencatat batas toleransi ketidaktepatan waktu dan memperlakukan sumber tanpa sinkronisasi sebagai data dengan tingkat keyakinan rendah. Penjelasan sumber ketidakpastian ini dapat ditampilkan pada layar triase sehingga petugas memahami bahwa urutan log adalah rekonstruksi berbasis catatan, bukan representasi sempurna proses aktual.

Pengukuran Kapasitas Sistem dalam Arsitektur Streaming

Sistem deteksi waktu nyata juga dibatasi oleh kapasitas antrean data, penyimpanan, dan inferensi. Saat terjadi lonjakan peristiwa, model yang memerlukan komputasi besar mungkin tertinggal dari aliran data dan menyebabkan peringatan datang terlambat. Karena itu, pengujian beban seharusnya melaporkan throughput, latensi pada persentil tinggi, ukuran antrean, dan proporsi peristiwa yang gagal diproses. Strategi pemrosesan bertahap dapat menjalankan pemeriksaan ringan pada seluruh aliran lalu menggunakan analisis kompleks hanya pada bagian yang layak diselidiki. Namun, penyaringan awal berpotensi membuang peristiwa penting; rancangan harus mencatat syarat penyaringan dan meninjau kesalahan yang mungkin timbul. Penentuan kapasitas berdasarkan pola operasi normal dan kondisi puncak membantu menjaga keselamatan layanan.

Perbedaan Data Sintetis dan Pengamatan Operasional

Kumpulan data publik berguna untuk pembandingan awal, tetapi sering tidak mewakili keragaman versi aplikasi, infrastruktur, dan kebiasaan pengguna. Simulasi serangan pada jaringan pengujian biasanya mempunyai kondisi lebih terkendali daripada sistem produksi, sehingga artefak lingkungan dapat dipelajari sebagai ciri kelas serangan. Pengujian berbasis data sintetis harus menjelaskan cara skenario dibangkitkan dan batas realismenya. Jika model diuji pada data yang dibuat menggunakan aturan sama dengan data pelatihan, skor tinggi mungkin mencerminkan pengenalan pola generator. Tahap validasi berikutnya perlu melibatkan pengamatan independen serta dokumentasi perubahan domain. Transparansi mengenai asal data merupakan prasyarat agar klaim kemampuan deteksi tidak melampaui bukti yang tersedia.

Keseimbangan Deteksi dan Keamanan Pengguna

Pengawasan perilaku entitas perlu mempertimbangkan hak dan ekspektasi privasi pengguna. Peristiwa autentikasi atau perubahan akses memang relevan bagi keamanan, tetapi penggabungan riwayat aktivitas dapat membentuk profil perilaku yang sensitif. Fitur sebaiknya dibatasi pada kebutuhan risiko yang telah didefinisikan; informasi yang tidak membantu deteksi tidak perlu disimpan tanpa batas. Akses terhadap rekonstruksi aktivitas individual harus tersedia hanya bagi petugas yang berwenang. Kebijakan juga perlu menjelaskan jangka retensi, proses koreksi label keliru, dan mekanisme audit penyalahgunaan. Dengan rancangan tersebut, keamanan sistem dan perlindungan informasi pribadi diperlakukan sebagai tujuan yang harus dijaga bersama, bukan sebagai pilihan yang saling meniadakan.

This Article is licensed under a CC BY-SA 4.0 International License

Vol. 1 No. 1, Oktober 2026, hal. 57–70 e-ISSN: 3165-3677 | p-ISSN: 3165-3723

Umpan Balik Analis sebagai Sumber Pembelajaran

Setelah triase, petugas dapat memberi kategori penyebab peringatan, konteks tindakan sah, bukti kompromi, atau status belum terkonfirmasi. Informasi ini berpotensi meningkatkan pemodelan, tetapi kualitas label tidak otomatis seragam. Dua analis dapat berbeda pandangan karena memperoleh bukti yang berlainan atau menggunakan definisi insiden berbeda. Standar label, contoh kasus, serta mekanisme peninjauan silang perlu disusun agar pembaruan model tidak memperkuat ketidakkonsistenan. Hasil investigasi juga dapat berubah setelah pemeriksaan forensik; sistem harus mempertahankan riwayat revisi label. Proses pembelajaran sebaiknya memisahkan data yang telah diverifikasi dari data yang hanya ditandai berdasarkan dugaan awal. Pendekatan tersebut memperbaiki integritas umpan balik dan memudahkan evaluasi versi.

Kewaspadaan terhadap Bias Evaluasi

Bias dapat muncul ketika pengujian melibatkan jenis serangan yang memiliki representasi jauh lebih baik daripada teknik lain. Nilai rata-rata mungkin tampak baik meski model gagal mengenali kategori berisiko tinggi yang jarang terjadi. Peneliti perlu menjelaskan komposisi kategori dan tingkat kesulitan tiap skenario, sekaligus memisahkan kemampuan menemukan serangan lama dari kemampuan mengenali anomali baru. Ketika label terlalu sedikit, ketidakpastian skor pada setiap kategori mungkin besar dan perlu dilaporkan. Penggunaan satu dataset secara berulang untuk memilih arsitektur juga dapat menyebabkan overfitting terhadap benchmark. Data evaluasi baru atau pengujian lintas organisasi membantu mengungkap keterbatasan itu, meskipun pelaksanaannya membutuhkan koordinasi serta pengamanan data.

Risiko Konsentrasi pada Infrastruktur Pengawasan

Arsitektur terpusat menyediakan pandangan menyeluruh, tetapi juga menciptakan komponen yang bernilai tinggi bagi penyerang. Sistem pengumpul log, penyimpan fitur, dan antarmuka analis dapat mengandung informasi detail topologi serta pola operasional organisasi. Pengamanan identitas layanan, segmentasi akses, pencatatan perubahan konfigurasi, serta pengujian pemulihan perlu menjangkau komponen deteksi itu sendiri. Pengoperasian model tanpa pembatasan hak akses berpotensi memberi pihak yang tidak berwenang kesempatan mengubah nilai ambang atau meniadakan jenis alarm tertentu. Sistem pengawasan harus diawasi melalui kontrol terpisah dan tidak boleh dianggap tepercaya semata karena ditujukan untuk keamanan. Prinsip pemisahan tugas dapat membatasi perubahan kritis tanpa persetujuan.

Perbandingan Desain Berbasis Biaya dan Manfaat

Tidak setiap organisasi mempunyai anggaran dan sumber daya yang cukup untuk melatih model kompleks serta mempertahankan infrastruktur inferensi sepanjang waktu. Keputusan pengembangan perlu membandingkan biaya akuisisi log, penyimpanan, pelatihan, pembaruan model, dan kebutuhan analis dengan manfaat risiko yang mungkin berkurang. Baseline statistik yang cepat, stabil, dan transparan dapat memberi manfaat lebih besar dalam kondisi data terbatas. Sebaliknya, lingkungan dengan pola interaksi kompleks dan telemetri yang baik mungkin memperoleh nilai dari model lanjutan. Kriteria investasi perlu didasarkan pada uji yang relevan terhadap operasi, bukan klaim teknologi. Keputusan juga mempertimbangkan kemampuan pemeliharaan setelah proyek penelitian berakhir.

Rencana Uji Prospektif

Penelitian empiris lanjutan dapat menetapkan periode pengamatan dasar lalu menjalankan model dalam mode bayangan tanpa memicu respons otomatis. Pada tahap ini, peneliti mengukur jumlah alarm, waktu deteksi, proporsi kasus yang layak diselidiki, dan perbedaan hasil terhadap kontrol yang telah digunakan. Setelah prosedur stabil, evaluasi dapat diperluas

This Article is licensed under a CC BY-SA 4.0 International License

ke beberapa kelompok sistem dengan konteks yang sebanding. Hasil perlu dinilai oleh petugas keamanan berdasarkan prosedur yang konsisten dan sebanyak mungkin tidak dipengaruhi identitas model yang memberikan peringatan. Untuk menilai dampak pada ketahanan, catatan kejadian dan waktu pemulihan perlu tersedia, sambil mengakui bahwa tidak semua peristiwa menyediakan ukuran dampak yang sama.

Pengelolaan Perubahan dan Kesiapan Manusia

Keberhasilan implementasi membutuhkan pelatihan petugas, pemahaman batas model, serta jalur eskalasi yang dapat dilakukan pada kondisi tekanan tinggi. Analis perlu mengetahui cara membaca skor, memeriksa log mentah, mengenali gangguan sensor, dan menggunakan prosedur rollback tindakan. Latihan berkala dapat memperlihatkan apakah peringatan yang dihasilkan cukup jelas serta apakah peran antarunit telah dipahami. Dokumentasi teknis yang hanya menjelaskan parameter algoritma belum cukup bagi operator yang harus memutuskan tindakan dalam beberapa menit. Pedoman operasional hendaknya memakai contoh realistis, menjelaskan kesalahan umum, dan memperbarui prosedur ketika konteks infrastruktur berubah. Kesiapan manusia merupakan bagian substantif dari ketahanan digital.

Indikator Keberhasilan dalam Pemeliharaan Jangka Panjang

Model yang baik pada awal penerapan masih dapat menurun kegunaannya akibat perubahan perilaku pengguna, peralatan baru, atau revisi kebijakan akses. Organisasi perlu menetapkan jadwal pengukuran performa dan indikator kesehatan pipeline secara terpisah. Ketersediaan sumber data, waktu tunda inferensi, frekuensi alarm, dan proporsi insiden yang benar-benar dikonfirmasi dapat dipakai untuk mengenali perubahan. Namun, indikator tersebut harus dibaca bersama volume kerja serta karakteristik layanan. Lonjakan aktivitas sah pada periode sibuk dapat meningkatkan alarm tanpa ada penurunan intrinsik mutu algoritma. Pengujian ulang dengan data independen dan peninjauan model oleh tim lintas disiplin dapat membantu menafsirkan perubahan sebelum keputusan pembaruan diambil.

Batas Generalisasi dan Etika Klaim

Manfaat sistem deteksi tidak seharusnya digeneralisasikan dari satu rangkaian uji yang sempit ke seluruh jenis serangan dan kondisi jaringan. Kinerja di laboratorium berbeda dari lingkungan yang memiliki gangguan pencatatan, perubahan hak akses, serta pengguna yang beragam. Penulis penelitian perlu memisahkan hasil terbukti dari usulan fitur dan kemungkinan penerapan. Jika penelitian hanya mengembangkan arsitektur konseptual, kontribusinya terletak pada kejelasan rancangan, integrasi proses, serta hipotesis yang dapat diuji; bukan pada angka keberhasilan yang belum tersedia. Prinsip pelaporan ini mendukung proses ilmiah yang dapat direplikasi dan membantu organisasi menghindari pembelian atau penerapan sistem berdasarkan klaim yang tidak didukung data.

Pengujian manfaat sebuah model sebaiknya membedakan kemampuan menemukan sinyal dengan kemampuan menghasilkan keputusan keamanan yang benar. Terdapat keadaan ketika peringatan berhasil mendeteksi penyimpangan tetapi investigasi tidak menemukan insiden, dan terdapat kasus ketika tanda awal insiden terlewat karena belum tersedia dalam log. Pemisahan hasil deteksi, hasil triase, serta hasil pemulihan dapat membantu organisasi mengidentifikasi bagian proses yang membutuhkan perbaikan. Bila seluruh kegagalan dianggap sebagai kesalahan algoritma, persoalan pengumpulan data dan tata kelola tanggapan dapat luput dari perhatian. Evaluasi lintas tahap membantu memusatkan investasi pada kelemahan yang benar-benar menghambat operasi.

Penguatan keamanan digital juga memerlukan komunikasi risiko yang tidak berlebihan. Para pemimpin organisasi membutuhkan ringkasan yang menjelaskan jenis penyimpangan, aset

This Article is licensed under a CC BY-SA 4.0 International License

utama, batas cakupan pemantauan, dan tindakan yang sudah dilakukan. Laporan yang hanya memuat skor deteksi dapat memberi gambaran keliru tentang besarnya ancaman. Indikator ketahanan sebaiknya memasukkan kesiapan pencadangan, kemampuan isolasi layanan terbatas, serta keberhasilan latihan pemulihan. Dengan demikian, keputusan manajemen tidak terjebak dalam ukuran kinerja teknis yang terpisah dari kesinambungan layanan dan prioritas publik.

Pada tingkat implementasi, penilaian hasil harus mempertimbangkan keragaman kondisi organisasi. Infrastruktur yang dikelola oleh tim kecil, misalnya, mungkin lebih membutuhkan penyaringan awal yang andal dan dapat dijelaskan daripada arsitektur sangat kompleks dengan kebutuhan pemeliharaan tinggi. Pilihan lain adalah penggunaan layanan terkelola dengan pengaturan akses dan kontrol data yang diperiksa secara ketat. Setiap skenario memerlukan pencatatan risiko dependensi, komitmen layanan, dan rencana ketika penyedia tidak tersedia. Ukuran keberhasilan akhirnya adalah pengurangan risiko yang dapat diperiksa, bukan sekadar keberadaan komponen artificial intelligence di dalam arsitektur.

E. CONCLUSION (KESIMPULAN)

Simpulan dan Batasan

Pengembangan sistem deteksi anomali berbasis artificial intelligence memiliki potensi untuk memperkuat keamanan informasi ketika digunakan sebagai bagian dari pengawasan berlapis. Model statistik, pembelajaran tanpa pengawasan, klasifikasi terawasi, serta pendekatan berbasis urutan mempunyai keunggulan dan batasan yang berbeda. Pemilihan tidak boleh hanya didasarkan pada kecanggihan algoritma, tetapi pada jenis data, tersedianya label, kebutuhan interpretasi, dan konsekuensi kesalahan. Skor anomali merupakan indikator untuk investigasi, bukan bukti mandiri adanya serangan.

Kontribusi kajian ini adalah kerangka yang menghubungkan kualitas telemetri, pembuatan fitur, validasi temporal, penetapan ambang, korelasi peristiwa, keputusan manusia, dan evaluasi hasil respons. Ketahanan digital meningkat bila organisasi tidak hanya mendeteksi, tetapi juga mampu mempertahankan layanan, membatasi dampak, dan pulih dari gangguan. Sistem AI tanpa tata kelola atau mekanisme fallback justru dapat menambah ketergantungan dan risiko operasional. Oleh karena itu, kontrol keamanan dasar, audit, serta pengujian pemulihan tetap menjadi kebutuhan utama.

Artikel ini tidak menyajikan hasil percobaan model pada dataset tertentu, sehingga tidak mengklaim angka akurasi, recall, atau peningkatan efisiensi yang belum diukur. Penelitian lanjutan perlu melakukan validasi prospektif pada telemetri yang representatif, melaporkan false alarm per satuan waktu, serta menilai keterlambatan peringatan dan dampak terhadap kesinambungan layanan. Keputusan implementasi seyogianya mempertimbangkan biaya, privasi, sumber daya manusia, dan kemampuan organisasi menanggapi peringatan. Dengan cara ini, kecerdasan buatan dapat digunakan secara terukur dan dapat dipertanggungjawabkan untuk memperkuat ketahanan sistem digital.

F. BIBLIOGRAPHY (DAFTAR PUSTAKA)

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

An, J., & Cho, S. (2015). Variational autoencoder based anomaly detection using reconstruction probability. SNU Data Mining Center.

Breiman, L. (2001). Random forests. Machine Learning, 45, 5–32. https://doi.org/10.1023/A:1010933404324

This Article is licensed under a CC BY-SA 4.0 International License

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15. https://doi.org/10.1145/1541880.1541882

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 785–794. https://doi.org/10.1145/2939672.2939785

Davis, J., & Goadrich, M. (2006). The relationship between Precision-Recall and ROC curves. Proceedings of the 23rd International Conference on Machine Learning, 233–240. https://doi.org/10.1145/1143844.1143874

Goldstein, M., & Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PLOS ONE, 11(4), e0152173. https://doi.org/10.1371/journal.pone.0152173

He, H., & Garcia, E. A. (2009). Learning from imbalanced data. IEEE Transactions on Knowledge and Data Engineering, 21(9), 1263–1284. https://doi.org/10.1109/TKDE.2008.239

Karim, F., Majumdar, S., Darabi, H., & Chen, S. (2018). LSTM fully convolutional networks for time series classification. IEEE Access, 6, 1662–1669. https://doi.org/10.1109/ACCESS.2017.2779939

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521, 436–444. https://doi.org/10.1038/nature14539

Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. 2008 Eighth IEEE International Conference on Data Mining, 413–422. https://doi.org/10.1109/ICDM.2008.17

Mitchell, T. M. (1997). Machine learning. McGraw-Hill.

National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1

Pedregosa, F., et al. (2011). Scikit-learn: Machine learning in Python. Journal of Machine Learning Research, 12, 2825–2830.

Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167. https://doi.org/10.1016/j.cose.2019.06.005

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN Computer Science, 2, 160. https://doi.org/10.1007/s42979-021-00592-x

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. 2010 IEEE Symposium on Security and Privacy, 305–316. https://doi.org/10.1109/SP.2010.25

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 1–6. https://doi.org/10.1109/CISDA.2009.5356528

Verkerken, M., D'hooge, L., Wauters, T., Volckaert, B., & De Turck, F. (2022). Towards model generalization for intrusion detection: Unsupervised machine learning techniques. Journal of Network and Systems Management, 30, Article 15. https://doi.org/10.1007/s10922-021-09612-8

Xu, H., Chen, W., Zhao, N., Li, Z., Bu, J., Li, Z., Liu, Y., Zhao, Y., Pei, D., Feng, Y., Chen, J., Wang, Z., & Qiao, H. (2018). Unsupervised anomaly detection via variational auto-encoder for seasonal KPIs in web applications. Proceedings of the 2018 World Wide Web Conference, 187–196. https://doi.org/10.1145/3178876.3185996

Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big heterogeneous data: A survey. Journal of Big Data, 2, Article 3. https://doi.org/10.1186/s40537-015-0013-4

This Article is licensed under a CC BY-SA 4.0 International License