Smart Comp: Jurnalnya Orang Pintar Komputer
Volume 15, Nomor 2, Tahun 2026, hlm. 550-560
Terakreditasi Sinta, Peringkat 4, SK No. 295/C/C3/KPT/2026
DOI : 10.30591/smartcomp.v15i2.10644

P-ISSN : 2089-676X
E-ISSN : 2549-0796

Deteksi Anomali Login Berbasis Analisis Perilaku dan Penilaian Risiko Sadar Konteks pada Sistem Informasi Akademik di Politeknik Kepribadian Bangsa

Indra Permana[1]
[1)]Teknologi Rekayasa Perangkat Lunak, Politekmik Kepribadian
Email: [1]anamrepindra2@gmail.com

(Naskah masuk: *12 Januari 2026*, diterima untuk diterbitkan: *27 Februari 2026*)

Abstrak: *Berikut adalah terjemahan bahasa Inggris dari abstrak Anda: Keamanan akun dalam sistem informasi akademik tidak dapat hanya mengandalkan nama pengguna dan kata sandi. Perubahan perangkat, jaringan, waktu akses, dan kegagalan autentikasi dapat menjadi indikator awal penggunaan akun yang menyimpang dari pola normal. Penelitian ini mengkaji penerapan analitik perilaku dan penilaian risiko berbasis konteks untuk mendeteksi anomali login di lingkungan akademik. Kumpulan data yang dianalisis mencakup 1.819 aktivitas login dari 107 pengguna antara tanggal 1 Juni dan 30 Juli 2026. Pada bulan Juni, sebagian besar aktivitas terkait dengan pemeriksaan transkrip akademik (KHS), sedangkan pada bulan Juli, aktivitas beralih ke pendaftaran mata kuliah (KRS). Lokasi login dalam kumpulan data tersebut meliputi Karawang, Bekasi, dan Purwakarta. Tiga algoritma dibandingkan: Isolation Forest, One-Class SVM, dan Local Outlier Factor (LOF). Fitur yang digunakan mencakup percobaan gagal, perubahan perangkat, perubahan IP, waktu login yang tidak biasa, dan representasi waktu siklikal. Hasil pengujian menunjukkan bahwa Isolation Forest mencapai skor F1 tertinggi sebesar 0,305, sementara One-Class SVM dan LOF masing-masing mencapai 0,110 dan 0,047. Isolation Forest juga menghasilkan nilai ROC-AUC sebesar 0,594. Temuan ini mengindikasikan bahwa Isolation Forest lebih sesuai dengan karakteristik kumpulan data yang digunakan, meskipun tingkat deteksinya masih perlu ditingkatkan. Label anomali yang digunakan bersifat sintetis, sehingga hasil penelitian ini sebaiknya ditafsirkan sebagai evaluasi eksperimental dan bukan sebagai jumlah insiden keamanan yang terverifikasi.*

Kata kunci: *deteksi anomali; analitik perilaku; keamanan siber; Isolation Forest; penilaian risiko*

Login Anomaly Detection Based on Behavioral Analytics and Context-Aware Risk Scoring in the Academic Information System at Politeknik Kepribadian Bangsa

Abstract: *Here is the English translation of your abstract: Account security in academic information systems cannot rely solely on usernames and passwords. Changes in devices, networks, access times, and authentication failures can serve as early indicators of account usage that deviates from normal patterns. This study examines the application of behavioral analytics and context-aware risk scoring to detect login anomalies in an academic environment. The dataset analyzed consists of 1,819 login activities from 107 users between June 1 and July 30, 2026. In June, most activities were related to checking academic transcripts (KHS), while in July, activities shifted to course registration (KRS). The login locations in the dataset include Karawang, Bekasi, and Purwakarta. Three algorithms were compared: Isolation Forest, One-Class SVM, and Local Outlier Factor (LOF). The features used include failed attempts, device changes, IP changes, unusual login times, and cyclical time representations. Testing results show that Isolation Forest achieved the highest F1-score of 0.305, while One-Class SVM and LOF achieved 0.110 and 0.047, respectively. Isolation Forest also yielded a ROC-AUC of 0.594. These findings indicate that Isolation Forest is more suitable for the characteristics of the dataset used, although the detection rate still needs improvement. The anomaly labels used are synthetic, so the results of this study should be interpreted as an experimental evaluation rather than as the number of verified security incidents.*

Keywords – *anomaly detection; behavioral analytics; cybersecurity; Isolation forest; risk scoring*

1. PENDAHULUAN

Sistem informasi akademik telah menjadi infrastruktur penting dalam mendukung berbagai aktivitas akademik sehari-hari. Akun pengguna tidak hanya berfungsi sebagai sarana untuk

memantau informasi perkuliahan, tetapi juga menyediakan akses terhadap data penting seperti Kartu Hasil Studi (KHS) dan Kartu Rencana Studi (KRS) [1]. Oleh karena itu, potensi pengambilalihan akun (account takeover) dapat menimbulkan risiko serius yang tidak hanya berkaitan dengan kegagalan autentikasi, tetapi juga mencakup kebocoran data pribadi dan rekam akademik pengguna. Namun, tantangan utama dalam mengamankan sistem tersebut terletak pada pola perilaku pengguna yang bersifat dinamis dan dapat berubah sepanjang semester. Sebagai contoh, pada saat pengumuman hasil studi atau KHS, intensitas login mahasiswa cenderung meningkat secara drastis karena mahasiswa melakukan pengecekan nilai. Selanjutnya, peningkatan aktivitas akses juga terjadi pada periode pengisian atau pendaftaran KRS. Meskipun peningkatan aktivitas tersebut merupakan fenomena yang normal secara kolektif, sistem keamanan yang masih menggunakan ambang batas (threshold) tetap berisiko tinggi mengidentifikasinya secara keliru sebagai ancaman atau aktivitas mencurigakan [2].

Melalui pendekatan analisis perilaku (behavioral analytics), evaluasi akses tidak lagi hanya terbatas pada validasi kredensial, tetapi juga berfokus pada pemetaan kebiasaan pengguna. Berbagai variabel multidimensi, seperti perubahan perangkat, lokasi jaringan, waktu login, serta riwayat kegagalan login, dianalisis secara bertahap untuk membentuk pola perilaku pengguna. Penelitian sebelumnya menunjukkan bahwa pemanfaatan dimensi temporal dan spasial memiliki peran penting dalam mendeteksi anomali perilaku yang menyimpang dari profil asli pemilik akun. Implementasi risk-based authentication (RBA) memberikan fleksibilitas dalam merespons kondisi keamanan melalui penyesuaian tingkat risiko berdasarkan konteks.

Sistem dapat memberikan respons secara adaptif, yaitu memberikan akses secara lebih sederhana ketika kondisi risiko rendah atau menerapkan autentikasi tambahan (step-up authentication) ketika tingkat risiko meningkat. Mekanisme tersebut dirancang untuk meminimalkan gangguan terhadap kenyamanan pengguna sekaligus meningkatkan perlindungan sistem secara dinamis.

Di sisi lain, literatur mengenai deteksi anomali perilaku pengguna (user behavior anomaly detection) menekankan pentingnya integrasi berbagai sinyal jejak digital serta penanganan permasalahan ketidakseimbangan data (class imbalance) [3], misalnya, menggunakan pendekatan ensemble untuk mengolah log aktivitas pengguna dan mengurangi tingkat false alarm atau kesalahan dalam memberikan peringatan.

Berdasarkan temuan tersebut, penelitian ini difokuskan pada lingkungan sistem informasi akademik yang memiliki karakteristik khusus, yaitu jumlah dan jenis pengguna yang relatif terdefinisi dengan baik serta adanya pengaruh konteks kalender akademik yang spesifik dan terstruktur.

Penelitian ini bertujuan untuk membandingkan kinerja algoritma Isolation Forest, One-Class SVM, dan Local Outlier Factor (LOF) dalam mendeteksi anomali pada aktivitas login pengguna, serta merumuskan mekanisme untuk mengonversi hasil deteksi tersebut menjadi tingkat risiko adaptif (adaptive risk level) sebagai dasar penerapan autentikasi adaptif (adaptive authentication). Selain itu, penelitian ini juga mengevaluasi pengaruh konteks kalender akademik, khususnya pada periode KHS dan KRS, untuk memastikan bahwa peningkatan aktivitas login yang secara kolektif merupakan kondisi normal tidak secara keliru diklasifikasikan sebagai ancaman keamanan.

2. METODE PENELITIAN

Penelitian ini dilakukan dalam lingkungan sistem informasi akademik di Politeknik Kepribadian Bangsa Indonesia, dengan periode pengamatan selama dua bulan, mulai dari 1 Juni hingga 30 Juli 2026. Selama periode tersebut, dikumpulkan sebuah dataset yang mencatat 1.819 kejadian *login* dari 107 pengguna aktif [4]. Distribusi aktivitas pada bulan Juni terutama mencerminkan pola akses mahasiswa untuk memeriksa transkrip akademik (KHS), sementara dinamika transaksi *login* pada bulan Juli dipengaruhi oleh intensitas kegiatan pendaftaran mata kuliah (KRS).

Tabel 1. Data Login Atribut

No.	Deskripsi Objek Penelitian	Keterangan
1	user_id	Pengenal anonim untuk penggun
2	Timestamp	Tanggal dan waktu masuk (login)
3	login_status	Status autentikasi (berhasil atau gagal)
4	device_hash	Pengenal perangkat yang telah dianonimkan
5	ip_hash	Pengenal jaringan yang telah dianonimkan
6	Browser	Kategori peramban (browser)
7	operating_system	operating_system Kategori sistem operasi
8	Location	Kategori lokasi umum (kasar)
9	failed_attempts	Jumlah percobaan gagal dalam rentang waktu tertentu
10	session_duration	Session_duration Durasi sesi yang terautentikasi

2.1. Dataset dan Variabel

Dataset log autentikasi mencakup beberapa atribut utama, seperti identitas pengguna yang telah dianonimisasi, stempel waktu, status login, spesifikasi perangkat, peramban, alamat IP, lokasi akses, dan frekuensi percobaan login yang gagal. Selain atribut-atribut dasar tersebut, dataset ini juga memuat indikator turunan seperti perubahan perangkat, perubahan alamat IP, dan pola akses pada waktu yang tidak lazim. Cakupan geografis data lokasi login secara khusus dibatasi pada tiga wilayah: Karawang, Bekasi, dan Purwakarta [5].

Tabel 2. Dataset Karakteristik

No	Item	Value
1	Total login events	1.819
2	Users	107
3	Observation period	1 June–30 July 2026
4	June context	KHS checking
5	July context	KRS completion
6	Login areas	Karawang, Bekasi, Purwakarta

2.1.1. Persiapan Fitur

Pemilihan fitur didasarkan pada atribut informasi standar yang tercatat dalam log autentikasi. Indikator percobaan gagal diekstraksi untuk mendeteksi kegagalan akses, sementara perubahan perangkat dan perubahan IP digunakan untuk mengidentifikasi penyimpangan dalam penggunaan perangkat dan jaringan dibandingkan dengan riwayat aktivitas pengguna. Untuk dimensi temporal, variabel waktu masuk (login) yang tidak lazim digunakan sebagai penanda waktu akses yang anomali. Selain itu, jam masuk ditransformasikan menggunakan fungsi trigonometri (sinus dan kosinus) untuk menjaga kontinuitas siklus waktu, sehingga transisi antara pukul 23.00 dan 00.00 tidak terputus secara linear. Demi menjaga integritas validasi penelitian, variabel `synthetic_anomaly_label` secara ketat dikeluarkan dari kumpulan fitur yang digunakan untuk pelatihan model dan dialokasikan semata-mata sebagai acuan evaluasi (*ground truth*). Pemisahan yang jelas ini sangat penting untuk menghilangkan risiko kebocoran data, yang dapat menyebabkan estimasi kinerja model menjadi terlalu tinggi atau terdistorsi dibandingkan dengan kondisi dunia nyata [6].

2.2. Model Deteksi Anomali

Isolation Forest dipilih sebagai metode utama kami karena sangat efektif dalam mengisolasi data anomali yang tampak mencolok dibandingkan kelompoknya. Sebagai pembanding, kami menggunakan One-Class SVM untuk menentukan batas-batas yang dianggap normal. Terakhir, LOF melengkapi analisis ini dengan memeriksa kepadatan lingkungan di sekitar setiap titik data. Untuk memastikan perbandingan yang adil dan objektif, ketiga algoritma tersebut diuji menggunakan kumpulan fitur yang sama.

2.2.1. Evaluasi Model

Evaluasi model dilakukan menggunakan beberapa metrik utama: precision, recall, F1-score, ROC-AUC, PR-AUC, false positive rate (FPR), dan false negative rate (FNR). Precision mengukur sejauh mana data yang terdeteksi sebagai anomali benar-benar merupakan anomali. Sementara itu, recall mencerminkan kemampuan model dalam menemukan seluruh anomali yang ada, dengan F1-score menyeimbangkan kedua metrik tersebut. Dalam konteks keamanan, recall dan FNR memegang peranan krusial; anomali yang terlewat dapat menyebabkan akun yang berisiko tidak terdeteksi. Di sisi lain, FPR juga tidak boleh diabaikan, karena tingkat alarm palsu yang tinggi dapat mengganggu kenyamanan pengguna akibat adanya verifikasi tambahan yang berlebihan.

2.2.2. Penilaian Risiko Berbasis Konteks

Evaluasi risiko (penilaian risiko) dilakukan setelah skor anomali diperoleh. Demi menjaga keseimbangan sistem, pemblokiran akun tidak dilakukan secara terburu-buru hanya berdasarkan satu indikator saja. Sistem mengombinasikan berbagai sinyal untuk mengategorikan aktivitas masuk (*login*) ke dalam tingkat risiko rendah, sedang, atau tinggi. Aktivitas masuk dengan risiko rendah diberikan akses langsung, aktivitas risiko sedang diarahkan ke verifikasi tambahan, sedangkan aktivitas risiko tinggi memicu pemblokiran sementara, pemeriksaan *Multi-Factor Authentication* (MFA), serta notifikasi kepada administrator [7]. Keunggulan pendekatan ini terletak pada pemanfaatan kalender akademik sebagai variabel kontekstual. Lonjakan lalu lintas *login* secara massal selama periode KRS atau KHS dianggap sebagai perilaku kolektif yang wajar. Sebaliknya, eskalasi risiko difokuskan pada akun yang menunjukkan anomali spesifik dan berurutan, seperti kombinasi penggunaan perangkat baru, alamat IP yang tidak dikenal, waktu akses yang tidak lazim, serta kegagalan autentikasi yang berulang.

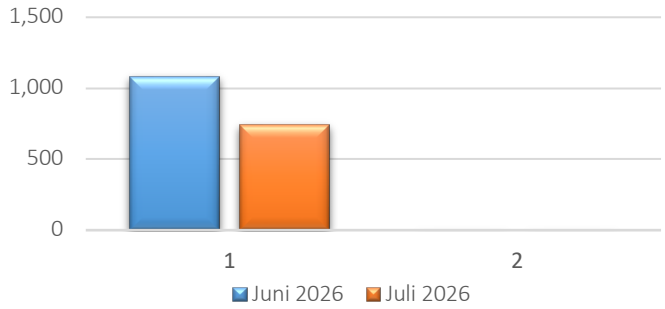
3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

Analisis dilakukan terhadap 1.819 aktivitas masuk (*login*) dari 107 pengguna. Distribusi aktivitas tersebut tidak tersebar merata sepanjang waktu, melainkan terkonsentrasi pada periode-periode tertentu: bulan Juni mencatat 1.080 transaksi *login*, sedangkan bulan Juli mencatat 739 *login*. Pola distribusi ini selaras dengan konteks akademik yang mendasari penelitian, di mana lonjakan pada bulan Juni bertepatan dengan periode pengecekan transkrip akademik (KHS), sementara aktivitas pada bulan Juli didominasi oleh pengajuan pendaftaran mata kuliah (KRS). Hasil dan pembahasan dapat disajikan dalam bentuk tabel atau gambar serta harus dikaitkan dengan teori yang digunakan. Hindari penggunaan sitasi yang berlebihan dan pembahasan literatur yang telah dipublikasikan [8].

Tabel 3. Aktivitas Login Bulanan

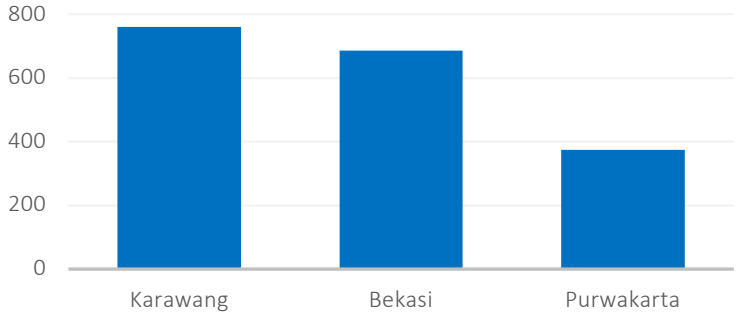
Periode	Login Events	Akademik Content
Juni 2026	1.080	KHS chek
Juli 2026	739	KRS completion
Total	1.819	—



Gambar 1. Aktivitas Login Perbulan

3.1.1. Catatan Perwilayah

Berdasarkan wilayah, Karawang mencatat 759 login, Bekasi mencatat 685 login, dan Purwakarta mencatat 375 login. Perbedaan angka ini tidak digunakan untuk menyimpulkan bahwa suatu wilayah lebih berbahaya dibandingkan wilayah lainnya. Wilayah hanya berfungsi sebagai salah satu faktor kontekstual bagi perilaku login



Gambar 2. Login Events

Tabel 4. Aktivitas Login berdasarkan Wilayah

Area	Login Events
Karawang	759
Bekasi	685
Purwakarta	375
Total	1.819

Data dapat disajikan dalam bentuk tabel atau gambar. Hasil dan pembahasan juga harus dikaitkan dengan teori yang digunakan. Hindari penggunaan sitasi yang berlebihan serta pembahasan literatur yang telah dipublikasikan.

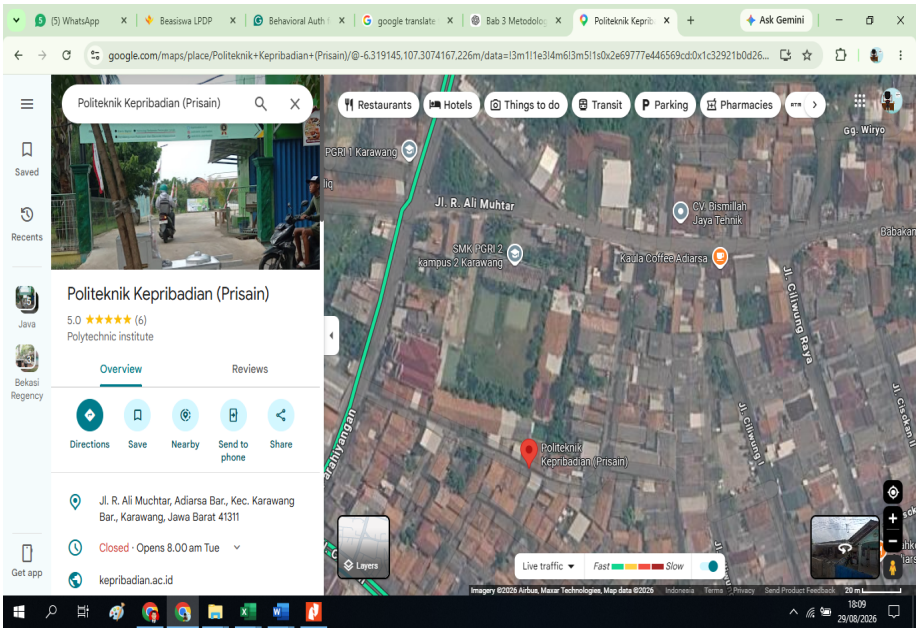
3.2. Lokasi Penelitian dan Objek

Penelitian ini dilaksanakan di Politeknik Kepribadian Bangsa, dengan objek penelitian berupa aktivitas autentikasi pengguna pada Sistem Informasi Akademik. Data aktivitas masuk (login) yang digunakan dapat berasal dari pengguna sistem seperti:

1 Administrator
2 Dosen
3 Staf akademik
4 Mahasiswa

Pengguna lain yang memiliki hak akses ke Sistem Informasi Akademik. Objek utama penelitian ini adalah perilaku masuk pengguna, yang direpresentasikan melalui berbagai atribut seperti waktu masuk, alamat IP, perangkat yang digunakan, informasi lokasi atau geografis,

frekuensi masuk, dan pola aktivitas pengguna. Data identitas pribadi pengguna tidak digunakan secara langsung dalam proses analisis. Identitas pengguna dapat disamarkan (pseudonimisasi) atau dianonimkan sehingga penelitian berfokus pada pola perilaku dan keamanan sistem.



Gambar 3. Lokasi Penelitian dan Objek

3.3. Komposisi Dataset

Dari 1.819 kejadian, label sintetis mengklasifikasikan 85 kejadian (atau 4,67%) sebagai anomali dan 1.734 kejadian (atau 95,33%) sebagai normal. Komposisi ini menunjukkan kondisi yang tidak seimbang, sehingga akurasi saja tidak cukup untuk mengevaluasi model. Model yang selalu memilih kelas mayoritas mungkin tampak baik dari segi akurasi, namun tidak membantu dalam mengidentifikasi anomali.

Tabel 5. Komposisi Dataset

Kelas	Count	Presentase
Normal	1.734	95,33%
Synthetic anomalous	85	4,67%
Total	1.819	100,00%

3.4. Profil Prilaku

Profil perilaku pengguna disusun berdasarkan berbagai kebiasaan yang dapat diamati dalam log. Waktu masuk (login) yang umum, perangkat yang sering digunakan, jaringan yang biasa dipakai, serta jumlah kegagalan autentikasi membentuk sebuah tolok ukur dasar (baseline). [9] Tolok ukur ini tidak dianggap sebagai aturan baku karena perilaku mahasiswa dapat berubah mengikuti aktivitas akademik. Sebagai contoh, seorang mahasiswa yang biasanya masuk ke sistem dari pagi hingga sore menggunakan perangkat yang sama akan terlihat berbeda jika akunnya tiba-tiba diakses pada waktu yang tidak lazim menggunakan perangkat serta alamat IP yang baru. Satu perubahan saja tidak serta-merta mengindikasikan adanya masalah. Namun, kombinasi dari beberapa perubahan memberikan sinyal yang lebih kuat.

3.5. Perbandingan Kinerja Model

Hasil pengujian menunjukkan bahwa Isolation Forest mencapai presisi sebesar 0,316, recall sebesar 0,294, dan F1-score sebesar 0,305. One-Class SVM menghasilkan presisi sebesar 0,066, recall

sebesar 0,329, dan F1-score sebesar 0,110. Sementara itu, LOF mencapai presisi sebesar 0,047, recall sebesar 0,047, dan F1-score sebesar 0,047.

Table 6. Comparative Model Performance

Algorithm	**Precision**	**Recall**	**F1-Score**	**ROC-AUC**	**PR-AUC**	**FPR**	**FNR**
Isolation Forest	0,316	0,294	0,305	0,594	0,187	0,031	0,706
One-Class SVM	0,066	0,329	0,110	0,556	0,139	0,228	0,671
LOF	0,047	0,047	0,047	0,588	0,061	0,047	0,953

3.6. Pembahasan Kinerja Model

Setiap metode menunjukkan karakteristik kinerja yang kontras. Isolation Forest mencatat skor F1 tertinggi pada dataset ini. Namun, keunggulan ini tidak serta-merta menunjukkan bahwa model tersebut optimal dalam menangkap seluruh anomali. Nilai recall yang hanya mencapai 0,294 mengindikasikan bahwa sebagian besar sampel anomali yang sebenarnya masih lolos dari deteksi. Di sisi lain, One-Class SVM mencapai nilai recall sebesar 0,329, sedikit lebih tinggi dibandingkan Isolation Forest. Akan tetapi, nilai presisinya yang sangat rendah (0,066) menunjukkan bahwa sebagian besar kejadian yang diidentifikasi sebagai anomali sebenarnya merupakan aktivitas normal berdasarkan label evaluasi. Dalam konteks sistem informasi akademik, kurangnya presisi ini berisiko memicu alarm palsu dalam jumlah berlebihan, yang pada akhirnya dapat mengganggu kenyamanan pengguna akibat seringnya permintaan verifikasi tambahan. LOF menunjukkan hasil terendah. Skor F1 sebesar 0,047 mengindikasikan bahwa pendekatan berbasis kepadatan lokal (local density-based) belum sesuai untuk representasi fitur yang digunakan. Hal ini mungkin disebabkan oleh pola *login* pengguna yang tidak selalu membentuk klaster kepadatan yang jelas. [10]

Temuan penelitian ini sejalan dengan penelitian yang mengidentifikasi perilaku login sebagai sumber informasi penting untuk mendeteksi penggunaan akun yang tidak wajar. Studi mengenai autentikasi berbasis risiko menunjukkan bahwa pemilihan fitur dan konfigurasi risiko perlu disesuaikan dengan karakteristik layanan. Penelitian lain juga menunjukkan bahwa pendekatan adaptif dapat digunakan untuk menyesuaikan tingkat tantangan autentikasi berdasarkan konteks risiko. Dari sisi perilaku pengguna, Folino dkk. menunjukkan bahwa pemodelan perilaku berdasarkan *log* dapat digunakan untuk mengurangi alarm palsu. Sementara itu, studi lain mengenai autentikasi perilaku menunjukkan bahwa karakteristik perilaku dapat melengkapi metode autentikasi tradisional. Temuan-temuan ini mendukung gagasan bahwa kejadian login sebaiknya tidak diperlakukan sebagai peristiwa yang berdiri sendiri.

3.7. Interpretasi Risiko

Tingkat risiko sebaiknya tidak dijadikan keputusan akhir melihat tanpa konteks. Misalnya, login dari perangkat baru pada awal semester dapat terjadi karena siswa mengganti perangkat. Sistem sebaiknya memberi ruang untuk verifikasi tambahan, bukan langsung memblokir akun.

Tabel 7. Risiko Respondens

Skenario	**Risko level**	**Rekomendasi Respondens**
Perangkat dan jaringan konsisten	Rendah	Izinkan akses
Perangkat baru atau IP baru	Sedang	Verifikasi tambahan
Waktu tidak biasa ditambah satu penyimpangan	Sedang	OTP / verifikasi
Berbagai penyimpangan serta kegagalan berulang	Tinggi	Peringatan MFA dan administrator

Pendekatan ini juga sejalan dengan gagasan otentikasi berbasis risiko yang menempatkan keamanan dan kegunaan dalam satu keputusan. Studi pengguna terhadap RBA menunjukkan bahwa pendekatan berbasis risiko dapat dipandang lebih nyaman dibandingkan autentikasi dua faktor yang diterapkan secara seragam

3.8. Implikasi bagi Sistem Informasi Akademik

Bagi administrator sistem informasi akademik, temuan penelitian ini memberikan beberapa implikasi praktis. Log masuk (login logs) sebaiknya disimpan secara konsisten untuk memastikan sistem memiliki data historis yang memadai guna menetapkan tolok ukur dasar (baseline). Data seperti stempel waktu, perangkat, alamat IP, status autentikasi, dan perubahan lokasi dapat disimpan dalam format yang diminimalkan dan dianonimkan. [11] Kalender akademik juga perlu diperhitungkan dalam konteks keamanan. Sistem dapat mengenali periode yang terkait dengan pendaftaran mata kuliah (KRS) dan penerbitan laporan hasil studi (KHS), sehingga lonjakan aktivitas kolektif tidak serta-merta memicu alarm. Sebaliknya, aktivitas individu yang menyimpang dari pola pengguna dan konteks sistem yang telah terbentuk dapat diberikan skor risiko yang lebih tinggi.

Terkait implementasinya, skor anomali dapat diintegrasikan di antara proses masuk dan keputusan akses, yang memungkinkan sistem menentukan respons berdasarkan skor risiko yang telah dihitung. Arsitektur sederhana ini dapat dikembangkan menjadi sistem autentikasi adaptif tanpa mengubah mekanisme nama pengguna dan kata sandi yang sudah ada.

3.9. Keterbatasan

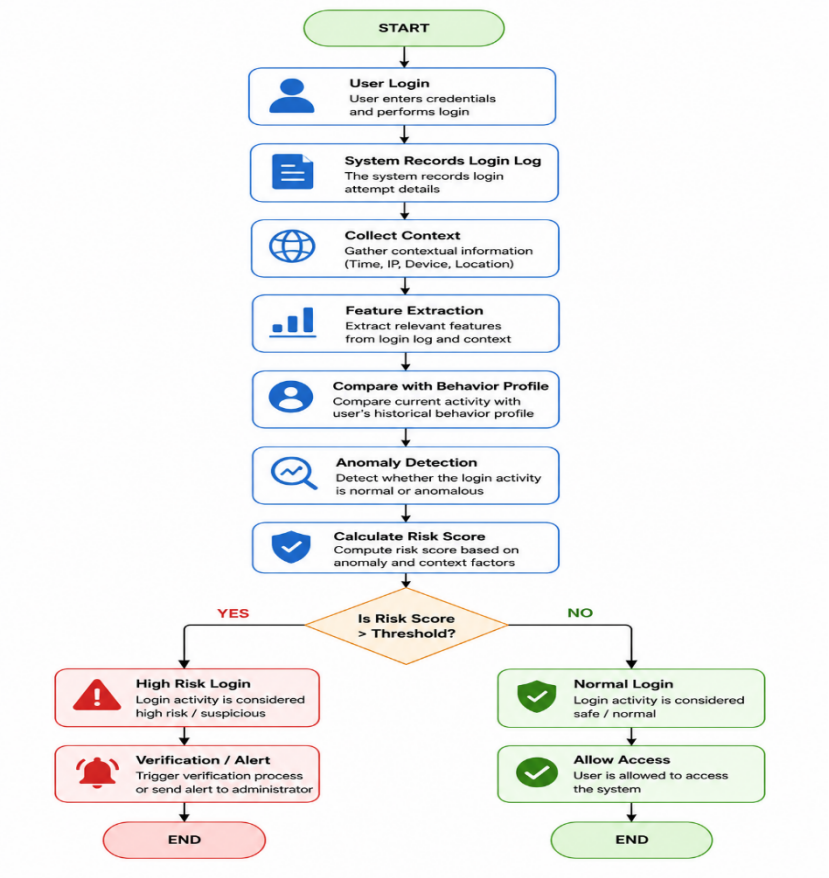
Studi ini memiliki beberapa keterbatasan. Pertama, label anomali dalam dataset bersifat sintetis. Oleh karena itu, 85 peristiwa yang dilabeli sebagai anomali tidak dapat dianggap sebagai 85 serangan nyata atau 85 akun yang benar-benar telah disusupi.

Kedua, periode pengamatan hanya mencakup dua bulan. Meskipun data tersebut memadai untuk mengamati perbedaan aktivitas antara periode KHS dan KRS, data tersebut tidak mencakup perubahan perilaku sepanjang satu tahun akademik penuh. Ketiga, data wilayah dan IP yang digunakan dalam dataset bersifat eksperimental; akibatnya, data tersebut tidak dapat digunakan untuk menentukan asal geografis serangan.

3.10. Alur proses sistem

Alur proses sistem deteksi anomali login dimulai ketika pengguna masuk ke Sistem Informasi Akademik dengan memasukkan kredensial mereka. Pada tahap ini, sistem menerima permintaan autentikasi dan mencatat setiap aktivitas login sebagai log login.

Selanjutnya, sistem mengumpulkan informasi kontekstual yang berkaitan dengan aktivitas login tersebut. Informasi yang dikumpulkan meliputi waktu login, alamat IP, perangkat yang digunakan, dan lokasi login. Informasi ini menjadi dasar untuk mengidentifikasi karakteristik lingkungan selama proses login berlangsung.



Gambar 4. Tahapan Alur Proses Sistem

3.11. Tinjauan Kembali

Kesenjangan Penelitian Penelitian sebelumnya telah menunjukkan efektivitas deteksi anomali, rekayasa fitur login, dan autentikasi berbasis risiko ketika diterapkan secara terpisah. Penelitian ini menggabungkan elemen-elemen tersebut dalam konteks akademik serta secara eksplisit memperhitungkan perubahan aktivitas yang dapat diprediksi akibat kalender akademik.

Oleh karena itu, pendekatan ini beralih dari definisi anomali yang murni bersifat statistik menuju definisi yang bersifat kontekstual. Suatu peristiwa dianggap mencurigakan bukan hanya karena sifatnya yang jarang terjadi, melainkan karena karakteristiknya tidak selaras dengan pola dasar (baseline) pengguna maupun konteks akademik di sekitarnya.

Penelitian di masa mendatang sebaiknya menggunakan log aktual yang telah dianonimisasi, label insiden yang telah diverifikasi oleh administrator, serta periode pengamatan yang lebih panjang. Pengujian juga dapat diperluas dengan menggunakan model ensemble atau pendekatan ambang batas (threshold) yang dikalibrasi berdasarkan biaya akibat false positive dan false negative.

3.12. Populasi dan Sampel Data

Populasi penelitian mencakup seluruh aktivitas login yang tercatat dalam Sistem Informasi Akademik selama periode penelitian. Jika memungkinkan, penelitian ini dapat menggunakan metode total sampling, yang berarti seluruh log login yang memenuhi kriteria penelitian digunakan sebagai dataset.

Sebagai contoh:

Data penelitian menggunakan log aktivitas login dari Sistem Informasi Akademik untuk periode Januari–Juni 2026. Jika jumlah data sangat besar, data tersebut dapat dibagi menjadi data pelatihan (training data) dan data pengujian (testing data), misalnya:

1. 80% data pelatihan

2. 20% data pengujian

Pembagian ini didasarkan pada periode waktu untuk mencegah kebocoran informasi (data leakage) antara data historis dan data pengujian.

3.13. Evaluasi Model

Untuk penelitian deteksi anomali, Precision, Recall, F1-Score, dan False Positive Rate harus menjadi fokus utama, karena sistem keamanan yang terlalu sering menandai login*normal sebagai ancaman dapat mengganggu pengalaman pengguna.

1. Akurasi=\frac{TP+TN}{TP+TN+FP+FN}
2. Presisi=\frac{TP}{TP+FP}
3. Recall=\frac{TP}{TP+FN}
4. F1-Score=2 \times \frac{Presisi \times Recall}{Presisi+Recall}

Keterangan:

1. TP = True Positive;
2. TN = True Negative;
3. FP = False Positive;
4. FN = False Negative.

4. KESIMPULAN

Berdasarkan hasil penelitian mengenai Deteksi Anomali Login Menggunakan Analisis Perilaku dan Penilaian Risiko Berbasis Konteks pada Sistem Informasi Akademik di Politeknik Kepribadian Bangsa, dapat ditarik kesimpulan sebagai berikut:

1 Sistem deteksi anomali login dapat dirancang berdasarkan pola perilaku pengguna dan informasi kontekstual dari aktivitas login. Data seperti waktu login, alamat IP, perangkat, lokasi, frekuensi login, dan riwayat aktivitas dapat digunakan sebagai fitur untuk menyusun profil perilaku pengguna.

2 Analisis perilaku pengguna dapat digunakan untuk mengidentifikasi aktivitas login yang menyimpang dari kebiasaan normal. Membandingkan aktivitas login saat ini dengan profil historis pengguna dapat membantu sistem mengenali perubahan pola, seperti login pada waktu yang tidak lazim, penggunaan perangkat baru, perubahan lokasi, atau perubahan alamat IP.

3 Pendekatan deteksi anomali dapat membantu meningkatkan kemampuan sistem dalam mengidentifikasi aktivitas login yang mencurigakan. Algoritma seperti Isolation Forest dapat digunakan untuk mengidentifikasi pola aktivitas yang berbeda dari pola normal.

4 Penilaian risiko berbasis konteks dapat memberikan hasil deteksi yang lebih adaptif. Dengan menggabungkan skor anomali dengan faktor-faktor seperti waktu, alamat IP, perangkat, lokasi, dan karakteristik perilaku pengguna, sistem dapat menghasilkan skor risiko yang mencerminkan tingkat risiko dari suatu aktivitas login tertentu.

Berdasarkan hasil penelitian ini, beberapa rekomendasi dapat disampaikan sebagai berikut:

1 Pengembangan dataset yang lebih besar dan lebih beragam perlu dilakukan dengan menggunakan data log aktivitas masuk (*login*) dalam rentang waktu yang lebih panjang, sehingga profil perilaku pengguna dapat dibentuk secara lebih akurat.

2 Fitur konteks tambahan dapat disertakan dalam penelitian mendatang, seperti jenis jaringan, penggunaan VPN/proksi, perubahan lokasi yang signifikan, *browser fingerprinting*, pola kegagalan *login*, dan aktivitas pengguna setelah berhasil masuk.

3 Perbandingan beberapa algoritma deteksi anomali dapat dilakukan untuk menentukan metode mana yang memberikan kinerja terbaik. Selain *Isolation Forest*, penelitian selanjutnya dapat membandingkan metode seperti *Local Outlier Factor*, *One-Class SVM*, *Autoencoder*, atau algoritma *machine learning* lainnya.
4 Penentuan ambang batas (*threshold*) Skor Risiko harus didasarkan pada hasil eksperimen dan karakteristik data aktual. Ambang batas yang terlalu rendah dapat meningkatkan *false positive*, sedangkan ambang batas yang terlalu tinggi dapat meningkatkan *false negative*.

DAFTAR PUSTAKA

[1] K. A. Nugroho, "Deteksi Anomali Trafik Jaringan dan Aktivitas Pengguna Menggunakan Isolation Forest untuk Meningkatkan Keamanan Jaringan," *Jurnal Pendidikan dan Teknologi Indonesia*, vol. 5, no. 5, pp. 1365–1376, May 2025, doi: 10.52436/1.jpti.790.
[2] A. F. Baig, S. Eskeland, and B. Yang, "Privacy-preserving continuous authentication using behavioral biometrics," *Int. J. Inf. Secur.*, vol. 22, no. 6, pp. 1833–1847, Dec. 2023, doi: 10.1007/s10207-023-00721-y.
[3] G. Folino, C. Otranto Godano, and F. S. Pisani, "An ensemble-based framework for user behaviour anomaly detection and classification for cybersecurity," *Journal of Supercomputing*, vol. 79, no. 11, pp. 11660–11683, Jul. 2023, doi: 10.1007/s11227-023-05049-x.
[4] A. R. Manik, D. Kiswanto, M. B. Akbar, and J. Purba, "Academic Portal with MFA (WhatsApp OTP via Fonnte), Role-Based Access Control, and Logging System for Network Monitoring," *Jurnal Ilmiah Sistem Informasi*, vol. 4, no. 3, pp. 674–687, Nov. 2025, doi: 10.51903/qwz6pt87.
[5] C. Chandra and D. Prima Mulya, "Deteksi Serangan Siber Menggunakan Machine Learning: Studi Pada Sistem Informasi Akademik," 2025. [Online]. Available: http://jurnal.unidha.ac.id/index.php/jiska
[6] A. K. Jailani and A. Erna, "Deteksi Anomali pada Rasio Jam Belajar dan Aktivitas Sosial terhadapPerforma Akademis Mahasiswa menggunakan Metode Local Outlier Factor (LOF)," 2012.
[7] P. B. Ramadani, A. Andhyka, and S. Mu'min, "ANALISIS KEAMANAN INFORMASI PADA SISTEM AKADEMIK TERPADU MENGGUNAKAN FRAMEWORK COMPTIA SECURITY+," 2026.
[8] L. Mohamed Hagrassi, A Behavioral Anomaly Detection Framework for Academic Information Systems Using Isolation Forest: A Case Study of Students and Academic Staff," *Comprehensive Journal of Science*, no. 11, 2026.
[9] J. Zhao *et al.*, "Detecting compromised email accounts via login behavior characterization," *Cybersecurity*, vol. 6, no. 1, Dec. 2023, doi: 10.1186/s42400-023-00167-8.
[10] M. Nerini, E. Favarelli, and M. Chiani, "Augmented PIN Authentication through Behavioral Biometrics," *Sensors*, vol. 22, no. 13, Jul. 2022, doi: 10.3390/s22134857.
[11] U. Uslu, Ö. D. Incel, and G. I. Alptekin, "Evaluation of Deep Learning Models for Continuous Authentication Using Behavioral Biometrics," in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 1272–1281. doi: 10.1016/j.procs.2023.10.115.