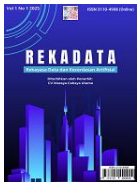

Rekayasa Data dan Kecerdasan Artifisial (REKADATA)
Volume: 2, **Issue:** 1, August 2026
Pages: 123-128
URL: https://journal.mazayacahayautama.com/index.php/rd
ISSN: 3110-4908 (ONLINE)

URL ISSN

Analisis Kebutuhan Sistem AI untuk Mendeteksi Perilaku Stalking pada Platform Media Sosial

Refinda Cheysar Wulandari [1]*, Riski Zulkarnain [2], Nasruddin Bin Idris [3]

[1] *Sistem Informasi, Universitas Mulia, Indonesia*
* *Email Penulis Korespondensi: refindacheysar@gmail.com*

Abstrak: Perkembangan pesat media sosial telah meningkatkan risiko perilaku stalking digital yang berdampak signifikan terhadap kesehatan mental dan privasi pengguna. Sistem keamanan konvensional saat ini masih bersifat reaktif dan kurang efektif dalam mendeteksi pola penguntitan yang tersembunyi. Penelitian ini bertujuan untuk mengidentifikasi karakteristik perilaku stalking dan merumuskan analisis kebutuhan sistem berbasis Kecerdasan Buatan (AI) untuk deteksi dini yang proaktif. Metode yang digunakan adalah kualitatif deskriptif dengan pengumpulan data melalui kuesioner terbuka terhadap 10 responden di Indonesia yang dipilih secara purposive untuk mewakili berbagai latar belakang demografis. Hasil penelitian menunjukkan bahwa perilaku stalking di Indonesia mencakup penggunaan akun anonim secara berulang, pemantauan lokasi (geotagging), dan pengawasan intensif terhadap riwayat aktivitas digital. Temuan utama penelitian ini mengidentifikasi kebutuhan sistem AI yang mampu menganalisis parameter frekuensi kunjungan profil oleh non-follower, deteksi pembuatan akun dari alamat IP yang sama, serta analisis sentimen pesan yang bersifat obsesif. Kebaruan penelitian ini terletak pada perumusan fitur proteksi preventif yang diinginkan pengguna, seperti Auto-Restrict, Stealth Mode, dan Photo Tracker. Kesimpulannya, implementasi sistem AI sangat mendesak untuk mentransformasi sistem keamanan media sosial dari pendekatan reaktif menjadi preventif guna memulihkan rasa aman pengguna tanpa melanggar hak privasi.

Keywords: Media Sosial, Stalking, Kecerdasan Buatan, Keamanan Digital, Analisis Kebutuhan Sistem.

Introduction

Transformasi digital global telah mendorong masyarakat untuk semakin bergantung pada teknologi informasi, khususnya platform media sosial yang kini menjadi ruang utama interaksi sosial dan pertukaran informasi [1]. Secara ideal, media sosial seharusnya menjadi lingkungan digital yang aman, interaktif, dan mendukung kreativitas pengguna. Namun, realitas yang terjadi menunjukkan adanya kesenjangan signifikan; kemudahan akses dan anonimitas yang ditawarkan platform digital justru membuka peluang bagi perilaku menyimpang, salah satunya adalah penguntitan digital atau stalking [2]. Perilaku ini mencakup pemantauan aktivitas seseorang secara berulang tanpa persetujuan, yang sering kali berkembang menjadi pelecehan siber (cyber harassment).

Penelitian terdahulu oleh Muhammad Akmal menunjukkan bahwa hukum pidana di Indonesia belum secara spesifik mengatur tindakan stalking sebagai kejahatan mandiri, sehingga penanganannya sering kali tidak efektif [3]. Di sisi lain, sistem keamanan pada platform media sosial saat ini masih bersifat reaktif, di mana tindakan baru diambil setelah adanya laporan pengguna (user report). Padahal, karakteristik stalking digital memungkinkan pelaku bekerja secara tersembunyi menggunakan akun anonim dalam jangka waktu lama sebelum korban menyadari dampaknya secara psikologis [4], [5].

Penggunaan teknik data mining sebenarnya telah terbukti efektif untuk menganalisis pola perilaku pengguna di media sosial [6]. Namun, terdapat celah penelitian (research gap) dalam merumuskan kebutuhan sistem yang spesifik untuk mendeteksi indikasi stalking secara proaktif sebelum eskalasi terjadi. Sebagian besar sistem moderasi saat ini masih kesulitan membedakan antara interaksi sosial normal dengan pola penguntitan yang obsesif. Oleh karena itu, diperlukan

pendekatan inovatif berbasis Kecerdasan Buatan (Artificial Intelligence/AI) yang mampu mengenali anomali perilaku berdasarkan data historis dan aktivitas real-time.

1.1 Novelty and Contribution

Kebaruan dalam penelitian ini terletak pada analisis kebutuhan sistem yang berfokus pada perspektif pengguna di Indonesia, mencakup identifikasi parameter teknis seperti frekuensi kunjungan profil non-pengikut dan pola pembuatan akun baru dari alamat IP yang sama. Berbeda dengan penelitian sebelumnya yang lebih banyak membahas aspek hukum atau dampak psikologis secara umum, penelitian ini berupaya merumuskan kebutuhan fungsional dan non-fungsional sistem AI yang dapat menjadi dasar pengembangan teknologi keamanan preventif di media sosial.

1.2 Research Objective

Tujuan utama dari penelitian ini adalah untuk mengidentifikasi karakteristik dan pola perilaku stalking pada platform media sosial, serta merumuskan indikator dan jenis data yang dibutuhkan oleh sistem berbasis AI untuk melakukan deteksi dini. Melalui analisis kebutuhan ini, diharapkan dapat tercipta kerangka kerja bagi pengembang sistem untuk membangun fitur keamanan yang lebih cerdas, akurat, dan tetap menghormati aspek etika serta privasi pengguna.

Methodology

Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk mengeksplorasi kebutuhan sistem keamanan digital dari perspektif pengguna. Berbeda dengan penelitian kuantitatif, metode ini dipilih untuk mendapatkan pemahaman mendalam mengenai pola perilaku subjektif dan harapan teknis terhadap implementasi Kecerdasan Buatan (AI) dalam mendeteksi penguntitan (stalking).

2.1 Objek dan Subjek Penelitian

Objek penelitian ini adalah pola interaksi digital yang mengarah pada perilaku stalking di berbagai platform media sosial (Instagram, TikTok, X, WhatsApp, dan Facebook). Subjek penelitian terdiri dari 10 responden yang dipilih menggunakan teknik purposive sampling untuk mewakili keragaman demografi pengguna di Indonesia, mulai dari generasi Z (mahasiswa dan atlet) hingga generasi X (orang tua dan pensiunan), guna mendapatkan spektrum kebutuhan sistem yang luas.

2.2 Instrumen dan Pengumpulan

Data Instrumen utama penelitian adalah kuesioner terbuka yang disebarkan melalui platform Google Form. Kuesioner ini dirancang untuk menggali tiga parameter utama: (1) pemahaman subjektif mengenai batasan perilaku stalking, (2) pengalaman empiris terkait bentuk penguntitan yang paling umum ditemui, dan (3) preferensi fitur serta mekanisme peringatan pada sistem deteksi berbasis AI. Prosedur penelitian dilakukan dalam tiga tahap: observasi awal terhadap tren keamanan digital, penyebaran kuesioner, dan verifikasi temuan melalui diskusi terfokus.

2.3 Teknik Analisis Data

Data yang terkumpul dianalisis menggunakan Teknik Analisis Tematik (Thematic Analysis). Langkah-langkah analisis meliputi:

- Kodifikasi: Memberikan label pada jawaban responden yang memiliki kemiripan pola perilaku (misalnya: penggunaan akun anonim, pelacakan lokasi).
- Kategorisasi: Mengelompokkan kode-kode tersebut ke dalam tema besar kebutuhan sistem (fungsional dan non-fungsional).
- Abstraksi: Merumuskan indikator teknis yang dapat diterjemahkan ke dalam algoritma AI, seperti frekuensi kunjungan profil dan pola pergantian alamat IP.
- Validasi: Membandingkan temuan dengan referensi penelitian terdahulu [6], [4] untuk memastikan bahwa kebutuhan sistem yang dirumuskan relevan dengan standar keamanan siber terkini.

Analisis difokuskan pada upaya menjembatani kebutuhan privasi pengguna dengan efektivitas algoritma pendeteksi tanpa menimbulkan kesalahan identifikasi (false positive).

Results and Discussions

Bagian ini memaparkan temuan penelitian yang diperoleh melalui kuesioner terbuka serta diskusi mendalam mengenai implikasi temuan tersebut terhadap pengembangan sistem AI untuk deteksi stalking.

Results

Data yang dikumpulkan dari 10 responden mencerminkan keragaman pengalaman dan kebutuhan terkait keamanan digital di berbagai lapisan masyarakat Indonesia.

1. **Karakteristik dan Pola Perilaku Stalking**
   Responden mengidentifikasi bahwa perilaku stalking di media sosial telah bergeser dari rasa ingin tahu (kepo) menjadi tindakan invasif yang sistematis. Responden 1 (Gen Z) dan Responden 10 (Atlet SMA) menyoroti penggunaan "akun kedua" atau akun palsu sebagai metode utama untuk menghindari blokir. Sementara itu, Responden 3 (Digital Nomad) menekankan bahwa fitur pelacakan lokasi (geotagging) sering disalahgunakan oleh pengikut obsesif untuk memantau keberadaan fisik korban secara real-time. Tabel 1 merangkum temuan bentuk stalking yang paling umum dialami oleh responden.
2. **Dampak Psikologis dan Sosial terhadap Korban**
   Temuan menunjukkan dampak yang signifikan terhadap perilaku digital korban. Responden 7 (Seniman) menyatakan bahwa tindakan penguntitan menyebabkan "matinya kreativitas" karena korban merasa tidak aman untuk mengunggah karya atau kehidupan pribadi. Responden 10 merasa diteror oleh pesan "Aku tahu kamu sedang online," yang memicu kecemasan akut. Secara umum, korban merespons dengan melakukan "ghosting" digital atau membatasi lingkaran pertemanan secara ekstrem, yang pada akhirnya mengurangi manfaat sosial dari platform tersebut.
3. **Analisis Kebutuhan Sistem AI**
   Responden menyepakati bahwa sistem moderasi manual saat ini terlalu lambat. Kebutuhan utama yang dirumuskan mencakup kemampuan AI untuk mengenali pola anomali sebelum terjadi kontak langsung. Parameter utama yang disarankan untuk dianalisis oleh AI meliputi:
   - Analisis Frekuensi: Deteksi akun non-pengikut yang melihat profil lebih dari frekuensi wajar dalam waktu singkat.
   - Korelasi IP Address: Mengenali jika akun baru yang dibuat berasal dari perangkat atau jaringan yang sama dengan akun yang telah diblokir sebelumnya.
   - Analisis Sentimen: Mendeteksi perubahan nada komunikasi dari apresiatif menjadi obsesif atau intimidatif.

Discussions

Diskusi ini mengaitkan temuan lapangan dengan teori keamanan siber dan potensi implementasi teknologi AI.

1. **Transformasi Paradigma Keamanan: Dari Reaktif ke Preventif** Hasil penelitian mendukung argumen bahwa sistem keamanan media sosial saat ini gagal melindungi privasi pengguna secara memadai. Kesenjangan antara realitas stalking yang agresif dan fitur keamanan yang pasif menciptakan kebutuhan akan sistem AI yang bekerja secara proaktif. Sistem AI yang diusulkan tidak hanya menunggu laporan pengguna, tetapi juga melakukan deteksi anomali perilaku (behavioral anomaly detection). Misalnya, penggunaan fitur Auto-Restrict berbasis AI dapat langsung membatasi akses akun mencurigakan terhadap konten sensitif milik korban tanpa perlu intervensi manual.
2. **Integrasi Fitur Proteksi Berbasis Konteks** Berdasarkan temuan, fitur yang paling relevan adalah kontrol berbasis konteks. Fitur Stealth Mode yang disarankan oleh

Responden 9 menunjukkan perlunya AI yang mampu menyembunyikan status pengguna hanya dari subjek yang terdeteksi sebagai penguntit. Hal ini sejalan dengan teori etika TI yang menekankan keseimbangan antara fungsionalitas teknologi dan perlindungan data pribadi. Implementasi Photo Tracker juga menjadi inovasi penting untuk mencegah penyalahgunaan identitas digital yang sering menimpa pengguna dari kalangan orang tua (Responden 4).

3. **Tantangan Etika dan Privasi dalam Implementasi AI** Meskipun responden sangat menginginkan bantuan AI, terdapat kekhawatiran mengenai privasi (Responden 5 dan 9). Jika AI menganalisis setiap interaksi, muncul risiko pengawasan massal oleh platform media sosial itu sendiri. Oleh karena itu, arsitektur sistem deteksi ini sebaiknya mengadopsi prinsip On-Device AI atau enkripsi end-to-end pada pemrosesan datanya. Hal ini penting agar tujuan awal untuk melindungi korban dari penguntit tidak berubah menjadi pelanggaran privasi oleh penyedia layanan platform.
4. **Perbandingan dengan Penelitian Terdahulu** Penelitian ini memperkuat temuan Dhir et al. mengenai analisis perilaku [4], namun menambahkan dimensi baru berupa kebutuhan akan fitur respons otomatis yang spesifik untuk kasus stalking. Jika penelitian sebelumnya lebih fokus pada klasifikasi data secara umum, penelitian ini memberikan landasan operasional bagi pengembang sistem untuk memprioritaskan fitur-fitur yang secara langsung merespons ketakutan terbesar pengguna di Indonesia, seperti pelacakan lokasi dan akun palsu berulang.

Table 1. Bentuk Perilaku Stalking yang Teridentifikasi

Kategori Stalking	Deskripsi Perilaku	Responden Terkait
Pengawasan Profil	Melihat Story secara anonim dan berulang melalui situs pihak ketiga.	R1, R7, R10
Interaksi Invasif	Deep-liking foto lama dan komentar berlebihan yang bersifat pribadi.	R2, R7
Pelacakan Lokasi	Memantau unggahan lokasi untuk mendatangi korban di dunia nyata.	R3, R6
Manipulasi Identitas	Pencurian foto pribadi untuk akun palsu atau penipuan.	R4
Spionase Digital	Pemantauan status "Online" atau "Last Seen" secara konstan.	R9, R10

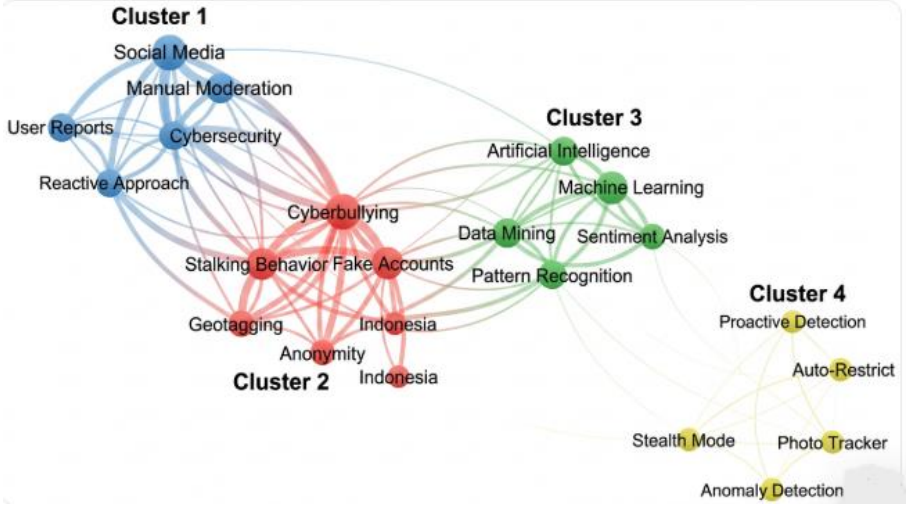

Figure 1. final network map

Conclusion

Penelitian ini berhasil merumuskan analisis kebutuhan sistem AI untuk mendeteksi perilaku stalking di media sosial dengan mengintegrasikan perspektif pengguna di Indonesia. Hasil penelitian menyimpulkan bahwa karakteristik stalking telah berevolusi menjadi tindakan invasif sistematis yang memanfaatkan fitur anonimitas dan pelacakan lokasi, yang menyebabkan dampak psikologis serius berupa kecemasan dan pembatasan ekspresi digital. Analisis kebutuhan menunjukkan bahwa sistem keamanan saat ini yang bersifat reaktif tidak lagi memadai, sehingga diperlukan transformasi menuju sistem AI proaktif yang mampu melakukan deteksi anomali perilaku melalui analisis frekuensi kunjungan profil, korelasi alamat IP, dan analisis sentimen komunikasi.

Fitur inovatif seperti Auto-Restrict, Stealth Mode, dan Photo Tracker diidentifikasi sebagai solusi teknis yang paling diinginkan pengguna untuk memberikan perlindungan tanpa memicu konflik langsung dengan pelaku. Namun, implementasi sistem ini harus tetap memperhatikan batasan etika dan privasi melalui arsitektur On-Device AI agar tidak menjadi alat pengawasan massal oleh platform. Sebagai saran, pengembang platform media sosial perlu memprioritaskan integrasi algoritma machine learning yang fokus pada pencegahan dini, sementara peneliti selanjutnya dapat mengeksplorasi efektivitas model deteksi tersebut dalam skala data yang lebih besar guna meningkatkan akurasi dan meminimalkan kesalahan identifikasi.

References

[1] C. S. Octiva, T. I. Fajri, E. B. Sulistiarini, S. Suharjo, and U. W. Nuryanto, "Penggunaan Teknik Data Mining untuk Analisis Perilaku Pengguna pada Media Sosial," *J. Minfo Polgan*, vol. 13, no. 1, pp. 1074–1078, Jul. 2024, doi: 10.33395/jmp.v13i1.13936.

[2] D. Yunika Zebua and A. P. Zebua, "TANTANGAN ETIKA DALAM PROFESI TEKNOLOGI INFORMASI," 2025.

[3] M. Akmal, F. Riyadi, K. Andana, and A. Haq, "SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika Deteksi Pelecehan Seksual dan Predator Obrolan Media Sosial Menggunakan Naive Bayes," 2024, doi: 10.31284/p.snestik.2024.5882.

[4] A. Dhir, S. Talwar, P. Kaur, S. Budhiraja, and N. Islam, "The dark side of social media: Stalking, online self-disclosure and problematic sleep," *Int. J. Consum. Stud.*, vol. 45, no. 6, pp. 1373–1391, Nov. 2021, doi: 10.1111/ijcs.12659.

[5] Y. Yusman, N. Anida, and Z. M. Noor, "Pendekatan Big Data dalam Mendeteksi Deviasi Perilaku Seksual Remaja pada Platform Media Sosial," *Pros. Semin. Nas. Teknol. Komput. dan Sains*, vol. 3, no. 1, pp. 48–52, 2025, [Online]. Available: https://prosiding.seminars.id/sainteks

[6] L. Rachmaria and A. Susanto, "Jurnal Netnografi Komunikasi (JNK) POTENTIAL FOR ONLINE-BASED GENDER VIOLENCE IN THE MISUSE OF ARTIFICIAL INTELLIGENCE

TECHNOLOGY FOR WOMEN IN SOCIAL MEDIA," 2024. [Online]. Available: http://netnografiikom.org/index.php/netnografi