

Deteksi dan Respons Defacement Judi Daring pada Situs Web Indonesia melalui Tinjauan Literatur Terstruktur

¹Gilbert Aldrich Rumahorbo, ²Ammar Kamil Al-Abror, ³Akbar Alif Haikal

^{1,2,3}Program Studi Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan

Jl. Willem Iskandar, Pasar V, Medan Estate, Kecamatan Percut Sei Tuan, Kabupaten Deli Serdang, Sumatera Utara 20221, Indonesia

e-mail: ¹aldrichgar@gmail.com, ²ammarkamil1310@gmail.com, ³akbaralifhaikal92@gmail.com

Abstrak

Defacement judi daring pada situs sah dapat menimbulkan perubahan berkas, tautan tersembunyi, pengalihan, dan promosi visual. Kajian ini memetakan bukti deteksi, mengaudit konsistensi pelaporan, serta merumuskan kerangka evaluasi deteksi, karantina, dan pemulihan. Tinjauan literatur terstruktur menggunakan korpus lokal 30 PDF, bukan pencarian komprehensif basis data. Deduplikasi dan pemeriksaan kelayakan menghasilkan 26 karya; satu review terbuka ditambahkan sebagai pembandingan, sehingga terdapat 27 rujukan terbitan 2020–2026, terdiri atas 21 studi teknis dan enam sumber pendukung. Ekstraksi mencatat objek, sumber data, metode, jumlah data, skema pengujian, metrik, hasil, dan keterbatasan. Sintesis membedakan deteksi kompromi halaman, webshell, promosi perjudian, dan domain perjudian karena unit analisis serta tujuan pengujiannya berbeda. Prototipe telah menghubungkan deteksi dengan karantina, tetapi bukti tersebut belum menetapkan keselamatan tindakan atau pemulihan layanan. Audit ringkas menunjukkan ketidaksesuaian beberapa metrik dengan matriks konfusi dan penafsiran pembulatan sebagai hasil sempurna. Skor tidak digabungkan atau diperingkat lintas tugas. Kerangka evaluasi yang diusulkan menempatkan positif palsu, dampak karantina, verifikasi integritas, salinan tepercaya, dan kejadian ulang sebagai keluaran yang perlu diuji bersama. Kontribusi kajian berupa sintesis bukti yang terbatas pada korpus, bukan algoritma baru atau validasi sistem operasional.

Kata kunci: defacement situs web; judi daring; deteksi; respons insiden; tinjauan literatur

Abstract

Online gambling defacement of legitimate websites can involve file changes, hidden links, redirects, and visual promotions. This review maps detection evidence, audits reporting consistency, and develops an evaluation framework for detection, quarantine, and recovery. The structured literature review uses a local corpus of 30 PDFs rather than a comprehensive database search. Deduplication and eligibility assessment retained 26 works; one open access review was added for comparison, yielding 27 references published in 2020–2026, comprising 21 technical studies and six supporting sources. Extraction covered objects, data sources, methods, sample sizes, testing schemes, metrics, findings, and limitations. The synthesis distinguishes compromised page detection, webshell detection, gambling promotion detection, and gambling domain detection because their units and testing objectives differ. Prototypes connect detection with quarantine, but this evidence does not establish action safety or service recovery. A concise audit identifies discrepancies between some metrics and confusion matrices, including rounding interpreted as perfect performance. Scores were neither pooled nor ranked across tasks. The proposed framework treats false positives, quarantine impact, integrity verification, trusted copies, and recurrence as outcomes requiring joint evaluation. The contribution is a corpus limited evidence synthesis, not a new algorithm or an operationally validated system.

Keywords: web defacement; online gambling; detection; incident response; literature review

1. Pendahuluan

Defacement judi daring adalah perubahan tanpa izin pada situs sah untuk menampilkan atau mengarahkan pengunjung ke materi perjudian. Dampaknya mencakup hilangnya integritas konten dan terganggunya layanan. Nurseno, Aditiawarman, Al Qodri Maarif, dan Mantoro (2024) menelaah tautan perjudian tersembunyi pada domain .go.id, sedangkan Zagi, Digdo, dan Shalannanda (2025) mengamati perubahan judul, tautan, pengalihan, dan kejadian berulang. Pengenalan situs operator perjudian saja belum menjelaskan kompromi pada situs institusi yang domainnya tetap sah.

Saepul dan Rifa'i (2025) memberi konteks perjudian di Asia Tenggara, sementara Hong et al. (2022) menunjukkan kanal aplikasi dan penipuan seluler. Konteks ini membantu memahami distribusi materi perjudian, tetapi tidak menjadi ukuran prevalensi kompromi server Indonesia. Bukti teknis juga terpisah: Erawan et al. (2024) mengamati berkas, Rizal dan Widodo (2026) mengklasifikasikan webshell, dan Ajhari, Aji, Mantau, Jatmiko, dan Pratama (2026) mengolah gambar serta teks. Keberhasilan pada salah satu objek belum menetapkan keberhasilan pertahanan situs secara keseluruhan.

Review Albalawi et al. (2022) telah merangkum deteksi dan pemantauan defacement berdasarkan anomali, signature, pembelajaran mesin, serta alat pemantauan. Kajian ini melanjutkan pembahasan pada konteks judi daring Indonesia dengan menautkan objek pengamatan, keterlacakan hasil, dan keselamatan respons. Kontribusi ilmiahnya ialah pemetaan bukti menurut unit analisis, audit konsistensi pelaporan, dan kerangka evaluasi terpadu deteksi-karantina-pemulihan. Kerangka ini merupakan usulan berbasis sintesis, bukan algoritma baru atau sistem yang telah divalidasi.

Tiga pertanyaan penelitian memandu kajian: (1) objek dan lapisan apa yang dideteksi; (2) sejauh mana data serta skema pengujian mendukung klaim kinerja; dan (3) tindakan respons serta keluaran pemulihan apa yang telah diuji.

Jawabannya dibatasi pada dokumen yang tersedia. Istilah terstruktur merujuk pada seleksi, ekstraksi, dan sintesis yang dicatat, tanpa menyatakan cakupan systematic review komprehensif.

2. Metode Penelitian

2.1 Cakupan dan Seleksi Literatur

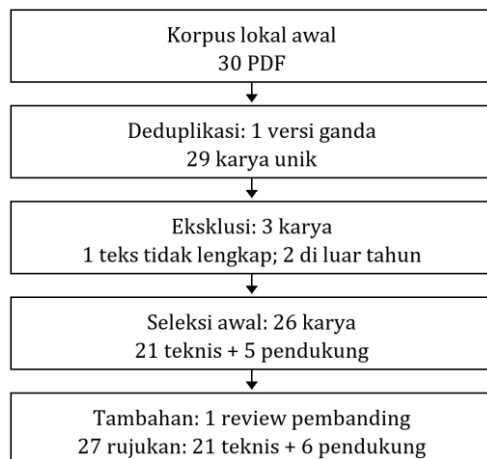
Tinjauan ini menggunakan sintesis naratif atas korpus lokal yang diinventarisasi pada 1 Oktober 2026. Unit inventaris ialah PDF, sedangkan unit telaah ialah karya ilmiah. Tersedia 30 PDF pada folder Referensi dan subfolder SAINSTECH. Kueri dan hasil penelusuran basis data yang mendahului pengumpulan berkas tidak tersedia; seleksi lokal tidak menggantikan rekaman tersebut. Karena itu, hasil tidak dianggap mewakili seluruh literatur.

Kriteria inklusi diterapkan berurutan: karya terbit pada 2017–2026; teks yang tersedia memadai untuk memeriksa klaim; dan isi membahas kompromi situs, webshell, situs/domain perjudian, promosi, kanal distribusi, atau dukungan metodologis dan autentikasi yang relevan. Studi teknis harus menjelaskan metode, implementasi, atau hasil. Ketidadaan ukuran kinerja tidak menyebabkan eksklusi otomatis: studi implementasi dipertahankan dengan batas bukti, tanpa dianggap evaluasi akurasi. Sumber konteks dan metode dipisahkan dari studi teknis.

Eksklusi mencakup versi ganda dari karya yang sama, teks yang tidak memuat metode/hasil yang diperlukan, serta tahun di luar rentang. Dua PDF Hong et al. (2022) dihitung sebagai satu karya dan versi publikasi dipilih. Dari 29 karya unik, tiga dikeluarkan: satu tugas akhir yang hanya tersedia bagian awal, panduan review 2007, dan artikel VOSviewer 2010. Dua terakhir dikeluarkan berdasarkan tahun, bukan penilaian mutu. Seleksi awal menghasilkan 26 karya: 21 teknis dan lima pendukung.

Untuk membandingkan posisi kajian saat revisi, penelusuran terbatas Crossref pada 7 Oktober 2026 memakai kueri “website defacement detection survey”

dan lima hasil teratas. Review Albalawi et al. (2022) dipilih karena secara langsung membahas deteksi/pemantauan defacement; teks penuh penerbit tersedia bebas dengan lisensi CC BY 4.0. Penambahan ini terpisah dari seleksi awal dan bukan pencarian sistematis tambahan. Total menjadi 27 rujukan, dengan enam sumber pendukung. Gambar 1 merangkum alurnya; rentang terpilih aktual adalah 2020–2026.



Gambar 1. Seleksi korpus lokal dan tambahan review pembandingan

2.2 Ekstraksi dan Verifikasi

Ekstraksi mencatat delapan bidang: objek, dataset/sumber, metode, jumlah data, skema pengujian, metrik, hasil utama, dan keterbatasan. Pemeriksaan kualitatif menilai kejelasan data dan label, pemisahan data, konsistensi angka, serta bukti operasional; tidak diberikan skor kualitas baku. Nilai yang tidak dapat dipastikan ditulis sebagai tidak jelas atau tidak dilaporkan. Penghitungan ulang dilakukan hanya jika matriks dan penyebut tersedia, tanpa menjalankan ulang model atau merekonstruksi data yang hilang.

Teks penuh menjadi dasar klaim. Ekspor bibliografi yang menyertai penyusunan awal digunakan sebagai bantuan, kemudian dibandingkan dengan halaman artikel dan metadata penerbit/Crossref yang tersedia. Catatan halaman dan keputusan disimpan dalam lampiran verifikasi. Page et al. (2021) mendukung transparansi pelaporan tanpa klaim pemenuhan semua butir PRISMA.

Syahadat, Anashir, dan Zulfa (2026) memberi contoh tinjauan naratif dan Kusuma (2025) contoh bibliometrik lintas bidang; keduanya hanya mendukung pembedaan metode. Kajian ini tidak menghasilkan jaringan sitasi atau peta VOSviewer.

3. Hasil dan Pembahasan

3.1 Objek Deteksi dan Pemetaan Bukti

Empat tugas utama perlu dibedakan. Deteksi defacement menilai perubahan tanpa izin pada halaman situs sah; webshell menilai kode yang menyediakan akses penyerang; promosi judi menilai pesan atau gambar promosi; domain judi menilai identitas tujuan perjudian. Webshell dapat menjadi sarana kompromi tanpa materi judi, sedangkan promosi dapat muncul pada komentar tanpa kompromi host. Domain resmi yang terdefacement juga tidak identik dengan domain operator judi. Karena itu, label positif dan tindakan yang tepat berbeda untuk setiap tugas.

Dari 21 studi teknis, tujuh berfokus pada host/webshell, empat pada halaman/teks situs, dua pada domain/permintaan, enam pada promosi teks/gambar, dan dua pada kanal seluler. Enam pendukung mencakup konteks, metode, autentikasi, dan review pembandingan. Tabel 1–3 menyajikan delapan bidang ekstraksi; jumlah korpus dibedakan dari jumlah uji. Hasil bertanda hitung ulang merupakan aritmetika matriks yang tersedia; hasil lain mengikuti laporan sumber. Ketidadaan informasi merupakan keterbatasan pelaporan, bukan bukti bahwa pengujian tidak dilakukan. Kode S menghubungkan baris dengan atribusi sumber dan lampiran verifikasi.

Tabel 1.
Matriks bukti host dan webshell

Studi dan objek	Data dan sumber	Metode	Jumlah data	Skema pengujian	Metrik	Hasil utama	Batas bukti
S05 Injeksi berkas	Server terkena injeksi	Bash, inotify, karantina	Tidak tercatat	Mesin virtual AlmaLinux	CPU memori	≈1% <20 MB Telegram	Akurasi belum diukur
S03 Webshell PHP	Korpus PHP unik	Fitur kode, Random Forest, FIM	6.015 uji 1.207	Uji 20% laporan prototipe	Akurasi presisi recall	97,02% hitung ulang karantina	Metrik per kelas berbeda
S06 Webshell halaman	Sampel internet	Wazuh, auditd, active response	10 kode 5 halaman 5 reverse shell	Skenario serangan	Deteksi fungsi respons	10/10 5/5 karantina 5/5 blokir	2 alert berkas besar tidak tampil
S07 Berkas unggah	Uji FIM dan unggahan	Wazuh Snort signature	80 aksi 13 unggahan	Uji serangan terpilih	Rasio deteksi	80/80 FIM 10/13 Snort	Tanpa penyebut negatif sah
S10 Webshell PHP	Repositori PHP	Token keamanan, CodeBERT	6.430 berkas	Repositori dan partisi lain	Akurasi F1	99,02% 96,95% akurasi	512 token bukan family holdout
S09 Webshell	Direktori 5 host	Shelltrap	1.085–2.664 berkas per host	Pindai host	Deteksi memori	98% dilaporkan	Host/rumus berbeda
S20 Aktivitas webshell	Situs uji penelitian	Webshell diberi log email	Tidak tercatat	Uji fungsi	Fungsi logging	Log terkirim	Hanya artefak diberi log

Sumber: S05 = Erawan et al. (2024); S03 = Rizal dan Widodo (2026); S06 = Arman, Wahyu Azinar, Senja Fitriani, dan Eviyanti (2026); S07 = Reza Pahlevi, Umam, dan Handoko (2025); S10 = Adli Pratama et al. (2026); S09 = Waliulu dan Jumame (2020); S20 = Gumilang dan Chandra (2021). Informasi tidak tercatat/tidak jelas mengikuti ketersediaan pelaporan sumber. FIM: file integrity monitoring. CPU: central processing unit.

Tabel 2.
Matriks bukti halaman, domain, permintaan, dan seluler

Studi dan objek	Data dan sumber	Metode	Jumlah data	Skema pengujian	Metrik	Hasil utama	Batas bukti
S21 Halaman .go.id	Kandidat hasil scraping	Kata kunci, verifikasi	1.482 calon 958 kasus	Saring halaman	Positif akurasi laporan	970 positif –12 positif palsu	Bukan prevalensi daftar domain
S08 Halaman situs	Perayapan situs Indonesia	Dork dan crawl	453 calon 346 pada 147 situs	Observasi ≈1 bulan	Waktu reaksi	Pertama rata-rata 74,7 jam	Indikator hilang ≠ akar teratasi
S19 Konten situs	Halaman situs pada server	Laravel wordlist	Tidak tercatat	Uji fungsi	Hitungan kata	High Middle Low	Uji angka belum memadai

Studi dan objek	Data dan sumber	Metode	Jumlah data	Skema pengujian	Metrik	Hasil utama	Batas bukti
S11 Teks situs judi	Scraping Blog SEMrush	SVM CNN	24.336 judi 36.529 sah uji 9.734	80:20 validasi lima lipatan	Akurasi F1	CNN 99,60% hitung ulang	Bulat ke 100% transfer terbatas
S16 Domain judi	Sertifikat dan nama domain	Fusi fitur	10.000 judi 10.000 sah	Latih:uji 4:1	Akurasi	99,36% dilaporkan	Integritas host tak diuji
S18 POST dan perilaku	POST: cookie, badan, kata kunci	Word2Vec TF-IDF SDAE kelompok	Tidak jelas	Uji antar kelompok	Siluet akurasi recall	0,57 98,216% 98,942%	Ukuran dan split tak jelas
S29 SMS/URL judi	SMS KISA, Korea	Morfologi hashing SVM	30.527 pesan	75:25 stratifikasi pencarian empat lipatan	Akurasi	97,96% dilaporkan	Bahasa dan kanal spesifik
S14 Penipuan aplikasi	Aplikasi dan laporan 2020	Analisis empiris	1.487 aplikasi 1.461 laporan	Observasi insiden	Pola penipuan	Pemetaan modus aplikasi	Bukan uji detektor halaman

Sumber: S21 = Nurseno et al. (2024); S08 = Zagi et al. (2025); S19 = Hikmatyar, Sudiarjo, Ruuhwan, Ismu Arief, dan Fadilah (2024); S11 = Simanjuntak dan Muhammad (2025); S16 = Sun et al. (2023); S18 = Zhang, Han, Wu, Sun, dan Shi (2025); S29 = Min, Lee, dan Lee (2022); S14 = Hong et al. (2022). Informasi tidak tercatat/tidak jelas mengikuti ketersediaan pelaporan sumber. SVM: support vector machine; CNN: convolutional neural network; SDAE: stacked denoising autoencoder. Siluet merujuk pada silhouette score. Sebanyak 958 kasus S21 terkonfirmasi mengandung indikator perjudian.

Tabel 3.

Matriks bukti promosi teks dan gambar

Studi dan objek	Data dan sumber	Metode	Jumlah data	Skema pengujian	Metrik	Hasil utama	Batas bukti
S30 Komentar	Satu video YouTube	Regex normalisasi fuzzy match	1.493 uji 448/298	70:30 dan 80:20	Akurasi	90,85% / 87,58%	Nama kelas tidak konsisten
S12 Teks judi	Kalimat contoh	Levenshtein Ambang 70%	10 kalimat	Uji contoh input	Blokir teks	Kata cocok diblokir	Sampel kecil label berbeda
S04 Promosi teks	Komentar YouTube	IndoBERT Naïve Bayes SVM	Uji 2.264	Data uji disebut terpisah	Akurasi matriks	SVM 98,85% hitung ulang	Kelas/kategori terbaik berbeda
S17 Promosi teks	Komentar YouTube	IndoBERT model lain	3.241 narasi uji 342	80:10:10 standar rata	Akurasi F1	98,53% 97,24%	Jumlah uji beda rasio
S24 Spam sama-r	Subset komentar YouTube	IndoBERT + LinearSVC	6.000 uji 900	Uji 50:50 spam sama-r	Akurasi matriks	99,78% sama dengan IndoBERT	Transfer pre-revalensi belum diuji

Studi dan objek	Data dan sumber	Metode	Jumlah data	Skema pengujian	Metrik	Hasil utama	Batas bukti
S13 Gambar judi	Gambar ragam bahasa OCR	Cross-modal attention	4.485 uji 755	Uji label 70:15:15 laporan	Akurasi F1 recall	99,47% 99,47% 100%	Split berbeda latensi parsial

Sumber: S30 = Cahyo, Hermawan, Wijaya, dan Sari (2025); S12 = Puji Saputra (2025); S04 = Samuel dan Prasetya Kristiadi (2025); S17 = Liem, Djatmiko Utomo, Ignasio, dan Cenggoro (2025); S24 = Hidayat, Chamid, dan Jazuli (2026); S13 = Ajhari et al. (2026). Informasi tidak tercatat/tidak jelas mengikuti ketersediaan pelaporan sumber.

3.2 Makna Bukti Pada Tiap Lapisan

Pada host, pemantauan integritas berkas atau file integrity monitoring (FIM) mengenali penambahan, perubahan, dan penghapusan; klasifikasi kode memberi penilaian lanjutan. Erawan et al. (2024) sudah mengintegrasikan pemeriksaan, karantina, dan Telegram dengan biaya rendah pada satu mesin virtual. Rizal dan Widodo (2026) memindahkan webshell terdeteksi ke luar web root, sedangkan Arman et al. (2026) memperlihatkan keberhasilan fungsi karantina bersama keterbatasan keterlihatan alert. Bukti ini mendukung integrasi awal, tetapi biaya sumber daya dan keberhasilan skenario belum mengukur dampak pada seluruh layanan.

Keterbatasan representasi tetap menentukan cakupan. Reza Pahlevi et al. (2025) melewati tiga dari 13 unggahan berbahaya yang menyamar sebagai gambar. Adli Pratama et al. (2026) menunjukkan bahwa skor tinggi masih dapat bergantung pada komposisi token; pemotongan kode dan kamus membatasi generalisasi. Pemindaian Waliulu dan Jumame (2020) tidak menyediakan matriks lengkap, sementara pencatatan Gumilang dan Chandra (2021) memerlukan webshell yang diinstrumentasi. Penilaian keamanan perlu memisahkan deteksi perubahan, klasifikasi artefak, pencatatan aktivitas, dan keberhasilan tindakan.

Perayapan memberi pandangan dari luar host. Nurseno et al. (2024) mengonfirmasi kandidat konten tersembunyi dan Zagi et al. (2025) mengukur reaksi terhadap indikator defacement; keduanya tidak menguji

penghapusan semua akses penyerang. Pemindai Hikmatyar et al. (2024) berguna untuk penandaan berbasis kata, sedangkan Simanjuntak dan Muhammad (2025) menilai teks situs setelah penyeimbangan kelas. Klasifikasi teks situs tidak membedakan secara otomatis situs operator dari situs sah yang disusupi. Ground truth harus menyatakan status tersebut agar keluaran dapat digunakan untuk respons yang tepat.

Domain dan jejak permintaan menambah konteks, bukan pengganti inspeksi host. Sun et al. (2023) mengenali domain melalui nama dan sertifikat; Zhang et al. (2025) mengelompokkan pesan POST serta perilaku. Domain tujuan yang berisiko dapat memperkuat indikasi tautan, tetapi situs institusi sah bisa tetap memakai sertifikat dan nama yang normal. Min et al. (2022) dan Hong et al. (2022) memperluas pemahaman kanal seluler; hasil dari SMS Korea atau aplikasi penipuan tidak ditransfer langsung sebagai ukuran deteksi kompromi situs Indonesia.

Pada promosi teks, aturan Cahyo et al. (2025) dan Puji Saputra (2025) menyediakan pembandingan sederhana yang perlu diuji terhadap variasi bahasa dan salah pemblokiran. Samuel dan Prasetya Kristiadi (2025) dan Liem et al. (2025) mengevaluasi model bahasa pada komentar, sedangkan fusi Hidayat et al. (2026) menyamai IndoBERT pada pengujian yang dilaporkan. Ini tidak menetapkan manfaat tambahan fusi secara umum. Ajhari et al. (2026) menggabungkan citra dan teks hasil optical character recognition (OCR) untuk promosi tersamar; keberhasilan klasifikasi gambar tidak menentukan

keberadaan webshell atau asal perubahan tanpa izin. Latensi model juga harus dibedakan dari keseluruhan alur OCR, pemrosesan, dan respons.

3.3 Audit Ringkas dan Validitas Evaluasi

Tiga contoh utama menunjukkan fungsi audit. Pada Rizal dan Widodo (2026), 555 prediksi positif benar, 616 negatif benar, tujuh positif palsu, dan 29 negatif palsu menghasilkan akurasi 97,02%, presisi 98,75%, serta recall 95,03%; statistik per kelas pada tabel sumber berbeda. Pada Simanjuntak dan Muhammad (2025), 9.695 prediksi benar dari 9.734 menghasilkan 99,60%, sehingga pembulatan 100% tidak berarti tanpa kesalahan. Pada Samuel dan Prasetya Kristiadi (2025), matriks SVM menghasilkan 98,85%, berbeda dari angka 98,3% pada uraian. Nilai hitung ulang menguji konsistensi aritmetika, bukan validitas label atau desain eksperimen.

Masalah lain cukup dicatat pada kolom keterbatasan dan lampiran. Validitas eksternal bergantung pada duplikasi, templat situs, komposisi kelas, serta waktu. Data yang mirip pada pelatihan dan pengujian berpotensi menaikkan skor; potensi ini perlu diperiksa dan tidak dianggap kebocoran yang terbukti pada semua studi. Uji berdasarkan domain, repositori, keluarga artefak, dan periode baru diperlukan sesuai objek. Akurasi pada dataset seimbang juga tidak memperkirakan langsung beban alarm ketika data sah mendominasi.

3.4 Posisi Kajian Terhadap Karya Terdahulu

Review Albalawi et al. (2022) mengelompokkan pendekatan anomali, signature, pembelajaran mesin, dan alat pemantauan, serta membahas kelebihan, kekurangan, akurasi, dan alarm palsu. Review itu juga mencakup alat yang dapat mengunggah kembali konten asli dan rancangan proteksi dengan backup. Karena itu, hubungan pemantauan dan pemulihan bukan gagasan yang pertama kali diajukan di sini. Posisi kajian ini ialah sintesis khusus judi daring Indonesia yang menelusuri unit uji, konsistensi penyebut, dan konsekuensi tindakan lintas objek;

perbedaan dataset tetap menghalangi klaim model terbaik lintas studi.

Dibanding penelitian primer, Rizal dan Widodo (2026), Erawan et al. (2024), dan Arman et al. (2026) memberi bukti implementasi deteksi-karantina; Zagi et al. (2025) memberi observasi reaksi di lapangan; Ajhari et al. (2026) dan Hidayat et al. (2026) memberi evaluasi pengenalan promosi. Kajian ini menghubungkan keluaran yang terpisah tersebut menjadi kebutuhan evaluasi bersama: apakah alarm benar, tindakan aman, layanan pulih, dan kompromi tidak berulang. Kebaruannya bersifat sintesis serta perumusan keluaran evaluasi pada korpus ini. Tidak diklaim sebagai review pertama, cakupan lengkap, atau peningkatan kinerja algoritma.

3.5 Implikasi Deteksi Karantina dan Pemulihan

Kerangka yang diusulkan dimulai dari korelasi sinyal berkas, kode, halaman, konten, serta domain dengan identitas berkas/URL dan waktu kejadian. Alarm kemudian diverifikasi sebelum tindakan sesuai risiko. Halaman yang mengutip perjudian untuk pelaporan atau pendidikan dan perubahan sah akibat pembaruan merupakan contoh negatif yang perlu dimasukkan ke evaluasi. Ambang keputusan perlu dinilai menggunakan presisi, recall, dan jumlah alarm per satuan waktu pada komposisi data yang mendekati layanan sasaran. Rekomendasi ini merupakan hasil sintesis, belum diuji sebagai sistem baru.

Karantina harus dinilai terhadap integritas sekaligus ketersediaan. Memindahkan berkas aplikasi yang sah dapat merusak dependensi, sementara webshell yang terlewat dapat mempertahankan akses. Rancangan uji perlu membedakan isolasi otomatis artefak berisiko tinggi dari alarm yang memerlukan pemeriksaan. Catatan tindakan sebaiknya menyimpan hash, lokasi, waktu, alasan keputusan, dan salinan bukti sebelum pemindahan. Uji salah karantina, kegagalan tindakan, serta pembatalan tindakan diperlukan agar pemulihan kesalahan detektor tidak menimbulkan kerusakan tambahan.

Pemulihan dari salinan tepercaya memerlukan baseline yang disimpan terpisah dan diketahui asal serta waktunya. Salinan yang sudah mengandung injeksi tidak menjadi rujukan integritas yang sah. Setelah isolasi, penyebab kompromi, kredensial, dan artefak lain perlu diperiksa; berkas/konfigurasi dipulihkan dari baseline yang tervalidasi. Pengujian kemudian memeriksa kesesuaian hash atau manifest, fungsi aplikasi, tampilan dan tautan, serta kemunculan ulang. Tidak munculnya kata judi pada satu perayapan belum cukup untuk menyatakan layanan pulih.

Kontrol akses merupakan pelengkap. Fitriyansyah dan Hazri (2020) menjelaskan kata sandi dan OTP terbatas waktu melalui SMS, tanpa membuktikan pencegahan eksploitasi server atau ketahanan phishing. Evaluasi terpadu pada server terkontrol sebaiknya mencatat presisi/recall per objek, positif palsu pada berkas sah, latensi median dan persentil ke-95 tiap tahap, CPU/memori, gangguan layanan akibat karantina, keberhasilan integritas dan fungsi setelah pemulihan, waktu pemulihan, serta kejadian ulang. Aturan sederhana, model tunggal, dan fusi perlu dibandingkan pada data/perangkat yang sama. Ukuran tersebut menguji manfaat respons, bukan hanya kualitas pengenalan konten.

3.6 Keterbatasan Kajian

Korpus lokal berisiko bias pemilihan, bahasa, dan ketersediaan; satu penelusuran pembandingan terbatas tidak memperbaiki cakupan menjadi komprehensif. Versi preprint digunakan untuk Zagi et al. (2025), sedangkan teks in press Ajhari et al. (2026) dipadankan dengan metadata terbit akhir. Kajian tidak menguji ulang kode/data atau melaporkan reliabilitas antarpenilai. Audit hanya memeriksa pelaporan dan aritmetika yang tersedia. Transfer dari media sosial/seluler ke situs institusi dan kerangka pemulihan merupakan hipotesis yang masih membutuhkan validasi.

4. Kesimpulan

Deteksi defacement, webshell, promosi judi, dan domain judi memiliki unit serta tujuan berbeda. Pemetaan bukti menjawab perlunya observasi lintas lapisan, sedangkan pemeriksaan data dan metrik menunjukkan bahwa skor harus dibaca bersama penyebut serta skema uji. Integrasi deteksi-karantina sudah diperlihatkan pada prototipe, tetapi keberhasilan tindakan belum menetapkan pemulihan layanan yang aman. Kontribusi kajian ialah sintesis bukti dan kerangka evaluasi yang menghubungkan positif palsu, dampak karantina, verifikasi integritas, salinan tepercaya, serta kejadian ulang. Simpulan berlaku pada korpus yang ditelaah; penelitian berikutnya perlu menguji kerangka tersebut dengan data sah, serangan berlabel, pembandingan, dan ukuran operasional yang konsisten.

Daftar Pustaka

- Adli Pratama, M. K., Daffa Sampe, M. G., Ariando Ferdian, M., Zahrary, P. T., Rifa'i, A., Septiarini, A., ... Irsyad, A. (2026).** Semantic-preserving hybrid tokenization with CodeBERT for robust webshell detection in hypertext preprocessor source code. *Jurnal Teknik Informatika (JUTIF)*, 7(4), 4018–4034.
<https://doi.org/10.52436/1.jutif.2026.7.4.6121>
- Ajhari, A. A., Aji, R. F., Mantau, A. J., Jatmiko, W., & Pratama, M. (2026).** A cross-modal attention for detecting hidden online gambling promotion in multilingual multimodal watermarked advertising images. *Journal of King Saud University Computer and Information Sciences*, 38(5), 313.
<https://doi.org/10.1007/s44443-026-00725-3>
- Albalawi, M. M., Aloufi, R. B., Alamrani, N. A., Albalawi, N. N., Aljaedi, A. O., & Alharbi, A. R. (2022).** Website defacement detection and monitoring methods: A review. *Electronics*, 11(21), 3573.
<https://doi.org/10.3390/electronics11213573>

- Arman, F., Wahyu Azinar, A., Senja Fitrani, A., & Eviyanti, A. (2026).** Implementasi monitoring dan pencegahan serangan defacement judi online menggunakan Wazuh. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 10(1), 1309–1317. <https://doi.org/10.36040/jati.v10i1.16988>
- Cahyo, A. N., Hermawan, R., Wijaya, M. A. D., & Sari, A. P. (2025).** Deteksi teks promosi judi online pada kolom komentar YouTube dengan metode regex dan fuzzy matching. *Jurnal RESTIKOM: Riset Teknik Informatika dan Komputer*, 7(2), 176–187.
- Erawan, E., Satria, R. P., Nastiti, A. D., Juniardi, W., Anbiya, D. R., & Go Reinnamah, D. A. (2024).** A lightweight design approach to detect malicious injections in government websites: Combating hidden online gambling pages. In *2024 Beyond Technology Summit on Informatics International Conference (BTS-I2C)* (pp. 365–369). IEEE. <https://doi.org/10.1109/BTS-I2C63534.2024.10942063>
- Fitriyansyah, A. Y., & Hazri, M. (2020).** Analisis security web login mahasiswa menggunakan algoritma two-factor time-based one time password. *Sainstech: Jurnal Penelitian dan Pengkajian Sains dan Teknologi*, 30(1). <https://doi.org/10.37277/stch.v30i1.725>
- Gumilang, P. M. R., & Chandra, D. W. (2021).** Implementasi dan modifikasi WebShell untuk monitoring serangan berbasis website. *AITI: Jurnal Teknologi Informasi*, 18(1), 54–68. <https://doi.org/10.24246/aiti.v18i1.54-68>
- Hidayat, D. B., Chamid, A. A., & Jazuli, A. (2026).** Implementasi model hybrid IndoBERT-LinearSVC untuk deteksi spam judol obfuscated pada komentar YouTube. *Progresif: Jurnal Ilmiah Komputer*, 22(3), 820–833. <https://doi.org/10.35889/progresif.v22i3.3914>
- Hikmatyar, M., Sudiarjo, A., Ruuhwan, Ismu Arief, M., & Fadilah, N. (2024).** Pengembangan aplikasi scanning defacement judi online untuk website profile pada server. *Informatics and Digital Expert (INDEX)*, 6(2), 171–175. <https://doi.org/10.36423/index.v6i2.2023023>
- Hong, G., Yang, Z., Yang, S., Liao, X., Du, X., Yang, M., & Duan, H. (2022).** Analyzing ground-truth data of mobile gambling scams. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 2176–2193). IEEE. <https://doi.org/10.1109/SP46214.2022.9833665>
- Kusuma, I. M. (2025).** Analisis bibliometrik dengan visualisasi VOSviewer tentang pengetahuan kosmetik herbal antijerawat pada remaja. *Sainstech: Jurnal Penelitian dan Pengkajian Sains dan Teknologi*, 35(3), 1–7. <https://doi.org/10.37277/stch.v35i3.2384>
- Liem, J. A., Djatmiko Utomo, D. T., Ignasio, B., & Cenggoro, T. W. (2025).** Deep learning and machine learning for Indonesian online gambling website promotion detection. *Procedia Computer Science*, 269, 979–992. <https://doi.org/10.1016/j.procs.2025.09.040>
- Min, M., Lee, J. J., & Lee, K. (2022).** Detecting illegal online gambling (IOG) services in the mobile environment. *Security and Communication Networks*, 2022, 3286623. <https://doi.org/10.1155/2022/3286623>
- Nurseno, M., Aditiawarman, U., Al Qodri Maarif, H., & Mantoro, T. (2024).** Detecting hidden illegal online gambling on .go.id domains using web scraping algorithms. *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, 23(2), 365–378. <https://doi.org/10.30812/matrik.v23i2.3824>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... Moher, D. (2021).** The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Puji Saputra, I. (2025).** Mekanisme deteksi dan pemblokiran konten perjudian daring berbasis kata kunci menggunakan algoritma Levenshtein distance. *Jurnal Komputer Terapan*, 11(2), 60–66.

Reza Pahlevi, M. R., Umam, C., & Handoko, L. B. (2025). Deteksi dan pencegahan web defacing judi online dengan Wazuh SIEM dan Snort IDS berbasis signature. *Jurnal Algoritma*, 22(1), 197–208. <https://doi.org/10.33364/algoritma/v.22-1.2220>

Rizal, N. K., & Widodo, W. (2026). Otomatisasi deteksi dan mitigasi webshell PHP menggunakan algoritma Random Forest. *Bulletin of Computer Science Research*, 6(5), 1978–1987. <https://doi.org/10.47065/bulletincsr.v6i5.1290>

Saepul, M. R., & Rifa'i, M. (2025). Analisis kasus judi online di Asia Tenggara. *Jurnal Ilmiah Wahana Pendidikan*, 11(12.A), 349–359. Retrieved from <https://jurnal.peneliti.net/index.php/JIWP/article/view/12023>

Samuel, & Prasetya Kristiadi, D. (2025). Deteksi teks promosi judi online menggunakan AI dengan kombinasi NLP dan deep learning. *Jurnal Sistem Informasi dan Teknologi (SINTEK)*, 5(2), 179–185. <https://doi.org/10.56995/sintek.v5i2.179>

Simanjuntak, N., & Muhammad, A. H. (2025). Analisis perbandingan algoritma SVM dan CNN dalam mendeteksi website judi online berdasarkan konten teks. *Bulletin of Computer Science Research*, 5(4), 361–371. <https://doi.org/10.47065/bulletincsr.v5i4.586>

Sun, G., Ye, F., Chai, T., Zhang, Z., Tong, X., & Prasad, S. (2023). Gambling domain name recognition via certificate and textual analysis. *The Computer Journal*, 66(8), 1829–1839. <https://doi.org/10.1093/comjnl/bxac043>

Syahadat, R. M., Anashir, M. I., & Zulfa, N. (2026). Tinjauan literatur bahaya ergonomi di restoran, café, dan kantin dari perspektif pengunjung sebagai konsumen. *Sainstech: Jurnal Penelitian dan Pengkajian Sains dan Teknologi*, 36(3), 47–57. <https://doi.org/10.37277/stch.v36i3.2541>

Waliulu, R. F., & Jumame, S. T. (2020). Desain dan implementasi deteksi WebShell malicious web shell (backdoor trap). *Jurnal Sistem Informasi Bisnis*, 10(2), 188–194. <https://doi.org/10.21456/vol10iss2pp188-194>

Zagi, L. M., Digdo, G. P., & Shalannanda, W. (2025). Just dork and crawl: Measuring illegal online gambling defacement in Indonesian websites (arXiv:2508.19368v1). *arXiv*. <https://doi.org/10.48550/arXiv.2508.19368>

Zhang, Z., Han, D., Wu, S., Sun, W., & Shi, S. (2025). Identification and detection of illegal gambling websites and analysis of user behavior. *Computer Science and Information Systems*, 22(3), 859–879. <https://doi.org/10.2298/CSIS240930019Z>