JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume xx, **Number** xx, Month Year

Audit Kerentanan Infrastruktur Siber Dan Korelasinya Terhadap Eskalasi Ketidakpercayaan Publik: Studi Kasus Layanan Digital Pemerintah Indonesia

Muhammad Ulya Farhan[1], Rayyatun Nadia[2*], Muhammad Alzi Naziva[3], Muhammad Al Idrisi[4], Nicoiwan Adha Kobat[5]
[1,2,3,4,5]Universitas Malikussaleh, Indonesia
[1]muhammad.240170155@mhs.unimal.ac.id, [2]rayyatun.240170190@mhs.unimal.ac.id,
[3]muhammad.240170182@mhs.unimal.ac.id, [4]muhammad.240170178@mhs.unimal.ac.id,
[5]nicoiwan.240170207@mhs.unimal.ac.id

ABSTRACT

Digital transformation in Indonesia's public sector faces a dual challenge: technical infrastructure vulnerabilities and a crisis of public trust due to recurring cyber incidents. This study aims to empirically test whether the level of technical vulnerability in government systems correlates linearly with the intensity of public negative sentiment (public distrust). Using a mixed-method approach, this research combines passive security audits (Passive Reconnaissance) based on Open Source Intelligence (OSINT) on 30 government domains (.go.id) and sentiment analysis based on Large Language Models (LLM) on 55,451 social media comments. The results reveal a counterintuitive finding of no significant correlation between technical vulnerability and public distrust (Pearson $r = -0.0023, p > 0.05$*). Data analysis uncovered a "Reputation Paradox," where agencies with critical vulnerability scores exhibited low negative sentiment, whereas agencies with seemingly secure technical profiles faced the highest levels of distrust. This study concludes that public perception of security is driven by service availability and User Experience (UX) rather than technical cybersecurity parameters.*

Keywords: *Cybersecurity, Public Trust, OSINT, Sentiment Analysis, Reputation Paradox.*

PENDAHULUAN

Tahun 2025 menjadi fase krusial bagi kedaulatan digital Indonesia, di mana infrastruktur siber nasional menghadapi paradoks yang mengkhawatirkan. Di satu sisi, transformasi digital digalakkan secara masif pada sektor pelayanan publik melalui *E-Government*; namun di sisi lain, insiden kebocoran data (*data breach*) dan kelumpuhan layanan (*downtime*) terus berulang dengan pola yang identik (Yuwana, Surya, Baihaqy, & Fauzi, 2025). Fenomena ini bukan lagi sekadar isu teknis, melainkan telah bermetamorfosis menjadi krisis kepercayaan publik (*public trust crisis*) yang serius terhadap kompetensi pemerintah dalam menjaga mandat keamanan data warga negara (Direktorat Operasi Keamanan Siber, 2023).

Secara teoritis, keamanan informasi harus memenuhi pilar *Confidentiality*, *Integrity*, dan *Availability* (CIA Triad). Namun, fakta di lapangan sering kali menunjukkan anomali (Kurniawan & Riadi, 2018). Evaluasi keamanan berbasis standar seperti COBIT 5 dan CMMI sangat diperlukan untuk memetakan tingkat kematangan tata kelola TI instansi pemerintah (Umar, Riadi, & Handoyo, 2019). Pemindaian awal menggunakan mesin pencari infrastruktur *Open Source Intelligence* (OSINT) seperti Shodan mengindikasikan bahwa sejumlah besar peladen (*server*) instansi pemerintah masih beroperasi dengan mengekspos *port* berisiko dan memiliki kerentanan (*vulnerabilities*) yang belum ditambal (*unpatched*) (Riadi et al., 2020). Kondisi ini memunculkan pertanyaan mendasar: apakah masyarakat menyadari kerentanan teknis ini, dan sejauh mana hal tersebut memengaruhi kepercayaan mereka?

Ketidakselarasan antara klaim keamanan pemerintah dan realitas di lapangan memicu respons reaktif dari masyarakat. Media sosial menjadi kanal utama bagi publik untuk menumpahkan frustrasi, kritik, dan ketidakpercayaan mereka. Data opini publik ini, jika dianalisis dengan tepat, dapat menjadi indikator valid untuk mengukur dampak sosiologis dari kegagalan teknis sebuah sistem.

Oleh karena itu, penelitian ini hadir untuk mengaudit korelasi antara dua variabel yang jarang disandingkan secara kuantitatif: kerentanan teknis infrastruktur (variabel teknis) dan sentimen negatif publik (variabel sosial). Dengan menggabungkan metode audit pasif teknis dan analisis sentimen berbasis *Large Language Models* (LLM), penelitian ini bertujuan untuk menguji secara empiris apakah tingkat kerentanan sistem siber berkorelasi lurus dengan degradasi kepercayaan publik terhadap negara (Umar, Riadi, & Elfatiha, 2023).

KAJIAN LITERATUR

Keamanan Informasi dan CIA Triad

Keamanan informasi pada sektor pemerintahan merupakan elemen fundamental dalam menjaga kedaulatan data negara. Standar keamanan siber secara universal merujuk pada pemenuhan tiga pilar utama yang dikenal sebagai *CIA*

Triad. Pilar tersebut meliputi *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan). Penelitian ini menggunakan kerangka kerja *CIA Triad* sebagai landasan untuk menentukan parameter audit teknis, di mana temuan kerentanan (*vulnerability*) dikategorikan berdasarkan potensi dampaknya terhadap ketiga aspek tersebut.

Audit Keamanan Pasif (*Passive Reconnaissance*)

Dalam etika keamanan siber (Riadi, Fadlil, & Mumin, 2023), terdapat perbedaan tegas antara uji penetrasi aktif dan audit pasif. Penelitian ini menerapkan metode *Passive Reconnaissance*, yaitu teknik pengumpulan data intelijen tanpa berinteraksi langsung atau mengirimkan paket berbahaya ke sistem target. Instrumen utama yang digunakan adalah mesin pencari infrastruktur berbasis *Open Source Intelligence* (OSINT) seperti Shodan. Shodan efektif mendeteksi *Common Vulnerabilities and Exposures* (CVE) pada infrastruktur publik melalui analisis *banner grabbing*. Keamanan siber tidak hanya soal teknologi, tetapi juga tata kelola. Badan Siber dan Sandi Negara (2024) menegaskan pentingnya manajemen kerentanan sebagai bagian dari ketahanan siber nasional. Untuk mendeteksi celah keamanan, metode *Vulnerability Assessment* menjadi instrumen vital. Elfatiha (2024) juga menyatakan bahwa sistem perlu dievaluasi kerentanannya secara berkala.

Analisis Sentimen Hibrida (*Hybrid Knowledge Distillation*)

Analisis sentimen tradisional sering kali menghadapi dilema *trade-off* antara akurasi dan biaya komputasi. Penelitian ini mengusulkan pendekatan modern berupa *Hybrid Knowledge Distillation* . Dalam skema ini, *Large Language Model* (LLM) bertindak sebagai "Guru" (*Teacher Model*) yang melabeli sampel data secara otomatis. Label berkualitas tinggi yang dihasilkan LLM kemudian digunakan untuk melatih model SVM ("Murid" atau *Student Model*) untuk efisiensi komputasi pada data skala besar. Analisis sentimen modern memanfaatkan algoritma pembelajaran mesin untuk klasifikasi otomatis. Pendekatan yang dipadukan dengan *Support Vector Machine* (SVM) dapat mencapai akurasi tinggi dalam klasifikasi sentimen, sebagaimana diterapkan pada analisis opini terhadap tokoh publik (Ratnaswari, Wibowo, & Kartika, 2025). Metode ini relevan untuk diterapkan dalam mengukur tingkat kepercayaan publik terhadap layanan digital pemerintah.

Teori Kepercayaan Publik

Kepercayaan publik (*Public Trust*) adalah elemen kunci dalam *E-Government*. Teori *Cyber-Physical Systems Sociology* mempostulatkan bahwa insiden teknis pada infrastruktur digital tidak lagi dipandang sebagai gangguan teknis semata, melainkan sebagai indikator inkompetensi tata kelola (Prayugah et al., 2024).

METODE PENELITIAN

Penelitian ini menerapkan pendekatan kuantitatif dengan desain korelasional. Objek penelitian terdiri dari 30 domain instansi pemerintah Indonesia (.go.id) yang dipilih berdasarkan kriteria vitalitas layanan.

Teknik Pengumpulan Data

Data kerentanan teknis dikumpulkan menggunakan metode *Passive Reconnaissance* berbasis OSINT menggunakan API Shodan dan CriminalIP. Parameter yang diekstraksi meliputi alamat IP, *open ports*, dan CVE untuk menghasilkan Skor Risiko (*Risk Score*) dengan skala 0-100. Data opini publik diekstraksi dari YouTube menggunakan algoritma *Hybrid Harvesting* (API dan Scraping). Total sampel yang berhasil diakuisisi sebanyak 55.451 data komentar teks pada periode Desember 2025.

Teknik Pengolahan Data

Penelitian ini menerapkan metode *Hybrid Knowledge Distillation*. Sebagian kecil data sampel dilabeli oleh LLM (*Teacher Model*) menggunakan mekanisme *Dynamic Routing* (Groq/Gemini). Data terlabeli kemudian digunakan untuk melatih *Support Vector Machine* (SVM) sebagai *Student Model* untuk mengklasifikasikan sisa data secara massal.

Teknik Analisis Data

Analisis data meliputi: (1) Statistik Deskriptif untuk memetakan profil risiko; (2) Uji Asumsi Klasik (Normalitas Shapiro-Wilk); (3) Uji Hipotesis Korelasi Pearson untuk mengukur hubungan variabel; dan (4) Visualisasi Data menggunakan *Scatter Plot* dan *Word Cloud*.

HASIL DAN PEMBAHASAN

Statistik Deskriptif Keamanan Siber

Data hasil audit terhadap 30 domain instansi pemerintah dan analisis sentimen terhadap 55.451 komentar publik menunjukkan profil risiko yang beragam. Rangkuman statistik disajikan pada Tabel 1.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume xx, **Number** xx, Month Year

Table 1. Statistik Deskriptif Skor Risiko Teknis dan Sentimen Negatif

Parameter	Skor Risiko Teknis (0-100)	Skor Distrust Publik (%)
Rata-rata (Mean)	22.50	13.29%
Standar Deviasi	15.03	11.96%
Nilai Minimum	0 (Aman)	0% (Percaya)
Nilai Maksimum	100 (Rentan)	60% (Tidak Percaya)

Distribusi data divisualisasikan pada Fig. 1. Terlihat mayoritas instansi memiliki skor risiko teknis seragam (sekitar 20), kemungkinan akibat penggunaan WAF, namun sentimen publik menyebar variatif.

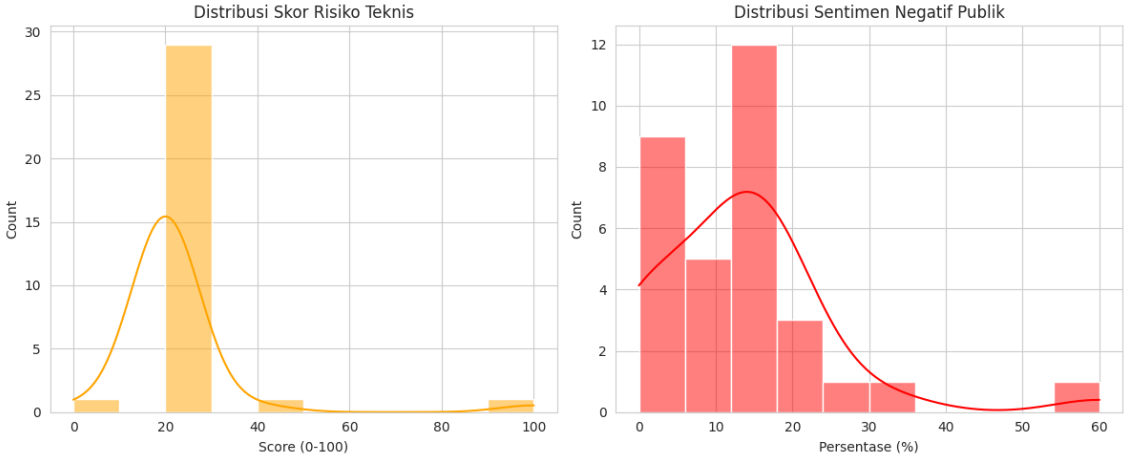

Fig. 1 Distribusi Skor Risiko Teknis (Kiri) dan Sentimen Negatif Publik (Kanan)

Analisis Korelasi dan Paradoks Reputasi

Berdasarkan uji korelasi Pearson, diperoleh nilai r = -0.0023 dengan p-value = 0.9898 . Hasil ini menunjukkan tidak terdapat korelasi signifikan antara kerentanan teknis dengan ketidakpercayaan publik. Fenomena ini digambarkan dalam peta korelasi (Fig. 2).

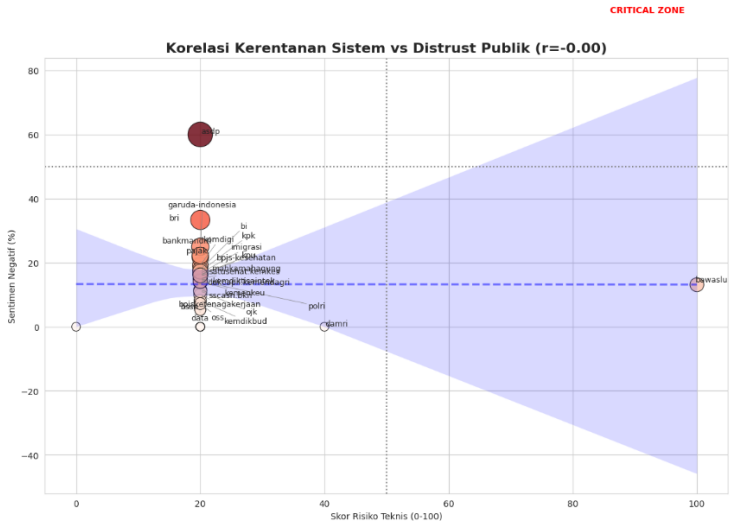

Fig. 2 Peta Korelasi Kerentanan Sistem vs Distrust Publik

Gambar di atas menunjukkan anomali "Paradoks Reputasi". Instansi seperti Bawaslu berada di kuadran kanan bawah (Risiko Tinggi, Distrust Rendah), sedangkan instansi perbankan dan transportasi (ASDP) berada di kiri atas (Risiko Rendah, Distrust Tinggi).

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume xx, **Number** xx, Month Year

Peringkat Instansi dan Analisis Isu

Untuk mendalami penyebab tingginya distrust, dilakukan pemeringkatan instansi (Fig. 3) dan analisis semantik Word Cloud (Fig. 4).

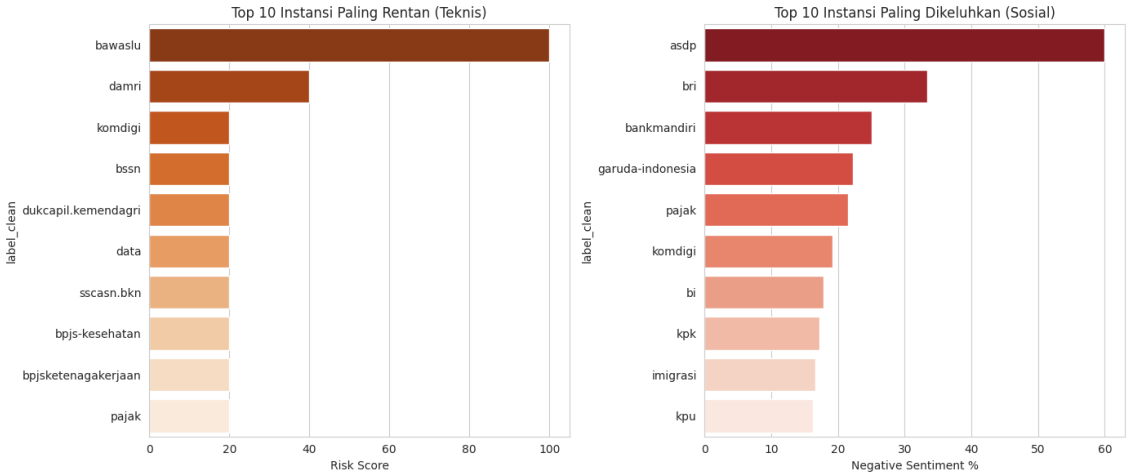

Fig. 3 Perbandingan Top 10 Instansi Paling Rentan (Kiri) vs Paling Dikeluhkan (Kanan)

Fig. 4 Word Cloud: Isu Utama Keluhan Masyarakat.

Kata kunci dominan "Gak bisa", "Ribet", "Error", dan "Lemot" mengonfirmasi bahwa pemicu utama kemarahan publik adalah masalah ketersediaan layanan (*Availability*) dan pengalaman pengguna (UX), bukan keamanan teknis.

Validasi Triangulasi Data (Survei Pengguna)

Untuk memvalidasi temuan analisis sentimen berbasis *Big Data* (AI), penelitian ini melakukan triangulasi data melalui survei kuesioner terhadap 17 responden yang merupakan pengguna aktif layanan digital pemerintah. Langkah ini bertujuan untuk mengonfirmasi apakah sentimen yang terdeteksi di media sosial selaras dengan pengalaman nyata pengguna.

Hasil survei menunjukkan dua temuan kunci yang memperkuat analisis sebelumnya:

1. **Konfirmasi Krisis Kepercayaan:** Rata-rata skor kepercayaan responden terhadap keamanan data pemerintah berada pada angka **2.94 dari skala 5.00**. Skor di bawah ambang batas netral (3.00) ini mengindikasikan bahwa responden cenderung ragu dan tidak percaya, yang memvalidasi temuan tingginya *Distrust Score* pada analisis sentimen media sosial.
2. **Konsistensi Objek Keluhan:** Sebagaimana divisualisasikan pada **Fig. 5**, responden menempatkan **BPJS**

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume xx, **Number** xx, Month Year

Kesehatan (Mobile JKN) dan **Kominfo/PDN** sebagai layanan yang paling sering bermasalah.

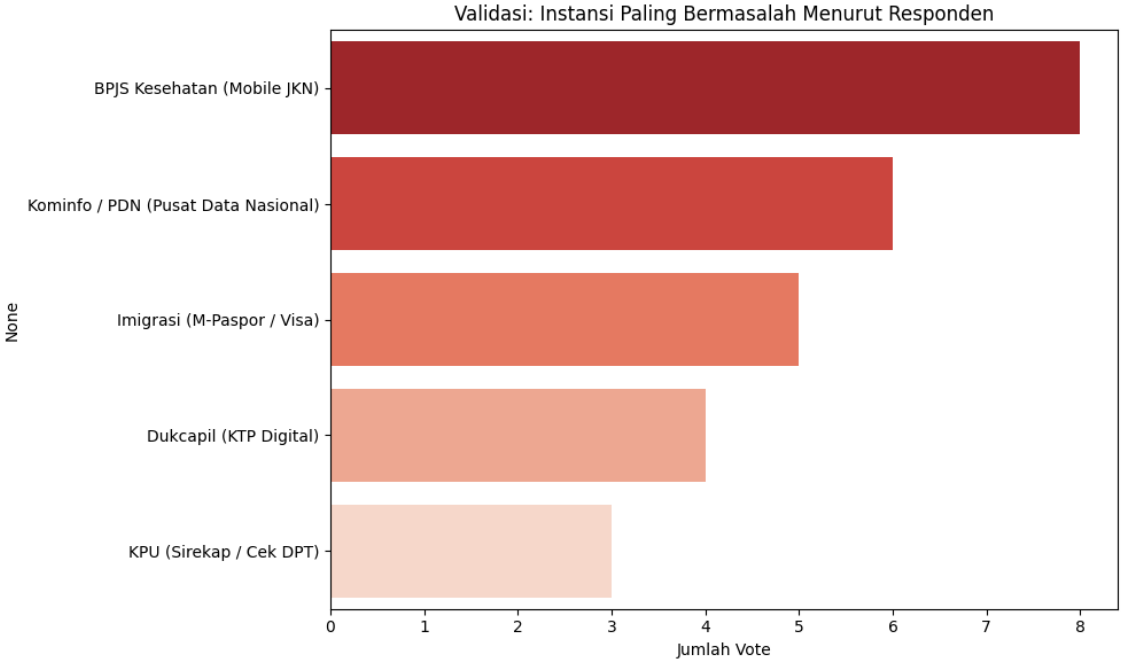

Fig. 5 Peringkat Instansi Paling Bermasalah Berdasarkan Survei Responden.

Temuan survei ini memiliki keselarasan (*alignment*) dengan hasil analisis sentimen AI pada sub-bab sebelumnya, di mana BPJS Kesehatan dan sektor vital (PDN) juga menjadi topik dominan dalam percakapan negatif. Konsistensi antara data persepsi manusia (survei) dan data perilaku digital (medsos) ini memperkuat validitas internal penelitian, membuktikan bahwa "Paradoks Reputasi" yang ditemukan bukan sekadar anomali statistik, melainkan refleksi akurat dari keresahan masyarakat.

KESIMPULAN

Berdasarkan hasil analisis komprehensif yang menggabungkan audit teknis OSINT, analisis sentimen berbasis AI, dan validasi survei pengguna, penelitian ini menyimpulkan empat poin utama:

1. **Profil Risiko Teknis:** Mayoritas infrastruktur siber pemerintah (87%) terdeteksi memiliki skor risiko teknis kategori rendah (Skor rata-rata: 22.50) berdasarkan pemindaian pasif. Kondisi ini mengindikasikan adanya upaya pengamanan perimeter (seperti penggunaan *Firewall*), meskipun masih ditemukan anomali kritis pada beberapa instansi tertentu yang memiliki skor kerentanan maksimal.
2. **Absennya Korelasi Linear:** Uji statistik membuktikan bahwa tidak terdapat korelasi signifikan antara tingkat kerentanan teknis sistem dengan intensitas sentimen negatif publik (Pearson $r = -0.0023, p > 0.05$). Hipotesis awal bahwa "semakin rentan sistem, semakin marah masyarakat" dinyatakan **ditolak**.
3. **Paradoks Reputasi:** Penelitian ini menemukan fenomena "Paradoks Reputasi", di mana persepsi ketidakpercayaan publik (*public distrust*) tidak dipengaruhi oleh parameter keamanan teknis (*Confidentiality/Integrity*), melainkan didominasi oleh faktor ketersediaan layanan (*Availability*) dan pengalaman pengguna (*User Experience*). Masyarakat cenderung memberikan sentimen negatif ekstrem pada layanan yang sering mengalami gangguan operasional, terlepas dari apakah sistem tersebut aman dari peretasan atau tidak.
4. **Validasi Triangulasi Data:** Hasil survei terhadap pengguna layanan mengonfirmasi temuan analisis *Big Data*, di mana tingkat kepercayaan publik berada pada angka 2.94 (skala 5.00) yang masuk dalam kategori "Kurang Percaya". Konsistensi antara keluhan di media sosial dan hasil kuesioner menunjukkan bahwa krisis kepercayaan ini bersifat nyata dan persisten, bukan sekadar riuh sesaat di dunia maya.

REFERENSI

Badan Siber dan Sandi Negara. (2024). *Kajian ketahanan siber: Manajemen kerentanan*. Politeknik Siber dan Sandi Negara.

Direktorat Operasi Keamanan Siber. (2023). *Lanskap Keamanan Siber Indonesia 2023*. Badan Siber dan Sandi Negara.

E-ISSN: 3090-739X
Volume xx, **Number** xx, Month Year

Elfatiha, M. I. A. (2024). Analisis keamanan dan penilaian kerentanan sistem informasi akademik berbasis web menggunakan framework OWASP dan ISSAF. Tesis, Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta.

Kurniawan, E., & Riadi, I. (2018). Analisis tingkat keamanan sistem informasi akademik berdasarkan standar ISO/IEC 27002:2013 menggunakan SSE-CMM. *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi, 2*(1), 1–12. **https://doi.org/10.29407/intensif.v2i1.11830**

Prayugah, M. I., Indahyanti, U., & Ariyanti, N. (2024). Analisis sentimen publik pada pemerintah dalam serangan ransomware dengan pendekatan SMOTE. *Journal of Information Systems and Informatics Engineering, 8*(2), 333–343. **https://doi.org/10.35145/joisie.v8i2.4764**

Ratnaswari, S., Wibowo, N. C., & Kartika, D. S. Y. (2025). Analisis sentimen menggunakan metode Lexicon-Based dan Support Vector Machine pada presiden dan wakil presiden Indonesia periode 2024–2029. *Jurnal Informatika dan Teknik Elektro Terapan, 13*(1), 362–368. **https://doi.org/10.23960/jitet.v13i1.5604**

Riadi, I., Fadlil, A., & Mumin, M. A. (2023). OWASP framework-based network forensics to analyze the SQLi attacks on web servers. *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, 22*(3), 481–494. **https://doi.org/10.30812/matrik.v22i3.3018**

Riadi, I., Yudhana, A., & Yunanri, W. (2020). Analisis keamanan website Open Journal System menggunakan metode vulnerability assessment. *Jurnal Teknologi Informasi dan Ilmu Komputer, 7*(4), 853–860. **https://doi.org/10.25126/jtiik.2020701928**

Umar, R., Riadi, I., & Elfatiha, M. I. A. (2023). Analisis keamanan sistem informasi akademik berbasis web menggunakan framework ISSAF. *JUTISI: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, 12*(1), 280–292. **https://doi.org/10.35889/jutisi.v12i1.1191**

Umar, R., Riadi, I., & Handoyo, E. (2019). Analysis security of SIA based DSS05 on COBIT 5 using Capability Maturity Model Integration (CMMI). *Scientific Journal of Informatics, 6*(2), 240–258.

Yuwana, M. A. S. A., Surya, A. P. A., Baihaqy, A. H. A., & Fauzi, M. A. N. (2025). Analisa dampak kebocoran data Pusat Data Nasional (PDN) 2024 dalam perspektif HAM. *Jurnal Hukum dan HAM Wicarana, 4*(1), 31–37.