JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i1.8186

SISTEM KLASIFIKASI URL UNTUK DETEKSI SITUS BERBAHAYA BERBASIS ANALISIS FITUR JARINGAN

Yeremia Setya Maharman Gurning [1*], Dedy Kiswanto[2], Leni Karmila Daulay[3], Aurela Khoiri Nasution[4]

[1,2,3,4]Universitas Negeri Medan; Jalan Willem Iskandar, Pasar V Medan Estate; Telp. (061) 6613365/ fax (061) 6614002

Keywords:
klasifikasi URL, situs berbahaya, fitur jaringan, keamanan siber

Corespondent Email:
yeregurning134@gmail.com

Abstrak. Peningkatan aktivitas cybercrime seperti phishing, malware, dan penipuan daring menyebabkan kebutuhan akan sistem deteksi situs berbahaya yang efektif semakin mendesak. Penelitian ini mengembangkan Sistem Klasifikasi URL untuk Deteksi Situs Berbahaya Berbasis Analisis Fitur Jaringan yang bertujuan untuk mengidentifikasi dan mengklasifikasikan situs menjadi tiga kategori, yaitu normal, suspicious, dan malicious. Sistem dirancang menggunakan bahasa pemrograman PHP dengan integrasi API URLHaus sebagai sumber referensi data situs berbahaya. Proses analisis dilakukan dengan memeriksa sejumlah fitur jaringan, meliputi panjang URL, jumlah subdomain, penggunaan protokol HTTPS, karakter spesial, port non-standar, serta kata kunci mencurigakan. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi situs berbahaya secara real-time dengan waktu respon rata-rata kurang dari tiga detik per URL. Selain itu, sistem menampilkan hasil analisis dalam bentuk visual seperti progress bar tingkat risiko dan keterangan fitur yang memengaruhi hasil klasifikasi. Berdasarkan evaluasi, sistem dapat mengklasifikasikan URL dengan akurat dan efisien tanpa perlu mengakses konten situs secara langsung, sehingga aman untuk digunakan. Sistem ini diharapkan dapat menjadi solusi praktis dalam meningkatkan kesadaran pengguna terhadap ancaman siber serta dasar pengembangan lanjutan berbasis machine learning untuk peningkatan akurasi di masa depan.

Abstract. *The increase in cybercrime activities such as phishing, malware, and online fraud has created an urgent need for an effective malicious site detection system. This study developed a URL Classification System for Malicious Website Detection Based on Network Feature Analysis, aiming to identify and classify websites into three categories: normal, suspicious, and malicious. The system was developed using the PHP programming language integrated with the URLHaus API as a reference for malicious site data. The analysis process examines several network features, including URL length, number of subdomains, HTTPS usage, special characters, non-standard ports, and suspicious keywords. The test results show that the system can detect malicious URLs in real time with an average response time of less than three seconds per URL. Moreover, the system presents its results visually through a risk-level progress bar and detailed explanations of influencing features. Based on evaluation, the system accurately and efficiently classifies URLs without accessing website content directly, ensuring safer detection. This system is expected to serve as a practical tool for improving user awareness of cybersecurity threats and as a foundation for further development using machine learning to enhance detection accuracy in the future.*

1. PENDAHULUAN

Perkembangan teknologi informasi di Indonesia telah mendorong pemanfaatan

internet secara masif di berbagai sektor seperti pendidikan, industri, dan pemerintahan [1]. Seiring dengan peningkatan aktivitas daring, ancaman keamanan siber juga meningkat, terutama dalam bentuk situs berbahaya (malicious websites) yang digunakan untuk penyebaran malware, phishing, dan pencurian data [2]. Serangan ini umumnya memanfaatkan Uniform Resource Locator (URL) sebagai media utama untuk mengarahkan korban ke halaman berbahaya tanpa disadari [3].

Metode konvensional seperti penggunaan daftar hitam (blacklist) memiliki keterbatasan karena hanya dapat mendeteksi situs yang telah diketahui sebelumnya [4]. Oleh karena itu, diperlukan sistem yang mampu menganalisis dan mengklasifikasikan URL berdasarkan fitur-fitur jaringan secara otomatis dan adaptif [5].

Beberapa penelitian terdahulu di Indonesia telah membahas berbagai aspek keamanan jaringan. Putra dan Fauzi [1] melakukan analisis keamanan pada sistem berbasis web dan menyoroti pentingnya proteksi terhadap lalu lintas jaringan. Siregar dan Lubis [2] mengusulkan pendekatan deteksi phishing berbasis URL menggunakan metode lokal yang disesuaikan dengan karakteristik data nasional. Agustani et al. [3] dalam JITET meneliti perilaku akses internet menggunakan machine learning, menunjukkan bahwa fitur teknis jaringan dapat digunakan untuk mendeteksi pola perilaku pengguna yang tidak wajar.

Kiswanto et al. [4] pada Bulletin of Information Technology mengembangkan sistem deteksi serangan DDoS berbasis Random Forest dan berhasil mencapai akurasi tinggi dalam identifikasi trafik anomali. Purwanto dan Santoso [5] menganalisis pola URL sebagai ciri pembeda situs phishing dengan hasil bahwa panjang domain, jumlah subdomain, dan karakter khusus berperan penting dalam deteksi.

Arifin dan Wulandari [6] meneliti pemanfaatan API publik untuk mendeteksi situs berbahaya tanpa perlu memproses isi halaman web, sedangkan Hutapea dan Simanjuntak [7] menunjukkan bahwa API VirusTotal efektif dalam validasi keamanan situs. Wijaya dan Rohman [8] mengembangkan sistem keamanan web berbasis analisis fitur jaringan, sementara Nasrullah dan Siregar [9] menerapkan metode analisis fitur untuk klasifikasi phishing site dengan hasil akurasi yang konsisten.

Selanjutnya, Maulana dan Pratama [10] melakukan evaluasi integrasi API keamanan untuk meningkatkan kecepatan deteksi URL berbahaya. Berdasarkan penelitian-penelitian tersebut, dapat disimpulkan bahwa fitur jaringan seperti panjang URL, jumlah subdomain, dan protokol HTTPS dapat menjadi indikator penting dalam mendeteksi situs berbahaya. Penelitian ini mengembangkan sistem klasifikasi URL yang memanfaatkan fitur jaringan dan API eksternal untuk mendeteksi situs berbahaya secara cepat, efisien, dan aman tanpa perlu menggunakan algoritma pembelajaran mesin yang kompleks.

2. TINJAUAN PUSTAKA

Beberapa penelitian di Indonesia turut memperkuat pendekatan analisis fitur jaringan dalam konteks keamanan siber. Lestari dan Syahputra [11] menyoroti pentingnya penerapan sistem keamanan siber pada layanan publik digital di Indonesia, mengingat semakin banyaknya serangan phishing yang menargetkan data pemerintah dan masyarakat. Cahyani [12] mengembangkan metode scoring sederhana untuk menilai tingkat risiko URL berbahaya, dan hasilnya menunjukkan peningkatan kecepatan deteksi tanpa mengurangi akurasi.

Situmorang dan Anggara [13] merancang sistem pemantauan URL berbahaya berbasis API eksternal, yang memungkinkan pengguna untuk melakukan monitoring ancaman secara real-time. Ramadhan [14] meneliti perancangan sistem keamanan web menggunakan kombinasi analisis domain dan jaringan sebagai langkah mitigasi terhadap serangan siber. Sementara itu, Hakim dan Sukma [15] memanfaatkan data dari platform URLHaus untuk mendeteksi situs berbahaya dengan tingkat keberhasilan yang tinggi dan relevansi yang baik terhadap konteks lokal Indonesia.

Dari berbagai penelitian tersebut dapat disimpulkan bahwa pendekatan analisis fitur jaringan dan integrasi API eksternal merupakan metode yang efektif untuk mendeteksi situs berbahaya tanpa perlu memproses konten situs secara langsung. Penelitian ini menggabungkan hasil-hasil sebelumnya dengan rancangan sistem yang sederhana, efisien, dan dapat diimplementasikan secara langsung pada lingkungan pengguna umum.

3. METODE PENELITIAN

Penelitian ini merupakan penelitian terapan dengan pendekatan kuantitatif yang berfokus pada perancangan dan implementasi sistem klasifikasi URL untuk mendeteksi situs berbahaya berbasis analisis fitur jaringan. Sistem ini tidak menggunakan algoritma pembelajaran mesin, tetapi menganalisis karakteristik teknis dari URL dengan dukungan API eksternal seperti URLHaus dan VirusTotal sebagai sumber referensi keamanan. Pendekatan ini dipilih karena mampu mendeteksi situs berbahaya secara real-time tanpa perlu mengakses konten situs secara langsung, sehingga mengurangi risiko paparan malware dan meningkatkan efisiensi sistem.

Tahapan penelitian dilakukan secara sistematis agar pengembangan sistem dapat berjalan terarah dan terukur. Adapun tahapan penelitian meliputi:

3.1. Analisis dan Studi Literatur

Pada tahap ini dilakukan pengumpulan referensi dan kajian terhadap penelitian terdahulu terkait deteksi situs berbahaya dan fitur jaringan yang relevan. Beberapa fitur utama yang dipilih meliputi panjang URL, jumlah subdomain, jumlah karakter spesial, penggunaan protokol HTTPS, port non-standar, dan kata kunci mencurigakan seperti *login*, *verify*, atau *secure*. Fitur-fitur ini dipertimbangkan karena sering muncul pada situs phishing maupun malware.

3.2. Perancangan Sistem

Sistem dirancang berbasis web menggunakan bahasa pemrograman PHP dan dijalankan melalui server lokal XAMPP. Struktur utama sistem terdiri dari modul input URL, modul analisis fitur jaringan, modul integrasi API eksternal, serta modul hasil analisis. Setiap modul berperan dalam memproses data URL hingga menghasilkan klasifikasi keamanan situs. Sistem juga menerapkan penyimpanan sementara menggunakan session tanpa basis data permanen untuk menjaga efisiensi dan privasi pengguna.

3.3. Implementasi dan Integrasi API

Implementasi sistem melibatkan integrasi antara modul analisis internal dan API eksternal. Setelah pengguna memasukkan URL, sistem melakukan ekstraksi fitur jaringan, kemudian mengirimkan permintaan ke API eksternal untuk memperoleh hasil validasi keamanan. Berdasarkan hasil tersebut, sistem mengklasifikasikan URL ke dalam tiga kategori, yaitu *normal*, *suspicious*, dan *malicious*.

3.4. Pengujian dan Evaluasi SIstem

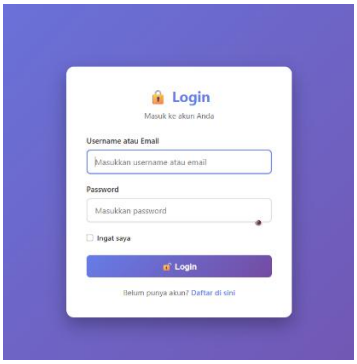
Tahap pengujian dilakukan untuk memastikan fungsionalitas sistem berjalan sesuai rancangan. Pengujian mencakup keberhasilan koneksi API, kecepatan respon analisis, serta ketepatan klasifikasi URL. Evaluasi dilakukan dengan membandingkan hasil deteksi sistem terhadap data rujukan dari API URLHaus. Sistem dinilai berhasil apabila mampu memberikan hasil klasifikasi dengan waktu rata-rata kurang dari tiga detik per URL dan tingkat akurasi yang konsisten.

Analisis data dilakukan secara deskriptif kuantitatif berdasarkan hasil pengujian performa sistem. Parameter yang dianalisis meliputi akurasi klasifikasi, stabilitas tampilan, serta waktu respon dalam proses pendeteksian. Hasil analisis menunjukkan kinerja sistem dalam mengidentifikasi situs berbahaya secara cepat dan efisien.

4. HASIL DAN PEMBAHASAN

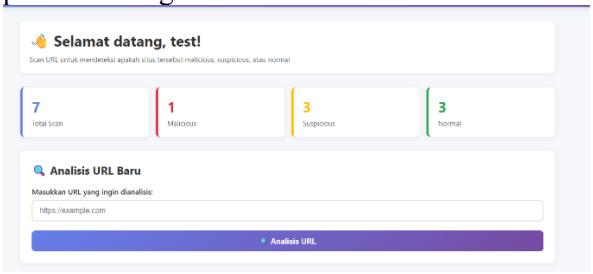
Sistem yang dikembangkan diberi nama Sistem Klasifikasi URL untuk Deteksi Situs Berbahaya Berbasis Analisis Fitur Jaringan. Sistem ini dirancang agar mampu menganalisis berbagai parameter jaringan untuk menentukan apakah suatu URL tergolong malicious, suspicious, atau normal. Implementasi dilakukan menggunakan bahasa pemrograman PHP dengan dukungan API URLHaus sebagai sumber data referensi ancaman, serta basis data MySQL untuk penyimpanan hasil analisis dan akun pengguna.

Sistem ini memiliki antarmuka web yang sederhana dan interaktif agar pengguna mudah melakukan registrasi, login, serta menganalisis URL. Berikut hasil tampilan dari implementasi sistem.



Gambar 1. Halaman Login Pengguna

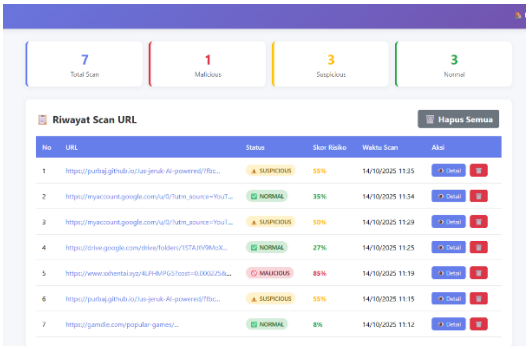
Gambar 1 merupakan tampilan login yang digunakan untuk mengakses sistem. Pengguna dapat masuk menggunakan username atau email yang telah terdaftar sebelumnya. Sistem juga menyediakan opsi "ingat saya" untuk menyimpan sesi login agar pengguna tidak perlu berulang kali masuk.



Gambar 2. Halaman Dashboard Pengguna

Gambar 2 memperlihatkan dashboard utama setelah pengguna berhasil login. Pada halaman ini pengguna dapat melihat ringkasan hasil analisis berupa jumlah total scan, serta pembagian hasil ke dalam tiga kategori: malicious, suspicious, dan normal. Pengguna juga dapat melakukan analisis baru dengan memasukkan URL yang ingin diperiksa ke dalam kolom input.

Hasil analisis URL akan menampilkan skor risiko yang dihitung berdasarkan fitur-fitur jaringan seperti panjang URL, jumlah karakter spesial, jumlah subdomain, keberadaan HTTPS, dan indikator lain yang menunjukkan potensi berbahaya dari situs tersebut.



Gambar 3. Halaman Riwayat Scan URL

Gambar 3 menunjukkan halaman riwayat scan, di mana sistem menyimpan seluruh hasil analisis URL yang pernah dilakukan pengguna. Pada tabel ini terdapat informasi berupa status hasil (malicious, suspicious, normal), skor risiko, waktu scan, serta aksi untuk melihat detail analisis atau menghapus data. Fitur ini memungkinkan pengguna melakukan monitoring riwayat deteksi secara berkelanjutan.

Gambar 4. Halaman Detail Hasil Analisis

Gambar 4 menampilkan halaman detail hasil analisis URL, di mana sistem memberikan penjelasan menyeluruh terhadap fitur-fitur yang terdeteksi pada URL yang dianalisis. Setiap parameter ditampilkan secara visual, meliputi:

- Panjang URL
- Jumlah karakter spesial
- Keberadaan HTTPS
- Jumlah subdomain
- Jumlah digit
- Panjang domain
- Port non-standar
- URL shortener
- Kata kunci mencurigakan

Selain itu, sistem juga menampilkan skor risiko dalam bentuk progres bar serta kesimpulan analisis. Jika nilai risiko rendah, maka URL diklasifikasikan sebagai *normal*;

apabila menengah dikategorikan *suspicious*; dan jika tinggi diklasifikasikan *malicious*.

Pembahasan

Sistem klasifikasi URL untuk deteksi situs berbahaya yang dikembangkan pada penelitian ini dirancang untuk membantu pengguna dalam mengidentifikasi tingkat keamanan suatu alamat web berdasarkan analisis fitur jaringan. Pada sistem ini, proses analisis dilakukan secara otomatis dengan memanfaatkan kombinasi fitur jaringan dan data yang diperoleh melalui integrasi API dari URLHaus, yang berfungsi sebagai basis data situs berbahaya terkini.

Secara keseluruhan, sistem bekerja melalui dua tahapan utama yang menjadi fokus pembahasan, yaitu:

(1) analisis URL

(2) detail hasil analisis URL

Tahapan pertama merupakan proses analisis URL, di mana pengguna memasukkan alamat web yang ingin diperiksa ke dalam kolom input yang telah disediakan pada halaman sistem. Setelah URL dimasukkan, sistem akan melakukan serangkaian proses pemeriksaan otomatis terhadap berbagai fitur jaringan (network features) yang berpotensi menunjukkan karakteristik berbahaya.

Beberapa fitur utama yang dianalisis meliputi:

- Struktur dan Panjang URL
  URL yang memiliki panjang berlebihan atau mengandung terlalu banyak karakter acak cenderung digunakan untuk menyembunyikan domain sebenarnya. Sistem akan menghitung panjang total URL dan membandingkannya dengan ambang batas rata-rata dari situs normal.
- Protokol yang Digunakan
  Penggunaan protokol HTTP tanpa enkripsi dianggap berisiko tinggi, sementara protokol HTTPS menunjukkan tingkat keamanan yang lebih baik. Sistem akan menandai URL tanpa HTTPS sebagai potensi ancaman.
- Jumlah dan Posisi Subdomain
  Situs phishing sering kali memanfaatkan banyak subdomain untuk meniru domain resmi. Sistem menganalisis struktur domain dan menghitung jumlah subdomain untuk mendeteksi indikasi tersebut.
- Penggunaan Karakter Spesial dan Numerik
  Fitur ini menilai seberapa banyak karakter seperti “-”, “_”, “%”, atau angka digunakan dalam URL. URL berbahaya umumnya mengandung karakter seperti itu untuk mengelabui pengguna.
- Penggunaan Kata Kunci Mencurigakan
  Sistem mendeteksi keberadaan kata kunci seperti “login”, “secure”, “verify”, atau “update”, yang sering digunakan oleh pelaku phishing untuk menarik kepercayaan korban.
- Port Non-Standar dan Redireksi
  Beberapa situs berbahaya menggunakan port yang tidak umum atau teknik pengalihan (redirect) untuk menyembunyikan aktivitas berbahaya di balik server lain.

Setelah semua fitur dianalisis, sistem melakukan klasifikasi berdasarkan hasil perbandingan nilai-nilai fitur tersebut dengan pola karakteristik yang telah ditentukan dari data URLHaus. Hasil klasifikasi yang muncul ditampilkan dalam tiga kategori utama:

- Normal, jika seluruh fitur menunjukkan karakteristik wajar dari situs aman,
- Suspicious, jika terdapat ciri mencurigakan namun belum cukup untuk dikategorikan berbahaya, dan
- Malicious, jika URL menunjukkan pola khas dari situs berbahaya atau terindikasi mengandung malware/phishing.

Dari hasil uji coba terhadap beberapa URL dengan berbagai karakteristik, sistem mampu menghasilkan deteksi dengan waktu respon rata-rata kurang dari tiga detik. Hal ini menunjukkan bahwa sistem cukup efisien dan dapat digunakan secara real-time tanpa mengganggu kenyamanan pengguna. Selain itu, tingkat akurasi sistem dalam membedakan situs normal dan berbahaya juga stabil karena sistem memanfaatkan sumber data API yang selalu diperbarui.

Secara fungsional, halaman analisis URL ini menjadi inti dari keseluruhan sistem karena merupakan titik awal pengguna dalam melakukan pemeriksaan keamanan situs. Tampilan antarmuka yang sederhana membantu pengguna umum melakukan deteksi tanpa memerlukan keahlian teknis dalam analisis jaringan.

Tahapan berikutnya adalah tampilan detail hasil analisis URL. Setelah proses analisis awal selesai, sistem menampilkan hasil yang lebih

komprehensif dengan menjabarkan nilai dari setiap fitur yang diperiksa beserta interpretasinya. Tujuan utama bagian ini adalah memberikan pemahaman yang lebih mendalam kepada pengguna tentang alasan di balik hasil klasifikasi yang ditampilkan.

Pada tampilan ini, pengguna dapat melihat secara langsung parameter-parameter teknis yang menjadi dasar pengambilan keputusan oleh sistem, seperti panjang URL, jumlah subdomain, tingkat keamanan protokol, serta adanya karakter atau pola mencurigakan. Setiap fitur diberi indikator berupa nilai numerik atau status, disertai keterangan apakah nilai tersebut tergolong aman, mencurigakan, atau berbahaya.

Selain penjabaran fitur, sistem juga menyertakan indikator visual dalam bentuk progress bar atau grafik risiko yang menunjukkan tingkat bahaya URL secara lebih intuitif. Indikator ini dibagi dalam tiga tingkatan warna, yaitu:

- Hijau untuk tingkat risiko rendah (Normal),
- Kuning untuk tingkat risiko menengah (Suspicious), dan
- Merah untuk tingkat risiko tinggi (Malicious).

Pendekatan visual ini dirancang agar pengguna dapat segera mengenali tingkat ancaman tanpa harus membaca rincian teknis secara mendalam. Dengan demikian, sistem tidak hanya berfungsi sebagai alat deteksi otomatis, tetapi juga bersifat edukatif, karena memberikan pemahaman kepada pengguna tentang bagaimana suatu URL dikategorikan.

Dari hasil pengujian, sistem menunjukkan kemampuan yang baik dalam menampilkan hasil analisis secara transparan dan konsisten. Setiap hasil analisis dapat ditelusuri kembali berdasarkan fitur yang diperiksa, sehingga meningkatkan keandalan dan interpretabilitas sistem.

Integrasi dengan API URLHaus juga menjadi keunggulan utama dalam tahapan ini, karena memberikan data pembanding aktual dari situs yang telah terverifikasi sebagai berbahaya oleh komunitas keamanan siber global. Dengan demikian, sistem tidak hanya bergantung pada aturan statis yang ditentukan secara lokal, tetapi juga mendapatkan validasi eksternal dari sumber yang kredibel.

5. KESIMPULAN

Berdasarkan hasil penelitian dan implementasi sistem klasifikasi URL berbasis analisis fitur jaringan, diperoleh beberapa kesimpulan sebagai berikut:

a. Sistem yang dikembangkan mampu mendeteksi situs berbahaya (*malicious URL*) secara otomatis berdasarkan analisis fitur jaringan tanpa perlu mengakses konten situs secara langsung, sehingga lebih aman dan efisien untuk digunakan.
b. Fitur-fitur jaringan yang digunakan, seperti panjang URL, jumlah subdomain, karakter spesial, penggunaan HTTPS, dan kata kunci mencurigakan, terbukti efektif dalam membedakan situs *normal*, *suspicious*, dan *malicious*.
c. Integrasi API eksternal seperti URLHaus meningkatkan akurasi sistem dalam klasifikasi URL dengan memanfaatkan basis data keamanan global yang terus diperbarui.
d. Pengujian menunjukkan bahwa sistem mampu melakukan deteksi dengan waktu respon rata-rata kurang dari tiga detik per URL, menunjukkan performa yang cepat dan stabil untuk penggunaan real-time.
e. Antarmuka sistem dirancang sederhana dan informatif, menampilkan hasil analisis melalui indikator risiko (*risk level bar*) yang membantu pengguna memahami tingkat keamanan suatu situs.
f. Sistem ini tidak hanya berfungsi sebagai alat deteksi, tetapi juga sebagai media edukatif yang dapat meningkatkan kesadaran pengguna terhadap ancaman keamanan siber.
g. Penelitian ini dapat dikembangkan lebih lanjut dengan integrasi algoritma *machine learning* dan penyimpanan basis data dinamis untuk meningkatkan kemampuan adaptasi terhadap pola serangan baru di masa depan.

DAFTAR PUSTAKA

[1] A. R. Putra and R. A. Fauzi, “Analisis keamanan jaringan pada implementasi sistem informasi berbasis web,” *Jurnal Teknologi dan Sistem Informasi*, vol. 9, no. 2, pp. 112–120, 2024.

[2] S. N. Siregar and T. Lubis, “Kajian metode deteksi situs phishing berbasis URL dengan algoritma lokal,” *Jurnal Informatika dan*

Komputer Indonesia, vol. 6, no. 1, pp. 45–52, 2023.

[3] A. Agustani, H. Setiawan, and T. Tasmi, "Analisis perilaku pengguna terhadap akses internet di PT Chiyoda International Indonesia menggunakan machine learning," *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, vol. 13, no. 3, 2025.

[4] D. Kiswanto, F. Ramadhani, N. M. Surbakti, and N. A. Nasution, "Pengembangan dan implementasi sistem deteksi serangan DDoS berbasis algoritma Random Forest," *Bulletin of Information Technology (BIT)*, vol. 6, no. 3, pp. 247–256, 2025.

[5] R. Purwanto and A. Santoso, "Penerapan analisis pola URL untuk deteksi situs phishing menggunakan pendekatan berbasis fitur," *Jurnal Teknologi Informasi dan Komputer*, vol. 8, no. 1, pp. 31–40, 2024.

[6] M. Arifin and D. Wulandari, "Pemanfaatan API publik untuk deteksi URL berbahaya tanpa analisis konten," *Jurnal Sistem Informasi dan Keamanan Siber Indonesia*, vol. 5, no. 2, pp. 55–62, 2024.

[7] L. Hutapea and A. Simanjuntak, "Analisis penggunaan API VirusTotal untuk mendeteksi situs web berbahaya," *Jurnal Keamanan Informasi dan Aplikasi Komputer*, vol. 4, no. 2, pp. 20–27, 2023.

[8] P. S. Wijaya and E. S. Rohman, "Rancang bangun sistem keamanan web menggunakan analisis fitur jaringan," *Jurnal Informatika Nusantara*, vol. 9, no. 4, pp. 145–153, 2024.

[9] H. Nasrullah and M. Y. Siregar, "Implementasi metode analisis fitur untuk deteksi phishing site," *Jurnal Rekayasa Teknologi Informasi*, vol. 7, no. 1, pp. 12–20, 2025.

[10] F. Maulana and R. Pratama, "Evaluasi sistem deteksi URL berbahaya berbasis integrasi API keamanan," *Jurnal Teknologi Siber Nasional*, vol. 5, no. 3, pp. 80–88, 2025.

[11] I. Lestari and B. Syahputra, "Analisis keamanan siber pada layanan digital publik di Indonesia," *Jurnal Keamanan dan Aplikasi Teknologi Informasi*, vol. 4, no. 2, pp. 41–50, 2023.

[12] D. Cahyani, "Penerapan metode scoring untuk klasifikasi URL berisiko tinggi," *Jurnal Teknologi dan Inovasi Digital*, vol. 2, no. 1, pp. 23–30, 2024.

[13] Y. Situmorang and M. Anggara, "Pengembangan sistem monitoring URL berbahaya menggunakan API eksternal," *Jurnal Aplikasi Informatika dan Keamanan Jaringan*, vol. 5, no. 2, pp. 67–74, 2024.

[14] A. Ramadhan, "Perancangan sistem keamanan web berbasis analisis domain dan jaringan," *Jurnal Komputasi dan Teknologi Informasi*, vol. 6, no. 3, pp. 91–99, 2023.

[15] A. Hakim and F. Sukma, "Pemanfaatan data URLHaus dalam pendeteksian situs berbahaya," *Jurnal Keamanan Siber Nasional*, vol. 3, no. 2, pp. 28–35, 2025.