IMPLEMENTASI *INTRUSION DETECTION SYSTEM* (IDS) BERBASIS *RANDOM FOREST* UNTUK DETEKSI SERANGAN *PHISHING* PADA JARINGAN WI-FI PUBLIK

Christian Mariano Benny Nara Sanjaya, Yohanes Suban Belutowe, Semlinda Juszandri Bulan
Teknik Informatika, STIKOM Uyelindo Kupang
Jl. Perintis Kemerdekaan I, Kayu Putih, Kec. Oebobo, Kota Kupang, Nusa Tenggara Tim. 85228.
crisannara99@gmail.com

ABSTRAK

Penggunaan jaringan Wi-Fi publik yang semakin luas memberikan kemudahan akses internet, namun juga meningkatkan risiko keamanan, khususnya serangan *phishing* yang memanfaatkan rekayasa sosial pada jaringan terbuka. Permasalahannya dalam penelitian ini adalah keterbatasan sistem dalam mendeteksi aktivitas *phishing* secara akurat pada lalu lintas jaringan. Penelitian ini bertujuan untuk mengembangkan *Intrusion Detection System* (IDS) berbasis *machine learning* untuk mendeteksi serangan *phishing* berbasis URL pada jaringan Wi-Fi publik. Metode yang digunakan meliputi pengumpulan dataset dari sumber publik dan hasil pengumpulan mandiri berbasis URL sebanyak 5.000 data, prapemrosesan data, ekstraksi fitur, pelatihan model menggunakan algoritma Random Forest, serta evaluasi kinerja dalam lingkungan simulasi. Hasil penelitian menunjukkan bahwa model mampu mencapai akurasi sebesar 92,45%, *precision* 88,63%, *recall* 97,40%, *F1-score* 92,81% dan *ROC-AUC* 0,9632, yang menunjukkan performa klasifikasi yang sangat baik dalam mendeteksi URL *phishing*. Sistem ini dapat digunakan untuk meningkatkan keamanan jaringan Wi-Fi publik.

Kata kunci : *Intrusion Detection System, Phishing, Random Forest, Wi-Fi Publik.*

1. PENDAHULUAN

Kemudahan, koneksi internet, adalah salah satu dari banyak manfaat pertumbuhan teknologi informasi yang lebih maju. Ketersediaan jaringan *Wireless Fidelity* (Wi-Fi) publik, yang dapat diakses publik di berbagai lokasi publik, termasuk universitas, kafe, kantor, bandara, dan bahkan pusat perbelanjaan, adalah salah satu contoh kemudahan ini. Akses internet yang mudah melalui situs web, termasuk penggunaan jaringan publik, menimbulkan bahaya serangan *phishing* yang cukup besar, yang sangat sulit dibedakan antara situs asli dan palsu, Untuk itu dipilih algoritma *Random Forest* yang mampu mengidentifikasi situs web *phishing* dengan akurasi hingga 94,36% [6]. Namun, meningkatnya risiko keamanan, seperti serangan siber, juga menyertai kemudahan ini. Meskipun ada banyak jenis serangan siber yang berbeda, *phishing* adalah upaya yang paling sering terjadi karena *phishing* dibuat untuk mencuri informasi sensitif seperti nama pengguna, kata sandi, dan data pribadi secara curang melalui rekayasa sosial atau situs web palsu adalah jenis yang paling umum yang menargetkan Wi-Fi publik.

Upaya *phishing* menjadi semakin berbahaya karena pengguna sering terhubung ke jaringan Wi-Fi publik tanpa otentikasi keamanan. Penyerang dapat memanfaatkan hal ini dengan membuat halaman *login* palsu, mengubah DNS, atau mengarahkan korban ke URL berbahaya. Klasifikasi URL berbasis *Random Forest* bermanfaat untuk mendeteksi koneksi *phishing* dengan cepat di jaringan publik [7].

Penggunaan Sistem Deteksi Intrusi (IDS), alat keamanan jaringan yang penting untuk melacak lalu lintas jaringan dan mengidentifikasi tren yang mencurigakan, adalah salah satu pendekatan yang mungkin. Namun demikian, versi *phishing* baru belum dapat diidentifikasi oleh IDS konvensional, seperti yang berbasis tanda tangan. Sistem deteksi intrusi kini dapat secara otomatis mendeteksi serangan dengan belajar dari pola data berkat munculnya pembelajaran mesin (ML) dan pendekatan berbasis kecerdasan buatan lainnya [5]. Karena dapat diandalkan, tahan terhadap *overfitting*, dan mampu menangani berbagai fitur URL, algoritma *Random Forest* adalah pilihan terbaik. Penggunaan *Random Forest* dalam deteksi *phishing* dapat mempercepat identifikasi risiko dan memberikan peringatan dini kepada pengguna [6].

Penelitian ini berfokus pada identifikasi URL yang diakses melalui jaringan Wi-Fi publik dengan merancang IDS yang berfungsi pada tingkat aplikasi (*Application-Layer* NIDS). Metode ini menggunakan *Random Forest* yang dilatih pada kumpulan URL *phishing* untuk mengklasifikasikan URL yang diekstrak secara *real-time* dari lalu lintas DNS dan HTTP. Dengan metode ini, sistem dapat mengidentifikasi bahaya secara andal tanpa memeriksa setiap paket jaringan secara menyeluruh.

Diharapkan bahwa dengan menerapkan IDS berbasis *Random Forest* pada jaringan Wi-Fi publik, sistem akan fleksibel, efektif, dan menawarkan tingkat keamanan ekstra kepada konsumen. Diantisipasi bahwa penelitian ini akan secara signifikan meningkatkan keamanan jaringan publik dan bertindak sebagai panduan untuk pembuatan sistem deteksi intrusi berbasis pembelajaran mesin di masa mendatang.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian tentang Analisis Efektivitas Sistem Deteksi Intrusi Terhadap Serangan DdoS: Investigasi Berbasis Simulasi membahas pembuatan sistem deteksi intrusi (IDS) berbasis pembelajaran mesin untuk mengidentifikasi serangan DDoS pada jaringan komputer menggunakan algoritma XGBoost dan *dataset* CICIDS2017 dalam Investigasi Berbasis Simulasi. Pra-pemrosesan data, undersampling untuk keseimbangan kelas, normalisasi fitur, pelatihan model, dan pencarian grid untuk optimasi *hyperparameter* semuanya termasuk dalam studi ini. Presisi, *recall*, F1-score, matriks kebingungan, dan ROC-AUC digunakan untuk evaluasi. Model tersebut mampu memperoleh nilai evaluasi di atas 99%, menurut data, menunjukkan bahwa algoritma XGBoost berhasil dalam mengidentifikasi serangan DDoS pada jaringan komputer [5].

Sistem Deteksi *Phishing* Menggunakan Algoritma *Random Forest*, berfokus pada penerapan algoritma *Random Forest* dalam sistem deteksi *phishing* berbasis pembelajaran mesin. Meningkatkan efektivitas sistem deteksi terhadap jenis serangan *phishing* yang lebih canggih adalah tujuan dari studi ini. Campuran metode ekstraksi fitur dari *dataset* URL dan perbandingan algoritma *Random Forest* dengan algoritma lain seperti Naïve Bayes dan Decision Tree digunakan dalam metodologi penelitian. Menurut temuan, *Random Forest* dianggap lebih dapat diandalkan dalam mengidentifikasi *phishing* dengan cepat dan efektif karena menawarkan tingkat akurasi maksimum dengan tingkat false positive yang rendah [11].

2.2. Jaringan Wi-Fi Publik

Jaringan Wi-Fi publik adalah jaringan nirkabel yang terbuka untuk umum di area publik termasuk pusat perbelanjaan, bandara, kampus, dan kafe. Jaringan ini memiliki risiko keamanan yang cukup besar, termasuk upaya *phishing* yang menipu pengguna agar menggunakan halaman login atau tautan palsu untuk mencuri informasi sensitif, meskipun sebenarnya jaringan ini menyediakan akses internet yang sederhana. Kerentanan ini menunjukkan bahwa mekanisme keamanan tambahan, seperti sistem deteksi otomatis, diperlukan untuk melindungi konsumen [10].

2.3. *Intrusion Detection System* (IDS)

Sistem keamanan yang disebut sistem deteksi intrusi (IDS) mengawasi aktivitas jaringan atau sistem komputer untuk mendeteksi aktivitas yang mencurigakan dan potensi risiko keamanan. IDS mendeteksi tanda-tanda intrusi dari penyerang eksternal dan pengguna internal yang tidak berwenang dengan memeriksa lalu lintas jaringan dan perilaku sistem [8].

2.4. *Machine Learning* dan *Random Forest*

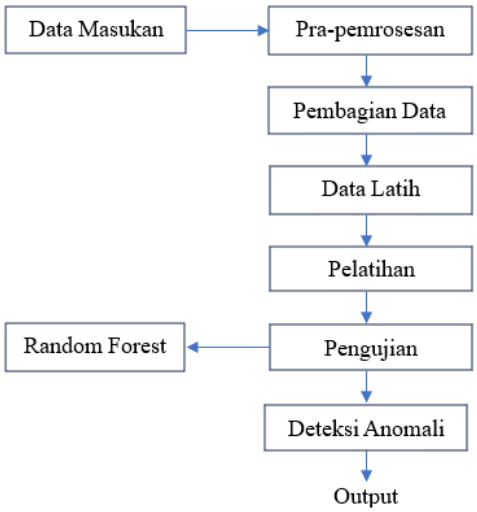
Dalam bidang kecerdasan buatan (AI), pembelajaran mesin memungkinkan sistem komputer untuk belajar dari data guna mengidentifikasi pola, mengkategorikan, dan memprediksi tanpa memerlukan pemrograman eksplisit. Pembelajaran mesin digunakan dalam keamanan jaringan untuk memeriksa lalu lintas jaringan dan secara otomatis mengidentifikasi serangan siber atau aktivitas yang tidak biasa [1]. Salah satu algoritma populer adalah *Random Forest*, teknik pembelajaran *ensemble* yang menggabungkan beberapa Pohon Keputusan dan menggunakan suara mayoritas untuk memilih hasilnya. Menurut penelitian, *Random Forest* meningkatkan akurasi klasifikasi dengan mendeteksi URL *phishing* dengan akurasi 97,2%, yang lebih besar daripada Pohon Keputusan (96,3%) dan *Naïve Bayes* (85,3%) [4].

2.5. Fitur Dalam Deteksi *Phishing*

Komponen kunci dalam meningkatkan efektivitas model deteksi *phishing* berbasis pembelajaran mesin adalah pemilihan fitur. Fitur adalah atribut data, seperti struktur domain dan URL, yang digunakan untuk membedakan antara situs *web phishing* dan situs *web* asli. Beberapa fitur dapat dikelola menggunakan algoritma *Random Forest*, yang juga dapat mengidentifikasi fitur mana yang memiliki dampak terbesar pada hasil prediksi [2]. Panjang URL yang tidak biasa, penggunaan karakter khusus, struktur domain atau subdomain yang meniru situs web asli, dan kemiripan nama domain (*typosquatting*) adalah elemen yang sering digunakan. Selain itu, karena banyak situs *web phishing* juga menggunakan HTTPS, penggunaannya tidak selalu menjamin keamanan. Untuk meminimalkan *noise*, menghindari *overfitting*, dan meningkatkan akurasi model, pemilihan fitur sangat penting.

2.6. IDS Berbasis *Random Forest* Untuk Deteksi *Phishing*

Upaya *phishing* semakin banyak dideteksi melalui penggunaan teknik pembelajaran mesin yang dikombinasikan dengan sistem deteksi intrusi (IDS). Salah satu pendekatan populer adalah *Random Forest*, metodologi pembelajaran *ensemble* yang menciptakan model prediksi yang lebih andal dan akurat dengan menggabungkan banyak pohon keputusan. Beberapa pohon keputusan *Random Forest* meningkatkan akurasi, sehingga sangat baik dalam membedakan antara URL yang sah dan URL phishing [6]. Diagram alir IDS berbasis *Random Forest* terlihat seperti berikut:



Gambar 1. Diagram Alur IDS *Berbasis Random Forest*

Gambar 1 menampilkan alur kerja sistem deteksi *phishing* berbasis *Random Forest*. Proses dimulai dari data masukan yang kemudian melalui tahap pra-pemrosesan untuk membersihkan dan menyiapkan data. Selanjutnya, data dibagi menjadi data latih dan data uji. Data latih digunakan dalam tahap pelatihan untuk membangun model *Random Forest*. Model yang telah dilatih kemudian digunakan pada tahap pengujian untuk menganalisis data uji. Hasil pengujian digunakan untuk mendeteksi anomali atau indikasi *phishing*, yang selanjutnya menghasilkan output berupa keputusan klasifikasi.

3. METODE PENELITIAN

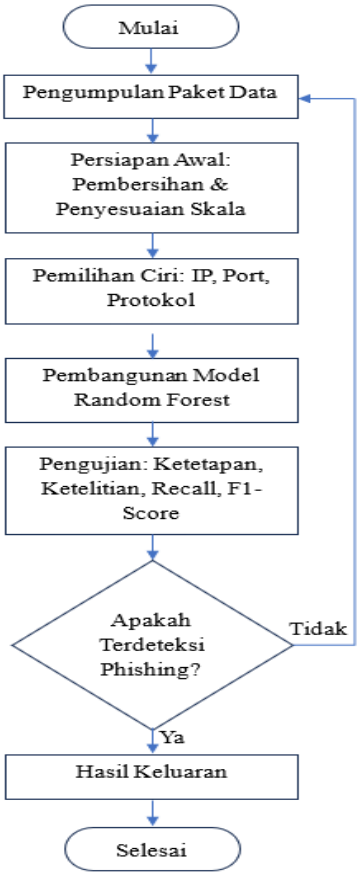
3.1. Analisis Data

Analisis data dilakukan untuk mengevaluasi performa model *Random Forest* dalam mendeteksi serangan *phishing* pada jaringan *Wi-Fi* publik. Tahapan utamanya meliputi:

a. Eksplorasi dan Pra-pemrosesan Data
   Mengkodekan karakteristik kategorikal, menangani data yang hilang, melakukan analisis distribusi data *phishing* dan URL regular, serta mempersiapkan data untuk pelatihan model.
b. Pelatihan Model
   Model *Random Forest* dilatih dengan *dataset* latih, pengaturan parameter sepertri jumlah pohon dan kedalaman maksimum untuk meningkatkan kinerja model.
c. Evaluasi Model
   Evaluasi model dilakukan menggunakan data uji dengan metrick *Accuracy, Precision, Recall*, dan *F1-Score* serta serta *confusion matrix* untuk mengukur kinerja dan efektivitas model dalam mendeteksi *phishing* [3].
d. Analisis dan Validasi
   Mengevaluasi efektivitas algoritma *Random Forest* dalam mengidentifikasi *phishing* berbasis URL dengan menganalisis hasil penilaian model dan membandingkannya dengan penelitian sebelumnya sebagai metode validasi.
e. Visualisasi
   Hasil prediksi dan metrik peforma model divisualisasikan dalam bentuk grafik untuk mempermudah interpretasi dan analisis kinerja model.

3.2. Alur Sistem

Untuk memahami spesifikasi dan pengoperasian Sistem Deteksi Intrusi (IDS) berbasis *Random Forest*, dilakukan analisis sistem. Untuk melindungi privasi pengguna, sistem memantau permintaan DNS dan header Host HTTP/SNI tanpa menggunakan *Deep Packet Inspection*. *Random Forest* digunakan untuk pra-pemrosesan, ekstraksi fitur, dan klasifikasi URL yang diperoleh. Alur sistem meliputi input paket jaringan secara *real-time*, pemrosesan dan klasifikasi data, serta laporan kinerja dan temuan deteksi *phishing* sebagai output.



Gambar 2. Diagram Alur Evaluasi Sistem IDS

Gambar 2. Menunjukan proses deteksi *phishing* yang dimulai dari pengumpulan dan pembersihan data, dilanjutkan dengan pemilihan fitur dan pelatihan model *Random Forest*. Model kemudian diuji, dan sistem menentukan ada tidaknya *phishing*; jika terdetksi, hasil dikeluarkan, jika tidak, proses ulang.

4. HASIL DAN PEMBAHASAN

4.1. Implementasi Antarmuka

Dashboard sistem dapat diakses melalui peramban (*browser*) dengan menuju ke alamat server lokal. Antarmuka pengguna dirancang untuk menyajikan informasi hasil pemantauan secara menyeluruh dan langsung (*real-time*). Di bagian atas halaman, terdapat indikator status sistem yang memperlihatkan kondisi terkini, seperti apakah fitur pemantauan aktif, model siap digunakan, dan proses *sniffer* berjalan dengan normal. *Dashboard* sistem dapat dilihat dibawa ini:

Gambar 3. *Dashboard* Sistem IDS

Gambar 3. Menunjukan *dashboard* sistem deteksi *phishing* berbasis IDS. Bagian atas menampilkan ringkasan statistika. Terdapat juga fitur analisis URL untuk deteksi *phishing*. Di bagian bawah, menampilkan distribusi hasil klasifikasi dan beberapa tabel lainnya.

Tabel 1. Statistik Utama *Dashboard*

Nama Statistik	Keterangan
Total DNS Queries	Total permintaan DNS yang terdeteksi
Active Threats	Jumlah ancaman aktif yang teridentifikasi
Blocked Attacks	Jumlah serangan yang harus diblokir
Risk Score	Skor risiko yang mencerminkan tingkat keamanan jaringan

Tabel 1 menampilkan ringkasan statistik keamanan jaringan pada *dashboard*. Total DNS Queries menunjukan jumlah permintaan DNS, Active Threats jumlah ancaman yang terdeteksi, Blocked Attacks jumlah serangan yang berhasil diblokir, dan Risk Score menunjukkan tingkat risiko keamanan jaringan secara keseluruhan.

4.2. Pengujian Model *Machine Learning*

Pengujian terhadap model machine learning dilakukan untuk mengukur tingkat akurasi serta kemampuan model dalam membedakan antara URL *phishing* dan *legimate*. Model yang diimplementasikan dalam sistem ini adalah algoritma *Random Forest* yang telah melalui proses pelatihan dengan menggunakan dataset pengujian sebanyak 2000 sampel data yang terdiri dari 1000 Url Legit dan 1000 Url *Phishing*. Pengujian model dilakukan dengan menghitung beberapa metrik evaluasi klasifikasi yang umum digunakan dalam penelitian *machine learning*, yaitu *accuracy*, *precision*, *recall*, *F1-score*, dan ROC. Hasil pengujian sebagai berikut:

Tabel 2. Hasil Pengujian *Random Forest*

Metrik Evaluasi	Nilai
Accuracy	0.9245
Precision	0.8863
Recall	0.9740
F1-Score	0.9281
ROC-AUC	0.9632
Jumlah Sampel Uji	2000

Tabel 2 menampilkan hasil pengujian dengan kinerja baik, dimana sebagian besar data URL dengan benar dengan nilai *accuracy* 92,45%. Dengan *precision* 88,63%, sebagian besar URL yang ditemukan sebenarnya adalah *phishing*, menunjukkan bahwa prediksi URL *phishing* yang dihasilkan cukup akurat. Dengan *recall* yang tinggi sebesar 97,40%, model tersebut dapat mengidentifikasi hampir setiap URL *phishing* dalam *dataset*, yang sangat penting untuk keamanan. Kinerja klasifikasi model cukup stabil, seperti yang dibuktikan oleh *F1-Score* sebesar 92,81%, yang menunjukkan keseimbangan yang baik antara *precision* dan *recall*. Selain itu, nilai ROC-AUC sebesar 0,9632, yang mendekati 1, menunjukkan bahwa model tersebut secara umum sangat baik dalam membedakan antara URL asli dan URL *phishing*.

4.3. Pengujian Fungsional Sistem

Pengujian dilakukan dengan menggunakan metode *Black Box Testing* untuk menilai fungsionalitas tanpa melihat kode program, digunakan untuk menguji fungsionalitas sistem. Tujuan pengujian ini adalah untuk memastikan bahwa setiap fungsionalitas, termasuk tampilan hasil deteksi, pemantauan jaringan, dan analisis URL, bekerja sebagaimana mestinya.

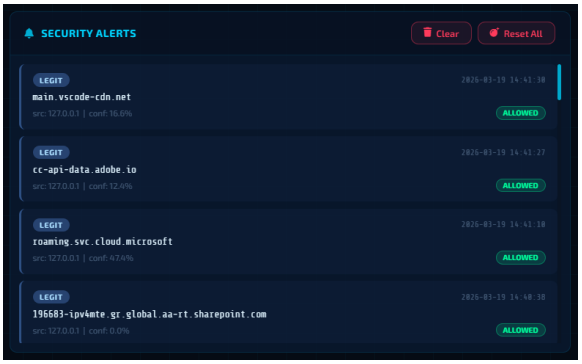
Tabel 3. Hasil Pengujian Sistem

Fitur Sistem	Skenario Pengujian	Hasil
Input URL	Pengguna memasukan URL untuk dianalisis	Berhasil
Analisis URL	Sistem melakukan klasifikasi URL	Berhasil
Monitoring Network	Sistem menampilkan aktivitas jaringan	Berhasil
Dashboard IDS	Sistem menampilkan informasi keamanan jaringan	Berhasil

Tabel 3 menunjukan hasil pengujian fungsional sistem yang diuji berdasarkan skenario penggunanya, dan seluruhnya menghasilkan status "berhasil", yang berarti semua fungsi sistem berjalan dengan baik sesuai yang diharapkan.

4.4. Pengujian Monitoring *Real-Time*

Pengujian terhadap fitur pemantauan *real-time* dilaksanakan untuk memastikan bahwa sistem IDS dapat memonitoring aktivitas jaringan secara langsung dan menyajikan informasi deteksi ancaman melalui *dashboard* secara tepat waktu. Setiap URL yang berhasil dikumpulkan selanjutnya dianalisis oleh model *machine learning* untuk diklasifikasikan apakah termasuk dalam kategori *phishing* atau bukan.



Gambar 4. Monitoring *Real-Time*

Gambar 4 menampilkan hasil dari proses analisis tersebut langsung ditampilkan pada *dashboard* monitoring pada bagian *security alerts*, sehingga pengguna dapat mengamati secara langsung aktivitas jaringan yang sedang berlangsung serta mengetahui potensi ancaman *phishing* yang berhasil diidentifikasi oleh sistem.

4.5. Kelebihan Sistem

Berdasarkan hasil implementasi dan pengujian sistem yang telah dilakukan, terdapat beberapa kelebihan dari sistem yang dibangun, yaitu sebagai berikut:

a. Tingkat akurasi algoritma *Random Forest* mencapai 92,45% dalam mengklasifikasikan URL *phishing* dan normal, menunjukan peforma yang baik.
b. Kemampuan mendeteksi ancaman URL *phishing* yang baik dengan nilai *recall* 97,40% sehingga sebagian besar potensi ancaman dapat teridentifikasi.
c. Proses analisis yang cepat dengan rata-rata 41 milidetik per prediksi.
d. Dashboard monitoring berbasis *web* yang disediakan untuk memudahkan pengguna memantau aktivitas jaringan dan melihat hasil deteksi secara langsung.
e. Monitoring jaringan secara *real-time* sehingga dapat menangkap lalulintas jaringan dan melihat hasil deteksi secara langsung.

4.6. Kekurangan Sistem

Selain memiliki beberapa kelebihan,sistem yang dibangun juga masi memiliki beberapa keterbatasan yang perlu diperhatikan dan dapat dijadikan sebagai referensi untuk pengembangan lebih lanjut, yaitu sebagai berikut:

a. Akurasi model sangat bergantung pada kualitas dataset yang digunakan pada proses pelatihan.
b. Masih terdapat kemungkinan melakukan kesalahan klasifikasi seperti *false positive* maupun *false negative*.
c. Analisis hanya berdasarkan fitur URL yang dipakai.
d. Belum terintegrasi dengan sistem keamanan lain seperti firewall atau SIEM.
e. Pengujian masih terbatas, sehingga perlu validasi di lingkungan yang lebih kompleks.
f. Belum mendukung pembelajaran berkelanjutan (retraining otomatis)

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil mengembangkan sistem IDS untuk mengidentifikasi *phishing* pada jaringan Wi-Fi publik menggunakan algoritma *Random Forest*, yang dapat mengevaluasi URL dari lalu lintas jaringan dan memberikan *dashboard* pemantauan, berdasarkan desain, implementasi, dan hasil pengujian. Dengan *acuracy* 92,45%, *precision* 88,63%, *recall* 97,40%, dan waktu pemrosesan rata-rata 41 milidetik per prediksi, model ini menunjukkan kinerja yang baik pada 2000 data uji, menunjukkan efektivitas dan responsivitasnya dalam deteksi ancaman. Namun, sistem ini masih memiliki kekurangan, sehingga diperlukan lebih banyak pekerjaan. Ini termasuk menambahkan dan memperbarui *dataset* agar lebih beragam, mengoptimalkan model melalui penyetelan atau teknik lain, menambahkan analisis selain struktur URL (seperti konten dan sertifikat), mengintegrasikan dengan sistem keamanan lain, menguji di lingkungan yang lebih kompleks, dan menerapkan mekanisme pelatihan ulang otomatis untuk menjaga sistem tetap adaptif terhadap pola phishing terbaru.

DAFTAR PUSTAKA

[1] A. Al-qasmi, A. Al-anazi, L. Al-shehri, S. A-Ishaman,W. Al-atawi, dan Onytra, "Machine Learning-Based Phishing Detection System," *International Journal of Intelligent System and Application in Engineering*, vol. 12, no. 4, pp. 4367-4372, 2024.
[2] S. Budiman, A. Sunyoto, dan A. Nasiri, "Analisa Performa Penggunaan Feature Selection untuk Mendeteksi Intrusion Detection Systems dengan Algoritma Random Forest Classifier," *Jurnal Sistem Informasi*, vol. 10, no. 3, pp. 753–760, 2021.
[3] M. Fahri, "Penerapan Algoritma Random Forest untuk Deteksi Phishing pada Website," *JITSI Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 2, pp. 186–194, 2025.

[4] R. Fauzan, A. V. Vitianingsih, D. Cahyono, A. L. Maukar, dan Y. A. B. Suprio, "Penerapan Algoritma Klasifikasi pada Machine Learning untuk Deteksi Phishing," *Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 2, pp. 531–540, 2025.

[5] Zy. A. T. Isarianto, D. Maulana, dan A. Susilo, "Analisis Efektivitas Sistem Deteksi Intrusi Terhadap Serangan DDoS: Investigasi Berbasis Simulasi," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 4, pp. 6983–6987, 2025.

[6] A. K. Kencana, F. D. Ananda, A. D. Hartanto, dan Hartatik, "Implementasi Metode Random Forest Klasifikasi untuk Phishing Link," *Information Technology Journal*, vol. 4, no. 2, pp. 55–59, 2022.

[7] A. D. Harahap, D. Juardi, dan A. S. Y. Irwan, "Rancang Bangun Sistem Pendeteksi Link Phishing Menggunakan Algoritma Random Forest," *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, vol. 12, no. 3, pp. 2677–2686, 2024.

[8] K. Inayah dan K. Ramli, "Analisis Kinerja Intrusion Detection System Berbasis Algoritma Random Forest Menggunakan Dataset Unbalanced," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 4, no. 11, pp. 867–876, 2024.

[9] R. Jayaraj, A. Pushpalatha, K. Sangeetha, T. Kamaleshwar, S. U. Shree, dan D. Damodaran, "Intrusion Detection Based on Phishing Detection with Machine Learning," *Measurement: Sensors*, vol. 31, pp. 1–5, 2023.

[10] M. Nurdin, A. Pranandi, F. U. Dwi, Y. Hermawan, dan R. Fadlapi, "Serangan Phishing Wifi Menggunakan ESP8266: Replikasi Jaringan untuk Penangkapan Informasi Otentikasi," *Jurnal Humaniora Sosial dan Bisnis*, vol. 2, no. 7, pp. 638–649, 2024.

[11] G. Ramesh, R. B. Lokitha, R. R. Monisha, dan N. S. Neha, "Phishing Detection System using Random Forest Algorithm," *IJRTI*, vol. 8, no. 4, pp. 510–514, 2023.