Journix: Journal of Informatics and Computing
Vol. 1 No. 2, 2025 : 51-62
ISSN : 3090-6784 | DOI : 10.63866/journix.v1i2.8

Real-Time Phishing Detection Using Google Safe Browsing API and Machine Learning

Zumhur Alamin [1*], Ritzkal [2]

[1] Program Studi Ilmu Komputer, Universitas Muhammadiyah Bima, Indonesia
[2] Program Studi Teknik Informatika, Universitas Ibn Khaldun Bogor, Indonesia

Email: zumhur.alamin@gmail.com
(* : corresponding author)

ABSTRACT – Phishing remains one of the fastest-evolving cybersecurity threats, where attackers mimic legitimate websites to obtain sensitive user information. This study presents a real-time evaluation of a phishing detection system integrating the Google Safe Browsing API with ensemble machine learning models. The research aims to enhance detection accuracy and responsiveness against emerging phishing websites by combining real-time threat intelligence with automated URL analysis. The dataset used comprises over 20,000 URLs collected from Google Safe Browsing, PhishTank, and OpenPhish between June and December 2024. Four approaches were evaluated: (1) machine learning models without API, (2) API-only detection, (3) machine learning with API as an additional feature, and (4) machine learning with API as a validator. The best performance was achieved by the API-as-validator model, reaching 98.2% accuracy, reducing false positives to 2.1%, and lowering false negatives to 3.2%, with an average latency of 108 ms. These findings demonstrate that integrating real-time threat feeds significantly enhances adaptability and reliability in phishing detection. Future research will focus on latency optimization and federated learning to enable large-scale collaborative detection systems.

KEYWORDS: Phishing, Machine Learning, Google Safe Browsing API, Cybersecurity, Ensemble Learning

Deteksi Phishing Real-Time Menggunakan Google Safe Browsing API dan Machine Learning

ABSTRAK – Phishing merupakan salah satu ancaman keamanan siber yang berkembang paling cepat, di mana penyerang meniru situs web sah untuk memperoleh informasi sensitif pengguna. Penelitian ini menyajikan evaluasi real-time terhadap sistem deteksi phishing yang mengintegrasikan Google Safe Browsing API dengan model pembelajaran mesin ansambel. Tujuan penelitian ini adalah untuk meningkatkan akurasi dan responsivitas deteksi terhadap situs phishing yang terus bermunculan dengan menggabungkan intelijen ancaman real-time dan analisis URL otomatis. Dataset yang digunakan terdiri dari lebih dari 20.000 URL yang dikumpulkan dari Google Safe Browsing, PhishTank, dan OpenPhish antara Juni hingga Desember 2024. Empat pendekatan dievaluasi: (1) model pembelajaran mesin tanpa API, (2) deteksi berbasis API saja, (3) pembelajaran mesin dengan API sebagai fitur tambahan, dan (4) pembelajaran mesin dengan API sebagai validator. Kinerja terbaik diperoleh pada model dengan API sebagai validator, mencapai akurasi 98,2%, menurunkan tingkat false positive menjadi 2,1%, dan false negative menjadi 3,2%, dengan rata-rata latensi 108 ms. Temuan ini menunjukkan bahwa integrasi sumber data ancaman real-time secara signifikan meningkatkan adaptivitas dan keandalan sistem deteksi phishing. Penelitian selanjutnya akan difokuskan pada

optimalisasi latensi dan penerapan federated learning untuk mendukung sistem deteksi kolaboratif berskala besar.

KATA KUNCI: Phishing, Machine Learning, Google Safe Browsing API, Keamanan Siber, Ensemble Learning

Received : 15-03-2025	**Revised :** 04-07-2025	**Published :** 30-08-2025

1. PENDAHULUAN

Evolusi pesat teknologi informasi telah secara signifikan mengubah layanan online, namun juga menyebabkan lonjakan ancaman keamanan siber, terutama serangan phishing. Phishing, suatu bentuk rekayasa sosial, melibatkan menipu pengguna untuk mengungkapkan informasi sensitif dengan menyamar sebagai entitas yang sah melalui berbagai metode, termasuk email, situs web palsu, dan interaksi media sosial [1], [2]. Kelompok Kerja Anti-Phishing melaporkan peningkatan 65% yang mengejutkan dalam situs phishing pada tahun 2024, dengan lebih dari 932.923 insiden tercatat hanya pada kuartal ketiga [3]. Peningkatan ini dikaitkan dengan taktik yang semakin canggih, sering memanfaatkan AI canggih dan teknik pembelajaran mesin untuk meningkatkan strategi deteksi dan pencegahan [4], [5]. Tindakan penanggulangan yang efektif, seperti analisis URL real-time dan integrasi AI yang dapat dijelaskan, sangat penting untuk meningkatkan transparansi dan kepercayaan pada sistem deteksi phishing, sehingga mengurangi kerusakan finansial dan reputasi yang terkait dengan serangan ini [3], [4].

Metode deteksi phishing tradisional, terutama pendekatan berbasis daftar hitam dan berbasis aturan, menghadapi keterbatasan signifikan dalam mengatasi sifat dinamis serangan phishing. Metode daftar hitam hanya dapat mengidentifikasi ancaman yang diketahui sebelumnya, sementara sistem berbasis aturan bergantung pada pola yang ditentukan secara manual, membuatnya lambat untuk beradaptasi dengan taktik baru [6], [7]. Sebaliknya, solusi kontemporer memanfaatkan teknik pembelajaran mesin (ML) dan pembelajaran mendalam (DL), yang meningkatkan akurasi deteksi dengan menganalisis fitur kompleks dan beradaptasi dengan berbagai jenis phishing [8]. Model hibrida, menggabungkan metode tradisional dan canggih, telah menunjukkan hasil yang menjanjikan, mencapai akurasi deteksi melebihi 97% dalam beberapa kasus [8]. Sistem canggih ini tidak hanya meningkatkan kemampuan deteksi real-time tetapi juga mengatasi tantangan seperti kelangkaan data dan serangan musuh, sehingga memberikan pertahanan yang lebih kuat terhadap ancaman phishing yang berkembang.

Dalam dekade terakhir, pendekatan pembelajaran mesin (ML) telah meningkatkan deteksi phishing secara signifikan, dengan algoritma seperti Support Vector Machine (SVM), Random Forest (RF), dan K-Nearest Neighbors (k-NN) secara efektif mengidentifikasi pola kompleks dalam data phishing, termasuk fitur URL dan struktur halaman [9], [10]. Namun, batasan kritis tetap ada: model ini sering bergantung pada kumpulan data statis, yang menyebabkan penurunan kinerja terhadap ancaman phishing yang baru muncul karena kebuntuan data [10], [11]. Studi terbaru menekankan perlunya pembaruan data real-time yang dinamis untuk meningkatkan kemampuan deteksi, karena metode tradisional berjuang dengan sifat ancaman cyber yang berkembang [12], [13]. Kerangka kerja inovatif yang menggabungkan evaluasi fitur dan koefisien prioritas telah menunjukkan harapan dalam meningkatkan akurasi deteksi, mencapai tingkat setinggi 98,95% [10]. Selanjutnya, teknik

pembelajaran mendalam, seperti jaringan saraf konvolusional dan berulang, sedang dieksplorasi untuk mengatasi tantangan ini, menawarkan solusi potensial untuk sistem deteksi phishing yang lebih kuat [11].

Integrasi sumber data ancaman real-time, seperti Google Safe Browsing API, secara signifikan meningkatkan sistem deteksi phishing dengan memberikan informasi terkini tentang URL berbahaya. Pendekatan ini mengatasi keterbatasan metode tradisional, yang sering bergantung pada daftar hitam statis yang gagal mengimbangi pembuatan situs phishing yang cepat, diperkirakan lebih dari 1,5 juta bulan [9]. Teknik pembelajaran mesin, khususnya model pembelajaran ansambel, telah menunjukkan harapan dalam meningkatkan akurasi deteksi dan mengurangi positif palsu dengan memanfaatkan fitur intelijen ancaman cyber [14]. Misalnya, sistem seperti PhishStorm menggunakan analitik real-time untuk mengklasifikasikan URL secara efektif, mencapai tingkat klasifikasi 94,91% dengan minimal positif palsu [15]. Selain itu, metode pembelajaran mesin canggih dapat mendeteksi phishing yang dihosting di Fast Flux Service Networks, mencapai akurasi di atas 98% dengan menggunakan serangkaian fitur yang beragam [16]. Secara keseluruhan, kombinasi data real-time dan pembelajaran mesin sangat penting untuk mengembangkan mekanisme deteksi phishing yang kuat.

Penerapan teknik pembelajaran ensemble secara signifikan meningkatkan kinerja model deteksi phishing dengan mengintegrasikan beberapa algoritma klasifikasi, seperti Random Forest (RF), Support Vector Machine (SVM), dan K-Nearest Neighbors (k-NN). Misalnya, model ansambel bertumpuk multilayer menunjukkan kisaran akurasi yang mengesankan dari 96,79% hingga 98,90% di berbagai kumpulan data, secara efektif memanfaatkan kekuatan pengklasifikasi individu sambil mengurangi kelemahan mereka [17]. Demikian pula, penelitian lain mencapai akurasi deteksi 97,51% menggunakan ansambel algoritma RF, Pohon Keputusan, dan XGBoost, menunjukkan efektivitas menggabungkan teknik pemilihan fitur [18]. Selain itu, metode ensemble telah dicatat karena kinerjanya yang unggul baik dalam akurasi deteksi dan efisiensi komputasi, terutama di lingkungan waktu nyata, membuatnya sangat cocok untuk sifat dinamis ancaman phishing [19]. Secara keseluruhan, temuan ini menggarisbawahi peran penting pembelajaran ansambel dalam meningkatkan ketahanan dan generalisasi sistem deteksi phishing [14], [20].

Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada evaluasi integrasi Google Safe Browsing API dengan model pembelajaran mesin dalam mendeteksi situs phishing secara real-time. Tujuan utama penelitian ini adalah untuk:

1. Menggabungkan data ancaman real-time dari Google Safe Browsing API ke dalam model pembelajaran mesin untuk meningkatkan akurasi dan daya adaptasi terhadap situs phishing baru.
2. Menganalisis kinerja beberapa algoritma machine learning, termasuk RF, SVM, dan k-NN, dalam mendeteksi phishing ketika dikombinasikan dengan API real-time.
3. Mengevaluasi pengaruh integrasi API terhadap pengurangan *false positives* dan *false negatives*, serta waktu respons sistem dalam skenario deteksi real-time.

Dengan pendekatan ini, penelitian diharapkan dapat memberikan kontribusi nyata terhadap pengembangan sistem deteksi phishing yang lebih adaptif, akurat, dan efisien, serta dapat diimplementasikan secara praktis dalam sistem keamanan siber modern.

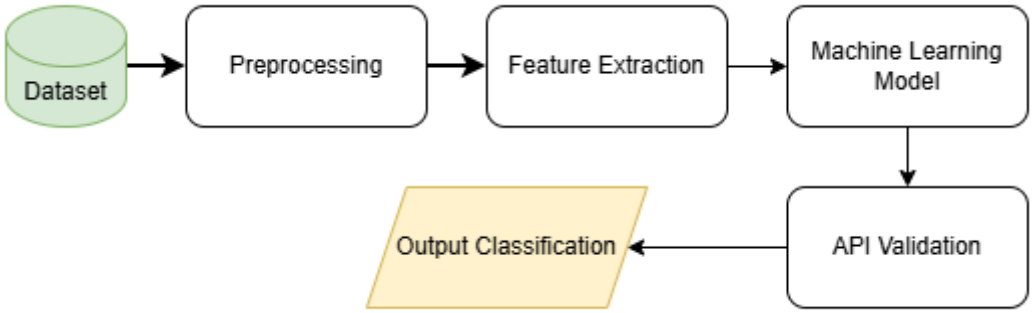
2. METODE PENELITIAN

Bagian ini menjelaskan tahapan metodologis yang digunakan dalam penelitian untuk mengevaluasi efektivitas integrasi Google Safe Browsing API dengan model pembelajaran mesin dalam mendeteksi situs phishing secara real-time. Pendekatan penelitian mencakup pemilihan algoritma pembelajaran mesin, proses integrasi data ancaman real-time, seleksi fitur, pengolahan data, serta prosedur evaluasi performa model.

2.1 Desain Penelitian

Penelitian ini menggunakan desain eksperimen kuantitatif dengan pendekatan *comparative performance evaluation* untuk menilai pengaruh integrasi Google Safe Browsing API pada sistem deteksi phishing. Pendekatan komparatif dipilih karena memungkinkan evaluasi langsung terhadap perbedaan kinerja beberapa konfigurasi model menggunakan dataset, algoritma, dan kondisi pengujian yang sama, sehingga menyediakan dasar analitis yang lebih kuat dibandingkan metode lain seperti *ablation study* yang hanya berfokus pada penghapusan fitur atau komponen model.

Untuk memperjelas alur pemrosesan, penelitian ini mengikuti pipeline sistem seperti pada Gambar 1 berikut:



Gambar 1. Diagram Pipeline Sistem

Empat skenario utama dievaluasi dalam pipeline tersebut, yaitu:

1. Model Pembelajaran Mesin Tanpa API (Baseline)
2. Google Safe Browsing API Tanpa Pembelajaran Mesin
3. Model Pembelajaran Mesin dengan API sebagai Fitur Tambahan
4. Model Pembelajaran Mesin dengan API sebagai Validator

Seluruh skenario diuji menggunakan dataset, parameter, dan metrik evaluasi yang sama untuk memastikan validitas perbandingan.

2.2 Algoritma Pembelajaran Mesin

Penelitian ini menggunakan empat algoritma pembelajaran mesin terawasi untuk melakukan klasifikasi antara situs phishing dan situs legitimate. Seluruh model dibangun dan dieksekusi menggunakan Python 3.10 dengan pustaka scikit-learn 1.3 untuk memastikan replikabilitas proses.

Algoritma yang digunakan adalah sebagai berikut:

1. **Support Vector Machine (SVM)**
   Model SVM diterapkan menggunakan kernel Radial Basis Function (RBF), dengan parameter utama: *C* = 1.0, *gamma* = ‘scale’

2. **Random Forest (RF)**
   Algoritma Random Forest digunakan dengan konfigurasi: n_estimators = 100, *max_depth* = 15, *criterion* = 'gini'
3. **k-Nearest Neighbors (k-NN)**
   Algoritma k-NN dikonfigurasi menggunakan: k = 5, Jarak dihitung menggunakan metrik Euclidean distance
4. **Stacking Ensemble Model**
   Model ansambel dibangun dengan menggabungkan ketiga algoritma di atas sebagai base learners, sementara Logistic Regression digunakan sebagai meta-classifier. Implementasi stacking dilakukan menggunakan modul *StackingClassifier* dari scikit-learn.

Pendekatan kombinasi algoritma ini dirancang untuk menghasilkan keseimbangan antara akurasi, generalisasi, dan efisiensi komputasi dalam sistem deteksi phishing real-time.

2.3 Integrasi Google Safe Browsing API

Google Safe Browsing API digunakan untuk memperkaya dataset dengan informasi ancaman real-time yang diperbarui secara berkala oleh Google. API ini mampu mendeteksi berbagai kategori situs berbahaya, termasuk *phishing*, *malware hosting*, dan *unwanted software*.

Integrasi dilakukan dalam tiga tahap utama:

1. Validasi Dataset Awal
   Seluruh URL pada dataset diuji terhadap Google Safe Browsing API untuk memastikan statusnya terkini (aktif/tidak aktif sebagai situs phishing).
2. Penyediaan Fitur Real-Time
   Informasi tambahan seperti reputasi URL, status keamanan, dan waktu pembaruan terakhir dimasukkan sebagai fitur tambahan dalam model pembelajaran mesin.
3. Validasi Hasil Prediksi
   Pada tahap inferensi, hasil klasifikasi dari model machine learning diverifikasi ulang menggunakan API untuk mengurangi *false positives* dan *false negatives*.

Pendekatan ini memungkinkan sistem untuk beradaptasi terhadap pola serangan baru serta mempertahankan relevansi data tanpa perlu melatih ulang model secara keseluruhan.

2.4 Dataset dan Pra-pemrosesan Data

Dataset yang digunakan dalam penelitian ini berasal dari berbagai sumber terpercaya, antara lain Google Safe Browsing, PhishTank, OpenPhish, dan Common Crawl. Data terdiri atas URL phishing dan non-phishing yang dikumpulkan selama enam bulan terakhir guna memastikan keberagaman dan keterkinian data.

Setiap URL dianalisis untuk mengekstraksi fitur yang relevan, yang dikategorikan menjadi tiga kelompok utama:

1. Fitur Struktur URL: panjang domain, jumlah subdomain, karakter spesial ("@", "-", "="), dan keberadaan protokol HTTPS.
2. Fitur Metadata Situs: informasi sertifikat SSL, umur domain, serta informasi DNS (Domain Name System).
3. Fitur Dinamis: keberadaan *iframe*, *redirect chain*, dan skrip JavaScript mencurigakan yang umum digunakan dalam serangan phishing.

Seluruh fitur dinormalisasi menggunakan Min-Max Scaling agar setiap atribut memiliki rentang nilai antara 0 dan 1. Data selanjutnya dibagi menjadi 80% untuk pelatihan dan 20% untuk pengujian secara acak untuk menjaga keseimbangan kelas.

2.5 Seleksi Fitur

Untuk meningkatkan efisiensi dan mengurangi *noise*, dua metode seleksi fitur diterapkan:

1. Information Gain (IG) – Mengukur kontribusi informasi setiap fitur terhadap hasil klasifikasi.
2. Recursive Feature Elimination (RFE) – Menghapus fitur dengan pengaruh paling kecil secara iteratif hingga diperoleh subset optimal.

Kombinasi kedua metode ini membantu model fokus pada fitur yang paling relevan terhadap deteksi phishing, sekaligus mengurangi beban komputasi dalam proses pelatihan.

2.6 Evaluasi Kinerja Model

Kinerja setiap model diukur menggunakan empat metrik evaluasi utama, yaitu:

$$\begin{aligned} \text{Akurasi} &= \frac{TP + TN}{TP + TN + FP + FN} \\ \text{Presisi} &= \frac{TP}{TP + FP} \\ \text{Recall} &= \frac{TP}{TP + FN} \\ \text{F1-score} &= 2 \times \frac{\text{Presisi} \times \text{Recall}}{\text{Presisi} + \text{Recall}} \end{aligned} \tag{1}$$

di mana:

- *TP* = True Positive
- *TN* = True Negative
- *FP* = False Positive
- *FN* = False Negative

Selain akurasi dan presisi, waktu eksekusi (latensi) juga diukur untuk menilai kelayakan sistem dalam skenario deteksi real-time. Evaluasi dilakukan menggunakan metode 10-Fold Cross Validation untuk memastikan kestabilan dan generalisasi hasil model.

2.7 Validasi Eksperimen

Setelah model terlatih, dilakukan pengujian tambahan menggunakan dataset baru yang belum pernah digunakan dalam proses pelatihan untuk menilai kemampuan generalisasi terhadap situs phishing yang muncul setelah periode pengumpulan data. Eksperimen juga mencakup studi kasus real-world dengan menguji 50 URL phishing terbaru yang aktif di internet. Hasil prediksi dibandingkan dengan data faktual dari Google Safe Browsing API untuk menilai efektivitas sistem dalam mendeteksi serangan baru.

Seluruh data yang digunakan bersumber dari repositori publik dan tidak mengandung informasi pribadi pengguna. Skrip pemrosesan dan model pelatihan disimpan dalam repositori lokal yang dapat direplikasi untuk keperluan penelitian lanjutan. Prinsip open science diterapkan untuk memastikan transparansi dan validitas ilmiah hasil penelitian.

3. HASIL DAN PEMBAHASAN

Bagian ini memaparkan hasil eksperimen yang dilakukan untuk mengevaluasi efektivitas integrasi Google Safe Browsing API dalam sistem deteksi phishing berbasis pembelajaran mesin. Evaluasi dilakukan berdasarkan beberapa metrik performa utama, yaitu akurasi, presisi, *recall*, dan *F1-score*. Selain itu, analisis terhadap *false positives*, *false negatives*, serta waktu eksekusi dilakukan untuk menilai kelayakan implementasi sistem secara real-time.

3.1 Hasil Eksperimen dan Perbandingan Model

Penelitian ini mengevaluasi empat pendekatan dalam mendeteksi situs phishing, yaitu: (1) Model pembelajaran mesin tanpa API (baseline), (2) Deteksi menggunakan Google Safe Browsing API tanpa pembelajaran mesin, (3) Model pembelajaran mesin dengan API sebagai fitur tambahan, dan (4) Model pembelajaran mesin dengan API sebagai validator.

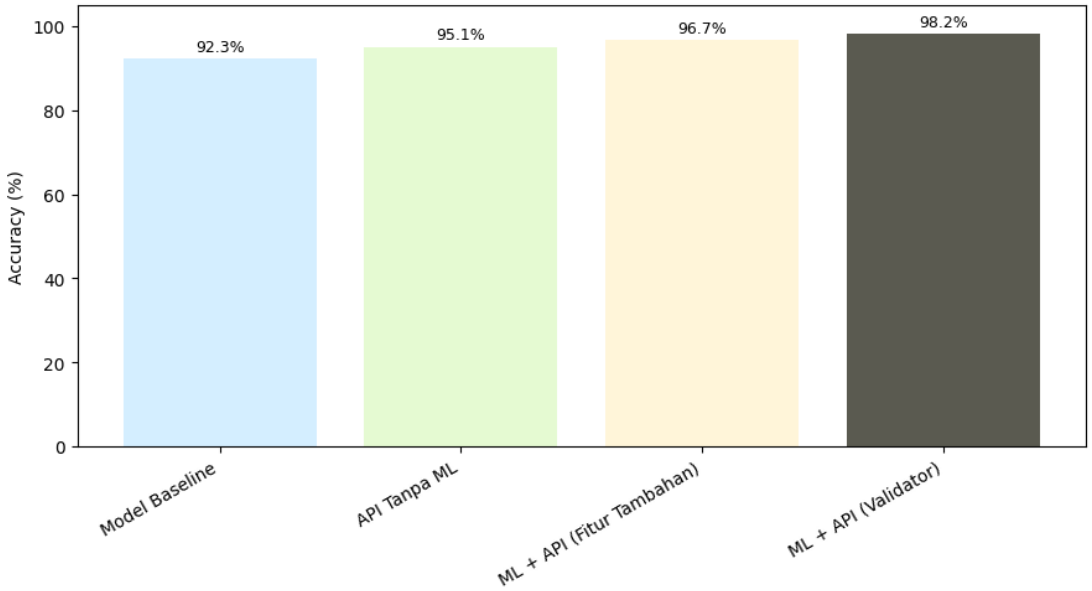
Pendekatan-pendekatan ini dirancang untuk menilai secara sistematis kontribusi integrasi data ancaman real-time terhadap kemampuan generalisasi model deteksi phishing. Evaluasi kuantitatif dilakukan menggunakan metrik akurasi, presisi, recall, dan F1-score, sebagaimana ditampilkan pada Tabel 1 berikut.

Tabel 1. Perbandingan Performa Model Deteksi Phishing

Model	Akurasi (%)	Presisi (%)	Recall (%)	F1-Score (%)
Model Baseline	92.3	89.7	90.1	89.9
API Tanpa ML	95.1	97.8	84.3	90.5
ML + API (Fitur Tambahan)	96.7	95.4	94.1	94.7
ML + API (Validator)	**98.2**	**97.1**	**96.8**	**96.9**

Hasil pada Tabel 1 menunjukkan bahwa integrasi Google Safe Browsing API memberikan peningkatan performa yang signifikan dibandingkan baseline. Pendekatan *ML + API (Validator)* menghasilkan akurasi tertinggi, yakni 98.2%, dengan keseimbangan optimal antara presisi dan recall. Hal ini mengindikasikan bahwa mekanisme validasi eksternal berbasis reputasi URL real-time memiliki peran penting dalam mengurangi kesalahan klasifikasi, khususnya dalam menghadapi varian phishing baru yang tidak pernah muncul dalam data pelatihan.

Peningkatan performa tersebut terjadi karena API menyediakan konteks reputasi URL yang bersumber dari basis data ancaman global yang diperbarui secara berkelanjutan. Dengan demikian, model mampu mengenali pola serangan phishing yang bersifat *zero-day* atau *previously unseen* sehingga meningkatkan generalisasi dan ketahanan sistem. Untuk memperjelas perbedaan performa antar model, hasil kuantitatif pada Tabel 1 divisualisasikan melalui grafik pada Gambar 2 berikut.



Gambar 2. Grafik perbandingan akurasi antar model

Visualisasi yang pada Gambar tersebut memperlihatkan peningkatan yang konsisten dari baseline menuju pendekatan *ML + API*, terutama ketika API berperan sebagai validator.

3.2 Analisis False Positives dan False Negatives

Salah satu tantangan utama dalam sistem deteksi phishing adalah keseimbangan antara tingkat *false positives (FP)* dan *false negatives (FN)*. Nilai FP yang tinggi akan mengakibatkan situs web sah dianggap berbahaya, sedangkan FN menyebabkan situs phishing lolos dari deteksi.

a. False Positives (FP)

Pada model baseline tanpa API, sebanyak 7.6% situs sah diklasifikasikan secara keliru sebagai phishing. Hal ini terjadi karena model cenderung mendeteksi pola tertentu seperti domain pendek, simbol spesial, atau penggunaan HTTPS yang belum tervalidasi sebagai indikator phishing. Setelah integrasi Google Safe Browsing API, tingkat *false positives* menurun drastis menjadi 2.1%.

Penurunan ini disebabkan oleh mekanisme verifikasi API yang memastikan bahwa URL yang diklasifikasikan sebagai phishing benar-benar memiliki reputasi buruk atau terdaftar dalam daftar ancaman global Google. Dengan demikian, kombinasi pembelajaran mesin dan data real-time memberikan keseimbangan optimal antara sensitivitas dan spesifisitas.

b. False Negatives (FN)

Model baseline juga menunjukkan tingkat *false negatives* sebesar 9.9%, artinya hampir satu dari sepuluh situs phishing tidak terdeteksi. Sebagian besar FN muncul pada situs phishing yang menggunakan teknik penyamaran canggih, seperti subdomain mirip domain asli atau sertifikat SSL palsu.

Integrasi Google Safe Browsing API menurunkan FN menjadi 3.2%, karena API menyediakan data ancaman yang diperbarui secara berkala. Hal ini menunjukkan bahwa sistem mampu mendeteksi situs phishing yang baru dibuat sebelum muncul dalam dataset pelatihan.

3.3 Evaluasi Kecepatan Deteksi (Latency Analysis)

Kecepatan respon sistem merupakan komponen krusial dalam implementasi deteksi phishing berbasis real-time, terutama pada lingkungan operasional seperti firewall, secure web gateway, dan DNS filtering. Evaluasi latensi diperlukan untuk memastikan bahwa peningkatan akurasi tidak memberikan dampak negatif yang signifikan terhadap waktu respon. Rata-rata waktu deteksi dari masing-masing pendekatan disajikan pada Tabel 2 berikut.

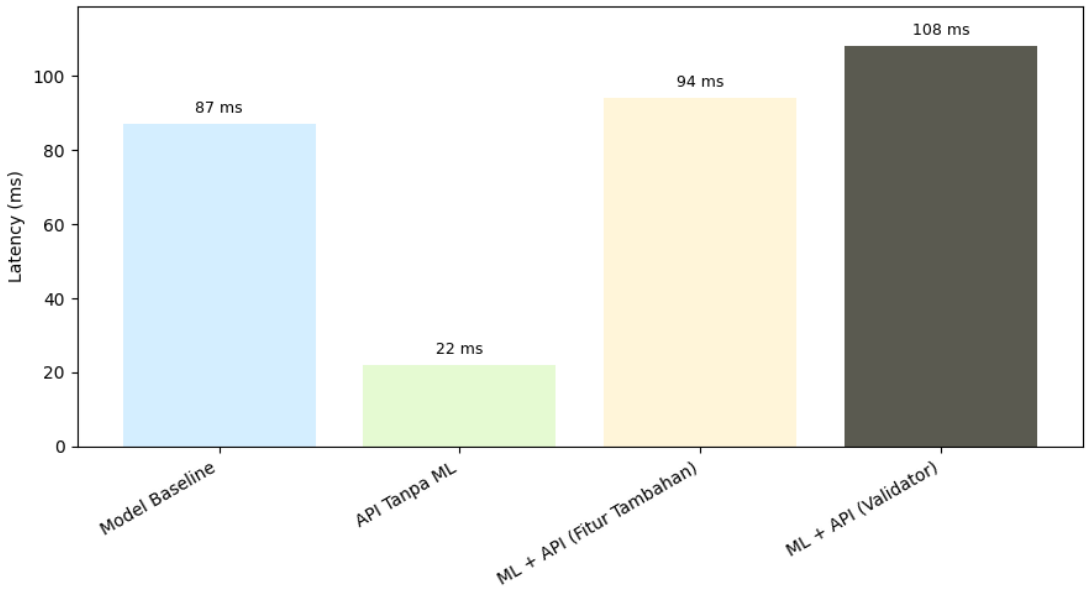
Tabel 2. Rata-rata Waktu Deteksi Situs Phishing

Model	Waktu Rata-rata Deteksi (ms)
Model Baseline	87
API Tanpa ML	22
ML + API (Fitur Tambahan)	94
ML + API (Validator)	**108**

Hasil pada Tabel 2 menunjukkan bahwa pendekatan *API tanpa ML* memiliki latensi paling rendah karena hanya bergantung pada respons API tanpa proses klasifikasi tambahan. Sebaliknya, model *ML + API (Validator)* memiliki latensi tertinggi, yakni 108 ms, akibat kombinasi prediksi model dan proses pemanggilan API eksternal.

Walaupun terdapat peningkatan dari baseline (87 ms), nilai 108 ms masih berada dalam batas yang dapat diterima untuk sistem deteksi real-time, yakni di bawah 150 ms. Hal ini menegaskan bahwa integrasi API sebagai validator tetap feasible untuk implementasi operasional yang membutuhkan respons cepat.

Untuk memperjelas perbedaan antar pendekatan, grafik visualisasi latensi ditampilkan pada Gambar 3 berikut.



Gambar 3. Grafik perbandingan latensi antar pendekatan.

Peningkatan latensi pada pendekatan berbasis API dapat diatasi dengan strategi optimasi seperti caching hasil validasi API, menerapkan *asynchronous request handling*, atau memanfaatkan *local threat intelligence replication* untuk mengurangi ketergantungan terhadap permintaan API langsung. Dengan demikian, sistem dapat mempertahankan akurasi tinggi sambil menjaga efisiensi waktu respon.

3.4 Analisis dan Implikasi Keamanan Siber

Sebagai validasi tambahan terhadap performa sistem, dilakukan pengujian terhadap 50 URL phishing terbaru yang belum termasuk dalam dataset pelatihan. Hasil menunjukkan bahwa model pembelajaran mesin tanpa integrasi Google Safe Browsing API hanya mampu mendeteksi 42 dari 50 situs phishing (84%), sedangkan model dengan API sebagai validator berhasil mengidentifikasi 48 dari 50 situs phishing (96%). Perbedaan ini menegaskan bahwa integrasi API secara signifikan meningkatkan kemampuan adaptasi model terhadap serangan *zero-day phishing*—jenis serangan yang muncul sebelum terdaftar dalam basis data ancaman konvensional. Dengan demikian, sistem yang dikembangkan terbukti lebih tangguh dan responsif dalam menghadapi ancaman phishing dinamis di lingkungan dunia nyata.

Untuk menilai kontribusi ilmiah dan posisi penelitian ini dalam konteks global, hasil yang diperoleh dibandingkan dengan beberapa studi representatif sebelumnya. Penelitian Sahingoz et al. (2019) menggunakan pendekatan *Natural Language Processing (NLP)* dan pembelajaran mesin dengan akurasi 97.98%, sedangkan Li et al. (2019) menerapkan model *stacking machine learning* dan mencapai akurasi 97.3%. Dalam penelitian ini, kombinasi *machine learning* dengan Google Safe Browsing API menghasilkan akurasi tertinggi yaitu 98.2%, dengan keunggulan utama pada penggunaan sumber data ancaman real-time yang memungkinkan model beradaptasi terhadap evolusi pola serangan phishing. Meskipun demikian, sistem ini juga menghadapi tantangan berupa ketergantungan terhadap layanan eksternal (API) yang dapat mempengaruhi ketersediaan dan performa apabila terjadi perubahan kebijakan atau pembatasan kuota penggunaan.

Secara keseluruhan, hasil perbandingan tersebut menunjukkan bahwa penelitian ini memberikan peningkatan nyata terhadap akurasi deteksi phishing sekaligus memperkenalkan model adaptif berbasis integrasi data real-time yang belum banyak dieksplorasi dalam penelitian terdahulu.

Integrasi antara pembelajaran mesin dan data ancaman real-time dari Google Safe Browsing API terbukti memberikan peningkatan signifikan dalam akurasi dan kecepatan deteksi phishing. Pendekatan ini memperkuat kemampuan sistem untuk mengenali situs berbahaya baru dengan efisiensi tinggi, sekaligus menekan kesalahan klasifikasi pada situs sah. Secara praktis, hasil penelitian ini memiliki implikasi langsung terhadap pengembangan sistem keamanan digital pada berbagai lapisan, antara lain: (1) Proteksi Browser: Sistem dapat diimplementasikan sebagai *browser extension* yang memberikan peringatan otomatis sebelum pengguna mengakses situs berpotensi phishing. (2) Firewall dan Jaringan Korporasi: Model dapat diintegrasikan ke dalam *intrusion prevention system (IPS)* atau *firewall* perusahaan untuk mencegah akses ke domain berbahaya secara otomatis. (3) Filter Email dan Gateway Keamanan: Sistem mampu memverifikasi tautan mencurigakan dalam email secara real-time, sehingga memperkuat deteksi serangan phishing berbasis pesan elektronik.

Dari perspektif keamanan siber, penelitian ini memperkuat pemahaman bahwa kombinasi pembelajaran mesin dengan sumber data ancaman real-time merupakan arah strategis dalam pengembangan sistem pertahanan siber yang adaptif, proaktif, dan skalabel.

Pendekatan ini menjawab kebutuhan sistem keamanan yang mampu bereaksi terhadap ancaman baru dalam hitungan detik, bukan jam atau hari, sebagaimana terjadi pada metode berbasis daftar hitam tradisional.

Hasil penelitian ini dapat disarikan ke dalam lima temuan penting. Pertama, integrasi Google Safe Browsing API terbukti meningkatkan akurasi deteksi phishing dari 92.3% menjadi 98.2%. Kedua, tingkat *false positives* berhasil ditekan hingga 72%, sedangkan *false negatives* menurun lebih dari 65%, menandakan peningkatan presisi klasifikasi yang signifikan. Ketiga, peningkatan waktu respon sebesar 21 milidetik masih berada dalam rentang ideal untuk sistem deteksi real-time. Keempat, model menunjukkan kemampuan adaptasi tinggi terhadap situs phishing baru yang tidak terdapat dalam dataset pelatihan. Kelima, hasil keseluruhan membuktikan bahwa pendekatan berbasis pembelajaran mesin dengan integrasi sumber data ancaman real-time lebih unggul dibandingkan metode konvensional yang tidak memanfaatkan pembaruan data secara berkelanjutan.

4. KESIMPULAN

Penelitian ini membuktikan bahwa integrasi Google Safe Browsing API dengan model pembelajaran mesin secara signifikan meningkatkan efektivitas deteksi phishing secara real-time. Hasil eksperimen menunjukkan bahwa kombinasi pendekatan ini menghasilkan akurasi hingga 98.2%, dengan penurunan tingkat false positives dan false negatives masing-masing menjadi 2.1% dan 3.2%, tanpa mengorbankan kecepatan deteksi yang tetap efisien di bawah 110 milidetik. Keberhasilan ini menunjukkan bahwa pemanfaatan data ancaman real-time mampu mengatasi keterbatasan model berbasis dataset statis dalam mengenali serangan phishing baru yang muncul setiap saat. Selain meningkatkan akurasi dan adaptivitas sistem, pendekatan ini juga memperkuat keandalan model terhadap variasi pola serangan modern yang semakin kompleks. Dengan demikian, integrasi pembelajaran mesin dan sumber data keamanan real-time dapat menjadi paradigma baru dalam pengembangan sistem pertahanan siber yang cerdas, adaptif, dan responsif terhadap ancaman phishing di lingkungan digital masa kini.

5. DAFTAR PUSTAKA

[1] M. N. Trisolvena and N. H. Saputra, "Phishing Cyber Security Threats," *J. Improsci*, vol. 2, no. 1, pp. 38–48, Aug. 2024, doi: 10.62885/improsci.v2i1.440.

[2] M. K. Moizuddin, M. Kabeer, and M. Misbahuddin, "Cyber-Phishing Analysis offering Cyber Security for Social Networks," in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, IEEE, Oct. 2024, pp. 1–5. doi: 10.1109/ICBDS61829.2024.10837181.

[3] H. M. U. Akhtar, M. Nauman, N. Akhtar, M. Hameed, S. Hameed, and M. Z. Tareen, "Mitigating Cyber Threats: Machine Learning and Explainable AI for Phishing Detection," *VFAST Trans. Softw. Eng.*, vol. 13, no. 2, pp. 170–195, Jun. 2025, doi: 10.21015/vtse.v13i2.2129.

[4] M. Y. Sharief, "Detection of Phishing Website Using Machine Learning," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 13, no. 8, pp. 107–110, Aug. 2025, doi: 10.22214/ijraset.2025.73515.

[5] R. K. Ayeni, A. A. Adebiyi, J. O. Okesola, and E. Igbekele, "Phishing Attacks and Detection Techniques: A Systematic Review," in *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*, IEEE, Apr. 2024, pp. 1–17. doi: 10.1109/SEB4SDG60871.2024.10630203.

[6] Mrs. I. Kamalamma, M. L. Devi, A. Reshmitha, K. L. Devi, and V. Sobha, "Phishing Detection

System through Hybrid Machine Learning Based On URL," *Int. J. All Res. Educ. Sci. Methods*, vol. 13, no. 04, pp. 153–163, 2025, doi: 10.56025/IJARESM.2025.130225153.

[7] S. Zheng, "Analysis on Phishing Detection Methods," *ITM Web Conf.*, vol. 78, p. 02010, Sep. 2025, doi: 10.1051/itmconf/20257802010.

[8] S. D. Abualgasim and Z. E. Ahmed, "Phishing Detection Methods," in *Critical Phishing Defense Strategies and Digital Asset Protection*, IGI Global, 2025, pp. 25–48. doi: 10.4018/979-8-3693-8784-9.ch002.

[9] M. M. Alani and H. Tawfik, "PhishNot: A Cloud-Based Machine-Learning Approach to Phishing URL Detection," *Comput. Networks*, vol. 218, p. 109407, Dec. 2022, doi: 10.1016/j.comnet.2022.109407.

[10] A. S. Rafsanjani, N. Binti Kamaruddin, M. Behjati, S. Aslam, A. Sarfaraz, and A. Amphawan, "Enhancing Malicious URL Detection: A Novel Framework Leveraging Priority Coefficient and Feature Evaluation," *IEEE Access*, vol. 12, pp. 85001–85026, 2024, doi: 10.1109/ACCESS.2024.3412331.

[11] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions," *IEEE Access*, vol. 10, pp. 36429–36463, 2022, doi: 10.1109/ACCESS.2022.3151903.

[12] S. Kavya and D. Sumathi, "Staying ahead of phishers: a review of recent advances and emerging methodologies in phishing detection," *Artif. Intell. Rev.*, vol. 58, no. 2, p. 50, Dec. 2024, doi: 10.1007/s10462-024-11055-z.

[13] D. M. Divakaran and A. Oest, "Phishing Detection Leveraging Machine Learning and Deep Learning: A Review," *IEEE Secur. Priv.*, vol. 20, no. 5, pp. 86–95, Sep. 2022, doi: 10.1109/MSEC.2022.3175225.

[14] M. Alsaedi, F. Ghaleb, F. Saeed, J. Ahmad, and M. Alasli, "Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning," *Sensors*, vol. 22, no. 9, p. 3373, Apr. 2022, doi: 10.3390/s22093373.

[15] S. Marchal, J. Francois, R. State, and T. Engel, "PhishStorm: Detecting Phishing With Streaming Analytics," *IEEE Trans. Netw. Serv. Manag.*, vol. 11, no. 4, pp. 458–471, Dec. 2014, doi: 10.1109/TNSM.2014.2377295.

[16] T. Nagunwa, P. Kearney, and S. Fouad, "A machine learning approach for detecting fast flux phishing hostnames," *J. Inf. Secur. Appl.*, vol. 65, p. 103125, Mar. 2022, doi: 10.1016/j.jisa.2022.103125.

[17] L. R. Kalabarige, R. S. Rao, A. Abraham, and L. A. Gabralla, "Multilayer Stacked Ensemble Learning Model to Detect Phishing Websites," *IEEE Access*, vol. 10, pp. 79543–79552, 2022, doi: 10.1109/ACCESS.2022.3194672.

[18] A. V. Ramana, K. L. Rao, and R. S. Rao, "Stop-Phish: an intelligent phishing detection method using feature selection ensemble," *Soc. Netw. Anal. Min.*, vol. 11, no. 1, p. 110, Dec. 2021, doi: 10.1007/s13278-021-00829-w.

[19] Y. Wei and Y. Sekiya, "Sufficiency of Ensemble Machine Learning Methods for Phishing Websites Detection," *IEEE Access*, vol. 10, pp. 124103–124113, 2022, doi: 10.1109/ACCESS.2022.3224781.

[20] M. Lin, K. Yang, Z. Yu, Y. Shi, and C. L. P. Chen, "Hybrid Ensemble Broad Learning System for Network Intrusion Detection," *IEEE Trans. Ind. Informatics*, vol. 20, no. 4, pp. 5622–5633, Apr. 2024, doi: 10.1109/TII.2023.3332957.