BAB 1
PENDAHULUAN

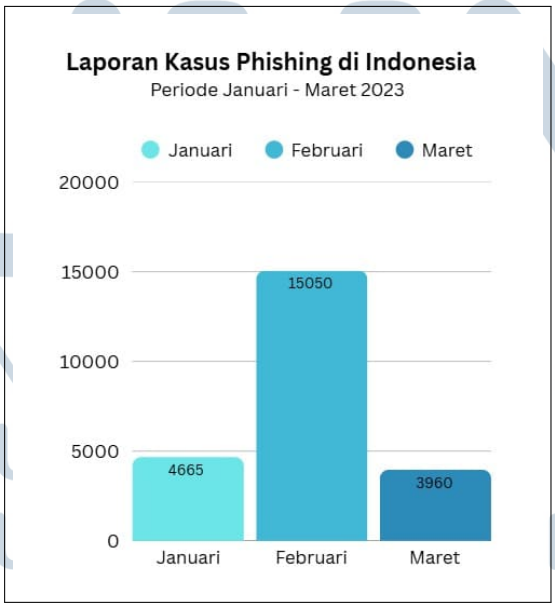
1.1 Latar Belakang Masalah

Perkembangan era digital dan modern ditandai oleh percepatan serta perkembangan inovasi yang eksponensial dalam bidang Teknologi Informasi dan Komunikasi (TIK). Teknologi Informasi (TI) merupakan suatu bidang yang berkaitan dengan perangkat canggih dan penggunaan komputer, perangkat keras, perangkat lunak, jaringan, serta infrastruktur digital lainnya [1]. Tugas dari perangkat tersebut adalah untuk mengelola, menyimpan, memproses dan menyebarkan informasi dalam berbagai bentuk, baik teks, gambar, suara, maupun video [2]. TI berperan penting dalam berbagai aspek kehidupan pada bisnis, pemerintah, pendidikan, kesehatan, layanan perbankan, hingga hiburan. Salah satu perubahan signifikan dari adanya revolusi internet adalah halaman website [3]. Website merupakan sekumpulan halaman yang berfungsi menampilkan beragam jenis konten, baik dalam bentuk teks, gambar, suara, animasi, video, maupun perpaduan dari semuanya, dengan karakteristik statis atau dinamis [4]. Dengan kemampuannya menyajikan informasi yang efisien dan terbaru, website menjadi Solusi praktis bagi masyarakat di berbagai daerah untuk mendapatkan akses informasi hanya dengan internet [5]. Meningkatnya pengguna website yang semakin luas, website juga menjadi target utama yang celahnya sering dimanfaatkan oleh pelaku kejahatan siber, terutama untuk melancarkan serangan phishing [6].

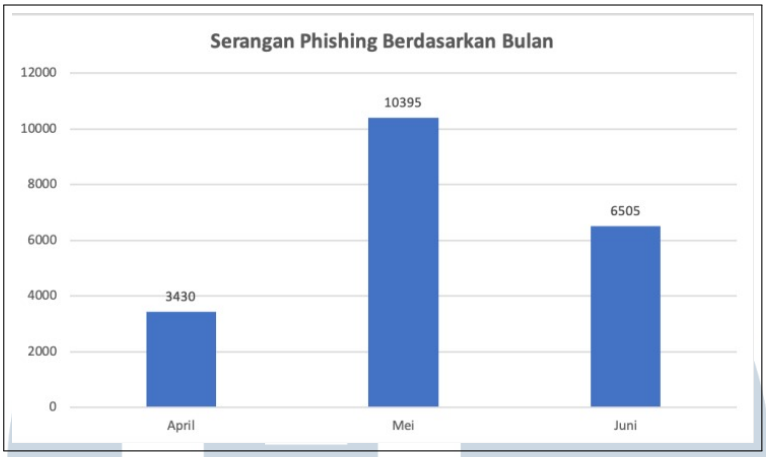
Phishing merupakan tindakan kejahatan siber yang menggunakan teknik rekayasa sosial (*social engineering*) untuk mendapatkan informasi berharga secara tidak sah. Pelaku phishing (*phiser*) membuat situs web atau mengirim email palsu (*fake email*) yang meyakinkan, agar korban terdorong untuk memasukkan data pribadi dan finansial mereka, mulai dari kata sandi akun hingga informasi kartu kredit [7]. Situs *Phishing* merupakan website tiruan yang sengaja direkayasa untuk menyerupai antarmuka sebuah situs terpercaya dan berakreditasi tinggi [8]. Dengan memalsukan elemen seperti tampilan, konten, dan URL, situs ini dirancang untuk mengelabuhi korban agar meyakini bahwa mereka sedang berinteraksi dengan entitas yang sah [9]. Teknik tersebut dieksekusi dengan cara menyisipkan sebuah script atau memanipulasi protokol HTTPS pada website yang digunakan oleh phiser. Protokol HTTPS pada dasarnya sangat aman karena mengenkripsi semua

data menggunakan algoritma kuat. Reputasi keamanan inilah yang disalahgunakan oleh phiser dengan sengaja memasang protokol HTTPS pada situs *phishing* untuk mengelabuhi korban [10].

Laporan *Kaspersky Security Network* pada tahun 2021 bahwa serangan *phishing* telah menjadi ancaman keamanan siber utama di Indonesia. Terdapat sekitar 1,6 juta serangan *phishing* yang terdeteksi selama periode kuartal keempat 2020 [11]. Angka ini menunjukkan bahwa *phishing* merupakan salah satu ancaman siber paling dominan di dunia, melampaui jenis serangan lain seperti malware tradisional. Berdasarkan diagram batang Laporan Kasus Phishing di Indonesia IDADX mencatatkan pada periode kuartal pertama tahun 2023 jumlah *phishing* di Indonesia mencapai 23.675 kasus dan organisasi yang menjadi sasaran adalah *facebook* dengan jumlah 207 serangan. Pada bulan Januari meliputi 4.665 serangan, bulan Februari menepatkan angka paling banyak berjumlah 15.050 serangan, serta pada bulan maret sebanyak 3.960 serangan. Dilanjutkan pada kuartal kedua 2023 sebanyak 20.330, dimana mengalami penurunan sebanyak 3.345 laporan *phishing* dari kuartal pertama 2023. Indonesia tercatat sebagai lokasi utama yang paling banyak menjadi tuan rumah bagi domain .id yang disalahgunakan, disusul Amerika Serikat di peringkat kedua. Sebuah tren yang juga teramati pada kuartal ini adalah meningkatnya keragaman negara yang dimanfaatkan sebagai *host*, menunjukkan sebaran geografis yang lebih luas dibandingkan dengan periode sebelumnya [12].



Gambar 1.1. Diagram Batang Kasus *Phishing* di Indonesia pada kuartal pertama.
Sumber: Indonesia Anti-Phishing Data Exchage (IDADX)



Gambar 1.2. Diagram Batang Kasus Phishing di Indonesia pada kuartal kedua.
Sumber: Indonesia Anti-Phishing Data Exchage (IDADX)

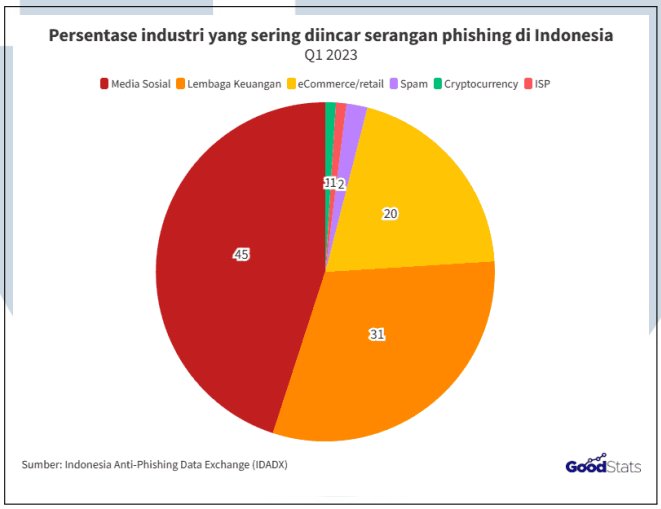
Peningkatan kasus *phishing* di Indonesia sangat dipengaruhi oleh faktor ketidaktelitian pengguna, rendahnya tingkat literasi digital, dan kurangnya kebiasaan riset sebuah informasi sebelum bertindak. Jenis serangan yang paling umum memanfaatkan kelemahan ini adalah situs judi online, investasi bodong, undangan pernikahan, pembayaran pajak, dan pinjaman online, yang sering kali memanipulasi URL dan *SSL Certificate* kode keamanan yang seharusnya membangun kepercayaan untuk menjerat korbannya [13]. Oleh karena itu, dibutuhkan pendekatan yang lebih adaptif melalui *machine learning*, yang mampu menganalisis pola teknis pada URL untuk mendeteksi anomali secara otomatis. Penetapan penelitian deteksi URL phishing berbasis karakteristik URL dilakukan karena serangan berbasis *social engineering* semakin meningkat dan terus berevolusi. Permasalahan utama yang menjadi fokus penelitian ini adalah tingginya tingkat keberhasilan penipuan digital yang disebabkan oleh ketidakmampuan pengguna awam dalam membedakan entitas asli dan palsu secara visual, sehingga diperlukan sebuah sistem otomatis yang mampu memberikan peringatan seketika sebelum data sensitif terlanjur dimasukkan ke dalam situs berbahaya tersebut. Dalam mendeteksi situs berbahaya, terdapat beberapa pendekatan utama seperti analisis berbasis konten (teks dan gambar pada halaman web), analisis identitas sertifikat digital, hingga penggunaan daftar hitam (*blacklist*) URL yang sudah dilaporkan. Namun, metode berbasis konten memerlukan waktu komputasi yang tinggi dan akses penuh ke server, sementara daftar hitam sering kali gagal mendeteksi situs phishing baru yang hanya aktif dalam hitungan jam (*zero-day phishing*). Oleh karena itu, penelitian ini memilih pendekatan karakteristik URL

(*lexical feature*) karena metode ini lebih efisien secara komputasi, dapat dilakukan secara *real-time* tanpa harus mengunduh seluruh konten halaman web, dan mampu mengidentifikasi pola anomali pada struktur alamat web yang sengaja disamarkan oleh pelaku kejahatan.

Penelitian ini bertujuan untuk menguji dan membuktikan efektivitas serta akurasi algoritma *Decision Tree* dan Random Forest dalam membangun model deteksi situs *URL phishing* berdasarkan karakteristik URL (*lexical feature*) yang akurat. Dimulai dengan menguji algoritma *Decision Tree* (DT) sebagai model *baseline* yang memiliki keunggulan karena kesederhanaan dalam interpretasi suatu klasifikasi. Namun, DT tunggal rentan mengalami *overfitting* pada dataset dengan fitur yang kompleks yang dapat menurunkan tingkat akurasi pada data baru. Sehingga sebagai antisipasi maka diterapkan algoritma *Random Forest* (RF) yang merupakan metode *ensemble learning* berbasis *Decision Tree* (DT) yang akan diuji dan dibuktikan efektifitas algoritma tersebut. Analisis akan difokuskan pada fitur-fitur kunci yang sering menjadi indikator *phishing* yaitu struktur dan karakteristik URL (*lexical-based features*). Karakteristik URL dapat dijadikan dasar untuk melakukan klasifikasi apakah sebuah website termasuk *Phishing* atau *Legitimate* dengan menggunakan metode evaluasi berupa *Recall*, *Accuracy*, *Precision*, dan *F1 Score*. Algoritma *Random Forest* dipilih karena merupakan metode *ensemble* yang menggabungkan banyak *decision tree* untuk meningkatkan akurasi dan stabilitas prediksi pada data berdimensi banyak seperti karakteristik URL dengan melakukan kalkulasi nilai setiap fitur karakter URL.

Breiman menjelaskan bahwa hasil teoritis *Random Forest* menunjukkan alasan mengapa model ini tidak mudah mengalami *overfitting* ketika jumlah pohon ditambah, yaitu "*This result explains why random forests do not overfit as more trees are added, but produce a limiting value of the generalization error*" yang memiliki arti "Hasil ini menjelaskan mengapa *Random Forest* tidak mengalami overfitting seiring bertambahnya jumlah pohon, melainkan menghasilkan nilai batas pada kesalahan generalisasi" [14]. Selain itu, pada konteks deteksi URL *phishing*, penelitian komparatif menyatakan bahwa *Random Forest* memiliki performa yang konsisten dan reliabel, yaitu "*Using ensemble learning, the random forest demonstrated superior accuracy and reliability compared to traditional methods*" yang memiliki arti "Dengan menggunakan *ensemble learning* (pembelajaran ansambel), *Random Forest* menunjukkan akurasi dan keandalan yang lebih unggul dibandingkan dengan metode-metode tradisional" [15]. Dengan demikian, Random Forest sesuai digunakan sebagai model utama untuk klasifikasi URL *phishing*

karena *robust* terhadap variasi pola URL dan mampu memberikan wawasan melalui analisis kontribusi fitur (*feature importance*). Pengembangan sistem deteksi *phishing* menggunakan dataset berupa Kaggle untuk menjadi basis pelatihan dan pengujian algoritma *Random Forest*. Dengan demikian, hasil penelitian ini diharapkan dapat memberikan kontribusi praktis berupa model klasifikasi *Random Forest* yang andal untuk meningkatkan keamanan siber dan mengurangi risiko serangan *phishing* bagi pengguna internet.



Gambar 1.3. Diagram *Pie Chart* Target Industri Serangan Phishing.
Sumber: Indonesia Anti-Phishing Data Exchage (IDADX)

Diagram *Pie Chart* Target Industri Serangan Phishing 1.3 menggambarkan persentasi industri yang menjadi sasaran serangan *phishing* di Indonesia pada kuartal pertama 2023. Media sosial tercatat sebagai industri yang paling banyak menjadi sasaran serangan *phishing* di Indonesia dengan persentase mencapai 45%. Tingginya angka ini disebabkan oleh karakteristik media sosial yang bersifat terbuka, interaktif, serta melibatkan jutaan pengguna aktif yang sering membagikan informasi tanpa disadari, sehingga dimanfaatkan oleh pelaku kejahatan siber untuk melakukan manipulasi dan pencurian data. Selain media sosial, sektor lembaga keuangan menempati posisi kedua dengan persentase sebesar 31%, diikuti oleh sektor *e-commerce* dan ritel sebesar 20%. Industri yang berkaitan langsung dengan sektor keuangan transaksi finansial menjadi target utama serangan *phishing* yang dapat menciptakan kerugian ekonomi. Disisi lain, sektor lain seperti *spam*, *cryptocurrency*, dan penyedia layanan internet memiliki persentase lebih kecil, namun tetap tidak boleh diabaikan ancaman yang mungkin terjadi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana proses deteksi dan klasifikasi suatu URL yang tergolong *phishing* dan *legitimate* dengan memanfaatkan analisis karakteristik URL menggunakan pendekatan *supervised machine learning* serta pengaruh seleksi fitur terhadap kinerja model?
2. Bagaimana perbandingan kinerja algoritma Decision Tree (CART) dan Random Forest sebagai metode *ensemble learning* dalam mendeteksi dan mengklasifikasikan URL *phishing* dan *legitimate*?
3. Bagaimana mengukur tingkat akurasi, *recall*, *precision*, *F1-score*, serta melakukan evaluasi kinerja model Random Forest sebagai model utama dalam membedakan website *phishing* dan *legitimate* sehingga dapat diketahui efektivitas metode yang digunakan?

1.3 Batasan Permasalahan

Ruang lingkup penelitian ini dibatasi pada beberapa hal, di antaranya:

1. Topik Penelitian

   Penelitian ini berfokus pada penerapan algoritma *ensemble learning Random Forest* sebagai model utama dan menggunakan *Decision Tree* (CART) sebagai model *baseline* pembanding. Perbandingan dan pembahasan terbatas hanya pada kedua algoritma tersebut. Penelitian tidak membahas atau membandingkan dengan algoritma klasifikasi lain seperti KNN, maupun SVM yang lebih canggih.

2. Objek Penelitian

   Objek penelitian terbatas pada URL website, yang dikelompokkan ke dalam dua kategori yaitu *Phishing* Website (URL berbahaya) dan *Legitimate* Website (URL sah).

3. Dataset yang Digunakan

   Dataset yang akan digunakan untuk mendukung proses pembelajaran mesin bersumber dari Kaggle Dataset dimiliki oleh Shashwat Tiwari (*Web Page*

Phishing Detection Dataset) yang terdiri dari 11.430 URL terbagi dalam 50% *Phishing* dan 50% *Legitimate*.

4. Lingkup Penelitian

   Implementasi penelitian hanya sampai pada tahap perbandingan antara algoritma *Random Forest* dan *Decision Tree*, serta sebuah sistem sederhana yang dapat menerima input URL dan memberikan hasil klasifikasi berupa *phishing* atau *legitimate* menggunakan algoritma Random Forest. Penelitian tidak mencakup integrasi dengan *browser extension*, aplikasi mobile, ataupun sistem keamanan jaringan skala besar yang kompleks.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Pengembangan proses deteksi dan klasifikasi URL yang tergolong *phishing* dan *legitimate* dengan memanfaatkan analisis karakteristik URL menggunakan pendekatan *supervised machine learning*, serta analisis pengaruh seleksi fitur terhadap kinerja model klasifikasi yang dibangun.
2. Perbandingan kinerja algoritma *Decision Tree* (CART) dan *Random Forest* sebagai metode *ensemble learning* dalam mendeteksi dan mengklasifikasikan URL *phishing* dan *legitimate* berdasarkan karakteristik URL.
3. Pengukuran dan evaluasi kinerja model *Random Forest* sebagai model utama dalam mendeteksi URL *phishing* dan *legitimate* dengan menggunakan metrik evaluasi *confusion matrix* seperti *accuracy*, *precision*, *recall*, dan *F1-score* untuk mengetahui tingkat efektivitas metode yang digunakan.

1.5 Manfaat Penelitian

Berdasarkan Tujuan Penelitian, manfaat dari penelitian ini berupa:

1. Manfaat Teoritis (Akademik)
   a. Membuktikan bahwa penerapan algoritma *ensemble Random Forest* efektif dalam klasifikasi dan mendeteksi serangan URL *phishing*.

b. Menjadi referensi kuat terhadap penelitian selanjutnya dalam pengembangan model deteksi phishing berbasis *Machine Learning* dengan algoritma lain atau dataset yang lebih kompleks.

c. Memperluas pengetahuan dan literatur akademik dalam bidang keamanan siber dan *machine learning*.

2. Manfaat Praktis (Kehidupan sehari-hari)

a. Meningkatkan kesadaran dan kewaspadaan pengguna internet dalam aktivitas digital sehari-hari melalui sistem deteksi *phishing* berbasis analisis karakteristik URL. Hasil penelitian ini diharapkan dapat membantu pengguna dalam memahami ciri-ciri URL yang berpotensi berbahaya, membangun perilaku penggunaan internet yang lebih aman, serta menjadi referensi dalam pengembangan sistem keamanan informasi untuk mendukung lingkungan digital yang lebih aman dalam kehidupan sehari-hari.

b. Bagi penulis, penelitian ini bermanfaat untuk melatih kemampuan dalam mengimplementasikan teori *machine learning* terutama random forest yang telah dipelajari dalam perkuliahan ke praktik nyata serta menambah pengalaman di bidang keamanan siber (*cyber security*) serta dapat memberi manfaat bagi seluruh kalangan masyarakat agar terhindar dari tindakan kejahatan *phishing*.

1.6 Sistematika Penulisan

Bab ini menjelaskan secara ringkas struktur dan isi laporan penelitian yang disusun secara sistematis mulai dari pendahuluan hingga penarikan kesimpulan dan saran. Adapun sistematika penulisan laporan penelitian ini adalah sebagai berikut:

- Bab I PENDAHULUAN
  Bab ini berisi pendahuluan yang meliputi latar belakang penelitian, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, serta sistematika penulisan laporan. Bab ini memberikan gambaran umum mengenai permasalahan phishing website dan urgensi penerapan metode deteksi berbasis karakteristik URL.

- Bab II LANDASAN TEORI
  Bab ini membahas landasan teori dan tinjauan pustaka yang mendukung

penelitian. Pembahasan mencakup konsep dasar keamanan informasi, phishing website, karakteristik URL, metode ekstraksi fitur URL-based dan external-based, algoritma Decision Tree dan Random Forest, serta penelitian-penelitian terdahulu yang relevan sebagai pembanding dan dasar pengembangan metode yang digunakan.

- Bab III METODOLOGI PENELITIAN
  Bab ini menjelaskan metodologi penelitian yang digunakan. Pembahasan meliputi tahapan pengumpulan dataset, proses preprocessing data, ekstraksi dan seleksi fitur, pembagian data latih dan data uji, perancangan sistem deteksi phishing berbasis URL, serta metode evaluasi performa model menggunakan metrik seperti akurasi, precision, recall, dan F1-score.

- Bab IV HASIL DAN DISKUSI
  Bab ini menyajikan hasil implementasi sistem dan pembahasan hasil penelitian. Pembahasan mencakup hasil pelatihan dan pengujian model Decision Tree dan Random Forest, analisis performa model berdasarkan confusion matrix dan metrik evaluasi, perbandingan hasil kedua algoritma, serta analisis kasus khusus seperti false positive dan false negative dalam deteksi phishing berbasis karakteristik URL.

- Bab V KESIMPULAN DAN SARAN
  Bab ini berisi kesimpulan yang diperoleh dari hasil penelitian dan pembahasan yang telah dilakukan. Selain itu, bab ini juga menyajikan saran untuk pengembangan penelitian selanjutnya, khususnya dalam peningkatan akurasi sistem deteksi phishing dan pengembangan fitur tambahan di luar karakteristik URL yang lebih canggih dengan menerapkan algoritma dan metode lain.