BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet telah menjadi aspek fundamental dalam kehidupan modern karena mampu menghubungkan individu dan organisasi dalam berbagai aktivitas kehidupan. Berdasarkan data dari Data Reportal Jumlah pengguna internet global mencapai 5.35 miliar orang pada Januari 2024, atau 66,2% dari populasi dunia, Angka ini meningkat 1,8% dari tahun sebelumnya, dengan 97 juta pengguna baru [1]. Di Indonesia sendiri menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah penduduk Indonesia yang menggunakan internet pada tahun 2024 mencapai 221.563.479 jiwa, dari total populasi 278.696.200 jiwa pada tahun 2023, menurut survei penetrasi internet APJII pada tahun 2024, tingkat penetrasi internet Indonesia mencapai 79,5%, meningkat 1,4% dibandingkan dengan periode sebelumnya [2]. Perkembangan ini telah mengubah cara manusia berkomunikasi, berbelanja, bekerja, dan berinteraksi secara umum. Banyak sektor tradisional mulai beralih dari layanan offline ke platform *online* seperti ritel dan katering. Namun, seiring dengan meningkatnya layanan digital, muncul pula risiko penyalahgunaan data pengguna seperti nama pengguna, nama akun, kata sandi, pertanyaan privasi, informasi pribadi, dan nomor kartu kredit oleh pihak-pihak yang tidak bertanggung jawab [3].

Seiring pesatnya penggunaan internet, kejahatan siber menjadi ancaman yang nyata, metode dan bentuk serangan mereka juga terus berubah dengan cepat. Serangan siber yang paling umum terjadi terhadap pengguna internet adalah serangan *phishing*. *Phishing* adalah serangan jaringan yang memanfaatkan teknologi komputer dan rekayasa sosial untuk mencuri informasi pribadi pengguna. Dalam praktiknya, pelaku *phishing* mengirimkan tautan berbahaya melalui email, sms, atau media sosial yang tampak seolah sah, padahal bertujuan untuk menipu pengguna agar memberikan data sensitif [4]. Informasi yang dicuri dapat berupa nama pengguna, kata sandi, nomor kartu kredit, hingga data privasi lainnya. Dampak dari serangan ini tidak hanya berupa kerugian finansial, tetapi juga

menyebabkan hilangnya kepercayaan terhadap layanan *online*. Selain itu, perusahaan dan organisasi yang ditiru mengalami penyalahgunaan nama baik dan reputasi, bahkan pelanggaran data yang merugikan [5].

Skala serangan *phishing* yang terjadi di Indonesia menunjukkan bahwa masalah ini perlu mendapat perhatian serius dari berbagai pihak. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), pada tahun 2023 terdapat sebanyak 47.231.390 serangan *phishing* yang tercatat [6]. Angka ini menggambarkan betapa masif dan sistematisnya serangan yang dilakukan oleh pelaku kejahatan siber. Oleh karena itu, upaya untuk mendeteksi dan mencegah *phishing* perlu melibatkan pendekatan teknologi yang adaptif, salah satunya adalah dengan menggunakan *machine learning*. Teknologi ini memungkinkan sistem untuk mempelajari pola-pola dari data historis dan mengenali situs web *phishing* secara otomatis. Pendekatan *machine learning* diyakini dapat meningkatkan efektivitas deteksi serangan *phishing* yang semakin canggih dan sulit dikenali secara manual.

Penelitian ini mengusulkan penggunaan algoritma *machine learning* untuk mendeteksi situs web *phishing* melalui metode klasifikasi. Tiga algoritma yang digunakan dalam penelitian ini adalah *Support Vector Machine* (SVM), *Random Forest*, dan *Naive Bayes*. Tujuan utama dari penelitian ini adalah untuk mengevaluasi dan membandingkan performa ketiga algoritma tersebut dalam mendeteksi situs *phishing*. Evaluasi dilakukan menggunakan metrik seperti *accuracy*, *precision*, *recall*, *F1-score*, dan *confusion matrix* untuk menilai keakuratan serta efisiensi masing-masing metode. Dengan membandingkan hasil dari ketiga algoritma tersebut, diharapkan dapat diperoleh metode terbaik yang paling efektif untuk mendeteksi *phishing*. Hasil penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan sistem keamanan berbasis *machine learning* dalam menghadapi ancaman *phishing* secara lebih akurat dan efisien.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, terdapat beberapa permasalahan yang perlu diteliti lebih lanjut agar tujuan dari penelitian ini dapat tercapai secara optimal. Permasalahan utama dalam penelitian ini adalah sebagai berikut:

1. Bagaimana kinerja algoritma *Support Vector Machine*, *Random Forest*, dan *Naive Bayes* dalam mendeteksi situs *phishing* berbasis URL?
2. Algoritma manakah di antara *Support Vector Machine*, *Random Forest*, dan *Naive Bayes* yang menghasilkan performa terbaik berdasarkan metrik evaluasi *accuracy*, *precision*, *recall*, *F1-score*, dan *confusion matrix*?

1.3 Batasan Masalah

Penelitian ini memiliki sejumlah batasan yang perlu diperhatikan secara seksama, guna memberikan pemahaman yang komprehensif mengenai ruang lingkup, keterbatasan metodologis, serta faktor-faktor yang mungkin memengaruhi validitas dan generalisasi hasil yang diperoleh. Penjelasan mengenai batasan-batasan tersebut disampaikan sebagai berikut:

1. Penelitian ini hanya difokuskan pada perbandingan performa tiga algoritma klasifikasi, yaitu *Support Vector Machine*, *Random Forest*, dan *Naive Bayes*, dalam mendeteksi *website phishing*.
2. Penelitian ini menggunakan *dataset* publik yang tersedia secara daring, sehingga hasil penelitian bergantung pada kualitas dan cakupan *dataset* tersebut.
3. Evaluasi algoritma dilakukan berdasarkan metrik *accuracy*, *precision*, *recall*, *F1-score*, dan *confusion matrix* tanpa mempertimbangkan aspek waktu komputasi secara mendalam.

1.4 Tujuan Penelitian

Merujuk pada rumusan masalah yang telah dijelaskan sebelumnya, penelitian ini bertujuan untuk menjawab permasalahan tersebut. Tujuan spesifik dari penelitian ini adalah sebagai berikut::

1. Melakukan analisis terhadap performa masing-masing algoritma dengan menggunakan metrik evaluasi berupa *accuracy*, *precision*, *recall*, *F1-score*, dan *confusion matrix*.
2. Menentukan algoritma klasifikasi yang memiliki tingkat akurasi dan efektivitas terbaik dari tiga algoritma, yaitu *Support Vector Machine*, *Random Forest*, dan *Naive Bayes*, dalam proses deteksi situs *phishing*.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dapat diperoleh dari penelitian ini mencakup kontribusi penting baik secara teoritis maupun praktis, yang secara lengkap dijelaskan sebagai berikut:

1. Penelitian ini diharapkan memberikan kontribusi terhadap perkembangan ilmu pengetahuan, khususnya dalam bidang pembelajaran mesin yang berkaitan dengan keamanan siber dan deteksi situs *phishing*.
2. Penelitian ini diharapkan dapat mendukung pengembangan alat bantu otomatis yang mampu mengenali dan memblokir situs *phishing* secara *real-time* dengan memanfaatkan algoritma *machine learning* yang telah dievaluasi performanya,

1.6 Sistematika Penulisan

Untuk memudahkan pemahaman isi penelitian, skripsi ini disusun secara sistematis dalam beberapa bab yang saling berkaitan. Adapun sistematika penulisan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini memuat studi literatur dari penelitian-penelitian sebelumnya dan membahas teori-teori yang mendasari penelitian, termasuk konsep dasar mengenai internet, *phishing*, *machine learning*, dan algoritma yang digunakan dalam penelitian ini.

BAB III METODE PENELITIAN

Bab ini menjelaskan metode yang digunakan dalam penelitian, mulai dari objek penelitian, tahapan penelitian, pengumpulan dan *preprocessing* data, pemilihan algoritma, hingga evaluasi model.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil evaluasi model menggunakan *confusion matrix* dan metrik evaluasi lainnya, serta pembahasan perbandingan performa masing-masing algoritma.

BAB V PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya agar dapat dikembangkan lebih baik.