BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Transformasi *digital* yang terjadi secara global saat ini telah mengalihkan mayoritas aktivitas manusia ke ruang *digital*, mulai dari transaksi finansial hingga pertukaran data sensitif[1]. Namun, perkembangan teknologi yang cepat ini menciptakan celah keamanan siber yang semakin kompleks dan sulit diprediksi, salah satunya adalah serangan *phishing*[2]. Serangan *phishing* tetap menjadi skema rekayasa sosial (*social engineering*) yang paling sering dilakukan dan ampuh karena efektivitasnya dalam memanipulasi psikologi pengguna untuk mencuri kredensial[3]. Kerentanan internal yang bersumber dari kesalahan pengguna, seperti penggunaan kredensial yang lemah, ditambah dengan kurangnya pengawasan serta konfigurasi sistem yang tidak optimal, menjadi faktor utama yang memperbesar risiko kebocoran data sensitif[4].

Phishing (password harvesting fishing) merupakan bentuk penipuan siber di mana pelaku sengaja memanipulasi atau menjebak target agar memberikan data pribadi yang bersifat rahasia, sehingga informasi sensitif tersebut dapat dikuasai dan disalahgunakan oleh pihak yang tidak berwenang demi keuntungan ilegal. [5]. Biasanya, *link phishing* ini dikirim melalui *email*, pesan teks, atau situs *website* palsu yang tampilannya menyerupai *website* yang asli[6]. Salah satu kelompok yang paling rentan dalam menjadi korban *phishing* adalah kelompok remaja[7]. Menurut laporan dari *Anti phishing Working Group (AWG)*, tercatat 892.494 serangan *phishing* di quartal ke-3 di tahun 2025 (Juli - September) dengan rincian 351.590 situs di bulan Juli, 289.848 situs di bulan Agustus, dan 251.056 situs di bulan September[8].

Metode deteksi konvensional yang bergantung pada daftar hitam (*blacklist*) sudah tidak efektif dalam menghadapi serangan *cyber* yang sudah berkembang[9]. Keberagaman perangkat dan *platform digital* saat ini menciptakan celah keamanan yang sangat luas, sehingga informasi ancaman harus disampaikan secara cepat agar penanganan bahaya dapat dilakukan dengan tepat sasaran[10]. Keterbatasan sistem tradisional dalam mengelola data yang besar dan pola serangan yang dinamis sering kali memicu tingginya angka *false positive*, yang pada akhirnya menghambat efisiensi operasional akibat banyaknya peringatan keamanan yang tidak akurat[11].

Berbagai teknik deteksi *phishing* memiliki keterbatasan, di antaranya kesulitan metode *visual* dalam mengenali halaman dengan kemiripan logo dan struktur *HTML*, ketidakmampuan pendekatan berbasis *URL* dalam mengidentifikasi anomali tertentu, serta keterbatasan metode berbasis mesin pencari dalam mendeteksi phishing secara langsung[12].

Implementasi *machine learning* dalam mendeteksi serangan siber telah membuktikan efektivitasnya melalui kemampuan sistem untuk menganalisis data secara mandiri dan mengambil keputusan tanpa memerlukan pemrograman manual yang mendetail[13]. Efektivitas deteksi *website phishing* sangat bergantung pada penggunaan *dataset* yang mengintegrasikan karakteristik leksikal URL dengan elemen struktural konten HTML, di mana fitur-fitur seperti *iframe*, skrip eksternal, dan *HasPasswordField* berperan sebagai indikator krusial dalam mengidentifikasi *malicious intent* guna meningkatkan akurasi pembedaan antara situs legal dan situs *phishing* [14]. Selain itu, pendekatan berbasis *machine learning* juga memungkinkan pemanfaatan berbagai jenis fitur dari sebuah *website*, seperti *URL*, konten *HTML*, maupun representasi *visual* halaman web, sehingga mampu meningkatkan kemampuan sistem dalam mengenali pola *phishing* secara lebih efektif [15].

Dalam pemilihan model klasifikasi, algoritma *Extreme Gradient Boosting (XGBoost)* menunjukkan performa yang superior dibandingkan algoritma *ensemble* lainnya. Penelitian terbaru menunjukkan bahwa *XGBoost* memiliki kemampuan unggul dalam mendeteksi situs *phishing* dengan tingkat akurasi mencapai 95,5%, didukung oleh nilai presisi sebesar 95,5%, *recall* 95,1%, dan *F1-score* 95,3%, sehingga efektif dalam meminimalkan kesalahan deteksi, khususnya *false negative*, serta berkontribusi dalam melindungi pengguna internet dari ancaman *phishing* yang terus berkembang [16]. Selain akurasi, efisiensi waktu juga menjadi faktor krusial; berdasarkan analisis komparatif, *XGBoost* terbukti lebih efisien secara komputasi dengan waktu pelatihan 73% lebih cepat dibandingkan *Random Forest*, sehingga ideal untuk pengolahan dataset skala besar secara *real-time* [17].*XGBoost* dipilih karena efisiensi komputasinya dalam menangani data kompleks serta kemampuannya mencegah *overfitting* melalui mekanisme regularisasi yang efektif[18]. Hal ini didukung oleh penelitian Ramadan dkk. yang menyatakan bahwa kemampuan adaptasi *XGBoost* terhadap fitur yang kompleks sangat krusial dalam menjaga stabilitas performa model pada data *phishing* yang bersifat dinamis[19].

Keterbatasan akses masyarakat awam terhadap teknologi yang dapat

mendeteksi *website phishing* sering kali menimbulkan keraguan dalam memverifikasi keamanan tautan akibat proses yang dianggap terlalu teknis dan rumit. Oleh karena itu, penelitian ini bertujuan untuk merancang dan membangun sistem deteksi *website phishing* berbasis web dengan mengintegrasikan algoritma *Extreme Gradient Boosting (XGBoost)*. Sistem ini dikembangkan untuk mempermudah pengguna melalui antarmuka sederhana yang hanya memerlukan *input URL*, di mana sistem akan secara otomatis melakukan ekstraksi data konten melalui teknik *web scraping* untuk dianalisis oleh model klasifikasi. Penelitian ini berfokus pada pengolahan dataset untuk menghasilkan model klasifikasi yang memiliki akurasi tinggi serta responsif dalam memberikan penilaian keamanan secara instan. Melalui pengembangan aplikasi ini, diharapkan pengguna dapat memperoleh klasifikasi keamanan suatu *website* secara *real-time* tanpa memerlukan pengetahuan teknis yang mendalam, sehingga mampu memberikan kontribusi nyata dalam upaya meminimalkan risiko kejahatan siber bagi masyarakat luas di Indonesia.

1.2 Rumusan Masalah

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

- Bagaimana merancang dan membangun sebuah aplikasi pendeteksi *website phishing* berbasis web dengan mengintegrasikan algoritma *Extreme Gradient Boosting* (XGBoost)?
- Bagaimana hasil pengukuran nilai *Accuracy*, *Precision*, *Recall*, dan *F1-Score* melalui implementasi *confusion matrix* terhadap performa model *XGBoost*?

1.3 Batasan Masalah

Mengingat luasnya cakupan dalam bidang keamanan siber, maka penelitian ini dibatasi oleh beberapa hal sebagai berikut:

- Algoritma: Penelitian ini hanya menggunakan algoritma *Extreme Gradient Boosting* (XGBoost) sebagai mesin klasifikasi utama.
- Dataset: *Dataset* yang digunakan bersumber dari data sekunder *PhiUSIIL Phishing URL Dataset* yang diperoleh melalui *UCI Machine Learning*

Repository[20]. Data berjumlah 235.795 *instances* yang mencakup fitur leksikal URL dan konten *Hypertext Markup Language* (HTML).

- Input Sistem: Sistem hanya menerima masukan berupa *single* URL (tautan tunggal) yang diinputkan secara manual oleh pengguna ke dalam *website*.
- Fokus Deteksi: Sistem difokuskan untuk mendeteksi situs *phishing* yang bertujuan mencuri kredensial (seperti halaman *login* palsu) dan tidak ditujukan untuk mendeteksi jenis *malware* lainnya secara spesifik.

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai melalui pelaksanaan penelitian ini adalah:

- Merancang dan membangun sebuah aplikasi pendeteksi *website phishing* berbasis *web* yang mengintegrasikan algoritma *Extreme Gradient Boosting* (XGBoost) agar dapat digunakan oleh masyarakat luas dengan mudah.
- Mengukur nilai *Accuracy*, *Precision*, *Recall*, dan *F1-Score* dari model klasifikasi *XGBoost* menggunakan *confusion matrix* dalam mendeteksi tautan *phishing*.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat bagi berbagai pihak, di antaranya:

- Bagi Masyarakat: Menyediakan alat verifikasi mandiri untuk mendeteksi potensi ancaman *phishing* guna melindungi kredensial pribadi serta data keuangan dari penyalahgunaan pihak yang tidak bertanggung jawab.
- Bagi Ilmu Pengetahuan: Memberikan bukti mengenai keunggulan efisiensi komputasi dan akurasi algoritma *Extreme Gradient Boosting* (XGBoost) dalam menangani data ancaman siber berskala besar.
- Bagi Keamanan Informasi: Membantu mengurangi dampak kerugian akibat kejahatan siber melalui penyediaan teknologi deteksi yang adaptif terhadap perubahan metode penyerangan modern yang terus berkembang.

1.6 Sistematika Penulisan

Berisikan uraian singkat mengenai struktur isi penulisan laporan penelitian, dimulai dari Pendahuluan hingga Simpulan dan Saran.

Sistematika penulisan laporan adalah sebagai berikut:

- Bab 1 PENDAHULUAN
  Berisi latar belakang masalah mengenai ancaman *phishing*, rumusan masalah, tujuan penelitian, batasan masalah, serta manfaat yang diharapkan dari pengembangan sistem deteksi menggunakan *XGBoost*.

- Bab 2 LANDASAN TEORI
  Memaparkan landasan teori yang mendukung penelitian, meliputi definisi *phishing*, struktur *website*, konsep *machine learning*, penjelasan mendalam mengenai mekanisme algoritma *Extreme Gradient Boosting* (XGBoost), teknik *web scraping*, metrik evaluasi model, serta metode *feature selection* untuk menentukan atribut yang paling berpengaruh dalam klasifikasi.

- Bab 3 METODOLOGI PENELITIAN
  Menjelaskan metodologi penelitian yang mencakup tahapan pengumpulan *dataset*, *preprocessing* data, perancangan model, hingga desain arsitektur sistem berbasis *web* menggunakan *framework Flask* untuk *backend* dan *ReactJS* untuk *frontend*.

- Bab 4 HASIL DAN DISKUSI
  Berisi hasil implementasi sistem dan analisis terhadap performa model XGBoost berdasarkan metrik evaluasi seperti *accuracy*, *precision*, *recall*, dan *f1-score*, serta pembahasan mengenai hasil deteksi pada aplikasi *web*.

- Bab 5 KESIMPULAN DAN SARAN
  Menyajikan kesimpulan dari seluruh rangkaian penelitian yang telah dilakukan serta saran untuk pengembangan sistem deteksi *phishing* di masa mendatang.