BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Phishing merupakan tindakan penipuan dimana pengguna *email* diarahkan pada sebuah *website* untuk memberikan informasi pribadi atau informasi yang bersifat rahasia kepada pihak-pihak tertentu dengan tujuan pelanggaran hukum (Merriam-Webster, 2017). Pada *website phising,* tampilan *website* dibuat semirip mungkin dengan *website* aslinya agar korban yakin sedang berada pada situs yang benar (Febry, 2017). Selain itu, ada pula *website phising* yang didesain khusus untuk memberikan informasi atau petunjuk palsu yang menyesatkan. Jika korban berhasil dikelabui dan memasukkan informasi yang diminta, data tersebut dapat dengan mudah disalahgunakan pada situs yang sah untuk melakukan aktifitas-aktifitas yang tidak diinginkan dan menimbulkan kerugian yang cukup signifikan bagi korbannya mulai dari kerugian finansial hingga *data loss* (Febry, 2017). Berdasarkan data dari Anti-Phising Working Group (APWG), pada quartal ketiga tahun 2019, tercatat sebanyak 266.687 serangan *phising* dilakukan (Comparitech, 2020). Berdasarkan informasi dari *cofense*, hampir 74% serangan *phising* dalam kurun waktu Oktober 2018 sampai dengan Maret 2019 berkaitan dengan pencurian data *username* dan *password* (Comparitech, 2020).

Ekstensi *browser* adalah aplikasi kecil yang membantu pengalaman dalam *browsing.* Ekstensi membiarkan *user* untuk mengubah fungsionalitas *browser* dan

behavior-nya sesuai kebutuhan dari *user* (Chrome Developer, 2020). Ekstensi dibangun dari teknologi *web* seperti *JavaScript*, HTML dan CSS (Chrome Developer, 2020). Ekstensi harus memenuhi tujuan utamanya yang spesifik dan mudah dipahami (Chrome Developer, 2020).

Terdapat banyak penelitian yang telah melakukan klasifikasi *website phising*. Pada penelitian Rizki (2018) menggunakan algoritma C.45 dan CART didapatkan tingkat akurasi *testing* algoritma CART sebesar 94.4% dan algoritma C.45 sebesar 94.3%. Dalam penelitian ini, digunakan dataset sebanyak 11055 data dan 30 atribut.

Pada karya ilmiah yang disusun oleh Sukhpreet Singh Dhaliwal, dibuat sebuah sistem pedeteksian intrusi (IDS) pada jaringan menggunakan algoritma XGBoost. Menggunakan dataset dari NSL-KDD yang berisi 41 fitur, target dari klasifikasi ini adalah untuk menentukan pemberian label normal atau anomali. Dari hasil penelitian ini didapatkan akurasi sebesar 98.7%.

Berdasarkan hal-hal yang telah dijabarkan sebelumnya, penelitian ini menggunakan algoritma XGBoost untuk mengklasifikasi *website phising*. *Dataset* diambil dari UCI *Repository Phising*. Untuk metode evaluasi dari algoritma XGBoost dilihat dari *precission, recall* dan F1 *score* serta dilakukan pembuatan ekstensi *browser* untuk membantu pendeteksian *website phishing*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan, rumusan masalah dalam penelitian ini terdiri dari

1. Bagaimana merancang dan membangun *browser extension* untuk *website phising detector* menggunakan algoritma XGBoost

2. Berapa nilai *precision, recall*, dan F1 *score* pada pendeteksian *website phising*

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Dataset diambil dari UCI Repository Phising
2. Jumlah data yang digunakan sebanyak 11055 data dengan 30 atribut.
3. Data untuk *training* sebanyak 70% dan data untuk *test* sebanyak 30% dari data.
4. Plugin browser yang dibuat ditujukan untuk chrome browser versi 62.0.3202.75 keatas.
5. Ekstensi bekerja dengan memberikan hasil prediksi kepada penggunanya tentang *website* yang diminta.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang dan membangun *browser extension* untuk *website phising detector* menggunakan algoritma XGBoost
2. Mengetahui nilai *precision, recall*, dan F1 *score* pada pendeteksian *website phising*

1.5 Manfaat Penelitian

Melalui penelitian ini, diharapkan aplikasi yang dibuat dapat membantu pengguna *Internet* agar terhindar dari *website phising*.

1.6 Sistematika Penulisan

Sistematika penulisan laporan skripsi ini dapat dijabarkan dalam detail sebagai berikut:

BAB 1 PENDAHULUAN

Bab I Pendahuluan berisi perihal latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan juga sistematika penulisan dari skripsi yang berjudul "RANCANG BANGUN BROWSER EXTENSION UNTUK WEBSITE PHISING DETECTOR MENGGUNAKAN ALGORITMA XGBOOST".

BAB 2 LANDASAN TEORI

Bab II Landasan Teori berisi penjelasan mengenai teori-teori dan metode yang berkaitan dengan penelitian yang dilakukan. Teori-teori dan metode yang digunakan adalah tentang *phising, Extreme Gradient Boosting, Holdout Validation dan K-Fold Validation, browser extension, recursive feature elminiation,* dan parameter evaluasi performa.

BAB 3 METODOLOGI PENELITIAN

Bab III Metodologi Penelitian berisi penjelasan mengenai metodologi penelitian yang digunakan dan perancangan sistem atau *flowchart* yang digunakan, yaitu *flowchart* utama, *flowchart* pembuatan model, *flowchart* ekstensi *browser*, dan *flowchart* proses ekstraksi pada *web service*.

BAB 4 HASIL DAN DISKUSI

Bab IV Hasil dan Diskusi berisi penjelasan mengenai implementasi sistem dan pengujian hasil uji coba terhadap metode XGBoost dengan pemilihan fitur dan menggunakan *hyperparameter* terhadap model yang digunakan.

BAB 5 KESIMPULAN DAN SARAN

BAB V Kesimpulan dan Saran berisi perihal kesimpulan dari hasil uji coba telah dilakukan dan saran untuk pengembangan penelitian lebih lanjut di kemudian hari.