BAB 1

PENDAHULUAN

1.1. Latar Belakang

Di zaman teknologi ini penggunaan internet merupakan suatu hal yang lumrah bahkan vital di kehidupan keseharian masyarakat. Dengan bertambahnya kebutuhan akan informasi, internet membantu kehidupan menjadi lebih mudah dalam berkomunikasi, edukasi, berbelanja dan berbisnis. Hampir segala aktivitas maupun transaksi sekarang ini dapat dilakukan dan diakses secara daring tanpa mengenal tempat dengan bantuan internet.

Namun, dengan segala manfaatnya internet dapat digunakan oleh oknum tertentu untuk melakukan berbagai macam kejahatan yaitu salah satunya membuat situs web *phishing* sebagai alat bantu dalam melancarkan penipuan, mereka menargetkan para pengguna internet yang masih awam atau lalai terhadap keamanan bertransaksi di dunia maya. Data pribadi seperti ID pengguna, kata sandi, bahkan informasi finansial seperti akun bank dan data kartu kredit merupakan hal yang diincar para penjahat internet ini.

Menurut Phishing.org (n.d.) *phishing* adalah *cybercrime* yang berusaha memancing informasi penting atau rahasia seperti detail perbankan atau kartu kredit serta kata sandi dari pengguna yang biasanya dikirim melalui *email*, telepon atau teks pesan yang dilakukan dengan menyamar menjadi institusi atau individu dan membuat situs web palsu dengan sedemikian rupa sehingga menyerupai situs web yang autentik dan sah.

Banyak korban tanpa sadar terkena penipuan dari situs web *phishing* karena URL domain, konten, tampilan dan lain-lain dibuat semirip mungkin dengan situs web aslinya. Jika korban berhasil ditipu dan memasukkan data pribadinya ke situs web *phishing*, data atau informasi korban tersebut akan digunakan oleh penjahat internet untuk kepentingannya sendiri, seperti menggunakan akun korban dan mengubah kata sandi atau mengambil sejumlah uang sehingga akan menimbulkan kerugian mulai dari pencurian identitas hingga kerugian finansial.

Menurut laporan transparansi Google (n.d.) serangan *phishing* meningkat tajam hingga 4-5 kali lipat saat terjadinya pandemi COVID-19. Situs web seperti *e-commerce*, perbankan atau yang baru-baru ini situs web dompet digital untuk *cryptocurrency* kerap dijadikan sasaran *phishing*. Situs web berbasis *social media* juga tidak luput dari para penjahat internet untuk mengambil akun para korban. Terlepas dari pencurian data, situs web *phishing* juga dapat digunakan untuk melakukan menyebarkan virus atau *malware* dengan mengatasnamakan situs web asli.

Dilihat dari bahaya dan maraknya kejahatan *phishing* para peneliti mencoba untuk mengatasi hal tersebut dengan berbagai metode seperti pendeteksian situs web *phishing*. Untuk mendeteksi situs web *phishing* pendekatan yang paling umum digunakan yaitu metode *blacklist* dan *whitelist*, metode ini menggunakan *database* yang berisi kumpulan situs web yang sudah diklasifikasikan sebagai situs web *phishing* atau bukan. Pendekatan ini mempunyai kelemahan yaitu cakupannya yang kurang luas, karena tentunya tidak semua URL atau URL yang baru dibuat langsung ada pada *database* tersebut (Dudhe and Ramteke 2015). Oleh karena itu untuk mengatasi hal tersebut penulis menggunakan pendekatan *machine learning* dengan membuat model yang dapat membedakan situs web *phishing* atau situs web yang autentik dan sah secara langsung. Berdasarkan penelitian terdahulu algoritma *machine learning* yang baik dalam mendeteksi situs web *phishing* yaitu *Random Forest* sehingga penulis menggunakan algoritma tersebut dalam penelitian ini.

Salah satu cara agar metode ini bisa dimanfaatkan oleh pengguna yaitu dengan mengimplementasikannya ke dalam ekstensi peramban seperti Google Chrome. Cara tersebut akan memperingatkan secara langsung ketika pengguna mengunjungi situs web *phishing*. Sistem pendeteksi situs web *phishing* dengan pendekatan *machine learning* yang sudah ada saat ini yaitu dengan cara mengirim URL ke server untuk diklasifikasikan dan hasilnya akan dikembalikan lagi. Dengan pendekatan tersebut tentunya privasi pengguna terganggu (mengirim URL situs web apa yang dikunjungi) dan juga deteksi akan terhambat oleh jaringan internet yang mana mempunyai kemungkinan gagal dalam memperingatkan pengguna di waktu yang tepat. Karena pentingnya masalah privasi dan keamanan, penulis menggunakan implementasi ekstensi Google Chrome yang bisa mengklasifikasikan

situs web *phishing* menggunakan algoritma *Random Forest* secara langsung tanpa bergantung dengan server dan *web service*.

1.2. Rumusan Masalah

a. Bagaimana membangun model *Random Forest* dalam mendeteksi situs web *phishing*?
b. Bagaimana mengimplementasikan model *Random Forest* yang sudah dibuat ke ekstensi Google Chrome yang ingin dibangun?
c. Bagaimana hasil kinerja dari model dan ekstensi yang sudah dibuat?

1.3. Ruang Lingkup

a. Ekstensi hanya tersedia di peramban Google Chrome saja.
b. Fitur yang digunakan hanya *client-based* saja tidak bergantung pada *web service* dengan total fitur yang digunakan sebanyak 16.
c. Bahasa pemrograman yang digunakan yaitu JavaScript dan Python.
d. Ekstensi ini hanya tersedia di peramban komputer saja, tidak bisa di *handphone.*

1.4. Tujuan Penelitian

a. Membuat model klasifikasi yang dapat mendeteksi situs web *phishing*.
b. Mengimplementasikan model tersebut ke dalam bentuk ekstensi peramban agar bisa digunakan oleh pengguna.
c. Mengetahui kinerja model dan implementasi *machine learning* di ekstensi peramban dalam mendeteksi situs web *phishing* dengan pengukuran tingkat ketepatan akurasi.

1.5. Manfaat Penelitian

a. Pada hasil penelitian ini, pengguna dapat menggunakan ekstensi peramban yang dibangun untuk terhindar dari serangan *phishing*.
b. Meningkatkan kesadaran terhadap *cybercrime* agar para peneliti selanjutnya dapat membuat teknik metode yang lebih baik dalam menangkalnya.

1.6. Luaran yang Diharapkan

Luaran yang diperoleh dari penelitian ini berupa ekstensi peramban Google Chrome yang cukup baik dalam mendeteksi dengan akurasi yang cukup tinggi dan dapat memperingatkan pengguna terhadap situs web *phishing*.

1.7. Sistematika Penulisan

Untuk mengetahui permasalahan yang ada dalam penulisan proposal ini, sehingga menggunakan sistematika penulisan dengan tujuan agar mempermudah pembaca dalam memahami proposal tugas akhir ini.

BAB 1 PENDAHULUAN

Dalam bab ini menjelaskan mengenai latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup yang membatasi permasalahan, luaran yang diharapkan dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Dalam bab ini menjelaskan konsep dan teori dari literatur dan peralatan pendukung yang menjadi acuan dalam penyusunan laporan tugas akhir ini.

BAB 3 METODOLOGI PENELITIAN

Dalam bab ini penulis menjelaskan tahapan penelitian mulai dari tahap riset, sumber data, metode pengumpulan data, pengolahan, dan analisis data sesuai dengan tujuan dari penelitian.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini berisikan tentang tahapan dalam perancangan dan implementasi model klasifikasi dan *software* yang dibuat serta evaluasi hasil dari uji coba penelitian.

BAB 5 KESIMPULAN

Bab ini berisikan tentang kesimpulan yang dapat diambil dari seluruh rangkaian penelitian, serta saran-saran yang diberikan peneliti untuk penelitian selanjutnya.

DAFTAR PUSTAKA

LAMPIRAN