BAB I

PENDAHULUAN

1.1 Latar Belakang

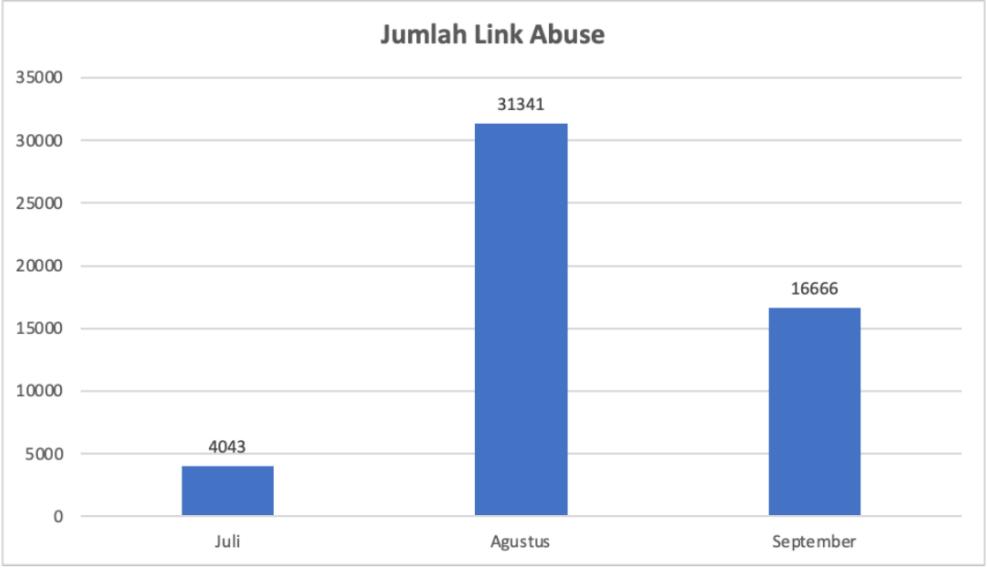
Perkembangan teknologi informasi dan komunikasi telah membawa banyak kemudahan dan inovasi dalam berbagai aspek kehidupan manusia. Dalam sektor perbankan, teknologi memungkinkan transaksi menjadi lebih cepat, mudah, dan aman. Layanan perbankan digital, seperti internet banking dan mobile banking, memberikan akses yang lebih luas bagi nasabah untuk mengelola keuangan mereka kapan saja dan di mana saja. Namun, di balik kemajuan teknologi ini, ancaman keamanan siber juga semakin berkembang. Salah satu ancaman yang paling signifikan adalah serangan phishing, khususnya melalui URL phishing [1].

Dalam beberapa dekade terakhir, penggunaan internet dan teknologi digital telah mengalami pertumbuhan eksponensial. Hal ini mengubah cara orang berkomunikasi, bertransaksi, dan melakukan berbagai aktivitas lainnya. Bank-bank besar, termasuk PT Bank Central Asia, Tbk, terus berinovasi dengan menyediakan layanan digital yang memungkinkan nasabah melakukan transaksi perbankan tanpa harus datang ke kantor cabang. Transaksi seperti transfer uang, pembayaran tagihan, dan pengecekan saldo dapat dilakukan dengan mudah melalui perangkat elektronik. Transformasi digital ini memberikan banyak manfaat, seperti efisiensi waktu dan biaya, namun juga menimbulkan risiko baru dalam bentuk ancaman siber [2].

Serangan phishing merupakan salah satu bentuk ancaman siber yang paling umum dan merugikan. Phishing adalah tindakan penipuan yang dilakukan dengan mengelabui target untuk mengungkapkan informasi pribadi atau keuangan mereka. Metode ini sering kali dilakukan melalui url yang tampak seperti berasal dari sumber tepercaya, seperti bank atau lembaga keuangan [3]. Pelaku phishing menggunakan berbagai teknik untuk membuat email mereka terlihat sah dan

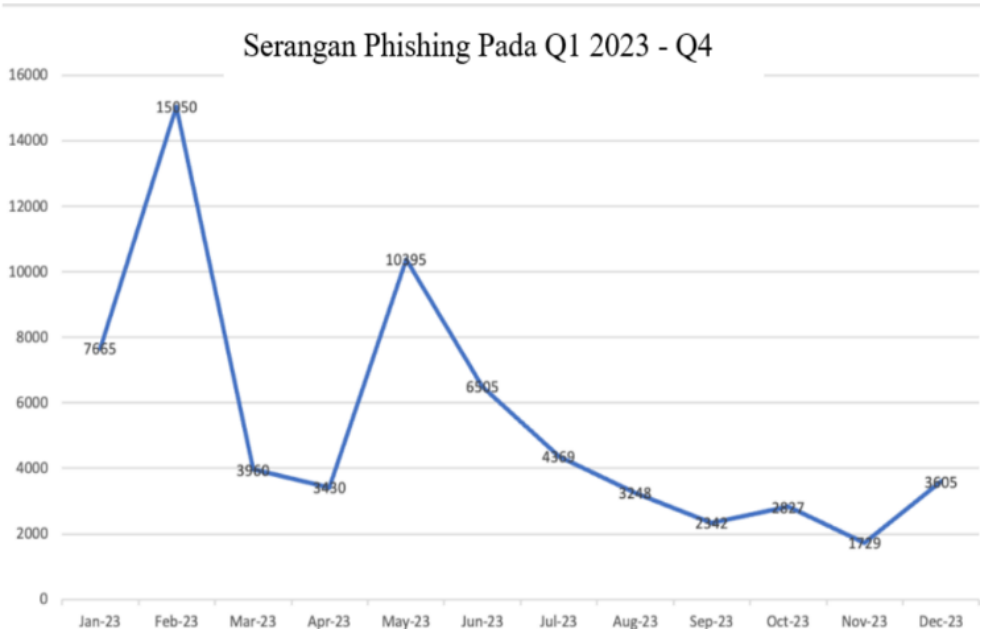
meyakinkan, sering kali meniru logo, bahasa, dan format komunikasi resmi dari perusahaan target.

Serangan phishing di sektor keuangan Indonesia meningkat karena tingginya ketergantungan masyarakat pada layanan perbankan digital dan transaksi online yang sering menjadi target utama penyerang. Pelaku kejahatan siber memanfaatkan metode manipulasi sosial untuk menipu nasabah dengan mengirimkan email atau pesan teks yang mengatasnamakan bank atau lembaga keuangan lain, meminta informasi pribadi atau data login. Peningkatan penggunaan mobile banking, e-wallet, dan aplikasi finansial lainnya semakin memperbesar peluang penyerang untuk memperoleh akses ilegal ke akun nasabah. Menurut laporan dari IDADX, Jumlah laporan phishing yang diterima oleh IDADX dalam Q3 tahun 2024 sebanyak 52.050 kasus [4].



Gambar 1. 1 Serangan Phising Pada Q3 tahun 2024 [4]

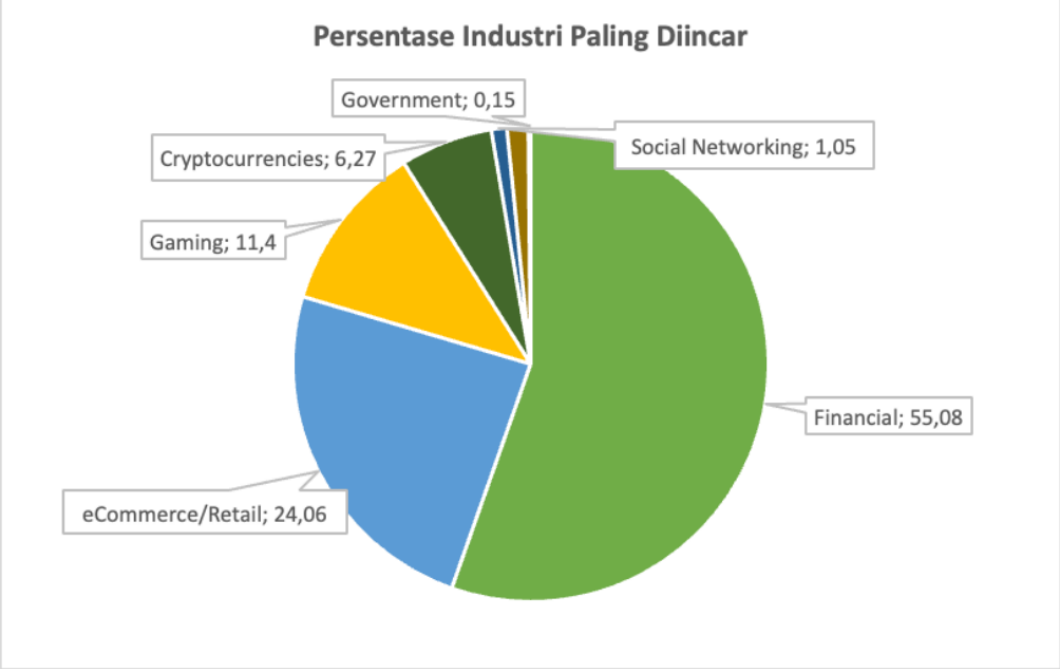
Pada gambar 1.1 terlihat bahwa kasus serangan phising paling banyak terjadi pada bulan Agustus 2024 dengan total kasus serangan phising sebanyak 31341 kasus.dan untuk kasus serangan phising paling sedikit terjadi pada bulan Juli 2024 dengan kasus serangan phising sebanyak 4043 kasus.Terjadi penurunan pada bulan agustus – september tetapi terlihat pada bulan juli – agustus terjadi peningkatan yang signifikan yaitu sebesar 27.298 kasus.



Gambar 1. 2 Serangan Phising Pada tahun 2023 [4]

Berdasarkan Gambar 1.2, terlihat bahwa serangan phishing sempat mengalami penurunan pada akhir tahun 2023. Namun, jika merujuk kembali pada Gambar 1.1, terlihat bahwa serangan phishing kembali mengalami peningkatan yang signifikan pada tahun 2024. Bahkan, jumlah kasus pada bulan September 2024 melampaui jumlah kasus pada Februari 2023, yang sebelumnya merupakan bulan dengan jumlah serangan phishing tertinggi di tahun 2023. Kondisi ini menjadi salah satu alasan utama dilakukannya penelitian ini, guna merespons tren peningkatan ancaman phishing yang semakin mengkhawatirkan.

Bank-bank besar, termasuk PT Bank Central Asia, Tbk, sering kali menjadi sasaran serangan phishing karena mereka memiliki jumlah nasabah yang besar dan mengelola data keuangan yang sangat sensitif. Serangan phishing dapat berdampak serius pada reputasi bank dan kepercayaan nasabah, serta menyebabkan kerugian finansial yang signifikan.



Gambar 1. 3 Serangan Phising terhadap Industri paling diincar Pada tahun 2023 [4]

Menurut laporan dari IDADX pada Q3 tahun 2024 seperti pada gambar diagram 1.3 , sebanyak 50,08% serangan phising mengarah ke Lembaga keuangan yang ada di indonesia. Setengah dari kasus serangan phsing yang ada di Indonesia Hal ini menunjukkan betapa pentingnya bagi bank-bank untuk meningkatkan keamanan dan edukasi terhadap nasabah mereka mengenai ancaman phishing [4].

Pada 22 Juli 2023, PT Bank Central Asia Tbk (BCA), salah satu bank terbesar di Indonesia, menghadapi dua insiden siber serius yang menyoroti risiko keamanan digital di sektor perbankan. Berdasarkan laporan CNN Indonesia [5], dugaan kebocoran data pengguna kartu kredit yang melibatkan 6,4 juta informasi sensitif seperti alamat dan nomor telepon menjadi ancaman besar terhadap privasi nasabah dan reputasi perusahaan. Selain itu, potensi infeksi virus pada aplikasi mobile banking menambah kekhawatiran akan keamanan layanan digital BCA. Insiden-insiden ini tidak hanya menyebabkan potensi kerugian finansial, tetapi juga mengakibatkan penurunan kepercayaan nasabah terhadap layanan digital bank. Ketidakamanan ini dapat mendorong nasabah untuk mengurangi penggunaan aplikasi atau bahkan beralih ke bank lain.

Peningkatan serangan phishing melalui URL palsu yang menyasar Bank BCA mencerminkan masalah serius dalam keamanan digital, di mana pelaku kejahatan siber memanfaatkan kepercayaan nasabah terhadap institusi keuangan untuk mencuri informasi sensitif seperti kredensial login dan data keuangan. Serangan ini dilakukan karena data tersebut memiliki nilai tinggi untuk pencurian identitas, akses ilegal, dan penipuan finansial. Dengan menggunakan teknik manipulasi sosial dan pemalsuan domain, pelaku mampu menipu nasabah, terutama di tengah tingginya adopsi layanan digital. Fenomena ini tidak hanya menyebabkan kerugian finansial, tetapi juga mengancam kepercayaan nasabah terhadap layanan perbankan digital, menegaskan pentingnya pengembangan sistem deteksi phishing yang canggih dan edukasi bagi nasabah untuk mengurangi risiko ini [5].

Melihat permasalahan tersebut, pengembangan sistem deteksi URL phishing berbasis machine learning menjadi langkah strategis untuk mencegah serangan melalui manipulasi URL berbahaya. Sistem ini diharapkan mampu melindungi data nasabah sekaligus memulihkan kepercayaan terhadap layanan digital bank. Penelitian sebelumnya mendukung urgensi ini, menunjukkan bahwa algoritma Support Vector Machine (SVM) secara konsisten unggul dalam mendeteksi URL phishing dengan akurasi tinggi. Misalnya, Ahmad et al [6]. melaporkan bahwa SVM

mencapai akurasi 95,6% melalui analisis fitur URL seperti panjang dan simbol tertentu. Temuan ini diperkuat oleh Chen et al [7], yang menunjukkan bahwa metode whitelist filtering pada SVM menghasilkan akurasi 90,2%, lebih baik dibandingkan algoritma Decision Tree yang hanya mencapai 85%.

Oleh karena itu, pengembangan website untuk mendeteksi URL phishing tidak hanya relevan dalam konteks ancaman yang dihadapi oleh BCA, tetapi juga menjadi alat penting untuk membangun kesadaran dan kewaspadaan di kalangan nasabah dan perusahaan. Dengan demikian, langkah ini menjadi bagian integral dari strategi keamanan digital di sektor perbankan [8].

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas ditemukan rumusan masalah sebagai berikut.

1. Bagaimana serangan phishing yang memanfaatkan URL phishing dapat berdampak pada kerugian finansial dan reputasi PT Bank Central Asia, Tbk?
2. Bagaimana proses pemodelan deteksi URL phishing di PT Bank Central Asia Tbk menggunakan algoritma Support Vector Machine (SVM), Decision Tree, Naïve Bayes, dan Random Forest, serta implementasi model dengan performa optimal.
3. Bagaimana hasil evaluasi komparatif terhadap kinerja setiap model yang digunakan dalam penelitian ini.
4. Bagaimana tahapan pengembangan sistem berbasis website untuk deteksi URL phishing, serta bagaimana efektivitas sistem tersebut dalam mengidentifikasi URL phishing.

1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah sebagai berikut.

1. Penelitian ini hanya menggunakan empat model pembelajaran mesin yang difokuskan pada analisis akurasi hasil.

2. Data yang digunakan dalam penelitian ini dibatasi pada ruang lingkup PT Bank Central Asia, Tbk , dengan periode pengumpulan data mulai 1 Januari 2023 hingga 1 Juli 2024, Data penelitian ini terdiri dari data URL dan label terkait yang berasal dari PT Bank Central Asia, Tbk.
3. Penelitian ini berfokus pada pengembangan model algoritma dan implementasi website sederhana tanpa menyertakan fitur login atau basis data.
4. Fungsi dari situs web deteksi URL phishing ini terbatas pada pendeteksian URL phishing yang secara khusus berkaitan dengan PT Bank Central Asia, Tbk. Tujuan dan Manfaat Penelitian

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Adapun tujuan yang ingin dicapai pada penelitian ini adalah sebagai berikut.

1. Mengidentifikasi Dampak Serangan Url Phishing pada kerugian finansial dan reputasi PT Bank Central Asia, Tbk
2. Mengembangkan model deteksi URL phishing untuk PT Bank Central Asia, Tbk dengan menggunakan algoritma Support Vector Machine (SVM), Decision Tree, Naïve Bayes, dan Random Forest, serta mengimplementasikan model dengan performa terbaik pada sistem deteksi.
3. Menganalisis dan membandingkan performa setiap model deteksi berdasarkan hasil evaluasi untuk menentukan algoritma dengan kinerja terbaik dalam mendeteksi URL phishing.
4. Merancang dan membangun sistem deteksi berbasis website yang efektif dalam mengidentifikasi URL phishing, serta memastikan sistem tersebut mudah digunakan oleh nasabah dan karyawan.

1.4.2 Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai

berikut.

1. Mendukung perusahaan dalam mengimplementasikan teknologi berbasis machine learning untuk meningkatkan keandalan sistem digital mereka.
2. Menyediakan alat berbasis web yang dapat digunakan untuk memvalidasi URL mencurigakan, membantu Perusahaan PT Bank Central Asia, Tbk dalam menghindari ancaman phishing secara lebih mudah dan efisien.

1.5 Sistematika Penulisan

Dokumentasi penelitian ini disusun secara terstruktur untuk memudahkan pembaca dalam memahami isi dan alur penelitian. Dokumen ini dibagi menjadi lima bab yang mencakup topik-topik berbeda sebagai berikut:

BAB I PENDAHULUAN

Bab ini mencakup latar belakang, rumusan masalah, batasan masalah, serta tujuan dan manfaat penelitian. Pendahuluan bertujuan untuk menjelaskan permasalahan utama yang menjadi fokus penelitian sekaligus alasan pentingnya membahas topik tersebut.

BAB II LANDASAN TEORI

Bab ini menyajikan berbagai teori yang mendasari penelitian, termasuk framework, tools, dan algoritma yang digunakan. Referensi teori diperoleh dari sumber terpercaya seperti jurnal ilmiah dan buku yang relevan dengan metode atau penelitian serupa.

BAB III METODOLOGI PENELITIAN

Bab ini menguraikan objek penelitian, metode atau tahapan yang diterapkan, teknik pengumpulan data, serta deskripsi variabel penelitian.

Penjelasan ini dirancang untuk memberikan gambaran rinci mengenai pendekatan yang digunakan dalam penelitian.

BAB IV ANALISIS DAN HASIL PENELITIAN

Bab ini membahas penerapan metodologi pada objek penelitian guna mencapai tujuan yang telah ditetapkan. Analisis mencakup pengolahan data, evaluasi, serta hasil yang diperoleh dari penelitian.

BAB V SIMPULAN DAN SARAN

Bab terakhir berisi kesimpulan yang dirumuskan berdasarkan hasil penelitian, serta saran untuk mengatasi kendala yang ditemukan. Saran yang disampaikan diharapkan dapat memberikan kontribusi bagi penelitian selanjutnya dengan topik atau tujuan serupa.