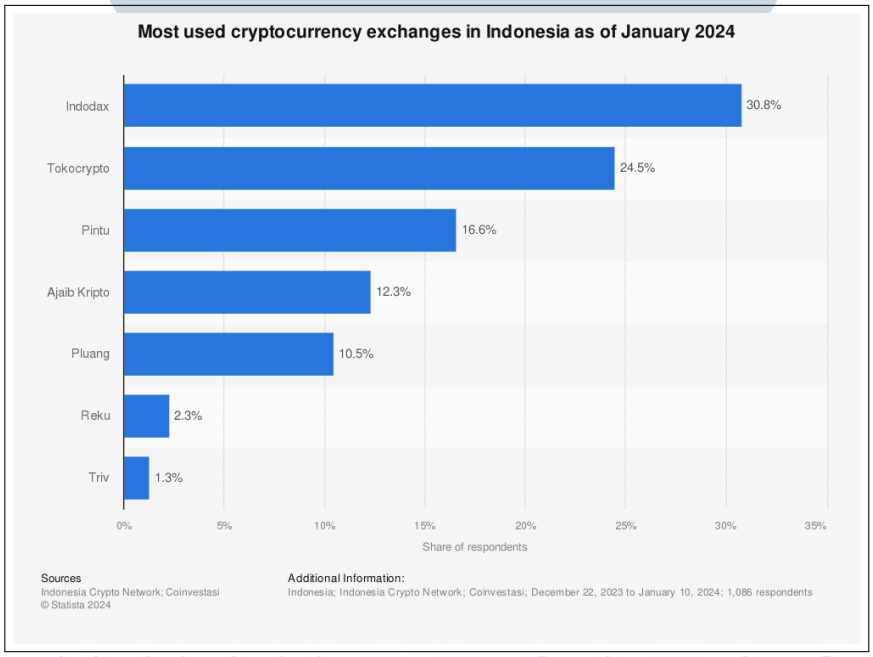
BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring dengan pesatnya adopsi teknologi dalam sektor keuangan, termasuk internet banking dan layanan keuangan digital, keamanan siber menjadi aspek fundamental dalam melindungi sistem keuangan dari ancaman yang meningkat akibat tingginya volume transaksi daring [1]. Mata uang digital yang diciptakan melalui teknologi kriptografi dikenal sebagai *cryptocurrency*. *Cryptocurrency* dapat digunakan sebagai alat tukar dalam transaksi digital, serta untuk pembayaran dan investasi [2]. Sebagai salah satu bursa *cryptocurrency* terbesar di Indonesia, Indodax memainkan peran yang signifikan dalam ekosistem keuangan digital.



Gambar 1.1. Statistik bursa kripto yang paling banyak digunakan

Pada Januari 2024, sebanyak 30,8 persen responden di Indonesia menyatakan bahwa Indodax merupakan bursa kripto yang paling banyak digunakan [3]. Statistik ini menunjukkan bagian yang signifikan dari populasi yang aktif dalam penggunaan mata uang digital, sebagaimana ditunjukkan pada Gambar 1.1. Dengan minat yang terus meningkat terhadap mata uang digital, Indonesia telah mencatat pencapaian penting dengan meluncurkan bursa *cryptocurrency* yang didukung

negara pertama di dunia pada Juli 2023. Namun, dengan bertambahnya jumlah pengguna *cryptocurrency* di Indonesia, bursa kripto juga menghadapi tantangan keamanan, termasuk insiden peretasan yang dapat mempengaruhi persepsi publik.

Insiden peretasan pada bursa kripto bukanlah hal baru. Sebelumnya pada 30 Maret 2019, Bithumb sebagai bursa kripto terbesar di Korea Selatan, mengumumkan melalui akun media sosial *X (Twitter)* bahwa operasi bursa tersebut sementara dihentikan akibat serangan siber [4]. Meskipun Bithumb adalah bursa yang memiliki reputasi baik, serangan siber yang berulang kali terjadi menyebabkan defisit kepercayaan yang signifikan terhadap bursa tersebut. Akibat insiden keamanan ini, persentase sentimen positif pelanggan sebesar 35% dikarenakan kurangnya transparansi dan terjadinya serangan secara berulang. Binance Exchange merupakan bursa kripto terbesar di dunia yang mengalami serangan siber besar-besaran pada Mei 2019 yang menyebabkan kehilangan lebih dari 7000 bitcoin dengan total kerugian sekitar $40 juta [4]. Para peretas dapat masuk ke sistem keamanan dan mencuri data API, kode autentikasi dua faktor, dan data pribadi lainnya. Semua dana yang dicuri disimpan dalam satu dompet kripto, dan Binance menggunakan *Secure Asset Fund for Users (SAFU)* untuk mengganti kerugian pelanggan [5]. Akibat insiden keamanan ini, persentase sentimen positif di kalangan anggota forum bitcointalk.org mencapai 54%.

Kejadian serupa terjadi pada 11 September 2024, Indodax mengklarifikasi adanya indikasi masalah keamanan dan menyatakan bahwa sistem sedang menjalani pemeliharaan menyeluruh untuk memastikan seluruh sistem berfungsi dengan baik [6]. Selama proses ini, bursa kripto Indodax sementara tidak dapat diakses. Oscar Darmawan, CEO Indodax, menjelaskan bahwa insiden ini bermula dari seorang karyawan yang tanpa sadar telah mengunduh *malware* ke dalam laptop perusahaan setelah menerima tawaran kerja lepas dari pihak yang tidak dikenal. *Malware* ini kemudian digunakan untuk menyusup ke sistem Indodax, menyebabkan peretasan yang berdampak signifikan pada keamanan aset pengguna (DetikFinance, 2024). Akibat insiden keamanan ini, Indodax mengalami kerugian sebesar 300 M Rupiah.

Klasifikasi adalah metode untuk mengelompokkan data ke kategori tertentu berdasarkan karakteristiknya, sementara klasifikasi teks merupakan penerapan teknik untuk mengategorikan dokumen atau teks ke berbagai kelas, seperti analisis sentimen, pengelompokan topik, atau deteksi spam. Proses klasifikasi teks mencakup ekstraksi fitur, dimensi, model klasifikasi, dan evaluasi performa [7]. Analisis sentimen merupakan metode yang digunakan untuk mengidentifikasi polaritas teks, seperti dokumen, kalimat, atau paragraf [8]. Analisis sentimen

bertujuan untuk mengidentifikasi sentimen dalam teks dan sekaligus mengevaluasi apakah pendapat dalam teks cenderung positif atau negatif terkait dengan suatu masalah atau objek tertentu [9]. Penelitian yang dilakukan oleh Prismahardi Aji Riyantoko dan Amri Muhaimin berjudul *"A Simple Data Sentiment Analysis using Bjorka Phenomenon on Twitter"* ini berfokus pada reaksi publik terhadap peretasan data pemerintah di Indonesia [10]. Hasil analisis menemukan bahwa sentimen publik terkait kasus ini terdiri dari 75% sentimen netral, 18% negatif, dan 8% positif.

Support Vector Machine (SVM) adalah algoritma pembelajaran mesin berbasis klasifikasi yang efisien dalam berbagai aplikasi, termasuk analisis sentimen [11]. Berdasarkan penelitian yang dilakukan oleh Muhammad Muhajir dkk [12], yang berjudul *Sentiment Analysis and Topic Modeling of Bjorka Using Support Vector Machine and Latent Dirichlet Allocation*, metode *Support Vector Machine* (SVM) menunjukkan efektivitas yang tinggi dalam mengklasifikasikan serta memprediksi sentimen dengan tingkat akurasi yang konsisten di atas 85%. Selain itu, dominasi sentimen positif dalam diskusi terkait Bjorka, yang mencapai 75,2%, menunjukkan bahwa persepsi publik secara umum cenderung positif. Selanjutnya, penelitian lain yang berjudul *Analisis Sentimen Publik pada Pemerintah dalam Serangan Ransomware dengan Pendekatan SMOTE* [13] menemukan bahwa mayoritas komentar publik terkait serangan *ransomware* bersentimen negatif (4.728 komentar). Penerapan *SMOTE* meningkatkan akurasi model *machine learning* secara signifikan, di mana dengan *SMOTE*, SVM mencapai akurasi tertinggi sebesar 96%, diikuti oleh *Random Forest* (95%) dan *Naïve Bayes* (89%). Sementara itu, tanpa *SMOTE*, akurasi tertinggi diperoleh oleh *Random Forest* (80%), SVM (79%), dan *Naïve Bayes* (76%). Selain itu, penelitian lain membandingkan metode *Naïve Bayes Classifier* (NBC) dan *Support Vector Machine* (SVM) dalam analisis sentimen terhadap serangan *ransomware* pada data KIP menggunakan data dari media sosial *X (Twitter)*. Data dikumpulkan melalui proses *crawling* dengan API media sosial *X(Twitter)* dan diproses menggunakan Python. Setelah melalui tahapan *labelling*, *preprocessing*, dan klasifikasi, hasil menunjukkan bahwa metode SVM memiliki akurasi lebih tinggi (88%) dibandingkan NBC (70%) [14].

Dalam konteks ini, analisis sentimen berbasis machine learning dapat digunakan untuk memahami pola opini publik terhadap insiden peretasan Indodax. Penelitian ini bertujuan untuk menganalisis opini publik terhadap insiden peretasan Indodax menggunakan SVM dan mengevaluasi efektivitas model berdasarkan metrik akurasi, presisi, *recall*, dan *F1-Score*. Dengan memahami reaksi publik

secara lebih mendalam, penelitian ini diharapkan dapat memberikan wawasan bagi platform pertukaran aset kripto dalam menyusun strategi komunikasi dan mitigasi krisis pasca-insiden siber.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, terdapat beberapa rumusan masalah yang ditemukan pada penelitian ini.

1. Bagaimana mengimplementasikan algoritma *Support Vector Machine* untuk melakukan klasifikasi opini publik terhadap insiden peretasan Indodax?
2. Bagaimana mengukur akurasi implementasi algoritma *Support Vector Machine* dalam klasifikasi opini publik menggunakan *confusion matrix*?

1.3 Batasan Permasalahan

Batasan masalah yang ditemukan pada penelitian ini adalah sebagai berikut.

1. Sumber data didapatkan dari hasil *crawling* pada sosial media X(Twitter) yang berkaitan dengan insiden peretasan indodax.
2. Berfokus pada insiden peretasan indodax
3. Rentang waktu pengambilan data ini dibatasi dari 11 September 2024 sampai 13 september 2024

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang ditentukan, terdapat tujuan dari penelitian yang akan dilakukan.

1. Mengimplementasikan algoritma *Support Vector Machine* (SVM) untuk melakukan klasifikasi opini publik terhadap insiden peretasan Indodax.
2. Mengukur tingkat akurasi hasil klasifikasi dengan menggunakan *confusion matrix* untuk menentukan apakah reaksi masyarakat terhadap peristiwa tersebut cenderung bersifat positif, netral atau negatif.

1.5 Manfaat Penelitian

Hasil analisis sentimen yang diperoleh dapat digunakan sebagai bahan evaluasi bagi Indodax dalam meningkatkan sistem keamanannya serta mengidentifikasi respons publik terhadap insiden peretasan yang terjadi. Selain itu, hasil ini juga dapat dimanfaatkan untuk mengedukasi pengguna mengenai pentingnya keamanan data pribadi serta langkah-langkah pencegahan agar terhindar dari ancaman serupa di masa mendatang.

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
  Bab ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan.
- Bab 2 LANDASAN TEORI
  Bab ini menjelaskan mengenai teori yang mendukung penelitian, serta terdapat beberapa penelitian terdahulu yang sesuai dengan topik penelitian.
- Bab 3 METODOLOGI PENELITIAN
  Bab ini menjelaskan mengenai metode, Variable penelitian, teknik pengumpulan data dan tahapan yang dilaksanakan pada penelitian.
- Bab 4 HASIL DAN DISKUSI
  Bab ini menjelaskan analisis yang telah dilakukan, dengan memaparkan kode program dan menjelaskan temuan penelitian.
- Bab 5 SIMPULAN DAN SARAN
  Bab ini menjelasakan kesimpulan dan saran dari hasil penelitian yang telah dilakukan.

UNIVERSITAS MULTIMEDIA NUSANTARA