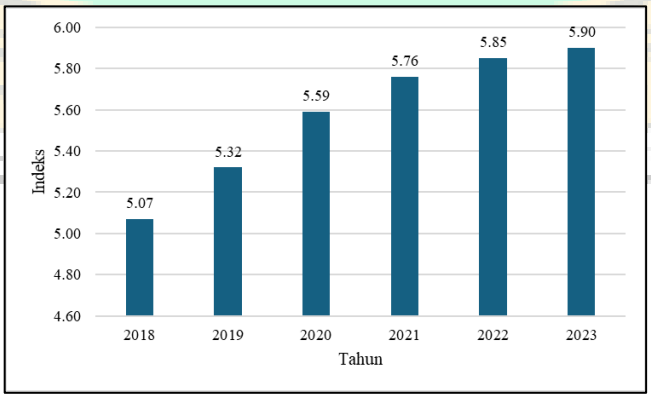
BAB I
PENDAHULUAN

Bab ini akan menjelaskan mengenai latar belakang penelitian, rumusan masalah, tujuan penelitian, batasan masalah, serta sistematika penulisan laporan. Berikut merupakan bab 1 dari penelitian ini.

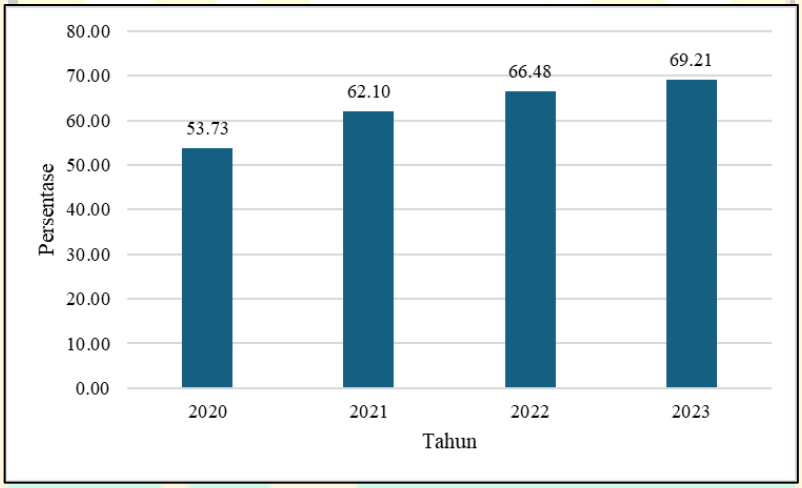
1.1 Latar Belakang

Dewasa ini, gelombang globalisasi sangat dirasakan bagi seluruh aspek kehidupan di Indonesia seperti ekonomi, sosial, politik, dan budaya. Kedatangan gelombang globalisasi tersebut ditandai dengan munculnya banyak perusahaan besar berskala internasional beserta cabangnya yang berdiri di Indonesia. Hal tersebut berdampak kepada perkembangan bangsa Indonesia dan tentunya berpengaruh secara positif maupun negatif. Pengaruh positif yang dibawa oleh globalisasi seperti penyerapan tenaga kerja, perkembangan ilmu pengetahuan, serta perkembangan teknologi informasi dan komunikasi, telah memberikan peluang bagi Indonesia untuk menjadi negara maju. Dampak yang dirasakan oleh perkembangan teknologi dapat diperlihatkan dari grafik berikut.



Gambar 1. 1 Tren Indeks Pembangunan TIK di Indonesia, 2018–2023 (Sumber: BPS)

Berdasarkan **Gambar 1.1**, dapat diketahui bahwa perkembangan teknologi dan komunikasi di Indonesia mengalami peningkatan tren. Hal ini ditandai dengan indeks pembangunan Teknologi Informasi dan Komunikasi (TIK) di Indonesia yang memperlihatkan data dari tahun 2018 mengalami 16% hingga pada tahun 2023 (BPS, 2024a). Indeks pembangunan Teknologi, Informasi dan Komunikasi di Indonesia tersusun atas subindeks seperti akses dan infrastruktur TIK, penggunaan TIK, dan keahlian TIK. Berdasarkan hal tersebut, Akses dan Infrakstruktur TIK di Indonesia yang saat ini menjadi kebutuhan primer bagi masyarakat Indonesia adalah internet.



Gambar 1. 2 Peningkatan persentase pengguna internet di Indonesia, 2020–2023 (Sumber: BPS)

Berdasarkan **Gambar 1.2**, diketahui bahwa persentase jumlah pengguna internet di Indonesia pada tahun 2020 hingga 2023 mengalami peningkatan yang cukup signifikan yaitu pada angka 53.73% pada 2020 dan 69.21% pada tahun 2023. Hal ini sejalan dengan kemudahan yang diperoleh dalam penggunaan internet dalam kehidupan sehari-hari seperti komunikasi, akses dalam memperoleh edukasi, penentuan alamat dan pemetaan, kemudahan dalam berniaga, dan masih banyak lagi.

Manfaat yang diperoleh dari penggunaan internet tersebut sejalan dengan dampak negatif yang dihasilkan dari peningkatan intensitas penggunaan internet

khususnya dalam kegiatan kriminalitas. Kriminalitas yang terjadi di internet atau biasa disebut kejahatan siber merupakan suatu kegiatan yang menggunakan sistem dari komputer atau melibatkan jaringan internet (Maskun, 2013). Kejahatan siber sendiri biasanya menyerang korbannya melalui banyak cara seperti melakukan penyusupan ke sistem jaringan komputer secara ilegal, mempublikasikan suatu data atau informasi yang tidak benar, pemalsuan data, dan lain sebagainya (Beridiansyah, 2023).

Beberapa bentuk dari jenis kejahatan siber dalam melakukan penyusupan ke jaringan komputer adalah *phishing* dan spam. *Phishing* dalam kejahatan siber diartikan sebagai sebuah upaya yang dilakukan oleh seseorang untuk memancing korban agar melakukan tindakan yang dapat menyebabkan data dari korban mengalami kebocoran, sementara *spam* diartikan pengiriman konten elektronik secara massal yang seringkali berisikan konten yang tidak relevan, tindakan penipuan, atau konten bahaya lainnya (Yanto, 2021).

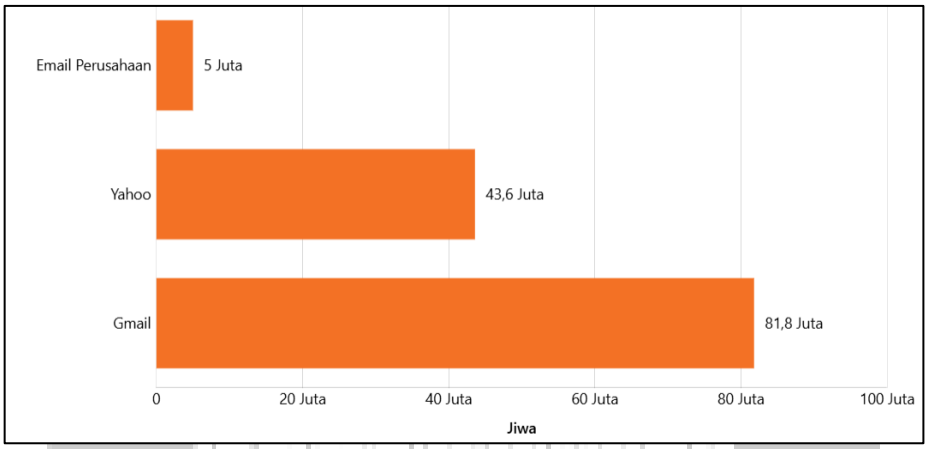
Adapun beberapa kasus yang pernah terjadi akibat kejahatan siber dalam bentuk *phishing* dan spam salah satunya melibatkan PayPal, layanan pembayaran *online* yang terjadi pada rentang 6-8 Desember 2022. Dalam kasus ini, korban diberi tahu bahwa akun mereka telah diretas dan akan dinonaktifkan kecuali mereka mengonfirmasi detail kartu kredit mereka. Akibat dari kasus tersebut, pelaku berhasil mengakses setidaknya 35.000 data pelanggan dan berhasil memperoleh informasi sensitif korban seperti nama, alamat, nomor pokok wajib pajak, nomor jaminan sosial, dan tanggal lahir (Tim StrongDM, 2024).

Kasus lain yang berkaitan mengenai kejahatan siber pernah terjadi di Indonesia pada tahun 2014 yang menargetkan nasabah Bank Mandiri melalui fitur *internet banking*. Dalam kasus ini, nasabah diarahkan ke sebuah link yang terlihat seperti alamat resmi Bank Mandiri (www.bankmandiri.co.id), namun kemudian mereka "dibelokkan" ke situs web palsu milik pelaku. Dari situs tersebut, pelaku berhasil memperoleh data pribadi nasabah, seperti *username*, *password*, dan nomor PIN ATM. (Azahrah, 2018).

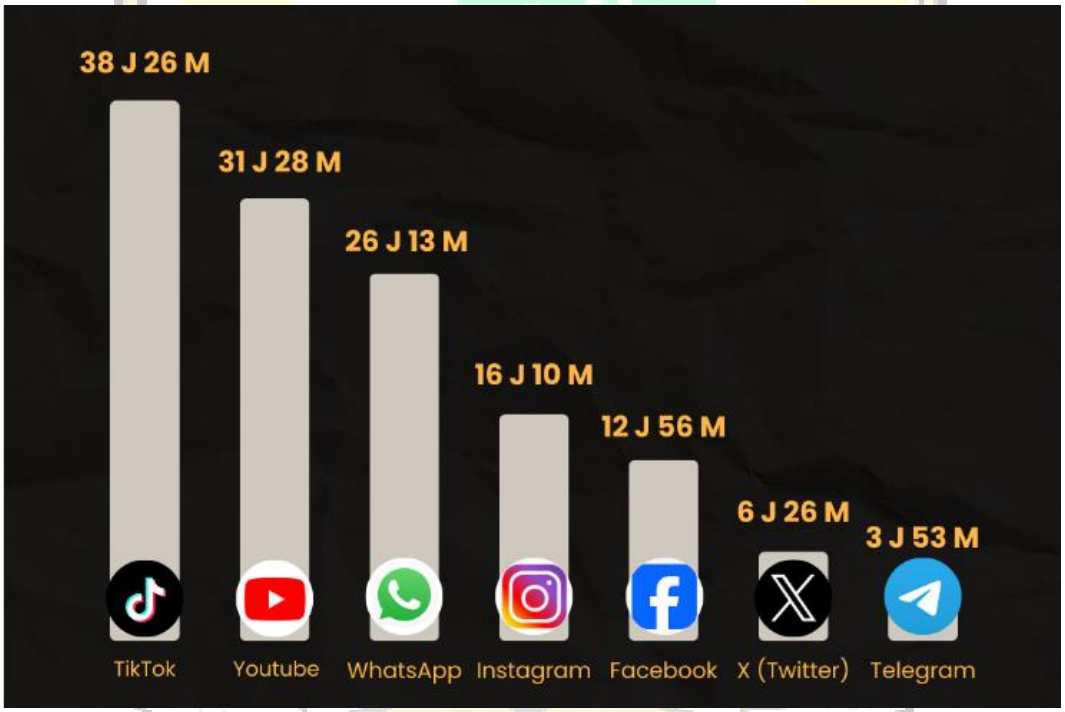
Kerugian yang diakibatkan oleh *phishing* tentunya memiliki dampak yang cukup signifikan khususnya pada dampak finansial. Berdasarkan data yang ada, kasus yang terjadi akibat kejahatan siber mengakibatkan kerugian secara finansial, contohnya Asia Tenggara yang menjadi wilayah dengan rekor tertinggi mengalami kerugian akibat dari *phishing* pada tahun 2024 dengan rata-rata kerugian mencapai angka 3,23 juta dolar Amerika dan angka tersebut mengalami peningkatan sebesar 6% dibandingkan dengan tahun sebelumnya (Fa'izi, 2024).

Kasus lain yang cukup menjadi perhatian adalah kasus ransomware WannaCry yang menjadi perhatian dunia pada tahun 2017. Kasus tersebut menyebar melalui email spam yang memberikan *file* berbahaya yang dapat mengenkripsi *file* pada komputer. Akibat dari serangan tersebut, tercatat sekitar 230.000 komputer yang terserang oleh WannaCry dan diperkirakan kerugian yang dicapai dari kejahatan ini mencapai angka USD 4 miliar dolar Amerika (NP, 2023). Kasus lainnya mengenai email spam pernah terjadi dengan melibatkan Sanford Wallace sebagai pelaku penyebar email spam. Sanford Wallace menyebarkan 27 juta email spam yang berisikan iklan palsu dan promosi produk tanpa izin melalui Facebook. Akibat dari kasus tersebut, Facebook mengalami kerugian sebesar 711 juta dolar (Dent, 2015).

Kerugian yang diperoleh dari kasus-kasus kejahatan siber tersebut tentu menjadi perhatian, mengingat banyaknya pengguna platform elektronik seperti email maupun sosial media di Indonesia. Penggunaan email dan sosial media yang cukup tinggi dikarenakan platform elektronik tersebut sering digunakan oleh masyarakat Indonesia untuk kepentingan formal seperti email dan kepentingan non formal seperti sosial media. Berikut ditampilkan data terkait jumlah pengguna email dan waktu yang dihabiskan per bulan untuk menggunakan sosial media di Indonesia.



Gambar 1. 3 Pengguna Email di Indonesia
(Sumber: Databoks)



Gambar 1. 4 Rata-Rata Waktu Penggunaan Sosial Media di Indonesia Per Bulan
(Sumber: GoodStats)

Berdasarkan **Gambar 1.3**, diketahui bahwa pengguna Gmail saat ini menyentuh angka 81.8 juta pengguna kemudian diikuti dengan Yahoo dengan angka sebesar 43.6 juta dan email perusahaan sebesar 5 juta ("Alamat Email Pengguna Internet di Indonesia," 2016). Sementara itu, **Gambar 1.4** menggambarkan 7 sosial media yang paling sering digunakan oleh masyarakat di Indonesia. Melihat dari tingginya penggunaan email dan sosial media tersebut,

maka potensi dari masyarakat Indonesia untuk terkena dampak dari kejahatan siber juga tinggi. Maka dari itu perlu dilakukan upaya dalam pencegahan kejahatan siber tersebut. Berdasarkan Panduan Penanganan Insiden *Phishing* yang diterbitkan oleh Mahkamah Agung Computer Security Incident Response Team (MA-CSIRT), terdapat beberapa tahapan yang perlu diperhatikan untuk memitigasi dari adanya kejahatan siber, tahapan tersebut meliputi a). persiapan yaitu dengan cara memabangun kontak, menentukan prosedur, dan mengumpulkan informasi serangan. b). identifikasi yaitu dengan cara mendeteksi adanya kejahatan siber, menentukan ruang lingkup, dan melibatkan pihak-pihak untuk menangani kejahatan siber. c). *eradication* yang bertujuan untuk mengentikan kejahatan siber. d). pemulihan yaitu cara agar sistem dapat bekerja secara normal kembali. e). tindak lanjut (MA-CSIRT, 2023).

Adapun beberapa penelitian yang telah dilakukan bertujuan untuk menghadirkan upaya dalam pencegahan dari kejahatan siber dengan menggunakan metode SCP (*Situational Crime Prevention*) yaitu dengan cara mencegah adanya kejahatan siber dengan menggunakan filter spam seperti deteksi intrusi dan memberikan edukasi dini kepada pengguna terhadap bahaya dari kejahatan siber. Tak hanya itu, metode ini juga dapat mengurangi jumlah kejahatan siber dengan cara menggunakan perangkap untuk melacak dari pelaku kejahatan siber (Suzuki & Monroy, 2022).

Melihat dari solusi dalam pencegahan kejahatan siber tersebut, maka pencegahan dari kejahatan siber perlu dilakukan untuk melakukan identifikasi terhadap adanya kejahatan siber dan hal tersebut dapat mencegah seseorang terkena dampak dari kejahatan siber. Hadirnya teknologi kecerdasan buatan dengan *machine learning* memungkinkan kejahatan siber dapat dideteksi secara otomatis mengingat kemampuan *machine learning* yang dapat mempelajari data melalui pola dari data tersebut tanpa di program secara eksplisit (Cholissodin et al., 2019).

Penggunaan *machine learning* untuk melakukan analisis big data telah banyak dilakukan. Hal ini dikarenakan kemampuan *machine learning* dalam

mengolah data kompleks dengan sangat baik karena *machine learning* mampu mengenali hubungan *non-linear* yang sulit diketahui oleh manusia. Salah satu contoh dalam penerapan *machine learning* yaitu penelitian mengenai analisis klasifikasi terhadap Keluarga Sejahtera menunjukkan hasil keakuratan yang baik yaitu sebesar 93,99% (Ninditama, 2021). Penelitian kali ini yang berkaitan dengan upaya pencegahan kasus kejahatan siber menggunakan *machine learning* dilakukan karena kemampuan dari *machine learning* yang mampu menangkap pola dari data yang kompleks. Hal ini tentu menjadi cara yang tepat dalam deteksi kejahatan siber mengingat pola dari kejahatan siber juga bervariasi sehingga dengan begitu sangat tepat apabila mengenali pola bahasa tersebut dengan menggunakan *machine learning*.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini yaitu bagaimana cara melakukan pencegahan terhadap kejahatan siber?

1.3 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian ini diantaranya:

1. Merancang model yang dapat mengenali pola dari kejahatan siber.
2. Mendapatkan model yang dapat mengenali pola dari kejahatan siber.

1.4 Batasan Masalah

Berikut merupakan batasan masalah dalam penelitian ini:

1. Jenis dari kejahatan siber yang akan dideteksi berupa kasus *phishing* melalui media email dan *website* serta kasus spam yang terjadi melalui media email, Facebook, dan Twitter (X)
2. Data yang digunakan diakses pada laman *website* Kaggle.

1.5 Sistematika Penulisan Laporan Penelitian

Sistematika penulisan laporan penelitian adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisikan mengenai latar belakang penelitian, rumusan masalah, tujuan dilakukannya penelitian, batasan masalah, serta sistematika penulisan laporan penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini akan menjelaskan mengenai teori dan literatur yang digunakan dalam penelitian seperti *cyber*-security, cyber-*crime*, AI (*Artificial Intelligent*), *Big Data Analytics*, *machine learning*, jenis-jenis *machine learning*, algoritma *machine learning*, *deep* learning, *Natural Language Processing* (NLP), *Long Short-Term Memory* (LSTM), *Knowladge Disovery from Data* (KDD), bahasa pemrograman Python, Modul *Library* Python, dan lain-lain.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai tahapan dilakukannya penelitian yang dimulai dilakukannya studi pendahuluan, studi pustaka, identifikasi masalah, pemilihan metode, pengumpulan data, pengolahan data, analisis, dan penutup.

BAB IV PENGOLAHAN DATA

Bab ini akan menjelaskan langkah-langkah dalam pengolahan data yang dimulai dari pengumpulan data, pengolahan data, dan pengujian model. Pada tahap pengolahan data, dilakukan dua tahap yaitu preprocessing data dan text mining.

BAB V ANALISIS

Di bab ini, akan dilakukan analisis mendalam berdasarkan proses text mining yang telah dilakukan. Analisis ini membandingkan berbagai kombinasi penggunaan parameter terhadap kinerja model serta membandingkan model dengan beberapa penelitian lain yang serupa. Analisis juga membahas mengenai dampak terhadap lingkungan dari model yang dihasilkan.

BAB VI PENUTUP

Bab ini akan menutup penelitian dengan memberikan kesimpulan dari penelitian yang telah dilakukan serta memberikan saran untuk penelitian mengenai pencegahan kejahatan siber kedepannya.