BAB 1. PENDAHULUAN

1.1 Latar Belakang

Pada tahun 1969, Departemen Pertahanan Amerika Serikat, yaitu U.S. *Defense Advanced Research Projects Agency* (DARPA) yang bekerja sama dengan laboratorium ilmu komputer di Amerika Serikat, Inggris, dan Perancis, sedang membangun jaringan internet. Pada awalnya jaringan internet dikenal dengan nama ARPANET (*Advanced Research Projects Agency Networking*). Kehadirain istilah internet mulai digunakan pada tahun 1990 yang di mana muncul sebagai pengganti dari ARPANET dengan sistem komersialnya yang dikenal sebagai *Internet Service Provider* (ISP), dengan ISP ini lah jaringan internet semakin berkembang pesat dan jauh lebih luas, yang sebelumnya hanya skala nasional hingga menjadi skala internasional dan dapat mencakup keseluruhan negara meskipun kualitas internet tersebut masih lambat pada awalnya (Nurfauzi, A.N., 2022). Seiring berkembangnya zaman, dengan adanya peningkatan sumber daya manusia dan infrastruktur yang memenuhi, internet saat ini menjadi salah satu aspek yang tak dapat dipisahkan dalam kehidupan manusia. Internet menghubungkan setiap pengguna di dunia maya secara global, tidak ada batasan seperti waktu, wilayah maupun *gender*, adapun kelebihan dan kekurangan yang dimiliki internet, salah satu kelebihannya yaitu dapat memudahkan pekerjaan manusia dan memberikan akses ke beragam informasi yang bermanfaat, sedangkan kekurangannya yaitu penggunaan internet untuk melakukan aktivitas yang dapat merugikan orang lain, contohnya *cyber attack* atau serangan siber (Arifin et al., 2024).

Negara Indonesia adalah salah satu negara yang berkembang dan aktif tentang perkembangan teknologi. Selain itu, Indonesia menjadi bagian dari negara yang mendapatkan serangan siber dengan intensitas lumayan tinggi dibandingkan dengan negara-negara seperti di Eropa dan Amerika (Nurfauzi, A.N., 2022). Menurut data hasil laporan monitoring tahunan keamanan siber yang dilansir oleh Badan Siber dan Sandi Negara (BSSN) dengan judul "Lanskap Keamanan Siber Indonesia", laporan tersebut diterbitkan pada situs resmi milik Direktorat Operasi Keamanan Siber BSSN tepatnya pada Id-SIRTII/CC (*Indonesian Security Incident*

Response Team on Internet Infrastructure/ Coordination Center), hasil laporan tersebut menunjukkan bahwa terdapat jumlah serangan siber di Indonesia mencapai 232.447.974 pada tahun 2018, yang kemudian meningkat signifikan menjadi 290.381.283 pada tahun 2019 dan 495.337.202 pada tahun 2020, dan terus meningkat hingga mencapai 1.637.973.022 pada tahun 2021. Namun, pada tahun 2022, jumlah serangan siber mengalami penurunan yang signifikan hingga 40% dengan total serangan menjadi 976.429.996. Penurunan ini disebabkan karena terjadinya penurunan trafik pada sensor yang dipasang di ISP dan penurunan jumlah *Indicator of Compromise* (IoC) yang terdeteksi. Pada tahun 2023, jumlah serangan tercatat 403.990.813, yang meskipun lebih rendah dari tahun sebelumnya, tetapi tetap menunjukkan tingkat aktivitas serangan siber yang masih tergolong tinggi (BSSN, 2023). Berikut adalah grafik jumlah serangan siber di Indonesia dari tahun 2018 hingga 2023:

Gambar 1.1 Grafik Jumlah Serangan Siber

Penurunan jumlah serangan siber pada tahun 2022 hingga 2023 tidak berarti ancaman ini hilang atau berkurang, seperti insiden serangan siber terhadap PT Bank Syariah Indonesia Tbk (BSI) pada tahun 2023 menunjukkan dampak signifikan yang dapat ditimbulkan oleh serangan siber terhadap organisasi besar.

Pada tanggal 8 Mei 2023, PT Bank Syariah Indonesia Tbk (BSI) menjadi salah satu korban dari adanya serangan siber yaitu *ransomware*, sehingga menyebabkan kebocoran data nasabah yang ditandai dengan adanya gangguan pada layanan digital yang dimiliki oleh BSI. Dengan adanya insiden peretasan ini, aktivitias rutin nasabah menjadi terganggu dikarenakan layanan BSI *Mobile*, ATM,

dan *teller* di berbagai kantor cabang mengalami masalah atau *error*. Diketahui bahwa *Dark Tracer*, kelompok *ransomware Lockbit* 3.0 telah mencuri data nasabah sebanyak 15 juta, sekitar 1,5 *terabyte* data dalam sistem BSI, termasuk data informasi karyawan. Data yang bocor meliputi nama, alamat, nomor ponsel, saldo rekening, riwayat transaksi, tanggal pembukaan rekening, serta informasi penting lainnya. Kelompok tersebut memberikan ancaman terhadap pihak BSI dengan menyatakan bahwa data-data informasi yang telah dicuri akan disebar jika pihak BSI tidak menebus uang sebesar Rp295,61 miliar. Insiden ini tentunya menimbulkan kekhawatiran di kalangan nasabah BSI karena adanya pencurian data pribadi nasabah (Ma'rifa, H.S.F., 2023).

Gunawan A. Hartoyo, selaku sekertaris perusahaan BSI menegaskan bahwa beberapa hari setelah insiden kebocoran data, informasi dan dana nasabah BSI tetap dalam keadaan aman. BSI akan terus mengambil langkah-langkah preventif atau antisipasi mencegah terjadinya sesuatu untuk memperkuat sistem keamanan teknologi informasi dari potensi gangguan data, dengan peningkatan proteksi dan ketahanan sistem. Secara bersamaan, BSI melakukan investigasi internal dan terus berkoordinasi dengan berbagai pihak terkait, termasuk Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), Bank Indonesia (BI), serta instansi lainnya (Ma'rifa, H.S.F., 2023). Perlu disadari bahwa insiden ini menyoroti pentingnya sistem keamanan yang kuat dan perlunya sistem deteksi dini terhadap serangan siber atau *cyber attack*.

Serangan siber atau *cyber attack* adalah salah satu kegiatan kriminal yang dilakukan dengan cara memanfaatkan teknologi komputer sebagai alat kejahatan utama dan memanfaatkan kemajuan teknologi khususnya internet. Dengan adanya penggunaan teknologi sehari-hari, serangan siber menjadi salah satu ancaman yang nyata, ancaman yang diakibatkan sangat tidak main-main, dari perusakan data hingga manipulasi informasi data kita, penjahat siber menargetkan penyerangan terhadap data yang berisi informasi sensitif, yang nilainya akan semakin berharga seiring dengan meningkatnya kerahasiaan data (Saragih, N.R., 2022). Berbagai jenis serangan siber, seperti *Malware*, *Ransomware*, *Phising*, *Trojan Horses*, hingga *Worms*, semua jenis-jenis serangan tersebut memiliki tujuan untuk melakukan

tindakan pencurian informasi, memanipulasikan data, pencurian identitas dan gangguan layanan yang dapat menimbulkan kerugian finansial signifikan bagi individu ataupun organisasi (Saragih, N.R., 2022). Karena masih banyak pengguna yang minim akan pengetahuan terhadap keamanan informasi data pribadi terhadap teknologi, maka akan menjadi salah satu faktor utama penyebab terjadinya serangan siber, oleh karena itu diperlukan suatu sistem pakar yang dapat mengidentifikasi jenis serangan siber pada komputer dan cara penanganannya, sehingga pengguna dapat melakukan analisa secara mandiri tanpa memerlukan bantuan dari ahli.

Sistem pakar adalah sistem yang mengadopsi pengetahuan dari seorang ahli atau pakar pada bidang tertentu ke dalam komputer yang menggabungkan dasar pengetahuan (*knowledge base*) dengan sistem inferensi untuk menggantikan fungsi seorang pakar dalam menyelesaikan suatu suatu permasalahan (Arifin et al., 2024).

Adapun penelitian terdahulu yang menjadi rujukan dalam penelitian ini mengenai sistem pakar jenis serangan siber dengan judul Sistem Pakar Diagnosa *Phising* Dengan Metode *Certainty Factor* Berbasis *Web,* sistem tersebut mampu memperoleh nilai dari hasil pengujian aplikasi sebesar 85,1%. Pada penelitian selanjutnya yang berjudul Deteksi Serangan *Malware* Pada *Cloud Server* Menggunakan Metode *Anomaly Base* menghasilkan akurasi sebesar 47,30%, precision sebesar 93,47%, *recall* sebesar 47,05%, dan *f1-score* sebesar 62,59%. Pada penelitian ini menggunakan jenis – jenis serangan siber secara umum sebagai objek dan menggunakan *Certainty Factor* sebagai metodenya, yang di harapkan mampu untuk membantu pengguna dalam mengetahui dan mengidentifikasi jenis serangan siber pada komputer serta memberikan solusi terkait cara penanganannya.

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang di atas, terdapat beberapa rumusan masalah dalam penelitian ini, yaitu:

1) Bagaimana menentukan indikasi-indikasi yang diperlukan untuk membedakan jenis serangan siber yang berbeda?
2) Bagaimana merumuskan aturan (*rule*) berdasarkan pengetahuan pakar yang dipindahkan ke dalam sistem pakar?

3) Bagaimana mengimplementasikan mesin inferensi yang efektif untuk mendeteksi jenis serangan siber menggunakan metode *Certainty Factor*?
4) Bagaimana cara menerapkan metode *Certainty Factor* yang tepat untuk sistem pakar deteksi dini jenis serangan siber pada komputer?

1.3 Tujuan

Berdasarkan uraian rumusan masalah di atas, terdapat beberapa tujuan dari penelitian ini, yaitu:

1) Menetapkan indikasi-indikasi yang diperlukan untuk membedakan jenis-jenis serangan siber yang berbeda dengan mempertimbangkan berbagai karakteristik dan pola yang terkait.
2) Merumuskan aturan (*rule*) berdasarkan pengetahuan pakar yang dipindahkan ke dalam sistem pakar untuk memungkinkan identifikasi dan penanganan serangan siber dengan tepat dan efektif.
3) Mengimplementasikan mesin inferensi yang efektif untuk mendeteksi jenis serangan siber dengan menggunakan metode *Certainty Factor*.
4) Mengimplementasikan metode *Certainty Factor* secara tepat dalam pengembangan sistem pakar untuk deteksi dini jenis serangan siber pada komputer guna meningkatkan akurasi dan keandalan sistem.

1.4 Manfaat

Berdasarkan uraian tujuan di atas, terdapat manfaat yang diharapkan dalam penelitian ini, yaitu:

1) Dapat membantu para pengguna mengetahui jenis serangan siber pada komputer dengan menggunakan sistem pakar.
2) Dapat membantu para pengguna dalam mengidentifikasi, memberikan solusi, dan mengatasi jenis serangan siber pada komputer tanpa harus menemui seorang ahli.
3) Dapat membantu meningkatkan kesadaran dan pemahaman masyarakat tentang ancaman serangan siber.