BAB I
PENDAHULUAN

1.1 Latar Belakang

Kerentanan dalam konteks keamanan sistem didefinisikan sebagai kelemahan atau cacat dalam prosedur keamanan, desain, implementasi, atau kontrol internal yang dapat dieksploitasi, baik secara tidak sengaja maupun sengaja, yang dapat mengakibatkan pelanggaran keamanan atau pelanggaran terhadap kebijakan keamanan sistem. Dalam beberapa tahun terakhir, jumlah kerentanan yang teridentifikasi telah meningkat secara signifikan, dengan data dari dari BSSN juga menunjukkan bahwa potensi ancaman siber diperkirakan akan terus meningkat dengan berbagai jenis serangan seperti *ransomware, malware*, dan serangan DDoS yang semakin umum (Situs Resmi BSSN, 2024). Peningkatan jumlah kerentanan ini sebagian besar disebabkan oleh kemampuan deteksi yang lebih baik, di mana perusahaan kini lebih mampu mengidentifikasi potensi ancaman melalui teknologi berbasis cloud dan alat yang didukung AI. Namun, meskipun jumlah kerentanan meningkat, tidak semua kerentanan yang terdaftar memiliki tingkat risiko yang sama. Penyerang kini lebih fokus pada kerentanan yang paling dapat dieksploitasi, yang sering kali tidak termasuk dalam kategori kerentanan kritis (Situs Resmi NVD, 2024). Ini menunjukkan tren yang mengkhawatirkan dalam keamanan siber, di mana kerentanan yang ada semakin banyak dieksploitasi oleh pelaku kejahatan siber. Hal ini menunjukkan perlunya mengubah data kerentanan yang besar ini menjadi informasi yang dapat ditindaklanjuti untuk meningkatkan keamanan sistem.

Analisis tren kerentanan menjadi penting untuk memahami bagaimana jumlah kerentanan bervariasi dari waktu ke waktu, berdasarkan tingkat keparahan dan klasifikasi kerentanan. Penelitian ini bertujuan untuk menganalisis tren kerentanan dengan data yang terklasifikasi, serta mengidentifikasi kelas kerentanan yang mengikuti tren umum dan yang menyimpang dari tren tersebut. Dengan pemahaman yang lebih baik tentang karakteristik dampak dasar dari kelas kerentanan, administrator sistem dapat

membuat keputusan yang lebih tepat dalam merancang kebijakan keamanan dan mekanisme pencegahan kerentanan.

Sumber data utama untuk analisis kerentanan adalah *Common Vulnerabilities and Exposures* (CVE) yang dikelola oleh MITRE dari 5 tahun sebelumnya yaitu dari Tahun 2020 hingga 2024. CVE menyediakan nama umum untuk masalah keamanan yang dikenal secara publik, yang memudahkan berbagi data di antara berbagai alat dan repositori kerentanan. Untuk menganalisis tren kerentanan secara lebih efektif, pendekatan yang digunakan adalah model ARIMA (*Autoregressive Integrated Moving Average*). Model ini memungkinkan analisis deret waktu untuk memprediksi dan memahami pola perkembangan kerentanan dari waktu ke waktu. Dengan menggunakan ARIMA, kita dapat mengidentifikasi tren yang signifikan dan membuat proyeksi yang lebih akurat mengenai kerentanan di masa depan, sehingga memberikan wawasan yang lebih baik bagi para profesional keamanan dalam merencanakan langkah-langkah mitigasi yang tepat (Ampatzoglou, A. 2021).

Salah satu studi yang relevan adalah penelitian oleh Alazab et al. (2022), yang menunjukkan bagaimana ARIMA dapat digunakan untuk memprediksi tren dalam data yang kompleks, termasuk dalam konteks epidemiologi. Meskipun fokus utama penelitian tersebut adalah pada prediksi kasus COVID-19, metodologi yang digunakan dapat diterapkan pada analisis tren kerentanan. Dalam studi ini, ARIMA digunakan untuk menganalisis data historis dan menghasilkan proyeksi yang dapat membantu dalam pengambilan keputusan. Hasilnya menunjukkan bahwa model ARIMA mampu menangkap pola yang ada dalam data dan memberikan prediksi yang dapat diandalkan.

Keunggulan ARIMA terletak pada kemampuannya untuk menangani data yang tidak stasioner dengan melakukan *differencing*, yang membantu menghilangkan tren dan membuat data lebih stabil. Ini sangat penting dalam analisis kerentanan, di mana fluktuasi jumlah kerentanan dapat dipengaruhi oleh berbagai faktor eksternal, seperti rilis perangkat lunak baru atau

peningkatan kesadaran keamanan. Dengan menggunakan ARIMA, para peneliti dapat mengidentifikasi tren yang signifikan dan membuat proyeksi yang lebih akurat mengenai kerentanan di masa depan.

Selain itu, ARIMA juga memungkinkan analisis residual yang mendalam, yang membantu dalam mengevaluasi kecocokan model. Dengan memeriksa residual, peneliti dapat mengidentifikasi pola yang tidak terdeteksi oleh model, memberikan wawasan tambahan tentang faktor-faktor yang mempengaruhi kerentanan. Penelitian oleh Ampatzoglou (2021) juga mendukung penggunaan ARIMA dalam konteks analisis kerentanan, menunjukkan bahwa model ini dapat memberikan hasil yang lebih baik dalam memodelkan data kerentanan yang kompleks dan berfluktuasi.

Secara keseluruhan, penggunaan model ARIMA dalam analisis tren kerentanan memberikan pendekatan yang kuat dan efektif untuk memahami dan memprediksi pola kerentanan dari waktu ke waktu. Dengan dukungan dari penelitian terbaru, jelas bahwa ARIMA adalah alat yang berharga bagi para profesional keamanan dalam merencanakan langkah-langkah mitigasi yang tepat dan memahami dinamika kerentanan yang terus berkembang.

Penelitian sebelumnya telah menganalisis distribusi jenis kerentanan dalam CVE, dengan fokus pada 15 jenis kerentanan yang paling umum, seperti masalah otentikasi, *buffer overflow*, kesalahan kriptografi, dan SQL *injection*. Penelitian-penelitian ini umumnya menggunakan analisis frekuensi dan metrik dasar CVSS untuk mengevaluasi dampak dan prevalensi jenis kerentanan tersebut. Hasil dari analisis ini diharapkan dapat memberikan wawasan yang berguna bagi para profesional TI dan keamanan dalam pengembangan perangkat lunak, solusi antivirus, dan strategi keamanan TI.

Namun, penelitian ini mengambil pendekatan yang lebih inovatif dengan menggunakan model ARIMA untuk menganalisis tren kerentanan berdasarkan data terbaru dari CVE. Dengan memanfaatkan data yang lebih mutakhir dan teknik analisis deret waktu, penelitian ini bertujuan untuk

memberikan pemahaman yang lebih mendalam tentang pola perkembangan kerentanan dari waktu ke waktu. Penggunaan model ARIMA memungkinkan identifikasi tren yang lebih akurat dan proyeksi yang lebih baik mengenai kerentanan di masa depan, yang dapat membantu para profesional keamanan dalam merencanakan langkah-langkah mitigasi yang lebih efektif. Dengan demikian, penelitian ini tidak hanya memperbarui analisis kerentanan yang ada, tetapi juga menawarkan metode yang lebih canggih dan relevan untuk menghadapi tantangan keamanan yang terus berkembang.

Secara keseluruhan, pemahaman tentang tren kerentanan dan klasifikasi yang tepat dapat membantu administrator keamanan dalam merancang kebijakan yang lebih efektif dan mengidentifikasi kombinasi mekanisme pencegahan kerentanan yang tepat untuk melindungi sistem dari serangan yang mungkin terjadi.

1.2 Rumusan Masalah

Pertanyaan penelitian utama yang akan dijawab dalam penelitian ini adalah, "Bagaimana model ARIMA dapat digunakan untuk menganalisis dan memprediksi tren kerentanan dalam data CVE yang terbaru?"

Untuk mendalami pertanyaan utama tersebut, beberapa sub pertanyaan yang akan dijadikan fokus dalam penelitian ini adalah sebagai berikut :

a. Bagaimana karakteristik data kerentanan yang terdapat dalam CVE dan bagaimana data tersebut berfluktuasi dari waktu ke waktu?
b. Apa saja jenis kerentanan yang paling umum dan bagaimana distribusinya dalam periode waktu tertentu?

1.3 Tujuan Tugas Akhir

Tujuan penelitian ini adalah untuk memberikan pemahaman yang lebih mendalam mengenai penggunaan model ARIMA dalam analisis dan prediksi tren kerentanan yang terdapat dalam data CVE terbaru. Secara spesifik, tujuan penelitian ini dapat dirinci sebagai berikut :

a. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis karakteristik data kerentanan yang terdapat dalam CVE, serta memahami fluktuasi data tersebut dari waktu ke waktu. Dengan demikian, diharapkan dapat diperoleh gambaran yang jelas mengenai pola dan dinamika kerentanan yang ada.
b. Penelitian ini juga bertujuan untuk mengidentifikasi jenis-jenis kerentanan yang paling umum dan menganalisis distribusinya dalam periode waktu tertentu. Hal ini penting untuk memahami tren yang ada dan untuk memberikan informasi yang relevan bagi para profesional keamanan TI dalam mengembangkan strategi mitigasi.

1.4 Manfaat Tugas Akhir

Penelitian ini diharapkan dapat memberikan manfaat yang signifikan bagi berbagai pihak yang terkait, termasuk organisasi, profesional keamanan TI, dan peneliti di bidang keamanan siber.

1. Bagi organisasi dan perusahaan, hasil penelitian ini dapat memberikan wawasan yang lebih mendalam tentang tren kerentanan yang ada dalam data CVE. Dengan memahami karakteristik dan distribusi jenis kerentanan yang paling umum, organisasi dapat mengembangkan strategi mitigasi yang lebih efektif dan responsif terhadap ancaman keamanan. Ini akan membantu mereka dalam mengalokasikan sumber daya secara lebih efisien dan meningkatkan postur keamanan mereka secara keseluruhan.
2. Bagi profesional keamanan TI, penelitian ini dapat menjadi sumber informasi yang berharga dalam pengambilan keputusan terkait pengembangan perangkat lunak dan implementasi solusi keamanan. Dengan memanfaatkan hasil analisis tren kerentanan, mereka dapat merancang langkah-langkah pencegahan yang lebih tepat dan memprioritaskan tindakan mitigasi berdasarkan jenis kerentanan yang paling relevan. Ini akan meningkatkan kemampuan mereka dalam melindungi sistem dan data dari potensi ancaman.

3. Bagi komunitas akademis dan peneliti serupa, penelitian ini dapat memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang keamanan siber. Dengan menggunakan model ARIMA dan data terbaru, penelitian ini dapat menjadi referensi bagi studi-studi selanjutnya yang ingin mengeksplorasi metode analisis deret waktu dalam konteks kerentanan. Hasil penelitian ini juga dapat mendorong penelitian lebih lanjut yang menggabungkan teknik analisis lain untuk mendapatkan pemahaman yang lebih komprehensif tentang tren kerentanan.

Secara keseluruhan, penelitian ini diharapkan dapat memberikan manfaat yang luas dan berkelanjutan bagi berbagai pihak, dengan tujuan akhir meningkatkan keamanan siber dan mengurangi risiko yang dihadapi oleh organisasi dan individu di era digital yang terus berkembang.

1.5 Batasan dan Asumsi Tugas Akhir

Batasan penelitian ini mencakup beberapa aspek yang perlu diperhatikan untuk memberikan konteks dan mengatur ruang lingkup analisis. Pertama, data yang digunakan dalam penelitian ini terbatas pada periode tahun 2020 hingga 2024. Keterbatasan ini berarti bahwa analisis hanya mencakup kerentanan yang terdaftar dalam database CVE selama periode tersebut, sehingga tidak mencakup kerentanan yang mungkin muncul sebelum tahun 2020 atau yang akan muncul setelah 2024.

Kedua, penelitian ini menggunakan model ARIMA sebagai metode tunggal untuk analisis dan prediksi tren kerentanan. Meskipun ARIMA memiliki keunggulan dalam analisis deret waktu, penggunaan metode ini sebagai satu-satunya pendekatan dapat membatasi pemahaman yang lebih luas tentang kerentanan, karena metode lain, seperti model pembelajaran mesin atau teknik statistik lainnya, mungkin dapat memberikan hasil yang lebih baik dalam konteks tertentu.

Ketiga, waktu penelitian juga menjadi batasan, mengingat data kerentanan terus diperbarui dalam database CVE. Dengan adanya pembaruan yang terus-menerus, ada kemungkinan bahwa hasil penelitian ini dapat sedikit bias atau tidak sepenuhnya mencerminkan kondisi terkini dari tren kerentanan. Oleh

karena itu, penting untuk mempertimbangkan bahwa hasil analisis ini mungkin hanya relevan untuk periode waktu yang diteliti dan dapat berubah seiring dengan munculnya data baru.

Dengan menyadari batasan-batasan ini, penelitian ini bertujuan untuk memberikan pemahaman yang lebih baik tentang tren kerentanan dalam data CVE, meskipun dengan keterbatasan yang ada.

1.6 Sistematika Laporan

BAB I – PENDAHULUAN

Bab ini menjelaskan latar belakang masalah, rumusan masalah, tujuan, batasan, serta manfaat dari penelitian. Disajikan juga justifikasi pentingnya menganalisis tren kerentanan keamanan informasi menggunakan data CVE dan model ARIMA. Bab ini membantu pembaca memahami konteks dan urgensi penelitian, serta ruang lingkup yang ditetapkan peneliti.

BAB II – LANDASAN TEORI

Berisi uraian tentang penelitian terdahulu yang relevan, landasan teori terkait kerentanan sistem informasi, serta alasan pemilihan metode ARIMA dibandingkan pendekatan lain. Penjabaran ini memperkuat posisi penelitian dalam konteks akademik dan memperjelas kontribusi orisinalnya.

BAB III – METODE PENYELESAIAN MASALAH

Bab ini menyajikan langkah-langkah penyelesaian masalah mulai dari studi literatur, pengumpulan dan pengolahan data, hingga analisis model. Penggunaan ARIMA diuraikan secara teknis, termasuk proses pembersihan dan transformasi data, identifikasi parameter, serta evaluasi model. Bab ini membantu pembaca memahami prosedur ilmiah yang digunakan untuk mencapai tujuan penelitian.

BAB IV – PENGOLAHAN DATA DAN ANALISIS HASIL

Membahas hasil pemodelan tren kerentanan berdasarkan data CVE periode 2020–2024. Ditampilkan analisis statistik awal, hasil penerapan model ARIMA, evaluasi residual dan akurasi model, serta analisis tren jenis kerentanan berdasarkan kode CWE. Bab ini juga menguraikan strategi mitigasi berdasarkan hasil analisis. Dengan struktur ini, pembaca diajak melihat bagaimana data mentah diproses menjadi wawasan yang dapat ditindaklanjuti.

BAB V – KESIMPULAN DAN SARAN

Bab ini merangkum hasil utama penelitian dan implikasinya terhadap keamanan siber, serta memberikan saran untuk penelitian selanjutnya. Kesimpulan merujuk langsung pada rumusan masalah dan menunjukkan bagaimana model ARIMA dapat memberikan prediksi yang dapat diandalkan dalam konteks keamanan informasi.