BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi yang pesat meningkatkan ketergantungan terhadap layanan berbasis web di berbagai sektor, seperti pemerintahan, bisnis, pendidikan, dan hiburan. Namun, peningkatan ini juga diiringi dengan ancaman siber yang semakin kompleks, salah satunya adalah serangan Distributed Denial of Service (DDoS). Studi yang dilakukan oleh Wang et al (2019), menyatakan bahwa serangan DDoS telah mengalami peningkatan signifikan dari segi skala dan kompleksitas, terutama dengan adanya kemunculan berbagai vektor serangan baru yang memanfaatkan kelemahan pada protokol jaringan. Studi ini menunjukkan bahwa DDoS tidak hanya meningkat dalam frekuensi, namun juga dalam variasi serangan yang mampu menargetkan lapisan aplikasi dan infrastruktur secara bersamaan. Serangan DDoS bertujuan untuk melumpuhkan layanan dengan membanjiri server menggunakan lalu lintas palsu dalam jumlah besar. Akibatnya, seperti pada laporan yang disampaikan oleh Abhishta et al (2019), layanan menjadi lambat, tidak responsif, serta dapat mengganggu operasi platform online seperti pertukaran kripto dengan menurunkan volume perdagangan dan menyebabkan ketidaktersediaan layanan meskipun pemulihan sering terjadi dalam satu hari atau bahkan tidak dapat diakses sama sekali. Banyak perangkat yang memiliki sistem keamanan lemah, sehingga mudah diretas dan dijadikan bagian dari botnet untuk melancarkan serangan DDoS.

Kemudahan dalam menyewa layanan DDoS-as-a-Service kini tidak hanya dilakukan oleh peretas berpengalaman, tetapi juga dapat dilakukan oleh individu dengan kemampuan teknis rendah melalui layanan DDoS-as-a-Service yang tersedia di *dark web*. Pada penelitian yang dilakukan oleh Cho et al (2019), menjelaskan bahwa terdapat banyak kesamaan pada setiap organisasi yang masih menggunakan metode deteksi serangan yang reaktif yaitu, hanya merespons setelah serangan terjadi, bukan mencegahnya sejak dini. Dampak dari Serangan DDoS

tidak hanya mengganggu layanan tetapi juga memiliki dampak yang luas seperti pada laporan oleh Zayo DDoS Insights Report (2024), rata-rata kerugian bisnis akibat serangan sekitar 68 menit mencapai US $408,000, menandakan bahwa setiap menit *downtime* dihargai US $6,000. Kerusakan reputasi website yang sering mengalami *downtime* akan kehilangan kepercayaan pelanggan dan pengguna serta gangguan operasional yang dapat melumpuhkan layanan penting seperti sistem perbankan, layanan kesehatan digital, hingga infrastruktur kritikal. Menurut Netscout (2023), serangan DDoS menunjukkan kekuatan meningkat secara signifikan, terjadi lebih dari 9,75 juta insiden pada tahun 2021, dan mencapai sekitar 7,9 juta serangan di awal tahun 2023. Menurut hasil literatur internasional dari studi Shaikh et al (2023), sektor pendidikan memang mengalami lonjakan signifikan dalam serangan DDoS setelah pandemi COVID-19. Disebutkan bahwa lebih dari 95% infrastruktur IT institusi pendidikan tidak siap menghadapi serangan cyber saat e-learning diterapkan secara penuh.

Fenomena ini juga disebabkan oleh meningkatnya perangkat internet yang tidak dilengkapi dengan sistem keamanan yang cukup. Gelgi et al (2024), mengungkapkan bahwa banyak perangkat pintar saat ini menjadi target mudah untuk diretas dan dimanfaatkan dalam botnet. Sebagai hasilnya, kerugian global yang disebabkan oleh serangan DDoS mengalami peningkatan yang signifikan. Sebaliknya, riset dari Aladaileh (2022), menemukan bahwa penggunaan batas dinamis yang didasarkan pada metode statistik seperti EWMA dapat meningkatkan tingkat deteksi hingga 96% dengan jumlah false positive yang sedikit. Pendekatan ini dianggap lebih efektif dibandingkan dengan metode berbasis machine learning yang memerlukan pelatihan ulang data. Studi Jiang et al (2019), juga menyoroti bahwa penerapan algoritma statistik dasar untuk thresholding mampu memberikan deteksi cepat dengan latensi di bawah satu detik, menjadikannya pilihan yang tepat dalam sistem pemantauan waktu nyata.

Saat ini, beberapa teknologi deteksi DDoS telah dikembangkan, seperti penggunaan machine learning, behavioral analysis, dan rate-limiting. Namun, teknologi ini masih memiliki keterbatasan dalam memberikan respons yang efisien secara real-time (Gaur et al, 2025). Oleh karena itu, metode Threshold-Based

Detection dan Filtering muncul sebagai pendekatan alternatif yang menjanjikan. Metode ini bekerja dengan menetapkan ambang batas lalu lintas jaringan berdasarkan data historis, sehingga dapat mendeteksi anomali dengan akurasi yang lebih tinggi. Metode ini bekerja dengan menetapkan ambang batas (*threshold*) tertentu berdasarkan lalu lintas jaringan yang normal. Ketika jumlah lalu lintas melampaui ambang batas tersebut, sistem akan mengidentifikasinya sebagai anomali yang dapat mengindikasikan serangan DDoS. Setelah itu, proses filtering dilakukan untuk menyaring lalu lintas palsu, sehingga hanya lalu lintas yang valid yang diteruskan ke server. Jika dilihat hasil dari akurasi tinggi penetapan ambang batas yang dioptimalkan menurut Bojović et al (2018), bisa menggunakan data historis memungkinkan pengurangan kesalahan dalam deteksi (false positives dan false negatives). Implementasi yang sederhana tidak memerlukan algoritma yang kompleks untuk menghadapi ancaman ini. Metode kombinasi Threshold-Based Detection dan Filtering menjadi salah satu pendekatan yang baru. Metode ini bekerja dengan menetapkan ambang batas lalu lintas jaringan untuk mendeteksi anomali yang mengindikasikan serangan. Ambang batas ini dioptimalkan berdasarkan analisis data historis, sehingga dapat memberikan deteksi yang lebih akurat. Penelitian ini bertujuan untuk mengembangkan sistem monitoring dan mitigasi DDoS yang mengintegrasikan metode Threshold-Based Detection dan Filtering secara real-time guna meningkatkan efisiensi deteksi dan respons yang signifikan terhadap serangan. Hasil penelitian ini diharapkan dapat menjaga stabilitas layanan web, mengurangi risiko kerugian finansial secara signifikan, serta meningkatkan kepercayaan pengguna.

1.2. Identifikasi Masalah

Berdasarkan latar belakang di atas, terdapat beberapa masalah yang dapat diidentifikasi:

1. Serangan DDoS terus meningkat baik dari segi frekuensi maupun kompleksitasnya, yang mengancam keberlangsungan layanan berbasis web.
2. Sebagian besar sistem mitigasi yang tersedia masih kurang optimal dalam memberikan perlindungan secara real-time.

3. Sebagian besar penelitian dan sistem yang ada hanya menerapkan salah satu pendekatan, yakni antara Threshold-Based Detection saja atau Filtering saja, tanpa mengkombinasikan keduanya secara terintegrasi.

1.3. Rumusan Masalah

Berdasarkan identifikasi masalah, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana merancang dan membangun sistem yang dapat memonitor lalu lintas jaringan dan mendeteksi serangan DDoS secara real-time ?
2. Bagaimana mengimplementasikan metode Threshold-Based Detection dan Filtering untuk mitigasi serangan DDoS pada website ?
3. Sejauh mana evaluasi sistem yang dikembangkan dalam mendeteksi dan melakukan mitigasi serangan DDoS secara real-time ?

1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Merancang dan membangun sistem yang dapat memonitor lalu lintas jaringan dan mendeteksi serangan DDoS secara real-time.
2. Mengimplementasikan metode Threshold-Based Detection dan Filtering sebagai solusi mitigasi serangan DDoS.
3. Mengevaluasi kinerja sistem dalam mendeteksi dan melakukan mitigasi serangan DDoS untuk memastikan keandalannya.

1.5. Manfaat Penelitian

Sub bab ini menguraikan manfaat yang diharapkan dari penelitian yang dilakukan, baik secara teoritis maupun praktis, sebagai kontribusi terhadap pengembangan ilmu pengetahuan dan pemecahan masalah yang diteliti.

1. Manfaat Teoritis
   a. Memberikan Kontribusi ilmiah dalam pengembangan metode deteksi dan mitigasi serangan DDoS Berbasis Threshold-Based Detection dan Filtering.
   b. Memperkaya referensi di bidang keamanan jaringan, khususnya terkait pengembangan teknologi mitigasi serangan siber jaringan.

2. Manfaat Praktis
   a. Membantu administrator server web dalam mengidentifikasi serangan DDoS dengan lebih cepat dan akurat.
   b. Menyediakan solusi sistem yang dapat diimplementasikan dengan mudah untuk menjaga keandalan layanan berbasis web.
   c. Mengurangi potensi kerugian finansial yang diakibatkan oleh *downtime* layanan akibat serangan DDoS.
   d. Memperbaiki pengalaman pengguna dengan menjaga ketersediaan layanan secara optimal.

1.6. Sistematika Penulisan Laporan

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakang penelitian yang menyoroti meningkatnya ancaman serangan DDoS terhadap website, pentingnya mitigasi serangan secara real-time, serta urgensi penerapan metode Threshold-Based Detection dan Filtering. Selain itu, bab ini juga mencakup identifikasi masalah, rumusan masalah, tujuan penelitian, manfaat teoritis dan praktis, serta sistematika penulisan laporan.

BAB 2 TINJAUAN PUSTAKA

Bab ini berisi studi literatur mengenai penelitian terdahulu yang berkaitan dengan metode deteksi dan mitigasi DDoS, konsep dasar serangan DDoS, dampak serangan terhadap perusahaan, serta metode deteksi dan mitigasi yang telah dikembangkan. Selain itu, dibahas pula teknologi yang digunakan dalam real-time monitoring serta sistem pendukung yang dapat membantu implementasi penelitian ini.

BAB III METODE PENELITIAN

Bab ini menguraikan pendekatan penelitian yang digunakan, tahapan penelitian yang meliputi analisis kebutuhan, perancangan sistem, implementasi, serta pengujian. Metode pengumpulan data, analisis sistem yang sudah ada, serta metode analisis data juga dijelaskan dalam bagian ini.

Selain itu, dibahas pula estimasi kerugian yang dapat dicegah dengan metode yang dikembangkan serta validasi dan evaluasi sistem.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil implementasi sistem monitoring dan mitigasi serangan DDoS menggunakan metode Threshold-Based Detection dan Filtering. Hasil pengujian sistem dibandingkan dengan metode lain yang telah ada untuk mengevaluasi keunggulan pendekatan yang diusulkan. Pembahasan dilakukan dengan menganalisis efektivitas sistem dalam mendeteksi dan mengurangi dampak serangan DDoS secara real-time.

BAB V KESIMPULAN DAN SARAN

Bab terakhir berisi kesimpulan dari penelitian yang mencakup pencapaian tujuan penelitian, evaluasi metode yang diterapkan, serta rekomendasi untuk pengembangan lebih lanjut. Saran diberikan untuk perbaikan sistem dan potensi penelitian lanjutan dalam bidang mitigasi serangan siber.

DAFTAR PUSTAKA

Bagian ini berisi referensi yang digunakan dalam penelitian, termasuk jurnal ilmiah, buku, serta sumber terpercaya lainnya yang mendukung kajian dan pengembangan sistem.