Penerapan Relasi Rekurens untuk Menganalisis Pola Serangan *Distributed Denial of Service* (DDoS)

Filbert Engyo - 13523163[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]filbert.engyo7@gmail.com, 13523163@std.stei.itb.ac.id

***Abstract*—Perkembangan teknologi yang pesat telah membawa perubahan signifikan dalam kehidupan modern, dengan adopsi luas interaksi dan transaksi berbasis internet yang merevolusi cara manusia menjalankan aktivitas sehari-hari, baik secara individu maupun dalam konteks bisnis. Teknologi jaringan komputer, sebagai tulang punggung berbagai layanan digital, memungkinkan terciptanya efisiensi dan aksesibilitas yang belum pernah terjadi sebelumnya. Namun, kemajuan ini juga menghadirkan tantangan besar berupa ancaman keamanan siber, khususnya serangan *Distributed Denial of Service* (DDoS), yang bertujuan merusak layanan dengan membanjiri sistem menggunakan lalu lintas berlebihan. Serangan ini berdampak luas, mulai dari kerugian finansial hingga hilangnya reputasi dan kepercayaan pengguna. Dengan meningkatnya skala dan kompleksitas serangan DDoS, pendekatan konvensional sering kali tidak memadai dalam mendeteksi pola serangan baru yang terus berevolusi. Oleh karena itu, diperlukan solusi inovatif seperti penerapan relasi rekurens, sebuah kerangka matematis yang mampu menganalisis pola serangan secara iteratif dan terstruktur. Pendekatan ini memungkinkan identifikasi dan prediksi pola serangan yang lebih akurat berdasarkan data historis, termasuk pola linier, eksponensial, dan stokastik yang mencerminkan dinamika serangan nyata. Hasil penelitian menunjukkan bahwa penerapan relasi rekurens dapat melengkapi metode konvensional dengan memberikan wawasan mendalam mengenai karakteristik serangan, sehingga membantu dalam pengambilan keputusan yang lebih efektif untuk mitigasi. Dengan demikian, pendekatan ini menawarkan potensi besar untuk menghadapi ancaman siber yang semakin kompleks, sekaligus menjadi landasan bagi pengembangan solusi keamanan siber yang lebih adaptif dan inovatif di masa depan.**

***Keywords*—keamanan siber, interaksi, *Distributed Denial of Service* (DDoS), relasi rekurens**

I. Pendahuluan

Tidak dapat dipungkiri bahwa perkembangan teknologi di masa kini sedang berada pada masa keemasannya, dengan adopsi teknologi yang semakin merata di berbagai aspek kehidupan. Kompetisi yang semakin sengit antar perusahaan teknologi mendorong inovasi tiada henti, di mana setiap perusahaan berlomba-lomba menciptakan solusi terbaik demi menguasai pasar global. Inovasi ini tidak hanya bertujuan untuk meningkatkan efisiensi dan produktivitas, tetapi juga untuk memberikan dampak positif terhadap kualitas hidup manusia. Dengan demikian, teknologi tidak hanya menjadi alat, tetapi juga menjadi fondasi yang menopang berbagai aspek kehidupan modern.

Salah satu bentuk implementasi teknologi yang kini hampir tak terpisahkan dari kehidupan sehari-hari adalah interaksi dan transaksi berbasis jaringan komputer. Berkat perkembangan internet, banyak aktivitas yang sebelumnya dilakukan secara manual kini dapat dilakukan secara digital, mulai dari komunikasi hingga transaksi bisnis. Jaringan komputer, yang sering kali dioperasikan melalui *server* yang dirancang secara bespoke atau khusus sesuai kebutuhan, menjadi tulang punggung dari berbagai layanan modern. Dalam konteks bisnis, interaksi ini sering kali diklasifikasikan sebagai *business-to-business* (B2B) atau *business-to-customer* (B2C), di mana hampir seluruh prosesnya kini memanfaatkan jaringan internet untuk mempermudah komunikasi dan transaksi di antara berbagai pihak. Keberadaan internet telah mengubah cara perusahaan dan individu menjalankan aktivitas mereka, menciptakan dunia yang lebih terhubung dan efisien.

Namun, kemajuan teknologi ini tidak selalu berjalan mulus. Di balik manfaat besar yang ditawarkan, terdapat ancaman yang terus mengintai, terutama dalam bentuk serangan siber. Setiap sistem teknologi, tidak peduli seberapa canggih dan sempurna perangkat lunaknya, tetap memiliki celah keamanan yang bisa dimanfaatkan oleh pihak tidak bertanggung jawab. Kekurangan ini sering kali menjadi sasaran empuk bagi para pelaku serangan untuk mengeksploitasi sistem, mengganggu kelancaran layanan, atau bahkan merusak data yang berharga. Salah satu bentuk serangan yang paling umum dan merusak adalah *Distributed Denial of Service* (DDoS). Serangan ini melibatkan pengiriman sejumlah besar permintaan ke *server* atau layanan jaringan dengan tujuan membanjiri kapasitasnya, sehingga mengganggu atau bahkan menghentikan lalu lintas normal dari sistem tersebut. Serangan semacam ini dapat menyebabkan kerugian besar bagi perusahaan maupun individu yang bergantung pada layanan tersebut, baik dalam bentuk finansial, reputasi, maupun hilangnya kepercayaan pengguna.

Untuk mengatasi ancaman ini, banyak perusahaan dan institusi mulai mengembangkan langkah-langkah preventif yang dirancang untuk meminimalkan dampak dari serangan DDoS. Langkah-langkah ini mencakup berbagai solusi teknologi, mulai dari penggunaan perangkat keras khusus

hingga penerapan algoritma canggih untuk mendeteksi dan menangani pola serangan. Namun, dalam praktiknya, serangan DDoS terus berevolusi dengan pola yang semakin kompleks, sehingga menuntut pendekatan yang lebih inovatif untuk mengidentifikasi dan mengatasinya.

Berdasarkan tantangan ini, penulis berupaya mengeksplorasi metode alternatif untuk menganalisis pola serangan DDoS, yaitu dengan memanfaatkan konsep relasi rekurens. Pendekatan ini menawarkan cara yang iteratif dan sistematis dalam menganalisis data serangan, sehingga memungkinkan identifikasi pola secara lebih terstruktur. Meskipun tidak dimaksudkan untuk menggantikan metode konvensional, pendekatan berbasis relasi rekurens ini berpotensi menjadi solusi yang lebih optimal dan akurat dalam menghadapi pola serangan yang terus berkembang. Dengan memadukan analisis matematis dan teknologi modern, makalah ini diharapkan dapat memberikan kontribusi bagi upaya kolektif dalam menghadapi ancaman siber yang semakin kompleks.

II. Dasar Teori

2.1. Deretan

Sebagai awalan, relasi rekurens memerlukan beberapa teori dasar yang meliputi deretan dan rekursif. Deretan atau *sequence* adalah daftar terurut dari elemen-elemen yang diskrit, deretan adalah fungsi dari subset suatu himpunan tertentu yang berisi bilangan bulat ke sebuah himpunan. deretan memiliki notasi khusus yaitu $\{a_n\}$. Sebuah deretan umumnya dinyatakan dalam suatu persamaan seperti[1]:

$$a_n = 2n$$
$$a_n = 1/n$$
$$a_n = 7 - 3n$$

sehingga menciptakan suatu barisan memiliki dasar dan terstruktur. Seluruh elemen dalam suatu deret dapat dijumlahkan seperti [1]:

Jumlah deretan

$$a_m, a_{m+1}, a_{m+2}, \ldots, a_n$$

adalah

$$a_m + a_{m+1} + a_{m+2} + \ldots + a_n$$

atau dapat dinyatakan dalam notasi sumasi yaitu

$$\sum_{k=m}^{n} a_k$$

dengan keterangan k adalah indeks sumasi, m adalah batas bawah index, dan m adalah batas atas indeks. Beberapa bentuk sumasi telah diturunkan menjadi suatu rumus yang tetap seperti [1]:

TABLE 2 Some Useful Summation Formulae.

Sum	*Closed Form*
$\sum_{k=0}^{n} ar^k \ (r \neq 0)$	$\frac{ar^{n+1} - a}{r-1}, r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \lvert x \rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x \rvert < 1$	$\frac{1}{(1-x)^2}$

Gambar 2.1. Tabel Formula Sumasi
(Sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2024-2025/10-Deretan,%20rekursi-dan-relasi-rekurens-(Bagian1)-2024.pdf)

Selain itu, sumasi tidak hanya dilakukan dalam bentuk tunggal yaitu hanya menggunakan variabel, tetapi sumasi juga bisa berbentuk ganda yang dimana sangat cocok untuk menghitung beberapa jenis operasi disaat bersamaan seperti yang biasanya diterapkan dalam suatu kalang bersarang atau yang lebih dikenal dengan *nested loop*. Mekanisme penghitungan sumasi ganda adalah mengekspansi sumasi terdalam dahulu baru dilanjutkan dengan ekspansi terluar seperti dibawah:

$$\sum_{i=1}^{4} \sum_{j=1}^{3} ij$$

$$\sum_{i=1}^{4} \sum_{j=1}^{3} ij = \sum_{i=1}^{4} (i + 2i + 3i) = \sum_{i=1}^{4} 6i = 6 + 12 + 18 + 24 = 60$$

2.2. Rekursif

Rekursi, jika sesuatu dapat didefinisikan dalam terminologinya sendiri maka itu disebut rekursif atau recursive, sedangkan proses pendefinisiannya disebut rekursi atau recursion. Suatu fungsi yang rekursif perlu didefinisikan dalam dua bagian yaitu[1]:

a. Basis
   Basis adalah bagian yang berisi nilai fungsi yang terdefinisi secara eksplisit yang berperan dalam menghentikan proses rekursi.

b. Rekurens
   Rekurens adalah bagian yang mendefinisikan fungsi berdasarkan terminologinya sendiri dimana diperlukan suatu kaidah yang dapat mengecilkan atau membesarkan suatu nilai fungsi seiring pemanggilan

terminologi berjalan untuk mencapai nilai eksplisit yang dinyatakan pada basis untuk bisa berhenti.

dari sini dapat dibentuk deretan rekursif yang merupakan setiap deret yang berisi elemen-elemen dari setiap proses rekurens.

2.3. Relasi Rekurens

Apabila deretan yang berupa persamaan a_n dapat dinyatakan secara rekursif dengan satu atau lebih untuk elemen sebelumnya, maka persamaan tersebut relasi rekurens. Pada relasi rekurens terdapat kondisi awal yaitu suatu barisan yang memiliki satu atau lebih nilai yang diperlukan sebagai dasar penghitungan elemen-elemen selanjutnya, kondisi awal dalam relasi rekurens merupakan langkah basis karena relasi rekurens dinyatakan barisan secara rekursif. Secara langsung kondisi awal akan menentukan elemen-elemen selanjutnya pada barisan, bentuk kondisi awal yang berbeda akan menghasilkan elemen barisan yang juga berbeda. Solusi dari suatu relasi rekurens adalah sebuah formula yang tidak lagi melibatkan aspek rekursif karena telah memenuhi relasi rekurens yang bersangkutan.

Relasi rekurens sendiri memiliki dua metode penyelesaian yaitu secara iteratif atau rekursif pada umumnya dan dengan metode sistematis. Metode sistematis adalah metode yang diterapkan untuk relasi rekurens yang berbentuk homogen lanjar atau *linear homogeneous*. Suatu relasi rekurens dapat dinyatakan homogen lanjar apabila berbentuk seperti [2]:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$$

dengan keterangan $c_1, c_2, \ldots, c_k$ adalah bilangan riil dan c_k bukan bernilai 0. Bentuk ini akan mencari solusi untuk homogen lancar berupa [2]:

$$a_n = r^n$$

dengan r adalah suatu konstanta yang kemudian bentuk tersebut masukkan kedalam persamaan utama sehingga terbentuk [2]:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$$

menjadi

$$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \ldots + c_k r^{n-k}$$

apabila kedua ruas dibagi dengan r^{n-k} maka akan menghasilkan [2]:

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \ldots - c_{k-1} r - c_k = 0$$

bentuk persamaan yang dihasilkan disebut sebagai persamaan karakteristik dari relasi rekurens. Solusi dari persamaan karakteristik tersebut dapat membentuk akar-akar karakteristik yang dapat menjadi komponen solusi dari relasi rekurens. Apabila akar-akar memiliki nilai yang berbeda maka dapat digunakan persamaan [2]:

$$a_n = \alpha_1 r^n{}_1 + \alpha_2 r^n{}_2$$

dengan keterangan α_1 dan α_2 adalah nilai konstan. Sedangkan apabila kedua akar bernilai sama atau akar kembar maka persamaan yang digunakan adalah [2]:

$$a_n = \alpha_1 r^n{}_0 + \alpha_2 n r^n{}_0$$

2.4. *Distributed Denial of Service* (DDoS)

Distributed Denial of Service (DDoS) adalah jenis serangan siber yang bertujuan untuk membuat layanan online, seperti situs web atau aplikasi, tidak dapat diakses oleh pengguna yang sah. Serangan ini dilakukan dengan membanjiri target dengan lalu lintas internet yang sangat besar, sehingga menghabiskan sumber daya sistem dan menyebabkan gangguan pada layanan tersebut.

Secara garis besar, DDoS biasanya melibatkan penggunaan botnet, yaitu jaringan komputer yang telah terinfeksi malware dan dikendalikan oleh penyerang. Dalam serangan ini, botnet mengirimkan permintaan akses secara bersamaan ke *server* target. Terdapat beberapa jenis serangan DDoS, antara lain [3]:

- Serangan Volumetrik: Menggunakan botnet untuk menciptakan lalu lintas tinggi yang dapat menyebabkan kemacetan pada *bandwidth server*.
- Serangan Protokol: Mengeksploitasi kerentanan pada protokol jaringan, seperti SYN Flood, di mana paket SYN dikirim tanpa respons dari *server*.
- Serangan Lapisan Aplikasi: Menargetkan aplikasi web dengan mengirimkan permintaan yang tampak sah tetapi berlebihan, sehingga membebani *server*.

Maka dari itu, DDoS memiliki efek yang sangat merugikan bagi banyak pihak entah itu individu maupun kelompok seperti [4]:

- Gangguan Layanan: Situs web atau aplikasi menjadi tidak dapat diakses oleh pengguna yang sah.
- Kerugian Finansial: Bisnis dapat kehilangan pendapatan jika layanan mereka tidak tersedia.
- Kerusakan Reputasi: Kepercayaan pelanggan dapat menurun akibat ketidakstabilan layanan.

Tapi serangan DDoS tidak terjadi semerta-merta tanpa suatu alasan, tentunya orang yang melakukan ini memiliki motivasi tertentu yang mendasarinya, secara umum ada beberapa motivasi dasar yaitu [5]:

- Finansial**:** Memeras organisasi melalui ancaman serangan (*ransom DDoS*).
- Kompetisi Bisnis**:** Merusak layanan pesaing.
- Motivasi Ideologis**:** Sebagai bentuk protes atau propaganda.
- Eksperimen atau Hiburan**:** Dilakukan oleh individu

untuk alasan pribadi.

III. Implementasi

Sebagai dasar, untuk analisis serangan DDoS, elemen a_n dapat merepresentasikan berbagai metrik, seperti jumlah paket data yang dikirimkan dalam satu interval waktu, jumlah permintaan HTTP, atau intensitas serangan pada waktu tertentu.

Maka dengan dasar itu, relasi rekurens dapat diturunkan persamaan baru berdasarkan elemen a_n yang sesuai dengan kebutuhannya seperti:

1. Pengumpulan dan Pra-Pemrosesan Data Historis
   Langkah pertama dalam penerapan relasi rekurens untuk mitigasi serangan DDoS adalah pengumpulan data historis yang mencakup berbagai metrik, seperti:
   - Jumlah paket data: Total jumlah paket yang dikirimkan selama interval waktu tertentu.
   - Sumber serangan: *IP address*, lokasi geografis, atau kelompok perangkat yang terlibat dalam serangan.
   - Durasi serangan: Berapa lama serangan berlangsung pada tingkat intensitas tertentu.
   - Jenis protokol: Apakah serangan dilakukan menggunakan protokol UDP, TCP, ICMP, atau kombinasi.
   - Distribusi waktu: Pola intensitas serangan terhadap waktu, baik secara *real-time* maupun *batch*.

   Untuk Pra-pemrosesan data meliputi beberapa langkah seperti :
   - Normalisasi: Menstandarkan data agar berada dalam skala yang seragam untuk memudahkan analisis.
   - Deteksi anomali: Mengidentifikasi lonjakan yang mencurigakan untuk ditandai sebagai bagian dari pola serangan.
   - Pengelompokan: Mengelompokkan data berdasarkan jenis serangan atau pola lalu lintas.

   Setelah seluruh data ini dikumpulkan dan diproses, langkah selanjutnya adalah mencari pola-pola yang dapat dimodelkan menggunakan relasi rekurens.

2. Deteksi Pola Serangan Periodik
   Mayoritas dari serangan DDoS menunjukkan pola periodik, di mana intensitas serangan meningkat pada interval waktu tertentu. Misalnya, jika a_n adalah jumlah paket data yang diterima pada waktu n, persamaan relasi rekurens sederhana untuk pola periodik dapat ditulis sebagai:
   $$a_n = a_{n-T} + P$$
   dengan keterangan:
   - T adalah periode serangan.
   - P adalah besar peningkatan intensitas serangan.

   Apabila ada data historis yang telah tersimpan sebelumnya dan menunjukkan bahwa serangan terjadi setiap 5 menit dengan peningkatan intensitas tertentu, relasi ini dapat digunakan untuk memprediksi waktu dan intensitas serangan berikutnya.

3. Pola Serangan Eksponensial
   Untuk beberapa serangan DDoS, terutama yang menggunakan botnet besar, menunjukkan pola eksponensial, di mana intensitas serangan meningkat secara drastis dalam waktu singkat. Pola ini dapat dimodelkan dengan persamaan relasi rekurens berupa:
   $$a_n = r \cdot a_{n-1}$$
   dengan r sebagai rasio peningkatan intensitas.
   Sebagai contoh, jika serangan awal mengirimkan 1.000 paket per detik dan rasio peningkatan adalah 2, maka intensitas serangan pada waktu berikutnya adalah 2.000, 4.000, 8.000, dan seterusnya. Pola ini membantu *administrator* jaringan untuk mempersiapkan sistem mitigasi yang mampu menangani lonjakan lalu lintas secara eksponensial.

4. Pola Serangan Acak
   Serangan DDoS juga dapat bersifat acak, di mana intensitasnya tidak mengikuti pola tertentu tetapi tetap memiliki hubungan dengan elemen sebelumnya. Pola ini dapat dimodelkan dengan relasi rekurens stokastik, seperti:
   $$a_n = a_{n-1} + \epsilon$$
   dengan ϵ adalah variabel acak yang merepresentasikan fluktuasi rata-rata dalam intensitas serangan. Dengan memanfaatkan komputasi untuk memperoleh distribusi probabilitas dari ϵ, maka dapat diperkirakan bagaimana serangan akan berkembang di masa depan dan semakin mempermudah menganalisis pola serangan acak yang terjadi.

5. Analisis Pola *Multi-Layer*
   Dalam serangan yang kompleks, pola serangan dapat melibatkan banyak lapisan, seperti serangan pada tingkat protokol (TCP, UDP) dan lapisan aplikasi (HTTP, HTTPS). Relasi rekurens dapat digunakan untuk memodelkan hubungan antara lapisan-lapisan tersebut. Maka dapat diturunkan pemodelan dengan persamaan relasi rekurens seperti:
   $$a_n^{(HTTP)} = f(a_{n-1}^{(TCP)}, a_{n-1}^{(HTTP)})$$
   Di mana $a_n^{(HTTP)}$ adalah intensitas serangan pada lapisan aplikasi, yang dipengaruhi oleh serangan pada

lapisan protokol dalam rupa $a_{n-1}^{(TCP)}$.

6. Penerapan untuk Prediksi dan Respons Proaktif
   Model rekurens yang telah diidentifikasi dapat digunakan untuk memprediksi intensitas serangan di masa depan. Proses prediksi ini melibatkan:
   - Simulasi: Mensimulasikan pola serangan berdasarkan model rekurens yang dibangun.
   - Eksperimen parameter: Menyesuaikan parameter model (misalnya, rasio *r* atau konstanta *c*) untuk mencocokkan data historis secara lebih akurat.

   Hasil prediksi kemudian digunakan untuk merancang respon proaktif, seperti:
   - Peningkatan kapasitas bandwidth: Menyiapkan kapasitas jaringan yang cukup untuk menangani lonjakan lalu lintas yang diprediksi.
   - Penyesuaian *firewall* dan IDS: Mengatur aturan *firewall* atau *intrusion detection system* (IDS) untuk memblokir lalu lintas mencurigakan sebelum mencapai *server* utama.
   - Pengalihan lalu lintas: Mengarahkan lalu lintas yang berpotensi membebani server ke layanan *cloud* atau *content distribution network* (CDN).

7. Evaluasi dan Optimalisasi Sistem Mitigasi
   Setelah model diterapkan, langkah terakhir adalah mengevaluasi efektivitasnya. Evaluasi ini mencakup:
   - Akurasi prediksi: Membandingkan intensitas serangan yang diprediksi dengan data aktual untuk menilai keandalan model.
   - Efektivitas mitigasi: Menilai apakah sistem mitigasi berhasil mengurangi dampak serangan berdasarkan hasil prediksi.
   - Pengembangan model lanjutan: Jika pola serangan berubah, model rekurens dapat disesuaikan atau diperbarui untuk mencerminkan dinamika baru.

IV. Studi Kasus

Untuk memperjelas penjelasan dan mempermudah penalaran, penulis membuat fakta fiktif yang melibatkan sebuah perusahaan e-commerce besar. Perusahaan ini bergantung pada layanan berbasis internet untuk menjalankan operasional bisnis mereka, termasuk pemrosesan pesanan pelanggan, pembayaran online, dan pengelolaan inventaris secara real-time. Pada suatu waktu, perusahaan ini menghadapi serangan DDoS besar yang menyebabkan penurunan kinerja sistem secara signifikan, bahkan hingga penghentian total layanan selama beberapa jam. Dampak serangan ini mencakup kerugian finansial karena terhentinya transaksi, penurunan reputasi karena keluhan pelanggan, serta meningkatnya biaya mitigasi dan pemulihan.

Penyelesaian terdiri dari beberapa langkah rinci dan terstruktur yang meliputi:

1. Analisis Pola Serangan
   Setelah serangan dihentikan sementara melalui langkah darurat seperti pengalihan lalu lintas (*traffic rerouting*) dan penyesuaian *firewall*, tim keamanan perusahaan mulai menganalisis data historis lalu lintas jaringan selama serangan terjadi. Data ini menunjukkan bahwa intensitas serangan meningkat secara bertahap, dengan jumlah paket yang dikirimkan ke *server* utama meningkat dua kali lipat setiap 10 menit. Hal ini mengindikasikan adanya pola eksponensial, yang dapat dimodelkan menggunakan relasi rekurens berikut:

   $$a_n = 2 \cdot a_{n-1}$$

   Di mana a_n mewakili jumlah paket pada interval waktu ke-n, dan a_{n-1} adalah jumlah paket pada interval waktu sebelumnya. Dengan kondisi awal a_0 = 1.000 paket per detik, jumlah paket pada interval waktu ke-5 diprediksi mencapai a_5 = 32.000 paket per detik.

2. Penerapan Relasi Rekurens untuk Prediksi
   Berdasarkan model ini, tim keamanan dapat memperkirakan intensitas serangan jika pola serangan tetap berlanjut. Prediksi ini memberikan waktu bagi perusahaan untuk mengimplementasikan langkah-langkah pencegahan sebelum serangan mencapai puncaknya. Langkah-langkah yang dilakukan meliputi:
   - Penambahan Kapasitas Jaringan: Perusahaan bekerja sama dengan penyedia layanan *cloud* untuk meningkatkan bandwidth *server* hingga mampu menangani hingga 50.000 paket per detik.
   - Penerapan Sistem Deteksi Dini: Menggunakan algoritma berbasis relasi rekurens, sistem deteksi dini dirancang untuk memantau dan menganalisis pola lalu lintas *real-time*. Jika pola eksponensial terdeteksi, sistem ini secara otomatis memicu protokol mitigasi.
   - Segmentasi Lalu Lintas: Lalu lintas yang mencurigakan dialihkan ke *server* khusus yang dirancang untuk menangani serangan, sementara lalu lintas yang sah tetap diarahkan ke *server* utama.

3. Evaluasi
   Setelah serangan berhasil diatasi, evaluasi dilakukan untuk menilai efektivitas strategi mitigasi yang diterapkan. Tim keamanan menemukan bahwa penggunaan relasi rekurens tidak hanya membantu dalam memprediksi pola serangan, tetapi juga memungkinkan pengoptimalan alokasi sumber daya.

Misalnya, peningkatan kapasitas jaringan dilakukan secara bertahap berdasarkan prediksi intensitas serangan, sehingga biaya tambahan dapat diminimalkan.

Selain itu, data dari serangan tersebut juga digunakan untuk memperbarui model prediktif yang lebih canggih. Misalnya, perusahaan mulai mengintegrasikan relasi rekurens stokastik untuk mengakomodasi elemen ketidakpastian dalam serangan mendatang. Dengan model ini, mereka dapat memperkirakan skenario terburuk (*worst-case scenario*) dan memastikan bahwa sistem tetap siap menghadapi ancaman dengan intensitas tak terduga.

4. Pengembangan Sistem Berbasis Relasi Rekurens
   Berdasarkan keberhasilan penerapan awal, perusahaan memutuskan untuk mengembangkan sistem mitigasi berbasis relasi rekurens yang lebih terintegrasi. Sistem ini mencakup:
   - Simulasi Serangan: Relasi rekurens digunakan untuk mensimulasikan berbagai pola serangan, termasuk pola linier, eksponensial, siklis, dan stokastik. Hasil simulasi ini membantu perusahaan mengidentifikasi potensi kelemahan dalam infrastruktur mereka.
   - Respon Otomatis: Sistem otomatis dirancang untuk menjalankan langkah-langkah mitigasi, seperti pengalihan lalu lintas, peningkatan kapasitas, atau penutupan akses sementara berdasarkan tingkat ancaman yang diprediksi.
   - Pelaporan dan Analitik: Data dari setiap serangan yang ditangani dianalisis dan digunakan untuk terus memperbarui model prediksi, sehingga sistem menjadi semakin adaptif terhadap ancaman baru.

Berdasarkan studi kasus ini dapat ditunjukkan bahwa penerapan relasi rekurens dalam analisis dan mitigasi serangan DDoS dapat memberikan manfaat yang signifikan, baik dari segi prediksi ancaman maupun efektivitas langkah mitigasi. Dengan memahami pola serangan secara matematis, perusahaan dapat merancang strategi respons yang lebih tepat sasaran, mengurangi dampak serangan, dan mengoptimalkan penggunaan sumber daya. Pendekatan ini juga dapat diterapkan di berbagai industri lain yang menghadapi ancaman serupa, menciptakan ekosistem keamanan siber yang lebih kuat dan tangguh di era digital.

V. Pembahasan

Berdasarkan implementasi yang telah dibuat dan studi kasus yang telah dianalisis dapat menjelaskan bahwa pemanfaatan relasi rekurens dalam analisis dan mitigasi serangan DDoS menawarkan berbagai keuntungan dan tantangan yang perlu dipertimbangkan. Salah satu keuntungannya adalah kemampuan untuk memberikan pemahaman yang lebih mendalam terhadap pola serangan, memungkinkan identifikasi karakteristik serangan dengan lebih jelas. Selain itu, model ini dapat memberikan prediksi yang akurat tentang intensitas serangan di masa depan, asalkan tersedia data historis yang cukup. Relasi rekurens juga dapat diterapkan pada berbagai lapisan jaringan, mulai dari protokol hingga aplikasi, sehingga analisis menjadi lebih komprehensif. Informasi yang diperoleh dari model ini dapat dimanfaatkan untuk meningkatkan sistem mitigasi, menjadikannya lebih responsif terhadap ancaman yang muncul. Namun, penerapannya juga menghadapi sejumlah tantangan. Serangan DDoS sering kali tidak memiliki pola yang konsisten, sehingga sulit untuk membangun model yang stabil. Analisis real-time dengan relasi rekurens membutuhkan sumber daya komputasi yang besar, yang dapat menjadi kendala dalam implementasi. Selain itu, kompleksitas serangan modern, seperti serangan multi-vektor, menambah kesulitan dalam memodelkan pola serangan dengan relasi yang sederhana. Ketergantungan pada data historis juga menjadi tantangan, karena ketepatan model sangat bergantung pada kualitas dan kelengkapan data yang tersedia. Oleh karena itu, meskipun relasi rekurens memiliki potensi besar, penggunaannya memerlukan pendekatan yang hati-hati untuk mengatasi tantangan yang ada.

VI. Kesimpulan

Teori relasi rekurens menawarkan pendekatan sistematis dan matematis untuk menganalisis pola serangan DDoS, memungkinkan pemahaman yang lebih mendalam, prediksi intensitas serangan, dan perancangan sistem mitigasi yang lebih efektif. Namun, tantangan muncul dalam menghadapi serangan yang kompleks dan dinamis, sehingga keberhasilan pendekatan ini sangat bergantung pada integrasinya dengan metode lain, seperti pembelajaran mesin, analitik data real-time, dan teknologi keamanan berbasis cloud. Dalam konteks dunia yang terus berkembang, pendekatan berbasis rekurens tidak hanya membantu menganalisis pola serangan tetapi juga menjadi komponen penting dalam strategi keamanan siber yang lebih luas. Dengan memahami pola serangan secara lebih baik, organisasi dapat meningkatkan ketahanan terhadap ancaman yang semakin canggih, menjaga kelangsungan layanan, serta melindungi data dan infrastruktur dari potensi kerusakan besar.

VII. Saran

Saran untuk penelitian selanjutnya bisa mendalami teori keamanan siber lebih dalam khususnya untuk DDoS lebih dalam agar dapat memberikan implementasi dalam bentuk program atau sistem yang lebih konkret dan dapat ditunjukkan sehingga bisa memberikan hasil analisis yang lebih optimal dan lebih kredibel, serta memberikan pembahasan yang lebih akurat.

VIII. Acknowledgment

Pertama-tama, penulis mengucapkan puji syukur kepada Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya penulis dapat menyelesaikan makalah ini tepat waktu. Adapun

tujuan penulisan makalah ini adalah sebagai bentuk pemenuhan tugas mata kuliah IF1220 Matematika Diskrit.

Dalam penyusunan ini penulis ingin berterima kasih kepada berbagai pihak yang telah mendukung dan mendorong pembuatan makalah ini. Oleh karena itu, saya menyampaikan terima kasih kepada:

1. Seluruh dosen pengampu mata kuliah Matematika Diskrit yang telah memberikan bimbingan dan dorongan untuk membuat makalah ini dan telah menyiapkan bahan ajar yang juga digunakan dalam makalah ini.

2. Orang tua yang senantiasa memberikan dukungan secara moril maupun material kepada anak-anaknya sehingga bisa seperti saat ini.

Demikian ucapan terima kasih penulis kepada orang-orang yang mendukung dalam proses pembuatan makalah ini. Semoga dengan adanya makalah ini dapat memberikan gambaran dan sedikit pemikiran tentang masalah yang disampaikan.

References

[1] Munir, Rinaldi. "Deretan, rekursi, dan relasi rekurens (Bagian 1)". https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2024-2025/10-Deretan,%20rekursi-dan-relasi-rekurens-(Bagian1)-2024.pdf. Diakses pada tanggal 4 Januari 2025.

[2] Munir, Rinaldi. "Deretan, rekursi, dan relasi rekurens (Bagian 2)". https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2024-2025/11-Deretan,%20rekursi-dan-relasi-rekurens-(Bagian2)-2024.pdf. Diakses pada tanggal 4 Januari 2025.

[3] Nidasyifan. "DDoS : Definisi, Contoh, Cara Kerja, serta Penanganan". telkomuniversity.ac.id. https://jakarta.telkomuniversity.ac.id/distributed-denial-of-service-ddos-definisi-contoh-cara-kerja-penanganan-serangan-siber/. Diakses pada 4 Januari 2025.

[4] Ibm. "Apa itu serangan denial-of-service terdistribusi (DDos)?". ibm.com. https://www.ibm.com/id-id/topics/ddos. Diakses pada 4 Januari 2025.

[1] Alkazimy, Ahmad. "Memahami Motivasi Penyerang DDoS". idnic.net. https://idnic.net/blog/detail/memahami-motivasi-penyerang-ddos/Mjcw. Diakses pada 4 Januari 2025.

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 6 Januari 2025

Filbert Engyo, 13523163