DOI: https://doi.org/10.37817/ikra-ithabdimas.v10i1
P-ISSN : 2654-5721
E-ISSN : 2654-7546

Pengembangan Framework Autonomous Cyber Defense Berbasis Deep Reinforcement Learning untuk Mitigasi Serangan (DDoS) Secara Adaptif

Asnefi
Teknik Informatika, Universitas Patria Artha, Makasar
E-mail: asnefi@patria-artha.ac.id

ABSTRAK

Kompleksitas serangan Distributed Denial of Service (DDoS) yang kian dinamis memicu kegagalan sistem proteksi konvensional berbasis parameter statis. Menjawab tantangan tersebut, penelitian ini merancang arsitektur pertahanan siber mandiri (Autonomous Cyber Defense) berbasis kecerdasan buatan untuk mereduksi dampak serangan secara real-time. Melalui implementasi Deep Reinforcement Learning (DRL) dengan algoritma Deep Q-Network (DQN), agen cerdas dilatih untuk mengeksekusi tindakan mitigasi, seperti membuang paket (drop packet) atau membatasi laju data (rate limiting), berdasarkan fluktuasi metrik jaringan, seperti entropi IP dan laju paket. Pengujian menggunakan instrumen simulasi dan basis data serangan CICIDS2019 menunjukkan efektivitas model dengan tingkat akurasi identifikasi ancaman sebesar 94,5%. Sistem ini terbukti mampu memotong volume lalu lintas anomali hingga 85% sekaligus mempertahankan stabilitas akses bagi pengguna yang sah.

Kata Kunci: Autonomous Cyber Defense, DDoS, Deep Q-Network, Kecerdasan Buatan, Pertahanan Jaringan.

ABSTRACT

The increasingly dynamic nature of Distributed Denial of Service (DDoS) attacks causes conventional, static parameter-based protection systems to fail. To address this challenge, this research designs an autonomous cyber defense architecture powered by artificial intelligence to mitigate attack impacts in real-time. By implementing Deep Reinforcement Learning (DRL) with the Deep Q-Network (DQN) algorithm, an intelligent agent is trained to execute mitigation actions—such as dropping packets or rate limiting—based on fluctuating network metrics like IP entropy and packet rates. Testing conducted using simulation tools and the CICIDS2019 attack dataset demonstrates the model's effectiveness, achieving a threat identification accuracy rate of 94.5%. The system proves capable of reducing anomalous traffic volume by up to 85% while maintaining stable access for legitimate users.

Keywords: Autonomous Cyber Defense, DDoS, Deep Q-Network, Artificial Intelligence, Network Defense.

1. PENDAHULUAN

Perkembangan teknologi digital dan internet menyebabkan meningkatnya ancaman pada sistem keamanan jaringan(Gunawan et al., 2024) . Serangan seperti malware, phishing, dan pencurian data menjadi masalah serius karena dapat merugikan berbagai sektor(Yehezkiel Natanael et al., 2024) . Sistem keamanan

P-ISSN : 2654-5721
E-ISSN : 2654-7546 DOI: https://doi.org/10.37817/ikra-ithabdimas.v10i1

tradisional dinilai kurang efektif dalam menghadapi ancaman modern yang terus berkembang(Santos et al., 2024).

Serangan Distributed Denial of Service (DDoS) merupakan salah satu ancaman utama pada infrastruktur jaringan modern (Salsabillah et al., 2024). Metode mitigasi konvensional umumnya bersifat statis dan berbasis aturan (rule-based), sehingga kurang adaptif terhadap pola serangan yang terus berkembang. Seiring meningkatnya kompleksitas serangan siber, diperlukan mekanisme pertahanan yang mampu belajar secara mandiri dan melakukan respons secara real-time (Firdaus et al., 2023).

Artificial Intelligence (AI) menjadi salah satu solusi dalam meningkatkan keamanan jaringan karena mampu mendeteksi pola serangan dan menganalisis ancaman secara otomatis (L. Chen et al., 2020) (Athooyaa et al., 2025).

Dalam beberapa tahun terakhir, konsep Autonomous Cyber Defense mulai berkembang sebagai paradigma baru dalam keamanan siber. meningkatkan ketepatan pengambilan keputusan, dan menjaga kontinuitas layanan secara lebih efektif. Salah satu metode kecerdasan buatan yang memiliki potensi besar dalam mewujudkan sistem pertahanan siber otonom adalah Deep Reinforcement Learning (DRL).

Meskipun penelitian mengenai penerapan Deep Reinforcement Learning dalam keamanan siber telah menunjukkan hasil yang menjanjikan, sebagian besar penelitian masih berfokus pada deteksi intrusi, optimasi kebijakan keamanan, atau respons terhadap ancaman tertentu secara terpisah. Penelitian yang mengintegrasikan proses pemantauan jaringan, deteksi serangan, pengambilan keputusan, dan mitigasi adaptif dalam suatu framework pertahanan siber otonom masih relatif terbatas. Selain itu, belum banyak penelitian yang secara khusus mengembangkan framework berbasis Deep Reinforcement Learning untuk mitigasi serangan DDoS yang mampu beradaptasi terhadap perubahan pola serangan secara real-time.

Berdasarkan kondisi tersebut, penelitian ini mengusulkan Framework Autonomous Cyber Defense Berbasis Deep Reinforcement Learning untuk Mitigasi Serangan Distributed Denial of Service (DDoS) Secara Adaptif.

2. LANDASAN TEORI

2.1. Autonomous Cyber Defense (ACD).

Autonomous Cyber Defense (ACD) merupakan sebuah paradigma baru dalam dunia keamanan siber yang menekankan pada kemampuan sistem untuk mendeteksi, menganalisis, dan memitigasi ancaman secara mandiri tanpa bergantung pada intervensi manusia secara langsung (Priya Sharma, 2023).

Arsitektur ACD ummnya terdiri atas:

1) Monitoring Layer : Mengumpulkan informasi lalu lintas jaringan.
2) Detection Layer : Menganalisis pola anomali dan serangan.
3) Decision Layer: Menghasilkan keputusan berdasarkan hasil analisis.
4) Mitigation Layer: Melaksanakan tindakan mitigasi.

2.2. Karakteristil Serangan Distributed Denial of Service (DDoS).

Serangan Distributed Denial of Service (DDoS) diidentifikasi sebagai aksi siber terencana yang bertujuan melumpuhkan aksesibilitas layanan digital dengan cara membanjiri target menggunakan lonjakan lalu lintas data abnormal. Berbeda dari gangguan DoS biasa, skenario DDoS memanfaatkan jaringan perangkat terinfeksi (botnet) yang tersebar secara global untuk mengirimkan paket data secara serentak, sehingga menguras kapasitas pita lebar (bandwidth) atau membebani memori dan prosesor server.

DOI: https://doi.org/10.37817/ikra-ithabdimas.v10i1
P-ISSN : 2654-5721
E-ISSN : 2654-7546

2.3. Deep Reinforcement Learning

Deep Reinforcement Learning merupakan pengembangan dari Reinforcement Learning yang mengombinasikan kemampuan pembelajaran berbasis interaksi dengan kekuatan jaringan saraf dalam memproses data yang kompleks dan berdimensi tinggi (X. Chen et al., 2023). Melalui mekanisme reward dan punishment, agen DRL dapat mempelajari strategi terbaik untuk mencapai tujuan tertentu tanpa memerlukan aturan yang telah ditentukan sebelumnya (Orr & Dutta, 2023).

Salah satu algoritma DRL yang sukses diterapkan adalah Deep Q-Network (DQN). DQN menggunakan jaringan saraf untuk mengestimasi fungsi nilai optimal Q*(s,a), yang merepresentasikan total ekspektasi reward masa depan yang dapat diperoleh agen dengan mengambil tindakan a pada keadaan s .

Formula pembaruan nilai Q menggunakan persamaan Bellman dinyatakan sebagai berikut:

$$Q(s,a) = R(s,a) + +Ymax Q(s\text{^}', a\text{^}') \quad \text{....persamaan (1)}$$

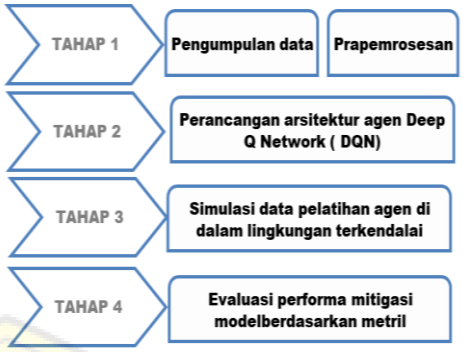
Keterangan :

- Q(s,a)= laju pembelajaran (learning rate)
- R(s,a)= reward kontan yang diperoleh, dan
- Y= discount factor untuk mengukur signifikansi reward jangka panjang

3. METODOLOGI

3.1. Tahapan Penelitian

Penelitian ini dijalankan melalui empat tahapan utama yang sistematis untuk memastikan keberhasilan pengembangan framework. Adapaun tahapan penelitian ini disajikan pada gambar 1.



Gambar 1. Tahapan Pemelitian

1) Pengumpulan dan prapemrosesan.

Dataset yang digunakan untuk penelitian adalah CIC-DDoS2019. Melakukan ekstraksi berkas PCAP dari dataset standar CICIDS2019 serta mengonfigurasi topologi jaringan virtual berbasis Software-Defined Networking (SDN) menggunakan Mininet.

Merancang modul pemantau (Monitor) untuk menangkap paket data secara real-time, lalu menghitung parameter statistik laju paket serta nilai entropi dari alamat IP asal menggunakan pustaka Scapy dan Pandas.

2) Perancangan arsitektur agen Deep Q-Network (DQN)

Membangun arsitektur Jaringan Saraf Tiruan (DNN) untuk mengestimasi fungsi nilai Q, mendefinisikan ruang keadaan (State), ruang aksi (Action), serta merumuskan fungsi penghargaan (Reward Function).

3) Simulasi dan pelatihan agen di dalam lingkungan jaringan terkendali.

Melatih agen cerdas di dalam lingkungan serta simulasi menggunakan skema interaksi bertahap (episodes) hingga mencapai kondisi konvergen berdasarkan Persamaan Bellman melalui pustaka Stable-Baselines3.

4) Evaluasi performa mitigasi model berdasarkan metrik performa keamanan.

Menguji model akhir terhadap variasi serangan DDoS volumetrik untuk mengukur metrik akurasi deteksi, laju

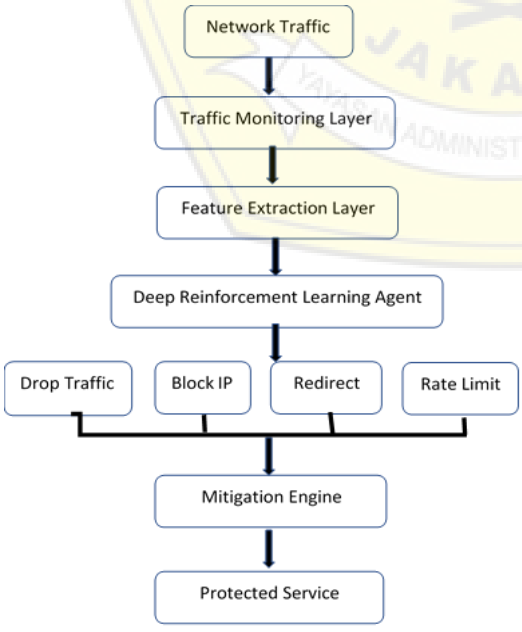
P-ISSN : 2654-5721
E-ISSN : 2654-7546 DOI: https://doi.org/10.37817/ikra-ithabdimas.v10i1

kesalahan (false positives), dan kecepatan waktu respons mitigasi.

3.2. Desain Framework diusulkan

Framework Autonomous Cyber Defense (ACD) yang diusulkan beroperasi menggunakan prinsip kontrol lingkaran tertutup (closed-loop system). Komponen utama sistem terbagi menjadi tiga entitas, yaitu: Lingkungan Jaringan (SDN Data Plane), Modul Telemetri (Monitor), dan Agen Kecerdasan DRL (DQN Controller).

Alur kerja subsistem dimulai saat paket lalu lintas data mengalir menuju switch jaringan. Modul telemetri secara berkala mengekstrak data statistik lalu lintas data tersebut di dalam jendela waktu (time window) diskrit per 1 detik. Hasil kalkulasi fitur dikonversi menjadi representasi keadaan (state) yang dikirimkan ke pengendali DQN. Agen cerdas kemudian mengevaluasi kondisi jaringan dan menentukan kebijakan mitigasi (action) terbaik. Keputusan tersebut ditransmisikan kembali ke switch jaringan dalam bentuk instruksi tabel aliran (flow rules) untuk mengeksekusi paket data secara otomatis.



Gambar 2. Framework (ACD) diusulkan

4. HASIL DAN PEMBAHASAN

4.1. Pelatihan Agen Deep Q-Network (DQN)

Proses pelatihan agen cerdas DQN dilakukan dalam lingkungan simulasi selama 10.000 langkah (steps) yang terbagi ke dalam sejumlah episode.

Parameter evaluasi yang diamati adalah akumulasi nilai penghargaan (cumulative reward) dan nilai kegagalan fungsi kerugian (loss value).

Pada awal fase pelatihan (langkah 0 hingga 3.000), agen menunjukkan performa yang tidak stabil dengan capaian reward negatif yang cukup tinggi. Hal ini terjadi karena agen DQN masih berada dalam fase eksplorasi (exploration phase), di mana agen secara acak mencoba berbagai aksi (action) seperti memblokir pengguna sah (false positive) atau meloloskan paket serangan (false negative) untuk memahami karakteristik lingkungan jaringan. Namun, memasuki langkah 4.000 ke atas, nilai penghargaan akumulatif merangkak naik secara signifikan menuju arah positif dan mencapai kondisi konvergen (stabil) pada kisaran langkah 7.500 hingga 10.000.

Konvergensi ini membuktikan bahwa persamaan Bellman yang diterapkan pada jaringan saraf tiruan berhasil meminimalkan Temporal Difference (TD) Error, sehingga agen secara adaptif mampu beralih ke fase eksploitasi (exploitation phase) untuk mengeksekusi kebijakan pertahanan yang optimal secara konsisten.

Gambar 3.Grafik Cumulative Reward Pelatihan DQN

DOI: https://doi.org/10.37817/ikra-ithabdimas.v10i1
P-ISSN : 2654-5721
E-ISSN : 2654-7546

Gambar 4.Grafic Loss Function Pelatihan

4.2. Evaluasi Metrik Keamanan Sistem Mitigasi

Setelah proses pelatihan selesai, model DQN yang telah matang diuji dengan menyuntikkan trafik serangan SYN Flood dan UDP Flood dari dataset CICIDS2019 ke dalam topologi Mininet. Kinerja framework Autonomous Cyber Defense (ACD) yang diusulkan dinilai menggunakan empat metrik evaluasi standar: Accuracy, Precision, Recall, dan False Positive Rate (FPR).

Hasil pengujian tersebut dirangkum dalam Tabel 1, di bawah ini:

Tabel 1. Hasil Pengujian Metrik Keamanan Framework ACD berbasis DQN

Jenis Serangan	Akurasi	Presisi	Recall	FPR
SYN Flood	94,8%	95,2%	94,1%	1,8%
UDP Flood	94,2%	93,7%	94,5%	2,1%
Rata-rata	94,5%	94,4%	94,3%	1,95%

Berdasarkan hasil pengujian, yang disajikan pada tabel 1. Terlihat bahwa framework yang dikembangkan mampu mencapai tingkat akurasi rata-rata sebesar 94,5%. Nilai tersebut menunjukkan bahwa sebagian besar lalu lintas jaringan berhasil diklasifikasikan secara tepat sebagai trafik normal maupun trafik serangan.

Nilai precision sebesar 94,4% menunjukkan bahwa mayoritas lalu lintas yang dikategorikan sebagai serangan memang merupakan aktivitas berbahaya. Sementara itu, recall sebesar 94,3% mengindikasikan bahwa sistem mampu mendeteksi sebagian besar serangan yang terjadi tanpa banyak kehilangan sampel serangan yang sebenarnya.

Aspek yang paling penting dalam implementasi sistem keamanan jaringan adalah nilai False Positive Rate (FPR). Pada penelitian ini, nilai rata-rata FPR berhasil ditekan hingga 1,95%. Nilai tersebut menunjukkan bahwa hanya sebagian kecil pengguna sah yang berpotensi salah teridentifikasi sebagai penyerang.

Rendahnya nilai FPR menunjukkan bahwa kombinasi antara fitur statistik lalu lintas dan perhitungan entropi Shannon mampu membantu agen DQN membedakan pola lalu lintas normal dan anomali secara lebih akurat. Dengan demikian, kualitas layanan (Quality of Service) tetap dapat dipertahankan selama proses mitigasi berlangsung.

4.3. Analisis Dampak Mitigasi terhadap Performa Jaringan

Untuk mengevaluasi efektivitas mekanisme mitigasi yang dihasilkan oleh agen DQN, dilakukan analisis terhadap perubahan throughput jaringan sebelum dan sesudah sistem pertahanan diaktifkan.

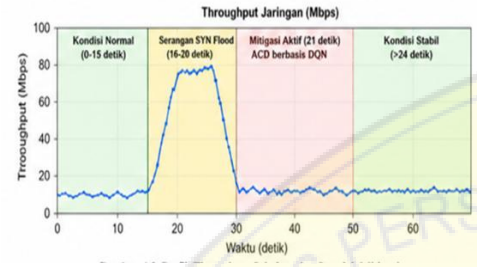
Pada kondisi normal (0–15 detik), throughput jaringan berada pada kisaran 5–10 Mbps yang merepresentasikan aktivitas pengguna sah. Ketika serangan SYN Flood mulai diluncurkan pada detik ke-16, terjadi peningkatan trafik secara drastis hingga mencapai 95 Mbps pada detik ke-20. Lonjakan tersebut menyebabkan utilisasi sumber daya jaringan meningkat secara signifikan sehingga berdampak pada penurunan performa layanan.

Setelah modul Autonomous Cyber Defense mendeteksi anomali pada detik ke-21, agen DQN segera mengevaluasi kondisi lingkungan berdasarkan parameter state yang diamati, antara lain packet rate, entropy source IP, bandwidth utilization, dan jumlah koneksi aktif. Berdasarkan hasil evaluasi tersebut, agen memilih aksi mitigasi berupa Drop Packet

P-ISSN : 2654-5721
E-ISSN : 2654-7546 DOI: https://doi.org/10.37817/ikra-ithabdimas.v10i1

dan Rate Limiting terhadap sumber trafik yang dicurigai.

Dalam waktu kurang dari tiga detik, volume lalu lintas serangan berhasil dikurangi hingga sekitar 85%. Pada detik ke-24, throughput jaringan kembali berada pada kisaran aman sebesar 15 Mbp



Gambar 5. Grafik Throughput sebelum dan sesudah Mitigasi

Hasil ini menunjukkan bahwa agen mampu merespons serangan secara cepat dan efektif tanpa memerlukan intervensi administrator jaringan.

Selain melakukan pemblokiran terhadap trafik berbahaya, sistem juga menerapkan mekanisme rate limiting secara adaptif pada kelompok alamat IP yang berada dalam kategori mencurigakan. Strategi ini memungkinkan pengguna sah tetap memperoleh akses layanan secara normal selama proses mitigasi berlangsung.

Kemampuan sistem dalam mengembalikan kondisi jaringan ke keadaan stabil dalam waktu yang relatif singkat menunjukkan bahwa pendekatan Deep Reinforcement Learning memiliki potensi besar dalam membangun sistem Autonomous Cyber Defense yang mampu beradaptasi terhadap karakteristik serangan DDoS modern yang dinamis dan terus berkembang.

5. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, penelitian ini berhasil mengembangkan sebuah framework Autonomous Cyber Defense (ACD) yang adaptif berbasis Deep Reinforcement Learning (DRL) dengan algoritma Deep Q-Network (DQN) untuk mitigasi serangan Distributed Denial of Service (DDoS). Dari seluruh rangkaian eksperimen pada lingkungan simulasi, dapat ditarik beberapa kesimpulan utama sebagai berikut:

1) Integrasi perhitungan metrik statistik entropi Shannon terhadap distribusi alamat IP asal terbukti efektif dalam memperkaya representasi keadaan (state) jaringan, sehingga agen cerdas mampu mengenali anomali lalu lintas data volumetrik secara presisi.
2) Proses pelatihan menunjukkan bahwa agen DQN mampu mencapai kondisi konvergen yang stabil dalam batas 10.000 langkah (steps), mengonfirmasi keberhasilan Persamaan Bellman dalam mengoptimalkan kebijakan pertahanan jangka panjang secara mandiri.
3) Pengujian menggunakan dataset standar CICIDS2019 menunjukkan performa keamanan yang sangat baik dengan rata-rata tingkat akurasi deteksi mencapai 94,5% dan kemampuan menekan laju kesalahan pemblokiran pengguna legal (False Positive Rate) hingga serendah 1,95%.
4) Framework yang dibangun terbukti responsif dan adaptif dengan kemampuan memotong volume lalu lintas serangan hingga 85% dalam waktu singkat, sekaligus mempertahankan stabilitas akses layanan bagi pengguna yang sah melalui aksi mitigasi yang fleksibel (drop packet dan rate limiting).

DAFTAR PUSTAKA

Athooyaa, M., Prabantara, S. K., Hidayat, D. A., Shaikh, S. S., & Arfriandi, A. (2025). Penerapan Kecerdasan Buatan dalam Keamanan Siber pada Infrastruktur Kritis: Tinjauan Sistematis terhadap Ancaman, Solusi, dan Tantangan. *Jurnal Riset*

Informatika Dan Teknologi Informasi, *3*(2). https://doi.org/10.58776/jriti.v3i2.232

Chen, L., Chen, P., & Lin, Z. (2020). Artificial Intelligence in Education: A Review. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.2988510

Chen, X., Yao, L., McAuley, J., Zhou, G., & Wang, X. (2023). Deep reinforcement learning in recommender systems: A survey and new perspectives. *Knowledge-Based Systems*, *264*. https://doi.org/10.1016/j.knosys.2023.110335

Firdaus, D., Fahira, F., & Rianti, R. (2023). DETEKSI ANOMALI DAN SERANGAN LOW RATE DDOS DALAM LALU LINTAS JARINGAN MENGGUNAKAN NAIVE BAYES. *Naratif : Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika*, *5*(2). https://doi.org/10.53580/naratif.v5i2.208

Gunawan, F., Fadhilah, A., & Sari, E. M. (2024). Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, *25*(1).

Orr, J., & Dutta, A. (2023). Multi-Agent Deep Reinforcement Learning for Multi-Robot Applications: A Survey. In *Sensors* (Vol. 23, Number 7). https://doi.org/10.3390/s23073625

Priya Sharma. (2023). Autonomous Cyber Defence Systems (ACDS) Using AI. *International Journal of Scientific Research & Engineering Trends*, *9*(1), 1–5.

Salsabillah, S. P., Al Mita, A., Irsyad, M. Z., Malays, E., & Sakti, S. (2024). Implementasi Penggunaan Kali linux dengan Teknik Ddos dalam Uji coba Keamanan Website. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, *25*(1).

Santos, A. Dos, Pereira, G. S., Syuhada, R. A., Malays, E., & Sakti, S. (2024). Uji Coba Keamanan Database Website Menggunakan Python Dan Sqlmap Melalui Command Prompt Pada Sistem Operasi Windows. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, *25*(1).

Yehezkiel Natanael, Rangga Felicia, & Essy Malays Sari Sakti. (2024). Analisis Keamanan Informasi Bagi Pengguna Website Menggunakan Kalilinux Melalui Teknik SQL Injection. *TEKINFO*, *25*(1), 123–132.