PERBANDINGAN SERANGAN DOS BERBASIS *DEEP REINFORCEMENT LEARNING* DAN KONVENSIONAL TERHADAP APLIKASI *GRAPHQL*

TUGAS AKHIR

Disusun oleh:

MUAMMAR AL FARUQI

210705080

Mahasiswa Fakultas Sains dan Teknologi

Program Studi Teknologi Informasi

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI AR-RANIRY

BANDA ACEH

2025M/1447H

LEMBAR PERSETUJUAN

PERBANDINGAN SERANGAN DOS BERBASIS DEEP REINFORCEMENT LEARNING DAN KONVENSIONAL PADA APLIKASI GRAPHQL

TUGAS AKHIR

Diajukan KepadaFakultas Sains dan Teknologi
Universitas Islam Negeri (UIN) Ar-Raniry Banda Aceh
Sebagai Salah Satu Beban Studi Memperoleh Gelar Sarjana (S1)
Dalam Prodi Teknologi Informasi

Oleh:
MUAMMAR AL-FARUQI
210705080
Mahasiswa Fakultas Sains dan Teknologi
Program Studi Teknologi dan Informasi

Disetujui untuk Dimunaqasyahkan Oleh:

Pembimbing 1,	Pembimbing 2,
Mulkan Fadhli, S.T., M.T.	Aulia Syarif Aziz, S.Kom., M.Sc.
NIP. 198811282020121006	NIP. 199305212022031001

Mengetahui,
Ketua Program Studi Teknologi Informasi

Malahayati, M.T.
NIP. 198301272015032003

LEMBAR PENGESAHAN

PERBANDINGAN SERANGAN DOS BERBASIS *DEEP REINFORCEMENT LEARNING* DAN KONVENSIONAL PADA APLIKASI *GRAPHQL*

TUGAS AKHIR

Telah Diuji Oleh Panitia Ujian Munaqasyah Tugas Akhir
Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh dan Dinyatakan Lulus
Serta Diterima Sebagai Salah Satu Beban Studi Program Sarjana (S1)
Dalam Program Studi Teknologi Informasi

Pada Hari/Tanggal: Kamis, 21 Agustus 2025
27 Safar 1447 H
Di Darussalam, Banda Aceh

Panitia Ujian Munaqasyah Tugas Akhir:

Ketua,	Sekretaris,
Mulkan Fadhli, S.T., M.T.	**Aulia Syarif Aziz, M.Sc**
NIP. 198811282020121006	**NIP. 199305212022031001**
Penguji I,	Penguji II,
Ghufran Ibnu Yasa, M.T	**Dr. Hendri Ahmadian, S.Si, M.I.M**
NIP.198409262014031005	**NIP. 198301042014031002**

Mengetahui:
Dekan Fakultas Sains dan Teknologi
UIN Ar-Raniry Banda Aceh,

Prof. Dr. Ir. Muhammad Dirhamsyah, M.T., IPU
NIP. 196210021988111001

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan dibawah ini:

Nama	: Muammar Al-Faruqi
NIM	: 210705080
Program Studi	: Teknologi Informasi
Fakultas	: Sains dan Teknologi
Judul	: PERBANDINGAN SERANGAN DOS BERBASIS *DEEP REINFORCEMENT LEARNING* DAN KONVENSIONAL PADA APLIKASI *GRAPHQL*

Dengan ini menyatakan bahwa dalam penulisan tugas akhir/skripsi ini, saya:

1. Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggungjawabkan;
2. Tidak melakukan plagiasi terhadap naskah karya orang lain;
3. Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya;
4. Tidak memanipulasi dan memalsukan data;
5. Mengerjakan sendiri karya ini dan mampu bertanggungjawab atas karya ini.

Bila di kemudian hari ada tuntutan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat dipertanggungjawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap dikenai sanksi berdasarkan aturan yang berlaku di Fakultas Sains dan Teknologi UIN Ar-Raniry Banda Aceh.

Banda Aceh,
Yang Menyatakan

Muammar Al-Faruqi

ABSTRAK

Nama : Muammar Al-Faruqi

NIM : 210705080

Program Studi : Teknologi Informasi

Judul : PERBANDINGAN SERANGAN DOS BERBASIS *DEEP REINFORCEMENT LEARNING* DAN KONVENSIONAL TERHADAP APLIKASI *GRAPHQL*

Jumlah Halaman : 71

Pembimbing I : Mulkan Fadhli, S.T., M.T.

Pembimbing II : Aulia Syarif Aziz, M.Sc.

Kata Kunci : *Wendigo*, *Deep Reinforcement Learning*, *GraphQL*, *Denial of Service*, DoS, *Slowloris*, Hping3, *Damn Vulnrtable GraphQL Application*, DVGA

Teknologi API yang semakin berkembang telah mendorong untuk mengadopsi *GraphQL* sebagai alternatif fleksibel dalam pengolahan data. Namun fleksibilitas ini membuka celah keamanan khususnya terhadap serangan *Denial of Service* (DoS). Serangan DoS konvensional seperti *slowloris* dan Hping3 sering digunakan untuk membajiri *server* tetapi efektivitasnya menurun seiring dengan meningkatnya sistem pertahanan. Pendekatan baru berbasis *Machine Learning* seperti *Wendigo* yang menggunakan metode *Deep Reinforcement Learning* (DRL) memungkinkan serangan yang lebih adaptif dan sulit terdeteksi. Penelitian ini bertujuan untuk membandingkan efektivitas serangan DoS berbasis DRL dan serangan DoS konvensional terhadap aplikasi *GraphQL*. Evaluasi dilakukan berdasarkan konsumsi sumber daya (CPU, Memory dan *Bandwidth*) serta *response time* dari *server*. Pengujian dilakukan dalam lingkungan simulasi yang terkontrol menggunakan perangkat lunak *VirtualBox* dan *Docker* sebagai *server* uji coba. Hasil penelitian ini menunjukkan bahwa *Slowloris* adalah serangan yang paling efektif dalam menyebabkan kelumpuhan total layanan hingga lebih dari 20 menit dengan dampak sumber daya yang minimal. Serangan *Wendigo* efektif menyebabkan *high latency* hingga 2 menit dengan membebani CPU. Sebaliknya *Hping3* terbukti paling tidak efektif dalam mengganggu ketersediaan layanan

meskipun menjadi serangan yang paling banyak mengonsumsi sumber daya. Penelitian ini menyimpulkan bahwa kerentanan server *GraphQL* tidak hanya terletak pada volume lalu lintas, tetapi juga pada manajemen koneksi dan logika pemrosesan *query* yang kompleks sehingga memerlukan strategi mitigasi berlapis.

Kata Kunci: *Wendigo*, *Deep Reinforcement Learning*, *GraphQL*, *Denial of Service*, DoS, *Slowloris*, Hping3, *Damn Vulnrtable GraphQL Application*, DVGA

KATA PENGANTAR

Bismillahirrahmanirrahim,

Alhamdulillahi Rabbil ‘alamin, puji dan syukur kepada Allah SWT. yang telah melimpahkan rahmat dan karunia-Nya yang telah memberikan kekuatan dan kemudahan sehingga penulis berhasil merampungkan Tugas Akhir ini, untuk melengkapi syarat dalam menyelesaikan pendidikan program S1 pada program studi Teknologi Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Ar-Raniry. Tulisan ini berjudul “PERBANDINGAN SERANGAN DOS BERBASIS *DEEP REINFORCEMENT LEARNING* DAN KONVENSIONAL TERHADAP APLIKASI *GRAPHQL*”. Shalawat dan salam semoga senantiasa tercurah kepada teladan kita, Nabi Muhammad SAW., yang telah membawa umat manusia menuju ke zaman yang penuh ilmu pengetahuan hingga akhir zaman.

Dalam proses penyusunan tugas akhir ini, penulis banyak mendapat bimbingan dan arahan dari berbagai pihak, maka dari itu penulis ingin mengucapkan terima kasih dan penghargaan yang tak terhingga kepada:

1. Ayahanda Amiruddin dan Ibunda Ruslaini, yang telah mendidik penulis dengan penuh keimanan, kesabaran dan ketulusann. Semua pengorbanan mereka, baik doa maupun dukungan yang tidak terhenti hingga saat ini.
2. Saudara penulis Alifia Fajri, Asyraf Arraniry dan Alfathiya Fitri yang selalu memberikan dukungan selama penulis menjalani masa kuliah.
3. Bapak Mulkan Fadhli, S.T., M.T., dan Bapak Aulia Syarif Aziz, S.Kom., M.Sc. selaku pembimbing tugas akhir yang telah bersedia meluangkan waktu, tenaga, pikiran serta memberikan arahan dan masukan yang sangat berguna dalam menyelesaikan tugas akhir.
4. Ibu Malahayati, M.T. selaku ketua Program Studi Teknologi Informasi Fakultas Sains dan Teknologi UIN Ar-Raniry.
5. Bapak Khairan AR, M.Kom. selaku pembimbing akademik yang telah memberikan arahan dan masukan kepada penulis selama menempuh studi.
6. Ibu Cut Ida Rahmadiana, S.Si. atas segala bantuan, kemudahan dan kesabaran dalam proses pengurusan administrasi akademik yang sangat menunjang kelancaran studi penulis.

7. Bapak Prof. Dr. Ir. M. Dirhamsyah, M.T., IPU. selaku Dekan Fakultas Sains dan teknologi UIN Ar-Raniry.
8. Seluruh Bapak dan Ibu Dosen di lingkungan Program Studi Teknologi Informasi dan Fakultas Sains dan Teknologi UIN Ar-Raniry yang telah membagikan ilmu pengetahuan dan wawasan yang tidak ternilai.
9. Teman-teman seperjuangan yang telah menjadi bagian penting dalam perjalanan akademik penulis yang tidak dapat penulis sebutkan satu per satu.
10. Semua pihak yang tidak dapat penulis sebutkan satu per satu yang telah memberikan kontribusi dalam penyelesaian Tugas Akhir ini.

Penulis sepenuhnya menyadari bahwa Tugas Akhir ini masih jauh dari sempurna, maka dari itu penulis menerima saran dan kritikan yang bersifat membangun tulisan ini demi penyempurnaan kedepannya. Akhir kata, semoga skripsi ini dapat menjadi amal ibadah dan memberikan manfaat yang luas bagi ilmu pengetahuan dan bagi para pembaca. Aamiin yaa Rabbal ‘alamiin.

Banda Aceh, 18 Agustus 2025

Penulis,

Muammar Al Faruqi

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi telah mendorong perkembangan web untuk mengadopsi *GraphQL* sebagai alternatif yang lebih fleksibel dibandingkan *RESTful* API dalam pengelolaan data. Keunggulan *GraphQL* memungkinkan klien untuk mengambil data secara spesifik membuat API ini semakin populer di berbagai sistem terkini. Akan tetapi fleksibilitas ini juga membuka celah keamanan terutama terhadap serangan *DoS* (*Denial of Service*) yang dapat menyebabkan kelumpuhan layanan akibat kelebihan beban permintaan (Firdaus et al., 2024).

Serangan *DoS* konvensional seperti *Hping3* dan *Slowloris* sering digunakan untuk membanjiri *server* dengan permintaan berlebih atau mempertahankan koneksi dalam waktu lama sehingga menyebabkan sumber daya terkuras (Sabri et al., 2021). Namun serangan ini memiliki pola yang mudah dikenali oleh sistem pertahanan seperti *firewall* dan *rate limiting* sehingga efektivitasnya menurun seiring berkembangya mekanisme pencegahan keamanan (Firdaus et al., 2024).

Kemajuan dalam *Machine Learning* (ML) di sisi lain telah melahirkan pendekatan baru dalam serangan *DoS*, salah satunya adalah *Wendigo* yang merupakan sebuah metode serangan yang berbasis *Reinforcement Learning* (RL). *Wendigo* memiliki kemampuan untuk beradaptasi dengan respon dari *server* sehingga terhindar dari deteksi dan dapat menyesuaikan strategi secara dinamis. *Wendigo* dapat memilih metode serangan yang paling efektif dengan memanfaatkan *Machine Learning* untuk menembus sistem pertahanan dan memaksimalkan dampak dengan sumber daya yang lebih efisien dibandingkan serangan *DoS* konvensional (McFadden et al., 2024).

Pada penelitian sebelumnya, metode *Deep Reinforcement Learning* (DRL) seperti yang digunakan pada *Wendigo* dapat mengeksploitasi kelemahan dalam sistem *GraphQL* secara efektif dengan menghasilkan *query* yang kompleks dan membebani *server* secara optimal. *Wendigo* dapat menemukan *query* yang menyebabkan serangan *DoS* hanya dengan dua *request* per jam yang dimana jauh

lebih efisien dibandingkan dengan serangan *DoS* Konvensional yang mengandalkan jumlah *traffic* yang besar (McFadden et al., 2024).

Mengingat potensi dari ancaman yang ditimbulkan, perbandingan antara serangan *DoS* berbasis *Deep Reinforcement Learning* (DRL) yang menggunakan *Wendigo* dan serangan *DoS* konvensional seperti *Slowloris* dan *Hping3* terhadap *server GraphQL* perlu untuk dilakukan. Penelitian ini memiliki tujuan untuk mengukur efektivitas masing-masing metode serangan serta kemampuan menembus sistem pertahanan. Hasil dari penelitian ini diharapkan dapat memberikan wawasan lebih mendalam tentang tingkat kerentanan *GraphQL* terhadap berbagai serangan *DoS* serta memberikan referensi dalam pengembangan strategi mitigasi yang lebih efektif.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, berikut adalah rumusan masalah pada penelitian ini:

1. Bagaimana efektivitas serangan *DoS* berbasis Deep Reinforcement dibandingkan serangan *DoS* konvensional dalam melumpuhkan *server GraphQL*?
2. Bagaimana perbedaan konsumsi sumber daya seperti *CPU*, *memory* dan *bandwidth* yang disebabkan oleh masing-masing serangan?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini berdasarkan latar belakang di atas, yaitu:

1. Menganalisis efektivitas serangan *Wendigo* dibandingkan dengan serangan *DoS* konvensional terhadap *server GraphQL*.
2. Mengukur dan membandingkan konsumsi sumber daya *server* seperti *CPU*, *memory* dan *bandwidth* selama serangan berlangsung.

1.4 Batasan Penelitian

Berikut adalah batasan masalah yang akan dibahas dalam penelitian ini agar sesuai dengan judul dan latar belakang yang telah diruaikan sebelumnya:

1. Penelitian ini hanya berfokus pada serangan *Denial of Service* (DoS) berbasis *Deep Reinforcement* dan *DoS* konvensional.
2. Penelitian difokuskan pada *server GraphQL* dengan lingkunan uji coba lokal menggunakan mesin virtual.
3. Efektifvitas serangan diukur berdasarkan konsumsi sumber daya *server* seperti *CPU*, *memory* dan *bandwidth* dan *response time* yang didapatkan saat membuka aplikasi target.
4. Pengujian ini dilakukan dalam lingkungan yang terkontrol menggunakan *virtual machine* atau *server* lokal dengan spesifikasi yang telah ditentukan.
5. Penelitian ini tidak mencakup analisis mendalam tentang deteksi berasis AI, melainkan hanya menguji efektivitas serangan yang dilakukan.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memerikan manfaat baik dari sisi akademis maupun praktis seperti berikut:

1. Menambah wawasan khususnya di bidang siber berkaitan dengan serangan *DoS* berbasis *Machine Learning* (*Wendigo*) dan *DoS* konvensional (*Slowloris* dan *Hping3*) terhadap *server GraphQL*.
2. Menjadi referensi bagi penelitian selanjutnya dalam mengembangkan metode serangan dan pertahanan terhadap ancaman *DoS* pada sistem berbasis *GraphQL*.
3. Memberikan informasi kepada administrator sistem dan pengembang web tentang tingkat kerentanan *server GraphQL* terhadap berbagai jenis serangan *DoS*.