PENGEMBANGAN MODEL *REINFORCEMENT LEARNING* DENGAN ALGORITMA *DEEP Q NETWORK* (DQN) DAN *PROXIMAL POLICY OPTIMIZATION* (PPO) UNTUK MULTIKLASIFIKASI SERANGAN SIBER

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana Komputer

Oleh:

Farrel Firjatullah

09011382126164

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

PENGEMBANGAN MODEL *REINFORCEMENT LEARNING* DENGAN ALGORITMA *DEEP Q NETWORK* (DQN) DAN *PROXIMAL POLICY OPTIMIZATION* (PPO) UNTUK MULTIKLASIFIKASI SERANGAN SIBER

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Koomputer

Oleh:

Farrel Firjatullah

09011382126164

Pembimbing 1 : **Dr. Ahmad Heryanto, S.Kom, M.T.**

NIP. 198701222015041002

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T

196612032006041001

AUTHENTICATION PAGE

FINAL TASK

DEVELOPMENT OF REINFORCEMENT LEARNING MODEL USING DEEP Q NETWORK (DQN) AND PROXIMAL POLICY OPTIMIZATION (PPO) ALGORITHMS FOR CYBER ATTACK MULTICLASSIFICATION

As one of the requirements for the completion of studies in the Bachelor's Degree Program in Computer Systems

By:

Farrel Firjatullah

09011382126164

Supervisor 1 : **Dr. Ahmad Heryanto, S.Kom, M.T.**

NIP. 198701222015041002

Acknowledge

Head of Computer System Department

Dr. Ir. Sukemi, M.T

196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 9 Mei 2025

Tim Penguji :

1. Ketua : Dr. Rossi Passarella, S.T., M.eng
2. Penguji : Prof. Ir. Deris Setiawan, M.T., Ph.D.
3. Pembimbing : Dr. Ahmad Heryanto, S.Kom, M.T.

Mengetahui, 5/6/25
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang Bertanda Tangan Di Bawah Ini :

Nama : Farrel Firjatullah

NIM : 09011382126164

Judul : PENGEMBANGAN MODEL REINFORCEMENT LEARNING DENGAN ALGORITMA DEEP Q NETWORK (DQN) DAN PROXIMAL POLICY OPTIMIZATION (PPO) UNTUK MULTIKLASIFIKASI SERANGAN SIBER

Hasil Pengecekan Software iThenticate/Turnitin : 1%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan

Palembang, Mei 2025

Penulis,

Farrel Firjatullah

NIM. 09011382126164

KATA PENGANTAR

Dengan penuh rasa Syukur dan sangat kerendahan hati, penulis panjatkan puji dan Syukur kehadirat Allah swt. Atas nikmat dan karunianya yang masih dilimpahkan, sehingga penulis dapat menyelesaikan penyusunan Skripsi dan Laporan Tugas Akhir ini yang berjudul " **PENGEMBANGAN MODEL *REINFORCEMENT LEARNING* DENGAN ALGORITMA *DEEP Q NETWORK* (DQN) DAN *PROXIMAL POLICY OPTIMIZATION* (PPO) UNTUK MULTIKLASIFIKASI SERANGAN SIBER**"

Dalam penyusunan Skripsi dan Tugas Akhir ini tidak terlepas dari peran serta beberapa orang dan pihak yang sangat membantu penulis oleh karena itu dengan hati yang tulus dan penuh dengan keihklasan, penulis ingin menyampaikan rasa syukur dan terima kasih yang sebesar – besarnya kepada :

1. Keluarga kecil saya, papa, kak caca dan mama yang telah memberikan banyak sekali dukungan dan doa – doa kepada penulis dalam mengerjakan pengerjaan Skripsi dan Tugas Akhir.
2. Bapak Prof. Dr, Erwin, S.Si., M.Si., selaku dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. Sukemi, M.T. selaku ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ahmad Heryanto, S.Kom., M.T., selaku dosen pembimbing Tugas Akhir yang telah membimbing saya dalam proses pengerjaan Skripsi dan Tugas Akhir ini, terima kasih atas ilmu dan waktu yang telah diberikan untuk membimbing saya dalam pengerjaan Tugas Akhir ini, semua arahan dan masukan dari bapak menjadi sebuah motivasi penulis dalam penyelesaian penelitian ini.
5. Bapak Iman Saladin B. Azhar S.Kom., M.MSI selaku dosen pembimbing akademik saya yang selalu penuh perhatian memberikan saran dan masukan selama masa studi saya di Universitas Sriwijaya.

6. Ibu Sari Nurhaliza selaku administrasi jurusan yang selalu sigap membantu mahasiswa dalam melakukan urusan administrasi akademik dengan penuh kesabaran dan mempermudah perjalanan saya selama menjadi mahasiswa Universitas Sriwijaya.
7. Saya juga ingin menyampaikan rasa terima kasih kepada teman terdekat sekaligus teman terbaik yaitu Guntur, Dean dan Aldi yang selalu menemani saya dan selalu support dalam menjadi mahasiswa Universitas Sriwijaya.
8. Ucapan terima kasih saya sampaikan kepada seseorang yang selalu memberikan dukungan, semangat dan motivasi dalam setiap langkah saya dalam menyelesaikan penelitian ini yaitu Mutia Yasmin Azzahra, kehadiran serta dorongan yang diberikan sangat berarti bagi saya dalam menghadapi berbagai tantangan selama proses ini.
9. Tak lupa, penghargaan ini saya persembahkan kepada diri saya sendiri. Terima kasih telah berjuang dari awal hingga akhir dalam melewati masa Pendidikan di Universitas Sriwijaya, terima kasih telah bertahan dan tidak menyerah di segala rintangan.

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis. Akhir kata penulis berharap, semoga proposal tugas akhir ini bermanfaat dan berguna bagi rekan lainnya.

Palembang, Maret 2025

Penulis,

Farrel Firjatullah

NIM 09011382126164

PENGEMBANGAN MODEL *REINFORCEMENT LEARNING* DENGAN ALGORITMA *DEEP Q NETWORK* (DQN) DAN *PROXIMAL POLICY OPTIMIZATION* (PPO) UNTUK MULTIKLASIFIKASI SERANGAN

Farrel Firjatullah

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : firjatulahfarel@gmail.com

ABSTRAK

Pada zaman digital sekarang yang makin pesat ini, keamanan sistem dan jaringan sangat penting dalam lingkungan komunikasi digital. Teknik pembelajaran mesin pada saat ini sangat banyak varian metode dan algoritma, salah satunya adalah *Reinforcment Learning* (RL) yang dapat digunakan dalam menyelesaikan masalah ini. Dalam penelitian ini akan membahas mengenai algoritma *Deep Q Network* (DQN) dan *Proximal Policy Optimization* (PPO) dari model *Reinforcement Learning* untuk mendeteksi multiklasifikasi dari serangan siber. Dalam implementasinya menggunakan dataset ISCX 2012, CICDDOS 2019, KDDCup 1999 dan NSL-KDD, agen RL berhasil mempelajari pola serangan secara efektif. Untuk menguji efisiensi dari implementasi penelitain ini, Hasil penelitian menunjukkan bahwa pada algortima DQN mendapatkan akurasi sebesar 89.27% pada dataset ISCX 2012, 97.49% pada dataset CICDDOS 2019, 94.48% pada dataset KDDCup 1999 dan 86.83% pada dataset NSL-KDD, untuk algoritma PPO sebesar 84.00% pada dataset ISCX 2012, 87.00% pada dataset CICDDOS 2019, 95.00% pada dataset KDDCup 1999 dan 85.19% pada dataset NSL-KDD.

Kata Kunci : *Reinforcement Learning*, Multiklasifikasi, *Deep Q Network*, *Proximal Policy Optimization*

DEVELOPMENT OF REINFORCEMENT LEARNING MODEL USING DEEP Q NETWORK (DQN) AND PROXIMAL POLICY OPTIMIZATION (PPO) ALGORITHMS FOR CYBER ATTACK MULTICLASSIFICATION

Farrel Firjatullah

Department of Computer Systems, Faculty of Computer Science, Sriwijaya University

Email : firjatulahfarel@gmail.com

ABSTRACT

In digital era right now, with the rapid advancement of time, system and network security is very important in the digital communication environment. Machine learning techniques are currently one of the many methods used to address this, including a method known as Reinforcement Learning (RL), which can be used to solve classification problems. In this study, we discuss the application of the Deep Q Network (DQN) and Proximal Policy Optimization (PPO) algorithms from the Reinforcement Learning model to detect multiclass classification of cyber attacks. The impleme'tation was conducted using the ISCX 2012, CICDDoS 2019, KDDCup 1999, and NSL-KDD datasets, and RL successfully learned attack patterns effectively. To evaluate the effectiveness of the model, performance measurements were carried out using the DQN algorithm and achieved an accuracy of 89.27% on the ISCX 2012 dataset, 97.49% on the CICDDoS 2019 dataset, 94.48% on the KDDCup 1999 dataset, and 86.83% on the NSL-KDD dataset. Meanwhile, the PPO algorithm achieved 84.00% on the ISCX 2012 dataset, 87.00% on the CICDDoS 2019 dataset, 95.00% on the KDDCup 1999 dataset, and 85.19% on the NSL-KDD dataset.

Keywords : *Reinforcement Learning*, *Multiclassification*, *Deep Q Network*, *Proximal Policy Optimization*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam zaman digital sekarang ini kita tidak asing dengan kata serangan jaringan atau disebut *Cyber Attack*, serangan jaringan dimulai dengan menggunakan serangkaian operasi komputer yang membahayakan keamanan sistem jaringan, termasuk integritas, kerahasiaan, dan ketersediaannya [1]. Ada banyak sekali jenis serangan jaringan yang dilakukan oleh beberapa kelompok ataupun individu salah satunya adalah *Denial of Service* (DoS) serangan DoS ini menargetkan ketersediaan data, seperti dengan membanjiri saluran komunikasi sehingga data yang diperlukan tidak tersedia [2]. Selain DoS ada salah satu serangan jaringan yang berbahaya juga yaitu *False Data Injection Attack* (FDIA), sistem serangan FDIA ini dengan cara merusak integritas data dengan menyisipkan data palsu ke dalam sistem komputer, sehingga mengganggu estimasi dan kontrol sistem komputer. FDIA juga dapat memanipulasi pengukuran atau sinyal sehingga sistem menghasilkan respon yang salah[3].

Masih banyak lagi serangan jaringan lainnya seperti *Phishing*, serangan *Malware*, SQL *Injection*. Bisa kita lihat berbagai jenis serangan jaringan sangat serius di zaman penuh teknologi ini dan menjadi ancaman yang berbahaya ada banyak sekali efek negatif dari serangan jaringan [4]. Salah satu dampak negatifnya adalah kerumitan dan kompleksitas sistem, sistem keamanan yang kompleks bisa menimbulkan kesulitan operasional terutama bagi tim yang tidak memiliki keahlian teknis yang cukup. Kompleksitas ini juga sangat memperlambat respon dalam situasi yang membutuhkan tindakan cepat, yang bisa berisikio bagi keamanan keseluruhan sistem [1]. Lalu serangan jaringan yang berhasil juga dapat mengakibatkan kerugian dari segi finansial yang siginifikan bagi perusahaan dan individu, hilangnya data penting, serta rusaknya reputasi organisasi. Selain itu, serangan jaringan seperti malware dan phishing dapat menyebabkan penyebaran infeksi ke berbagai perangkat lunak dan sistem komputer yang saling terhubung,

yang memperparah kerusakan dan menambah kerumitan dalam proses pemulihan [5].

Kendala lain dari serangan jaringan ini juga adalah tingginya biaya yang diperlukan untuk mempertahankan sistem keamanan yang canggih dan selalu diperbarui. Ada banyak perusahaan, terutama yang berskala kecil hingga menengah sering kali merasa terbebani oleh biaya operasional ini, yang pada akhirnya membuat mereka rentan terhadapa serangan jaringan. Dalam hal ini, model *Artificial Intelligence* khususnya pendekatan *Machine Learning* dan *Reinforcement learning* menjadi solusi yang menarik karena kemampuan adaptasinya terhadap ancaman yang dinamis penelitian-penelitian sebelumnya telah memanfaatkan berbagai dataset popular untuk pengembangan model deteksi serangan, seperti ISCX 2012, CICDDOS 2012, KDDCup 1999 dan NSL-KDD [6].

Pada penelitian [7] membahas tentang *cyber attack* dengan metode *Deep Neural Network* (DNN), dataset yang digunakan adalah dataset KDD – Cup'99 dan NSL-KDD, dari percobaan penelitian ini dataset KDD – Cup'99 menunjukkan akurasi sebesar 96.3% dan dataset dari NSL – KDD menunjukkan akurasi sebesar 91.5% pada saat uji coba pelatihan. Tetapi, kekurangan dari penelitian ini adalah metode DNN masih memiliki kekurangan dalam menangani ketidakseimbangan kelas pada dataset, sehingga Tingkat akurasi deteksi pada jenis serangan serangan tertentu terutama serangan yang jarang terjadi harus ditingkatkan. Selain itu, model ini juga memerlukan waktu komputasi yang cukup tinggi, sehingga kecepatan dalam mendeteksi serangan juga perlu dievakuasi lebih lanjut untuk meningkatkan efisiensi dalam aplikasi nyata.

Pada penelitian [8] membahas terkait dengan metode *Long-Short Term Memory – Multi-Scale Convolutional Neural Network* (LSTM-MSCNN) pada dataset NSL-KDD fungsi dari metode ini untuk mengekstraksi fitur spasial dari data jaringan pada berbagai Tingkat kedalaman dan skala, dari percobaan penelitian ini pada dataset NSL-KDD menunjukkan akurasi sebesar 83.45% pada saat uji coba pelatihan. Kekurangan yang menjadi sorotan pada penelitain ini adalah bahwa model sudah mencapai akurasi yang baik. Namun, Tingkat deteksi pada beberapa

kategori serangan minoritas seperti U2R dan R2L masih terlihat rendah, sehingga perlu peningkatan lebih lanjut. Selain itu, meskipun menggunakan Teknik data augmentasi dan kombinasi model CNN-LSTM, kecepatan deteksi masih memerlukan evaluasi yang lebih lanjut, mengingat kompleksitas komputasi yang tinggi dalam pelatihan dan pengujian model.

Metode *reinforcement learning*, seperti algoritma *Deep Q Network* (DQN) dan *Proximal Policy Optimization* (PPO), menawarkan pendekatan baru dalam sistem keamanan jaringan yang mampu mempelajari pola serangan yang ada maupun yang baru muncul, DQN, dengan kemampuan untuk beradaptasi melalui pembelajaran dari nilai Q yang terus diperbarui, memungkinkan sistem untuk mengenali ancaman yang kompleks dan mengambil Tindakan preventif secara optimal [9]. Dengan memanfaatkan jaringan saraf dalam pemetaan kondisi dan tindakan yang tepat, DQN mampu meningkatkan keakuratan deteksi serangan jaringan, sekaligus menyediakan solusi yang lebih efisien dibandingkan metode tradisional.

Sementara itu, PPO memiliki keunggulan dalam stabilitas dan efisiensi, terutama dalam pengambilan keputusan yang cepat dan akurat di lingkungan keamanan siber yang dinamis [10]. PPO menggunakan pendekatan berbasis kebijakan yang lebih stabil dibandingkan dengan metode berbasis nilai seperti DQN, sehingga lebih cocok untuk diterapkan pada sistem keamanan yang memerlukan respons *real-time*. Dalam PPO, pemangkasan (*clipping*) dan pembaruan yang konservatif pada kebijakan memungkinkan model untuk menghindari perubahan drastis yang dapat mengakibatkan ketidakstabilan, menjadikannya pilihan yang tepat untuk lingkungan yang sangat dinamis dan memerlukan respon yang cepat [11].

Berdasarkan latar belakang di atas, kedua algoritma tersebut diaplikasikan untuk mengklasifikasikan berbagai jenis serangan dalam dataset multiklasifikasi, sehingga sistem dapat mendeteksi serangan secara cepat dan efektif. Metode ini diharapkan mampu memberikan solusi yang tidak hanya lebih adaptif tetapi juga efisien dalam mendeteksi berbagai jenis serangan yang ada, sehingga dapat meningkatkan ketahanan keamanan siber di tengah perkembangan teknologi yang

pesat. Maka dari itu dalam penelitian yang diajukan dalam proposal ini akan meneliti terkait "PENGEMBANGAN MODEL *REINFORCEMENT LEARNING* DENGAN ALGORITMA *DEEP Q NETWORK* (DQN) DAN *PROXIMAL POLICY OPTIMIZATION* (PPO) MULTIKLASIFIKASI SERANGAN SIBER" dengan menggunakan berbagai dataset seperti ISCX 2012, CICDDOS 2019, KDDCup 1999 dan NSL-KDD.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah penulis buat, maka perumusan masalah penelitian ini adalah sebagai berikut:

1. Pengimplementasian pengguna metode *Reinforcement Learnig* dengan algoritma DQN dan PPO yang diharapkan mampu dalam melakukan pendeteksian serangan jaringan multiklasifikasi.
2. Seberapa besar tingkat akurasi dalam perancangan model sistem deteksi serangan jaringan multiklasifikasi menggunakan metode algoritma DQN dan PPO.

1.3 Tujuan

Berdasarkan rumusan masalah yang penulis buat sebelumnya, tujuan yang akan dicapai dalam penelitian ini adalah sebagai berikut:

1. Membuat sistem model metode *Reinforcement Learning* dengan algoritma DQN dan PPO untuk menghasilkan deteksi akurasi yang baik dalam dataset serangan jaringan multiklasifikasi.
2. Menyajikan hasil evaluasi model pada sistem deteksi multiklasifikasi menggunakan metode *Reinforcement Learning*.
3. Mengetahui efektivitas penggunaan metode *Reinforcement Learning* dalam pengujian beberapa jenis dataset serangan jaringan multiklasifikasi.

1.4 Manfaat

Berdasarkan Tujuan yang penulis buat sebelumnya, maka manfaat dari penelitian ini adalah sebagai berikut:

1. Mampu menghasilkan akurasi deteksi yang baik dalam mendeteksi dataset serangan jaringan multiklasifikasi.
2. Dapat membangun sistem deteksi serangan jaringan multiklasifikasi yang akurat dan efektif dalam mendeteksi serangan siber, sehingga dapat memberikan perlindungan yang lebih baik bagi sistem dan data.
3. Mewaspadai gangguan operasional agar tidak berkembang menjadi isu besar di Tingkat organisasi hingga Lembaga pemerintahan.

1.5 Batasan Masalah

Batasan masalah yang terdapat dalam penyusunan Skripsi ini adalah sebagai berikut:

1. Pada penelitian ini, menggunakan metode *Reinforcement Learning* dengan algoritma DQN dan PPO yang akan diimplementasikan pada beberapa jenis dataset, diantaranya adalah ISCSX 2012, CICDDOS 2019, KDDCup 1999, dan NSL-KDD.
2. Penelitian ini menghasilkan ouput akurasi model yang di gunakan sebagai tolak ukur dengan melihat Tingkat efisien yang dihasilkan dari pengguna metode *Reinforcement Learning* pada setiap dataset.

1.6 Metodologi Penelitian

Berikut ini adalah tahapan metodologi yang digunakan dalam melakukan penelitian ini adalah sebagai berikut:

1. Metode Studi Literatur

   Pada tahap awal ini akan membahasa terkait literatut dan referensi seperti buku, jurnal ilmia, dan karya ilmiah lainnya yang berkaitan dengan Multiklasifikasi serangan jaringan beserta konsep dari algoritma DQN dan PPO.
2. Metode Perancangan Model

   Pada metode ini, dilakukan pembuatan model untuk environment yang merepresentasikan scenario nyata dari serangan jaringan. Model ini akan

digunakan dalam pembuatan flowchart dan implementasi sistem deteksi intrusi berbasis algoritma DQN dan PPO.

3. Metode Pengujian

   Pada tahap ini akan dilakukan proses pengujian dari perancangan model yang telah dibuat. Pengujian akan menghasilkan nilai akurasi yang dapat digunakan untuk menganalisis hasil kinerja.

4. Metode analisis dan Kesimpulan

   Hasil pengujian pada penelitian ini akan dianalisis untuk mengetahui kekurangan dan kelebihan algoritma yang digunakan. Lalu akan dilakukan proses analisis dari output yang telah didapatkan, bertujuan untuk mengetahui kekurangan pada hasil perancangan dan factor apa saja yang menjadi penyebabnya. Berdasarkan dari analisis tersebut akan dibuat sebuah Kesimpulan dan saran untuk penelitian selanjutnya dalam penelitian ini.

1.7 Sistematikan Penulisan

BAB I PENDAHULUAN

Pada BAB I ini berisikan penjelasan secara sistematis mengenai topik penelitian yang diambil meliputi latar belakang, rumusan masalah, tujuan, manfaat, batasan masalah, metodologi penelitian yang digunakan, dan mengenai sistematika penulisan penelitian

BAB II TINJAUAN PUSTAKA

Pada BAB II ini akan menjelaskan sub-bab mengenai literatur dan penulisan terkait Metode Reinforcement Learning dan algoritma DQN dan PPO yang digunakan sebagai sebuah acuan dalam mengembangkan sistem model dan metode yang digunakan dalam penelitian.

BAB III METODOLOGI PENELITIAN

Pada BAB III ini menjelaskan Langkah – Langkah yang dilakukan dalam penelitian ini. Setiap rencana tahapan peneelitian dijelaskan lebih rinci menggunakan kerangka kerja.

BAB IV HASIL DAN PEMBAHASAN

Pada BAB IV ini akan menjelaskan mengenai hasil dari pengujian yang telah dilakukan selama penelitian. Hasil akhir dari pengujian tersebut akan dianalisis dari output algoritma DQN dan PPO seberapa besar atau kecil tingkatan akurasinya.

BAB V KESIMPULAN DAN SARAN

Pada BAB V ini berisi kesimpulan akhir dari pembahasan penelitian yang telah dilakukan. Pada bab ini juga terdapat saran yang diperlukan untuk pengembangan penelitian selanjutnya dari pengujian dan analisis penelitian.

DAFTAR PUSTAKA

[1] V. Rasikha and P. Marikkannu, “An ensemble deep learning-based cyber attack detection system using optimization strategy,” *Knowl Based Syst*, vol. 301, Oct. 2024, doi: 10.1016/j.knosys.2024.112211.

[2] Q. Liu, J. Wang, Y. Ni, C. Zhang, L. Shi, and J. Qin, “Performance analysis for cyber–physical systems under two types of stealthy deception attacks,” *Automatica*, vol. 160, Feb. 2024, doi: 10.1016/j.automatica.2023.111446.

[3] H. Qi, H. Wu, and X. Zheng, “Recursive state estimation for delayed complex networks with random link failures and stochastic inner coupling under cyber attacks,” *Digital Signal Processing: A Review Journal*, vol. 156, Jan. 2025, doi: 10.1016/j.dsp.2024.104784.

[4] R. Sepehrzad, A. Khodadadi, S. Adinehpour, and M. Karimi, “A multi-agent deep reinforcement learning paradigm to improve the robustness and resilience of grid connected electric vehicle charging stations against the destructive effects of cyber-attacks,” *Energy*, vol. 307, Oct. 2024, doi: 10.1016/j.energy.2024.132669.

[5] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, “Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach,” *IEEE Trans Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2018, doi: 10.1109/TSG.2018.2878570.

[6] S. Z. Golazad, A. Mohammadi, A. Rashidi, and M. Ilbeigi, “From raw to refined: Data preprocessing for construction machine learning (ML), deep learning (DL), and reinforcement learning (RL) models,” Dec. 01, 2024, *Elsevier B.V.* doi: 10.1016/j.autcon.2024.105844.

[7] S. Choudhary and N. Kesswani, “Analysis of KDD-Cup’99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT,” in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 1561–1573. doi: 10.1016/j.procs.2020.03.367.

[8] Z. Li, C. Huang, and W. Qiu, “An intrusion detection method combining variational auto-encoder and generative adversarial networks,” *Computer Networks*, vol. 253, Nov. 2024, doi: 10.1016/j.comnet.2024.110724.

[9] Y. Zhang, Z. Zhang, Q. Yang, D. An, D. Li, and C. Li, “EV charging bidding by multi-DQN reinforcement learning in electricity auction market,” *Neurocomputing*, vol. 397, pp. 404–414, Jul. 2020, doi: 10.1016/j.neucom.2019.08.106.

[10] S. Yin and Z. Xiang, “A hyper-heuristic algorithm via proximal policy optimization for multi-objective truss problems,” *Expert Syst Appl*, vol. 256, Dec. 2024, doi: 10.1016/j.eswa.2024.124929.

[11] X. Lü, S. Qian, X. R. Zhai, P. Wang, and T. Wu, “Adaptive energy management strategy for FCHEV based on improved proximal policy

optimization in deep reinforcement learning algorithm," *Energy Convers Manag*, vol. 321, Dec. 2024, doi: 10.1016/j.enconman.2024.118977.

[12] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," *Comput Secur*, vol. 92, May 2020, doi: 10.1016/j.cose.2020.101752.

[13] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset," *IEEE Access*, vol. 8, pp. 29575–29585, 2020, doi: 10.1109/ACCESS.2020.2972627.

[14] E. H. Asmaa, K. Jihad, T. Hicham, B. Faycal, and B. Youssef, "Cyber Attacks Management in IoT Networks Using Deep Learning and Edge Computing," *Procedia Comput Sci*, vol. 251, pp. 721–726, 2024, doi: 10.1016/j.procs.2024.11.175.

[15] W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei, and F. Sabrina, "Improving Performance of Autoencoder-Based Network Anomaly Detection on NSL-KDD Dataset," *IEEE Access*, vol. 9, pp. 140136–140146, 2021, doi: 10.1109/ACCESS.2021.3116612.

[16] S. Sengan, S. V, I. V, P. Velayutham, and L. Ravi, "Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning," *Computers and Electrical Engineering*, vol. 93, Jul. 2021, doi: 10.1016/j.compeleceng.2021.107211.

[17] A. Alzu'bi, A. Albashayreh, A. Abuarqoub, and M. A. M. Alfawair, "Explainable AI-Based DDoS Attacks Classification Using Deep Transfer Learning," *Computers, Materials and Continua*, vol. 80, no. 3, pp. 3785–3802, 2024, doi: 10.32604/cmc.2024.052599.

[18] S. Venkatraman, M. Alazab, and R. Vinayakumar, "A hybrid deep learning image-based analysis for effective malware detection," *Journal of Information Security and Applications*, vol. 47, pp. 377–389, Aug. 2019, doi: 10.1016/j.jisa.2019.06.006.

[19] Kunal and M. Dua, "Attribute Selection and Ensemble Classifier based Novel Approach to Intrusion Detection System," in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 2191–2199. doi: 10.1016/j.procs.2020.03.271.

[20] S. S. Volkov and I. I. Kurochkin, "Network attacks classification using Long Short-Term memory based neural networks in Software-Defined Networks," in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 394–403. doi: 10.1016/j.procs.2020.11.041.

[21] A. K. Silivery, R. M. Rao Kovvur, R. Solleti, L. S. Kumar, and B. Madhu, "A model for multi-attack classification to improve intrusion detection performance using deep learning approaches," *Measurement: Sensors*, vol. 30, Dec. 2023, doi: 10.1016/j.measen.2023.100924.

[22] L. Yuan *et al.*, "Semi-supervised anomaly detection with contamination-resilience and incremental training," *Eng Appl Artif Intell*, vol. 138, Dec. 2024, doi: 10.1016/j.engappai.2024.109311.

[23] K. N, V. Ravi, and V. Sowmya, “Unsupervised intrusion detection system for in-vehicle communication networks,” *Journal of Safety Science and Resilience*, vol. 5, no. 2, pp. 119–129, Jun. 2024, doi: 10.1016/j.jnlssr.2023.12.004.

[24] C. K V K and L. R. V. , “Automatic intrusion detection model with secure data storage on cloud using adaptive cyclic shift transposition with enhanced ANFIS classifier,” *Cyber Security and Applications*, vol. 3, Dec. 2025, doi: 10.1016/j.csa.2024.100073.

[25] V. Ciric, M. Milosevic, D. Sokolovic, and I. Milentijevic, “Modular deep learning-based network intrusion detection architecture for real-world cyber-attack simulation,” *Simul Model Pract Theory*, vol. 133, May 2024, doi: 10.1016/j.simpat.2024.102916.

[26] S. S. Bamber, A. V. R. Katkuri, S. Sharma, and M. Angurala, “A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system,” *Comput Secur*, vol. 148, Jan. 2025, doi: 10.1016/j.cose.2024.104146.

[27] A. K. Dey, G. P. Gupta, and S. P. Sahu, “Hybrid Meta-Heuristic based Feature Selection Mechanism for Cyber-Attack Detection in IoT-enabled Networks,” in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 318–327. doi: 10.1016/j.procs.2023.01.014.

[28] N. S. Alotaibi, “An Efficient Cyber Security and Intrusion Detection System Using CRSR with PXORP-ECC and LTH-CNN,” *Computers, Materials and Continua*, vol. 76, no. 2, pp. 2061–2078, Aug. 2023, doi: 10.32604/cmc.2023.039446.

[29] D. Mukherjee, “Detection of data-driven blind cyber-attacks on smart grid: A deep learning approach,” *Sustain Cities Soc*, vol. 92, May 2023, doi: 10.1016/j.scs.2023.104475.

[30] S. P. Priyadharshini and P. Balamurugan, “An efficient DDoS attack detection and prevention model using fusion heuristic enhancement of deep learning approach in FANET sector,” *Appl Soft Comput*, vol. 167, Dec. 2024, doi: 10.1016/j.asoc.2024.112438.

[31] A. Singh *et al.*, “Securing Cloud-Encrypted Data: Detecting Ransomware-as-a-Service (RaaS) Attacks through Deep Learning Ensemble,” *Computers, Materials and Continua*, vol. 79, no. 1, pp. 857–873, 2024, doi: 10.32604/cmc.2024.048036.

[32] M. A. Suharto and M. N. Apriyani, “Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional,” 2021.

[33] C. Fei and J. Shen, “Machine learning for securing Cyber–Physical Systems under cyber attacks: A survey,” *Franklin Open*, vol. 4, p. 100041, Sep. 2023, doi: 10.1016/j.fraope.2023.100041.

[34] E. Budi, D. Wira, and A. Infantono, “Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0,” *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, vol. 3, pp. 223–234, Dec. 2021, doi: 10.54706/senastindo.v3.2021.141.

[35] U. Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia Wahyu Beny Mukti Setiyawan, E. Churniawan, F. Silaswaty Faried, and W. Beny Mukti Setiyawan, "UPAYA REGULASI TEKNOLOGI INFORMASI DALAM MENGHADAPI SERANGAN SIBER GUNA MENJAGA KEDAULATAN NEGARA KESATUAN REPUBLIK INDONESIA," *Jurnal USM Law Review*, vol. 3, no. 2, p. 275, 2020.

[36] C. L. Mindara, A. Zulianto, H. P. Utomo, T. Hatati, and G. P. Mindara, "Deteksi Intrusi Untuk Klasifikasi Serangan Jaringan Dengan Penerapan Algoritma Convolutional Neural Network," *Jurnal ICT : Information Communication & Technology*, vol. 23, pp. 517–522, 2023.

[37] B. Jaya, Y. Yuhandri, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *Jurnal Sistim Informasi dan Teknologi*, pp. 115–123, Dec. 2020, doi: 10.37034/jsisfotek.v2i4.32.

[38] A. Qasem and A. Tahat, "Machine learning-based detection of the man-in-the-middle attack in the physical layer of 5G networks," *Simul Model Pract Theory*, vol. 136, Nov. 2024, doi: 10.1016/j.simpat.2024.102998.

[39] D. Risqiwati, E. Ari Irawan, F. Teknik, and P. Studi Teknk Informatika, "Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server Realtime Prevention of Brute Force and DDOS Attacks On Ubuntu Server," vol. 17, no. 4, pp. 347–354, 2018.

[40] K. S. N. Sushma, C. Viji, N. Rajkumar, J. Ravi, M. Stalin, and H. Najmusher, "Healthcare 4.0: A Review of Phishing Attacks in Cyber Security," in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 874–878. doi: 10.1016/j.procs.2023.12.045.

[41] M. Dawood *et al.*, "The Impact of Domain Name Server (DNS) over Hypertext Transfer Protocol Secure (HTTPS) on Cyber Security: Limitations, Challenges, and Detection Techniques," 2024, *Tech Science Press*. doi: 10.32604/cmc.2024.050049.

[42] S. Krishnapriya and S. Singh, "A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques," 2024, *Tech Science Press*. doi: 10.32604/cmc.2024.052447.

[43] S. Yuan, G. Reniers, and M. Yang, "Integrated management of safety and security barriers in chemical plants to cope with emerging cyber-physical attack risks under uncertainties," *Reliab Eng Syst Saf*, vol. 250, Oct. 2024, doi: 10.1016/j.ress.2024.110320.

[44] F. Fotis, "Economic Impact of Cyber Attacks and Effective Cyber Risk Management Strategies: A light literature review and case study analysis," *Procedia Comput Sci*, vol. 251, pp. 471–478, 2024, doi: 10.1016/j.procs.2024.11.135.

[45] H. V. Vo, H. P. Du, and H. N. Nguyen, "AI-powered intrusion detection in large-scale traffic networks based on flow sensing strategy and parallel deep

analysis," *Journal of Network and Computer Applications*, vol. 220, Nov. 2023, doi: 10.1016/j.jnca.2023.103735.

[46] R. Prasad and Y. Moon, "Architecture for Preventing and Detecting Cyber Attacks in Cyber-Manufacturing System," in *IFAC-PapersOnLine*, Elsevier B.V., 2022, pp. 2246–2251. doi: 10.1016/j.ifacol.2022.10.042.

[47] H. M. A. Mohammed, A. N. Omeroglu, E. A. Oral, and I. Y. Ozbek, "ISAFusionNet: Involution and soft attention based deep multi-modal fusion network for multi-label skin lesion classification," *Computers and Electrical Engineering*, vol. 122, Mar. 2025, doi: 10.1016/j.compeleceng.2024.109966.

[48] Z. Ding, X. Wang, Y. Wu, G. Cao, and L. Chen, "Tagging knowledge concepts for math problems based on multi-label text classification," *Expert Syst Appl*, vol. 267, Apr. 2025, doi: 10.1016/j.eswa.2024.126232.

[49] H. Liu, P. Liu, and C. Bai, "Combining long and short spatiotemporal reasoning for deep reinforcement learning," *Neurocomputing*, vol. 619, Feb. 2025, doi: 10.1016/j.neucom.2024.129165.

[50] C. Han and X. Wang, "TPN:Triple network algorithm for deep reinforcement learning," *Neurocomputing*, vol. 591, Jul. 2024, doi: 10.1016/j.neucom.2024.127755.

[51] R. Misra, R. Wisniewski, and C. S. Kallesøe, "On Bellman's principle of optimality and Reinforcement learning for safety-constrained Markov decision process," Feb. 2023, doi: 10.1016/j.ifacol.2024.10.192.

[52] P. Ladosz, L. Weng, M. Kim, and H. Oh, "Exploration in deep reinforcement learning: A survey," *Information Fusion*, vol. 85, pp. 1–22, Sep. 2022, doi: 10.1016/j.inffus.2022.03.003.

[53] P. Razzaghi *et al.*, "A survey on reinforcement learning in aviation applications," Oct. 01, 2024, *Elsevier Ltd*. doi: 10.1016/j.engappai.2024.108911.

[54] A. Corrêa, A. Jesus, C. Silva, P. Peças, and S. Moniz, "Rainbow Versus Deep Q-Network: A Reinforcement Learning Comparison on the Flexible Job-Shop Problem," in *IFAC-PapersOnLine*, Elsevier B.V., Aug. 2024, pp. 870–875. doi: 10.1016/j.ifacol.2024.09.176.

[55] Y. Yin, L. Zhang, X. Shi, Y. Wang, J. Peng, and J. Zou, "Improved Double Deep Q Network Algorithm Based on Average Q-Value Estimation and Reward Redistribution for Robot Path Planning," *Computers, Materials and Continua*, vol. 81, no. 2, pp. 2769–2790, 2024, doi: 10.32604/cmc.2024.056791.

[56] M. Park, J. Kim, and D. Enke, "A novel trading system for the stock market using Deep Q-Network action and instance selection," *Expert Syst Appl*, vol. 257, Jan. 2024, doi: 10.1016/j.eswa.2024.125043.

[57] H. Dana Mazraeh and K. Parand, "An innovative combination of deep Q-networks and context-free grammars for symbolic solutions to differential equations," *Eng Appl Artif Intell*, vol. 142, Feb. 2025, doi: 10.1016/j.engappai.2024.109733.

[58] G. Liu, W. Chen, B. Chen, B. Feng, P. Wang, and H. Liu, “Supervised contrastive deep Q-Network for imbalanced radar automatic target recognition,” *Pattern Recognit*, vol. 161, May 2025, doi: 10.1016/j.patcog.2024.111264.

[59] X. Ji, F. Gong, N. Wang, C. Du, and X. Yuan, “Task offloading with enhanced Deep Q-Networks for efficient industrial intelligent video analysis in edge–cloud collaboration,” *Advanced Engineering Informatics*, vol. 62, Oct. 2024, doi: 10.1016/j.aei.2024.102599.

[60] D. Yuan and Y. Wang, “Sustainable supply chain management: A green computing approach using deep Q-networks,” *Sustainable Computing: Informatics and Systems*, vol. 45, Jan. 2025, doi: 10.1016/j.suscom.2024.101063.

[61] B.-S. Kim, H.-W. Suk, Y.-H. Choi, D.-S. Moon, and M.-S. Kim, “Optimal Cyber Attack Strategy Using Reinforcement Learning Based on Common Vulnerability Scoring System,” *Computer Modeling in Engineering & Sciences*, vol. 0, no. 0, pp. 1–10, 2024, doi: 10.32604/cmes.2024.052375.

[62] H. Shahbazi, V. Tikani, and R. Fatahi, “Layered learning in a quadrotor drone: Simultaneous controlling and path planning using optimal fuzzy fractional order proportional integral derivative and proximal policy optimization,” *Eng Appl Artif Intell*, vol. 136, Oct. 2024, doi: 10.1016/j.engappai.2024.108926.

[63] S. Anbazhagan and R. K. Mugelan, “Next-gen resource optimization in NB-IoT networks: Harnessing soft actor–critic reinforcement learning,” *Computer Networks*, vol. 252, Oct. 2024, doi: 10.1016/j.comnet.2024.110670.

[64] A. Unnikrishnan, “Financial News-Driven LLM Reinforcement Learning for Portfolio Management,” Nov. 2024, [Online]. Available: http://arxiv.org/abs/2411.11059

[65] E. Diederichs, “Reinforcement Learning: A Technical Introduction – Part I,” *Journal of Autonomous Intelligence*, vol. 2, no. 2, pp. 25–41, 2019, doi: 10.32629/jai.v2i2.45.

[66] Z. Tan and M. Karaköse, “A new approach for drone tracking with drone using Proximal Policy Optimization based distributed deep reinforcement learning,” *SoftwareX*, vol. 23, Jul. 2023, doi: 10.1016/j.softx.2023.101497.

[67] B. Zhao, H. Dong, Y. Wang, and T. Pan, “PPO-TA: Adaptive task allocation via Proximal Policy Optimization for spatio-temporal crowdsourcing,” *Knowl Based Syst*, vol. 264, Mar. 2023, doi: 10.1016/j.knosys.2023.110330.

[68] A. Alagha, S. Singh, R. Mizouni, J. Bentahar, and H. Otrok, “Target localization using Multi-Agent Deep Reinforcement Learning with Proximal Policy Optimization,” *Future Generation Computer Systems*, vol. 136, pp. 342–357, Nov. 2022, doi: 10.1016/j.future.2022.06.015.

[69] T. Purves, K. G. Kyriakopoulos, S. Jenkins, I. Phillips, and T. Dudman, “Causally aware reinforcement learning agents for autonomous cyber

defence," *Knowl Based Syst*, vol. 304, Nov. 2024, doi: 10.1016/j.knosys.2024.112521.

[70] V. Hnamte and J. Hussain, "Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach," *Telematics and Informatics Reports*, vol. 11, Sep. 2023, doi: 10.1016/j.teler.2023.100077.

[71] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, Apr. 2021, doi: 10.1016/j.comnet.2021.107840.

[72] H. A. Sakr, M. M. Fouda, A. F. Ashour, A. Abdelhafeez, M. I. El-Afifi, and M. Refaat Abdellah, "Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems," *Egyptian Informatics Journal*, vol. 28, Dec. 2024, doi: 10.1016/j.eij.2024.100540.

[73] M. Mittal, K. Kumar, and S. Behal, "DL-2P-DDoSADF: Deep learning-based two-phase DDoS attack detection framework," *Journal of Information Security and Applications*, vol. 78, Nov. 2023, doi: 10.1016/j.jisa.2023.103609.

[74] M. A. Talukder *et al.*, "A dependable hybrid machine learning model for network intrusion detection," *Journal of Information Security and Applications*, vol. 72, Feb. 2023, doi: 10.1016/j.jisa.2022.103405.

[75] A. Verma, R. Saha, G. Kumar, and M. Conti, "PETRAK: A solution against DDoS attacks in vehicular networks," *Comput Commun*, vol. 221, pp. 142–154, May 2024, doi: 10.1016/j.comcom.2024.04.025.

[76] M. Zakariah, S. A. AlQahtani, A. M. Alawwad, and A. A. Alotaibi, "Intrusion Detection System with CustomizedMachine Learning Techniques for NSL-KDD Dataset," *Computers, Materials and Continua*, vol. 77, no. 3, pp. 4025–4054, 2023, doi: 10.32604/cmc.2023.043752.

[77] S. A. Chelloug, "A Robust Approach for Multi Classification-Based Intrusion Detection through Stacking Deep Learning Models," *Computers, Materials and Continua*, vol. 79, no. 3, pp. 4845–4861, 2024, doi: 10.32604/cmc.2024.051539.