OPTIMALISASI KLASIFIKASI *MULTICLASS* SERANGAN SIBER DENGAN ALGORITMA *PROXIMAL POLICY OPTIMIZATION* (PPO) DAN *ADVANTAGE ACTOR-CRITIC* (A2C) PADA *REINFORCEMENT LEARNING*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana Komputer

OLEH:

Ahmed Athallah Toyyib

09011382126165

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

OPTIMALISASI KLASIFIKASI MULTICLASS SERANGAN SIBER DENGAN ALGORITMA PROXIMAL POLICY OPTIMIZATION (PPO) DAN ADVANTAGE ACTOR-CRITIC (A2C) PADA REINFORCEMENT LEARNING

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

AHMED ATHALLAH TOYYIB

09011382126165

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

OPTIMIZING MULTICLASS CLASSIFICATION OF CYBER ATTACKS WITH PROXIMAL POLICY OPTIMIZATION (PPO) AND ADVANTAGE ACTOR-CRITIC (A2C) ALGORITHMS IN REINFORCEMENT LEARNING

Submitted to Complete One of the Requirements for Obtaining a Bachelor's Degree in Computer Science

By:

AHMED ATHALLAH TOYYIB

09011382126165

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

NIP. 198701222015041002

Acknowledge

Head of Computer Systems Department

Dr. Ir. Sukemi, M.T

196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Jum'at

Tanggal : 9 Mei 2025

Tim Penguji :

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

Mengetahui, 5/6/25
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 199612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

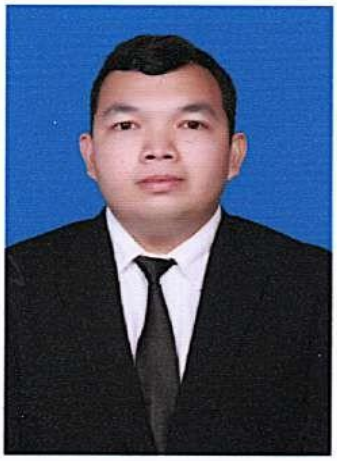
Nama : Ahmed Athallah Toyyib

NIM : 09011382126165

Judul ; Optimalisasi Klasifikasi *Multiclass* Serangan Siber dengan Algoritma *Proximal Policy Optimization* (PPO) dan *Advantage Actor-Critic* (A2C) Pada *Reinforcement Learning*

Hasil pengecekan *Software Turnitin* : **3 %**

Menyatakan bahwa Laporan Tugas Akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam Laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



Palembang, 15 Mei 2025

Ahmed Athallah Toyyib
09011382126165

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Segala puji dan syukur penulis panjatkan ke hadirat Allah Subhanahu wa Ta'ala atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul **" Optimalisasi Klasifikasi *Multiclass* Serangan Siber dengan Algoritma *Proximal Policy Optimization* (PPO) dan *Advantage Actor-Critic* (A2C) pada *Reinforcement Learning* ".**

Dalam laporan ini, penulis menguraikan proses klasifikasi multikelas terhadap berbagai jenis serangan siber, dengan fokus pada metode yang diterapkan serta kriteria evaluasi dan pengujian yang digunakan. Penelitian ini dilakukan menggunakan empat dataset berbeda sebagai variasi data untuk menguji dan memvalidasi performa metode. Penulis juga menyajikan data yang diperoleh selama kegiatan penelitian serta hasil analisis yang dilakukan secara mendalam. Melalui penyusunan laporan ini, penulis berharap karya ilmiah ini dapat memberikan kontribusi positif bagi para pembaca, baik dalam memperluas wawasan mengenai klasifikasi multikelas serangan siber maupun dalam penerapan praktis di bidang keamanan jaringan. Penulis juga berharap hasil penelitian ini dapat menjadi rujukan yang berguna bagi kalangan akademisi, peneliti, maupun praktisi yang tertarik pada bidang terkait.

Pada kesempatan ini, penulis menyampaikan penghargaan dan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan, saran, serta bantuan selama proses penyusunan tugas akhir ini. Oleh karena itu, penulis dengan tulus menyampaikan rasa syukur kepada Allah SWT dan ucapan terima kasih kepada pihak-pihak berikut:

1. Allah SWT, telah memberikan rahmat, kesehatan, dan kemudahan, sehingga saya dapat menyelesaikan penulisan tugas akhir ini dengan baik dan lancar.

2. Penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada orang tua tercinta, Bapak Syahrial dan Ibu Rita Afriliza, serta kakak penulis, Zahra Sahira, atas segala cinta, doa, dukungan moral dan materi yang tak pernah henti mengalir sepanjang perjalanan ini. Bapak dan Ibu telah membesarkan penulis dengan penuh kasih sayang, mengajarkan nilai-nilai kehidupan seperti kejujuran, kedisiplinan, dan kepedulian terhadap sesama yang menjadi pedoman dalam menjalani hidup. Kakak juga selalu hadir memberikan semangat di saat-saat sulit. Penulis merasa sangat bersyukur dan terhormat memiliki keluarga yang begitu pengertian dan penuh kasih, dan berharap setiap pencapaian ini dapat menjadi wujud kecil dari rasa terima kasih dan kebanggaan yang dipersembahkan kepada keluarga tercinta.
3. Bapak Prof. Dr. Erwin, S. Si., M. Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Iman Saladin B. Azhar S.Kom., M.MSI selaku Dosen Pembimbing Akademik Saya di Jurusan Sistem Komputer, yang sudah melakukan bimbingan akademik selama menjadi Mahasiswa Fasilkom Universitas Sriwijaya.
6. Penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada Bapak Dr. Ahmad Heryanto, S.Kom., M.T. yang telah dengan sepenuh hati membimbing penulis dalam penyusunan Tugas Akhir ini. Waktu dan tenaga yang beliau curahkan sangat berarti dalam mendukung kelancaran proses tersebut. Dalam setiap sesi bimbingan, beliau senantiasa memberikan arahan yang jelas serta arahan yang menguatkan yang sangat membantu penulis dalam memahami dan mendalami topik penelitian ini.
7. Penulis mengucapkan terima kasih kepada Mba Sari Anhar selaku admin Jurusan Sistem Komputer yang telah memberikan bantuan dalam pengurusan seluruh berkas dengan baik dan lancar selama proses penyelesaian Tugas Akhir ini.
8. Teman-teman Sistem Komputer Unggulan Angkatan 2021 yang telah memberikan dukungan dan semangat.
9. Serta Semua pihak yang telah membantu atas selesainya skripsi ini

Dalam penyusunan skripsi ini, penulis menyadari sepenuhnya bahwa masih terdapat banyak kekurangan baik dalam hal isi maupun penyajian. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang bersifat membangun guna perbaikan di masa mendatang dari semua pihak yang berkenan.

Akhir kata, dengan segala keterbatasan yang ada, penulis berharap semoga skripsi ini dapat memberikan manfaat dan menjadi referensi yang berguna, khususnya bagi mahasiswa/i Jurusan Sistem Komputer Universitas Sriwijaya.

Wassalamu'alaikum Wr. Wb.

Palembang, 15 Mei 2025

Penulis,

Ahmed Athallah Toyyib

NIM. 09011382126165

OPTIMALISASI KLASIFIKASI *MULTICLASS* SERANGAN SIBER DENGAN ALGORITMA *PROXIMAL POLICY OPTIMIZATION* (PPO) DAN *ADVANTAGE ACTOR-CRITIC* (A2C) PADA *REINFORCEMENT LEARNING*

Ahmed Athallah Toyyib (09011382126165)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email**:** athallahtoyyibahmed@gmail.com

ABSTRAK

Metode Proximal Policy Optimization (PPO) dan Advantage Actor-Critic (A2C) terbukti efektif dalam mendeteksi, mengevaluasi, dan melakukan klasifikasi multikelas pada serangan siber. Penelitian ini mengimplementasikan kedua algoritma dalam kerangka Reinforcement Learning untuk mengklasifikasikan jenis serangan berdasarkan fitur lalu lintas jaringan. Dataset yang digunakan dalam pengujian mencakup CIC-IDS2018, CIC-IDS2017, ISCX2012, dan NSL-KDD. Setiap dataset melalui tahapan pra-pemrosesan, normalisasi, serta seleksi fitur menggunakan metode SelectKBest untuk memperoleh fitur paling relevan. Hasil eksperimen menunjukkan bahwa algoritma PPO dan A2C mampu mendeteksi serangan dengan tingkat akurasi yang tinggi, dengan variasi performa tergantung karakteristik dataset. Metode PPO unggul dalam kestabilan pelatihan dan pemanfaatan reward, sedangkan A2C memiliki kemampuan adaptasi yang baik terhadap strategi eksploitasi berkelanjutan. Dengan pendekatan yang cermat terhadap pemilihan fitur, rasio data, dan parameter model, sistem ini dapat menghasilkan deteksi yang akurat dan efisien dalam klasifikasi multikelas serangan siber modern.

Kata Kunci : Proximal Policy Optimization (PPO), Advantage Actor-Critic (A2C), Reinforcement Learning, Deteksi Serangan Siber, Klasifikasi Multikelas, Lalu Lintas Jaringan, Seleksi Fitur SelectKbest.

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. Sukemi, M.T.	**Dr. Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

OPTIMIZING MULTICLASS CLASSIFICATION OF CYBER ATTACKS WITH PROXIMAL POLICY OPTIMIZATION (PPO) AND ADVANTAGE ACTOR-CRITIC (A2C) ALGORITHMS IN REINFORCEMENT LEARNING

Ahmed Athallah Toyyib (09011382126165)

Department of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email: athallahtoyyibahmed@gmail.com

ABSTRACT

The Proximal Policy Optimization (PPO) and Advantage Actor-Critic (A2C) methods have proven effective in detecting, evaluating, and performing multi-class classification of cyberattacks. This study implements both algorithms within a Reinforcement Learning framework to classify types of attacks based on network traffic features. The datasets used for testing include CIC-IDS2018, CIC-IDS2017, ISCX2012, and NSL-KDD. Each dataset undergoes preprocessing, normalization, and feature selection using the SelectKBest method to obtain the most relevant features. Experimental results show that both PPO and A2C algorithms are capable of detecting attacks with high accuracy, with performance variations depending on the characteristics of the dataset. The PPO method excels in training stability and reward utilization, while A2C demonstrates strong adaptability to continuous exploitation strategies. With a careful approach to feature selection, data ratio, and model parameters, this system can deliver accurate and efficient detection in modern multi-class cyberattack classification.

Keywords : Proximal Policy Optimization (PPO), Advantage Actor-Critic (A2C), Reinforcement Learning, Cyberattack Detection, Multiclass Classification, Network Traffic, SelectKBest Feature Selection.

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. Sukemi, M.T.	**Dr. Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SYNTAX

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan meningkatnya ketergantungan pada teknologi saat ini, terdapat peningkatan upaya untuk mengganggu dan mengganggu sistem teknologi, menyebabkan layanan terhenti. Karena berbagai jenis serangan baru terus muncul, keamanan jaringan sangat penting bagi setiap negara. Salah satu masalah utama dalam bidang teknologi informasi (TI) adalah keamanan internet, khususnya yang berkaitan dengan *Internet of Things* (IoT), perangkat seluler, dan data medis. Potensi serangan siber meningkat seiring dengan meningkatnya permintaan layanan TI[1]. Serangan siber terus berkembang dengan cepat, dan saat ini individu yang tidak bertanggung jawab atas berbagai insiden siber menargetkan server web yang beroperasi menggunakan Protokol Transfer Hypertext (HTTP), yang rentan terhadap serangan *Denial of Service* (DoS). Server yang tidak memiliki perlindungan yang memadai menjadi lebih mudah diserang, memungkinkan pelaku untuk mengganggu layanan secara besar-besaran dan berkepanjangan[2].

Serangan siber melalui lalu lintas jaringan ini mencakup aktivitas seperti penelusuran web, streaming video, penggunaan perangkat lunak perkantoran, dan pengiriman email. Seperti yang terjadi dalam situasi nyata selama pelatihan keamanan siber, lalu lintas jaringan yang disimulasikan memiliki kemampuan untuk memicu serangan *Distributed Denial of Servi*ce (DDoS) dengan menggunakan berbagai vektor serangan.Selain itu, klasifikasi lalu lintas jaringan normal terus menjadi masalah besar[3]. Klasifikasi dalam mendeteksi serangan siber adalah proses membagi aktivitas sistem komputer ke dalam kategori yang berbeda berdasarkan fiturnya. Untuk mendeteksi serangan siber, ada dua jenis klasifikasi klasifikasi biner dan klasifikasi multikelas. Klasifikasi biner membagi data menjadi dua kategori yang saling eksklusif. Dalam klasifikasi *multiclass*, data dibagi menjadi lebih dari satu kelas.

Dalam klasifikasi *multiclass* untuk deteksi serangan siber, metode *Proximal Policy Optimization* (PPO) dapat dioptimalkan untuk mengklasifikasi secara rinci pola serangan dan pola normal yang spesifik pada suatu lingkungan jaringan. Seiring dengan peningkatan jumlah klaster, potensi deteksi intrusi cenderung meningkat karena data dapat diklasifikasikan dengan lebih presisi. Namun, hal ini tidak selalu berlaku secara linier. Selain itu, penentuan jumlah klaster optimal merupakan tantangan tersendiri, mengingat waktu deteksi dapat meningkat secara signifikan seiring bertambahnya jumlah klaster[4]. Metode ini menggunakan dua model jaringan saraf yang saling melengkapi. Model pertama, yang disebut *Actor network*, bertugas untuk memutuskan tindakan apa yang harus diambil dalam situasi tertentu berdasarkan informasi yang ada. Model kedua, yaitu *Critic network*, berfungsi untuk menilai seberapa baik keputusan yang diambil oleh *Actor*. Dengan bekerja sama, kedua model ini memungkinkan sistem untuk belajar secara mandiri dan mengidentifikasi lalu lintas jaringan yang mencurigakan dengan semakin baik[5].

Pada Penelitian [6], Setelah analisis menyeluruh, ditemukan bahwa kinerja PPO sangat bergantung pada trik optimasi, tetapi tidak sepenuhnya pada mekanisme pemisahan inti. Namun, seperti yang kami temukan, meskipun mekanisme pemisahan tidak dapat membatasi kebijakan secara ketat, mekanisme pemisahan tetap berdampak besar pada stabilitas dan pembatasan kebijakan. Metode PPO mengubah fungsi tujuan untuk menindaklanjuti pembaruan kebijakan yang terlalu besar. Ini menstabilkan proses pembelajaran dan menyeimbangkan eksplorasi strategi baru dengan eksploitasi kebijakan yang telah dipelajari. Algoritma *Advantage Actor-Critic* (A2C), sebuah algoritma berpengaruh dalam pembelajaran penguatan yang menggabungkan elemen dari metode berbasis kebijakan dan berbasis nilai, menugaskan aktor untuk memilih tindakan berdasarkan kebijakan, sementara kritikus menilai tindakan tersebut menggunakan fungsi nilai algoritma A2C mendukung metode ini[7].

Dataset yang akan digunakan untuk klasifikasi serangan siber *multiclass* dalam penelitian ini mencakup dataset CIC-IDS 2018, CIC-IDS 2017, ISCX 2012, dan NSL-KDD. Salah satu kendala yang diidentifikasi adalah keterbatasan metode PPO dan A2C dalam memodelkan dependensi temporal, khususnya dalam mendeteksi serangan

jaringan yang memiliki urutan tertentu. Kedua metode ini lebih efektif untuk pola serangan yang sudah dikenal namun kurang adaptif terhadap pola baru yang belum pernah ditemui. Oleh karena itu, sebelum menerapkan metode PPO dan A2C pada dataset, penelitian ini akan terlebih dahulu menganalisis dan mengoptimalkan metode tersebut untuk menilai kecocokannya dengan tugas klasifikasi yang dihadapi.

Pada Penelitian[8], Dengan metode PPO diterapkan pada sistem Intrusion Detection System (IDS) menggunakan beberapa dataset, yaitu NSL-KDD, UNSW-NB15, CICDDoS2019, dan AWID, untuk memungkinkan klasifikasi serangan baru secara efektif pada dataset UNSW-NB15, setelah dilakukan seleksi fitur dan diperoleh 196 mendapatkan akurasi mencapai 88%. Dataset CIC-IDS 2017 dan CICDDoS2019, yang mengandung data *multiclass* modern dengan berbagai jenis serangan, dieksplorasi lebih lanjut dan menghasilkan akurasi sebesar 99%. Sementara itu, pada dataset NSL-KDD, seleksi fitur dilakukan untuk menggabungkan informasi terkait lalu lintas normal atau serangan, menghasilkan akurasi sebesar 89%. Terakhir, untuk dataset AWID yang memiliki empat label klasifikasi (*normal*, *flooding*, *injection*, dan *impersonation*), distribusi frekuensi label yang mirip pada set pelatihan dan pengujian menghasilkan akurasi 95%. Hasil ini menunjukkan bahwa metode PPO dan A2C efektif dalam meningkatkan akurasi IDS di berbagai dataset, menjadikannya solusi yang dapat diandalkan untuk deteksi intrusi dalam jaringan.

Pada penelitian[9], menggunakan PPO dan A2C dengan dataset NSL-KDD dan AWID pada data set NSL-KKD memiliki nilai akurasi 78 % - 80% untuk data AWID memiliki nilai akurasi 92% Hasil menunjukkan bahwa skenario dengan data berlabel sangat dipengaruhi oleh pemilihan faktor diskonto temuan ini signifikan, karena tanpa interaksi langsung dengan lingkungan dan umpan balik dari dampak tindakan, pendekatan yang lebih konservatif diperlukan dalam memperbarui kebijakan. Akibatnya, proses konvergensi menjadi lebih lambat tetapi lebih stabil. Sedangkan pada penelitian[10], dengan menggunakan metode A2C dengan dataset CIC-IDS-2017, CIRA-CIC-DoHBrw-2020 dan NSL-KDD pada dataset NSL-KDD memperoleh akurasi mendekati 98% dalam mendeteksi anomali jaringan. ada dataset CICIDS2017, yang mengandung lebih banyak tipe serangan, akurasi A2C berkisar antara 95% hingga 99%,

menandakan bahwa A2C cukup efisien dalam mendeteksi pola-pola anomali jaringan yang kompleks. Selain itu, ketika digunakan pada dataset DoHBrw-2020, yang berfokus pada deteksi anomali dalam permintaan HTTP terenkripsi, model A2C menunjukkan performa yang baik dengan akurasi sekitar 96%, yang menunjukkan kemampuan algoritma ini untuk menangani pola-pola sulit dalam jaringan yang aman. Dengan demikian A2C mampu mencapai akurasi tinggi dalam berbagai jenis dataset, mirip atau bahkan lebih baik dari hasil dalam jurnal terkait, dengan performa yang sedikit bervariasi tergantung kompleksitas datasetnya.

Maka pada metode A2C berperan signifikan dalam mengidentifikasi pola dan rute eksploitasi optimal di jaringan yang telah disusupi dalam ranah keamanan siber, tahapan pasca-eksploitasi melibatkan aktivitas seperti pengambilan data dan pemasangan *backdoor*, yang mengandalkan eksploitasi lingkungan target dengan strategi yang cermat. A2C memungkinkan model untuk belajar dari respons sistem terhadap berbagai aksi, mempercepat proses identifikasi jalur eksploitasi yang efektif, sekaligus mengurangi kemungkinan terdeteksi oleh mekanisme keamanan. Kelebihan utama A2C terletak pada kemampuannya untuk memperbarui kebijakan secara stabil dan efisien serta menghasilkan akurasi tinggi dalam menentukan langkah optimal di setiap tahap eksploitasi. Secara keseluruhan, A2C memperkuat otomatisasi dalam tahapan eksploitasi lanjutan dengan mengidentifikasi strategi yang lebih adaptif. Hal ini menjadikannya alternatif unggul dalam mengembangkan alat otomatis untuk keamanan siber berbasis reinforcement learning.[11].

Dengan mempertimbangkan uraian di atas, penulis memilih judul "**Optimalisasi Klasifikasi *Multiclass* Serangan Siber Menggunakan Algoritma Proximal Policy Optimization (PPO) dan Advantage Actor-Critic (A2C) dalam Reinforcement Learning**." Diharapkan hasil dari penelitian tugas akhir ini dapat memberikan kontribusi pengetahuan dan wawasan bagi pihak-pihak yang membutuhkan, serta menjadi salah satu metode untuk menghadapi serangan siber yang kian berkembang saat ini.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, peneliti merumuskan masalah yaitu sebagai berikut:

1. Bagaimana metode PPO dan A2C dapat digunakan untuk mendeteksi dan mengklasifikasikan serangan siber secara multiclass?
2. Bagaimana proses implementasi PPO dan A2C pada dataset serangan siber dilakukan?
3. Bagaimana kinerja metode PPO dan A2C dalam klasifikasi serangan siber dievaluasi dan dibandingkan?

1.3 Tujuan

Berdasarkan rumusan masalah di atas, penelitian ini memiliki beberapa tujuan yang harus dicapai yaitu:

1. Menerapkan metode PPO dan A2C pada dataset serangan siber untuk melakukan deteksi dan klasifikasi multiclass.
2. Mengevaluasi dan membandingkan kinerja metode PPO dan A2C dalam mengklasifikasikan jenis-jenis serangan siber.
3. Mengidentifikasi fitur-fitur yang paling berpengaruh dalam proses klasifikasi menggunakan PPO dan A2C.

1.4 Manfaat

Berdasarkan tujuan dari penelitian ini, memiliki beberapa manfaat antara lain sebagai berikut:

1. Implementasi metode PPO dan A2C dapat membantu mengidentifikasi jenis serangan, sehingga meningkatkan akurasi dan efisiensi dalam mendeteksi serangan siber.

2. Menunjukkan kemampuan metode PPO dan A2C dalam melakukan klasifikasi multikelas pada dataset serangan siber, yang dapat digunakan sebagai referensi untuk penelitian selanjutnya.
3. Mengoptimalkan penggunaan metode PPO dan A2C untuk mencapai tingkat akurasi yang tinggi.

1.5 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah:

1. Dataset yang digunakan pada penelitian ini mengggunakan lebih dari satu dataset yaitu NSL-KDD, CIC-IDS2017, CID-IDS2018 dan Dataset ISCX2012.
2. Pada penelitian ini, melakukan deteksi serangan siber dan klasifikasi *multiclass* dengan menggunakan metode PPO dan A2C.
3. Optimalisasi pada klasifikasi *multiclass* yang dilakukan dalam penelitian ini akan memanfaatkan metode PPO dan A2C.

1.6 Metode Penelitian

Penelitian ini akan mencakup beberapa tahapan sebagai berikut:

1. Tahapan Pertama (perumusan masalah)

   Tahap pertama adalah perumusan masalah, yaitu penentuan pokok permasalahan terkait sistem deteksi dan *multiclass* serangan siber.
2. Tahapan Kedua (literatur)

   Tahap kedua adalah studi literatur, di mana penulis mencari informasi terkait optimalisasi klasifikasi multiclass untuk deteksi serangan siber menggunakan algoritma PPO dan A2C dalam Reinforcement Learning. Kegiatan yang dilakukan meliputi pencarian referensi berupa buku, jurnal, artikel ilmiah, dan sumber-sumber lain yang relevan untuk mendukung penelitian ini.

3. Tahap ketiga (rancang sistem)

   Tahap ketiga adalah perancangan sistem, yang dilakukan berdasarkan hasil dari tahap perumusan masalah dan studi literatur sebelumnya.

4. Tahap keempat (persiapan data)

   Pada tahap ini, dilakukan pengumpulan dataset yang akan diuji dan diklasifikasi, yaitu dataset NSL-KDD, CIC-IDS2018, CIC-IDS2017, dan ISCX2012, yang telah diubah ke dalam format *Comma-Separated Values* (CSV).

5. Tahapan kelima (pengujian dan klasifikasi)

   Tahap selanjutnya adalah kelanjutan dari persiapan data yang telah diselesaikan. Pada tahap ini, sistem deteksi diterapkan untuk mengidentifikasi serangan siber, diikuti dengan klasifikasi *multiclass* untuk beberapa jenis serangan siber menggunakan metode PPO dan A2C.

6. Tahapan keenam (Analisa)

   Pada tahap ini dilakukan analisis, di mana analisis data diperoleh dari proses pengujian sistem deteksi serangan siber serta hasil klasifikasi *multiclass* terhadap beberapa dataset.

7. Tahapan ketujuh (Kesimpulan dan saran)

   Pada tahap terakhir, dilakukan pembuatan kesimpulan serta saran yang dapat bermanfaat bagi peneliti selanjutnya sebagai acuan.

1.7 Sistematika Penulisan

Dalam proses penyusunan laporan tugas akhir ini, penulis menerapkan sistematika penulisan untuk memudahkan pemahaman terhadap isi dari setiap bab yang disusun dalam skripsi ini.

BAB I PENDAHULUAN

Bab ini akan menjelaskan mengenai latar belakang, perumusan masalah, tujuan, manfaat, metode penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini akan membahas latar belakang, perumusan masalah, tujuan, manfaat, metode penelitian, serta sistematika penulisan.

BAB III METODOLOGI PENELITIAN

Pada bab ketiga, akan dibahas mengenai dataset, perangkat-perangkat yang digunakan, serta penyusunan diagram proses penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil pengujian dan menganalisis hasil penelitian yang disajikan berdasarkan metode yang digunakan untuk setiap hasil yang diperoleh.

BAB V KESIMPULAN DAN SARAN

Bab ini akan menyampaikan kesimpulan dan saran dari penelitian ini untuk pengembangan yang lebih lanjut di masa mendatang.

DAFTAR PUSTAKA

[1] S. ur Rehman *et al.*, "DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU)," *Futur. Gener. Comput. Syst.*, vol. 118, pp. 453–466, 2021, doi: 10.1016/j.future.2021.01.022.

[2] H. Setia *et al.*, "Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments," *Cyber Secur. Appl.*, vol. 2, no. January, 2024, doi: 10.1016/j.csa.2024.100037.

[3] Y. Jang *et al.*, "An Investigation of Learning Model Technologies for Network Traffic Classification Design in Cyber Security Exercises," *IEEE Access*, vol. 11, no. October, pp. 138712–138731, 2023, doi: 10.1109/ACCESS.2023.3336674.

[4] H. Han, H. Kim, and Y. Kim, "An Efficient Hyperparameter Control Method for a Network Intrusion Detection System Based on Proximal Policy Optimization," *Symmetry (Basel).*, vol. 14, no. 1, 2022, doi: 10.3390/sym14010161.

[5] R. Learning, M. Traffic, D. Model, and I. Entropy, "Efficient Detection of Malicious Traffic Using a Decision," 2024.

[6] W. Meng, Q. Zheng, G. Pan, and Y. Yin, "Off-Policy Proximal Policy Optimization," *Proc. 37th AAAI Conf. Artif. Intell. AAAI 2023*, vol. 37, pp. 9162–9170, 2023, doi: 10.1609/aaai.v37i8.26099.

[7] Y. K. Purwanto and D. Kang, "Multi-Agent Deep Reinforcement Learning for Fighting Game : A Comparative Study of PPO and A2C," vol. 16, no. 3, pp. 192–198, 2024.

[8] M. Lopez-Martin, A. Sanchez-Esguevillas, J. I. Arribas, and B. Carro, "Network Intrusion Detection Based on Extended RBF Neural Network with Offline Reinforcement Learning," *IEEE Access*, vol. 9, pp. 153153–153170, 2021, doi: 10.1109/ACCESS.2021.3127689.

[9] M. Lopez-Martin, B. Carro, and A. Sanchez-Esguevillas, “Application of deep reinforcement learning to intrusion detection for supervised problems,” *Expert Syst. Appl.*, vol. 141, p. 112963, 2020, doi: 10.1016/j.eswa.2019.112963.

[10] K. Zhou, W. Wang, T. Hu, and K. Deng, “Application of improved asynchronous advantage actor critic reinforcement learning model on anomaly detection,” *Entropy*, vol. 23, no. 3, pp. 1–22, 2021, doi: 10.3390/e23030274.

[11] R. Maeda and M. Mimura, “Automating post-exploitation with deep reinforcement learning,” *Comput. Secur.*, vol. 100, p. 102108, 2021, doi: 10.1016/j.cose.2020.102108.

[12] Z. Li, C. Huang, S. Deng, W. Qiu, and X. Gao, “A soft actor-critic reinforcement learning algorithm for network intrusion detection,” *Comput. Secur.*, vol. 135, no. September, p. 103502, 2023, doi: 10.1016/j.cose.2023.103502.

[13] L. Chavali, A. Krishnan, P. Saxena, B. Mitra, and A. Chivukula, “Off-policy actor-critic deep reinforcement learning methods for alert prioritization in intrusion detection systems,” *Comput. Secur.*, vol. 142, no. April, p. 103854, 2024, doi: 10.1016/j.cose.2024.103854.

[14] G. Caminero, M. Lopez-Martin, and B. Carro, “Adversarial environment reinforcement learning algorithm for intrusion detection,” *Comput. Networks*, vol. 159, pp. 96–109, 2019, doi: 10.1016/j.comnet.2019.05.013.

[15] K. Ren, Y. Zeng, Y. Zhong, B. Sheng, and Y. Zhang, “MAFSIDS: a reinforcement learning-based intrusion detection model for multi-agent feature selection networks,” *J. Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00814-4.

[16] B. Darabi, M. Bag-Mohammadi, and M. Karami, “A micro Reinforcement Learning architecture for Intrusion Detection Systems,” *Pattern Recognit. Lett.*, vol. 185, no. January, pp. 81–86, 2024, doi: 10.1016/j.patrec.2024.07.010.

[17] A. Sharma and M. Singh, “Dual replay memory reinforcement learning framework for minority attack detection,” *Eng. Appl. Artif. Intell.*, vol. 144, no. August 2024, p. 110083, 2025, doi: 10.1016/j.engappai.2025.110083.

[18] N. Abedzadeh and M. Jacobs, “A Reinforcement Learning Framework with Oversampling and Undersampling Algorithms for Intrusion Detection System,” *Appl. Sci.*, vol. 13, no. 20, 2023, doi: 10.3390/app132011275.

[19] C. Rookard and A. Khojandi, “RRIoT: Recurrent reinforcement learning for cyber threat detection on IoT devices,” *Comput. Secur.*, vol. 140, no. January, p. 103786, 2024, doi: 10.1016/j.cose.2024.103786.

[20] S. R. Jeremiah, H. Chen, S. Gritzalis, and J. H. Park, “Leveraging application permissions and network traffic attributes for Android ransomware detection,” *J. Netw. Comput. Appl.*, vol. 230, no. May, p. 103950, 2024, doi: 10.1016/j.jnca.2024.103950.

[21] X. Yang, E. Howley, and M. Schukat, “ADT: Time series anomaly detection for cyber-physical systems via deep reinforcement learning,” *Comput. Secur.*, vol. 141, no. January, p. 103825, 2024, doi: 10.1016/j.cose.2024.103825.

[22] Y. Li, Y. Wang, X. Zhao, and Z. Chen, “A deep reinforcement learning-based intelligent fault diagnosis framework for rolling bearings under imbalanced datasets,” *Control Eng. Pract.*, vol. 145, no. January, p. 105845, 2024, doi: 10.1016/j.conengprac.2024.105845.

[23] A. Li, R. Liu, and S. Yi, “Integrating communication networks with reinforcement learning and big data analytics for optimizing carbon capture and utilization strategies,” *Alexandria Eng. J.*, vol. 108, no. August, pp. 937–951, 2024, doi: 10.1016/j.aej.2024.08.100.

[24] M. Yousaf, M. Farhan, Y. Saeed, M. J. Iqbal, F. Ullah, and G. Srivastava, “Enhancing driver attention and road safety through EEG-informed deep reinforcement learning and soft computing,” *Appl. Soft Comput.*, vol. 167, no. PB, p. 112320, 2024, doi: 10.1016/j.asoc.2024.112320.

[25] Z. Qian, Q. Yu, H. Zhu, J. Liu, and T. Fu, “Reinforcement learning for test case prioritization based on LLEed K-means clustering and dynamic priority factor,” *Inf. Softw. Technol.*, vol. 179, no. January 2024, p. 107654, 2025, doi: 10.1016/j.infsof.2024.107654.

[26] Z. Cui, W. Guan, W. Luo, and X. Zhang, “Intelligent navigation method for multiple marine autonomous surface ships based on improved PPO algorithm,” *Ocean Eng.*, vol. 287, no. P1, p. 115783, 2023, doi: 10.1016/j.oceaneng.2023.115783.

[27] P. TS and P. Shrinivasacharya, “Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security,” *Glob. Transitions Proc.*, vol. 2, no. 2, pp. 448–454, 2021, doi: 10.1016/j.gltp.2021.08.017.

[28] S. Iglesias Pérez, S. Moral-Rubio, and R. Criado, “A new approach to combine multiplex networks and time series attributes: Building intrusion detection systems (IDS) in cybersecurity,” *Chaos, Solitons and Fractals*, vol. 150, 2021, doi: 10.1016/j.chaos.2021.111143.

[29] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, “IntruDTree: A machine learning based cyber security intrusion detection model,” *Symmetry (Basel).*, vol. 12, no. 5, pp. 1–15, 2020, doi: 10.3390/SYM12050754.

[30] A. K. Sangaiah, A. Javadpour, and P. Pinto, “Towards data security assessments using an IDS security model for cyber-physical smart cities,” *Inf. Sci. (Ny).*, vol. 648, no. January, p. 119530, 2023, doi: 10.1016/j.ins.2023.119530.

[31] Maskun, Irwansyah, A. Yunus, A. Safira, and S. N. Lubis, “Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with It,” *Jambe Law J.*, vol. 4, no. 2, pp. 131–150, 2021, doi: 10.22437/jlj.4.2.131-150.

[32] I. Kotenko, I. Saenko, O. Lauta, and A. Kribel, “Ensuring the survivability of embedded computer networks based on early detection of cyber attacks by integrating fractal analysis and statistical methods,” *Microprocess. Microsyst.*, vol. 90, no. January, p. 104459, 2022, doi: 10.1016/j.micpro.2022.104459.

[33] Y. Yang, Z. Wang, and W. Jin, “Security containment control for nonlinear MASs under DOS attacks: An improved adaptive method,” *Neurocomputing*, vol. 610, no. September, p. 128601, 2024, doi: 10.1016/j.neucom.2024.128601.

[34] A. H. Tahoun and M. Arafa, “Secure control design for nonlinear cyber–physical systems under DoS, replay, and deception cyber-attacks with multiple transmission channels,” *ISA Trans.*, vol. 128, pp. 294–308, 2022, doi: 10.1016/j.isatra.2021.11.033.

[35] I. Masud, K. Kusrini, and A. B. Prasetio, “Distributed Denial Of Service (DDOS) Attack Detection On Zigbee Protocol Using Naive Bayes Algoritm,” *Int. J. Artif. Intell. Res.*, vol. 5, no. 2, pp. 157–167, 2021, doi: 10.29099/ijair.v5i2.214.

[36] R. R. Nuiaa, S. Manickam, and A. H. Alsaeedi, “Distributed reflection denial of service attack: A critical review,” *Int. J. Electr. Comput. Eng.*, vol. 11, no. 6, pp. 5327–5341, 2021, doi: 10.11591/ijece.v11i6.pp5327-5341.

[37] F. A. Aboaoja, A. Zainal, F. A. Ghaleb, B. A. S. Al-rimy, T. A. E. Eisa, and A. A. H. Elnour, “Malware Detection Issues, Challenges, and Future Directions: A Survey,” *Appl. Sci.*, vol. 12, no. 17, 2022, doi: 10.3390/app12178482.

[38] R. Alabdan, “Phishing attacks survey: Types, vectors, and technical approaches,” *Futur. Internet*, vol. 12, no. 10, pp. 1–39, 2020, doi: 10.3390/fi12100168.

[39] M. Muniandy, N. A. Ismail, A. Y. Yahya Al-Nahari, and D. N. L. Yao, “Evolution and Impact of Ransomware: Patterns, Prevention, and Recommendations for Organizational Resilience,” *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 14, no. 1, pp. 585–599, 2024, doi: 10.6007/ijarbss/v14-i1/19803.

[40] A. Tellache, A. Mokhtari, A. A. Korba, and Y. Ghamri-doudane, “Multi-agent Reinforcement Learning-based Network Intrusion Detection System”.

[41] W. Shafik, S. M. Matinkhah, P. Etemadinejad, and M. N. Sanda, “Reinforcement Learning Rebirth , Techniques , Challenges , and Resolutions,” no. September, 2020, doi: 10.30630/joiv.4.3.376.

[42] R. R. Dos Santos, E. K. Viegas, A. O. Santin, and V. V. Cogo, “Reinforcement Learning for Intrusion Detection: More Model Longness and Fewer Updates,” *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 2, pp. 2040–2055, 2023, doi: 10.1109/TNSM.2022.3207094.

[43] H. Kheddar, D. W. Dawoud, A. I. Awad, Y. Himeur, and M. K. Khan, *Reinforcement-Learning-Based Intrusion Detection in Communication Networks: A Review*, vol. 00, no. 00. 2024. doi: 10.1109/COMST.2024.3484491.

[44] K. Sethi, Y. V. Madhav, R. Kumar, and P. Bera, “Attention based multi-agent intrusion detection systems using reinforcement learning,” *J. Inf. Secur. Appl.*, vol. 61, no. July, p. 102923, 2021, doi: 10.1016/j.jisa.2021.102923.

[45] M. H. L. Louk and B. A. Tama, “Dual-IDS: A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system,” *Expert Syst. Appl.*, vol. 213, no. PB, p. 119030, 2023, doi: 10.1016/j.eswa.2022.119030.

[46] J. L. Leevy and T. M. Khoshgoftaar, “A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data,” *J. Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00382-x.

[47] M. A. Khan, M. R. Karim, and Y. Kim, “A scalable and hybrid intrusion detection system based on the convolutional-LSTM network,” *Symmetry (Basel).*, vol. 11, no. 4, 2019, doi: 10.3390/sym11040583.

[48] Zafar Iqbal Khan, Mohammad Mazhar Afzal, and Khurram Naim Shamsi, “A Comprehensive Study on CIC-IDS2017 Dataset for Intrusion Detection Systems,” *Int. Res. J. Adv. Eng. Hub*, vol. 2, no. 02, pp. 254–260, 2024, doi: 10.47392/irjaeh.2024.0041.

[49] B. M. Serinelli, A. Collen, and N. A. Nijdam, “On the analysis of open source datasets: Validating IDS implementation for well-known and zero day attack detection,” *Procedia Comput. Sci.*, vol. 191, no. January 2021, pp. 192–199, 2021, doi: 10.1016/j.procs.2021.07.024.

[50] S. Choudhary and N. Kesswani, “Analysis of KDD-Cup’99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT,” *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 1561–1573, 2020, doi: 10.1016/j.procs.2020.03.367.

[51] V. Q. Nguyen, L. T. Ngo, L. M. Nguyen, V. H. Nguyen, and N. Shone, “Deep clustering hierarchical latent representation for anomaly-based cyber-attack detection,” *Knowledge-Based Syst.*, vol. 301, no. July, p. 112366, 2024, doi: 10.1016/j.knosys.2024.112366.

[52] M. S. Korium, M. Saber, A. Beattie, A. Narayanan, S. Sahoo, and P. H. J. Nardelli, “Intrusion detection system for cyberattacks in the Internet of Vehicles environment,” *Ad Hoc Networks*, vol. 153, no. November 2023, 2024, doi: 10.1016/j.adhoc.2023.103330.

[53] G. S. Kushwah and V. Ranga, “Optimized extreme learning machine for detecting DDoS attacks in cloud computing,” *Comput. Secur.*, vol. 105, p. 102260, 2021, doi: 10.1016/j.cose.2021.102260.

[54] M. A. Siddiqi and W. Pak, “An Optimized and Hybrid Framework for Image Processing Based Network Intrusion Detection System,” *Comput. Mater. Contin.*, vol. 73, no. 2, pp. 3921–3949, 2022, doi: 10.32604/cmc.2022.029541.

[55] H. Mohammadian, A. A. Ghorbani, and A. H. Lashkari, “A gradient-based approach for adversarial attack on deep learning-based network intrusion detection systems,” *Appl. Soft Comput.*, vol. 137, p. 110173, 2023, doi: 10.1016/j.asoc.2023.110173.

[56] F. S. Alrayes, M. Zakariah, S. U. Amin, Z. I. Khan, and J. S. Alqurni, “CNN Channel Attention Intrusion Detection System Using NSL-KDD Dataset,” *Comput. Mater. Contin.*, vol. 79, no. 3, pp. 4319–4347, 2024, doi: 10.32604/cmc.2024.050586.

[57] M. H. Kamarudin, C. Maple, and T. Watson, “Hybrid feature selection technique for intrusion detection system,” *Int. J. High Perform. Comput. Netw.*, vol. 13, no. 2, p. 232, 2019, doi: 10.1504/ijhpcn.2019.097503.

[58] M. F. Azmi, H. A. Karim, and N. AlDahoul, “Anomaly Detection for Network Security,” *Int. J. Membr. Sci. Technol.*, vol. 10, no. 1, pp. 299–316, 2023, doi: 10.15379/ijmst.v10i1.1808.