ANALISIS EFEKTIVITAS *MULTILAYER PERCEPTRON* (MLP) DALAM MENDETEKSI SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS) PADA EKOSISTEM *SMART HOME* BERBASIS IOT

SKRIPSI

Oleh:

MUHAMMAD RAFI RIZQULLAH

09011282126091

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS EFEKTIVITAS MULTILAYER PERCEPTRON (MLP) DALAM MENDETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA EKOSISTEM SMART HOME BERBASIS IOT

Sebagai salah satu syarat untuk penyelesaian studi di
Program Studi S1 Sistem Komputer

Oleh:

MUHAMMAD RAFI RIZQULLAH

09011282126091

Pembimbing 1 : **Prof. Ir. Deris Stiawan, M.T., Ph.D.**
NIP. 197806172006041002

Pembimbing 2 : **Nurul Afifah, M.Kom.**
NIP. 199211102023212049

Mengetahui
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T
196612032006041001

AUTHENTICATION PAGE

THESIS

AN ANALYSIS OF MULTILAYER PERCEPTRON (MLP) EFFECTIVENESS IN DETECTING DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS WITHIN IOT-BASED SMART HOME ECOSYSTEMS

Submitted in Partial Fulfillment of Requirements for the
Degree of Bachelor of Computer Science

By:

MUHAMMAD RAFI RIZQULLAH

09011282126091

Supervisor	:	**Prof. Ir. Deris Stiawan, M.T., Ph.D.**
		NIP. 197806172006041002
Co - Supervisor	:	**Nurul Afifah, M.Kom.**
		NIP. 199211102023212049

Acknowledge

Head of Computer System Department

Dr. Ir. Sukemi, M.T

196612032006041001

LEMBAR PERSETUJUAN

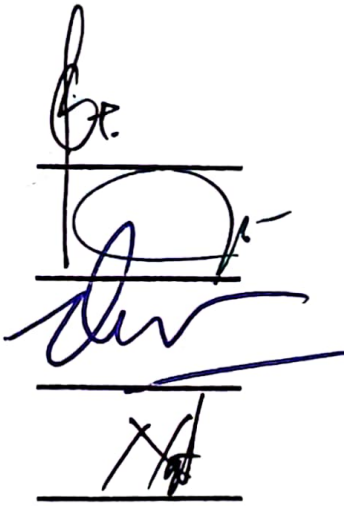
Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 13 Juni 2025

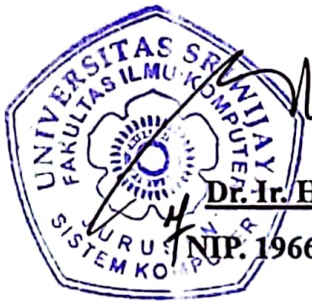
Tim Penguji :

1. Ketua : Sutarno, M.T.
2. Penguji : Kemahyanto Exaudi, M.T.
3. Pembimbing I : Prof. Ir. Deris Stiawan, M.T., Ph.D.
4. Pembimbing II : Nurul Afifah, M.Kom.



Mengetahui, 20/6/25

Ketua Jurusan Sistem Komputer



Dr. Ir. H. Sukemi. M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Muhammad Rafi Rizqullah

NIM : 09011282126091

Judul : Analisis Efektivitas *Multilayer Perceptron* (MLP) dalam Mendeteksi Serangan *Distributed Denial of Service* (DDoS) pada Ekosistem *Smart Home* Berbasis IoT

Hasil Pengecekan Plagiat/Turnitin: 1%

Menyatakan bahwa laporan tugas akhir ini adalah hasil karya saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Saya menyadari jika terbukti adanya penjiplakan atau plagiat dalam laporan tugas akhir ini, saya siap menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, Pernyataan ini saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.

Palembang, Juni 2025

Yang menyatakan

Muhammad Rafi Rizqullah

NIM. 09011282126091

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh. Puji dan syukur kepada Allah SWT, karena berkat Rahmat dan Karunia-Nya lah sehingga penulis dapat menyelesaikan penyusunan Skripsi ini dengan judul "**Analisis Efektivitas *Multilayer Perceptron* (MLP) dalam Mendeteksi Serangan *Distributed Denial of Service* (DDoS) pada Ekosistem *Smart Home* Berbasis IoT**". Shalawat beserta salam senantiasa tercurah kepada Nabi Muhammad Shallallahu 'Alaihi Wasallam yang telah membawa rahmat dan kedamaian bagi seluruh alam serta menjadi suri tauladan bagi umatnya.

Skripsi ini merupakan salah satu syarat untuk memenuhi sebagian kurikulum dan syarat kelulusan Mata Kuliah Skripsi pada Jurusan Sistem Komputer, Universitas Sriwijata. Dalam penyelesaian Skripsi ini, penulis ingin mengucapkan terima kasih kepada pihak-pihak yang telah memberikan bantuan, dorongan, motivasi, semangat, dan bimbingan dalam penyusunan Skripsi ini:

1. Tuhan Yang Maha Esa, yang telah melimpahkan Berkat dan Rahmat-Nya.
2. Ibu Nyimas Sopiah, Bapak Dedi Kurniawan, dan Adik-adik penulis tercinta serta seluruh keluarga besar yang telah banyak memberikan do'a, serta motivasi kepada penulis selama ini.
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 Universitas Sriwijaya.
5. Bapak Iman Saladin B. Azhar, S.Kom., M.MSI. selaku Dosen Pembimbing Akademik.
6. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D., IPU., ASEAN-Eng. selaku Dosen Pembimbing I Tugas Akhir.
7. Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing II Tugas Akhir.
8. Kak Angga selaku admin Jurusan Sistem Komputer.
9. Diah Ayuning Tyas selaku *partner* yang selalu ada saat susah maupun senang, dan selalu menjadi *support system* terbaik yang penulis miliki.

10. Aldi, Choi, Zaidan, Makiyah, Hepra, dan Tisa selaku sahabat seperjuangan kuliah yang selalu bersama saat menjalani proses perkuliahan.
11. Vandy, Irfan, Loza, Egar, Ghali, dan Firja selaku teman dekat penulis yang memberikan dukungan dan mendo'akan yang terbaik untuk penulis.
12. Arkan, Ribang, Ridho, Jep, Khemal, Delvin, dan Dazfa selaku teman dekat dalam NYEBUR yang selalu menemani penulis *refreshing* seperti minum kopi, bermain game, dan mengeluarkan penat dalam pikiran penulis.
13. Wahyu, Alief, dan Mufli selaku teman dari SD dan TK dari penulis.
14. Restu, Fariz, Aqshal, dan Abel selaku teman-teman minum kopi dari penulis.
15. Kakak-kakak tingkat SK Unggulan dan SK Reguler yang termasuk tim riset COMNETS.
16. Teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2021 terkhusus kelas C.
17. Seluruh pihak yang membantu dalam menyelesaikan Skripsi ini yang tidak bisa disebutkan satu persatu.
18. Almamater.

Penulis menyadari sepenuhnya bahwa Skripsi ini masih memiliki kekurangan dan jauh dari kata sempurna. Oleh karena itu, penulis sangat terbuka terhadap kritik dan saran yang membangun demi penyempurnaan Skripsi ini di masa mendatang.

Penulis memiliki harapan besar agar Skripsi ini tidak hanya bermanfaat sebagai salah satu syarat kelulusan, tetapi juga dapat menjadi sumber referensi yang berharga serta memberikan kontribusi positif dalam pengembangan ilmu pengetahuan, khususnya di bidang sistem komputer dan keamanan jaringan.

Palembang, Juni 2025
Penulis,

Muhammad Rafi Rizqullah
NIM. 09011282126091

ANALISIS EFEKTIVITAS MULTILAYER PERCEPTRON (MLP) DALAM MENDETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA EKOSISTEM SMART HOME BERBASIS IOT

Muhammad Rafi Rizqullah (09011282126091)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: 09011282126091@student.unsri.ac.id

ABSTRAK

Internet of Things (IoT) telah menghadirkan berbagai kemudahan dalam kehidupan sehari-hari, termasuk dalam penerapan *smart home*. Namun, peningkatan konektivitas ini juga meningkatkan risiko terhadap *cyber attack*, khususnya serangan *Distributed Denial of Service* (DDoS). Penelitian ini bertujuan untuk menganalisis efektivitas metode *Multilayer Perceptron* (MLP) dalam mendeteksi serangan DDoS pada ekosistem *smart home* berbasis IoT. Dataset yang digunakan berasal dari tim COMNETS dalam format *pcap* dan diekstraksi menggunakan *CICFlowMeter* menjadi format *csv*. Proses *pre-processing* dilakukan melalui *label encoding*, pemilihan fitur menggunakan *correlation matrix*, normalisasi data dengan *min-max scaler*, dan *split* data dengan berbagai rasio. Model MLP dirancang dengan dua *hidden layer* dan fungsi aktivasi *ReLU*, sementara *output layer* menggunakan aktivasi *sigmoid* untuk klasifikasi biner. Evaluasi model dilakukan menggunakan *confusion matrix* dan metrik evaluasi seperti *accuracy*, *precision*, *recall*, dan *f1-score*. Berdasarkan hasil pengujian, model MLP mencapai akurasi teroptimal sebesar 99,2% pada skenario *split* data 60:20:20. Penelitian ini menunjukkan bahwa MLP efektif dalam mendeteksi serangan DDoS pada perangkat IoT *smart home* dan dapat menjadi solusi potensial dalam sistem keamanan jaringan.

Kata Kunci: DDoS, IoT, Smart Home, Multilayer Perceptron, Deep Learning

AN ANALYSIS OF MULTILAYER PERCEPTRON (MLP) EFFECTIVENESS IN DETECTING DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS WITHIN IOT-BASED SMART HOME ECOSYSTEMS

Muhammad Rafi Rizqullah (09011282126091)

Department of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email: 09011282126091@student.unsri.ac.id

ABSTRACT

The Internet of Things (IoT) has brought various conveniences to everyday life, particularly in smart home applications. However, this increased connectivity also heightens the risk of cyber attacks, especially Distributed Denial of Service (DDoS) attacks. This study aims to analyze the effectiveness of the Multilayer Perceptron (MLP) method in detecting DDoS attacks within IoT-based smart home ecosystems. The dataset used was provided by the COMNETS team in pcap format and extracted into csv format using CICFlowMeter. The preprocessing stage involved label encoding, feature selection using a correlation matrix, data normalization with a min-max scaler, and data splitting with various ratios. The MLP model was designed with two hidden layers using ReLU activation functions, while the output layer employed a sigmoid activation function for binary classification. The model evaluation was conducted using a confusion matrix and evaluation metrics such as accuracy, precision, recall, and F1-score. Based on the test results, the MLP model achieved an optimal accuracy of 99.2% in the 60:20:20 data split scenario. This study demonstrates that MLP is effective in detecting DDoS attacks on IoT smart home devices and can serve as a potential solution for network security systems.

Keywords: DDoS, IoT, Smart Home, Multilayer Perceptron, Deep Learning

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada penelitian [1], *Internet of Things* (IoT) merupakan sebuah konsep teknologi yang memungkinkan perangkat-perangkat fisik untuk saling terhubung dan berkomunikasi melalui jaringan internet. Perangkat ini dilengkapi dengan sensor, *software*, dan teknologi lainnya yang dapat memungkinkan untuk menerima, berbagi, dan bertindak sesuai data yang diperoleh. IoT juga menciptakan ekosistem di mana perangkat-perangkat tersebut dapat diatur dan dikendalikan secara otomatis tanpa interaksi manusia secara langsung. Dalam lingkungan IoT ini, perangkat berkomunikasi satu sama lain dengan server pusat yang memungkinkan efisiensi operasional, penghematan biaya, dan meningkatkan kualitas hidup pengguna.

Penelitian [2] juga menjelaskan bahwa salah satu penerapan utama IoT adalah pada lingkungan *smart home*. *Smart home* sendiri memanfaatkan perangkat IoT untuk menjalankan tugas-tugas rumah tangga secara otomatis seperti contohnya pengaturan pencahayaan, pengendalian suhu, dan sistem keamanan. *smart home* juga memberikan kemudahan untuk penggunanya dengan kemampuan kontrol jarak jauh melalui aplikasi *mobile*. Walaupun *smart home* memiliki banyak sekali keunggulan, sistem *smart home* juga menghadapi resiko yang signifikan terhadap *cyber security*.

Penelitian [3] menjelaskan salah satu resiko yang dihadapi sistem *smart home* adalah serangan *Distributed Denial of Service* (DDoS). Serangan DDos merupakan salah satu ancaman *cyber* yang paling merusak, di mana penyerang menggunakan sejumlah besar perangkat untuk mengirimkan lalu lintas yang berlebih ke server target, sehingga dapat membuat layanan menjadi tidak dapat diakses oleh pengguna. Dengan meningkatnya pengguna IoT, maka resiko serangan DDoS juga semakin tinggi karena banyak perangkat IoT yang terhubung ke jaringan mempunyai tingkat keamanan yang lemah dan rentan terhadap eksploitasi. Maka dari itu, untuk mendeteksi serangan DDoS, *machine learning* dan *deep learning* adalah solusi yang populer digunakan sekarang. Terutama untuk *deep learning* sendiri, yang merupakan cabang dari *machine learning*, menawarkan pengguna

untuk dapat mengekstraksi fitur secara otomatis dan memiliki ketepatan yang tinggi dalam mengklasifikasikan data.

Pada penelitian [4], model yang digunakan adalah model *hybrid* bernama AE-MLP (*Autoencoder-Multilayer Perceptron*). Model ini menggunakan *autoencoder* untuk mengekstraksi fitur penting dari dataset serangan DDoS dan menggunakan MLP untuk mengklasifikasikan jenis-jenis serangan tersebut. Model ini memiliki kemampuan mengurangi waktu pemrosesan secara signifikan dengan fokus pada fitur, yang tidak hanya meningkatkan akurasi deteksi tetapi juga mempercepat proses analisis. Akan tetapi, peforma dari model ini dapat dipengaruhi oleh kualitas dataset yang digunakan. Model AE-MLP ini mendapatkan akurasi sebesar 98,34%, dengan *precision* sebesar 97,91%, *recall* 98,48 %, dan *F1-score* 98,18%, dalam mendeteksi serangan DDoS.

Pada penelitian [5], model yang digunakan adalah MLP yang dikombinasikan dengan *sequential feature selection* dan mekanisme feedback untuk mendeteksi serangan DDoS. Model ini memiliki kemampuan untuk beradaptasi secara *real-time* terhadap perubahan lalu lintas jaringan, yang meningkatkan kemampuan deteksi secara akurat. Namun, model ini masih terdapat resiko menghasilkan kesalahan deteksi seperti *false-positive* dan *false-negative*. Model ini mencapai tingkat akurasi sebesar 96% dalam mendeteksi serangan DDoS.

Pada penelitian [6], model yang digunakan merupakan *voting-based hybrid feature selection* yang digabungkan dengan algoritma *Multilayer Perceptron* dengan *Genetic algorithm* (MLP-GA) dalam mendeteksi serangan DDoS. Model ini memiliki kemampuan untuk meningkatkan akurasi deteksi dengan meminimalkan kesalahan deteksi dan mengurangi kompleksitas komputasi. Akan tetapi, model ini membutuhkan proses pemilihan fitur yang intensif dan memerlukan penyesuaian lebih lanjut pada aplikasi yang berbeda. Model MLP-GA ini mencapai tingkat akurasi sebesar 98,8% dalam mendeteksi serangan DDoS.

Pada penelitian [7], model yang digunakan adalah model *hybrid* yang menggabungkan MLP dan CNN (*Convolutional Neural Network*) untuk mendeteksi DDos di lingkungan SDN (*Software-Defined Networking*). Model ini memiliki kemampuan deteksi yang sangat akurat dan optimal dengan memanfaatkan kombinasi CNN untuk menangkap pola data temporal dan MLP untuk klasifikasi

akhir. Akan tetapi, kompleksitas model ini membutuhkan optimasi *hyperparameter* yang lebih intensif. Model ini mencapai akurasi yang sangat tinggi dengan 99,95% pada dataset CICDDoS-2019 dan 99,98% pada dataset InSDN.

Pada penelitian [8], model yang digunakan adalah model *hybrid* AE-MLP untuk mendeteksi ancaman terhadap *cyber-security* di sektor keuangan, contohnya seperti *fraud*, pelanggaran data, dan upaya akses tidak sah pada sistem keuangan. Model ini memiliki kemampuan dalam menangani data kompleks dan melakukan kompresi dan rekonstruksi data *fraud* dan akses tidak sah. Namun, model ini membutuhkan komputasi yang tinggi, terutama saat diterapkan pada data skala besar secara *real-time*. Akurasi yang dicapai oleh model ini mencapai 99% dalam mendeteksi ancaman *cyber-security* di sektor keuangan.

Pada penelitian [9], model yang digunakan adalah MLP yang diterapkan pada dataset CICIDS2017 untuk mendeteksi intrusi jaringan, termasuk serangan seperti DoS, DDoS, dan penyerangan berbasis web. Model ini memiliki akurasi yang tinggi dalam mendeteksi berbagai jenis serangan, dengan kecepatan komputasi yang lebih rendah jika dibandingkan dengan metode *deep learning* lainnya. Akan tetapi, model ini kurang optimal dalam mendeteksi serangan dengan data yang sangat sedikit. Akurasi yang dicapai oleh model ini mencapai 99,95% pada pengujian varian fitur yang optimal.

Pada penelitian [10], metode yang digunakan adalah MLP untuk mendeteksi lalu lintas botnet pada perangkat IoT, khususnya yang terinfeksi oleh mirai dan bashlite. Model ini memiliki kemampuan akurasi yang sangat tinggi dalam mendeteksi lalu lintas botnet IoT. Namun, model ini membutuhkan optimasi yang intensif untuk menangani berbagai jenis lalu lintas IoT. Model ini memiliki akurasi yang sempurna yaitu 100% dalam menguji data.

Berdasarkan uraian diatas, maka penulis memilih judul "Analisis Efektivitas *Multilayer Perceptron* (MLP) dalam Mendeteksi Serangan *Distributed Denial of Service* (DDoS) pada Ekosistem *Smart Home* Berbasis IoT" dengan harapan bahwa metode MLP serta penggabungannya dengan teknik *autoencoder* dapat mendeteksi serangan DDoS secara efektif.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang dibahas sebelumnya, maka dapat diketahui rumusan masalah pada penelitian ini sebagai berikut.

1. Bagaimana proses ekstraksi data dilakukan sebelum mendeteksi serangan DDoS (*Distributed Denial of Service*)?
2. Bagaimana proses metode MLP (*Multilayer Perceptron*) mampu mendeteksi serangan DDoS (*Distributed Denial of Service*) pada perangkat *smart home*?
3. Bagaimana cara mengukur peforma dari metode MLP (*Multilayer Perceptron*) dalam mendeteksi serangan DDoS (*Distributed Denial of Service*) pada perangkat *smart home*?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut.

1. Dataset yang digunakan merupakan dataset DDoS dari COMNETS.
2. Jenis serangan yang dideteksi adalah serangan DDoS (*Distributed Denial of Service*).
3. Algoritma yang digunakan untuk mendeteksi serangan adalah MLP (*Multilayer Perceptron*).

1.4 Tujuan

Adapun tujuan yang ingin dicapai pada penelitian ini adalah sebagai berikut.

1. Menerapkan proses ekstraksi data dengan membagi data menjadi beberapa bagian menggunakan *tools tcpdump* dan mengubah format data dari file *pcap* menjadi *csv* menggunakan *tools CICFlowmeter* agar data dapat digunakan dalam pelatihan model.
2. Menerapkan proses *pre-processing data* dengan melakukan *label encoding*, pemilihan fitur, normalisasi data, dan *split* data hingga metode MLP (*Multilayer Perceptron*) dapat mendeteksi serangan DDoS (*Distributed Denial of Service)*.
3. Menerapkan *confusion matrix* dan metrik evaluasi seperti *accuracy*, *precision*, *recall*, dan *f1-score* untuk mengukur peforma dari metode MLP

(*Multilayer Perceptron*) dalam mendeteksi serangan DDoS (*Distributed Denial of Service*).

1.5 Manfaat

Adapun manfaat yang didapat pada penelitian ini adalah sebagai berikut.

1. Mempermudah proses pengolahan dataset sehingga data yang diperoleh dapat digunakan untuk proses deteksi serangan DDoS (*Distributed Denial of Service*).
2. Mengetahui keberadaan serangan DDoS melalui metode MLP (*Multilayer Perceptron*) secara akurat.
3. Mengetahui peforma optimal dari metode MLP (*Multilayer Perceptron*) dalam mendeteksi serangan DDoS (*Distributed Denial of Service*) pada perangkat *smart home*.

1.6 Metodologi Penelitian

Adapun metodologi penelitian yang diterapkan pada penilitian yang berjudul "Analisis Efektivitas *Multilayer Perceptron* (MLP) dalam Mendeteksi Serangan *Distributed Denial of Service* (DDoS) pada Ekosistem *Smart Home* Berbasis IoT" adalah sebagai berikut.

1. Studi Literatur

   Pada metode ini, penulis melakukan eksplorasi dan menyusun referensi dari berbagai sumber, seperti jurnal ilmiah, internet, serta buku-buku yang relevan dengan penelitian tugas akhir yang sedang dilakukan.
2. Metode Konsultasi

   Pada metode ini, penulis berkonsultasi secara langsung maupun *online* dengan para ahli yang memiliki pengetahuan mendalam terkait topik yang dibahas dalam penelitian ini.
3. Metode Pengolahan Data

   Pada metode ini, penulis mengekstrak fitur dari data *pcap* yang digunakan dalam penelitian, kemudian mengkonversinya ke format CSV. Selanjutnya, dilakukan pemilihan fitur sesuai dengan pola serangan yang teridentifikasi.
4. Metode Perancangan Model dan Pengujian Data

Pada metode ini, penulis menggunakan metode tersebut untuk merancang model berdasarkan dataset yang telah diproses sebelumnya menggunakan teknik *deep learning*, dengan tujuan untuk mencapai akurasi yang optimal.

5. Metode Analisis dan Kesimpulan

   Pada metode ini, penulis melakukan analisis hasil, menarik kesimpulan, dan memberikan rekomendasi untuk pengembangan penelitian di masa mendatang.

1.7 Sistematika Penulisan

Adapun sistematika penulisan pada penelitian ini adalah sebagai berikut.

BAB I PENDAHULUAN

BAB I membahas latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi penelitian, dan juga sistematika penulisan pada penelitian ini.

BAB II TINJAUAN PUSTAKA

BAB II berisi ulasan literatur tentang penelitian sebelumnya serta teori yang relevan untuk mendukung penelitian ini. Teori-teori yang dibahas seperti mengenai *Internet of Things* (IoT), *smart home*, serangan *Distributed Denial of Service* (DDoS), *deep learning,* dan *Multilayer Perceptron* (MLP).

BAB III METODOLOGI PENELITIAN

BAB III menjelaskan tentang proses penelitian, kerangka kerja, dan perancangan model *Multilayer Perceptron* (MLP) yang digunakan untuk mendeteksi serangan *Denial of Service* (DDoS) pada perangkat *smart home*.

BAB IV HASIL DAN ANALISA

BAB IV menyajikan hasil penelitian, termasuk analisis efektiviras metode *Multilayer Perceptron* (MLP) dalam mendeteksi serangan *Distributed Denial of Service* (DDoS), serta perbandingan data normal dan data yang teridentifikasi serangan DDoS.

BAB V KESIMPULAN DAN SARAN

BAB V menyimpulkan hasil penelitian yang telah dilakukan dan memberikan rekomendasi untuk penelitian lebih lanjut yang dapat dilakukan di masa mendatang.

DAFTAR PUSTAKA

[1] A. A. Elsaeidy, A. Jamalipour, and K. S. Munasinghe, "A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City," *IEEE Access*, vol. 9, pp. 154864–154875, 2021, doi: 10.1109/ACCESS.2021.3128701.

[2] I. Cvitic, D. Perakovic, B. B. Gupta, and K.-K. R. Choo, "Boosting-Based DDoS Detection in Internet of Things Systems," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2109–2123, Feb. 2022, doi: 10.1109/JIOT.2021.3090909.

[3] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. Ben Dhaou, "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model," *IEEE Access*, vol. 11, no. October, pp. 119862–119875, 2023, doi: 10.1109/ACCESS.2023.3327620.

[4] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," *IEEE Access*, vol. 9, pp. 146810–146821, 2021, doi: 10.1109/ACCESS.2021.3123791.

[5] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," *Comput. Secur.*, vol. 88, p. 101645, Jan. 2020, doi: 10.1016/j.cose.2019.101645.

[6] U. S. Chanu, K. J. Singh, and Y. J. Chanu, "A dynamic feature selection technique to detect DDoS attack," *J. Inf. Secur. Appl.*, vol. 74, p. 103445, May 2023, doi: 10.1016/j.jisa.2023.103445.

[7] M. A. Setitra, M. Fan, B. L. Y. Agbley, and Z. E. A. Bensalem, "Optimized MLP-CNN Model to Enhance Detecting DDoS Attacks in SDN Environment," *Network*, vol. 3, no. 4, pp. 538–562, Dec. 2023, doi: 10.3390/network3040024.

[8] L. Almahadeen *et al.*, "Enhancing Threat Detection in Financial Cyber Security Through Auto Encoder-MLP Hybrid Models," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 4, pp. 924–933, 2024, doi: 10.14569/IJACSA.2024.0150495.

[9] A. Rosay *et al.*, "MLP4NIDS : An Efficient MLP-Based Network Intrusion Detection for CICIDS2017 Dataset To cite this version : HAL Id : hal-

03266466 MLP4NIDS : an efficient MLP-based Network Intrusion Detection for CICIDS2017 dataset," pp. 0–15, 2021.

[10] Y. Javed and N. Rajabi, "Multi-Layer Perceptron Artificial Neural Network Based IoT Botnet Traffic Classification," in *Advances in Intelligent Systems and Computing*, vol. 1069, no. June, 2020, pp. 973–984. doi: 10.1007/978-3-030-32520-6_69.

[11] B. Tushir, Y. Dalal, B. Dezfouli, and Y. Liu, "A Quantitative Study of DDoS and E-DDoS Attacks on WiFi Smart Home Devices," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6282–6292, Apr. 2021, doi: 10.1109/JIOT.2020.3026023.

[12] I. Lee, "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management," *Futur. Internet*, vol. 12, no. 9, p. 157, Sep. 2020, doi: 10.3390/fi12090157.

[13] W. Zhe, C. Wei, and L. Chunlin, "DoS attack detection model of smart grid based on machine learning method," in *2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, IEEE, Jul. 2020, pp. 735–738. doi: 10.1109/ICPICS50287.2020.9202401.

[14] J. A. Perez-diaz and J. A. Cantoral-ceballos, "Transport and Application Layer DDoS Attacks Detection to IoT," 2022.

[15] S. Hizal, U. Cavusoglu, and D. Akgun, "A novel deep learning-based intrusion detection system for IoT DDoS security," *Internet of Things (Netherlands)*, vol. 28. 2024. doi: 10.1016/j.iot.2024.101336.

[16] A. Lazcano, M. A. Jaramillo-Morán, and J. E. Sandubete, "Back to Basics: The Power of the Multilayer Perceptron in Financial Time Series Forecasting," *Mathematics*, vol. 12, no. 12, p. 1920, Jun. 2024, doi: 10.3390/math12121920.

[17] H. R. Arabnia *et al.*, *Advances in Artificial Intelligence and Applied Cognitive Computing*. in Transactions on Computational Science and Computational Intelligence. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-70296-0.

[18] T. Van Dao, H. Sato, and M. Kubo, "MLP-Mixer-Autoencoder: A Lightweight Ensemble Architecture for Malware Classification," *Inf.*, vol.

14, no. 3, 2023, doi: 10.3390/info14030167.

[19] C. Wang, H. Liu, Y. Sun, Y. Wei, K. Wang, and B. Wang, "Dimension Reduction Technique Based on Supervised Autoencoder for Intrusion Detection of Industrial Control Systems," *Secur. Commun. Networks*, vol. 2022, pp. 1–12, Jun. 2022, doi: 10.1155/2022/5713074.

[20] E. Pratama, "Deteksi Serangan DDoS DoS MITM Pada Jaringan Smarthome Dengan Menggunakan Metode Decision Tree," 2025.