SISTEM DETEKSI SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS) PADA PERANGKAT *SMARTHOME* MENGGUNAKAN METODE *RECCURENT NEURAL NETWORK* (RNN)

SKRIPSI

Oleh :
HEPRA OVILIA
09011282126090

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2025

LEMBAR PENGESAHAN

SKRIPSI

SISTEM DETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA PERANGKAT SMARTHOME MENGGUNAKAN METODE RECCURENT NEURAL NETWORK (RNN)

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

Oleh:

HEPRA OVILIA

09011282126090

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

DETECTION SYSTEM OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS ON SMARTHOME DEVICES USING THE RECURRENT NEURAL NETWORK (RNN) METHOD

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

Oleh:

HEPRA OVILIA

09011282126090

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 : Dr. Ahmad Zarkasi, M.T.
2. Penguji : Kemahyanto Exaudi, S.Kom., M.T.
3. Pembimbing I : Prof. Ir. Deris Stiawan, M.T., Ph.D.
4. Pembimbing II : Nurul Afifah, M.Kom

Mengetahui, 26/6/25

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

SURAT PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Hepra Ovilia

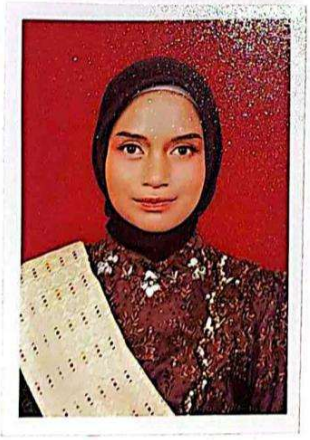
NIM : 090112821260930

Judul : Sistem Deteksi Serangan *Distributed Denial of Service (DDoS)* Pada Perangkat *Smarthome* Menggunakan Metode *Recurrent Neural Network (RNN)*

Hasil Pengecekan Plagiat/Turnitin: 7%

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, 26 Juni 2025

Yang Menyatakan

Hepra Ovilia

NIM. 09011282126090

KATA PENGANTAR

Puji dan syukur atas kehadiran Allah SWT, karena berkat Rahmat dan Karunia-Nya, sehingga penulis dapat menyelesaikan Skripsi ini yang berjudul **"Sistem Deteksi Serangan *Distributed Denial of Service* (DDoS) Pada Perangkat *Smarthome* Menggunakan Metode *Reccurent Neural Network* (RNN)"**. Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga, sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Dalam kesempatan ini penulis mengucapkan terima kasih kepada pihak yang telah memberikan bantuan serta motivasi sehingga penulis dapat menyelesaikan penulisan Skripsi ini :

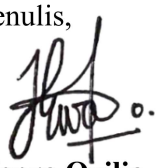
1. Allah SWT, yang telah melimpahkan Berkat dan Rahmatnya.
2. Bapak Prayogi, Johan Erlangga, dan Aldino yang selalu mendukung dan memotivasi penulis.
3. Pintu surgaku, ibunda tercinta yaitu Ibu Suhermi yang telah memberikan kasih sayang dan cinta kepada penulis, serta selalu menjadi tempat pulang yang paling ternyaman bagi penulis. Terima kasih untuk do'a yang beliau panjatkan selama ini sehingga penulis mampu menyelesaikan studinya sampai sarjana.
4. Keluarga besar supardi yang selalu mendukung dan memotivasi penulis.
5. Bapak Prof. Dr. Erwin, M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
7. Bapak Huda Ubaya, M.T. selaku Sekretaris Jurusan Sistem Komputer Universitas Sriwijaya
8. Bapak Iman Saladin B. Azhar, S.Kom., M.Msi selaku Dosen pembimbing akademik penulis di jurusan Sistem Komputer.
9. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D. dan Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.

10. Kak Angga Pratama selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas administrasi selama perkuliahan.
11. Chairul Ikhsan selaku *support system* yang selalu menjadi bagian dari proses perjalanan penulis selama menyusun skripsi, yang selalu memberikan dukungan, tenaga, dan waktu kepada penulis.
12. Sahabat penulis, Zaafira Nadira Putri, Nur Agustina Anggraini, dan Dwi Tessa Paramitha yang selalu menemani serta mendengarkan keluh kesah penulis selama masa perkuliahan.
13. Diah Ayuning Tyas, Makiyah, Alyatisa, Zaidan Amru Abdillah, M. Rafi Rizqullah, dan Aldi Hoirul Fatih selaku sahabat seperjuangan yang telah membantu dan memberikan dukungan kepada penulis dari awal perkuliahan hingga saat ini.
14. Teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2021, terkhusus kelas C.
15. Kakak tingkat Sistem Komputer Universitas Sriwijaya.

Penulis menyadari bahwa dalam penyusunan laporan ini masih sangat jauh dari kata sempurna. Oleh karena itu penulis mengharapkan kritik dan saran dari semua pihak yang berkenan agar laporan ini dapat lebih baik. Akhir kata penulis mengucapkan terima kasih banyak kepada semua pihak yang telah membantu penulis dalam proses penyelesaian serta penyusunan Skripsi ini. Penulis juga berharap agar Skripsi ini dapat bermanfaat dan berguna bagi siapa saja yang membacanya.

Palembang, 26 Juni 2025

Penulis,



Hepra Ovilia

NIM. 09011282126090

SISTEM DETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA PERANGKAT SMARTHOME MENGGUNAKAN METODE RECURRENT NEURAL NETWORK (RNN)

Hepra Ovilia (090112982126090)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: 09011282126090@student.unsri.ac.id

ABSTRAK

Internet of Things (IoT) telah memberikan kemudahan dalam mengelola perangkat rumah secara otomatis melalui implementasi konsep *smarthome*. Namun, semakin banyak perangkat yang terhubung dalam jaringan dapat meningkatkan risiko terhadap serangan siber, salah satunya adalah *Distributed Denial of Service* (DDoS) yang dapat mengganggu ketersediaan layanan. Penelitian ini bertujuan untuk mendeteksi serangan DDoS pada perangkat *smarthome* menggunakan metode *Recurrent Neural Network* (RNN), yang dikenal efektif dalam menangani data sekuensial. Dataset yang digunakan berasal dari tim *COMNETS Smarthome* dalam format *.pcap*, yang kemudian diekstraksi menjadi format .csv menggunakan *CICFlowMeter*. Tahapan pemodelan meliputi proses data *understanding, feature selection*, *label encoding*, normalisasi, *balancing* data menggunakan *SMOTE*, dan pembagian data untuk pelatihan dan pengujian model. Evaluasi dilakukan menggunakan metrik akurasi, *precision*, *recall*, dan *F1-score*. Hasil pengujian menunjukkan bahwa model RNN mampu mendeteksi serangan DDoS dengan akurasi 99,76%, presisi 99,53%, *recall* 100%, dan *F1-score* 99,76%, pada skenario split data 80:10:10. Dengan demikian, model RNN efektif dalam mengidentifikasi serangan DDoS pada perangkat *smarthome*.

kata kunci : *Internet of Things*, *Smarthome*, DDoS, SNORT, RNN, *Deep Learning*, Deteksi Serangan

DETECTION SYSTEM OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS ON SMARTHOME DEVICES USING THE RECURRENT NEURAL NETWORK (RNN) METHOD

Hepra Ovilia (090112982126090)

Department of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email: 09011282126090@student.unsri.ac.id

ABSTRACT

The Internet of Things (IoT) has facilitated the automation of household device management through the implementation of smart home concepts. However, the increasing number of connected devices in a network also raises the risk of cyberattacks, one of which is the Distributed Denial of Service (DDoS) attack that can disrupt service availability. This study aims to detect DDoS attacks on smart home devices using the Recurrent Neural Network (RNN) method, which is known for its effectiveness in handling sequential data. The dataset used originates from the COMNETS Smart Home team in .pcap format and is then extracted into .csv format using CICFlowMeter. The modeling stages include data understanding, feature selection, label encoding, normalization, data balancing using SMOTE, and data splitting for training and testing the model. Evaluation was conducted using accuracy, precision, recall, and F1-score metrics. The test results show that the RNN model is capable of detecting DDoS attacks with an accuracy of 99.76%, precision of 99.53%, recall of 100%, and an F1-score of 99.76% on an 80:10:10 data split scenario. Therefore, the RNN model has proven effective in identifying DDoS attacks on smart home devices.

Keywords: Internet of Things, Smarthome, DDoS, SNORT, RNN, Deep Learning, Attack Detection

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Smart Home merupakan salah satu konsep yang menggunakan teknologi *Internet of Things* (IoT) untuk menghubungkan berbagai perangkat dan sistem didalamnya. Menurut penelitian [1], Perangkat IoT yang terkoneksi dalam lingkungan *smart home* memberikan kemudahan dalam pengelolaan dan pengendalian rumah secara otomatis, seperti pengaturan lampu, suhu dan keamanan. Selain itu, [2] menjelaskan bahwa *smart home* membentuk jaringan energi dengan memanfaatkan aliran listrik dan informasi dua arah. Dibandingkan dengan jaringan konvensional, smart home menawarkan manajemen daya yang lebih efisien, skalabilitas yang tinggi, keandalan sistem yang lebih baik, ketahanan yang lebih baik, efektivitas biaya yang lebih tinggi, dan produksi energi bersih. Namun, dibalik semua keunggulan ini, muncul tantangan baru terutama dalam hal keamanan siber. Semakin banyaknya perangkat yang terhubung ke internet, ancaman terhadap keamanan siber juga semakin meningkat secara signifikan, salah satunya pada serangan *Distributed Denial of Service* (DDoS). Sifat perangkat IoT yang saling terhubung [3] menyebabkan peningkatan risiko keamanan, karena serangan pada satu perangkat dapat dengan cepat menyebar ke perangkat lainnya.

Pada penelitian yang dilakukan oleh Yousuf dan Mir (2022), dijelaskan bahwa serangan DDoS menargetkan ketersediaan sumber daya dan server jaringan dengan menyerang media komunikasi dari berbagai lokasi berbeda dengan memanfaatkan perangkat IoT. Pada penelitian [4] menunjukkan bahwa sekitar 48% dari semua perangkat IoT pada sistem *smart home* rentan terhadap ancaman dari serangan *Distributed Denial of Service* (DDoS). Hal ini membuat serangan DDoS semakin sulit untuk dideteksi karena lalu lintas jaringan yang dihasilkan dari berbagai sumber yang terdistribusi, sehingga sulit untuk membedakan antara lalu lintas yang sah dan yang berbahaya.

Berbagai penelitian telah dilakukan untuk mengembangkan metode yang lebih efektif dan akurat dalam meningkatkan deteksi serangan DDoS pada jaringan smart home. Dalam menghadapi kompleksitas dan evolusi serangan DDoS yang semakin canggih, pendekatan keamanan tradisional menjadi kurang efektif. Salah satu solusi untuk mengatasi keterbatasan ini adalah dengan menggunakan pendekatan *deep learning*. *Deep learning*, sebagaimana dijelaskan oleh [5], merupakan jaringan saraf dengan banyak lapisan yang mampu mengekstraksi fitur secara otomatis dari data, biasanya digunakan untuk tugas klasifikasi atau regresi. Pada penelitian [6] menjelaskan bahwa model *deep learning* mampu mengidentifikasi anomali dan pola serangan dengan akurasi yang jauh lebih tinggi dibandingkan dengan metode konvesional. Keunggulan utama dari *deep learning* terletak pada kemampuannya untuk mempelajari pola data yang tidak terlihat dengan jelas oleh metode konvensional. Diantara berbagai jenis arsitektur *deep learning*, *Recurrent Neural Network* (RNN) menunjukkan potensi yang bisa digunakan dalam konteks keamanan jaringan *smart home*. Pada penelitian [7] menjelaskan bahwa RNN memiliki keunggulan signifikan dalam menganalisis data sekuensial seperti lalu lintas jaringan, karena kemampuannya untuk mempertahankan memori dari input sebelumnya. Sehingga, RNN memiliki kemampuan untuk mempelajari urutan data dan hubungan antarwaktu dalam jaringan, yang sangat penting dalam mendeteksi serangan yang terjadi secara terus-menerus atau berulang-ulang [8]. Selain itu, pada penelitian [9] menjelaskan bahwa RNN bekerja baik dengan kumpulan data yang besar dan sangat mudah memahami data selama proses pelatihan, yang mana berdasarkan hasil demonstrasi model RNN mampu mencapai tingkat akurasi yang tinggi dalam mengklasifikasi serangan pada perangkat IoT.

Pada penelitian [2] menggunakan model RNN dan metode *Stacked Recurrent Neural Network* (SRNN) sebagai solusi untuk deteksi serangan botnet. Penelitian mengevaluasi efektivitas RNN dalam mengklasifikasikan lalu lintas jaringan yang sangat tidak seimbang. Beberapa lapisan RNN ditumpuk dalam SRNN untuk mempelajari representasi hirarkis dari data tersebut.

Pada penelitian [7] menerapkan solusi deteksi serangan DDoS pada

perangkat IoT yang lebih efektif dengan menggunakan model RNN dan arsitektur tiga lapis berbasis SDN. Model ini menghasilkan akurasi 99,68% serta metrik lainnya yang sangat baik, seperti *True Positive Rate* 0.999, *False Positive Rate* 0.01, *Precision* 0.999. Adapun keterbatasan dari penelitian ini terletak pada pengujian yang hanya menggunakan 177 *instance*, yang membuatnya kurang valid untuk skala besar. Pengujian lebih lanjut disarankan menggunakan dataset yang lebih besar dan mengoptimalkan algoritma untuk jaringan yang lebih kompleks.

Pada penelitian [10] menerapkan model RNN untuk deteksi intrusi (*Intrusion Detection Systems*/IDS), dengan hasil akurasi mencapai 74,19% dan F1-Score 90,26%. Namun, penelitian pada model ini masih rentan terhadap *gradient explosion* dan *gradient vanishing*, sehingga kurang mampu menangkap pola dari urutan yang panjang. Meskipun IDS berbasis *deep learning* menawarkan solusi keamanan untuk IoT, tantangan seperti pemrosesan data besar, ekstraksi pola kompleks serta desain eksperimen masih memerlukan penelitian lebih lanjut.

Berdasarkan pada ulasan diatas maka penulis mengusulkan untuk melakukan penelitian dengan judul "Sistem Deteksi Serangan *Distributed Denial of Service* (DDoS) Pada Perangkat *Smarthome* Menggunakan Metode *Reccurent Neural Network* (RNN)". Ini bertujuan agar dapat mendeteksi serangan DDoS pada perangkat *smart home* dengan tingkat akurasi yang tinggi.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka dapat disimpulkan rumusan masalah dalam penelitian ini antara lain sebagai berikut.

1. Bagaimana proses ekstraksi data dilakukan untuk mendeteksi serangan *Distributed Denial of Service* (DDoS) pada perangkat *Smarthome*?
2. Bagaimana cara mengatasi data yang tidak seimbang (*imbalance data*) agar mencapai kinerja optimal?
3. Bagaimana cara mengukur performa pada metode *Recurrent Neural Network* (RNN) untuk mendeteksi serangan *Distributed Denial of Service* (DDoS)?

1.3 Batasan Masalah

Batasan masalah dari ini meliputi hal-hal berikut:

1. Menggunakan dataset *Smarthome COMNETS*
2. Dataset yang digunakan hanya mencakup data normal dan data serangan *Distributed Denial of Service* (DDoS).
3. Menggunakan metode *Recurrent Neural Network* (RNN) untuk mendeteksi serangan *Distributed Denial of Service* (DDoS).

1.4 Tujuan

Adapun Tujuan dari penelitian yang ingin di capai berdasarkan rumusan masalah yang telah disusun yaitu sebagai berikut.

1. Melakukan proses ekstraksi data dari file *.pcap* ke CSV menggunakan *tools CICFlowmeter* untuk identifikasi pola serangan DDoS.
2. Menerapkan teknik *oversampling SMOTE* (*Synthetic Minority Oversampling Technique*) untuk menyeimbangkan distribusi kelas dalam dataset.
3. Mengukur dan mengevaluasi performa pada metode *Recurrent Neural Network* (RNN) menggunakan *accuracy*, *precision*, *recall*, *F1-score* dan *confusion matrix*.

1.5 Manfaat

Adapun manfaat dari penelitian ini, yaitu sebagai berikut.

1. Dapat mengolah data dari file pcap ke file CSV menggunakan *tools* serta dapat membantu analisis mendalam.
2. Dapat mengatasi ketidakseimbangan data dengan menerapkan metode *oversampling*.
3. Dapat mengetahui performa pada metode *Recurrent Neural Network* (RNN) untuk mendeteksi serangan *Distributed Denial of Service* (DDoS).

1.6 Metodologi Penelitian

Adapun penerapan metodologi penelitian yang digunakan pada penelitian yaitu sebagai berikut.

1. Studi Pustaka dan Literatur

   Dengan menggunakan metode ini, penulis dapat melakukan proses eksplorasi dan menggabungkan referensi dari berbagai sumber, seperti jurnal, internet, dan buku yang berkaitan dengan riset tugas akhir yang dilakukan.

2. Metode Konsultasi

   Metode ini memungkinkan penulis untuk berkonsultasi secara real-time atau secara online dengan narasumber yang memiliki ilmu dan pengertahuan yang luas tentang masalah yang dibahas pada riset ini.

3. Metode Pengolahan Data

   Dengan menggunakan metode ini, penulis dapat mengekstrak fitur dari data pcap yang digunakan dalam penelitian menjadi format CSV, kemudian memilih fitur sesuai dengan pola serangan yang diidentifikasi.

4. Metode Pengerjaan Model dan Pengujian Data

   Metode ini digunakan oleh penulis untuk membuat rancangan dari model dataset yang sudah diolah pada tahap sebelumnya dengan menggunakan deep learning untuk mencapai akurasi yang diharapkan.

5. Metode Analisa dan Kesimpulan

   Pada tahap ini penulis melakukan analisis, membuat kesimpulan, dan membuat rekomendasi untuk penelitian ke depannya.

1.7 Sistematika Penulisan

Adapun sistematika pada penulisan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

BAB I menjelaskan latar belakang, tujuan, manfaat, perumusan masalah, batasan masalah, metodologi penelitian, dan prosedur penulisan tugas akhir.

BAB II TINJAUAN PUSTAKA

BAB II mengandung *literature review* tentang penelitian sebelumnya dan teori yang relevan untuk mendukung penelitian ini. Teori–teori tersebut

termasuk *Distributed Denial of Service* (DDoS), *Deep Learning*, dan *Recurrent Neural Network* (RNN).

BAB III METODOLOGI PENELITIAN

BAB III memberikan penjelasan tentang proses penelitian, kerangka kerja, serta perancangan dari model *Recurrent Neural Network* (RNN) yang digunakan pada peneliian untuk mendeteksi serangan *Distributed Denial of Service* (DDoS).

BAB IV HASIL DAN ANALISA

BAB IV akan membahas temuan penelitian dan menganalisis deteksi serangan *Distributed Denial of Service* (DDoS) pada perangkat *smart home* dengan menggunakan metode *Recurrent Neural Network* (RNN) yang telah dilakukan.

BAB V KESIMPULAN DAN SARAN

BAB V berisi hasil penelitian dan rekomendasi untuk penelitian lanjutan.

DAFTAR PUSTAKA

[1] S. I. Popoola, B. Adebisi, M. Hammoudeh, H. Gacanin, and G. Gui, "Stacked recurrent neural network for botnet detection in smart homes," *Comput. Electr. Eng.*, vol. 92, no. August 2020, p. 107039, 2021, doi: 10.1016/j.compeleceng.2021.107039.

[2] C. Singh and A. K. Jain, "A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network," *e-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 8, no. April, p. 100543, 2024, doi: 10.1016/j.prime.2024.100543.

[3] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS Detection using Deep Learning," *Procedia Comput. Sci.*, vol. 218, pp. 2420–2429, 2022, doi: 10.1016/j.procs.2023.01.217.

[4] 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.

[5] O. Yousuf and R. N. Mir, "DDoS attack detection in Internet of Things using recurrent neural network," *Comput. Electr. Eng.*, vol. 101, no. April, p. 108034, 2022, doi: 10.1016/j.compeleceng.2022.108034.

[6] H. Liao *et al.*, "A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things," *IEEE Access*, vol. 12, no. December 2023, pp. 4745–4761, 2024, doi: 10.1109/ACCESS.2023.3349287.

[7] S. Yadav, H. Hashmi, D. Vekariya, Z. A. K. N, and V. F. J, "Mitigation of attacks via improved network security in IOT network environment using RNN," *Meas. Sensors*, vol. 32, no. December 2023, p. 101046, 2024, doi: 10.1016/j.measen.2024.101046.

[8] C. Y. Chen, L. A. Chen, Y. Z. Cai, and M. H. Tsai, "RNN-based DDoS Detection in IoT Scenario," *Proc. - 2020 Int. Comput. Symp. ICS 2020*, pp. 448–453, 2020, doi: 10.1109/ICS51289.2020.00094.

[9] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Comput. Secur.*, vol. 127, 2023,

doi: 10.1016/j.cose.2023.103096.

[10] 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.

[11] D. Akgun, S. Hizal, and U. Cavusoglu, “A new DDoS attacks intrusion detection model based on deep learning for cybersecurity,” *Comput. Secur.*, vol. 118, p. 102748, 2022, doi: 10.1016/j.cose.2022.102748.

[12] I. Ahmad, Z. Wan, and A. Ahmad, “A big data analytics for DDOS attack detection using optimized ensemble framework in Internet of Things,” *Internet of Things (Netherlands)*, vol. 23, no. May 2023, p. 100825, 2023, doi: 10.1016/j.iot.2023.100825.

[13] S. Dong and M. Sarem, “DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks,” *IEEE Access*, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.

[14] D. Yedilkhan and S. Smakova, “Machine Learning Approaches for Smart Home Device Recognition from Network Traffic,” *Procedia Comput. Sci.*, vol. 231, pp. 709–714, 2024, doi: 10.1016/j.procs.2023.12.157.

[15] B. R. KIKISSAGBE, M. Adda, P. Célicourt, I. T. HAMAN, and A. Najjar, “Machine Learning for DoS Attack Detection in IoT Systems,” *Procedia Comput. Sci.*, vol. 241, no. 2019, pp. 195–202, 2024, doi: 10.1016/j.procs.2024.08.027.

[16] K. Sahoo, A. K. Samal, J. Pramanik, and S. K. Pani, “Exploratory data analysis using python,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 12, pp. 4727–4735, 2019, doi: 10.35940/ijitee.L3591.1081219.

[17] J. Brandt and E. Lanzén, “A Comparative Review of SMOTE and ADASYN in Imbalanced Data Classification,” *2021*, p. 42, 2020, [Online]. Available: https://www.divaportal.org/smash/record.jsf?pid=diva2:1519153

[18] O. S. Nalçin, “StandardScaler vs. MinMaxScaler vs. RobustScaler: Which one to use for your next ML project?,” Medium. [Online]. Available: https://medium.com/@onersarpnalcin/standardscaler-vs-minmaxscaler-vs-robustscaler-which-one-to-use-for-your-next-ml-project-ae5b44f571b9

[19] S. Aktar and A. Yasin Nur, “Towards DDoS attack detection using deep learning approach,” *Comput. Secur.*, vol. 129, p. 103251, 2023, doi: 10.1016/j.cose.2023.103251.

[20] G. Abbas, M. Tanveer, Z. H. Abbas, M. Waqas, T. Baker, and D. Al-Jumeily OBE, “A secure remote user authentication scheme for 6LoWPAN-based Internet of Things,” *PLoS One*, vol. 16, no. 11 November, pp. 1–18, 2021, doi: 10.1371/journal.pone.0258279.

[21] M. Waqas and U. W. Humphries, “A Critical Review of RNN and LSTM Variants in Hydrological Time Series Predictions,” *MethodsX*, vol. 13, no. July, p. 102946, 2024, doi: 10.1016/j.mex.2024.102946.

[22] J. Erbani, P. É. Portier, E. Egyed-Zsigmond, and D. Nurbakova, “Confusion Matrices: A Unified Theory,” *IEEE Access*, vol. 12, no. December, 2024, doi: 10.1109/ACCESS.2024.3507199.

[23] Y. Wang, Y. Jia, Y. Tian, and J. Xiao, “Deep reinforcement learning with the confusion-matrix-based dynamic reward function for customer credit scoring,” *Expert Syst. Appl.*, vol. 200, no. March, p. 117013, 2022, doi: 10.1016/j.eswa.2022.117013.

[24] P. Edo, “Deteksi serangan ddos, dos, dan mitm pada jaringan smarthome dengan menggunakan metode decision tree”, Skripsi, 2025.