DETEKSI SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS) PADA SISTEM *SMARTHOME* MENGGUNAKAN METODE *CONVOLUTIONAL NEURAL NETWORK* (CNN)

SKRIPSI

Oleh:

Diah Ayuning Tyas

09011282126092

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA SISTEM SMARTHOME MENGGUNAKAN METODE CONVOLUTIONAL NEURAL NETWORK (CNN)

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

Oleh:

DIAH AYUNING TYAS

09011282126092

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 OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS ON SMART HOME SYSTEMS USING THE CONVOLUTIONAL NEURAL NETWORK (CNN) METHOD

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

By:

DIAH AYUNING TYAS

09011282126092

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. Rossi Passarella, M.Eng.
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, 24/6/25

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Diah Ayuning Tyas

NIM : 09011282126093

Judul : Deteksi Serangan *Distributed Denial of Service* (DDoS) pada Sistem *Smarthome* menggunakan Metode *Convolutional Neural Network* (CNN)

Hasil Pengecekan Plagiat/Turnitin: 4%

Menyatakan bahwa laporan tugas akhir ini merupakan hasil karya saya pribadi dan bebas dari unsur penjiplakan atau plagiarisme. Apabila di kemudian hari terbukti terdapat tindakan plagiarisme dalam laporan ini, saya bersedia menerima sanksi akademik yang ditetapkan oleh Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dengan penuh kesadaran dan tanpa tekanan dari pihak manapun.

Palembang, Juni 2025

Yang menyatakan

Diah Ayuning Tyas

NIM. 09011282126092

KATA PENGANTAR

Segala puji dan syukur penulis haturkan kepada Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul "Deteksi *Serangan Distributed Denial of Service* (DDoS) pada Sistem *Smarthome* Menggunakan Metode *Convolutional Neural Network* (CNN)". Laporan ini merupakan salah satu bentuk pemenuhan syarat akademik dalam rangka menyelesaikan Mata Kuliah Skripsi di Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya. Pembahasan dalam Tugas Akhir ini berfokus pada penerapan metode *Convolutional Neural Network* (CNN) untuk mendeteksi serangan DDoS yang menjadi ancaman bagi sistem *Smarthome* berbasis teknologi *Internet of Things* (IoT).

Dalam proses penyusunan Tugas Akhir ini, penulis mendapatkan bantuan dan dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada :

1. Tuhan Yang Maha Esa, atas rahmat dan bimbingan-Nya yang senantiasa mengiringi penulis.
2. Orang Tua yang saya cintai Ibu Emi Zarmilawati dan Bapak Yuslan, serta Kakak tercinta Dio Ananda Nikola yang selalu memberikan doa, dukungan, dan semangat selama proses penulisan Tugas Akhir 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 Huda Ubaya, S.T., M.T., selaku Dosen Pembimbing Akademik.
6. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing Tugas Akhir 1.
7. Ibu Nurul Afifah, M.Kom., selaku Dosen Pembimbing Tugas Akhir 2.
8. Kak Angga, selaku admin Jurusan Sistem Komputer, yang telah membantu proses administrasi.

9. Pemilik NIM 09011282126091 Muhammad Rafi Rizqullah, partner terbaik yang selalu memberikan dukungan terbaik dan selalu menemani penulis dalam melewati segala proses dan pengerjaan Tugas Akhir.
10. Sahabat seperti saudara, Dwinda Ayu Safitri yang selalu mendukung dan membimbing penulis.
11. Sahabat seperjuangan Hepra Ovilia, Makiyah, Alyatisa, Aldi Hoirul Fatih, Chairul Ikhsan, dan Zaidan Amru Abdillah, yang selalu ada dalam suka maupun duka yang selalu memberikan dukungan kepada Penulis.
12. Teman-teman Sistem Komputer Angkatan 2021 Indralaya, atas dukungan dan semangat selama masa studi.
13. Kakak tingkat Sistem Komputer Universitas Sriwijaya, atas masukan dan bimbingannya selama ini.
14. Seluruh pihak yang membantu dalam menyelesaikan laporan ini yang tidak bisa disebutkan satu persatu.
15. Almamater

Penulis menyadari bahwa Tugas Akhir ini masih memiliki banyak kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk menyempurnakan laporan ini di masa mendatang. Akhir kata, penulis berharap Tugas Akhir ini dapat memberikan manfaat, wawasan, dan pengetahuan bagi para pembaca maupun pihak lain yang memerlukannya.

Palembang, 23 June 2025

Diah Ayuning Tyas
NIM. 09011282126092

DETEKSI SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS) PADA SISTEM *SMARTHOME* MENGGUNAKAN METODE *CONVOLUTIONAL NEURAL NETWORK* (CNN)

Diah Ayuning Tyas (09011282126092)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: 09011282126092@student.unsri.ac.id

ABSTRAK

Internet of Things (IoT) menghadirkan banyak manfaat, namun juga meningkatkan risiko keamanan, salah satunya adalah serangan *Distributed Denial of Service* (DDoS). Serangan ini dapat melumpuhkan sistem *Smarthome* dengan membanjiri jaringan menggunakan lalu lintas data berlebih. Penelitian ini bertujuan untuk mendeteksi serangan DDoS pada perangkat *Smarthome* menggunakan metode *Convolutional Neural Network* (CNN). Dataset yang digunakan berasal dari COMNETS dalam bentuk file PCAP, yang kemudian diekstraksi menjadi CSV menggunakan *CICFlowMeter*. Data selanjutnya diproses melalui tahapan preprocessing seperti *label encoding, feature selection*, normalisasi, *reshaping*, dan pembagian data. Model CNN dibangun dengan arsitektur *Conv1D, MaxPooling1D, Flatten, Dense, dan Dropout*. Evaluasi dilakukan menggunakan metrik akurasi, presisi, *recall*, dan *F1-score*. Hasil terbaik diperoleh dengan akurasi sebesar 98,28%, presisi 98,23%, *recall* 100%, dan *F1-score* 98,28%. Hasil ini menunjukkan bahwa metode CNN sangat efektif dalam mendeteksi serangan DDoS pada sistem *Smarthome* berbasis *Internet of Things* (IoT) secara *real-time* dan akurat.

Kata kunci: *Internet of Things, Smarthome*, DDoS, CNN, *Deep Learning*, Keamanan Jaringan.

DETECTION OF DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS ON SMARTHOME SYSTEMS USING THE CONVOLUTIONAL NEURAL NETWORK (CNN) METHOD

Diah Ayuning Tyas (09011282126092)

Department of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email: 09011282126092@student.unsri.ac.id

ABSTRACT

The Internet of Things (IoT) offers numerous benefits but also increases security risks, one of which is Distributed Denial of Service (DDoS) attacks. These attacks can cripple Smarthome systems by flooding the network with excessive data traffic. This research aims to detect DDoS attacks on Smarthome devices using the Convolutional Neural Network (CNN) method. The dataset used was obtained from COMNETS in PCAP file format, which was then extracted into CSV format using CICFlowMeter. The data was processed through several preprocessing stages, including label encoding, feature selection, normalization, reshaping, and data splitting. The CNN model was built using an architecture consisting of Conv1D, MaxPooling1D, Flatten, Dense, and Dropout layers. The model was evaluated using accuracy, precision, recall, and F1-score metrics. The best results were obtained with an accuracy of 98.28%, precision of 98.23%, recall of 100%, and F1-score of 98.28%. These results indicate that the CNN method is highly effective in detecting DDoS attacks on IoT-based Smarthome systems in real time and with high accuracy.

Keywords: Internet of Things, Smarthome, DDoS, CNN, Deep Learning, Network Security.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) merupakan konsep yang menghubungkan berbagai perangkat ke internet sehingga dapat berkomunikasi dan bertukar data dimana saja dan kapan saja. Penggunaan *Internet of Things* (IoT) dapat ditemukan dalam pengembangan sistem rumah pintar (S*marthome*), *platform e-commerce* yang canggih, dan sistem kesehatan berbasis teknologi. Dengan adanya IoT, penerapan teknologi ini memberikan dampak signifikan dalam meningkatkan efisiensi dan produktivitas di berbagai sektor. Pada penelitian [1] menjelaskan bahwa teknologi IoT memungkinkan perangkat untuk saling terhubung melalui internet, berkomunikasi, dan bertukar data secara *real-time*. Penerapan teknologi IoT memberikan dampak besar terhadap efisiensi dan produktivitas karena mengurangi biaya operasional dan meningkatkan kualitas layanan di berbagai industri.

Salah satu ancaman terbesar dalam ekosistem *Internet of Things* (IoT) adalah serangan *Distributed Denial of Service* (DDoS) yang menyebabkan penyerang memanfaatkan jaringan perangkat IoT yang terdampak untuk membanjiri sistem dengan lalu lintas data berlebihan sehingga menyebabkan perangkat menjadi tidak responsif atau bahkan gagal berfungsi. Dalam penelitian [2] diketahui seperti pada *Smarthome*, serangan DDoS dapat melumpuhkan perangkat penting seperti kamera keamanan, sistem alarm, dan sistem keamanan lainnya, sehingga bisa membahayakan keselamatan dan keamanan pengguna.

Penelitian [3] menjelaskan permasalahan serangan DDoS membutuhkan solusi berbasis *deep learning* dengan berbagai model semakin banyak digunakan seperti *Convolutional Neural Network* (CNN), *Long short-Term Memory* (LSTM), *Autoencoder* telah terbukti mampu mendeteksi dan mencegah serangan DDoS dengan tingkat akurasi yang tinggi, bahkan ketika serangan tersebut memiliki karakteristik yang serupa. Pentingnya penerapan teknologi *deep* learning dalam mendeteksi serangan *Distributed Denial of Service* (DDoS) pada jaringan *Internet of Things* (IoT)

semakin menjadi fokus perhatian. Kelebihan metode *deep learning* dibandingkan teknik konvensional terletak pada kemampuannya untuk belajar dari data yang tidak berlabel, mengidentifikasi serangan berkecepatan rendah, dan *deep learning* juga dapat digunakan untuk mendeteksi serangan yang sebelumnya belum pernah terjadi atau belum dikenal yang seringkali sulit dideteksi oleh model berbasis aturan dan metode konvensional lainnya. Dalam penelitian [4] yang disusun secara sistematis ditemukan bahwa *deep learning* mampu mengatasi masalah deteksi serangan DDoS dengan akurasi yang lebih tinggi bahkan ketika data yang tersedia terbatas atau tidak terstruktur sepenuhnya. Beberapa model *deep learning* seperti *Convolutional Neural Network* (CNN) telah digunakan untuk mendeteksi serangan DDoS secara *real-time* dan menunjukkan kinerja yang baik dalan mengidentifikasi pola data dari paket jaringan.

Penelitian [5] menjelaskan bahwa *Convolutional Neural Network* (CNN) telah terbukti efektif dalam mendeteksi serangan *Distributed Denial of Service* (DDoS) yang memiliki kemampuan untuk mengenali pola kompleks dalam data jaringan yang seringkali menjadi ciri khas dari serangan DDoS. Kinerja CNN yang menghasilkan akurasi yang tinggi ini didukung oleh proses pembelajaran yang melibatkan banyak lapisan *convolution* dan *pooling*, yang membantu dalam mengekstraksi fitur-fitur penting dari data lalu lintas jaringan. Kemampuan ini membuat CNN sangat cocok untuk aplikasi deteksi DDoS secara *real-time*, karena dapat secara cepat dan akurat membedakan antara lalu lintas yang sah dan yang berpotensi sebagai ancaman. Implementasi CNN dalam sistem deteksi DDoS dapat membantu mengurangi dampak serangan terhadap infrastruktur penting.

Pada penelitian [6] mengembangkan *Intrusion Detection System* (IDS) yang kuat untuk mendeteksi dan mengklasifikasi *Distributed Denial of Service* (DDoS) menggunakan model CNN yang mencapai akurasi sebesar 96,82%. Pada penelitian [7] memilih CNN untuk perbandingan dan membedakan antara terdapat serangan dan tidak dengan akurasi mencapai 95%. Pada penelitian [8] CNN mampu belajar pola secara otomatis dari data besar, CNN digunakan untuk mendeteksi serangan jaringan dengan analisis lalu lintas jaringan dan klasifikasi serangan *cyber* dengan akurasi

sebesar 84,70%. Pada penelitian [9] CNN-LSTM menghasilkan kinerja terbaik dengan akurasi 95% membuktikan efektivitas IDS yang diusulkan dalam membedakan lalu lintas jaringan yang berbahaya dan yang tidak berbahaya. Pada penelitian [10] menggunakan berbagai metode regularisasi pada tiga model CNN (tanpa regularisasi, L1, dan L2) untuk membantu menghindari *overfitting* dan meningkatkan kemampuan deteksi serangan dengan akurasi mendekati 91%.

Berdasarkan penjelasan di atas, penulis memilih menggunakan metode *Convolutional Neural Network* (CNN) dalam penelitian yang berjudul "Deteksi Serangan *Distributed Denial of Service* (DDoS) pada Sistem *Smarthome* menggunakan Metode *Convolutional Neural Network* (CNN)" karena CNN memiliki kemampuan unggul dalam mengenali pola kompleks pada data jaringan, menghasilkan akurasi tinggi, serta mampu mendeteksi serangan DDoS secara *real-time*. Kemampuan ini menjadikan CNN lebih efektif dalam mendeteksi serangan yang bervariasi pada sistem *Smarthome*, sehingga meningkatkan keamanan dan respons terhadap ancaman *cyber*.

1.2 Rumusan masalah

Dari latar belakang yang telah dijelaskan, rumusan masalah dalam penelitian ini sebagai berikut.

1. Bagaimana proses ekstraksi data dilakukan untuk mendeteksi serangan *Distributed Denial of Service* (DDoS) pada perangkat *Smarthome*?
2. Bagaimana metode *Convolutional Neural Network* (CNN) mampu mendeteksi serangan *Distributed Denial of Service* (DDoS) pada perangkat *Smarthome*?
3. Bagaimana cara mengukur performa *Convolutional Neural Network* (CNN) terhadap nilai metrik evaluasi?

1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini yaitu sebagai berikut.

1. Dataset yang digunakan berasal dari COMNETS.

2. Penelitian ini hanya berfokus pada serangan *Distributed Denial of Service* (DDoS) yang terjadi pada perangkat smarthome dalam lingkungan *Internet of Things (*IoT).
3. Algoritma *Convolutional Neural Network* (CNN) digunakan pada penelitian ini untuk mendeteksi serangan.

1.4 Tujuan

Berdasarkan rumusan masalah yang ada, tujuan dari penelitian ini adalah sebagai berikut.

1. Proses mengekstraksi data dilakukan dengan cara mengubah data *pcap* menjadi *csv* menggunakan *CICFlowmeter* untuk mendeteksi serangan *Distributed Denial of Service* (DDoS) pada perangkat *Smarthome*.
2. Menggunakan *Convolutional Neural Network* (CNN) untuk mendeteksi serangan *Distributed Denial of Service* (DDoS) pada perangkat *Smarthome* melalui proses *Preprocessing* seperti *Label Encoder, Feature Selection*, Normalisasi Data, *Reshaphing* Data, *Split* Data hingga permodelan.
3. Mengetahui dan mengevaluasi performa *Convolutional Neural Network* (CNN) terhadap nilai metrik evaluasi seperti Akurasi, Presisi, *Recall*, dan *F1-Score*.

1.5 Manfaat

Adapun manfaat dari penelitian ini yaitu sebagai berikut.

1. Dapat mengoptimalkan proses ekstraksi data sehingga deteksi serangan *Distributed Denial of Service* (DDoS) pada perangkat *Smarthome* lebih cepat dan efisien.
2. Dengan menggunakan metode *Convolutional Neural Network* (CNN) dapat mendeteksi serangan *Distributed Denial of Service* (DDoS) pada perangkat *Smarthome*.
3. Membantu dalam mengevaluasi hasil deteksi serangan *Distributed Denial of Service* (DDoS) pada perangkat *Smarthome* dengan menggunakan berbagai metrik evaluasi, seperti akurasi, presisi, dan *recall*, sehingga dapat menentukan efektivitas metode *Convolutional Neural Network* (CNN).

1.6 Metodologi Penelitian

Adapun penerapan metodologi yang digunakan pada penelitian yang berjudul "Deteksi *Distributed Denial of Service* (DDoS) pada perangkat *Smarthome* dengan Menggunakan Metode *Convolutional Neural Network* (CNN)" yaitu sebagai berikut.

1. Studi Literatur

   Penulis melakukan kajian literatur untuk menggali informasi dari berbagai sumber yang relevan seperti jurnal ilmiah, buku, artikel daring. Studi ini difokuskan pan literatur yang berkaitan dengan serangan *Distributed Denial of Service* (DDoS), teknik *deep learning*, serta penggunaan *Convolutional Neural Network* (CNN) dalam mendeteksi serangan pada jaringan, khususnya di lingkungan *Internet of Things* (IoT).

2. Metode Konsultasi

   Penulis melakukan konsultasi dengan ahli di bidang keamanan jaringan, deep learning, dan IoT. Konsultasi dilakukan untuk mendapatkan wawasan mendalam mengenai masalah yang dibahas dalam penelitian ini, serta untuk memvalidasi metode yang digunakan dalam penelitian ini.

3. Metode Pengolahan Data

   Pada tahap ini, penulis mengumpulkan dataset yang berkaitan dengan serangan DDoS dan kemudian diolah dengan beberapa langkah *preprocessing* seperti konversi data, pemilihan fitur, dan normalisasi data.

4. Pengembangan Model dan Pengujian Data

   Pada tahap ini, penulis mengembangkan model *Convolutional Neural Network* (CNN) berdasarkan dataset yang telah diproses sebelumnya, kemudian melatih model menggunakan dataset pelatihan. Setelah pelatihan, model diuji dengan dataset pengujian untuk mengevaluasi akurasi dan efektivitasnya dalam mendeteksi serangan *Distributed Denial of Service* (DDoS).

5. Analisis dan Kesimpulan

Tahap terakhir adalah melakukan analisis hasil pengujian mengenai efektivitas *Convolutional Neural Network* (CNN) dalam mendeteksi serangan *Distributed Denial of Service* (DDoS) pada perangkat *Smarthome*.

1.7 Sistematika Penulisan

Adapun sistematika penulisan tugas akhir ini yaitu sebagai berikut.

BAB I PENDAHULUAN

BAB I Menjelaskan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat penelitian, metodologi yang digunakan dalam penelitian ini, dan sistematika penulisan tugas akhir ini.

BAB II TINJAUAN PUSTAKA

BAB II berisi tinjauan literatur yang mencakup penelitian sebelumnya dan teori yang relevan unruk mendukung penelitian ini seperti penjelasan mengenai *Smarthome*, *Distributed Denial of Service* (DDoS), *Deep Learning*, dan *Convolutional Neural Network* (CNN).

BAB III METODOLOGI PENELITIAN

BAB III menjelaskan desain penelitian, kerangka kerja, teknik pengumpulan data, dan proses penerapan metode *Convolutional Neural Network* (CNN) untuk mendeteksi serangan DDoS pada perangkat *Smarthome*.

BAB IV HASIL DAN ANALISA

BAB IV membahas hasil Penelitian, termasuk analisis efektivitas metode *Convolutional Neural Network* (CNN) 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 menyajikan kesimpulan dari penelitian ini dan memberikan saran kepada peneliti selanjutnya untuk fokus pada peningkatan deteksi serangan *Distributed Denial of Service* (DDoS) dan pengembangan teknik keamanan jaringan *Smarthome* yang lebih efektif.

DAFTAR PUSTAKA

[1] J. Wang, Y. Liu, W. Su, and H. Feng, "A DDoS attack detection based on deep learning in software-defined Internet of things," *IEEE Veh. Technol. Conf.*, vol. 2020-Novem, 2020, doi: 10.1109/VTC2020-Fall49728.2020.9348652.

[2] L. Huraj, T. Horak, P. Strelec, and P. Tanuska, "Mitigation against ddos attacks on an iot-based production line using machine learning," *Appl. Sci.*, vol. 11, no. 4, pp. 1–18, 2021, doi: 10.3390/app11041847.

[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] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," *Soft Comput.*, vol. 27, no. 18, pp. 13039–13075, 2023, doi: 10.1007/s00500-021-06608-1.

[5] R. Widodo, M. Delimayanti, and A. Wulandari, "DDoS Attacks Detection With Deep Learning Approach Using Convolutional Neural Network," *J. Appl. Informatics Comput.*, vol. 8, no. 2, pp. 235–240, 2024, [Online]. Available: https://jurnal.polibatam.ac.id/index.php/JAIC/article/view/8242

[6] A. A. Najar and M. N. S., "A Robust DDoS Intrusion Detection System Using Convolutional Neural Network," *Comput. Electr. Eng.*, vol. 117, no. May, p. 109277, 2024, doi: 10.1016/j.compeleceng.2024.109277.

[7] R. Ma, S. Yin, X. Feng, H. Zhu, and V. S. Sheng, "A lightweight deep learning-based android malware detection framework," *Expert Syst. Appl.*, vol. 255, no. PB, p. 124633, 2024, doi: 10.1016/j.eswa.2024.124633.

[8] K. Li, W. Ma, H. Duan, H. Xie, and J. ZHU, "Few-shot IoT attack detection based on RFP-CNN and adversarial unsupervised domain-adaptive

regularization," *Comput. Secur.*, vol. 121, p. 102856, 2022, doi: 10.1016/j.cose.2022.102856.

[9] 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, no. June 2024, p. 104146, 2025, doi: 10.1016/j.cose.2024.104146.

[10] B. I. Hairab, M. Said Elsayed, A. D. Jurcut, and M. A. Azer, "Anomaly Detection Based on CNN and Regularization Techniques Against Zero-Day Attacks in IoT Networks," *IEEE Access*, vol. 10, no. August, pp. 98427–98440, 2022, doi: 10.1109/ACCESS.2022.3206367.

[11] S. N. Swamy and S. R. Kota, "An empirical study on system level aspects of Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 188082–188134, 2020, doi: 10.1109/ACCESS.2020.3029847.

[12] Y. Al Mtawa, H. Singh, A. Haque, and A. Refaey, "Smart Home Networks: Security Perspective and ML-based DDoS Detection," *Can. Conf. Electr. Comput. Eng.*, vol. 2020-August, 2020, doi: 10.1109/CCECE47787.2020.9255756.

[13] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[14] M. Sadaf, Z. Iqbal, Z. Anwar, U. Noor, M. Imran, and T. R. Gadekallu, "A novel framework for detection and prevention of denial of service attacks on autonomous vehicles using fuzzy logic," *Veh. Commun.*, vol. 46, no. September 2023, p. 100741, 2024, doi: 10.1016/j.vehcom.2024.100741.

[15] A. Fathima, G. S. Devi, and M. Faizaanuddin, "Improving distributed denial of service attack detection using supervised machine learning," *Meas. Sensors*, vol. 30, no. September, p. 100911, 2023, doi: 10.1016/j.measen.2023.100911.

[16] G. Chen, “Jo u of,” *Intell. Geoengin.*, 2024, doi: 10.1016/j.ige.2024.10.001.

[17] L. E. Chuquimarca, B. X. Vintimilla, and S. A. Velastin, “A review of external quality inspection for fruit grading using CNN models,” *Artif. Intell. Agric.*, vol. 14, pp. 1–20, 2024, doi: 10.1016/j.aiia.2024.10.002.

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