DETEKSI SERANGAN *DISTRIBUTED DENIAL OF SERVICE (DDOS)* PADA PERANGKAT *SMARTHOME* MENGGUNAKAN METODE *LONG SHORT - TERM MEMORY (LSTM)*

SKRIPSI

Oleh :

Makiyah

09011282126093

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA PERANGKAT SMARTHOME MENGGUNAKAN METODE LONG SHORT - TERM MEMORY (LSTM)

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

MAKIYAH

09011282126093

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 SMARTHOME DEVICES USING LONG SHORT-TERM MEMORY (LSTM) METHOD

Submitted in Partial Fulfillment of Requirements for the

Degree of Bachelor of Computer Science

By:

MAKIYAH

09011282126093

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 : Aditya Putra Perdana Prasetyo, S.Kom., 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 : Makiyah

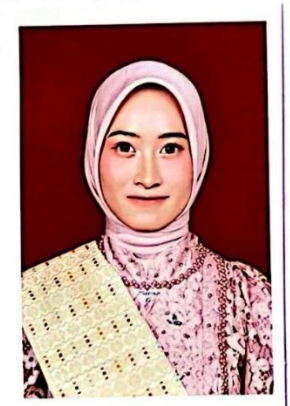
NIM : 09011282126093

Judul : Deteksi Serangan *Distributed Denial of Service (DDoS)* Pada Perangkat *Smarthome* Menggunakan Metode *Long Short-Term Memory (LSTM)*

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

Makiyah

NIM. 09011282126093

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh. Puji dan Syukur selalu penulis panjatkan atas kehadirat Allah SWT yang telah memberikan semua nikmat, rahmat dan karunia-Nya terutama nikmat kesehatan sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul "**Deteksi Serangan *Distributed Denial of Service (DDoS)* Pada Perangkat *Smarthome* Menggunakan Metode *Long Short-Term Memory (LSTM)"*** ini dengan baik. Shalawat serta salam yang selalu tercurah kepada Nabi agung kita Nabi Muhammad SAW yang telah membawa kita dari zaman kegelapan sampai ke zaman terang benderang seperti saat ini yang menjadi suri tauladan bagi umatnya. Ditengah berbagai hambatan dan tantangan dalam membuat tugas akhir ini, penulis pun telah menempuh perjalanan akademik yang menjadi salah satu hal yang sangat penting bagi penulis.

Penelitian ini dilatarbelakangi oleh semakin meluasnya penggunaan perangkat *smarthome* yang terhubung ke jaringan internet, yang membuat mereka rentan terhadap berbagai jenis serangan siber, terutama serangan DDoS yang dapat menghambat seluruh sistem. Ancaman DDoS telah menjadi masalah besar dalam lingkungan *Internet of Things (IoT),* dan kebutuhan akan sistem deteksi yang efisien dan responsive semakin mendesak. Melalui penelitian ini, penulis menggunakan pendekatan pembelajaran mendalam melalui metode LSTM yang mampu mengidentifikasi anomaly secara efektif.

Penulisan tugas akhir ini diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Sistem Komputer, Universitas Sriwijaya. Penulis menyadari sepenuhnya bahwa penyelesaian skripsi ini tidak terlepas dari bimbingan, dukungan, motivasi dan bantuan dari berbagai pihak, baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan yang berharga ini, dengan penuh kerendahan hati, penulis ingin menyampaikan ucapan terima kasih dan penghargaan yang sebesar besarnya penulis berikan untuk :

1. Allah SWT yang selalu melimpahkan rahmat dan karunia-Nya, terutama nikmat kesehatan kepada penulis.
2. Ibu Suryani, Bapak Musadek, sebagai kedua orang tua tercinta penulis yang dengan setulus hati memberikan dukungan moral, spiritual dan material serta do'a, support, motivasi dan selalu mengusahakan yang terbaik, serta menjadi

orang yang selalu ada baik dalam keadaan apapun dalam hidup penulis. Skripsi ini penulis persembahkan khusus untuk mereka sebagai bukti terima kasih atas segala pengorbanan yang telah diberikan.

3. Saudara saudara penulis, Kakak Tami, Septi dan Amrul yang selalu memberikan semangat dan menjadi inspirasi bagi penulis untuk terus berjuang menyelesaikan studi.
4. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D., IPU., ASEAN-Eng. selaku Dosen Pembimbing I Tugas Akhir dan juga Dosen Pembimbing Akademik.
7. Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing II Tugas Akhir.
8. Bapak Huda Ubaya, S.T., M.T. selaku Dosen Pembimbing Akademik.
9. Bapak Angga selaku admin Jurusan Sistem Komputer.
10. Bapak dan Ibu dosen Jurusan Sistem Komputer.
11. Pemilik NIM 09011282126069 Aldi Hoirul Fatih selaku teman terdekat penulis selama hampir 3 (tiga) tahun ini, yang selalu ada memberikan support, motivasi, dukungan dan selalu menemani penulis, serta selalu membantu penulis dalam hal apapun selama ini.
12. Hepra, Tyas, Tisa, Choi, Rafi dan Zaidan selaku teman dekat dalam MISI dan DATEDATE yang selalu ada bagi penulis dan teman sebimbingan dengan penulis.
13. Erina Aulia Putri dan Aisyah Hillal selaku sepupu penulis yang selalu memberikan dukungan dan mendengarkan keluh kesah penulis.
14. Yuli, Pau, Sintia, Rini, dan Utari selaku teman dekat penulis dari SMP yang selalu memberikan support bagi penulis.
15. Wisuda grup yang selaku teman SMA penulis.
16. Siti Nurhaliza selaku teman dari kecil penulis.
17. Kakak kakak Tingkat SK Regular dan SK Unggulan termasuk tim riset COMNETS.

18. Teman teman seperjuangan Jurusan Sistem Komputer Angkatan 2021, khususnya kelas C.
19. Seluruh Pihak yang membantu dalam menyelesaikan laporan ini yang tidak bisa disebutkan satu persatu.
20. Yung Kai karena telah menciptakan lagu Blue yang selalu menemani penulis dalam mengerjakan laporan tugas akhir ini.
21. Almamater.

Penulis menyadari sepenuhnya bahwa tugas akhir ini masih jauh dari kesempurnaan dan masih terdapat banyak kekurangan yang disebabkan oleh keterbatasan pengetahuan dan pengalaman penulis. Oleh karena itu, dengan segala kerendahan hati, penulis sangat mengharapkan kritik dan saran yang konstruktif dari berbagai pihak untuk penyempurnaan tugas akhir ini dan pengembangan penelitian selanjutnya di bidang yang sama.

Akhir kata, penulis berharap semoga tugas akhir ini dapat memberikan manfaat yang sebesar besarnya bagi perkembangan ilmu pengetahuan, khususnya dalam bidang keamanan siber dan perangkat IoT, serta dapat menjadi referensi berharga bagi penelian selanjutnya yang memiliki topik serupa. Semoga Tuhan Yang Maha Esa senantiasa melimpahkan rahmat dan hidayah-Nya kepada kita semua.

Palembang, 26 Februari 2025
Penulis

Makiyah
NIM. 09011282126093

DETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA PERANGKAT SMARTHOME MENGGUNAKAN METODE LONG SHORT - TERM MEMORY (LSTM)

Makiyah (09011282126093)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: 09011282126093@student.unsri.ac.id

ABSTRAK

Internet of Things (IoT) telah menghadirkan kemudahan dalam kehidupan sehari-hari, salah satunya melalui implementasi perangkat *smarthome*. Namun, keterhubungan perangkat tersebut juga menimbulkan kerentanan terhadap serangan siber, khususnya serangan *Distributed Denial of Service (DDoS)* yang dapat mengganggu layanan secara signifikan. Penelitian ini bertujuan untuk mendeteksi serangan DDoS pada perangkat *smarthome* menggunakan metode *Long Short-Term Memory* (LSTM), yang dikenal efektif dalam memproses data berurutan. Dataset yang digunakan berasal dari *COMNETS Smarthome* dengan data awal berformat .pcap yang diekstrak menggunakan *CICFlowMeter* menjadi format .csv. Proses pelatihan model dilakukan melalui beberapa tahap, yaitu: *data cleaning*, *feature selection*, *label encoding*, normalisasi, dan pembagian data (*train*, *validation*, *test*). Hasil evaluasi menunjukkan bahwa model LSTM mampu mendeteksi serangan DDoS dengan tingkat akurasi tertinggi sebesar 99.73%, *precision* 99.54%, *recall* 100%, dan *F1-score* 99.77% pada skala pembagian data 80:10:10. Dengan demikian, model LSTM terbukti efektif dalam mendeteksi serangan DDoS pada perangkat smarthome dan memiliki potensi untuk diterapkan sebagai sistem deteksi dini pada jaringan IoT.

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

DETECTION OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS ON SMARTHOME DEVICES USING THE LONG SHORT-TERM MEMORY (LSTM) METHOD

Makiyah (09011282126093)

Department of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email: 09011282126093@student.unsri.ac.id

ABSTRACT

The Internet of Things (IoT) has brought convenience to everyday life, particularly through the implementation of smarthome devices. However, the connectivity of these devices also increases their vulnerability to cyber threats, especially Distributed Denial of Service (DDoS) attacks, which can severely disrupt system operations. This study aims to detect DDoS attacks on smarthome devices using the Long Short-Term Memory (LSTM) method, known for its effectiveness in handling sequential data. The dataset used is derived from COMNETS Smarthome, initially in .pcap format and later extracted to .csv using CICFlowMeter. The training process includes several stages: data cleaning, feature selection, label encoding, normalization, and data splitting (training, validation, testing). Evaluation results show that the LSTM model can detect DDoS attacks with a peak accuracy of 99.73%, precision of 99.54%, recall of 100%, and F1-score of 99.77% using an 80:10:10 data split ratio. Therefore, the LSTM model is proven to be effective for DDoS attack detection on smarthome devices and has strong potential to be implemented as an early warning system in IoT networks.

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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar belakang

Internet of Things (IoT) [1] merupakan konsep jaringan yang terdiri dari entitas fisik yang tertanam dengan komponen elektronik, perangkat lunak, dan sensor. IoT berperan sebagai pembawa informasi[2]dan jaringan telekomunikasi, serta ditandai dengan kompleksitas dan keterbukaan yang kuat. Revolusi *Internet of Things (IoT)* sangat berpengaruh dalam kehidupan sehari-hari[3] serta IoT memungkinkan sejumlah besar perangkat pintar[4][5] untuk berkomunikasi secara langsung, berbagi, dan mengirim data dengan perangkat, orang, dan sistem lain. IoT terdiri dari sejumlah besar perangkat pintar dengan teknologi yang berbeda-beda, serta dengan kemampuan komputasi dan transmisi dan gigunakan dalam scenario aplikasi pintar.

Smarthome atau rumah pintar merupakan aplikasi penting dalam IoT *(Internet of Things)* [6] yang digunakan untuk memantau dan mengontrol rumah. Karena dampak signifikan yang menghasilkan perangkat dan data yang besar, maka dapat memicu masalah[5] yaitu sistem rumah pintar ini sangat rentan terhadap risiko keamanan[7] dan akivitas yang dapat mempengaruhi sistem kerjanya. serangan yang mungkin terjadi adalah serangan *Distributed Denial of Service* (DDoS).

Serangan *Distributed Denial of Service (DDoS)* [8] merupakan ancaman dalam keamanan *cyber* yang dapat terjadi secara umum dengan cara penyerang membanjiri perangkat online yang sudah ditargetkan. Serangan DDoS bertujuan menghalangi layanan yang sah dengan [9] menghabiskan jaringan target dengan permintaan yang berbahaya, serta mengganggu layanan online dengan pemakaian sumber daya yang besar. Untuk mendeteksi serangan tersebut dapat dilakukan analisis secara dinamis, di mana pada analisis ini dapat diketahui secara spesifik lalu lintas jaringan dan dapat menganalisis anomaly [8] yang berindikasi serangan, selain itu, analisis secara dinamis juga dilakukan agar dapat mengetahui adanya aktivitas mencurigakan serta dapat membedakan antara lalu lintas jaringan yang normal dan yang terkena serangan yang berbahaya.

Serangan DDoS ini sangat berbahaya dan mengancam arus lalu lintas jaringan pada perangkat *smarthome* yang terserang. Maka, hal tersebut harus diatasi sesegera mungkin. Untuk itu, mendeteksi serangan pada perangkat IoT[4] merupakan hal yang sangat penting untuk meningkatkan efektivitas layanan jaringan.

Pada penelitian [10] yang membahas tentang sistem deteksi botnet di *Internet of things (IoT)* menggunakan *hybrid deep learning.* Dataset yang digunakan ada 2 yaitu N-BAIoT2018 dan UNSW-NB15. Pada dataset N-BAIoT2018, model *Long Short-Term Memory (LSTM)* mampu mengklasifikasikan *true positives* dan menghasilkan akurasi sebesar 94.18% dan presisi sebesar 95.69% pada kelas *binary*. Sedangkan pada dataset UNSW-NB15, model *Long Short-Term Memory (LSTM)* secara akurat mampu mengklasifikasikan *positive and negative cases* dengan akurasi yang mencapai 95.97% dan recall 96.74 serta mampu menyeimbangkan presisi yaitu 94.13%. Namun, pada penelitian ini masih memiliki keterbatasan dalam hal skalabilitas, keamanan pada server, kompleksitas pada saat *training,* kemampuan interpretasi serta ketergantungan terhadap data.

Pada penelitian [11] membahas tentang sistem deteksi intrusi menggunakan metode *deep learning.* Model LSTM digunakan untuk mendeteksi serangan DDoS dengan sub-kelas. Data yang digunakan adalah kumpulan data mentah dari CICIoT2023 yang dilatih dan dievaluasi dalam model *deep learning* menggunakan *TensorFlow* 2.13. Dalam penelitian ini terdapat 5 *sample* yang digunakan dan pada setiap *sample* model LSTM menghasilkan performa yang baik dan menunjukkan kinerja akurasi dan metrik terbaik pada saat jumlah kelas dinaikkan. Pada model 1,2,3,4, dan 5 masing – masing menghasilkan akurasi yaitu 94.96%, 90.85%, 90.83%, 91.22%, dan 91.27%. Namun, pada penelitian ini masih memiliki kekurangan yaitu pengembangan model *deep learning* masih belum optimal dan efisien.

Pada Penelitian [12] yang membahas tentang deteksi serangan siber pada *Internet of Medical Things (IoTM)* menggunakan metode *deep learning* untuk mengidentifikasi dan menghindari ancaman. Ternyata pada penelitian ini Arsitektur LSTM dengan kekuatan optimal Adam mengungguli model lain dan mampu mengidentifikasi secara akurat dan efisien. LSTM menunjukkan kinerja yang luar

biasa yaitu akurasi mencapai 97%, presisi 93%, recall 96%, dan F1 score 94%. Penelitian memiliki kekurangan yaitu masih belum meningkatkan ketahanan sistem *Internet og Medical Things (IoTM).*

Pada penelitian [5] yang membahas tetang deteksi DDoS menggunakan *deep learning.* Dataset yang digunakan adalah dataset CICDDoS2019. model *deep learning* yaitu *Long Short-Term Memory (LSTM)* mendeteksi serangan DDoS mampu menampilkan performa kinerja yang baik dengan akurasi yang mencapai 98.6% dan menjadi model yang efektif. Namun, masih terdapat kekurangan yaitu penelitian hanya mendeteksi satu serangan saja.

Long Short-Term Memory (LSTM) merupakan metode yang efektif dan di beberapa penelitian karena mampu menunjukkan performa yang luar biasa baik . Maka, dalam penelitian ini penulis akan menggunakan metode *Long Short-Term Memory (LSTM)* untuk mendeteksi serangan pada perangkat *smarthome*. Model *deep learning* juga dipilih karena data yang akan digunakan cukup besar jadi model ini dianggap efektif.

Berdasarkan latar belakang tersebut, maka penulis ingin mengusulkan judul penelitian " Deteksi Serangan *Distributed Denial of Service (DDoS)* Pada Perangkat *Smarthome* Menggunakan Metode *Long Short-Term Memory (LSTM)* " dengan harapan model yang digunakan mampu mendeteksi serangan dengan baik dan meningkatkan performa kinerja dari penelitian sebelumnya.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka didapatkan rumusan masalah pada penelitian ini yaitu sebagai berikut.

1. Bagaimana ekstraksi data dilakukan sebelum pelatihan model ?
2. Bagaimana metode *Long Short-Term Memory (LSTM)* mampu mendeteksi serangan *Distributed Denial of Service (DDoS)* pada perangkat *smarthome*?
3. Bagaimana performa dari model *deep learning* terhadap nilai dari metrik evaluasi yang digunakan?

1.3 Batasan Masalah

Penelitian ini akan difokuskan pada masalah yang akan di bahas saja untuk menghindari agar penelitian ini tidak menyimpang dan terlalu luas, maka penulis

menetapkan batasan masalah pada penelitian ini, batasan masalah tersebut adalah sebagai berikut.

1. Dataset yang digunakan adalah dataset COMNETS *SMARTHOME.*
2. Penelitian ini hanya berfokus pada serangan *cyber attack* pada perangkat *smarthome* menggunakan metode *Long Short-Term Memory (LSTM).*
3. Penelitian ini tidak membahas tentang cara mengatasi serangan *cyber attack* pada perangkat *smarthome.*

1.4 Tujuan

Tujuan pada penelitian ini di buat berdasarkan rumusan masalah di atas, tujuannya adalah sebagai berikut.

1. Mengekstraksi data menggunakan tools *CICFlowmeter* sebelum data digunakan untuk pelatihan model.
2. Menggunakan metode *Long Short-Term Memory (LSTM)* untuk mendeteksi serangan *Distributed Denial Of Service (DDoS)* pada perangkat *smarthome.*
3. Menggunakan *confusion matrix* untuk mengukur performa dari model *deep learning.*

1.5 Manfaat

Penelitian ini diharapkan mempunyai manfaat sebagai berikut.

1. Untuk mengolah data mentah menggunakan tools serta untuk membantu analisis mendalam.
2. Untuk membandingkan antara kelas normal dan kelas *DDoS* pada dataset.
3. Untuk mengukur performa optimal dari model *deep learning* yaitu model *Long Short-Term Memory (LSTM)*.

1.6 Metodelogi Penelitian

Ada beberapa metodelogi penelitian yang digunakan penulis untuk penelitian yang berjudul "Deteksi Serangan Pada Perangkat *Smarthome* Menggunakan Algoritma *Long Short-Term Memory (LSTM)* Dengan Pendekatan *Multiclass* " yaitu sebagai berikut.

1. Metode Studi Pustaka dan Literatur

   Pada metode ini penulis melakukan literatur serta mencari informasi untuk dijadikan referensi dari berbagai sumber yang didapat seperti membaca

dan review jurnal, membaca buku yang berkaitan dengan penelitian yang akan dilakukan.

2. Metode Konsultasi

Pada metode ini penulis melakukan konsultasi secara *real time* dan *online* dengan narasumber yang memiliki wawasan dan ilmu pengetahuan yang lebih luas tentang masalah yang akan dibahas pada penelitian ini.

3. Metode Pengolahan Data

Pada metode ini penulis melakukan pengolahan data yaitu data mentah dengan cara mengekstrak fitur dari file data berupa format data *pcap* ke data dengan format *CSV*, setelah itu akan dilakukan pemilihan fitur dengan menyesuaikan serang yang akan diidentifikasi pada penelitian ini.

4. Metode Pengerjaan Model dan Pengujian Data

Pada metode ini penulis akan melakukan tahap selanjutnya setelah pengolahan data yaitu merancang model dengan menggunakan metode *deep learning* yang sudah dipilih untuk penelitian ini.

5. Metode Analisa dan Kesimpulan

Pada metode ini penulis melakukan Analisa serta membuat Kesimpulan dan menyampaikan saran juga rekomendasi untuk penelitian selanjutnya.

1.7 Sistematika Penulisan

Adapun sistematika penulisan dalam penelitian ini adalah sebagai berikut.

BAB I PENDAHULUAN

Pada BAB I menjelaskan tentang latar belakang, rumusan masalah, Batasan masalah, tujuan, manfaat, metodelogi penelitian, serta sistematika penulisan dalam penelitian ini.

BAB II TINJAUAN PUSTAKA

Pada BAB II menjelaskan tentang penelitian sebelumnya dan teori – teori yang berhubungan dengan judul penelitian dan penelitian sebelumnya harus yang berhubungan dengan permasalahan.

BAB III METODELOGI PENELITIAN

Pada BAB III menjelaskan tantang alur penelitian, kerangka kerja penelitian, dan perancangan model yang akan dignakan pada penelitian untuk mendeteksi serangan *cybber attack*.

BAB IV HASIL DAN ANALISA

Pada BAB IV menjelaskan hasil dari penelitian yang dilakukan dan analisa terkait studi yang digunakan.

BAB V KESIMPULAN DAN SARAN

Pada BAB V menjelaskan tantang hasil penelitian berupa pendapat penulis serta saran yang berisi tentang yang harus dilakukan pada penelitian selanjutnya.

DAFTAR PUSTAKA

[1] N. F. Syed, M. Ge, and Z. Baig, "Fog-cloud based intrusion detection system using Recurrent Neural Networks and feature selection for IoT networks," *Comput. Networks*, vol. 225, no. February, 2023, doi: 10.1016/j.comnet.2023.109662.

[2] S. Wang, W. Xu, and Y. Liu, "Res-TranBiLSTM: An intelligent approach for intrusion detection in the Internet of Things," *Comput. Networks*, vol. 235, no. April, p. 109982, 2023, doi: 10.1016/j.comnet.2023.109982.

[3] R. A. Osman, "Internet of Medical Things (IoMT) optimization for healthcare: A deep learning-based interference avoidance model," *Comput. Networks*, vol. 248, no. March, p. 110491, 2024, doi: 10.1016/j.comnet.2024.110491.

[4] P. Malini and D. K. R. Kavitha, "An efficient deep learning mechanisms for IoT/Non-IoT devices classification and attack detection in SDN-enabled smart environment," *Comput. Secur.*, vol. 141, no. June 2023, p. 103818, 2024, doi: 10.1016/j.cose.2024.103818.

[5] 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.

[6] V. Chang, Z. Wang, Q. Xu, L. Golightly, B. Liu, and M. Arami, "Smart Home based on Internet of Things and Ethical Issues," no. Femib, pp. 57–64, 2021, doi: 10.5220/0010178100570064.

[7] A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, "Deep learning for cyber threat detection in IoT networks: A review," *Internet Things Cyber-Physical Syst.*, vol. 4, no. October 2023, pp. 110–128, 2024, doi: 10.1016/j.iotcps.2023.09.003.

[8] R. Abu Bakar, L. De Marinis, F. Cugini, and F. Paolucci, "FTG-Net-E: A hierarchical ensemble graph neural network for DDoS attack detection," *Comput. Networks*, vol. 250, no. December 2023, 2024, doi: 10.1016/j.comnet.2024.110508.

[9] H. Zhou, Y. Zheng, X. Jia, and J. Shu, "Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based

approach with distributed SDN," *Comput. Networks*, vol. 225, no. February, p. 109642, 2023, doi: 10.1016/j.comnet.2023.109642.

[10] S. Ali *et al.*, "A novel approach of botnet detection using hybrid deep learning for enhancing security in IoT networks," *Alexandria Eng. J.*, vol. 103, no. March, pp. 88–97, 2024, doi: 10.1016/j.aej.2024.05.113.

[11] 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, no. April, p. 101336, 2024, doi: 10.1016/j.iot.2024.101336.

[12] K. Vaisakhkrishnan, G. Ashok, P. Mishra, and T. G. Kumar, "Guarding Digital Health: Deep Learning for Attack Detection in Medical IoT," *Procedia Comput. Sci.*, vol. 235, pp. 2498–2507, 2024, doi: 10.1016/j.procs.2024.04.235.

[13] H. Feng *et al.*, "Multi-domain collaborative two-level DDoS detection via hybrid deep learning," *Comput. Networks*, vol. 242, no. February, p. 110251, 2024, doi: 10.1016/j.comnet.2024.110251.

[14] K. A. Dhanya, S. Vajipayajula, K. Srinivasan, A. Tibrewal, T. S. Kumar, and T. G. Kumar, "Detection of Network Attacks using Machine Learning and Deep Learning Models," *Procedia Comput. Sci.*, vol. 218, pp. 57–66, 2023, doi: 10.1016/j.procs.2022.12.401.

[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] Ö. KASIM, "An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks," *Comput. Networks*, vol. 180, no. June, 2020, doi: 10.1016/j.comnet.2020.107390.

[17] H. Zhou, Y. Zheng, X. Jia, and J. Shu, "Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN," *Comput. Networks*, vol. 225, no. January, p. 109642, 2023, doi: 10.1016/j.comnet.2023.109642.

[18] S. Hosseini and M. Azizi, "The hybrid technique for DDoS detection with supervised learning algorithms," *Comput. Networks*, vol. 158, pp. 35–45,

2019, doi: 10.1016/j.comnet.2019.04.027.

[19] M. A. Almaiah, R. Alrawashdeh, T. Alkhdour, R. Al-Ali, G. Rjoub, and T. Aldahyani, “Detecting DDoS attacks using machine learning algorithms and feature selection methods,” *Int. J. Data Netw. Sci.*, vol. 8, no. 4, pp. 2307–2318, 2024, doi: 10.5267/j.ijdns.2024.6.001.

[20] R. K. Batchu and H. Seetha, “A generalized machine learning model for DDoS attacks detection using hybrid feature selection and hyperparameter tuning,” *Comput. Networks*, vol. 200, no. June, p. 108498, 2021, doi: 10.1016/j.comnet.2021.108498.

[21] M. H. Aysa, A. A. Ibrahim, and A. H. Mohammed, “IoT Ddos Attack Detection Using Machine Learning,” *4th Int. Symp. Multidiscip. Stud. Innov. Technol. ISMSIT 2020 - Proc.*, no. Layer 1, 2020, doi: 10.1109/ISMSIT50672.2020.9254703.

[22] by Yahya Sulaiman Al-hadhrami and F. Khadeer Hussain, “Intelligent Machine Learning Architecture for Detecting DDoS attacks in IoT networks,” 2020.

[23] D. Vakalis, R. T. Hellwig, M. Schweiker, and S. Gauthier, “Challenges and opportunities of Internet-of-Things in occupant-centric building operations: towards a life cycle assessment framework,” *Curr. Opin. Environ. Sustain.*, vol. 65, no. July 2022, p. 101383, 2023, doi: 10.1016/j.cosust.2023.101383.

[24] W. Choi, J. Kim, S. E. Lee, and E. Park, “Smart home and internet of things: A bibliometic study,” *J. Clean. Prod.*, vol. 301, p. 126908, 2021, doi: 10.1016/j.jclepro.2021.126908.

[25] A. Bajpai, D. Chaurasia, and N. Tiwari, “A novel methodology for anomaly detection in smart home networks via Fractional Stochastic Gradient Descent,” *Comput. Electr. Eng.*, vol. 119, no. PB, p. 109604, 2024, doi: 10.1016/j.compeleceng.2024.109604.

[26] A. Aljuhani, “Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments,” *IEEE Access*, vol. 9, pp. 42236–42264, 2021, doi: 10.1109/ACCESS.2021.3062909.

[27] I. G. A. Poornima and B. Paramasivan, “Anomaly detection in wireless

sensor network using machine learning algorithm," *Comput. Commun.*, vol. 151, no. December 2019, pp. 331–337, 2020, doi: 10.1016/j.comcom.2020.01.005.

[28] N. Bhavatarini, S. Muzamil Basha, and A. Thouheed Ahmed, *Practical Approach*, no. September. 2022. doi: 10.1007/978-81-322-0720-7_2.

[29] D. Adhikari, W. Jiang, J. Zhan, D. B. Rawat, and A. Bhattarai, "Recent advances in anomaly detection in Internet of Things: Status, challenges, and perspectives," *Comput. Sci. Rev.*, vol. 54, no. May 2021, p. 100665, 2024, doi: 10.1016/j.cosrev.2024.100665.

[30] N. Sharma, R. Sharma, and N. Jindal, "Machine Learning and Deep Learning Applications-A Vision," *Glob. Transitions Proc.*, vol. 2, no. 1, pp. 24–28, 2021, doi: 10.1016/j.gltp.2021.01.004.

[31] P. Fergus and C. Chalmers, *Performance Evaluation Metrics*. 2022. doi: 10.1007/978-3-031-04420-5_5.

[32] H. Okut, "Deep Learning for Subtyping and Prediction of Diseases: Long-Short Term Memory," *Www.Intechopen.Com*, no. September, pp. 0–12, 2022.

[33] A. Khan, M. M. Fouda, D. T. Do, A. Almaleh, and A. U. Rahman, "Short-Term Traffic Prediction Using Deep Learning Long Short-Term Memory: Taxonomy, Applications, Challenges, and Future Trends," *IEEE Access*, vol. 11, no. October, pp. 94371–94391, 2023, doi: 10.1109/ACCESS.2023.3309601.

[34] M. Hayaeian Shirvan, M. H. Moattar, and M. Hosseinzadeh, "Deep generative approaches for oversampling in imbalanced data classification problems: A comprehensive review and comparative analysis," *Appl. Soft Comput.*, vol. 170, no. March 2024, p. 112677, 2025, doi: 10.1016/j.asoc.2024.112677.

[35] B. Kolukisa, V. C. Yildirim, B. Elmas, C. Ayyildiz, and V. C. Gungor, "Deep learning approaches for vehicle type classification with 3-D magnetic sensor," *Comput. Networks*, vol. 217, no. July, p. 109326, 2022, doi: 10.1016/j.comnet.2022.109326.