DETEKSI SERANGAN DDOS PADA SISTEM *SMARTHOME* DENGAN METODE *DEEP LEARNING*

SKRIPSI

Oleh:

ALDI HOIRUL FATIH

09011282126069

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

LEMBAR PENGESAHAN

SKRIPSI

DETEKSI SERANGAN DDOS PADA SISTEM SMARTHOME DENGAN METODE DEEP LEARNING

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

Oleh:

ALDI HOIRUL FATIH

09011282126069

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 DDOS ATTACKS ON SMART HOME SYSTEMS USING DEEP LEARNING METHOD

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

By:

ALDI HOIRUL FATIH

09011282126069

Supervisor 1	**: Prof. Ir. Deris Stiawan, M.T., Ph.D.**
	NIP. 197806172006041002
Co - Supervisor 2	**: 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 : 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, 20/6/25

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Aldi Hoirul Fatih

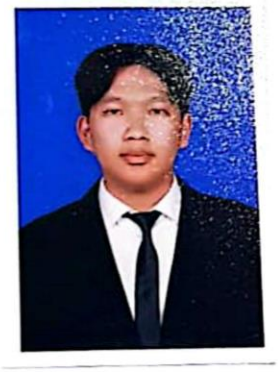
NIM : 09011282126069

Judul : Deteksi Serangan DDoS Pada Sistem *Smarthome* Dengan Metode *Deep Learning*

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, Juni 2025

Yang Menyatakan

Aldi Hoirul Fatih

NIM. 09011282126069

KATA PENGANTAR

Segala Puji dan syukur atas kehadiran Allah Subhanahu wa Ta'ala, karena berkat Rahmat dan Karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini yang berjudul "Deteksi Serangan DDoS Pada Sistem *Smarthome* Dengan Metode *Deep Learning*". Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad Shallallahu 'Alaihi Wasallam yang telah membawa kedamaian dan rahmat untuk keluarga, sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Tujuan dari penulisan Tugas Akhir ini adalah untuk melengkapi salah satu syarat memperoleh gelar sarjana komputer di jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis Dalam kesempatan ini penulis mengucapkan terima kasih kepada pihak yang telah memberikan bantuan serta motivasi sehingga penulis dapat menyelesaikan penulisan Tugas Akhir ini:

1. Allah Subhanahu wa Ta'ala, yang telah melimpahkan Berkat dan Rahmatnya kepada penulis.
2. Ibu, Mama, Ayah, Papa, Kakak, dan Adik penulis tercinta serta seluruh keluarga besar yang telah banyak memberikan do'a, nasihat, 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. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya
5. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D., IPU., ASEAN-Eng. selaku Dosen Pembimbing I Tugas Akhir.
6. Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing II Tugas Akhir.
7. Bapak Abdurahman, S. KOM., M. HAN. selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer.
8. Bapak Angga selaku admin Jurusan Sistem Komputer.
9. Bapak, Ibu dosen jurusan Sistem Komputer yang telah memberikan ilmunya serta pengalamannya kepada penulis.

10. Makiyah selaku *support system* penulis yang selalu menemani, meluangkan waktu, tenaga, pikiran ataupun materi kepada penulis, dan memberi semangat kepada penulis setiap saat.
11. Dean, Farrel, Guntur, Panggih, Dimas, dan SPTNK 2021 yang selalu ada disaat suka dan duka.
12. Rafi, Zaidan, Choi, Tyas, Tisa, dan Hepra selaku teman dekat yang menemani proses pengerjaan skripsi.
13. Skill Issue selaku sahabat seperjuangan yang selalu ada saat susah maupun senang.
14. Kakak - Kakak tingkat SK Unggulan dan SK Reguler yang termasuk tim riset COMNETS.
15. Teman teman seperjuangan Jurusan Sistem Komputer Angkatan 2021 terkhusus kelas A.
16. Seluruh pihak yang membantu dalam menyelesaikan laporan ini yang tidak bisa disebutkan satu persatu.
17. Almamater.

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 Tugas Akhir ini. Penulis juga berharap agar Tugas Akhir ini dapat bermanfaat dan berguna bagi siapa saja yang membacanya.

Palembang, June 2025

Penulis,

Aldi Hoirul Fatih

NIM. 09011282126069

DETEKSI SERANGAN DDOS PADA SISTEM SMARTHOME DENGAN METODE DEEP LEARNING

Aldi Hoirul Fatih (09011282126069)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: aldi.hoirul.fatih@gmail.com

ABSTRAK

Perkembangan *Internet of Things* (IoT) memungkinkan perangkat fisik seperti kamera, pintu rumah, tv, lampu dan peralatan rumah tangga lainnya yang terhubung ke internet untuk membentuk sistem *Smart Home* yang cerdas dan nyaman. Namun, konektivitas antar perangkat yang heterogen ini juga meningkatkan kerentanan terhadap serangan siber, khususnya *Distributed Denial of Service* (DDoS). Pada penelitian ini digunakan metode *Deep Learning*, khususnya *Deep Neural Network* (DNN) dan *Autoencoder* (AE) untuk mendeteksi serangan DDoS dalam dataset. Tools seperti *IDS Snort* juga digunakan pada penelitian ini untuk mengetahui serangan pada DDoS dan *CICFlowMeter* berperan sebagai ekstraksi data dari format *pcap* menjadi *csv*. Hasil dari penelitian tersebut menunjukan bahwa metode *Autoencoder* berhasil mengekstraksi fitur ataupun menreduksi dimensi dengan performa terbaik menggunakan perbandingan 80% *training* dan 20% *testing* dengan hasil *training loss* 0.0052 dan *validation loss* 0.0054 dan diklasifikasi oleh *Deep Neural Network* dengan *epoch* 250 berhasil menghasilkan evaluasi sebesar *accuracy* 99,53%, *precision* 99,53%, *recall* 99,53%, dan *f1-score* 99,53%.

Kata Kunci: Internet of Things, Smart home, Distributed Denial of Service, Snort, CICFlowMeter, Deep Learning, Deep Neural Network, Autoencoder.

DETECTION OF DDOS ATTACKS ON SMART HOME SYSTEMS USING DEEP LEARNING METHOD

Aldi Hoirul Fatih (09011282126069)

Department of Computer Systems, Faculty of Computer Science

Sriwijaya University

Email: aldi.hoirul.fatih@gmail.com

ABSTRACT

The advancement of the Internet of Things (IoT) enables physical devices such as cameras, home doors, televisions, lights, and other household appliances to connect to the internet, forming an intelligent and convenient Smart Home system. However, the connectivity among these heterogeneous devices also increases vulnerability to cyberattacks, particularly Distributed Denial of Service (DDoS) attacks. In this study, Deep Learning methods, specifically Deep Neural Networks (DNN) and Autoencoders (AE), are employed to detect DDoS attacks within the dataset. Tools such as the Snort Intrusion Detection System (IDS) are utilized to identify DDoS attacks, while CICFlowMeter is used to extract data from pcap format into csv format. The results of this study demonstrate that the Autoencoder method effectively performs feature extraction and dimensionality reduction, achieving optimal performance using an 80% training and 20% testing split, with a training loss of 0.0052 and validation loss of 0.0054. The features are then classified using a Deep Neural Network with 250 epochs, yielding evaluation metrics of 99.53% accuracy, 99.53% precision, 99.53% recall, and 99.53% F1-score.

Keyword: Internet of Things, Smart home, Distributed Denial of Service, Snort, CICFlowMeter, Deep Learning, Deep Neural Network, Autoencoder.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) adalah di mana perangkat fisik sudah dilengkapi dengan berbagai sensor inframerah, *global position systems* (GPS) dan *radio frequency identification devices* (RFID). Perangkat IoT [1] tersebut terhubung pada internet untuk memudahkan saling berkomunikasi dan juga berbagi informasi yang ada. Perangkat IoT tersebut sudah biasa ditemui di sistem *smart home* seperti berbagai sensor (sensor kelembapan, tekanan, dan suhu) dan berbagai barang rumah tangga seperti *smart ip camera*, *smart door*, *smart TV*, dan *smart bulb*. Konsep kerja sistem *smart home* [2] ini lah memudahkan dan memberikan kenyamanan bagi pengguna untuk mengatur rumah nya. Akan tetapi dari kemajuan itulah dapat memberikan kerentanan pada perangkat IoT di sistem *smart home*.

Keamanan pada jaringan *smart home* lebih rentan dikarenakan perangkat heterogen yang saling terhubung satu sama lain [3]. Serangan seperti ini biasa dikenal dengan *cyber attack* yang di mana membuat perangkat IoT dalam *smart home* terkena dampak kerugian. *Cyber attack* yang biasa dilakukan dalam sistem *smart home* adalah serangan *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS).

Pada penelitian [4] disebutkan bahwa DoS dan DDoS merupakan dua serangan yang sering dihadapi dalam lingkup IoT. Serangan DoS [5] bertujuan menggangu bertukarnya informasi di dalam node sensor membuat terganggunya saluran komunikasi, sehingga data akan gagal untuk di transmisikan ke tujuan. Sedangkan pada serangan DDoS [6] akan membanjiri lalu lintas internet palsu ke target secara bersamaan, sehingga membebani sistem dan membuat target tidak dapat mengakses. Dua serangan *cyber attack* [7] yang dilakukan pada sistem *smart home* inilah yang dapat menyebabkan berbagai dampak kerugian.

Serangan DDoS sendiri merupakan serangan yang lebih berbahaya dibandingkan DoS. Di mana contohnya pada tahun 2016, ketika penyedia *Domain Name System* (DNS) yaitu Dyn terkena serangan DDoS. Aktivitas tersebut berasal dari botnet bernama *Mirai* yang telah menginfeksi sebanyak 600 ribu perangkat IoT yang saling terhubung pada internet seperti kamera IP, telpon VoIP, router, printer

dan lain-lain. Serangan tersebut [8] menyebabkan layanan Dyn *offline* yang membuat situs web yang besar seperti *GitHub*, *PayPal*, *Visa*, *Amazon*, *Reddit* dan lain-lain tidak dapat diakses. Karena itulah dibutuhkan solusi untuk mendeteksi serangan DDoS pada sistem *smart home*.

Solusi untuk masalah tersebut yaitu dengan menerapkan algoritma *machine learning*. Pada penelitian [9] dengan penggunaan model berbasis *machine learning* dapat mampu mendeteksi serangan DDoS pada sistem *smart home*. Di mana hasil dari algoritma *machine learning* ini sendiri dapat membedakan trafik normal dan berbahaya. Akan tetapi terdapat masalah [10] dalam penggunan *machine learning* di mana data traffic jaringan semakin besar yang membuat *machine learning* menggalami kesulitan. Maka dari itu penggunaan *deep learning* memiliki potensi tinggi dalam membuat *smart home* jadi lebih aman lagi dibandingkan *machine learning*.

Pada penelitian [11] dengan menggunakan model *deep neural network* (DNN) berhasil mendeteksi serangan DDoS. Dataset yang digunakan yaitu CICDDoS2019 dan dibagi menjadi dua kategori yaitu refleksi dan eksploitasi. Pada dataset1, model DNN mampu dalam mendeteksi serangan DDoS dengan mendapatkan akurasi 99.97%, precision 99.99%, recall 99.98% dan f1-score 99.98%. Sedangkan pada dataset2, model DNN berhasil mengklasifikasi serangan DDoS dengan akurasi 94.57%, precision 80.49%, recall 95.15% dan f1-score 87.21%. Sehingga model DNN ini sendiri lebih unggul dibandingkan dengan algoritma *machine learning* yang ada karena adanya proses ekstraksi fitur dan klasifikasi di dalam strukturnya.

Pada penelitian lainnya [12] menerapkan model *deep neural network* (DNN) dan autoencoder (AE) menggunakan dataset NSL-KDD dan CICIDS2017. Dengan pendeketan DNN dan AE pada dataset NSL-KDD berhasil menghasilkan akurasi 98.43%, precision 99.22%, recall 97.12% dan f1-score 98.57%. Sedangkan dataset CICIDS2017 mendapatkan akurasi 98.92%, precision 97.45%, recall 98.97% dan f1-score 98.35%. Dari hasil tersebut model DNN dan AE mampu dalam mendeteksi serangan DDoS.

Penilitian ini dilakukan karena masih banyaknya kerentangan terhadap serangan *cyber attack* pada sistem *smarthome*. Pada penelitian [13] disebutkan

bahwa dengan meningkatnya perangkat IoT dan juga gaya teknik serangan DDoS yang baru, menimbulkan deteksi serangan menggunakan model *deep learning* (DL). Di mana model *deep learning* ini dapat berguna dalam mengidentifikasi pola antar keadaan normal dan serangan dalam dataset, serta model ini bisa memprediksi serangan yang bakal mungkin bisa terjadi di masa yang akan datang dengan belajar dari contoh yang telah ada.

Pada penelitian [12] disebutkan bahwa metode DNN dan AE merupakan metode efektif dan mampu dalam mendeteksi serangan *cyber attack*, di mana menunjukan hasil performa yang sangat bagus. Metode ini juga dapat mengatasi masalah dalam fitur learning, menangani data noise dan juga mencegah adanya overfitting pada data yang akan digunakan. Yang membuat metode ini menjadi efektif dalam penelitian ini. Sehingga dari latar belakang yang telah dijelaskan, maka penulis ingin mengambil judul "**Deteksi Serangan DDoS Pada Sistem *Smarthome* Dengan Metode *Deep Learning"*** dengan harapan metode DNN dan AE mampu mendeteksi serangan dengan baik dan menaikan performa kinerja penilitan sebelumnya.

1.2 Rumusan Masalah

Dari latar belakang yang sudah dibuat sebelumnya, maka terbentuklah rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana cara ekstraksi data sebelum mendeteksi serangan DDoS?
2. Bagaimana metode *deep neural network* (DNN) dan *autoencoder* (AE) dapat mendeteksi serangan DDoS pada sistem *smarthome*?
3. Bagaimana performa model *deep learning* terhadap metrik evaluasi yang digunakan?

1.3 Batasan Masalah

Batasan masalah ini terbentuk untuk memberikan fokus yang jelas dalam penelitian ini. Batasan masalah yang telah ditentukan pada penelitian ini adalah sebagai berikut:

1. Penelitian ini hanya akan berfokus pada serangan *cyber attack* pada sistem *smarthome* dengan metode *deep learning*.
2. Pada penelitian ini tidak membahas bagaimana cara untuk mencegah serangan *cyber attack* pada sistem *smarthome*.

3. Dataset yang digunakan adalah dataset COMNETS *SMARTHOME*.

1.4 Tujuan

Tujuan penelitian ini terbentuk dari rumusan masalah yang telah didapat sebelumnya, yang di mana mecakup sebagai berikut:

1. Mengolah ekstraksi data dengan menggunakan *tools CICFlowmeter* sebelum mendeteksi serangan DDoS.
2. Menggunakan metode *deep neural network* (DNN) dan *autoencoder* (AE) dalam mendeteksi serangan DDoS pada sistem *smarthome*.
3. Menggunakan *Confusion matrix* sebagai pengukur performa dari model *deep learning.*

1.5 Manfaat

Adapun manfaat dari penelitian yang telah dilakukan yaitu sebagai berikut:

1. Untuk mengetahui cara ekstraksi sehingga memberikan analisis mendalam terhadap data yang akan digunakan.
2. Untuk menyeleksi antara kelas normal dan kelas DDoS pada dataset.
3. Untuk mengetahui performa dari model *deep learning* dengan menggunakan metode *deep neural network* (DNN) dan *autoencoder* (AE).

1.6 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penelitian yang berjudul "Deteksi Serangan DDoS Pada Sistem *Smarthome* Dengan Metode *Deep Learning*" yaitu sebagai berikut:

1.6.1 Metode Studi Pustaka Literatur

Metode ini digunakan penulis untuk mengumpulkan literatur seperti jurnal, buku, artikel dan sumber online yang berhubungan dengan penelitian yang dilakukan.

1.6.2 Metode Konsultasi

Metode ini digunakan penulis untuk dapat berbicara langsung atau secara *online* dengan setiap orang yang mempunyai pengetahuan yang diperlukan untuk menyelesaikan masalah yang dibahasa pada penelitian ini.

1.6.3 Metode Pengolahan Data

Metode ini digunakan penulis untuk mengekstrak fitur dari data PCAP

menjadi format CSV yang digunakan dalam penelitian dan pemilihan fitur sesuai dengan pola serangan pada penelitian.

1.6.4 Metode Pengerjaan Model dan Pengujian Data

Metode ini digunakan penulis untuk dapat merancang model dari dataset yang telah diolah dengan model Metode *Deep Neural Network* (DNN) dan *AutoEncoder* (AE) agar bisa mencapai akurasi yang tinggi.

1.6.5 Metode Analisa dan Kesimpulan

Metode ini digunakan penulis untuk melakukan analisis, kesimpulan dan saran untuk penelitian kedepannya.

1.7 Sistematika Penulisan

Untuk mempermudah proses penyusunan dan memperjelas isi dari setiap bab maka akan dibuat sistematika pada penulisan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Membahas latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metode penelitian, serta sistematika penulisan yang digunakan dalam penulisan tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Membahas literature review tentang penilitian dan konsep yang relevan untuk mendukung penilitian ini. Konsep-konsep tersebut ialah *smarthome, cyber attack*, *Distributed Denial of Service* (DDoS), *deep learning*, *Deep Neural Network* (DNN) dan *AutoEncoder* (AE).

BAB III METODOLOGI PENELITIAN

Membahas proses penelitian, kerangka kerja penelitian dan perancangan dari model yang akan digunakan pada penelitian untuk mendeteksi serangan *Distributed Denial of Service* (DDoS).

BAB IV HASIL DAN ANALISA

Membahas hasil penelitian yang dilakukan dan menganalisis dari deteksi serangan.

BAB V KESIMPULAN DAN SARAN

Membahas Kesimpulan dan saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

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

[2] U. H. Garba, A. N. Toosi, M. F. Pasha, and S. Khan, “SDN-based detection and mitigation of DDoS attacks on smart homes,” *Comput. Commun.*, vol. 221, no. October 2023, pp. 29–41, 2024, doi: 10.1016/j.comcom.2024.04.001.

[3] U. Saxena, J. Sodhi, and Y. Singh, “An Analysis of DDoS Attacks in a Smart Home Networks,” vol. 6, pp. 272–276, 2020.

[4] A. Alabdulatif, N. N. Thilakarathne, and M. Aashiq, “Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System,” *Comput. Mater. Contin.*, vol. 80, no. 3, pp. 3655–3683, 2024, doi: 10.32604/cmc.2024.054610.

[5] X. Lin, Y. Hu, X. Zhang, and K. Peng, “Encoding–decoding-based distributed state estimation over sensor networks with limited sensing range under DoS attacks,” *Neurocomputing*, vol. 611, no. September 2024, p. 128713, 2025, doi: 10.1016/j.neucom.2024.128713.

[6] Y. A. Anli, Z. Ciplak, M. Sakaliuzun, S. Z. Izgu, and K. Yildiz, “DDoS detection in electric vehicle charging stations: A deep learning perspective via CICEV2023 dataset,” *Internet of Things (Netherlands)*, vol. 28, no. August, p. 101343, 2024, doi: 10.1016/j.iot.2024.101343.

[7] K. D. and R. R. , “Machine learning-based DDOS attack detection and mitigation in SDNs for IoT environments,” *J. Franklin Inst.*, vol. 361, no. 17, p. 107197, 2024, doi: 10.1016/j.jfranklin.2024.107197.

[8] J. I. I. Araya and H. Rifà-Pous, “Anomaly-based cyberattacks detection for smart homes: A systematic literature review,” *Internet of Things (Netherlands)*, vol. 22, no. January, p. 100792, 2023, doi: 10.1016/j.iot.2023.100792.

[9] 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-Augus, 2020, doi:

10.1109/CCECE47787.2020.9255756.

[10] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," *Proc. - 21st IEEE Int. Symp. a World Wireless, Mob. Multimed. Networks, WoWMoM 2020*, pp. 391–396, 2020, doi: 10.1109/WoWMoM49955.2020.00072.

[11] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," *Expert Syst. Appl.*, vol. 169, no. December 2020, p. 114520, 2021, doi: 10.1016/j.eswa.2020.114520.

[12] A. Bhardwaj, V. Mangat, and R. Vig, "Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of ddos attacks in cloud," *IEEE Access*, vol. 8, pp. 181916–181929, 2020, doi: 10.1109/ACCESS.2020.3028690.

[13] T. Khempetch and P. Wuttidittachotti, "Ddos attack detection using deep learning," *IAES Int. J. Artif. Intell.*, vol. 10, no. 2, pp. 382–388, 2021, doi: 10.11591/ijai.v10.i2.pp382-388.

[14] 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. July, p. 101336, 2024, doi: 10.1016/j.iot.2024.101336.

[15] A. Chakraborty, M. Islam, F. Shahriyar, S. Islam, H. U. Zaman, and M. Hasan, "Smart Home System: A Comprehensive Review," *J. Electr. Comput. Eng.*, vol. 2023, 2023, doi: 10.1155/2023/7616683.

[16] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Comput. Networks*, vol. 44, no. 5, pp. 643–666, 2004, doi: 10.1016/j.comnet.2003.10.003.

[17] P. Li, Y. Pei, and J. Li, "A comprehensive survey on design and application of autoencoder in deep learning," *Appl. Soft Comput.*, vol. 138, p. 110176, 2023, doi: 10.1016/j.asoc.2023.110176.

[18] K. Yang, J. Zhang, Y. Xu, and J. Chao, "DDoS Attacks Detection with AutoEncoder," *Proc. IEEE/IFIP Netw. Oper. Manag. Symp. 2020 Manag. Age Softwarization Artif. Intell. NOMS 2020*, no. 2, 2020, doi: 10.1109/NOMS47738.2020.9110372.

[19] 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.

[20] V. N. G. Raju, K. P. Lakshmi, V. M. Jain, A. Kalidindi, and V. Padma, "Study the Influence of Normalization/Transformation process on the Accuracy of Supervised Classification," *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, no. Icssit, pp. 729–735, 2020, doi: 10.1109/ICSSIT48917.2020.9214160.

[21] F. Shen, X. Zhao, G. Kou, and F. E. Alsaadi, "A new deep learning ensemble credit risk evaluation model with an improved synthetic minority oversampling technique," *Appl. Soft Comput.*, vol. 98, p. 106852, 2021, doi: 10.1016/j.asoc.2020.106852.

[22] A. R. Gad, M. Haggag, A. A. Nashat, and T. M. Barakat, "A Distributed Intrusion Detection System using Machine Learning for IoT based on ToN-IoT Dataset," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 6, pp. 548–563, 2022, doi: 10.14569/IJACSA.2022.0130667.

[23] J. Xu, Y. Zhang, and D. Miao, "Three-way confusion matrix for classification: A measure driven view," *Inf. Sci. (Ny).*, vol. 507, pp. 772–794, 2020, doi: 10.1016/j.ins.2019.06.064.

[24] A. de Giorgio, G. Cola, and L. Wang, "Systematic review of class imbalance problems in manufacturing," *J. Manuf. Syst.*, vol. 71, no. September, pp. 620–644, 2023, doi: 10.1016/j.jmsy.2023.10.014.