OPTIMALISASI PERFORMA ALGORITMA *CONVOLUTIONAL NEURAL NETWORK (CNN)* DALAM PROSES KLASIFIKASI MALWARE BOTNET PADA JARINGAN *INTERNET OF THINGS*

OLEH :

SONIAWATI RATFIANA

09011181924020

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2023

OPTIMALISASI PERFORMA ALGORITMA *CONVOLUTIONAL NEURAL NETWORK (CNN)* DALAM PROSES KLASIFIKASI MALWARE BOTNET PADA JARINGAN *INTERNET OF THINGS*

OLEH :

SONIAWATI RATFIANA

09011181924020

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

OPTIMALISASI PERFORMA ALGORITMA *CONVOLUTIONAL NEURAL NETWORK* (CNN) DALAM PROSES KLASIFIKASI MALWARE BOTNET PADA JARINGAN *INTERNET OF THINGS*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

SONIAWATI RATFIANA
09011181924020

Indralaya, 16 Oktober 2023

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. Sukemi, M.T.	**Ahmad Heryanto, M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : **Senin**

Tanggal : **2 Oktober 2023**

Tim Penguji :

1. **Ketua** : **Ahmad Fali Oklilas, M.T.**
2. **Sekretaris** : **Nurul Afifah, M.Kom.**
3. **Penguji** : **Dr. Ahmad Zarkasi, M.T.**
4. **Pembimbing** : **Ahmad Heryanto, M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T. 10/10/23

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Soniawati Ratfiana

Nim : 09011181924020

Judul : Optimalisasi Performa Algoritma *Convolutional Neural Network* (CNN) dalam proses Klasifikasi Malware Botnet pada Jaringan *Internet Of Things*

Hasil pengecekan software turnitin : 2 %

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya saya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian surat pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Indralaya, 11 Oktober 2023

Soniawati Ratfiana

09011181924020

KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Puji syukur Alhamdulillah penulis panjatkan atas kehadirat Allah SWT yang telah memberikan karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini yang berjudul **"Optimalisasi Performa Algoritma *Convolutional Neural Network* (CNN) Dalam Proses Klasifikasi Malware Botnet Pada Jaringan *Internet Of Things*".**

Dalam laporan ini penulis menjelaskan mengenai klasifikasi author terhadap suatu publikasi dengan disertai data-data yang diperoleh penulis saat melakukan penelitian dan pengujian data. Penulis berharap agar tulisan ini dapat bermanfaat bagi orang lain.

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan penulisan Skripsi ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur kepada Allah SWT dan terimakasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan baik dan lancar.
2. Orang tua saya tercinta yang telah membesarkan saya dengan penuh kasih sayang dan selalu mengajarkan saya dalam berbuat hal yang baik. Terimakasih untuk segala do'a, motivasi dan dukungannya baik materil maupun spritual selama ini.
3. Bapak Prof. Dr. Erwin, M.Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Iman Saladin B. Azhar, S.Kom., M.MSI selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer

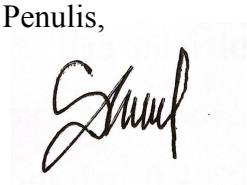
6. Bapak Ahmad Heryanto, S.Kom., M.T., selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya untuk membimbing, memberikan saran dan motivasi kepada penulis dalam menyelesaikan Tugas Akhir ini.
7. Mbak Renny selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
8. Cuh Meizi Sasfini, Salwa Ayu Rafika dan Lisa Agustina yang telah membimbing dan memotivasi selama penyelesaian Tugas Akhir ini.
9. Serta semua pihak yang telah membantu.

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis. Akhir kata penulis berharap, semoga proposal tugas akhir ini bermanfaat dan berguna bagi orang lain.

Wassalamu'alaikum Wr. Wb.

Indralaya, 11 Oktober 2023

Penulis,



Soniawati Ratfiana

NIM. 09011181924020

Optimalisasi Performa Algoritma *Convolutional Neural Network* (CNN) dalam proses Klasifikasi Malware Botnet pada Jaringan *Internet Of Things*

Soniawati Ratfiana (09011181924020)
Jurusan Sistem Komputer , Fakultas Ilmu Komputer, Universitas sriwijaya
Email: soniawatiratfiana@gmail.com

ABSTRAK

Ancaman terhadap jaringan internet salah satunya botnet (robot network). walaupun sudah banyak metode yang digunakan untuk mendeteksi botnet , namun masih ada yang kurang akurat. hal ini dilihat dari hasil akurasi, presisi dan lainnya yang berbeda jauh akibat terjadinya *imbalanced dataset*. Penelitian ini mengkaji tentang klasifikasi serangan botnet dan membangun model CNN yang terbaik serta akurat dengan melakukan optimalisasi dengan dataset CICIDS-17 yang terdiri dari 97718 data BENIGN dan 128027 data DDoS dengan menerapkan teknik *undersampling* serta arsitektur AlexNet dan LeNet pada metode *Convolutional Neural Network.* Setelah dioptimalkan, arsitektur AlexNet mendapatkan akurasi sebesar 99.97% dari 99.94% dan nilai loss menurun dari 0.49% menjadi 0.11%. sedangkan arsitektur Lenet akurasinya meningkat dari 99.88% menjadi 99.93% dan nilai lossnya menurun dari 0.40% menjadi 0.24%. Berdasarkan grafik akurasinya, kedua model tersebut tidak *overfitting* maupun *underfitting*. Sedangkan berdasarkan *confusion matrix* nya, terlihat bahwa model mampu mengklasifikasikan botnet dengan cukup baik.

Keywords : *Convolutional Neural Network, CICIDS-17, Botnet IoT, AlexNet, LeNet*

Performance Optimization of Convolutional Neural Network (CNN) Algorithm in the process of Botnet Malware Classification on Internet Of Things Networks

Soniawati Ratfiana (09011181924020)

Department of Computer Systems, Faculty of Computer Science, Sriwijaya University

Email: soniawatiratfiana@gmail.com

ABSTRACT

One of the threats to the internet network is botnet (robot network). although there are many methods used to detect botnet, but there are still less accurate. this can be seen from the results of accuracy, precision and others that differ greatly due to imbalanced datasets. This research examines the classification of botnet attacks and builds the best and accurate CNN model by optimizing the CICIDS-17 dataset consisting of 97718 BENIGN data and 128027 DDoS data by applying undersampling techniques and AlexNet and LeNet architectures in the Convolutional Neural Network method. After being optimized, AlexNet architecture gets an accuracy of 99.97% from 99.94% and the loss value decreases from 0.49% to 0.11%. while Lenet architecture the accuracy increases from 99.88% to 99.93% and the loss value decreases from 0.40% to 0.24%. Based on the accuracy graph, both models are neither overfitting nor underfitting. Meanwhile, based on the confusion matrix, it can be seen that the model is able to classify botnets quite well.

Keywords : *Convolutional Neural Network, CICIDS-17, Botnet IoT, AlexNet, LeNet*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) adalah ekosistem global teknologi informasi dan komunikasi yang bertujuan untuk menghubungkan semua jenis objek kapan saja dan dimana saja satu sama lain ke dalam jaringan internet. *Internet of Things* (IoT) terdiri dari kombinasi objek fisik dengan sensor, aktuator, dan pengontrol dengan konektivitas ke dunia digital melalui Internet. Biaya perangkat keras yang rendah, bersama dengan prevalensi perangkat seluler dan akses Internet yang meluas, telah membuat IoT menjadi bagian dari kehidupan modern sehari-hari. IoT memiliki sifat heterogen dari penyebaran yang menimbulkan kerentanan dalam bidang keamanan dan privasi [1] .

Hal inilah yang membuat para cracker untuk masuk ke jaringan tersebut dengan tujuan untuk mencuri informasi rahasia, merusak database, menonaktifkan sistem, menyebarkan virus temasuk malware yang dirancang untuk melakukan suatu tindakan jahat seperti mengirim spam, menghapus data sensitif, pencurian *crypto-wallet* sehingga mereka dapat menginfeksi karena Fitur IoT mempunyai akses internet penuh tanpa penyaringan paket apa pun, membuatnya sesuai untuk menjadi bagian dari jaringan zombie atau robot network (Botnet)[2].

Seorang individu atau kelompok dapat melakukan serangan ini. Jika sebuah kelompok yang melakukannya, maka dinamakan "botnet", sedangkan jika seorang individu yang meluncurkannya, maka dikenal sebagai *"bot-master"*.Bot-master adalah simpul penyerang yang dapat meluncurkan beberapa jenis serangan ke server, seperti *Phishing*, *spam*, *Click fraud*, dan lainnya [3] . Perangkat yang telah terinfeksi diatur oleh server *command and control* (C2) yang merupakan sebuah sistem yang digunakan oleh musuh untuk mengontrol dengan mengirimkan pesan dan perintah ke sistem yang dijanjikan dari jarak jauh. Musuh dapat mencuri data melalui perintah-perintah ini dan memanipulasi jaringan yang terinfeksi.

Tidak jarang banyak periset seperti M.Ferrag dkk. dalam jurnalnya [19] sudah menganjurkan berbagai metode deteksi botnet IoT yaitu DNN,CNN dan RNN dengan beberapa dataset yaitu BoT IoT dengan akurasi masing-masing metode (95.76%, 96.02%, 96.76%), MQTTset (90.06%, 89.77%, 89.29%) , TON_IoT dataset(99.68%, 98.87%, 99.98%), namun masih ada tantangan yang belum terselesaikan. Selain itu pada jurnal [10][16][17][19] yang menggunakan metode CNN dengan masing-masing dataset dan akurasinya yaitu *Microsoft's public dataset* 98%, *motor imagery signals with Brain-computer interface* (BCI) 93.54%, *self-generated dataset* 99% dan BoT-IoT 91% . Beberapa jurnal tersebut termasuk dalam kategori sangat baik dalam proses klasifikasi tetapi masih memiliki kekurangan dalam melihat kondisi keseimbangan data dimana data kelas abnormal lebih banyak(mayoritas) daripada kelas normal(minoritas) atau biasa disebut imbalanced dataset. Penelitian diatas hanya bisa memprediksi pada kelas mayoritas dengan baik tetapi sangat rendah dalam prediksi kelas minoritas.

Untuk menangani *imbalanced dataset* tersebut yaitu dengan melakukan resample data pelatihan atau undersampling dimana teknik ini akan memberikan distribusi kelas yang seimbang dengan mengurangi kelas mayoritas secara acak[32]. Berdasarkan riset yang telah dilakukan menunjukkan bahwa metode CNN merupakan metode terbaik dengan akurasi yang tetap tinggi walaupun menggunakan *dataset imbalanced*. Oleh karena itu, dilakukan penelitian tentang **Optimalisasi Performa Algoritma *Convolutional Neural Network* (CNN) Dalam Proses Klasifikasi Malware Botnet Pada Jaringan *Internet Of Things*** dengan menggunakan teknik *undersampling* guna memberikan akurasi yang tinggi dalam setiap kelas.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat disimpulkan bahwa masalah dalam penelitian ini yaitu kurangnya keakuratan model dalam memprediksi setiap kelas botnet . Oleh karena itu, penulis melakukan penelitian untuk bagaimana mendapatkan akurasi yang lebih bagus dari algoritma *convolutional neural network* dalam mengklasifikasi data kelas biner yang balanced / seimbang.

1.3 Tujuan

Tujuan dari penulisan tugas akhir ini, yaitu :

1. Untuk melakukan klasifikasi terhadap berbagai macam serangan malware botnet.
2. Untuk membuat simulasi serta model yang baik supaya meningkatkan keakuratan sistem dalam mendeteksi serangan yang masuk dengan menerapkan arsitektur ALexNet dan LeNet.

1.4 Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu :

1. Dataset yang digunakan merupakan dataset publik yang diakses melalui web kaggle yaitu CICIDS-17
2. Mengaplikasikan bahasa pemrograman *Python* dan platform *jupyter Notebook* untuk pengolahan data dan merancang model
3. Menggunakan arsitektur dari metode *Convolutional Neural Network* yaitu AlexNet dan LeNet
4. Menerapkan metrik evaluasi guna mengukur kemampuan model seperti akurasi, presisi, recall dan f1_score

1.5 Metodologi Penelitian

Pada tugas akhir ini menggunakan metodelogi sebagai berikut :

1. Metode Studi Pustaka dan Literature

   Dengan mengumpulkan referensi yang berupa literature yang terdapat pada buku, jurnal dan internet mengenai definisi serangan, metode/algoritma, serta proses klasifikasi yang nantinya berguna untuk proses pengerjaan tugas akhir ini.

2. Metode Konsultasi

   Pada metode ini melakukan konsultasi kepada pihak-pihak yang memiliki pengetahuan serta wawasan yang baik dalam mengatasi permasalahan yang ditemui pada penulisan tugas akhir ini.

3. Metode Pembuatan Model

Pada metode ini membuat suatu perancangan pemodelan dengan menggunakan simulasi dengan bisa menggunakan berbagai macam perangkat lunak agar bisa memperlancar proses pembuatan model.

4. Metode Pengujian

Pada metode ini melakukan pengujian terhadap simulasi yang telah dibuat, apakah simulasi tersebut dapat menghasilkan nilai akurasi yang baik atau tidak.

5. Metode Analisa dan Kesimpulan

Hasil dari pengujian pada tugas akhir ini akan dianalisis baik kelebihannya maupun kekurangannya serta membandingkannya dengan algoritma lain.

1.6 Sistematika

Sitstematika penulisan dalam penelitian ini yaitu :

BAB I PENDAHULUAN	Bab ini berisi latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penelitian.
BAB II TINJAUAN PUSTAKA	Bab ini berisi dasar teori yang menunjang penulisan mengenai deteksi *cybercrime* seperti arsitektur, dataset yang digunakan , dan model untuk membuat sistem tersebut
BAB III METODOLOGI PENELITIAN	Bab ini berisi kerangka kerja/prosedur/tahapan serta metode yang digunakan dalam membangun sistem tersebut.

BAB 4 HASIL DAN PEMBAHASAN	Bab ini berisi hasil dan pembahasan dari penelitian yang dilakukan dalam mendapatkan hasil yang akurat
BAB 5 KESIMPULAN DAN SARAN	Bab ini berisi kesimpulan yang didapatkan dari hasil penelitian yang sudah dilakukan dan memberikan solusi serta saran yang membangun untuk lebih baik kedepannya.

DAFTAR PUSTAKA

[1] S. Siboni *et al.*, "Security Testbed for Internet-of-Things Devices," *IEEE Trans Reliab*, vol. 68, no. 1, pp. 23–44, 2019, doi: 10.1109/TR.2018.2864536.

[2] M. Idhammad, K. Afdel, and M. Belouch, "Detection System of HTTP DDoS Attacks in a Cloud Environment Based on Information Theoretic Entropy and Random Forest," *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/1263123.

[3] F. Sattari, A. H. Farooqi, Z. Qadir, B. Raza, H. Nazari, and M. Almutiry, "A Hybrid Deep Learning Approach for Bottleneck Detection in IoT," *IEEE Access*, vol. 10, no. April, pp. 77039–77053, 2022, doi: 10.1109/ACCESS.2022.3188635.

[4] F. Hussain *et al.*, "A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks," *IEEE Access*, vol. 9, pp. 163412–163430, 2021, doi: 10.1109/ACCESS.2021.3131014.

[5] R. Xin, J. Zhang, and Y. Shao, "Complex network classification with convolutional neural network," *Tsinghua Sci Technol*, vol. 25, no. 4, pp. 447–457, 2020, doi: 10.26599/TST.2019.9010055.

[6] D. Wen *et al.*, "Task-State EEG Signal Classification for Spatial Cognitive Evaluation Based on Multiscale High-Density Convolutional Neural Network," *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 30, pp. 1041–1051, 2022, doi: 10.1109/TNSRE.2022.3166224.

[7] M. Amirian and F. Schwenker, "Radial Basis Function Networks for Convolutional Neural Networks to Learn Similarity Distance Metric and Improve Interpretability," *IEEE Access*, vol. 8, pp. 123087–123097, 2020, doi: 10.1109/ACCESS.2020.3007337.

[8] J. Jeon, J. H. Park, and Y. S. Jeong, "Dynamic Analysis for IoT Malware Detection with Convolution Neural Network Model," *IEEE Access*, vol. 8, pp. 96899–96911, 2020, doi: 10.1109/ACCESS.2020.2995887.

[9] M. Panda, A. A. A. Mousa, and A. E. Hassanien, "Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks," *IEEE Access*, vol. 9, pp. 91038–91052, 2021, doi: 10.1109/ACCESS.2021.3092054.

[10] H. Wang, H. Long, A. Wang, T. Liu, and H. Fu, "Deep Learning and Regularization Algorithms for Malicious Code Classification," *IEEE Access*, vol. 9, pp. 91512–91523, 2021, doi: 10.1109/ACCESS.2021.3090464.

[11] S. Rezaei, B. Kroencke, and X. Liu, "Large-Scale Mobile App Identification Using Deep Learning," *IEEE Access*, vol. 8, pp. 348–362, 2020, doi: 10.1109/ACCESS.2019.2962018.

[12] R. Kalakoti, S. Nomm, and H. Bahsi, “In-Depth Feature Selection for the Statistical Machine Learning-Based Botnet Detection in IoT Networks,” *IEEE Access*, vol. 10, no. September, pp. 94518–94535, 2022, doi: 10.1109/ACCESS.2022.3204001.

[13] C. Zhang, J. Feng, C. Hu, Z. Liu, L. Cheng, and Y. Zhou, “An Intelligent Fault Diagnosis Method of Rolling Bearing under Variable Working Loads Using 1-D Stacked Dilated Convolutional Neural Network,” *IEEE Access*, vol. 8, no. Ml, pp. 63027–63042, 2020, doi: 10.1109/ACCESS.2020.2981289.

[14] R. Alazrai, M. Hababeh, and B. A. Alsaify, “An End-to-End Deep Learning Framework for Recognizing Human-to-Human Interactions Using Wi-Fi Signals,” pp. 197695–197710, 2020, doi: 10.1109/ACCESS.2020.3034849.

[15] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, “Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis,” *IEEE Access*, vol. 9, no. Ml, pp. 138509–138542, 2021, doi: 10.1109/ACCESS.2021.3118642.

[16] D. Li, J. Wang, J. Xu, and X. Fang, “Densely Feature Fusion Based on Convolutional Neural Networks for Motor Imagery EEG Classification,” *IEEE Access*, vol. 7, pp. 132720–132730, 2019, doi: 10.1109/ACCESS.2019.2941867.

[17] M. W. Nadeem, H. G. Goh, Y. Aun, and V. Ponnusamy, “Detecting and Mitigating Botnet Attacks in Software-Defined Networks using Deep Learning Techniques,” *IEEE Access*, vol. 11, no. March, pp. 49153–49171, 2023, doi: 10.1109/ACCESS.2023.3277397.

[18] F. Khan, C. Ncube, and L. K. Ramasamy, “A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning,” vol. 8, 2020, doi: 10.1109/ACCESS.2020.3003785.

[19] 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. September, pp. 98427–98440, 2022, doi: 10.1109/ACCESS.2022.3206367.

[20] J. Velasco-Mata, V. Gonzalez-Castro, E. F. Fernandez, and E. Alegre, “Efficient Detection of Botnet Traffic by Features Selection and Decision Trees,” *IEEE Access*, vol. 9, pp. 120567–120579, 2021, doi: 10.1109/ACCESS.2021.3108222.

[21] A. M. Almuhaideb and D. Y. Alynanbaawi, “Applications of Artificial Intelligence to Detect Android Botnets: A Survey,” *IEEE Access*, vol. 10, no. April, pp. 71737–71748, 2022, doi: 10.1109/ACCESS.2022.3187094.

[22] D. Javaheri, M. Hosseinzadeh, and A. M. Rahmani, “Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines,” *IEEE Access*, vol. 6, pp. 78321–78332, 2018, doi: 10.1109/ACCESS.2018.2884964.

[23] A. H. Janabi, T. Kanakis, and M. Johnson, “Convolutional Neural Network Based Algorithm for Early Warning Proactive System Security in Software Defined Networks,” *IEEE Access*, vol. 10, pp. 14301–14310, 2022, doi: 10.1109/ACCESS.2022.3148134.

[24] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, vol. 2018-Janua, no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[25] M. Kulin, T. Kazaz, I. Moerman, and E. De Poorter, "End-to-End Learning From Spectrum Data : A Deep Learning Approach for Wireless Signal Identification in Spectrum Monitoring Applications," *IEEE Access*, vol. 6, pp. 18484–18501, 2018, doi: 10.1109/ACCESS.2018.2818794.

[26] M. Gjoreski, M. Ž. Gams, M. Luštrek, and P. Genc, "Machine Learning and End-to-End Deep Learning for Monitoring Driver Distractions From Physiological and Visual Signals," vol. 8, 2020, doi: 10.1109/ACCESS.2020.2986810.

[27] S. Zhai, D. Shang, S. Wang, and S. Dong, "DF-SSD: An Improved SSD Object Detection Algorithm Based on DenseNet and Feature Fusion," *IEEE Access*, vol. 8, pp. 24344–24357, 2020, doi: 10.1109/ACCESS.2020.2971026.

[28] H. Yang, C. Meng, and C. Wang, "Data-driven feature extraction for analog circuit fault diagnosis using 1-D convolutional neural network," *IEEE Access*, vol. 8, pp. 18305–18315, 2020, doi: 10.1109/ACCESS.2020.2968744.

[29] B. Zoph and Q. V Le, "Searching for activation functions," *6th International Conference on Learning Representations, ICLR 2018 - Workshop Track Proceedings*, pp. 1–13, 2018.

[30] T. Trajanovski and N. Zhang, "An Automated and Comprehensive Framework for IoT Botnet Detection and Analysis (IoT-BDA)," *IEEE Access*, vol. 9, pp. 124360–124383, 2021, doi: 10.1109/ACCESS.2021.3110188.

[31] W. Li, J. Jin, and J. H. Lee, "Analysis of Botnet Domain Names for IoT Cybersecurity," *IEEE Access*, vol. 7, pp. 94658–94665, 2019, doi: 10.1109/ACCESS.2019.2927355.

[32] Y. S. Jeon and D. J. Lim, "PSU: Particle Stacking Undersampling Method for Highly Imbalanced Big Data," *IEEE Access*, vol. 8, pp. 131920–131927, 2020, doi: 10.1109/ACCESS.2020.3009753.

[33] L. Dong *et al.*, "Very High Resolution Remote Sensing Imagery Classification Using a Fusion of Random Forest and Deep Learning Technique-Subtropical Area for Example," *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.*, vol. 13, pp. 113–128, 2020, doi: 10.1109/JSTARS.2019.2953234.

[34] R. Hazarika *et al.*, "An Improved LeNet-Deep Neural Network Model for Alzheimer ' s Disease Classification Using Brain Magnetic Resonance Images," *IEEE Access*, vol. 9, pp. 161194-161207, 2021, doi: 10.1109/ACCESS.2021.3131741

[35] A. Ullah *et al.*, "AlexNet , AdaBoost and Artificial Bee Colony Based Hybrid Model for Electricity Theft Detection in Smart Grids," *IEEE Access*, vol. 10, pp. 18681-18694, 2022, doi: 10.1109/ACCESS.2022.3150016