Klasifikasi *Botnet* pada Jaringan *Internet Of Things* (IOT) menggunakan *Autoencoder* dan *Artificial Neural Network* (ANN)

TUGAS AKHIR
Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :
ABDI BIMANTARA
09011381722100

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

HALAMAN PENGESAHAN

KLASIFIKASI BOTNET PADA JARINGAN INTERNET OF THINGS (IOT) MENGGUNAKAN AUTOENCODER DAN ARTIFICIAL NEURAL NETWORK (ANN)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

ABDI BIMANTARA
09011381722100

Indralaya Maret 2021

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T
Nip. 196612032006041001

Pembimbing

Deris Stiawan, Ph.D
Nip. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Senin

Tanggal : 1 Maret 2021

Tim Penguji :

1. Ketua Sidang : Ahmad Zarkasi, M.T.
2. Sekretaris Sidang : Iman Saladin B. Azhar ,S.Kom., M.SI
3. Penguji Sidang : Ahmad Heryanto, M.T.
4. Pembimbing : Deris Stiawan, Ph.D.

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T

Nip. 196612032006041001

HALAMAN PERNYATAAN

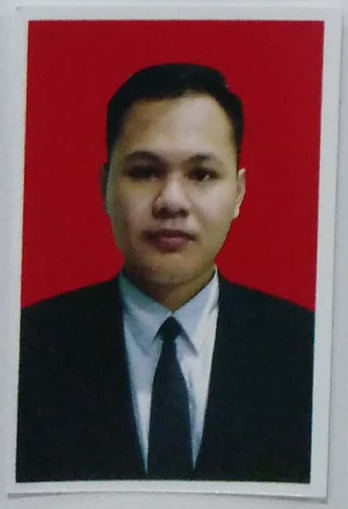
Yang bertanda tangan dibawah ini :

Nama	: Abdi Bimantara
Nim	: 09011381722100
Prorgram Studi	: Sistem Komputer
Judul Penelitian	: Klasfikasi Botnet pada Jaringan Internet of Things (IoT) Menggunakan Autoencoder dan Artificial Neural Network (ANN)

Hasil Pengecekkan *Software iTehnticate/ Turnitin* : 7%

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

Demikin surat pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



Indralaya, Maret 2021

Abdi Bimantara
Nim. 09011381722100

HALAMAN PERSEMBAHAN

"Hutang Jasa yang Harus Dilunasi"

"Jangan pernah takut dalam mencoba sesuatu, karena akan ada peluang untuk terwujudkan"

"Kupersembahkan karya ini, untuk cahaya hidupku, yang senantiasa ada saat suka maupun duka, tetesan keringatmu, jerih payahmu, do'amu yang selalu menyertai langkahku, AYAH dan IBUKU"

"Ayah, abim lulus S1 (S.Kom) ^-^"

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan tugas akhir dengan judul **"Klasifikasi Botnet pada jaringan Internet Of Things (IoT) menggunakan Autoencoder dan Artificial Neural Network (ANN) "**.

Penulisan laporan tugas akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan laporan ini. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan laporan tugas akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Orang Tua (Heriyansyah dan Erawati) serta keluarga penulis tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama mengikuti dan melaksanakan perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya hingga dapat menyelesaikan laporan tugas akhir ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Deris Stiawan, Ph. D. selaku Dosen Pembimbing Tugas Akhir penulis sekaligus Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya
5. Mbak Nurul Afifah, M.Kom yang telah sangat membantu saya dalam proses pengerjaan laporan tugas akhir ini.

6. Kakak-kakak panutan yang telah memberikan pengetahuan serta saran dan motivasi, Kak Ridho Ilham Renaldo S.kom., Kak Tri Wanda Septian M.Sc
7. Keluarga besar Lab Center of Excellent (CoE) yang juga sangat membantu selama proses pengerjaan tugas akhir
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Tiara Annisa Dina (09011381722124) yang telah menyediakan waktunya dalam menemani, membantu serta memberikan semangat saya dalam meyelesaikan tugas akhir ini.
10. Topek, Agung, Nadhya, dan Safek B yang telah membantu saya dalam menyelesaikan tugas akhir ini
11. Seluruh teman-teman seperjuangan angkatan 2017 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
12. Almamater.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan alporan tugas akhir ini. Karena sesungguhnya tak ada yang sempurna didunia ini. Untuk itu, segala saran dan kritik sangatlah penting bagi penulis. Akhir kata, semoga laporan tugas akhir ini dapat bermanfaat dan berguna bagi khalayak.

Indralaya, Maret 2021
Penulis

Botnet classification on Internet of Things (IoT) networks using Autoencoder and Artificial Neural Network (ANN)

Abdi Bimantara (09011381722100)

Departement of Computer Engineering, Faculty of Computer Science, Universitas Sriwijaya

Email : abdibimantara91@gmail.com

Abstract

Internet of Things (IoT) Allows every device to be connected to each other through internet intermediaries. However, in implementing this technology, there are various kinds of threats. One of the serious threats to IoT technology is the DDOS attack through an intermediary Botnet (Robot Network). This research uses a dataset from Tallinn University of Technology, namely the MedBIoT dataset. The autoencoder algorithm is used in the dimensional reduction process. In addition, Artificial Neural Network Algorithms are also used in the classification process. The classification results using the two algorithms show fairly good results in the binary case, namely an accuracy value of 99.72%, a precision value of 99.82, a sensitivity value of 99.83%, a specificity value of 99.31% and an f1-score of 99.82%. Furthermore, the classification results in the multiclass case also get pretty good results, namely an accuracy value of 99.78%, a precision value of 99.54%, a sensitivity value of 99.51%, a specificity value of 99.70%, and an F1-score of 99.52%.

Keywords : *BOTNET Classification, Autoencoder, Artificial Neural Network, Internet of Things, Machine Learning*

Klasifikasi Botnet pada jaringan Internet Of Things (IoT) menggunakan Autoencoder dan Artificial Neural Network (ANN)

Abdi Bimantara (09011381722100)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : abdibimantara91@gmail.com

Abstract

Internet of Things (IoT) memungkinkan setiap perangkat dapat saling terhubung melalui perantara internet. Namun dalam pengimplementasian teknologi tersebut, terdapat berbagai macam ancaman. Salah satu ancaman serius pada teknologi IoT yaitu serangan DDOS melalui perantara Botnet *(Robot Network)*. Penelitian ini menggunakan dataset yang berasal dari Tallinn University of Technology yaitu MedBIoT dataset. Algoritma *autoencoder* digunakan pada proses reduksi dimensi. Selain itu, Algoritma *Artificial Neural Network* juga digunakan pada proses klasifikasi. Hasil klasifikasi menggunakan kedua algoritma tersebut menunjukkan hasil yang cukup baik pada kasus *binary* yaitu nilai akurasi sebesar 99.72%, nilai presisi sebesar 99.82, nilai sensitivitas sebesar 99.83%, nilai spesifisitas sebesar 99.31% serta nial f1-score sebesar 99.82%. Selanjutnya hasil klasifikasi pada kasus *multiclass* juga mendapatkan hasil yang cukup baik yaitu nilai akurasi sebesar 99.78%, nilai presisi sebesar 99.54%, nilai sensitivitas sebesar 99.51%, nilai spesifisitas sebesar 99.70%, dan nilai F1-score sebesar 99.52%.

Keywords : *BOTNET Classification, Autoencoder, Artificial Neural Network, Internet of Things, Machine Learning*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1. Latar Belakang

Internet of Things (IoT) merupakan salah satu contoh perkembangan teknologi yang ada saat ini. IoT memungkinan setiap perangkat teknologi berbasis identifikasi seperti sensor, RFID dan lain sebagainya dapat saling terhubung ke internet berdasarkan protokol komunikasi standar [1]. Dalam penerapannya, IoT dapat memperluas bentuk interaksi antara user (manusia) dengan objek (perangkat teknologi) dan interkasi antara objek lainnya yang biasa disebut dengan komunikasi *Machine to Machine* (M2M)[2][3].

Namun seiring dengan berkembangnya pengimplementasian IoT dalam kehidupan, juga menimbulkan berbagai macam masalah. Masalah yang timbul tersebut meliputi masalah privasi, keamanan, konfigurasi sistem , kontrol akses, verifikasi dan lain sebagainya[4]. Selain itu IoT juga sangatlah rentan terhadap berbagai macam serangan yang mengakibatkan gangguan dalam proses komunikasi.

Distributed Denial of Service (DDOS) merupakan salah satu ancaman serius yang ada pada jaringan IoT. Serangan DDOS dapat menyebabkan suatu server menjadi sibuk dengan banyaknya permintaan-permintaan sehingga user sah atau normal tidak dapat mengakses jaringan tersebut. Dalam perkembangannya seorang *hacker* juga dapat menggunakan *botnet* (*Robot Network*) dalam melancarkan serangan DDOS. *Botnet* merupakan salah satu jenis *malware (Malicious Software)* yang dalam sistem kerjanya dapat dikendalikan oleh seorang *hacker* (*Botmaster*) secara teknis.

Saat ini jenis *botnet* sangatlah beragam seperti *Mirai, Torii, Okiru, Kenjiro* dan lain sebagainya. Penelitian mengenai *botnet* telah banyak dilakukan dalam beberapa tahun terkahir. Sehingga penelitian mengenai *botnet* bukanlah hal yang baru lagi, hal ini dapat dilihat dari cukup banyaknya penelitian yang dilakukan

sebelumnya. Pada penelitian sebelumnya [5], membahas bagaimana mengklasifikasikan *botnet* pada infrastruktur IoT dengan 80 perangkat yang terkoneksi berdasarkan *Network Traffic*. Pada penelitian ini menggunakan dataset yang memiliki format *.pcap*. Kemudian file tersebut di ekstraksi untuk selanjutnya diklasifikasi menggunakan tiga algoritma yaitu *k-Nearest Neighbors* (k-NN), *Decision Tree* (DT) dan *Random Forest* (RF). Dari hasil penelitian yang telah dilakukan, klasifikasi dengan bantuan tiga algoritma tersebut mendapatkan hasil yang cukup tinggi. Pada proses pengklasifikasian *Binary* mendapatkan akurasi 90,25% untuk K-NN, 93,15% untuk DT, dan 95,32% untuk RF. Selain itu pada pengklasifikasian *Multi-Class* mendapatkan hasil akurasi sebesar 87,06% untuk K-NN, 95,16% untuk DT, dan 97,66% untuk RF. Pada penelitian ini juga menyimpulkan bahwa pendekatan secara linear tidak cocok untuk data yang digunakan, sehingga algoritma SVM tidak direkomendasikan.

Selanjutnya, pada penelitan[6] membahas mengenai pendeteksian *botnet* pada jaringan IoT berdasarkan *Network Traffic.* Pada penelitian kali ini algoritma *autoencoder* digunakan dalam mendeteksi *botnet* pada perangkat yang tersambung pada jaringan IoT. Selain itu penelitian ini mendeteksi dua jenis *botnet* yaitu *Mirai* dan *Bashlite* dan tanpa menggunakan data yang berlabel. Data yang digunakan dalam pengklasifikasian berupa data *.pcap* yang terlebih dahulu diekstraksi sebelumnya. Hasil yang didapatkan dalam mendeteksi serangan cukup bagus dibuktikan dengan nilai tingkat positif palsu yang rendah.

Pada penelitian lainnya[7], Algoritma *Artificial Neural Network* (ANN) digunakan dalam pengklasifikasian *botnet*. Dataset yang digunakan pada penelitian tersebut berasal dari CTU-13. Hasil akurasi yang didapatkan pun cukup tinggi yaitu sebesar 96,5%.

Dari beberapa ulasan diatas, penulis akan membahas mengenai klasifikasi *botnet* pada jaringan IoT menggunakan dataset berbentuk *.pcap* yang terlebih dahulu diekstraksi sehingga dapat di proses oleh algoritma *autoencoder*. Selanjutnya hasil dari *dimensional reduction* tersebut akan diklasifikasi menggunakan algoritma *Artificial Neural Network*.

1.2. Perumusan Masalah

Berdasarkan penelitian sebelumnya[5], *botnet* pada jaringan *Internet of Things* (IoT) dapat dideteksi di *network traffic*. Namun pada penelittian ini hasil akurasi yang didapatkan masih bisa ditingkatkan lagi. Selain itu pada penelitian ini juga menyebutkan bahwa data yang digunakan tidak dapat diolah secara linear. Pada penelitian lainnya[7], menyebutkan bahwa algoritma *Artificial Neural Network* (ANN) telah memiliki performa yang sangat baik untuk klasifikasi *botnet* dibuktikan dengan mendapatkan nilai akurasi sebesar 96,5%. Selanjutnya pada penelitian [6], menyebutkan algoritma *autoencoder* yang bersifat non linear sangat mempengaruhi hasil dari sistem klasifikasi.

Berdasarkan latar belakang diatas, Maka didapatkanlah perumusan masalah yaitu :

1. Bagaimana cara mengklasifikasian *botnet* pada IoT di *network traffic* dengan menggunakan algoritma ANN ?
2. Bagaimana menerapkan sistem klasifikasi *Binary* dan *Multi-Class botnet* dengan bantuan algoritma ANN sehingga nilai akurasi meningkat dari penelitian sebelumnya?
3. Bagaimana pengaruh algoritma *autoencoder* terhadap kinerja sistem klasifikasi pada IoT berdasarkan *network traffic*?

1.3. Batasan Masalah

Adapun beberapa batasan masalah yang dirancang pada skripsi ini yaitu :

1. Dataset yang digunakan pada penelitian ini berasal *Tallinn University of Technology* yaitu MedBIoT dataset
2. Deteksi *botnet* pada penelitian ini di *network traffic*
3. Algoritma yang digunakan dalam pengklasifikasian *botnet* pada jaringan IoT yaitu algoritma ANN.
4. Proses *dimentionality reduction* yang digunakan adalah *autoencoder*
5. Analisa *botnet* dilakukan secara *dynamic*
6. Dalam penelitian ini tidak membahas bagaimana cara pencegahan *botnet* pada jaringan IoT

1.4. Tujuan

Adapun pada penelitian ini memiliki tujuan sebagai berikut :

1. Menerapkan algoritma ANN untuk mengklasifikasi data *botnet* pada jaringan IoT di *network traffic*
2. Menerapkan sistem klasifikasi *Binary* dan *Multi-Class botnet* serta meningkatkan nilai akurasi dari penelitian sebelumya
3. Mengetahui pengaruh algoritma *autoencoder* terhadap kinerja sistem klasifikasi *botnet* pada jaringan IoT di *network traffic*

1.5. Manfaat

Hasil yang didapatkan dari penelitian ini dapat menjadi landasan dalam pengembangan lebih lanjut mengenai klasifikasi *botnet* pada jaringan IoT. Selain itu manfaat dari penelitian ini secara praktis sebagai berikut :

1. Dapat mengklasifikasi *botnet* pada jaringan IoT di *network traffic* dengan menggunakan algoritma ANN
2. Algoritma *autoencoder* sangat berpengaruh dalam peningkatan kinerja sistem klasifikasi *botnet* pada jaringan IoT di *network traffic* dengan menggunakan algoritma ANN
3. Hasil yang didapatkan dari penelitian ini dapat menjadi dasar untuk meningkatkan nilai validasi seperti nilai akurasi, nilai spesifisitas, nilai sensitivitas, nilai f1-score serta nilai presisi dalam sistem klasifikasi *Binary* dan *Multi-Class* yang menerapkan algoritma *autoencoder* dan ANN.

1.6. Metodologi Penelitian

Metodologi yang digunakan pada penelitian ini akan melewati beberapa tahapan sebagai berikut :

1. Tahap Pertama (Persiapan data)

   Tahap ini ialah tahap yang dilakukan setelah masalah yang dibahas telah sesuai dan relevan diangkat sebagai penelitian. Pada tahap ini diharuskan untuk membaca literature yang sesuai dengan topik penelitian dan mencari dataset yang akan digunakan.

2. Tahap Kedua (Pengolahan data)

   Pada tahap ini membahas mengenai proses bagaimana mengolah suatu data mentah menjadi data siap olah, memvisualisasikan data, serta melakukan proses reduksi dimensi data dengan menggunakan algoritma *autoencoder*.

3. Tahap Ketiga (Klasifikasi)

   Pada tahap ini dilakukanlah proses pengklaifikasian data botnet dan data normal dengan menggunakan algortiman ANN. Setelah proses klasifikasi selesai, dilanjutkan pada proses validasi dengan menggunakan beberapa parameter pengujian.

4. Tahap Keempat (Analisis)

   Setelah mendapatkan data dari tahap pengklasifikasian, maka langkah selanjutnya adalah melakukan analisis terhapada hasil yang telah didapatkan sebelumnya sehingga didapatkan hasil yang objektif.

1.7. Sistematika Penulisan

Agar lebih mudah dalam proses penyusunan tugas akhir ini, maka dibuatlah suatu sistematika penulisan yang bertujuan untuk memperjelas isi dari setiap bab sebagai berikut :

BAB I. PENDAHULUAN

Pada Bab ini menjelasakan mengenai latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat dari topik yang diangkat berupa sistem klasifikasi *botnet* pada jaringan IoT menggunakan algoritma ANN.

BAB II. TINJAUAN PUSTAKA

Pada bab ini berisikan beberapa *literature riview* yang berhubungan dengan masalah klasifikasi *botnet* dengan

menggunakan algoritma ANN yang mengacu pada beberapa penelitian sebelumnya.

BAB III. METODOLOGI PENELITIAN

Pada bab ini menjelasakan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini meliputi tahapan-tahapan yang dilakukan untuk mempersiapkan data *botnet* dan normal, Penerapan algoritma *autoencoder* dan ANN serta model yang digunakan sehingga tujuan dari penulis tercapai.

BAB IV. ANALISA DAN PEMBAHASAN

Pada bab ini menjelaskan hasil yang telah diperoleh pada tahap sebelumnya, data yang diuji akan dianalisa menggunakan berbagai macam teknik serta validasi hasil.

BAB V. KESIMPULAN

Pada bab ini berisi penjelasan mengenai kesimpulan dan hasil yang diperoleh, serta merupakan jawaban yang diperoleh dari tujuan yang ingin dicapai.

Daftar Pustaka

[1] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[2] T. Fan and Y. Chen, "A scheme of data management in the Internet of Things," in *2010 2nd IEEE InternationalConference on Network Infrastructure and Digital Content*, 2010, pp. 110–114.

[3] Y. Chen and T. Kunz, "Performance evaluation of IoT protocols under a constrained wireless access network," in *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)*, 2016, pp. 1–7.

[4] J. S. Komputer, F. I. Komputer, and U. Sriwijaya, "Deteksi serangan denial of service menggunakan rule based signature analysis pada jaringan internet of things," 2018.

[5] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, and S. Nõmm, "MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network," *ICISSP 2020 - Proc. 6th Int. Conf. Inf. Syst. Secur. Priv.*, no. February, pp. 207–218, 2020, doi: 10.5220/0009187802070218.

[6] Y. Meidan *et al.*, "N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, 2018, doi: 10.1109/MPRV.2018.03367731.

[7] A. A. Ahmed, "Botnet Detection Using a Feed-Forward Backpropagation Artificial Neural Network," in *International Conference on Computational Intelligence in Information System*, 2018, pp. 24–35.

[8] V. G. T. Da Costa, S. Barbon, R. S. Miani, J. J. P. C. Rodrigues, and B. B. Zarpelao, "Detecting mobile botnets through machine learning and system calls analysis," *IEEE Int. Conf. Commun.*, 2017, doi: 10.1109/ICC.2017.7997390.

[9] A. A. Ahmed, W. A. Jabbar, A. S. Sadiq, and H. Patel, "Deep learning-based classification model for botnet attack detection," *J. Ambient Intell. Humaniz. Comput.*, no. 0123456789, 2020, doi: 10.1007/s12652-020-01848-9.

[10] N. Afifah, D. Stiawan, and S. Nurmaini, "The Implementation of Deep Neural Networks Algorithm for Malware Classification," *Comput. Eng. Appl.*, vol. 8, no. 3, pp. 189–202, 2019.

[11] R. (universitas S. HUSNA, *ANALISA PENDETEKSIAN BOTNET MENGGUNAKAN METODE K-MEDOIDS CLUSTERING*. 2017.

[12] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," *Proc. Int. Jt. Conf. Neural Networks*, vol. 2018-July, pp. 1–8, 2018, doi: 10.1109/IJCNN.2018.8489489.

[13] D. N. Fuadin, D. Pembimbing, P. Magister, D. T. Elektro, and F. T. Elektro, "Deteksi Botnet Menggunakan Naïve Bayes," *Thesis Fuadin, Didin Nizarul*, 2017.

[14] D. Zhao *et al.*, “Botnet detection based on traffic behavior analysis and flow intervals,” *Comput. Secur.*, vol. 39, no. PARTA, pp. 2–16, 2013, doi: 10.1016/j.cose.2013.04.007.
[15] K. Angrishi, “Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets,” pp. 1–17, 2017, [Online]. Available: http://arxiv.org/abs/1702.03681.
[16] R. Vishwakarma and A. K. Jain, “A survey of DDoS attacking techniques and defence mechanisms in the IoT network,” *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, 2020, doi: 10.1007/s11235-019-00599-z.
[17] M. Antonakakis *et al.*, “Understanding the Mirai Botnet This paper is included in the Proceedings of the Understanding the Mirai Botnet,” *USENIX Secur.*, pp. 1093–1110, 2017, [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.
[18] “New Vicious Torii IoT Botnet Discovered.” .
[19] A. Naway and Y. Li, “Android Malware Detection Using Autoencoder,” pp. 1–9, 2019, [Online]. Available: http://arxiv.org/abs/1901.07315.
[20] Y. N. Kunang, S. Nurmaini, D. Stiawan, A. Zarkasi, and F. Jasmir, “Automatic Features Extraction Using Autoencoder in Intrusion Detection System,” *Proc. 2018 Int. Conf. Electr. Eng. Comput. Sci. ICECOS 2018*, vol. 17, pp. 219–224, 2019, doi: 10.1109/ICECOS.2018.8605181.
[21] M. Inthachot, V. Boonjing, and S. Intakosum, “Artificial Neural Network and Genetic Algorithm Hybrid Intelligence for Predicting Thai Stock Price Index Trend,” *Comput. Intell. Neurosci.*, vol. 2016, 2016, doi: 10.1155/2016/3045254.
[22] C. Pascariu and I. D. Barbu, “Dynamic analysis of malware using artificial neural networks : Applying machine learning to identify malicious behavior based on parent process hierarchy,” *Proc. 9th Int. Conf. Electron. Comput. Artif. Intell. ECAI 2017*, vol. 2017-Janua, pp. 1–8, 2017, doi: 10.1109/ECAI.2017.8166505.
[23] C. Nwankpa, W. Ijomah, A. Gachagan, and S. Marshall, “Activation Functions: Comparison of trends in Practice and Research for Deep Learning,” pp. 1–20, 2018, [Online]. Available: http://arxiv.org/abs/1811.03378.
[24] V. B. Sriwijaya), “KLASIFIKASI BEAT EKG SECARA DEEP LEARNING MENGGUNAKAN AUTOENCODER DAN DEEP NEURAL NETWORK,” vol. lim, no. 2009, pp. 1–25, 2019.
[25] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.
[26] J. Patterson and A. Gibson, *Deep learning: A practitioner’s approach*. “ O’Reilly Media, Inc.,” 2017.
[27] I. D. Maysanjaya, “Klasifikasi Pneumonia pada Citra X-rays Paru-paru dengan Convolutional Neural Network (Classification of Pneumonia Based on Lung X-rays Images using Convolutional Neural Network),” vol. 9, no. 2, pp. 190–195, 2020.
[28] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” *arXiv Prepr. arXiv1412.6980*, 2014.
[29] A. Luque, A. Carrasco, A. Martín, and A. De Las Heras, “The impact of class imbalance in classification performance metrics based on the binary

confusion matrix," *Pattern Recognit.*, vol. 91, pp. 216–231, 2019, doi: 10.1016/j.patcog.2019.02.023.
[30] T. C. W. Landgrebe and R. P. W. Duin, "Efficient multiclass ROC approximation by decomposition via confusion matrix perturbation analysis," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, no. 5, pp. 810–822, 2008, doi: 10.1109/TPAMI.2007.70740.
[31] M. Lannon, "A balanced approach to investing," *Eng. Aust.*, vol. 73, no. 2, p. 36, 2001.
[32] K. H. Brodersen, C. Soon Ong, K. E. Stephan, and J. M. Buhmann, "The balanced accuracy and its posterior distribution," 2010, doi: 10.1109/ICPR.2010.764.
[33] A. H. Lashkari, G. Draper-Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of Tor Traffic using Time based Features.," in *ICISSP*, 2017, pp. 253–262.
[34] J. Alsamiri and K. Alsubhi, "Internet of things cyber attacks detection using machine learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, pp. 627–634, 2019, doi: 10.14569/ijacsa.2019.0101280.
[35] M. M. Rasheed, A. K. Faieq, and A. A. Hashim, "Android Botnet Detection Using Machine Learning," *Ingénierie des systèmes d Inf.*, vol. 25, no. 1, pp. 127–130, 2020, doi: 10.18280/isi.250117.