DETEKSI SERANGAN *MALWARE BOTNET* MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE*

SKRIPSI

OLEH:

KRISNA AGUSTINI

09011382025122

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI SERANGAN *MALWARE BOTNET* MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

KRISNA AGUSTINI

09011382025122

Palembang, 26 Juni 2024

Pembimbing I Tugas Akhir	Pembimbing II Tugas Akhir
Prof. Deris Stiawan, M.T., Ph.D.	**Nurul Afifah, M.Kom.**
NIP.197806172006041002	NIP.199211102023212049

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

LEMBAR PERSETUJUAN

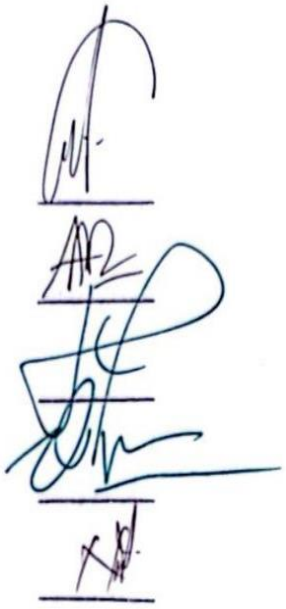
Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 17 Mei 2024

Tim Penguji :

1. Ketua : Dr. Ahmad Zarkasi, M.T.
2. Sekretaris : Aditya Putra Perdana Prasetyo, M.T.
3. Penguji : Huda Ubaya, M.T.
4. Pembimbing I : Prof. Deris Stiawan, M.T., Ph.D.
5. Pembimbing II : Nurul Afifah, M.Kom.



Mengetahui, 26/6/24

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	:	Krisna Agustini
NIM	:	09011382025122
Judul	:	Deteksi Serangan Malware Botnet Menggunakan Metode Support Vector Machine

Hasil Pengecekan Software *iThenticate/Turnitin* : 10%

Menyataka bahwa laporan tugas akhir saya merupaka hasil karya 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, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, Juni 2024

Menyatakan

Krisna Agustini

NIM. 09011382025122

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini yang berjudul *"*Deteksi Serangan *Malware Botnet* Menggunakan Metode *Support Vector Machine".*

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 mengambil berdasarkan hasil penelitian serta observasi dari berbagai sumber literatur yang mendukung dalam penulisan Tugas Akhir ini.

Atas selesainya Tugas Akhir ini, penulis mengucapkan rasa syukur kepada Tuhan Yang Maha Esa, dan juga terima kasih kepada yang terhormat:

1. Kedua Orang Tua dan Keluarga tercinta yang selalu mendoakan serta memberikan dukungan dan semangat yang besar selama penyelesaian Tugas Akhir ini.
2. Bapak Prof. Dr. Erwin, S.Si., M.Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Firdaus, M. Kom., selaku Dosen Pembimbing Akademik.
5. Bapak Prof. Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing I Tugas Akhir.
6. Ibu Nurul Afifah, M.Kom., Dosen Pembimbing II Tugas Akhir.
7. Mba Sari selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya yang tidak bisa saya sebutkan satu persatu.
9. Sahabat tercinta saya Siti Khaeronisyah dan Cynthia Anggraeni yang selalu mendoakan, membantu, mendukung, serta selalu memberikan semangat yang besar kepada penulis.

10. Seluruh teman-teman seperjuangan Angkatan 2020 Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
11. Seluruh pihak yang tidak dapat penulis sebutkan satu persatuyang telah memberikan doa dan bantuan dalam penyelesaian Tugas Akhir ini.
12. Almamater Universitas Sriwijaya.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Tugas Akhir ini. Oleh karena itu, segala saran dan kritik sangatla penting bagi penulis. Akhir kata, semoga Tugas Akhir ini dapat bermanfaat dan berguna bagi Akademik.

Palembang, Juni 2024
Penulis,

Krisna Agustini
NIM. 09011382025122

DETEKSI SERANGAN MALWARE BOTNET MENGGUNAKAN METODE SUPPORT VECTOR MACHINE

Krisna Agustini (09011382025122)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: 09011382025122@student.unsri.ac.id

ABSTRAK

Botnet merupakan kumpulan perangkat yang terinfeksi *malware* dan dikendalikan secara eksternal oleh penyerang untuk melakukan serangan jaringan, seperti serangan *ddos*, pencurian data, atau penyebaran *spam*. Pada penelitian ini menggunakan dataset dari CICIoT2023 yang terdiri dari tiga jenis kelas yaitu, *benign traffic*, *mirai greip flood*, dan *mirai udpplain* untuk mendeteksi serangan *malware botnet* dengan menggunakan metode *Support Vector Machine*. Pada metode *Support Vector Machine* menggunakan tiga jenis kernel yaitu, kernel Linear, Polynomial, dan RBF. Hasil dari penelitian ini membuktikan bahwa metode *Support Vector Machine* menggunakan kernel RBF mampu dalam mendeteksi serangan *malware botnet* dengan mencapai performa terbaik dengan tingkat *accuracy* sebesar 98.25%, *precision* sebesar 98.58%, *recall* sebesar 96.52%, dan *f1-score* sebesar 97.54%.

Kata Kunci : *Botnet Detection,* CICIoT2023, RBF, *Support Vector Machine*

DETECTION OF BOTNET MALWARE ATTACKS USING THE SUPPORT VECTOR MACHINE METHOD

Krisna Agustini (09011382025122)
Department of Computer Systems, Faculty of Computer Science
Sriwijaya University
Email: 09011382025122@student.unsri.ac.id

ABSTRACT

A botnet is a collection of devices infected with malware and controlled externally by an attacker to carry out network attacks, such as DDoS attacks, data theft, or spreading spam. This research uses a dataset from CICIoT2023 which consists of three types of classes, namely, tame traffic, mirai greip flood, and mirai udpplain to detect botnet malware attacks using the Support Vector Machine method. The Support Vector Machine method uses three types of kernels, namely, Linear, Polynomial and RBF kernels. The results of this research prove that the Support Vector Machine method using the RBF kernel is capable of detecting botnet malware attacks by achieving the best performance with an accuracy rate of 98.25%, precision of 98.58%, recall of 96.52%, and f1-score of 97.54%.

Kata Kunci : *Botnet Detection,* CICIoT2023, RBF, *Support Vector Machine*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Botnet merupakan kumpulan perangkat yang terinfeksi *malware* dan dikendalikan secara eksternal oleh penyerang untuk melakukan serangan jaringan, seperti serangan ddos, pencurian data, atau penyebaran *spam*. *Botnet* biasanya terdiri dari ribuan hingga jutaan perangkat yang terhubung ke internet, seperti komputer, server, atau perangkat IoT yang secara diam-diam dikendalikan oleh penyerang untuk mencapat tujuan jahat mereka [1].

Dalam sepuluh tahun terakhir, *botnet* telah berkembang menjadi ancaman serius bagi jaringan komputer dan komunikasi. *Botnet* adalah kumpulan perangkat yang terinfeksi yang dikelola oleh pihak ketiga yang dikenal sebagai "botmaster"[2]. *Malware* ini sering kali secara diam-diam menyusup ke dalam jaringan dari waktu ke waktu dengan menduplikasi dirinya sendiri sebelum menerima instruksi dari botmaster untuk meluncurkan serangan. *Bonet* dirancang untuk menimbulkan kekacauan dan menyebabkan penyediaan layanan berhenti beroperasi. Ada beberapa jenis *botnet* yang berbeda, termasuk *bashlite, mirai, tori, okiru,* dan *kenjiro*. Dalam beberapa tahun terakhir, banyak penelitian telah dilakukan pada *botnet* [3].

Dalam penelitian [4], menggunakan *machine learning* untuk mendeteksi serangan botnet pada perangkat IoT menggunakan dataset UNSW-NB15. Penelitian ini mencakup eksplorasi data, pengembangan model *machine learning*, dan analisis perbandingan dari berbagai model *machine learning*. Hasilnya menunjukkan bahwa model *decision tree* mendapatkan akurasi tertinggi sebesar 94%.

Penelitian ini [5], melakukan pengembangan model *machine learning* dalam mendeteksi *botnet* dalam IIoT dengan menggunakan dataset dari N-BaIoT. Model *machine learning* ini menggunakan algoritma pemilihan fitur yang baru dan pengklasifikasi jaringan saraf yang dioptimalkan dalam mendeteksi serangan

botnet. Hasilnya menunjukan bahwa model FGOA-KKN mendapatkan akurasi sebesar 98.7% dalam mendeteksi serangan *botnet* dalam lingkungan IIoT.

Dalam penelitian [6], disarankan bagaimana menggunakan pembelajaran mesin untuk menemukan serangan *botnet*. Penelitian ini menggunakan 2,5 juta catatan dari dataset dari BIoT dan UNSW-NB15 yang diklasifikasikan sebagai lalu lintas jaringan serangan atau lalu lintas biasa. *Naive Bayes, K-Nearest Neighbor*, SVM, dan *Decision Tree* adalah teknik *Machine Learning* yang digunakan. Menurut temuan penelitian, pendekatan *Decision Tree* (DT) memiliki kinerja terbaik dalam mengidentifikasi serangan *botnet*.

Dalam penelitian [7], melakukan pengembangan kerangka kerja multilayer untuk deteksi botnet dengan menggunakan dataset dari CTU-13. Penelitian ini berfokus pada analisis berbasis perilaku dan fitur berbasis aliran yang efektif dalam mendeteksi lalu lintas botnet. Didapatkan performa K-NN 91.51% dan algoritma SVM mendapatkan akurasi sebesar 85%. Sehingga disimpulkan bahwa algoritma K-NN memiliki performa terbaik dalam mendeteksi aktivitas botnet dalam lalu lintas jaringan.

Dalam penelitian [8], dibahas bagaimana menggunakan pendekatan BD-PSO-V (*Binary Discrete Particle Swarm Optimization with Voting*) untuk menganalisa dampak dari serangan yang tidak bersahabat terhadap akurasi deteksi sistem. Pendekatan BD-PSO-V dapat mengidentifikasi *botnet* dengan tingkat akurasi yang tinggi.

Penggunaan metode *machine learning* untuk mengidentifikasi lalu lintas *botnet* dibahas dalam penelitian [9]. Ketika kinerja algoritme *Random Forest* (RF) dan *Decision Tree* (DT) dievaluasi, para peneliti menemukan bahwa akurasi RF lebih tinggi. Juga melihat bagaimana memasukkan alamat IP dan port dalam penelitian ini akan mempengaruhi hasil dan menemukan bahwa hal itu akan meningkatkan akurasi tetapi mengurangi F1-Score. Penelitian ini menekankan betapa pentingnya untuk memperhitungkan berbagai fitur untuk berbagai jenis lalu lintas *botnet*. Penelitian ini dapat digunakan sebagai dasar untuk pembuatan model *machine learning* yang lebih baik di masa depan untuk mengidentifikasi dan menghentikan serangan *botnet*.

Penelitian ini [10], membahas tentang penggunaan pendekatan *machine learning* berbasis graf untuk deteksi *botnet*, dengan fokus pada pemilihan fitur, evaluasi fitur, dan perbandingan kinerja model. Penelitian ini mencoba untuk mengatasi masalah komputasi yang mahal dalam analisis payload dan kebutuhan untuk memilih fitur yang paling diskriminatif untuk meningkatkan kinerja algoritma machine learning. Metode yang digunakan dalam penelitian ini meliputi *logistic regression*, *support vector machine*. Hasil dari penelitian ini adalah pengembangan pendekatan deteksi *botnet* berbasis graf menggunakan pendekatan pembelajaran mesin. Model yang diusulkan mampu mengatasi beberapa keterbatasan teknik deteksi *botnet* yang ada dan memberikan hasil yang menjanjikan dalam hal tingkat deteksi, kompleksitas model, dan ketahanan terhadap serangan zero-day.

Bedasarkan uraian diatas, penulis akan melakukan deteksi *malware botnet* dengan menggunakan dataset yang berbentuk .pcap yang akan diekstraksi menjadi bentuk .csv dan menggunakan *machine learning* sebagai bahan analisa yang dapat digunakan sebagai referensi. Maka dari itu penulis akan melakukan penelitian dengan judul **Deteksi Serangan *Malware Botnet* Menggunakan Metode *Support Vector Machine*.**

1.2 Rumusan Masalah

Berdasarkan penulisan latar belakang masalah yang ada. Adapun permasalahan yang akan dibahas pada penelitian ini meliputi:

1. Bagaimana proses ekstraksi dataset *malware botnet*?
2. Bagaimana teknik *random undersampling* diterapkan pada kumpulan data yang tidak seimbang?
3. Bagaimana cara model *support vector machine* digunakan untuk mendeteksi *malware botnet*?

1.3 Batasan masalah

Batasan masalah dalam penulisan penelitian tugas akhir ini adalah sebagai berikut:

1. Dataset yang digunakan adalah dataset CICIoT2023.

2. Melakukan deteksi serangan *malware botnet mirai* dengan menggunakan algoritma *support vector machine.*
3. Serangan *botnet* yang dibahas adalah *malware mirai*.
4. Tidak ada pembahasan mengenai pencegahan serangan *botnet* pada penelitian ini.

1.4 Tujuan

Berdasarkan penulisan latar belakang dan rumusan masalah yang telah ditulis sebelumnya, adapun tujuan yang ingin dicapai dalam penulisan Tugas Akhir ini adalah sebagai berikut:

1. Melakukan ekstraksi dataset yang berbentuk .pcap menjadi .csv menggunakan *CICFlowMeter* pada kalilinux.
2. Menerapkan teknik *random undersampling* pada data yang tidak seimbang untuk proses deteksi serangan *malware botnet*.
3. Melakukan evaluasi performa algoritma *support vector machine* dalam mendeteksi serangan *malware botnet*.

1.5 Manfaat

Adapun manfaat dari penelitian tugas akhir ini antara lain adalah:

1. Memahami proses ekstraksi dataset menggunakan *CICFlowMeter* pada kalilinux.
2. Memberikan solusi terhadap ketidakseimbangan data, memastikan deteksi yang akurat dan handal terhadap serangan *malware botnet*.
3. Mengevaluasi seberapa baik model *support vector machine* dalam mendeteksi.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian Tugas Akhir ini akan melalui beberapa tahapan, yaitu:

1. Tahap Pertama Studi Pustaka/Studi Literatur

Tahap ini dilakukan setelah masalah yang didapatkan telah sesuai untuk dijadikan sebagai penelitian, membaca artikel, jurnal atau makalah yang berhubungan dengan tugas akhir.

2. Tahap Kedua Perancangan Sistem

   Tahap kedua ini akan membahas masalah proses bagaimana sistem tersebut di rancang dan di bangun untuk deteksi *botnet* menggunakan algoritma *Support Vector Machine*.

3. Tahap Pengujian

   Pada tahap ini dilakukan pengujian berdasarkan metode yang digunakan dalam penelitian dan metode-metode yang digunakan oleh penelitian sebelumnya, sehingga didapatan hasil yang sesuai

4. Analisa

   Tahap ini dilakukan pengolahan data dan analisa data yang didapatkan dari hasil pengujian yang dilakukan sebelumnya untuk mendapatkan data yang aktual. Kemudian hasil akan dianalisis dengan tujuan untuk mengetahui kekurangan pada hasil perancangan sistem tersebut.

5. Kesimpulan

   Tahapan ini merupakan langkah akhir, hasil dari semua langkah yang dilakukan sebelumnya akan dirumuskan menjadi suatu kesimpulan.

1.7 Sistematika Penulisan

Agar dapat mempermudah proses penyusunan dan memperjelas isi dari setiap bab maka akan dibuat sistematika dalam penulisan yaitu sebagai berikut:

BAB I PENDAHULUAN

Berisi penjelasan secara singkat dan sistematis mengenai topik-topik dalam penelitian yang meliputi latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan metodologi penelitian dan terakhir sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan mengenai beberapa literature review yang berhubungan dengan masalah deteksi *botne*t dengan menggunakan algoritma *Support Vector Machine* yang mengacu pada penelitian sebelumnya.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan mengenai bab ini meliputi tahapan-tahapan yang akan dilakukan serta mempersiapkan data *botnet* dan *normal*, penerapan algoritma *support vector machine* serta model yang akan digunakan sehingga tujuan dari penulis tercapai.

BAB IV HASIL DAN ANALISA

Pada bab ini menjelaskan hasil yang telah diperoleh pada tahap sebelumnya, serta analisa data yang didapat dari hasil pengujian.

BAB V KESIMPULAN

Bab ini berisikan kesimpulan tentang hasil pengujian yang telah dilakukan, serta merupakan jawaban yang diperoleh dari tujuan yang ingin dicapai, dan berisikan saran-saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] E. Carlos *et al.*, "CICIoT2023 : A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," 2023.

[2] M. Austin, "IoT Malicious Traffic Classification Using Machine Learning IoT Malicious Traffic Classification Using Machine Learning," 2021.

[3] C. D. Mcdermott, F. Majdani, and A. V Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," no. August, 2018, doi: 10.1109/IJCNN.2018.8489489.

[4] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, "Botnet Attack Detection in IoT Using Machine Learning," vol. 2022, 2022.

[5] F. Taher, S. Member, M. Abdel-salam, M. Elhoseny, S. Member, and I. M. El-hasnony, "Reliable Machine Learning Model for IIoT Botnet Detection," *IEEE Access*, vol. 11, no. March, pp. 49319–49336, 2023, doi: 10.1109/ACCESS.2023.3253432.

[6] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou, and F. Aloul, "Botnet Attack Detection using Machine Learning," no. February, 2021, doi: 10.1109/IIT50501.2020.9299061.

[7] W. A. N. Nur, H. Ibrahim, and S. Anuar, "Multilayer Framework for Botnet Detection Using Machine Learning Algorithms," pp. 48753–48768, 2021.

[8] M. Asadi, M. Ali, J. Jamali, D. Ph, and S. Parsa, "Detecting botnet by using particle swarm optimization algorithm based on voting system," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 95–111, 2020, doi: 10.1016/j.future.2020.01.055.

[9] R. Abrantes, P. Mestre, and A. Cunha, "ScienceDirect ScienceDirect Exploring Exploring Dataset Dataset Manipulation Manipulation via via Machine Machine Learning Learning for Botnet Traffic for Botnet Traffic,"

Procedia Comput. Sci., vol. 196, no. 2021, pp. 133–141, 2022, doi: 10.1016/j.procs.2021.11.082.

[10] A. Alharbi and K. Alsubhi, "Botnet Detection Approach Using Graph-Based Machine Learning," *IEEE Access*, vol. 9, pp. 99166–99180, 2021, doi: 10.1109/ACCESS.2021.3094183.

[11] C. Chen, A. Using, B. Language, M. A. Mohammed, S. M. Kadhem, and A. Ali, "Botnets Attack Detection Using Machine Learning Approach for IoT Environment Botnets Attack Detection Using Machine Learning Approach for IoT Environment," 2020, doi: 10.1088/1742-6596/1646/1/012101.

[12] I. Journal *et al.*, "IoT botnet detection using machine learning," vol. 6, no. March, pp. 5952–5962, 2022.

[13] M. Motylinski, Á. Macdermott, F. Iqbal, and B. Shah, "Computers & Security A GPU-based machine learning approach for detection of botnet attacks," *Comput. Secur.*, vol. 123, p. 102918, 2022, doi: 10.1016/j.cose.2022.102918.

[14] "BOTNETs A Network Security Issue.pdf."

[15] H. Alzahrani, M. Abulkhair, and E. Alkayal, "A Multi-Class Neural Network Model for Rapid Detection of IoT Botnet Attacks," vol. 11, no. 7, 2020.

[16] M. Palt and M. Palt, "ScienceDirect The Proposal of Undersampling Method for Learning from The Proposal of Undersampling Method for Learning from Imbalanced Datasets Imbalanced Datasets," *Procedia Comput. Sci.*, vol. 159, pp. 125–134, 2019, doi: 10.1016/j.procs.2019.09.167.

[17] A. Vaidya, M. Pande, S. Shankrod, T. Dorkar, and P. S. Aundhakar, "DETECTION OF MALWARE USING SVM," vol. 868, no. 03, pp. 2926–2931, 2023.

[18] M. Yang, X. Chen, Y. Luo, and H. Zhang, "An Android Malware Detection Model Based on DT-SVM," vol. 2020, 2020.

[19] K. Sahoo, A. K. Samal, J. Pramanik, and S. K. Pani, “Exploratory Data Analysis using Python,” vol. 3075, no. 12, pp. 4727–4735, 2019, doi: 10.35940/ijitee.L3591.1081219.

[20] F. Kotob, “What Is Sustainability?,” no. November 2011, 2015.

[21] S. Tang, S. Yuan, and Y. Zhu, “Data Preprocessing Techniques in Convolutional Neural Network Based on Fault Diagnosis Towards Rotating Machinery,” pp. 149487–149496, 2020, doi: 10.1109/ACCESS.2020.3012182.

[22] M. Nour, H. Sindi, and K. Polat, “Biomedical Datasets,” vol. 2020, 2020.