DETEKSI SERANGAN *MALWARE BOTNET* MENGGUNAKAN METODE *K-NEAREST NEIGHBOR*

SKRIPSI

OLEH:

SITI KHAERONISYAH

09011382025125

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI SERANGAN *MALWARE BOTNET* MENGGUNAKAN METODE *K-NEAREST NEIGHBOR*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

SITI KHAERONISYAH

09011382025125

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. H. 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	:	Siti Khaeronisyah
NIM	:	09011382025125
Judul	:	Deteksi Serangan Malware Botnet Menggunakan Metode K-Nearest Neighbor

Hasil Pengecekan Software *iThenticate/Turnitin* : 7%

Menyatakan bahwa laporan tugas akhir saya merupakan 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

Siti Khaeronisyah

NIM. 09011382025125

KATA PENGANTAR

Puji dan Syukur atas kehadirat Allah Subnahu Wa Ta'ala, atas segala karunia dan Rahmat-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul" Deteksi Serangan *Malware Botnet* Menggunakan Metode *K-Nearest Neighbor*"

Tujuan dari penelitian Tugas Akhir ini adalah untuk melengkapi salah satu syarat dalam 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 Allah subhanahu Wa Ta'ala Tuhan yang Maha Esa, dan juga terima kasih kepada yang terhormat:

1. Kedua orang tua tercinta bunda dan bapak, dan kakak ku tercinta yang selalu memberikan do'a, restu, serta dukungan yang sangat 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. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

4. Bapak Huda Ubaya, S.Kom., M.T., selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer.

5. Bapak Prof. Deris Stiawan, M.T., Ph.D., selaku Dosen Pembimbing I Tugas Akhir.

6. Ibu Nurul Afifah, M.Kom., selaku Dosen Pembimbing II Tugas Akhir.

7. Mba Sari Nuzulastri selaku Admin Jurusan Sistem Komputer yang telah membantu administrasi dalam menyelesaikan Tugas Akhir.

8. Seluruh dosen, Staff, serta Karyawan Fakultas Ilmu Komputer Universitas

Sriwijaya yang tidak bisa saya sebutkan satu persatu.

9. Sahabat seperjuangan tercinta, Krisna Agustini dan Cynthia Anggraeni yang selalu mendo'akan, membantu, serta memberikan semangat dan motivasi selama masa perkuliahan hingga proses penyelesaian Tugas Akhir.

10. Sahabat saya tercinta, Agustini Viani dan Nahrisyah yang selalu mendo'akan, serta memberikan semangat dan motivasi selama proses penyelesaian Tugas Akhir ini.

11. Sahabat saya selama masa perkuliahan Virginita Putri Lestari, Risky Wahyuni dan Indah Ria Andina yang selalu mendoakan, membantu, mendukung, serta selalu memberikan semangat yang besar kepada penulis.

12. Seluruh teman-teman seperjuangan Angkatan 2020 Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

13. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat serta Do'anya dalam penyelesaian Tugas Akhir.

14. Almamater Universitas Sriwijaya.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Tugas Akhir ini. Oleh karena itu, Segala saran dan Kritik sangatlah penting bagi penulis, Akhir kata, semoga Tugas Akhir ini dapat bermanfaat dan berguna bagi Khalayak.

Palembang, Juni 2024

Penulis,

Siti Khaeronisyah

09011382025125

DETEKSI SERANGAN MALWARE BOTNET MENGGUNAKAN METODE K-NEAREST NEIGHBOR

Siti Khaeronisyah (09011382025125)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: 09011382025125@student.unsri.ac.id

ABSTRAK

Botnet Mirai adalah jaringan komputer yang terdiri dari ribuan atau jutaan perangkat terhubung ke internet yang telah diretas oleh *malware mirai*. Tujuan dari *Botnet Mirai* adalah untuk mengendalikan perangkat *Internet of Things* (IoT) dengan keamanan yang lemah untuk menginfeksi perangkat dan mengubahnya menjadi *botnet* yang dapat menargetkan perangkat lain melalui serangan *Distributed Denial of Service* (DDoS) yang dapat melumpuhkan layanan web. 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 *K-Nearest Neighbor.* Hasil dari penelitian ini menunjukkan bahwa metode *K-Nearest Neighbor* menggunakan nilai k=12 mampu dalam mendeteksi serangan *malware botnet* dengan mencapai performa terbaik dengan tingkat *accuracy* sebesar 98.50%, *precision* sebesar 98.19%, *recall* sebesar 96.46%, dan *f1-score* sebesar 97.32%.

Kata Kunci : *Botnet Mirai, Botnet Detection,* CICIoT2023, *K-Nearest Neighbor*

BOTNET MALWARE ATTACK DETECTION USING *K-NEAREST NEIGHBOR* METHOD

Siti Khaeronisyah (09011382025125)
Department of Computer Systems, Faculty of Computer Science,
Sriwijaya University
Email: 09011382025125@student.unsri.ac.id

ABSTRACT

A *Mirai Botnet* is a computer network consisting of thousands or millions of internet connected devices that have been hacked by the *mirai malware*. The purpose of the *Mirai Botnet* is to control *Internet of Things* (IoT) devices with weak security to infect the device and turn it into a botnet that can target other devices through *Distributed Denial of Service* (DDoS) attacks that can paralyze web services. This study uses a dataset from CICIoT2023 which consists of three types of classes namely *benign traffic*, *mirai greip flood*, and *mirai udpplain* to detect *botnet malware* attacks using the *K-Nearest Neighbor* method. The results of this study show that the *K-Nearest Neighbor* method using the k=12 value is able to detect *botnet malware* attacks by achieving the best performance with an accuracy rate of 98.50%, precision of 98.19%, recall of 96.46%, and f1-score of 97.32%.

Keywords : *Botnet Mirai, Botnet Detection,* CICIoT2023, *K-Nearest Neighbor*

DAFTAR ISI

Halaman

LEMBAR PENGESAHAN ..... **ii**

LEMBAR PERSETUJUAN ..... **iii**

HALAMAN PERNYATAAN ..... **iv**

KATA PENGANTAR ..... **iv**

ABSTRAK ..... **vii**

ABSTRACT ..... **viii**

DAFTAR ISI ..... **ix**

DAFTAR GAMBAR ..... **xi**

DAFTAR TABEL ..... **xiii**

BAB I PENDAHULUAN **1**

1.1 Latar Belakang 1

1.2 Perumusan Masalah 3

1.3 Batasan Masalah 4

1.4 Tujuan 4

1.5 Manfaat 4

1.6 Metodologi Penelitian 4

1.7 Sistematika Penulisan 5

BAB II TINJAUAN PUSTAKA **7**

2.1 Pendahuluan 8

2.2 *Botnet* 9

2.3 *Botnet Mirai* 10

2.4 Dataset Botnet CICIoT 10

2.5 Karakteristik *Botnet Mirai* 12

2.6 Ekstraksi Data 13

2.7 Undersampling 13

2.8 K-Nearest Neighbor 15

2.9 Confusion Matrix 16

2.9.1 Confusion Matrix Multiclass 16

BAB III METODOLOGI PENELITIAN 19

3.1 Pendahuluan 19
3.2 Kerangka Kerja Penelitian..... 19
3.3 Kerangka Kerja Metodologi Penelitian 21
3.4 Dataset 22
3.5 Ekstraksi Data..... 22
3.6 Exploratory Data Analysis..... 23
3.7 Preprocessing..... 23
3.7.1 Feature Selection..... 23
3.7.2 Data Encoding..... 24
3.8 Undersampling 26
3.9 Algoritma K-Nearest Neighbor 27
3.10 Validasi 28

BAB IV HASIL DAN ANALISA 29

4.1 Pendahuluan 29
4.2 Analisis Dataset 29
4.3 Dataset 33
4.4 Ekstraksi Data..... 34
4.5 Exploratory Data Analysis..... 36
4.6 Preprocessing..... 38
4.6.1 Feature Selection..... 38
4.6.2 Data Encoding..... 38
4.7 Undersampling 39
4.8 Hasil Pengujian *K-Nearest Neighbor* 41
4.9 Hasil Validasi..... 44

BAB V KESIMPULAN DAN SARAN 51

5.1 Kesimpulan..... 51
5.2 Saran 51

DAFTAR PUSTAKA.....52

DAFTAR GAMBAR

Halaman

Gambar 2.1 Topologi Jaringan pada Dataset 12
Gambar 2.2 *K-Nearest Neighbor* 16
Gambar 3.1 Kerangka Kerja Penelitian 20
Gambar 3.2 Kerangka Kerja Metodologi Penelitian..... 21
Gambar 3.3 Bentuk Dataset 22
Gambar 3.4 Flowchart *Undersampling*..... 26
Gambar 3.5 Flowchart algoritma *K-Nearest Neighbor*..... 27
Gambar 4.1 Data pcap normal 29
Gambar 4.2 Data pcap *greip flood*..... 30
Gambar 4.3 Data pcap *udpplain*..... 30
Gambar 4.4 Virus Total Normal 32
Gambar 4.5 Virus Total *Mirai* 33
Gambar 4.6 Data *Benign* dan *Botnet Mirai*..... 33
Gambar 4.7 Proses Ekstraksi Data..... 35
Gambar 4.8 Hasil Ekstraksi Data..... 35
Gambar 4.9 Visualisasi data..... 36
Gambar 4.10 Distribusi Fitur 37
Gambar 4.11 Hasil Seleksi Fitur..... 38
Gambar 4.12 Hasil Encoding dengan Label Encoder..... 38
Gambar 4.13 *Undersampling*..... 39
Gambar 4.14 Membagi dataset 3 Kelas 40
Gambar 4.15 *k-fold cross validation*..... 41
Gambar 4.16 *K-Nearest Neighbor* 41
Gambar 4.17 *Train_test_split*..... 42
Gambar 4.18 Jumlah tetangga terdekat dalam model KNN 42
Gambar 4.19 Metrik Jarak *Euclidean* 42
Gambar 4.20 Melatih model KNN..... 43
Gambar 4.21 Deteksi model KNN dan akurasi..... 44
Gambar 4.22 Hasil Validasi 80-20% 44
Gambar 4.23 Grafik Akurasi berdasarkan nilai k……..46

Gambar 4.24 Visualisasi Grafik Komparasi 48
Gambar 4.25 *Confusion Matrix*..... 48

DAFTAR TABEL

Halaman

Tabel 2. 1 Penelitian mengenai *malware botnet* beberapa tahun terakhir 7
Tabel 2. 2 Jenis Serangan *Botnet Mirai* 10
Tabel 2. 3 Beberapa perangkat yang terhubung dalam topologi jaringan..... 11
Tabel 2. 4 Penjelasan Karakteristik *Botnet Mirai* 13
Tabel 2. 5 *Confusion Matrix Multiclass*..... 16
Tabel 3. 1 Hasil ekstraksi dataset menggunakan CICFlowMeter 23
Tabel 3. 2 Hyperparameter Validasi 28
Tabel 4. 1 Karakteristik Serangan..... 30
Tabel 4. 2 Hasil Validasi..... 45
Tabel 4. 3 Hasil Hyperameter *K-Nearest Neighbor*..... 45

BAB I
PENDAHULUAN

1.1. Latar Belakang

Serangan *botnet* adalah serangan yang melibatkan penggunaan perangkat IoT yang terinfeksi untuk membentuk sebuah jaringan botnet. Serangan DDoS (Distributed Denial of Service) yang menggunakan botnet berpotensi menggangu sistem target dan melumpuhkan layanan *website*. Serangan botnet ini dapat dilakukan dengan berbagai variasi, seperti serangan g*reip* yang menggunakan protokol GRE untuk mengirimkan serangan dan serangan UDP Plain yang mengirimkan protokol UDP berulang dengan payload yang berbeda untuk setiap paket yang dikirimkan ke sistem target yang bertujuan untuk menghabiskan sumber daya sistem target dan menggangu ketersedian layanan[1]. Pada saat tertentu, bot melakukan kontak dengan server yang jauh untuk menerima instruksi tentang apa yang harus dilakukan penyerang. Untuk mengubah situs web target menjadi sebuah serangan, bot menjalankan tugas-tugas seperti mengirim permintaan ke situs web tersebut. Untuk membuat perangkat IoT mudah dikenali, *Mirai* melakukan pemindahan alamat IP secara luas, yang dapat diakses dengan login *credentials* sehingga mudah diketahui[2].

Selama sepuluh tahun terakhir, *botnet* telah berkembang menjadi ancaman serius bagi jaringan komunikasi dan komputer. Jaringan perangkat yang dikenal sebagai *botnet* dimiliki oleh perangkat lunak jahat dan dikelola oleh *administrator* yang dikenal sebagai *botmaster*. Malware sering kali menyusup ke dalam jaringan secara diam-diam dari waktu ke waktu dengan cara mereplikasi diri, menunggu untuk meluncurkan serangan sampai diarahkan oleh botmaster. *Botnet* dirancang untuk mengganggu layanan dan memaksa penyedia layanan untuk menghentikan operasinya. Jenis *botnet* sangatlah bervariasi yaitu seperti *bashlite, mirai, torii, okiru, kenjiro* dan lainnya. Penelitian mengenai *botnet* telah banyak dilakukan dalam beberapa tahun terakhir ini[3].

Dalam penelitian sebelumnya [4], membahas penggunaan machine learning berbasis GPU untuk mendeteksi serangan *botnet* dalam Internet of Things

(IoT). Pertumbuhan pesat perangkat IoT telah menciptakan kerentanan keamanan baru, dan botnet dirancang untuk mengeksploitasi kerentanan ini. Artikel ini menyajikan metodologi untuk pra-pemrosesan dataset IoT-Bot dan mengklasifikasikan berbagai jenis serangan. Penulis membandingkan hasil yang dicapai dengan versi yang dipercepat oleh GPU dari berbagai pengklasifikasi dan menunjukkan bahwa penggunaan GPU secara signifikan mengurangi waktu pelatihan dan estimasi. Model terbaik yang dilatih mencapai skor tinggi untuk akurasi, presisi, *recall*, dan *f1-score*. Penelitian ini menekankan pentingnya mengamankan perangkat IoT dari serangan botnet dan peran *machine learning* dalam mendeteksi dan mengurangi ancaman ini.

Pada penelitian ini [5], membahas penggunaan algoritma machine learning untuk mendeteksi lalu lintas *botnet*. Peneliti membandingkan kinerja algoritma *Random Forest* (RF) dan *Decision Tree* (CART) dan menemukan bahwa RF memiliki akurasi yang lebih baik. Mereka juga menganalisis dampak inklusi alamat IP dan port dalam analisis dan menemukan bahwa hal tersebut meningkatkan akurasi namun menurunkan *F1-Score*. Hasil penelitian ini dapat menjadi dasar untuk pengembangan model *machine learning* yang lebih baik dalam mendeteksi dan melawan serangan *botnet* di masa depan.

Pada penelitian ini[6], dibahas tentang penggunaan model *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 *logistic regression* mendapatkan akurasi sebesar 78% dan model *decision tree* mendapatkan akurasi sebesar 94% pada dataset yang seimbang.

Pada penelitian ini[7], dibahas tentang pengembangan model *machine learning* yang dapat diandalkan untuk mendeteksi botnet dalam IIoT. Masalah dalam penelitian ini adalah kurangnya fokus pada pengujian model *machine learning* yang diusulkan pada dataset IIoT yang spesifik. Dataset yang digunakan dalam penelitian ini adalah N-BaIoT dataset. Hasil dari penelitian ini adalah pengembangan model *machine learning* yang dapat diandalkan untuk mendeteksi

botnet dalam IIoT. Model yang diusulkan telah menunjukkan kinerja yang unggul dalam mendeteksi serangan *botnet* dalam lingkungan IIoT dengan hasil evaluasi menunjukkan peningkatan akurasi sebesar 96,03% dengan model KNN dibandingkan dengan model sebelumnya. Model ini juga berhasil mengurangi tingkat kesalahan positif dan negatif palsu, menunjukkan keunggulan dalam mendeteksi serangan. Selain itu, penelitian ini juga memberikan kontribusi dalam memperluas literatur tentang deteksi *botnet* dalam IIoT.

Pada penelitian ini [8], dibahas 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*. penelitian ini juga mencakup eksplorasi fitur berbasis graf baru dan penggunaan teknik evaluasi fitur untuk memilih fitur yang paling diskriminatif untuk membangun sistem deteksi *botnet* yang efisien. Hasil dari penelitian ini adalah pengembangan pendekatan deteksi botnet berbasis graf menggunakan pendekatan *machine learning*.

Berdasarkan beberapa ulasan penelitian diatas, penulis akan melakukan deteksi *malware botnet* menggunakan dataset berbentuk pcap yang terlebih dahulu diekstraksi sehingga menjadi csv dan menggunakan *machine learning* sebagai bahan analisa yang dapat digunakan sebagai referensi. Dengan demikian, penulis mengusulkan penelitian dengan judul **Deteksi Serangan *Malware Botnet* Menggunakan Metode *K-Nearest Neighbor***.

1.2 Perumusan Masalah

Berikut adalah rumusan masalah dalam penulisan tugas akhir ini:

1. Bagaimana proses ekstraksi dataset *malware botnet*?
2. Bagaimana teknik *random undersampling* diterapkan pada kumpulan data yang tidak seimbang?
3. Bagaimana cara model *k-nearest neighbor* digunakan untuk mendeteksi *malware botnet*?

1.3 Batasan Masalah

Berikut adalah ruang lingkup masalah dalam penulisan tugas akhir ini:

1. Dataset yang digunakan adalah dataset CICIoT2023.
2. Deteksi serangan *Malware Botnet* Menggunakan Algoritma *K-Nearest Neighbor*.
3. Serangan Botnet yang dibahas adalah *Malware Mirai*.
4. Dalam penelitian ini tidak membahas bagaimana cara pencegahan *botnet.*

1.4 Tujuan

Adapun tujuan dari penulisan tugas akhir ini adalah sebagai berikut:

1. Melakukan proses 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 *K-Nearest Neighbor* dalam mendeteksi serangan *malware botnet.*

1.5 Manfaat

Adapun manfaat dari penelitian tugas akhir ini yang dilakukan antara lain:

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 performa algoritma *k-nearest neighbor* dalam mendeteksi serangan *malware botnet*.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini akan melewati beberapa tahapan sebagai berikut:

1. Tahap Pertama (Studi Pustaka/literature)

Dalam tahap ini dilakukan setelah masalah yang akan dibahas sudah sesuai dengan mencari informasi yang diperlukan melalui media pembelajaran seperti jurnal ilmiah, buku, internet, serta artikel-artikel terkait yang mendukung penulisan Proposal Tugas Akhir ini.

2. Tahap Kedua (Perancangan Sistem)

Pada tahap ini dilakukan penerapan metode pada sistem penelitian. Kemudian, pada tahapan ini juga membangun dan menerapkan metode yang akan digunakan serta menyiapkan *hardware* dan *software* serta melakukan kofigurasi ataupun menulis code untuk penerapan metode ada tugas akhir.

3. Tahap Ketiga (Pengujian)

Dalam tahap ini, peneliti melakukan tahapan pengujian metodologi penelitian dan penelitian sebelumnya sehingga didapatkan data hasil uji yang sesuai dan tepat dengan algoritma.

4. Tahap Keempat (Analisa)

Tahap ini merupakan tahapan menganalisa data hasil pengujian dengan diterapkan pendekatan tertentu, sehingga didapat hasil yang objektif dimana data diperoleh dari pengujian.

5. Tahap Kelima (Kesimpulan dan Saran)

Pada tahap ini akan dilakukan kesimpulan berdasarkan permasalahan, studi pustaka, metodologi penelitian, dan analisa hasil pengujian. Serta saran untuk penulis selanjutnya jika ingin dijadikan referensi.

1.7 Sistematika Penulisan

Adapun sistematika penulisan dalam Tugas Akhir ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Pada bab I akan berisikan latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat serta metodologi penelitian dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada Bab II berisikan mengenai beberapa literature review yang berhubungan dengan masalah deteksi serangan *Malware botnet* dengan menggunakan algoritma *K-Nearest Neighbor* yang mengacu pada penelitian sebelumnya.

BAB III. METODOLOGI PENELITIAN

Pada Bab III 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 *K-Nearest Neighbor* serta model yang akan digunakan sehingga tujuan dari penulis tercapai.

BAB IV. HASIL DAN ANALISA

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

BAB V. KESIMPULAN

Pada bab V 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. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023, doi: 10.3390/s23135941.

[2] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona, "IoDDoS -The internet of distributed denial of sevice attacks A case study of the mirai malware and IoT-Based botnets," *IoTBDS 2017 - Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, no. IoTBDS, pp. 47–58, 2017, doi: 10.5220/0006246600470058.

[3] M. Catillo, A. Pecchia, and U. Villano, "Botnet Detection in the Internet of Things through All-in-one Deep Autoencoding," *ACM Int. Conf. Proceeding Ser.*, no. 8489489, pp. 8–13, 2022, doi: 10.1145/3538969.3544460.

[4] M. Motylinski, Á. MacDermott, F. Iqbal, and B. Shah, "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.

[5] R. Abrantes, P. Mestre, and A. Cunha, "Exploring Dataset Manipulation via Machine Learning for Botnet Traffic," *Procedia Comput. Sci.*, vol. 196, no. 2021, pp. 133–141, 2021, doi: 10.1016/j.procs.2021.11.082.

[6] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, "Botnet Attack Detection in IoT Using Machine Learning," *Comput. Intell. Neurosci.*, vol. 2022, 2022, doi: 10.1155/2022/4515642.

[7] F. Taher, M. Abdel-Salam, M. Elhoseny, 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.

[8] 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.

[9] R. S. S. Moorthy and N. Nathiya, "Botnet Detection Using Artificial

Intelligence," *Procedia Comput. Sci.*, vol. 218, no. 2022, pp. 1405–1413, 2022, doi: 10.1016/j.procs.2023.01.119.

[10] H. T. Nguyen, Q. D. Ngo, D. H. Nguyen, and V. H. Le, "PSI-rooted subgraph: A novel feature for IoT botnet detection using classifier algorithms," *ICT Express*, vol. 6, no. 2, pp. 128–138, 2020, doi: 10.1016/j.icte.2019.12.001.

[11] F. E. Ayo, J. B. Awotunde, S. O. Folorunso, M. O. Adigun, and S. A. Ajagbe, "A genomic rule-based KNN model for fast flux botnet detection," *Egypt. Informatics J.*, vol. 24, no. 2, pp. 313–325, 2023, doi: 10.1016/j.eij.2023.05.002.

[12] A. Rahmatulloh, G. M. Ramadhan, I. Darmawan, N. Widiyasono, and D. Pramesti, "Identification of Mirai Botnet in IoT Environment through Denial-of-Service Attacks for Early Warning System," *Int. J. Informatics Vis.*, vol. 6, no. 3, pp. 623–628, 2022, doi: 10.30630/joiv.6.3.1262.

[13] I. Erna and W. Romi Satria, "Penggunaan Random Under Sampling untuk Penanganan Ketidakseimbangan Kelas pada Prediksi Cacat Software Berbasis Neural Network," *J. Softw. Eng.*, vol. 1, no. 2, pp. 92–100, 2015.

[14] M. Bach, A. Werner, and M. Palt, "The proposal of undersampling method for learning from imbalanced datasets," *Procedia Comput. Sci.*, vol. 159, pp. 125–134, 2019, doi: 10.1016/j.procs.2019.09.167.

[15] J. N. Sibarani, D. R. Sirait, and S. S. Ramadhanti, "Intrusion Detection Systems pada Bot-IoT Dataset Menggunakan Algoritma Machine Learning," *J. Masy. Inform.*, vol. 14, no. 1, pp. 38–52, 2023, doi: 10.14710/jmasif.14.1.49721.

[16] I. A. A. Angreni, S. A. Adisasmita, and M. I. Ramli, "Terhadap Tingkat Akurasi Identifikasi Kerusakan Jalan," vol. 7, no. 2, pp. 63–70, 2018.

[17] R. Vinayakumar, M. Alazab, S. Srinivasan, Q. V. Pham, S. K. Padannayil, and K. Simran, "A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities," *IEEE Trans.*

Ind. Appl., vol. 56, no. 4, pp. 4436–4456, 2020, doi: 10.1109/TIA.2020.2971952.

[18] M. Aly and <malaa@caltech Edu>, "Survey on multiclass classification methods," *Neural Netw*, vol. 4, no. November, pp. 1–9, 2005, [Online]. Available: https://www.cs.utah.edu/~piyush/teaching/aly05multiclass.pdf

[19] M. K. Uçar, M. Nour, H. Sindi, and K. Polat, "The Effect of Training and Testing Process on Machine Learning in Biomedical Datasets," *Math. Probl. Eng.*, vol. 2020, 2020, doi: 10.1155/2020/2836236.

[20] S. Patricia, C. P. Marpaung, L. R. Wijaya, M. A. Paramartha, W. D. Atmadja, and R. Y. Ningsih, "Implementasi Exploratory Data Analysis (EDA) Untuk Menganalisis Berbagai Faktor Risiko Penyakit Jantung Di Amerika Serikat," *J. Student Dev. Inf. Syst.*, vol. 3, no. 2, pp. 108–124, 2023.

[21] D. Irvantoro, I. Saifudin, and R. Umilasari, "Feature Selection Menggunakan Chi-Square Dan N-Gram Dengan Algoritma Naive Bayes Classifier Untuk Analisis Sentimen Review Produk Elektronik," *J. Tek. Inform. Univ. Muhammadiyah Jembar*, vol. 53, no. 1410651199, pp. 1689–1699, 2019.

[22] F. Alghifari and D. Juardi, "Penerapan Data Mining Pada Penjualan Makanan Dan Minuman Menggunakan Metode Algoritma Naïve Bayes," *J. Ilm. Inform.*, vol. 9, no. 02, pp. 75–81, 2021, doi: 10.33884/jif.v9i02.3755.