DETEKSI SERANGAN *DENIAL OF SERVICE* (DOS) PADA JARINGAN *SMARTHOME IPV6* MENGGUNAKAN METODE *NAÏVE BAYES*

SKRIPSI

DISUSUN OLEH:

MUNAWIRUL AKMAL

09011282126107

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI SERANGAN *DENIAL OF SERVICE* (DOS) PADA JARINGAN *SMARTHOME IPV6* MENGGUNAKAN METODE *NAÏVE BAYES*

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh**:**
MUNAWIRUL AKMAL
09011282126107

Pembimbing 1	**:**	**Prof. Ir. Deris Stiawan, M.T., Ph.D.** **NIP. 197806172006041002**
Pembimbing 2	**:**	**Adi Hermansyah, M.T.** **NIP. 198904302024211001**

Mengetahui
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T
196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Jum'at

Tanggal : 13 Juni 2025

Tim Penguji:

1. Ketua : Dr. Rossi Passarella, M.Eng.
2. Penguji : Aditya Putra Perdana Prasetyo, M.T.
3. Pembimbing I : Prof. Ir. Deris Stiawan, M.T., Ph.D.
4. Pembimbing II : Adi Hermansyah, M.T.

Mengetahui, 26/5/25

Ketua Jurusan Sistem Komputer

Falkultas Ilmu Komputer Universitas Sriwijaya

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	:	Munawirul Akmal
NIM	:	09011282126107
Judul	:	Deteksi Serangan *Denial of Service* (DoS) Pada Jaringan *Smarthome* IPv6 Menggunakan Metode *Naïve Bayes*

Hasil Pengecekan Software Turnitin: 15%

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 tanpa paksaan dari siapapun.

Palembang, 23 Juni 2025

Munawirul Akmal
NIM. 09011282126107

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Dengan penuh rasa syukur, penulis panjatkan kehadirat Allah SWT, yang telah memberikan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul "**Deteksi Serangan *Denial of Service* (DoS) Pada Jaringan *Smarthome* IPv6 Menggunakan Metode *Naïve Bayes***".

Maksud dari penulisan Tugas Akhir ini adalah untuk memenuhi salah satu syarat memperoleh gelar sarjana pada jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan dalam penulisan, penulis mengambil berdasarkan hasil penelitian serta observasi dari berbagai sumber literatur yang mendukung dalam penulisan Tugas Akhir ini.

Dalam menyelesaikan Tugas Akhir ini penulis mengucapkan terima kasih kepada seluruh pihak yang telah meluangkan waktu untuk membantu dalam penyelesaian Tugas Akhir ini. Untuk itu dalam kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan sehingga bisa menyelesaikan skripsi ini dengan sebaik-baiknya.
2. Untuk Kedua Orangtua dan Keluarga yang selalu memberikan nasihat, semangat, motivasi, dan doanya.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. Selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi., M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Aditya Putra Perdana P, S.Kom., M.T. selaku Dosen Pembimbing Akademik.
6. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing I Tugas Akhir.
7. Bapak Adi Hermansyah, M.T. selaku Dosen Pembimbing II Tugas Akhir.
8. Kakak Angga selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.

9. Semua Dosen dan Staff Administrasi Jurusan Sistem Komputer Universitas Sriwijaya.
10. Untuk Diri Sendiri terima kasih karena sudah mau terus berjuang dan tidak menyerah hingga menyelesaikan Tugas Akhir ini.
11. Untuk teman-teman dari riset Smarthome IPv6 dan teman-teman seperjuangan Angkatan 2021 Jurusan Sistem Komputer, terima kasih untuk segala bentuk dukungannya selama ini.
12. Almamater Universitas Sriwijaya.

Penulis menyadari bahwa penulisan Tugas Akhir ini masih memiliki beberapa kekurangan dan jauh dari sempurna. Oleh karena itu, penulis mengharapkan kritik dan saran yang konstruktif dari pembaca demi kesempurnaan Tugas Akhir ini. Penulis juga berharap semoga Tugas Akhir ini dapat bermanfaat bagi semua pihak yang berkepentingan. Atas segala bantuan, nasihat, saran, dan kritik yang telah diberikan selama proses penyusunan Tugas Akhir, penulis ucapkan terima kasih yang sebesar-besarnya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, Juni 2025
Penulis,

Munawirul Akmal
NIM. 09011282126107

DETEKSI SERANGAN *DENIAL OF SERVICE* (DOS) PADA JARINGAN *SMARTHOME* IPV6 MENGGUNAKAN METODE *NAÏVE BAYES*

MUNAWIRUL AKMAL (09011282126107)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: 09011282126107@student.unsri.ac.id

ABSTRAK

Serangan Denial of Service merupakan salah satu bentuk serangan yang mampu melumpuhkan sistem jaringan dengan membanjiri target menggunakan paket permintaan dalam jumlah besar seperti, ICMPv6 Flood "*Echo Request*". Serangan ini sangat efektif pada jaringan berbasis IPv6 yang menggunakan perangkat smarthome karena tingginya ketergantungan terhadap protokol ICMPv6. Dataset COMNETS *Smarthome* IPv6 digunakan dalam penelitian ini yang merupakan hasil simulasi lalu lintas jaringan smarthome berbasis IPv6 dengan dua kelas, yaitu Normal (*BENIGN*) dan Serangan (*DoS*). Penelitian ini bertujuan untuk mendeteksi serangan DoS berbasis ICMPv6 Flood dengan menerapkan algoritma klasifikasi *Naïve Bayes* dengan menerapkan model *Gaussian* dan *Bernoulli* untuk perbandingan. Hasil dari penelitian menunjukkan model *Naïve Bayes Gaussian* memperoleh akurasi sebesar 89.44%, presisi sebesar 91.33%, recall sebesar 89.50%, dan f1-score sebesar 89.39%. Sedangkan model *Naïve Bayes Bernoulli* memperoleh akurasi sebesar 90.43%, dengan presisi sebesar 92.02%, recall sebesar 90.50%, dan f1-score sebesar 90.41%. Temuan ini menunjukkan bahwa model *Naïve Bayes* mampu melakukan klasifikasi efektif terhadap lalu lintas serangan berbasis ICMPv6 dalam lingkungan smarthome.

Kata Kunci: *Denial of Service*, *Detection ICMPv6 Flood*, *IPv6*, *Naïve Bayes*, *Smarthome*.

DETECTION DENIAL OF SERVICE (DOS) ATTACKS ON IPV6 SMART HOME NETWORKS USING THE NAÏVE BAYES METHOD

MUNAWIRUL AKMAL (09011282126107)
Department of Computer Systems, Faculty of Computer Science
Sriwijaya University
Email: 09011282126107@student.unsri.ac.id

ABSTRACT

Denial of Service attacks are a type of attack that can cripple a network system by flooding the target with a large number of request packets, such as ICMPv6 Flood "Echo Request". This attack is highly effective on IPv6-based networks that use smarthome devices due to the high dependence on the ICMPv6 protocol. The COMNETS Smarthome IPv6 dataset is used in this study, which is the result of simulated IPv6-based smarthome network traffic with two classes: Normal (BENIGN) and Attack (DoS). This study aims to detect ICMPv6 Flood-based DoS attacks by applying the Naïve Bayes classification algorithm using Gaussian and Bernoulli models for comparison. The results of the study show that the Gaussian Naïve Bayes model achieved an accuracy of 89.44%, precision of 91.33%, recall of 89.50%, and f1-score of 89.39%. Meanwhile, the Bernoulli Naïve Bayes model achieved an accuracy of 90.43%, precision of 92.02%, recall of 90.50%, and f1-score of 90.41%. These findings show that the Naïve Bayes model is capable of effectively classifying ICMPv6-based attack traffic in a smarthome environment.

Keywords: *Denial of Service, Detection ICMPv6 Flood, IPv6, Naïve Bayes, Smarthome.*

DAFTAR ISI

Halaman

LEMBAR PENGESAHAN ..... **I**
LEMBAR PERSETUJUAN ..... **II**
HALAMAN PERNYATAAN ..... **III**
KATA PENGANTAR ..... **IV**
ABSTRAK ..... **VI**
ABSTRACT ..... **VII**
DAFTAR ISI ..... **VIII**
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 5
1.7 Sistematika Penulisan 6
BAB II TINJAUAN PUSTAKA **7**
2.1 Penelitian Terdahulu 7
2.2 Arsitektur Smarthome 18
2.2.1 Device Layer 18
2.2.2 Communication Layer 18
2.2.3 Application Layer 19
2.3 IPv6 19
2.3.1 Internet Control Message Protocol version 6 21
2.4 Jenis Denial of Service Attack 23
2.5 Dataset COMNETS Smarthome IPv6 24
2.6 Wireshark 25
2.7 Intrusion Detection System 25
2.8 Ekstrasi Data 26
2.9 Random Oversampling 26
2.10 Naïve Bayes 27
2.10.1 Naïve Bayes Gaussian 28

2.10.2 Naïve Bayes Bernoulli 29
2.11 Confusion Matrix 30
BAB III METODOLOGI PENELITIAN 32
3.1 Pendahuluan 32
3.2 Kerangka Kerja 32
3.3 Persiapan Perangkat dan Alat 33
3.3.1 Spesifikasi Perangkat Keras 34
3.3.2 Spesifikasi Perangkat Lunak 34
3.4 Pembuatan Dataset 35
3.4.1 Perancangan Topologi 35
3.4.2 Skenario 35
3.5 Pengolahan Data 36
3.5.1 Ekstraksi Data 37
3.5.2 Labeling Data 38
3.5.3 Penggabungan Data 39
3.5.4 Exploratory Data Analysis 40
3.5.5 Preprocessing 40
3.6 Oversampling 42
3.7 Implementasi Naïve Bayes 43
3.8 Validasi Peforma 44
BAB IV HASIL DAN ANALISA 45
4.1 Pendahuluan 45
4.2 Analisa Dataset 45
4.2.1 Analisa Wireshark 45
4.2.2 Analisa Snort 47
4.3 Ekstrasi Dataset 48
4.4 Exploratory Data Analysis 50
4.5 Preprocessing 55
4.5.1 Feature Selection 55
4.5.2 Data Encoding 55
4.6 Oversampling 56
4.7 Hasil Pengujian Naïve Bayes 57
4.8 Hasil Validasi 60
4.8.1 Confusion Matrix 60
4.8.2 ROC Curve 60
BAB V KESIMPULAN DAN SARAN 63

5.1 Kesimpulan 63
5.2 Saran 63
DAFTAR PUSTAKA.....65
LAMPIRAN.....70

DAFTAR GAMBAR

Halaman

Gambar 2. 1 Device Layer 18
Gambar 2. 2 Communication Layer 19
Gambar 2. 3 Tampilan Aplikasi Google Home 19
Gambar 2. 4 Perbedaan Header IPv4 dan IPv6 20
Gambar 3. 1 Kerangka Kerja Penelitian 33
Gambar 3. 2 Topologi COMNETS Smarthome IPv4/IPv6 35
Gambar 3. 3 Diagram Proses Pembuatan Label pada Dataset 39
Gambar 3. 4 Diagram Proses Preprocessing 40
Gambar 3. 5 Data Encoding 41
Gambar 3. 6 Normalisasi Fitur 41
Gambar 3. 7 Flowchart Oversampling 42
Gambar 3. 8 Flowchart Algoritma Naïve Bayes 43
Gambar 4. 1 Data Pcap BENIGN (Normal) 45
Gambar 4. 2 Data Pcap Serangan DoS 46
Gambar 4. 3 Validasi Serangan dengan Snort 47
Gambar 4. 4 Proses Ekstrasi T-Shark pada Ubuntu 49
Gambar 4. 5 Hasil Ekstrasi Data 49
Gambar 4. 6 Visualisasi Distribusi Kelas dalam Dataset 50
Gambar 4. 7 Visualisasi Hubungan Komunikasi antar IP 51
Gambar 4. 8 Visualisasi Hubungan antar Fitur 51
Gambar 4. 9 Visualisasi Hubungan IP dan Fitur 52
Gambar 4. 10 Visualisasi Distribusi Fitur 53
Gambar 4. 11 Feature Importance 54
Gambar 4. 12 Visualisasi Feature Importance 54
Gambar 4. 13 Hasil Seleksi Fitur 55
Gambar 4. 14 Hasil Encoding dengan Label Encoder 55
Gambar 4. 15 Jumlah Data Sebelum Oversampling 56
Gambar 4. 16 Jumlah Data Setelah Oversampling 57
Gambar 4. 17 Hasil Akurasi Sebelum Oversampling 58

Gambar 4. 18 Hasil Akurasi Setelah Oversampling 58
Gambar 4. 19 Confusion Matrix Gaussian 60
Gambar 4. 20 Confusion Matrix Bernoulli 60
Gambar 4. 21 Grafik ROC Gaussian 61
Gambar 4. 22 Grafik ROC Bernoulli 61

DAFTAR TABEL

Halaman

Tabel 2. 1 Penelitian Terkait 7
Tabel 2. 2 Subset Dari ICMPv6 Messages 21
Tabel 2. 3 Jenis serangan Denial of Service 23
Tabel 2. 4 Perangkat Terhubung dalam Topologi Jaringan IPv6 25
Tabel 2. 5 Confusion Matrix 30
Tabel 3. 1 Spesifikasi Perangkat Keras 34
Tabel 3. 2 Spesifikasi Perangkat Lunak 34
Tabel 3. 3 Deskripsi Fitur 37
Tabel 3. 4 Hyperparameter Validasi 44
Tabel 4. 1 Karakteristik Pola Serangan 46
Tabel 4. 2 Hasil Validasi Naïve Bayes Gaussian 59
Tabel 4. 3 Hasil Validasi Naïve Bayes Bernoulli 59
Tabel 4. 4 Hasil Model Tertinggi Gaussian dan Bernoulli 60

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada penelitian [1] penerapan dari IPv6 meningkat pesat dalam beberapa tahun terakhir karena jumlah IPv4 yang akan habis, ditambah sebagian besar sistem dan perangkat yang terhubung ke internet, seperti laptop, telepon seluler, router rumah, kini sudah mendukung IPv6 secara *default*. Bersamaan dengan itu juga, perangkat yang menggunakan teknologi *Internet of Things* (IoT) seperti *smarthome* dianggap sebagai pendorong utama penerapan IPv6 di rumah, kantor, dan ruang publik.

Pada penelitian [2] mengenai *smarthome* merujuk pada ruang hunian yang memanfaatkan teknologi IoT untuk menghubungkan berbagai perangkat dan sistem ke internet yang dapat dipantau, dikontrol, dan diotomatisasi dari jarak jauh. Berbagai perangkat dan sistem ini, seperti kamera keamanan, termostat, pengcahayaan, sistem alarm, speaker, serta perangkat lainnya dikembangkan untuk meningkatkan kenyamanan, efisiensi energi, dan kemudahan sekaligus keamanan bagi penggunanya. Di sisi lain, potensi akan ancaman keamanan siber juga dikaitkan dengan perangkat *smarthome*, yang mengarah pada kebutuhan terkait sistem deteksi anomali yang efektif untuk melindungi perangkat yang saling terhubung dan data yang dihasilkan. Dalam penelitian [3] dengan semakin banyak perangkat IoT yang terhubung ke internet menimbulkan isu dalam keterbatasan IPv4. Kebutuhan akan protokol jaringan yang mendukung skalabilitas dan efisiensi menjadi sangat penting kedepannya.

Untuk mengatasi masalah tersebut, Pemerintah Indonesia mengeluarkan Surat Edaran Menteri Komunikasi dan Informatika Nomor 5 Tahun 2024 yang berisi himbauan kepada Kementerian/Lembaga dan Pemerintah Daerah untuk mengaktifkan dan memanfaatkan alamat Protokol Internet Versi 6 (IPv6). Hal ini diharapkan menjadi langkah strategis dalam menjaga ketahanan dan fleksibilitas infrastruktur jaringan di Indonesia.

Dalam penelitian [4] Arsitektur IPv6 berbeda dari IPv4, seperti format dari header paket, otomatisasi konfigurasi tanpa DHCP server, mobilitas, dan rentang

alamat IP yang jauh lebih besar. IPv6 memperkenalkan *Internet Control Message Protocol version 6* (ICMPv6), yang berperan penting dalam operasional dan manajemen jaringan IPv6. IPv6 sangat bergantung pada protokol ICMPv6, karena ICMPv6 menjalankan berbagai fungsi penting yang memungkinkan pengiriman data melalui jaringan, termasuk perutean melalui *node*. Namun, *node* IPv6 tidak dapat memverifikasi pesan ICMPv6, karena protokol ini secara *default* dianggap sah. Sehingga, setiap node menjadi rentan terhadap pesan ICMPv6 palsu, yang membuka peluang untuk serangan seperti DoS dan DDoS melalui ICMPv6 *Flood*.

Berdasarkan penelitian [5] penerapan IPv6 secara global menimbulkan isu keamanan oleh sejumlah serangan seperti DoS dan DDoS, dimana DoS bertujuan untuk mengganggu ketersediaan layanan atau jaringan sehingga tidak dapat berfungsi secara normal untuk membuat suatu layanan atau jaringan tidak dapat menyediakan layanan yang normal dengan menyerang *bandwidth* atau sumber daya *host*. Dari penelitian [6] teknik yang dapat digunakan dalam serangan DoS pada IPv6. Meliputi, ICMPv6 *Flood*, UDP *Flood*, SYN *Flood*, HTTP *Flood*. Serangan ICMPv6 *Flood* melibatkan pembanjiran target dengan jumlah lalu lintas yang sangat besar secepat mungkin. Target yang terkena dampak serangan DoS akan mencoba memproses seluruh permintaan. Ketika *bandwidth* dan sumber daya dari target sudah habis, perangkat tersebut tidak akan responsif atau tidak dapat merespons pengguna yang sah.

Penelitian [7] menggunakan *machine learning* untuk mendeteksi serangan DoS terhadap perangkat IoT *smarthome* menggunakan dataset CICDDoS2019. Berdasarkan hasil evaluasi dari beberapa metode *machine learning* yang digunakan menunjukkan metode XGBoost mencapai hasil akurasi tertinggi dengan 99.98 %, diikuti oleh *Decision Tree* dan AdaBoost yang masing-masing dengan akurasi 99.96 %. Metode *Naïve Bayes* (NB) menunjukkan hasil yang cukup baik dengan akurasi 72.34 %.

Dalam penelitian [8] mendeteksi berbagai serangan IoT salah satunya DoS, metode *machine learning* yang digunakan seperti *Decision Tree* (DT), *Naïve Bayes* (NB), *K-Nearest Neighbors* (KNN), *Logistic Regression* (LR), *Support Vector Machine* (SVM), *Random Forest* (RF), dan XGBoost. Pada penelitian ini menggunakan dataset *IoT Network Intrusion* dari HCRL. Hasil temuan

menunjukkan bahwa model dari *Random Forest* (RF) mendapatkan akurasi terbaik dalam identifikasi serangan DoS pada IoT.

Pada penelitian [9] menggunakan lima metode *machine learning* untuk mendeteksi berbagai serangan pada perangkat IoT, salah satunya DoS. Metode yang digunakan terdiri dari, *Random Forest* (RF), S*upport Vector Machine* (SVM), *Multinomial Naive Bayes* (MNB), *Decision Tree* (DT), dan *Artificial Neural Network* (ANN). Metode tersebut digunakan untuk mengevaluasi dataset IoT *smarthome.* Hasil yang ditinjau terdiri dari dua aspek, yaitu deteksi *Malicious Traffic* dan deteksi *Attack Type*. Hasil penelitan menunjukkan untuk model *Multinomial Naive Bayes* (MNB) menunjukkan hasil yang cukup baik dengan akurasi 78.62 %.

Penelitian [10] berfokus pada memahami dan menguji dampak serangan *Adversarial Machine Learning* (AML) terhadap berbagai metode *supervised learning*, termasuk *Naïve Bayes*, serta mengeksplorasi bagaimana *adversarial training* dapat digunakan untuk meningkatkan ketahanan metode terhadap serangan tersebut. Performa keseluruhan direpresentasikan sebagai rata-rata dari *precision* (P), *recall* (R), dan *F1-score* (F) untuk semua eksperimen. Secara keseluruhan, performa klasifikasi dalam mendeteksi serangan spesifik DoS mencapai hasil yang tinggi. Hal ini intuitif karena serangan DoS memiliki nilai paket yang khas (misalnya, nilai len dan ip.ttl) dibandingkan dengan *traffic* jaringan yang bersifat *benign*. Secara khusus, performa klasifikasi dari *Decision Tree*, *Random Forest*, *Naïve Bayes*, dan SVM menunjukkan hasil terbaik, dengan *F1-score* mencapai 99,9%.

Dari pembahasan diatas, penulis akan melakukan penelitian "Deteksi Serangan *Denial of Service* (DoS) Pada Jaringan *Smarthome* IPv6 Menggunakan Metode *Naïve Bayes*" dengan harapan algoritma *Naïve Bayes* dapat memberikan hasil *accuracy*, *precission*, *recall* dan *f1-score* yang baik agar dapat menjadi referensi dalam penelitian terkait selanjutnya.

1.2 **Perumusan Masalah**

Berdasarkan latar belakang masalah yang telah dibahas sebelumnya maka permasalahan yang akan dibahas dalam penelitian ini dirumuskan sebagai berikut:

1. Bagaimana proses ekstraksi dari dataset *Denial of Service* (DoS) ICMPv6 pada jaringan *smarthome* IPv6?
2. Bagaimana teknik *random oversampling* diterapkan pada kumpulan data yang tak seimbang?
3. Bagaimana penerapan metode *Naïve Bayes* dalam mengidentifikasi serangan DoS berbasis ICMPv6 dalam jaringan *smarthome* IPv6?

1.3 Batasan Masalah

Agar penulisan penelitian ini tidak meluas di luar cakupan kajian, maka ditetapkan beberapa batasan masalah sebagai berikut:

1. Data yang dianalisis ialah dari dataset COMNETS *SMARTHOME* IPv6.
2. Melakukan deteksi terhadap serangan DoS dengan memanfaatkan model dari algoritma *Naïve Bayes*.
3. Jenis serangan DoS yang dibahas adalah ICMPv6 *Flood*.
4. Tidak dilakukan implementasi mengenai pencegahan serangan DoS dalam *smarthome* IPv6 dalam penelitian ini, hanya fokus pada deteksi serangan.

1.4 Tujuan

Berdasarkan dari latar belakang serta permasalahan yang telah dijelaskan sebelumnya, terdapat juga beberapa tujuan utama yang ingin dicapai pada penulisan penelitian, ialah:

1. Melakukan ekstrasi dataset yang berbentuk pcap menjadi csv dengan menggunakan T-shark pada Linux Ubuntu.
2. Menggunakan penerapan teknik *random oversampling* dalam proses menangani ketidakseimbangan data untuk proses deteksi serangan DoS.
3. Mengevaluasi performa dari metode *Naïve Bayes* saat deteksi serangan DoS berbasis ICMPv6 dalam jaringan smarthome IPv6.

1.5 Manfaat

Penelitian ini diharapkan dapat memberikan manfaat yang ingin dicapai, antara lain ialah sebagai berikut:

1. Memahami proses ektraksi dataset *smarthome* IPv6 menggunakann T-shark pada Linux Ubuntu.

2. Memberikan solusi terhadap ketidakseimbangan data dan memastikan deteksi yang handal terhadap serangan DoS dalam jaringan smarthome IPv6.
3. Mengevaluasi seberapa baik model algoritma *Naïve Bayes* saat deteksi serangan DoS dalam jaringan smarthome IPv6.

1.6 Metodologi Penelitian

Penelitian ini dilaksanakan dengan mengikuti sejumlah langkah yang tersusun secara sistematis. Setiap tahapan dirancang guna mendukung kelancaran proses penelitian dari awal hingga akhir, yang mencakup beberapa proses sebagai berikut:

1. Studi Literatur

   Tahap ini dilakukan dengan mengkaji dan mempelajari literatur yang sesuai untuk referensi dengan membaca artikel, jurnal, buku, dan sumber dari internet lainnya yang sesuai dengan penelitian tugas akhir.
2. Perancangan Sistem

   Pada tahap ini, membahas mengenai proses bagaimana sistem tersebut dirancang dengan menggunakan metode atau pendekatan tertentu. Menentukan perangkat dan topologi untuk membangun jaringan IPv6 pada infrastruktur smarthome, dilanjutkan dengan proses instalasi dan konfigurasi sistem, serta implementasi deteksi *Denial of Service* (DoS) dengan menggunakan model *Naïve Bayes* pada sistem yang dirancang.
3. Pengujian

   Dalam tahap ini, dilakukan pengujian menggunakan metodologi penelitian yang sesuai dengan penelitian sebelumnya sehingga data hasil pengujian sesuai dengan batasan masalah dan sesuai dengan parameter pengujian yang telah ditetapkan untuk mendapatkan hasil yang handal.
4. Analisa

   Tahap ini dilakukan dilakukan pengolahan data dan analisa data yang didapatkan dari hasil pengujian yang dilakukan sebelumnya untuk mendapatkan data aktual. Selanjutnya, hasil akan dianalisis dengan tujuan untuk menentukan kesalahan dalam perancangan dan penyebabnya, sehingga dapat dilakukan penelitian tambahan.
5. Kesimpulan

Tahap ini merupakan langkah akhir, dimana hasil dibuat berdasarkan seluruh langkah yang dilakukan sebelumnya dan akan dirumuskan dalam suatu kesimpulan agar dapat digunakan sebagai landasan untuk penelitian selanjutnya.

1.7 Sistematika Penulisan

Penelitian tugas akhir ini disusun secara terstruktur berdasarkan pembagian per bab yang tersusun secara sistematis. Setiap bab memuat sejumlah subbab yang dirancang untuk menguraikan secara rinci topik yang dibahas dalam bagian tersebut. Adapun sistematika penulisan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini menyajikan gambaran umum mengenai topik yang diteliti, mencakup latar belakang permasalahan, tujuan yang ingin dicapai, manfaat penelitian, serta perumusan masalah yang menjadi dasar dilakukannya penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini memuat kajian teoritis yang mendukung penelitian, termasuk penjelasan mengenai perangkat keras dan perangkat lunak yang digunakan, *tools* untuk memperoleh serta mengolah data, serta uraian tentang algoritma *Naïve Bayes* sebagai metode yang digunakan dalam deteksi anomali pada lalu lintas jaringan.

BAB III METODOLOGI PENELITIAN

Bab ini menguraikan tahapan-tahapan penelitian yang dilakukan, mulai dari proses pencarian dan pengumpulan dataset, analisis data, hingga teknik pengolahan data yang diterapkan dalam penyusunan tugas akhir ini.

BAB IV PENGUJIAN DAN ANALISA

Bab ini membahas pelaksanaan pengujian terhadap model yang dikembangkan serta analisis dari hasil pengujian tersebut, guna mengevaluasi efektivitas metode yang digunakan dalam mendeteksi serangan.

BAB V KESIMPULAN

Bab ini merupakan bab penutup yang berisikan kesimpulan dari pengujian dan analisa data yang dilakukan, dan memberikan saran untuk penelitan lanjutan.

DAFTAR PUSTAKA

[1] T. Hu, D. J. Dubois, and D. Choffnes, “IoT Bricks Over v6: Understanding IPv6 Usage in Smart Homes,” *Proc. ACM SIGCOMM Internet Meas. Conf. IMC*, pp. 595–611, 2024, doi: 10.1145/3646547.3688457.

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

[3] Pragya and B. Kumar, “IPv6 Addressing Strategy for IoT Network: A Comprehensive Review,” *2023 Int. Conf. Sustain. Emerg. Innov. Eng. Technol. ICSEIET 2023*, pp. 738–744, 2023, doi: 10.1109/ICSEIET58677.2023.10303477.

[4] O. E. Elejla, M. Anbar, S. Hamouda, S. Faisal, A. A. Bahashwan, and I. H. Hasbullah, “Deep-Learning-Based Approach to Detect ICMPv6 Flooding DDoS Attacks on IPv6 Networks,” *Appl. Sci.*, vol. 12, no. 12, 2022, doi: 10.3390/app12126150.

[5] M. Tayyab, B. Belaton, and M. Anbar, “ICMPV6-based DOS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review,” *IEEE Access*, vol. 8, no. September, pp. 170529–170547, 2020, doi: 10.1109/ACCESS.2020.3022963.

[6] A. H. Bdair, R. Abdullah, S. Manickam, and A. K. Al-Ani, “Brief of Intrusion Detection Systems in Detecting ICMPv6 Attacks,” *Lect. Notes Electr. Eng.*, vol. 603, no. June, pp. 199–213, 2020, doi: 10.1007/978-981-15-0058-9_20.

[7] Z. Iqbal, A. Imran, A. U. Yasin, and A. Alvi, “Denial of Service (DoS) Defences against Adversarial Attacks in IoT Smart Home Networks using Machine Learning Methods,” *NUST J. Eng. Sci.*, vol. Vol. 15, 2022, doi: https://doi.org/10.24949/njes.v15i1.666.

[8] Z. Liu, N. Thapa, A. Shaver, K. Roy, X. Yuan, and S. Khorsandroo, “Anomaly detection on lot network intrusion using machine learning,” *2020 Int. Conf. Artif. Intell. Big Data, Comput. Data Commun. Syst.*

icABCD 2020 - Proc., 2020, doi: 10.1109/icABCD49160.2020.9183842.

[9] T. Li, Z. Hong, and L. Yu, “Machine Learning-based Intrusion Detection for IoT Devices in Smart Home,” *IEEE Int. Conf. Control Autom. ICCA*, vol. 2020-Octob, pp. 277–282, 2020, doi: 10.1109/ICCA51439.2020.9264406.

[10] E. Anthi, L. Williams, A. Javed, and P. Burnap, “Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks,” *Comput. Secur.*, vol. 108, p. 102352, 2021, doi: 10.1016/j.cose.2021.102352.

[11] A. Mihoub, O. Ben Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, “Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques,” *Comput. Electr. Eng.*, vol. 98, no. January 2022, p. 107716, 2022, doi: 10.1016/j.compeleceng.2022.107716.

[12] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, “Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms,” *Sensors*, vol. 24, no. 2, 2024, doi: 10.3390/s24020713.

[13] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, “IoT DoS and DDoS Attack Detection using ResNet,” *Proc. - 2020 23rd IEEE Int. Multi-Topic Conf. INMIC 2020*, no. November, 2020, doi: 10.1109/INMIC50486.2020.9318216.

[14] B. R. KIKISSAGBE, M. Adda, P. Célicourt, I. T. HAMAN, and A. Najjar, “Machine Learning for DoS Attack Detection in IoT Systems,” *Procedia Comput. Sci.*, vol. 241, no. 2019, pp. 195–202, 2024, doi: 10.1016/j.procs.2024.08.027.

[15] D. D. Bikila and J. Čapek, “Machine Learning-Based Attack Detection for the Internet of Things,” *Futur. Gener. Comput. Syst.*, vol. 166, no. November 2024, p. 107630, 2025, doi: 10.1016/j.future.2024.107630.

[16] Z. Alwaisi, T. Kumar, E. Harjula, and S. Soderi, “Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention,” *Internet Things (The Netherlands)*, vol. 28, p. 101398,

2024, doi: 10.1016/j.iot.2024.101398.

[17] O. E. Elejla, B. Belaton, M. Anbar, B. Alabsi, and A. K. Al-Ani, "Comparison of classification algorithms on ICMPv6-based DDoS attacks detection," *Lect. Notes Electr. Eng.*, vol. 481, no. December 2018, pp. 347–357, 2019, doi: 10.1007/978-981-13-2622-6_34.

[18] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," *Comput. Electr. Eng.*, vol. 107, no. August 2022, p. 108626, 2023, doi: 10.1016/j.compeleceng.2023.108626.

[19] R. Wang, H. Jiang, and G. Shi, "A Multi-Layer Hybrid Intrusion Detection Method Based on Nb and SVM," *Proc. 2022 IEEE 4th Int. Conf. Civ. Aviat. Saf. Inf. Technol. ICCASIT 2022*, pp. 1384–1388, 2022, doi: 10.1109/ICCASIT55263.2022.9986813.

[20] E. Elmahfoud, S. Elhajla, Y. Maleh, and S. Mounir, "Machine Learning Algorithms for Intrusion Detection in IoT Prediction and Performance Analysis," *Procedia Comput. Sci.*, vol. 236, no. 2023, pp. 460–467, 2024, doi: 10.1016/j.procs.2024.05.054.

[21] S. Yadav, H. Hashmi, D. Vekariya, Z. A. K. N, and V. F. J, "Mitigation of attacks via improved network security in IOT network environment using RNN," *Meas. Sensors*, vol. 32, no. February, p. 101046, 2024, doi: 10.1016/j.measen.2024.101046.

[22] X. Nguyen and K. Le, "Internet of Things Robust detection of unknown DoS / DDoS attacks in IoT networks using a hybrid learning model," *Internet of Things*, vol. 23, no. June, p. 100851, 2023, doi: 10.1016/j.iot.2023.100851.

[23] S.-W. Y. Chia-wei Tseng, Li-Fan, Shih-Chun Hsu, "IPv6 DoS Attacks Detection Using Machine Learning Enhanced IDS in SDN NFV Environment," vol. 9, pp. 7–10, doi: 10.23919/APNOMS50412.2020.9237056.

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

2022, doi: 10.14569/IJACSA.2022.0130667.

[25] EC-Council, *Certified Network Defender (CND) Version 2*, vol. 1 through. 2020. [Online]. Available: https://bookshelf.vitalsource.com/books/97816

[26] M. R. Kadri, A. Abdelli, J. Ben Othman, and L. Mokdad, "Survey and classification of Dos and DDos attack detection and validation approaches for IoT environments," *Internet of Things (Netherlands)*, vol. 25, no. November 2023, p. 101021, 2024, doi: 10.1016/j.iot.2023.101021.

[27] S. Frankel and D. Green, "Internet protocol version 6," *IEEE Secur. Priv.*, vol. 6, no. 3, pp. 83–86, 2021, doi: 10.1109/MSP.2008.65.

[28] S. Zander and X. Wang, "Are we there yet? ipv6 in Australia and China," *ACM Trans. Internet Technol.*, vol. 18, no. 3, 2018, doi: 10.1145/3158374.

[29] A. Gankotiya, V. Kumar, and K. S. Vaisla, "Building IPv6 addressing scheme using Hybrid Duplicate Address Detection to prevent Denial of Service Attack," *Comput. Electr. Eng.*, vol. 117, no. April 2023, p. 109229, 2024, doi: 10.1016/j.compeleceng.2024.109229.

[30] B. J. Nikkel, "An introduction to investigating IPv6 networks," *Digit. Investig.*, vol. 4, no. 2, pp. 59–67, 2007, doi: 10.1016/j.diin.2007.06.001.

[31] N. C. Arjuman and S. Manickam, "A review on ICMPv6 vulnerabilities and its mitigation techniques: Classification and art," *I4CT 2015 - 2015 2nd Int. Conf. Comput. Commun. Control Technol. Art Proceeding*, no. I4ct, pp. 323–327, 2015, doi: 10.1109/I4CT.2015.7219590.

[32] R. Uddin, S. A. P. Kumar, and V. Chamola, "Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions," *Ad Hoc Networks*, vol. 152, no. July 2023, p. 103322, 2024, doi: 10.1016/j.adhoc.2023.103322.

[33] S. Mukherjee and N. Sharma, "Intrusion Detection using Naive Bayes Classifier with Feature Reduction," *Procedia Technol.*, vol. 4, pp. 119–128, 2012, doi: 10.1016/j.protcy.2012.05.017.

[34] Y. Zhai, N. Ma, B. An, and D. Ruan, "An effective over-sampling method for imbalanced data sets classification," *Chinese J. Electron.*, vol. 20, no. 3, pp. 489–494, 2011.

[35] O. Peretz, M. Koren, and O. Koren, "Naive Bayes classifier – An ensemble

procedure for recall and precision enrichment," *Eng. Appl. Artif. Intell.*, vol. 136, no. PB, p. 108972, 2024, doi: 10.1016/j.engappai.2024.108972.

[36] B. S. Sharmila and R. Nagapadma, "Intrusion detection system using naive bayes algorithm," *2019 5th IEEE Int. WIE Conf. Electr. Comput. Eng. WIECON-ECE 2019 - Proc.*, pp. 8–11, 2019, doi: 10.1109/WIECON-ECE48653.2019.9019921.

[37] A. Fadlil, I. Riadi, and S. Aji, "Review of detection DDOS attack detection using naive bayes classifier for network forensics," *Bull. Electr. Eng. Informatics*, vol. 6, no. 2, pp. 140–148, 2017, doi: 10.11591/eei.v6i2.605.

[38] M. Artur, "Review the performance of the Bernoulli Naïve Bayes Classifier in Intrusion Detection Systems using Recursive Feature Elimination with Cross-validated selection of the best number of features," *Procedia Comput. Sci.*, vol. 190, no. 2019, pp. 564–570, 2021, doi: 10.1016/j.procs.2021.06.066.

[39] M. Vishwakarma and N. Kesswani, "A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection," *Decis. Anal. J.*, vol. 7, no. January, p. 100233, 2023, doi: 10.1016/j.dajour.2023.100233.

[40] T. B. Sasongko, O. Arifin, and H. Al Fatta, "Optimization of hyper parameter bandwidth on naïve Bayes kernel density estimation for the breast cancer classification," *2019 Int. Conf. Inf. Commun. Technol. ICOIACT 2019*, pp. 226–231, 2019, doi: 10.1109/ICOIACT46704.2019.8938497.