DETEKSI SERANGAN *DDOS* PADA SMARTHOME MENGGUNAKAN METODE *NAÏVE BAYES*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

ACHMAD NANDIKA

09011282025069

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

Deteksi Serangan DDoS pada Smarthome Menggunakan Metode Naive Bayes

Sebagai salah satu syarat untuk penyelesaian studi di Program Studi S1

Sistem Komputer

Oleh:

ACHMAD NANDIKA

09011282025069

Pembimbing 1 : **Prof. Deris Stiawan, M.T., Ph.D**
NIP. 197806172006041002

Pembimbing 2 : **Kemahyanto Exaudi, S.Kom., M.T**
NIP. 198405252023211018

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T

196612032006041001

AUTHENTICATION PAGE

FINAL TASK

DDoS Attack Detection on Smarthome Using the Naive Bayes Method

Submitted to Complete One of The Requirements for Obtaining A Bachelor's Degree in Computer Science

By:

ACHMAD NANDIKA

09011282025069

Pembimbing 1 : **Prof. Deris Stiawan, M.T., Ph.D**
NIP. 197806172006041002

Pembimbing 2 : **Kemahyanto Exaudi, S.Kom., M.T**
NIP. 198405252023211018

Acknowledged

Head of Computer Systems Department

Dr. Ir. Sukemi, M.T

196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Kamis

Tanggal : 24 Juli 2025

Tim Penguji :

1. Ketua : Dr. Ahmad Zarkasi, M. T.
2. Penguji : Aditya Putra Perdana Prasetyo, M. T.
3. Pembimbing I : Prof. Deris Stiawan, M. T., Ph.D.
4. Pembimbing II : Kemahyanto Exaudi, M. T.

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

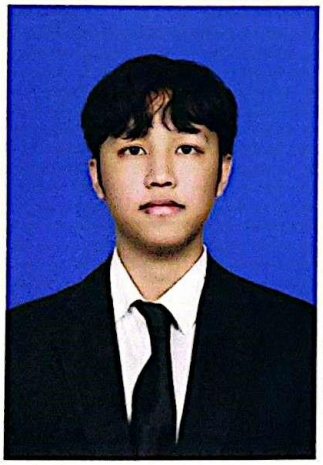
Nama : Achmad Nandika

NIM : 09011282025069

Judul : Deteksi Serangan DDoS pada SMARTHOME menggunakan Metode Naive Bayes

Hasil pengecekan Software Turnitin : 5 %

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



Palembang, Juli 2025 Penulis

Achmad Nandika

NIM. 09011282025069

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa, penulis telah diberikan kesehatan, kekuatan, serta kesanggupan sehingga penulis mampu menyelesaikan Proposal Tugas Akhir ini yang berjudul "DETEKSI SERANGAN *DDOS* PADA SMARTHOME MENGGUNAKAN METODE *NAÏVE BAYES*".

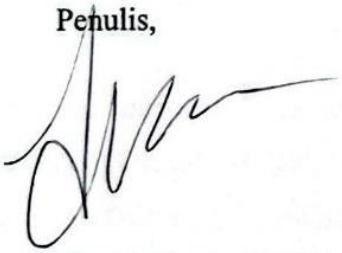
Dalam penulis Proposal Tugas Akhir ini, penulis masih dalam tahap pembelajaran dan bimbingan. Dengan demikian, penulis menyadari bahwa tanpa bantuan serta petunjuk dari semua pihak, penulis tentu tidak dapat menyelesaikan Proposal Tugas Akhir ini. Pada kesempatan kali ini saya ingin mengucapkan terima kasih kepada :

1. Orang Tua penulis, Bapak dan Ibu, yang selalu memberikan motivasi, doa,serta dukungannya untuk penulis dan menguatkan dalam menyelesaikan Proposal Tugas Akhir.
2. Bapak Prof. Dr. Erwin, S.Si., M.Si.,selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Ir. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu KomputerUniversitas Sriwijaya.
4. Bapak Abdurahman. S.Kom., M.Han., selaku dosen pembimbing akademik penulis pada program studi sistem komputer
5. Bapak Prof. Deris Stiawan, S.T., M.T., Ph.D., selaku Dosen Pembimbing Tugas Akhir penulis yang telah berkenan meluangkan waktu dalam membimbing penulis dalam penyusunan Proposal Tugas Akhir.
6. Bapak Kemahyanto Exaudi, S.Kom., M.T., selaku Dosen Pembimbing Akademik penulis pada Program Studi Sistem Komputer.
7. Ibu Sari selaku Admin Program Studi Sistem Komputer yang telah membantu administrasi dalam menyelesaikan Tugas Akhir.
8. Semua relasi penulis, rekan seangkatan penulis angkatan 2020 yang menjadi teman seperjuangan pada Sistem Komputer, Universitas Sriwijaya.

Penulis menyadari bahwa skripsi ini masih memiliki ruang untuk pengembangan lebih lanjut. Oleh karena itu, penulis terbuka terhadap kritik dan saran yang membangun sebagai bekal untuk peningkatan kualitas di masa mendatang. Penulis berharap skripsi ini dapat memberikan manfaat dan kontribusi positif bagi semua pihak yang terlibat, para pembaca, serta bagi penulis sendiri dalam pengembangan ilmu pengetahuan dan pengalaman akademik.

Palembang, juli 2025

Penulis,



ACHMAD NANDIKA
NIM. 09011282025069

DETEKSI SERANGAN DDOS PADA SMARTHOME MENGGUNAKAN METODE *NAÏVE BAYES*

Achmad Nandika (09011282025069)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : Achmadnandika04@gmail.com

ABSTRAK

Perkembangan teknologi smarthome membawa tantangan baru dalam aspek keamanan, terutama terhadap serangan Distributed Denial of Service (DDoS). Penelitian ini bertujuan untuk mendeteksi serangan DDoS pada jaringan smarthome dengan menggunakan algoritma Naïve Bayes. Dataset yang digunakan adalah COMNETS SMARTHOME dalam format .pcap, yang diekstraksi menjadi .csv menggunakan CiCFlowMeter di lingkungan Windows. Mengingat data bersifat tidak seimbang, metode Synthetic Minority Oversampling Technique (SMOTE) diterapkan untuk menyeimbangkan distribusi antar kelas. Hasil evaluasi menunjukkan bahwa model yang dibangun mampu mencapai akurasi sebesar 91,41%, precision 94,10%, recall 89,79%, f1-score 91,81%, dan specificity sebesar 93,33%. Temuan ini menunjukkan bahwa kombinasi antara Naïve Bayes dan SMOTE mampu memberikan performa yang baik dalam mengidentifikasi serangan DDoS pada jaringan smarthome, serta membuktikan potensi penggunaan pendekatan machine learning dalam sistem keamanan siber.

Kata Kunci: Smart Home, Serangan DDoS, Naïve Bayes, SMOTE, Deteksi Serangan, Keamanan Siber

DDOS ATTACK DETECTION ON SMARTHOME USING NAÏVE BAYES METHOD

Achmad Nandika (09011282025069)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : Achmadnandika04@gmail.com

ABSTRACT

The rapid development of smart home technology presents new challenges in terms of cybersecurity, particularly against Distributed Denial of Service (DDoS) attacks. This study aims to detect DDoS attacks in smart home networks using the Naïve Bayes algorithm. The dataset used is the COMNETS SMARTHOME dataset in .pcap format, which was converted to .csv using CiCFlowMeter on a Windows environment. Due to the imbalanced nature of the dataset, the Synthetic Minority Oversampling Technique (SMOTE) was applied to balance the distribution between classes. The evaluation results show that the model achieved an accuracy of 91.41%, a precision of 94.10%, a recall of 89.79%, an F1-score of 91.81%, and a specificity of 93.33%. These findings indicate that the combination of Naïve Bayes and SMOTE provides strong performance in detecting DDoS attacks within smart home networks, highlighting the potential of machine learning approaches in cybersecurity systems.

Keywords: Smart Home, DDoS Attack, Naïve Bayes, SMOTE, Attack Detection, Cybersecurity

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam Penelitian [1], Serangan *Distributed Denial of Service* (*DDoS*) merupakan salah satu jenis ancaman siber yang saat ini sering terjadi. Tujuan utama dari serangan ini adalah untuk membuat sistem server tidak dapat diakses dengan cara membanjiri jaringan menggunakan paket data atau permintaan dalam jumlah besar. Karena lalu lintas jaringan dari serangan *DDoS* sangat mirip dengan lalu lintas normal, maka deteksi serangan ini menjadi tantangan tersendiri. Oleh karena itu, diperlukan sebuah sistem yang mampu melakukan klasifikasi untuk membedakan antara trafik normal dan serangan *DDoS*. Dalam penelitian ini, dibangun sebuah sistem klasifikasi serangan *DDoS* dengan memanfaatkan algoritma *naïve bayes*. Penelitian ini menggunakan dataset CICIDS2018 yang memiliki 84 fitur dan dianggap mampu meningkatkan performa klasifikasi metode tersebut. Untuk pengujian sistem, data uji diperoleh dari simulasi serangan menggunakan program Slowloris. Lalu lintas jaringan dari simulasi tersebut dikumpulkan secara *real-time* dengan menggunakan TCPdump. Data yang diperoleh kemudian diekstrak fitur-fiturnya dan dikonversi ke dalam format .csv menggunakan alat bantu *CICFlowMeter*.

Dalam Penelitian [2], *DDoS* adalah ancaman utama terhadap ketersediaan dalam mengakses jaringan, menggunakan paket palsu dan mempekerjakan sejumlah besar agen yang telah diatur, penyerang mencoba mencegah yang sah lalu lintas antara klien dan server. Selama serangan itu,alamat IP sumber juga dipalsukan untuk menyembunyikannya identitas penyerang yang membuat penelusuran kembali menjadi sangat sulit. Pada penelitian ini menggunakan *discrete fourier transform* (DFT), *discrete wavelet transform* (DWT), dan *Naïve Bayes*.

Dalam penelitian [3], menggunakan *machine learning K-Nearest Neighbor dan naïve bayes* serta menggunakan KDD Cup 99 dan NSL-KDD dataset, keamanan jaringan yang bermaksud mengidentifikasi serangan berdasarkan penyimpangan spesifik dari lalu lintas yang ditangkap. Tingkat kejahatan dunia maya meningkat, kemampuan teroris dan peretas dunia maya tumbuh pada tingkat yang lebih tinggi. Saat ini terdapat kebutuhan akan inovasi dan eksplorasi untuk mitigasi serangan *DDoS*. Salah satu serangan paling populer di berbagai lapisan jaringan adalah *Distributed Denial of Service* (*DDoS*), sebuah upaya jahat untuk mengganggu lalu lintas reguler dari server, layanan, atau jaringan yang diarahkan dengan menyerang target infrastruktur terdekat dengan lalu lintas banjir yang tidak wajar. Dan menginginkan pembobolan pada server. Pada penelitian ini

Dalam Penelitian [4] memanfaatkan kombinasi metode *Artificial Neural Network* (ANN) dan *Synthetic Minority Over-sampling Technique* (*SMOTE*) dalam proses pendeteksian. Sementara itu, Penelitian [5] menerapkan metode *Convolutional Neural Network* (CNN) yang dilengkapi dengan beberapa tahap analisis menggunakan *Bayes Classifier*, ANN, dan *Support Vector Machine* untuk melakukan deteksi dan klasifikasi serangan. Adapun Penelitian [6] menggunakan pendekatan *ensemble learning*, yaitu dengan menggabungkan berbagai model klasifikasi untuk meningkatkan akurasi deteksi, dan terbukti lebih efektif dalam menangani data yang bersifat kompleks serta tidak seimbang.

Dalam Penelitian [7] mengusulkan penggunaan model *Long Short-Term Memory* (*LSTM*) yang mampu mengenali pola lalu lintas jaringan berdasarkan urutan waktu, sehingga efektif dalam mendeteksi serangan *DDoS* yang berbasis waktu. Penelitian [8] menerapkan metode *Random Forest* pada dataset UNSW-NB15, dan hasilnya menunjukkan bahwa model ini tidak hanya memiliki akurasi tinggi dalam mengidentifikasi pola serangan, tetapi juga tahan terhadap *overfitting*. Sementara itu, Penelitian [9] mengembangkan pendekatan *hybrid* yang menggabungkan *Decision Tree* dengan algoritma *boosting* untuk membangun model deteksi yang lebih tangguh terhadap berbagai variasi serangan.

Dalam Penelitian [10] menggunakan pendekatan *clustering* berbasis *K-Means* untuk mendeteksi anomali secara tidak terawasi (*unsupervised*), yang berguna dalam mengenali serangan baru yang belum teridentifikasi sebelumnya. Penelitian [11] mengimplementasikan metode *autoencoder* untuk merekonstruksi data dan mendeteksi anomali serangan *DDoS*, khususnya dalam arsitektur jaringan berbasis *cloud*. Penelitian [12] mengevaluasi efektivitas kombinasi *Principal Component Analysis* (PCA) untuk reduksi dimensi dan *Support Vector Machine* (SVM) untuk klasifikasi serangan. Penelitian [13] memanfaatkan *Gradient Boosting Machines* (GBM) guna meningkatkan presisi klasifikasi serangan dengan menggunakan fitur penting yang diseleksi secara otomatis. Selanjutnya, Penelitian [14] menyajikan penerapan *fuzzy logic* sebagai mekanisme pengambilan keputusan dalam sistem deteksi intrusi berbasis *rule* yang fleksibel dalam mendeteksi *DDoS*. Terakhir, Penelitian [15] mengembangkan sistem deteksi *DDoS* berbasis *federated learning* yang memungkinkan model untuk belajar dari data tersebar di berbagai lokasi tanpa perlu memindahkan data ke pusat, sehingga tetap menjaga privasi dan keamanan informasi.

Dalam penelitian ini, deteksi serangan *DDoS* pada perangkat *smarthome* akan dilakukan menggunakan metode *Naive Bayes*. Oleh karena itu, penelitian ini akan diberi judul **"Deteksi Serangan *DDoS* pada Perangkat *Smarthome* dengan Menggunakan Metode *Naive Bayes*"**. Diharapkan, penerapan metode *Naive Bayes* dalam penelitian ini dapat memberikan hasil yang efektif dalam mengidentifikasi serangan *DDoS* secara akurat dan efisien pada lingkungan *smarthome*.

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 *Distributed Denial of Service* (*DDOS*)?
2. Bagaimana Teknik mengumpulkan dan menganalisa arus lalu lintas jaringan??

3. Bagaimana cara model *Naïve Bayes* digunakan untuk mengklasifikasi *Distributed Denial of Service*(*DDOS*) pada jaringan *smarthome* ?

1.3 Batasan masalah

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

1. Dataset yang digunakan adalah dataset COMNETS SMARTHOME.
2. Melakukan deteksi serangan *Distributed denial of Service* dengan menggunakan teorema dan metode *Naive Bayes*.
3. Serangan *Distributed denial of Service* yang digunakan dalam penelitian ini menggunakan jenis *DDoS* SYN Flood.
4. Tidak ada pembahasan mengenai pencegahan serangan *Distributed denial of Service* 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 Windows.
2. Menerapkan teorema *naïve bayes* pada dataset COMNETS SMARTHOME yang tidak seimbang dan menyeimbangkannya untuk proses deteksi serangan *Distributed denial of Service*.
3. Melakukan evaluasi performa algoritma *Naive Bayes* dalam mendeteksi serangan *Distributed denial of Service*.

1.5 Manfaat

Adapun manfaat dari penelitian tugas akhir ini antara lain adalah:

1. Memahami proses ekstraksi dataset menggunakan *CicFlowMeter* pada Windows.
2. Memberikan solusi terhadap ketidakseimbangan data, memastikan deteksi yang akurat dan handal terhadap serangan *Distributed denial of Service*.
3. Mengevaluasi seberapa baik model *Naive Bayes* dalam mendeteksi.

1.6 Metodologi Penelitian

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

1. Studi Literatur

   Pada tahap awal, dilakukan pengumpulan dan penelaahan berbagai sumber pustaka yang relevan, seperti buku, jurnal ilmiah, artikel, serta dokumen penelitian terdahulu. Tujuan dari studi ini adalah untuk memperoleh pemahaman teoritis serta menelaah pendekatan yang telah digunakan pada penelitian sebelumnya yang berkaitan dengan sistem deteksi serangan *DDoS*.
2. Perancangan Sistem

   Tahap ini mencakup proses perencanaan dan pengembangan sistem yang dirancang untuk mengidentifikasi serangan *DDoS*. Sistem dikembangkan dengan menerapkan algoritma *Naïve Bayes* sebagai metode klasifikasi. Perancangan mencakup pemilihan dataset, pemrosesan data, serta desain arsitektur sistem.
3. Tahap Pengujian

   Setelah sistem selesai dirancang, tahap selanjutnya adalah implementasi dan pengujian. Pengujian dilakukan dengan menggunakan data uji untuk mengevaluasi akurasi serta efektivitas sistem dalam mendeteksi serangan. Selain itu, dilakukan perbandingan hasil dengan metode atau sistem serupa yang telah ada sebelumnya.
4. Analisa

   Data yang diperoleh dari hasil pengujian kemudian dianalisis untuk mengukur kinerja sistem. Analisis dilakukan secara kuantitatif guna

mengetahui sejauh mana sistem dapat mendeteksi serangan dengan tepat. Tahap ini juga bertujuan untuk mengidentifikasi kelemahan sistem dan memberikan evaluasi terhadap proses perancangan yang telah dilakukan.

5. Kesimpulan

   Merupakan tahap akhir dari keseluruhan proses penelitian. Pada tahap ini, seluruh temuan dari studi literatur, perancangan, implementasi, pengujian, dan analisis dirangkum menjadi kesimpulan. Hasil tersebut juga dijadikan dasar untuk memberikan rekomendasi terhadap pengembangan sistem di masa yang akan datang.

1.7 Sistematika Penulisan

Untuk mempermudah pemahaman dan menyusun tulisan secara terstruktur, penulis menyusun sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab pertama ini menyajikan gambaran umum tentang topik penelitian, yang mencakup latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat penelitian, metodologi yang digunakan, serta sistematika penulisan yang menjelaskan susunan bab-bab dalam skripsi ini.

BAB II TINJAUAN PUSTAKA

Pada bab ini, akan dibahas berbagai literatur yang relevan dengan topik penelitian, khususnya terkait dengan deteksi serangan *Distributed Denial of Service* (*DDoS*) menggunakan algoritma *Naïve Bayes*, serta mengacu pada penelitian-penelitian sebelumnya yang berhubungan.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan secara rinci mengenai tahapan-tahapan yang dilakukan dalam penelitian. Pembahasan meliputi persiapan data yang akan digunakan, termasuk data serangan *DDoS* dan data

normal, penerapan algoritma *Naïve Bayes*, serta proses pembuatan dan evaluasi model yang digunakan untuk mencapai tujuan penelitian.

BAB IV HASIL DAN ANALISA

Pada bab ini, akan dipaparkan hasil yang diperoleh dari proses penelitian, serta dilakukan analisis terhadap data yang terkumpul hasil dari pengujian dan implementasi sistem yang telah dilakukan.

BAB V KESIMPULAN

Bab terakhir ini menyajikan kesimpulan berdasarkan hasil pengujian dan analisis yang telah dilakukan. Selain itu, bab ini juga memberikan rekomendasi untuk penelitian selanjutnya serta saran-saran yang dapat memperbaiki atau mengembangkan sistem yang telah dibangun.

Applications, vol. 41, no. 4, pp. 1690–1700, 2014. doi: 10.1016/j.eswa.2013.08.066.

[8] N. Moustafa, J. Slay, "The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset," *Information Security Journal: A Global Perspective*, vol. 25, no. 1-3, pp. 18–31, 2016. doi: 10.1080/19393555.2016.1177546.

[9] M. Panda dan M. R. Patra, "Network intrusion detection using hybrid classification technique," *Computers & Electrical Engineering*, vol. 38, no. 2, pp. 371–383, 2012. doi: 10.1016/j.compeleceng.2011.11.008.

[10] M. H. Bhuyan, D. K. Bhattacharyya, dan J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 303–336, 2014. doi: 10.1109/SURV.2013.052313.00196.

[11] Y. Zhang, H. Xu, dan F. Tian, "Network intrusion detection using autoencoder," *Computers & Security*, vol. 92, p. 101736, 2020. doi: 10.1016/j.cose.2020.101736.

[12] A. Javaid, Q. Niyaz, W. Sun, dan M. Alam, "A deep learning approach for network intrusion detection system," *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, 2016. doi: 10.4108/eai.3-12-2016.2262519.

[13] Y. Chen dan H. Yu, "Feature selection using *Random Forest* and gradient boosting machine," *Journal of Information Security and Applications*, vol. 53, p. 102546, 2020. doi: 10.1016/j.jisa.2020.102546.

[14] H. Om dan C. Prakash, "Fuzzy logic based intrusion detection system," *Computers & Security*, vol. 68, pp. 1–13, 2017. doi: 10.1016/j.cose.2017.03.002.

[15] M. Shayan, A. Shokri, dan P. Mittal, "Biscotti: A blockchain system for federated learning," *Proceedings of the 36th International Conference on Machine Learning*, 2020. [Online]. Tersedia: http://proceedings.mlr.press/v97/shayan19a.html

LAMPIRAN