DETEKSI SERANGAN DDOS PADA SMARTHOME MENGGUNAKAN METODE RANDOM FOREST

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

ACHMAD ANDRIEO

09011381924121

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI SERANGAN DDOS PADA SMARTHOME MENGGUNAKAN METODE RANDOM FOREST

Sebagai salah Satu Syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

ACHMAD ANDRIEO
09011381924121

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

Pebimbing 2 : **Kemahyanto Exaudi, M.T.**
NIP.197806172006041002

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T
196612032006041001

AUTHENTICATION PAGE

FINAL TASK

DETECTION OF DDOS ATTACKS ON SMART HOME USING RANDOM FOREST METHOD

Submitted to Complete One of the Requirements for Obtaining a Bachelor's Degree in Computer Science

By:

ACHMAD ANDRIEO

09011381924121

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

Supervisor 2 : **Kemahyanto Exaudi, M.T.**
NIP.197806172006041002

Acknowledge

Head of Computer System 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** : **Huda Ubaya, M.T.**
3. **Pembimbing 1** : **Prof.Deris Stiawan , M.T., Ph.D.**
4. **Pembimbing 2** : **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 Andrieo

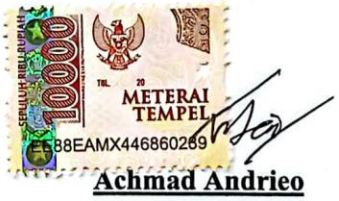
Nim : 09011381924121

Judul : DETEKSI SERANGAN DDOS PADA SMARTHOME MENGGUNAKAN METODE RANDOM FOREST

Hasil pengecekan *Software 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 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



Achmad Andrieo

NIM. 09011381924121

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat, karunia, dan petunjuk-Nya sehingga penulis dapat menyelesaikan penelitian dan menyusun Laporan Akhir ini dengan baik dan tepat waktu. Laporan Akhir ini berjudul **"Deteksi Serangan DDoS pada Smart Home Menggunakan Metode Random Forest"**.

Penyusunan laporan ini merupakan salah satu bentuk tanggung jawab akademik dalam menyelesaikan studi pada Program Studi Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Tentunya, laporan ini tidak dapat terselesaikan tanpa bantuan, dukungan, dan bimbingan dari berbagai pihak. Untuk itu, penulis menyampaikan ucapan terima kasih yang tulus kepada:

1. Kedua orang tua tercinta yang selalu memberikan doa, semangat, dan dukungan penuh selama proses pengerjaan Tugas Akhir ini.
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 Komputer Universitas Sriwijaya.
4. Ibu Ir. Siti Nurmaini, selaku dosen pembimbing akademik yang telah memberikan arahan selama masa studi penulis.
5. Bapak Prof. Deris Stiawan, M.T., Ph.D., selaku dosen pembimbing Tugas Akhir yang telah memberikan bimbingan, ilmu, dan waktunya dalam proses penyusunan laporan ini.
6. Bapak Kemahyanto Exaudi, S.Kom., M.T., selaku dosen pembimbing akademik pada Program Studi Sistem Komputer.
7. Ibu Sari, selaku staf administrasi Program Studi Sistem Komputer yang telah membantu dalam urusan administrasi penyusunan Tugas Akhir.
8. Seluruh dosen dan staf pengajar di Fakultas Ilmu Komputer Universitas Sriwijaya atas ilmu dan pengalaman berharga yang telah diberikan selama masa perkuliahan.
9. Rekan-rekan mahasiswa angkatan 2019 Program Studi Sistem Komputer Universitas Sriwijaya yang telah menjadi teman berbagi ilmu, pengalaman,

dan semangat selama masa perkuliahan.

10. Semua pihak lain yang tidak dapat disebutkan satu per satu namun telah berkontribusi dalam proses penyusunan tugas akhir ini.

Penulis menyadari bahwa Laporan Akhir ini masih jauh dari sempurna, baik dari segi isi maupun penyajiannya. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang bersifat membangun demi perbaikan di masa mendatang. Besar harapan penulis agar laporan ini dapat memberikan manfaat dan menjadi referensi bagi penelitian selanjutnya, serta memberikan kontribusi positif dalam pengembangan ilmu pengetahuan, khususnya di bidang keamanan jaringan pada perangkat Smart Home.

Akhir kata, semoga segala bentuk usaha dan kerja keras yang telah dicurahkan dalam penyusunan laporan ini dapat memberikan hasil yang bermanfaat bagi semua pihak.

Palembang, Juli 2025

Penulis,

ACHMAD ANDRIEO

NIM. 09011381924

DETEKSI SERANGAN DDOS PADA SMARTHOME MENGGUNAKAN METODE *RANDOM FOREST*

ACHMAD ANDRIEO (09011381924121)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Univerisas Sriwijaya
Email: Achmadandrieo@gmail.com

ABSTRAK

Perkembangan teknologi Internet of Things (IoT) telah mendorong penggunaan perangkat *smart home* secara luas. Namun, keterhubungan perangkat ini ke internet menjadikannya rentan terhadap serangan siber, salah satunya adalah serangan Distributed Denial of Service (DDoS). Penelitian ini bertujuan untuk menerapkan dan mengevaluasi algoritma Random Forest dalam mendeteksi serangan DDoS pada jaringan perangkat smart home. Data yang digunakan berasal dari dataset COMNETSSMARTHOME yang mencakup trafik normal dan trafik yang mengandung serangan SYN Flood. Tahapan penelitian meliputi pengumpulan data, preprocessing (data cleaning, encoding, dan normalisasi), pelatihan model Random Forest, serta evaluasi kinerja menggunakan metrik akurasi, presisi, recall, dan F1-score. Hasil pengujian menunjukkan bahwa model Random Forest mampu mendeteksi serangan DDoS dengan akurasi mencapai 100% tanpa kesalahan klasifikasi. Selain itu, fitur seperti Fwd Packet Length Std, Flow Bytes/s, dan SYN Flag Count terbukti menjadi fitur paling berpengaruh dalam proses klasifikasi. Penelitian ini menunjukkan bahwa algoritma Random Forest efektif dalam mendeteksi serangan DDoS pada perangkat smart home, serta dapat dijadikan dasar untuk pengembangan sistem keamanan otomatis berbasis machine learning.

Kata kunci: *Distributed Denial of Service*, *Smart Home, IoT, Random Forest*, Keamanan Jaringan

DETECTION OF DDOS ATTACKS ON SMART HOME USING RANDOM FOREST METHOD

ACHMAD ANDRIEO (09011381924121)
Department of Computer System, Faculyy of Computer Science
Sriwijaya University
Email: Achmadandrieo@gmail.com

ABSTRACT

The development of Internet of Things (IoT) technology has led to the widespread adoption of smart home devices. However, their connection to the internet also makes them vulnerable to cyberattacks, particularly Distributed Denial of Service (DDoS) attacks. This study aims to implement and evaluate the Random Forest algorithm in detecting DDoS attacks on smart home network environments. The dataset used in this research is COMNETSSMARTHOME, which includes both normal and malicious traffic data, specifically SYN Flood attacks. The research process involves data collection, preprocessing (data cleaning, encoding, and normalization), model training using Random Forest, and performance evaluation using accuracy, precision, recall, and F1-score metrics. The experimental results demonstrate that the Random Forest model can detect DDoS attacks with 100% accuracy and no classification errors. Furthermore, features such as Fwd Packet Length Std, Flow Bytes/s, and SYN Flag Count were identified as the most influential in the classification process. This research concludes that Random Forest is an effective method for detecting DDoS attacks on smart home devices and can serve as a foundation for developing automated security systems based on machine learning.

Keywords: DDoS, Smart Home, IoT, Random Forest, Network Security

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan majunya teknologi yang sangat pesat, banyak dari kita merasa terbantu mulai dari jaringan yang cepat(5G) yang mempermudah kita untuk meningkatkan produktifitas dan efisiensi, dengan jaringan yang cepat juga kita bisa mempercepat inovasi teknologi salah satu nya yaitu *smart home*.[1]

Smart home merupakan konsep rumah yang dilengkapi dengan perangkat pintar yang dapat dikendalikan dan dimonitor dari jarak jauh melalui jaringan internet. Sistem ini biasanya menggunakan teknologi IoT untuk menghubungkan perangkat seperti lampu, kunci pintu, kamera keamanan, hingga alat-alat rumah tangga lainnya [2][3]. Dengan penerapan smart home, pengguna dapat menikmati kenyamanan, efisiensi energi, serta keamanan yang lebih baik [4].

Ada berbagai macam perangkat yang dapat terhubung dengan adanya IOT seperti lampu, stop kontak, kunci rumah, dan perangkat keamanan lainya tetapi dengan adanya teknologi ini banyak dari kita tidak menyadari bahwa terdapat oknum-oknum jahat yang dapat memanfaatkan teknologi ini menjadi kejahatan cyber salah satunya yaitu *Distibuted Denial of Service* (DDoS).[5]

Distibuted Denial of Service atau yang dikenal dengan DDoS merupakan serangan *cyber* yang bertujuan untuk merusak suatu system yang menyebabkan sistem sulit atau tidak dapat diakses. Cara kerja DDos ialah dengan membanjiri atau mengirim banyak permintaan data secara bersamaan(BOTNET) yang membuat sistem tidak dapat diakses.[6]

Dampak dari serangan DDoS tidak hanya mengganggu kenyamanan pengguna, tetapi juga dapat menyebabkan kebocoran data, kerugian finansial, hingga potensi ancaman terhadap keselamatan penghuni rumah jika perangkat keamanan terganggu.[7] Dalam konteks Smart Home, serangan ini dapat menyebabkan perangkat seperti kunci pintu digital atau kamera keamanan menjadi tidak dapat diakses saat dibutuhkan.[8]

Untuk mengatasi ancaman ini, diperlukan pendekatan keamanan yang tidak hanya bersifat reaktif, tetapi juga proaktif, yaitu dengan mendeteksi serangan sedini mungkin sebelum dampak yang lebih besar terjadi. Salah satu metode yang efektif dalam mendeteksi serangan adalah melalui pemanfaatan teknologi *Machine Learning (ML).[*9]

Menganali pola serangan melalui analisis data lalu lintas jaringan,yaitu dengan menggunakan metode *random forest*, random forest adalah *menchine learning* yang cara kerja nya membangun beberapa *decision trees* dan menggambungkan nya menjadi 1 kesimpulan sehingga mendapatkan hasil akurasi yang tinggi. Dengan menggunakan metode *random forest* juga kita dapat membedakan mana trafik normal dan mana yg mencurigakan [10]

Random Forest memiliki keunggulan dalam hal akurasi, kecepatan pemrosesan, serta kemampuannya dalam menangani data dalam jumlah besar dan berdimensi tinggi. Selain itu, metode ini relatif lebih tahan terhadap overfitting jika dibandingkan dengan pohon keputusan tunggal.[11]

Berbagai studi sebelumnya telah membuktikan bahwa *Random Forest* mampu mendeteksi berbagai jenis serangan siber dengan tingkat akurasi yang tinggi, termasuk serangan DDoS. Penelitian juga menunjukkan bahwa kombinasi antara fitur ekstraksi data lalu lintas dan algoritma klasifikasi seperti Random Forest dapat meningkatkan kinerja sistem deteksi secara keseluruhan.[12][13]

Penggunaan dataset yang tepat, pemilihan fitur yang relevan, serta tuning parameter model Machine Learning yang optimal akan sangat berpengaruh terhadap kinerja model dalam mendeteksi serangan. Oleh karena itu, dalam penelitian ini, dilakukan proses *preprocessing*, *feature selection*, dan *validasi model* secara teliti untuk menghasilkan sistem deteksi yang andal.[14]

Dengan pendekatan ini, diharapkan sistem dapat secara otomatis mengenali adanya ancaman DDoS pada perangkat Smart Home, serta memberikan peringatan dini kepada pengguna atau sistem keamanan. Hal ini dapat membantu mencegah

kerusakan lebih lanjut dan menjaga keberlangsungan fungsi perangkat IoT secara optimal.[15]

Pada penelitian ini akan menggunakan dataset COMNET SMARTHOME yang melakukan simulasi serangan DDoS pada perangkat smarthome dengan cara membanjiri atau mengirim banyak permintaan pada jaringan IOT smarthome sehingga jaringan tersebut tidak dapat berfungsi.

Dalam penelitian ini akan mendeteksi serangan DDoS pada perangkat smarthome dengan metode yang akan digunakan adalah random forest oleh karena itu penelitian ini akan diberi judul "*Deteksi Serangan DDoS Pada Perangakat Smarthome Dengan Menggunakan Metode Random Forest"* dengan harapan penelitian ini akan memberikan efektifitas untuk mendeteksi serangan DDoS dengan menggunakan metode random forest.

1.2 Rumusan Masalah

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

1. Bagaimana cara model Random Forest digunakan untuk mengklasifikasi *Distributed Denial of Service*(DDOS) pada jaringan smarthome ?
2. Bagaimana Tingkat akurasi dan presisi dengan menggunakan random forest untuk mendeteksi serangan DDoS pada perangkat smarthome?
3. Apa saja fitur jaringan yang paling berpengaruh untuk mendeteksi serangan DDoS pada perangkat 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. Penelitian ini hanya mendeteksi 1 serangan cyber yaitu *Distributed denial of Service (DDoS)*

3. Studi hanya focus untuk mendeteksi serangan dan Tidak membahas mengenai pencegahan serangan *Distributed denial of Service (DDoS)*

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. Menjalankan dan mendapatkan hasil dari model *Random Forest* untuk mendeteksi serangan *Distributed denial of Service (DDoS)* pada perangkat smarthome.
2. Menganalisis Tingkat akurasi dalam mendeteksi serangan *Distributed denial of Service (DDoS)* pada perangkat smarthome dengan menggunakan metode *Random Forest.*
3. Mengidentifikasi fitur jaringan yang paling berpengaruh untuk mendeteksi serangan *Distributed denial of Service (DDoS)* pada perangkat smarthome menggunakan *Random Forest.*

1.5 Manfaat

Adapun manfaat dari penelitian tugas akhir ini antara lain adalah:

1. Memahami apa saja fitur jaringan yang paling berpengaruh dalam serangan *Distributed denial of Service (DDoS)* pada perangkat smarthome dengan menggunakan metode *Random Forest.*
2. Dapat memberikan hasil seberapa banyak data serangan dan data benign yang akan didapatkan dengan menggunakan metode *Random forest.*
3. Mengevaluasi seberapa tinggi Tingkat akurasi dari model *Random Forest* dalam mendeteksi serangan *Distributed denial of Service (DDoS)* pada perangkat smarthome.

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 *Distributed denial of Service* menggunakan algoritma *Random Forest*

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

Bab ini menjelaskan secara umum dan sistematis mengenai topik penelitian. Adapun pokok bahasan dalam bab ini meliputi **latar**

belakang, **rumusan masalah**, **batasan masalah**, **tujuan penelitian**, **manfaat penelitian**, **metodologi penelitian secara garis besar**, serta **sistematika penulisan** skripsi.

BAB II – TINJAUAN PUSTAKA

Bab ini memuat **kajian teoritis dan studi literatur** yang berkaitan dengan topik penelitian. Isi dari bab ini meliputi penjelasan konsep dasar mengenai **Distributed Denial of Service (DDoS)**, metode **machine learning**, khususnya algoritma **Random Forest**, serta pembahasan terhadap penelitian-penelitian sebelumnya yang relevan sebagai dasar dan pembanding dalam penyusunan skripsi ini.

BAB III – METODOLOGI PENELITIAN

Bab ini menguraikan secara rinci **metode yang digunakan dalam penelitian**. Penjelasan mencakup tahapan-tahapan pelaksanaan penelitian, seperti **pengumpulan data**, **pra-pemrosesan data**, **implementasi algoritma Random Forest**, dan **perancangan model deteksi DDoS**. Selain itu, dijelaskan pula desain sistem dan parameter evaluasi yang digunakan untuk mengukur performa model.

BAB IV – HASIL DAN PEMBAHASAN

Bab ini menyajikan **hasil penelitian** yang diperoleh dari proses implementasi dan pengujian model. Data hasil pengujian dianalisis secara menyeluruh untuk menilai efektivitas dan akurasi sistem deteksi yang dibangun. Pembahasan dalam bab ini juga mencakup interpretasi hasil serta perbandingan dengan penelitian sebelumnya apabila relevan.

BAB V – KESIMPULAN DAN SARAN

Bab terakhir ini berisi **kesimpulan** yang diambil berdasarkan hasil penelitian dan pembahasan yang telah dilakukan. Selain itu, disampaikan pula **saran-saran** yang ditujukan untuk pengembangan lebih lanjut, baik bagi peneliti selanjutnya maupun penerapan sistem di dunia nyata

DAFTAR PUSTAKA

[1] S. Sharma, "5G Wireless Technology: Future of Mobile Communication," *International Journal of Emerging Technology and Advanced Engineering*, vol. 6, no. 5, pp. 155–160, 2016.

[2] M. D. Othman, H. Hashim, and M. Z. A. A. Kadir, "Smart Home Technology Using IoT: A Review," *International Journal of Engineering and Technology (IJET)*, vol. 7, no. 2.29, pp. 34–38, 2018.

[3] A. Z. Alkar and U. Buhur, "An Internet Based Wireless Home Automation System for Multifunctional Devices," *IEEE Transactions on Consumer Electronics*, vol. 51, no. 4, pp. 1169–1174, 2005.

[4] M. H. Bhatti et al., "IoT DDoS Attack Detection Using Machine Learning," *Sensors*, vol. 20, no. 13, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/13/3697

[5] D. Singh and A. Kapoor, "Security Challenges in IoT: A Survey," *International Journal of Computer Applications*, vol. 159, no. 9, pp. 26–29, 2017.

[6] M. R. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 303–336, 2014.

[7] M. H. Bhatti et al., "IoT DDoS Attack Detection Using Machine Learning," *Sensors*, vol. 20, no. 13, p. 3697, 2020.

[8] J. M. Kizza, *Guide to Computer Network Security*, 4th ed. Cham: Springer, 2015.

[9] I. Ahmad et al., "Artificial Intelligence (AI) Applications for Cybersecurity," *IEEE Access*, vol. 7, pp. 124579–124612, 2019.

[10] L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[11] S. B. Kotsiantis, "Decision Trees: A Recent Overview," *Artificial Intelligence Review*, vol. 39, no. 4, pp. 261–283, 2013.

[12] A. Shone et al., "A Deep Learning Approach to Network Intrusion Detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[13] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2986–2998, 2016.

[14] S. A. Mehdi, M. S. Aslam, and H. F. Ahmad, "Data Preprocessing and Feature Selection for Machine Learning Intrusion Detection Systems," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 2, pp. 90–97, 2021.

[15] N. Moustafa and 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.