KLASIFIKASI SERANGAN DDoS PADA JARINGAN IoT DENGAN MENGGUNAKAN ALGORITMA *K-NEAREST NEIGHBORS (KNN)*

SKRIPSI

Oleh :

Said Usman Rizieq

09011281924075

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

KLASIFIKASI SERANGAN DDoS PADA JARINGAN IoT DENGAN MENGGUNAKAN ALGORITMA *K-NEAREST NEIGHBORS (KNN)*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

Said Usman Rizieq
09011281924075

Mengetahui, Desember 2023

Pembimbing TA,

Ketua Jurusan Sistem Komputer

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

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

ii

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Senin

Tanggal : 8 Januari 2024

Tim Penguji

1. Ketua : Ahmad Fali Okilas, M.T.
2. Sekretaris : Iman Saladin B. Azhar, S.Kom., M.SI.
3. Penguji : Ahmad Heryanto, M.T.
4. Pembimbing : Prof. Deris Stiawan, M.T., Ph.D.

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M. T.

NIP. 196612032006041001

iii

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Said Usman Rizieq

NIM : 09011281924075

Judul : Klasifikasi Serangan DDoS Pada Jaringan IoT Dengan Menggunakan Algoritma K-Nearest Neighbors (KNN)

Hasil Pengecekan Plagiat/Turnitin : 3%

Menyatakan bahwa laporan tugas akhir ini adalah hasil karya saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Saya sepenuhnya menyadari bahwa jika terbukti adanya penjiplakan atau plagiat dalam laporan tugas akhir ini, saya siap menerima sanksi akademik dari Universitas Sriwijaya. Pernyataan ini saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.

Palembang, Januari 2024

Yang menyatakan,

Said Usman Rizieq

NIM. 09011281924075

iv

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Penulis mengucapkan rasa puji dan syukur kepada Allah SWT yang telah melimpahkan rahmat dan karunia-Nya yang luar biasa serta tak henti-hentinya. Berkat anugerah tersebut, penulis berhasil menyelesaikan Tugas Akhir dengan judul **"Klasifikasi Serangan DDoS pada Jaringan IoT dengan Menggunakan Algoritma *K-Nearest Neighbors (KNN)"***. Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga, sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Penyelesaian penyusunan Tugas Akhir ini tidak terlepas dari kontribusi semua pihak yang memberikan ide, bimbingan, saran, serta bantuan dalam proses penulisan Tugas Akhir ini. antara lain :

1. Allah SWT yang melimpahkan segala kenikmatan dan kesempatan kepada penulis sehingga dapat menyelesaikan Tugas Akhir ini.
2. Kepada kedua orang tua saya Bpk. Said Ali dan almh. Ibu Syarifah Farah Delima serta saudara saya Said Muhammad Ghiffary yang selalu mendoakan serta mendorong dan mendukung baik secara moral dan material selama ini.
3. Bapak Prof.DR. Erwin, S.Si., M.Si., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Julian Supardi, S.Pd., M.T. selaku Wakil Dekan Bidang Akademik di Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. H. Sukemi, M.T., selaku ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Ahmad Heryanto. S.Kom., MT. selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer.
7. Bapak Prof.Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Tugas Akhir.
8. Mbak Nurul Afifah selaku dosen Sistem Komputer yang telah membantu dan memberikan masukan selama pengerjaan Tugas Akhir.

9. Bapak dan Ibu dosen Jurusan Sistem Komputer yang telah berkenan berbagi ilmu dan pengalamannya dengan saya.
10. Mbak Sari, selaku admin Jurusan Sistem Komputer yang turut membantu dalam pengurusan seluruh dokumen administrasi selama masa perkuliahan.
11. Teman – teman seperjuangan Jurusan Sistem Komputer Angkatan 2019.
12. Seluruh pihak yang tergabung dalam Comnets yang menjadi anggota dalam tim penelitian ini.
13. Teman – teman saya yang tergabung dalam Grup BACOD Mobile yang selalu memberikan dukungan kepada penulis.
14. Semua pihak yang tidak bisa penulis sebutkan satu per satu, namun telah memberikan semangat dan doa.
15. Jurusan Sistem Komputer.
16. Almamater.

Penulis menyadari bahwa dalam penyusunan Tugas Akhir ini masih sangat jauh dari kata sempurna. Oleh karena itu penulis mengharapkan kritik dan saran yang membangun, semoga Tugas Akhir ini dapat bermanfaat dan berguna bagi siapa saja yang membacanya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, Januari 2024

Penulis,

Said Usman Rizieq

NIM. 09011281924075

KLASIFIKASI SERANGAN DDoS PADA JARINGAN IoT DENGAN MENGGUNAKAN ALGORITMA K-NEAREST NEIGHBORS (KNN)

SAID USMAN RIZIEQ (09011281924075)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

Email : Saidusmanr@gmail.com

ABSTRAK

Dalam beberapa tahun terakhir, sensor Internet of Things (IoT) telah semakin terintegrasi dalam berbagai perangkat dan bidang. Oleh karena itu kemanan sensor IoT semakin rentan terhadap serangan.Dalam penelitian ini, digunakan Algoritma *K-Nearest Neighbors (KNN)* untuk mengklasifikasi serangan dalam dataset. Dataset diperoleh dari interaksi antara serangan DDos dan interaksi normal dan diseimbangkan dengan teknik oversampling *ADASYN*. Model terbaik mencapai akurasi 89,29%. Dengan perbandingan parameter pada *KNN*, model menunjukkan hasil yang konsisten dengan akurasi rata-rata mencapai 85,94%. Hasil ini mengindikasikan bahwa model memiliki kinerja yang konsisten dan dapat diandalkan dalam tugas klasifikasi yang diberikan.

Kata Kunci : *Internet of Things*, Klasifikasi Serangan, *K-Nearest Neighbors*

CLASSIFICATION OF DDoS ATTACKS ON IoT NETWORKS USING THE K-NEAREST NEIGHBORS (KNN) ALGORITHM

SAID USMAN RIZIEQ (09011281924075)

Computer Engineering Department, Computer Science Faculty

Sriwijaya University

Email : Saidusmanr@gmail.com

ABSTRACT

In recent years, Internet of Things (IoT) sensors have become increasingly integrated into various devices and fields. Therefore, the security of IoT sensors is becoming more vulnerable to attacks. In this research, the K-Nearest Neighbors (KNN) algorithm is employed to classify attacks in the dataset. The dataset is obtained from interactions between DDos attacks and normal interactions, and it is balanced using the ADASYN oversampling technique. The best model achieves an accuracy of 89.29%. Comparing the parameters in KNN, the model consistently shows results with an average accuracy of 85.94%. These results indicate that the model exhibits consistent and reliable performance in the given classification task.

Keywords : *Anomaly Detection, Attacks Classification, K-Nearest Neighbors*

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) diusulkan pertama kali pada tahun 1999 oleh Kevin Ashton. Pada Jurnal [1] dejelaskan bahwa IoT adalah *intellegent object* yang dapat menyalurkan data secara mandiri tanpa bantuan dari pihak ketiga. IoT dapat bekerja melalui jaringan internet dengan kemampuan mengarahkan banyak objek pintar dan peralatan komputasi cerdas lainnya untuk berinteraksi dengan lingkungannya.Pada jurnal penelitian [2] disebutkan bahwa sensor IoT sekarang ini sudah disisipkan dalam perangkat seluler, perangkat medis, lingkungan industri, dan lain sebagainya, dengan ini, ini akan berimplikasi terhadap masyarakat banyak. H.J Saleem dalam jurnal nya[3] menerangkan IoT sendiri telah memberikan banyak manfaat dan kelancaran pada banyak aspek dalam kehidupan manusia.Tuntutan terhadap sistem jaringan IoT yang aman sangat diharapkan guna meningkatkan pemanfaatan aplikasi IoT pada seluruh sensor perangkat IoT.

Keamanan jaringan merupakan aspek penting dalam sistem teknologi informasi modern, seperti yang diterangkan dalam jurnal [4] yang menjabarkan bahwa hal itu dikarenakan meningkatnya ketergantungan pada jaringan yang saling terhubung sehingga menjadikannya rentan terhadap berbagai ancaman dunia digital. Akses tidak sah, pelanggaran data, dan aktivitas jahat menimbulkan risiko signifikan terhadap kerahasiaan, integritas, dan ketersediaan sumber daya jaringan.

S.Shantos di dalam penelitiannya [5] menjelaskan bahwa keamanan untuk jaringan IoT sekarang ini dalam ancaman, ini dikarenakan serangan cyber yang sudah dapat menginfiltrasi perangkat IoT target (pengguna) dengan melalui beberapa serangan Denial of Service (DoS). Ini dapat terjadi dikarenakan perangkat IoT yang digunakan oleh pengguna dapat diakses dengan lebih mudah, sebab mempunyai tingkatan keamanan yang lebih rendah dikomparasikan dengan server.

Kaspersky Lab dan B2B International dalam jurnalnya [6] menyebutkan angka bahwa 40% lebih bisnis yang sudah menjadi korban serangan dari DDoS dan DoS.

Kimmi Kumari Pada jurnal nya [7] menyebutkan bahwa Beberapa tahun terakhir serangan *DDoS* telah menimbulkan dampak yang substansial untuk pengguna IoT dalam bidang industri, dan pemerintahan.Pada jurnal [8] [9] dijelaskan bahwa Adanya serangan

DDoS dapat menyulitkan organisasi seperti terganggunya aktivitas online, data cloud, dan perangkat yang terhubung dengan internet.

Pengklasifikasian suatu Serangan malware baik Botnet ataupun jenis lainnya memiliki tujuan untuk dapat mengetahui adanya Tindakan atau interaksi yang tidak normal dan mencurigakan pada suatu aliran jaringan umum. Beberapa penelitian seperti [10] melakukan pendeteksian serangan DDoS dengan beberapa Dataset serta metode termasuk support vector machines (SVM), naive Bayes (NB), dan K-nearest neighbors (KNN) menunjukkan bahwa mengidentifikasi serangan DDoS pada perangkat IoT perlu pendekatan yang lebih mutakhir serta lebih terperinci. Metode identifikasi tradisional seperti pengujian statistik telah digunakan untuk mengidentifikasi Aliran interaksi yang mencurigakan, namun teknik ini seringkali tidak efektif. Oleh karena itu, diperlukan pendekatan yang lebih canggih. Pendekatan yang digunakan ialah dengan Algoritma *k-Nearest Neighbors (KNN)* sebagai suatu metode *machine learning* yang lebih efisien dan terperinci.

K-Nearest-Neighbours (KNN) didefinisikan dengan metode klasifikasi non-parametrik, ini efektif untuk berbagai kasus dan sederhana prosesnya dalam mengimplementasikan KNN, dengan memilih nilai k yang tepat, kesuksesan klasifikasi dengan nilai yang tinggi bergantung dengan nilainya tersebut. Dalam arti tertentu, metode KNN dibiaskan oleh k. Terdapat berbagai metode dalam memilih nilai k, oleh karena itu KNN banyak digunakan dalam penelitian yang membutuhkan pengolahan data yang banyak seperti penelitian oleh Arvind Prasad [10] yang melakukan penelitian dengan lima dataset dengan masing – masing dataset berjumlah lebih dari lima juta data dan menunjukkan hasil akurasi yang sangat signifikan menggunakan metode KNN. Kemudian penelitian Gongde Guo [11] yang menjelaskan bahwa model KNN dapat digunakan untuk mengefisiansikan waktu dalam pengolahan data dalam jumlah besar.

Berdasarkan pada ulasan diatas maka penulis mengusulkan untuk melakukan penelitian dengan judul "*Klasifikasi Serangan DDoS pada Jaringan IoT dengan Menggunakan Algoritma K-Nearest Neighbors (KNN)*"., ini tujuannya agar dapat melakukan pengembangan model yang dapat mengklasifikasikan serangan DDoS pada jaringan IoT dengan tingkat akurasi yang tinggi.

1.2 Tujuan

Adapun tujuan dari penelitian ini, yaitu antara lain:

1. Membedakan antara data serangan dan data normal pada dataset.

2. Menyeimbangkan dataset dengan menggunakan oversampling
3. Mengklasifikasi serangan pada jaringan IoT dengan menggunakan Algoritma *K-Nearest Neighbor (KNN).*

1.3 Manfaat

Adapun manfaat dari penelitian ini yaitu:

1. Identifikasi perbedaan antara data serangan DDoS dan data normal dalam dataset.
2. Menangani ketidakseimbangan data dengan menerapkan metode oversampling
3. Klasifikasi data sebagai serangan DDoS atau data normal dalam konteks jaringan IoT menggunakan Algoritma K-Nearest Neighbor (KNN).

1.4 Rumusan Masalah

Dengan merujuk pada latar belakang di atas, rumusan masalah dalam penelitian ini dapat dirangkum sebagai berikut:

1. Bagaimana proses penyiapan dataset untuk klasifikasi serangan DDoS?
2. Bagaimana cara yang dapat dilakukan untuk mengatasi data yang tidak seimbang (*imbalance data*) agar mencapai kinerja optimal?
3. Bagaimana cara mengklasifikasikan data Serangan DDoS dan data normal pada jaringan IoT?

1.5 Batasan Masalah

Batasan masalah dalam ruang lingkup penelitian tugas akhir ini mencakup hal-hal berikut:

1. Menggunakan dataset *UNSW2018 Iot Botnet dataset(2018),*.
2. Dataset yang digunakan memiliki distribusi data yang tidak seimbang
3. Menggunakan Algoritma *K-Nearest Neighbor (KNN).*untuk mengklasifikasi serangan DDoS.

1.6 Metodologi Penelitian

1. Metode Studi Pustaka dan Literatur

   Dalam tahap ini, penulis melakukan pencarian dan pengumpulan referensi melalui buku dan berbagai jurnal berhubungan dengan penelitian ini.

2. Metode Konsultasi

   Metode ini melibatkan konsultasi dengan pihak yang memiliki pengetahuan dan pengalaman yang sesuai, baik langsung dan tidak, guna mengatasi permasalahan

yang timbul dalam penelitian ini..

3. Metode Pembuatan Model

   Dalam tahap ini, dilibatkan proses perancangan dan pembuatan model dengan memanfaatkan beragam simulasi dan perangkat lunak untuk mendukung proses pembuatan model yang diperlukan.

4. Metode Pengujian dan Validasi

   Pengujian dan validasi dilangsungkan pada sistem yang dikembangkan guna mengidentifikasi berbagai batasan dalam kinerja sistem, serta untuk mengevaluasi tingkat akurasi yang dihasilkan.

5. Metode Analisis

   Pada tahap analisis, hasil penelitian dianalisis dengan tujuan menghasilkan kesimpulan dan rekomendasi yang dapat menjadi acuan berharga untuk penelitian lanjutan.

1.7 Sistematika Penulisan

Adapun sistematika penulisan yang diterapkan dalam tugas akhir ini adalah sebagai berikut :

BAB I. PENDAHULUAN

Pada BAB I dijelaskan tentang landasan topik penelitian yang meliputi latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi penelitian dan sistematika penulisan yang digunakan dalam tugas akhir ini.

BAB II. TINJAUAN PUSTAKA

Pada BAB II berisi tentang penelitian terkait, dan teori terkait penelitian diantaranya *Internet of Things (IoT), DDoS, Instance-based learning*, dan juga metode *K-nearest neighbors (KNN).*

BAB III. METODOLOGI PENELITIAN

Pada BAB III akan dibahas tentang perancangan pada ruang pengujian dan perancangan pada model *KNN* untuk Klasifikasi serangan DDoS.

BAB IV. HASIL DAN PEMBAHASAN

Pada BAB IV akan dibahas tentang hasil pengujian dan pembahasan dari hasil yang didapat melelui penelitian yang dilakukan, serta hasil dari analisis dari klasifikasi serangan DDoS pada jaringan IoT dengan menggunakan algoritma K-nearest neighbors

(KNN).

BAB V. PENUTUP

Pada BAB V Akan dibahas mengenai kesimpulan yang diperoleh dari hasil penelitian serta rekomendasi terkait pengembangan sistem untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] R. Paudel, T. Muncy, and W. Eberle, “Detecting DoS Attack in Smart Home IoT Devices Using a Graph-Based Approach,” no. December, 2019, doi: 10.1109/BigData47090.2019.9006156.

[2] Y. S. Al-hadhrami, “Intelligent Machine Learning Architecture for Detecting DDoS attacks in IoT networks,” 2020.

[3] H. J. Saleem, *Internet of Things: Evolution and technologies from a security perspective*. Elsevier Ltd, 2019.

[4] V. Hnamte and J. Hussain, “Telematics and Informatics Reports Dependable intrusion detection system using deep convolutional neural network : A Novel framework and performance evaluation approach,” *Telemat. Informatics Reports*, vol. 11, no. April, p. 100077, 2023, doi: 10.1016/j.teler.2023.100077.

[5] S. Santhosh, “An Anomaly Behavior based Detection and Prevention of DoS Attack in IoT Environment,” *2017 Ninth Int. Conf. Adv. Comput.*, pp. 287–292, 2017.

[6] Warwick Ashford, “Businesses blame rivals for DDoS attacks,” 2017. [Online]. Available: https://www.computerweekly.com/news/450414239/Businesses-blame-rivals-for-DDoS-attacks.

[7] K. Kumari and M. Mrunalini, “Detecting Denial of Service attacks using machine learning algorithms,” *J. Big Data*, 2022, doi: 10.1186/s40537-022-00616-0.

[8] A. Mishra, P. S. Sharma, and A. Pandey, “An Enhanced DDoS TCP Flood Attack Defence System in a Cloud Computing.”

[9] J. Li, “DETECTION OF DDOS ATTACKS BASED ON DENSE NEURAL NETWORKS , AUTOENCODERS AND PEARSON Table of Contents,” no. April, 2020.

[10] A. Prasad and S. Chandra, “VMFCVD : An Optimized Framework to Combat Volumetric DDoS Attacks using Machine Learning,” *Arab. J. Sci. Eng.*, vol. 47, no. 8, pp. 9965–9983, 2022, doi: 10.1007/s13369-021-06484-9.

[11] C. Paper, G. Guo, H. Wang, D. A. Bell, and Y. Bi, “KNN Model-Based Approach in Classification KNN Model-Based Approach in Classification,” no. January, 2003, doi: 10.1007/978-3-540-39964-3.

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

[13] A. L. Yaser, H. M. Mousa, M. Hussein, A. L. Yaser, H. M. Mousa, and M. Hussein,

"Improved DDoS Detection Utilizing Deep Neural Networks and Feedforward Neural Networks as Autoencoder Improved DDoS Detection Utilizing Deep Neural Networks and Feedforward Neural Networks as Autoencoder."

[14] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics : Bot-IoT dataset," *Futur. Gener. Comput. Syst.*, vol. 100, pp. 779–796, 2019, doi: 10.1016/j.future.2019.05.041.

[15] R. A. Mouha, "Internet of Things (IoT)," pp. 77–101, 2021, doi: 10.4236/jdaip.2021.92006.

[16] S. S. Priya, "Machine Learning based DDOS Detection," pp. 234–237, 2020.

[17] D. Tree and E. Resolution, "Instance-based learning algorithms."

[18] J. S. Richman, *Multivariate Neighborhood Sample Entropy : A Method for Data Reduction and Prediction of Complex Data*, 1st ed., vol. 487, no. 11. Elsevier Inc., 2011.

[19] M. S. Shelke, P. R. Deshmukh, and P. V. K. Shandilya, "A Review on Imbalanced Data Handling Using Undersampling and Oversampling Technique," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 4, pp. 444–449, 2017, doi: 10.23883/ijrter.2017.3168.0uwxm.

[20] V. S. Spelmen and R. Porkodi, "A Review on Handling Imbalanced Data," *2018 Int. Conf. Curr. Trends Towar. Converging Technol.*, no. December, pp. 1–11, 2018.

[21] R. Susmaga, "Confusion Matrix Visualization," 2004.