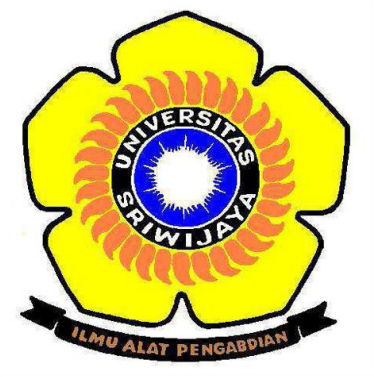
VISUALISASI DATA SERANGAN *UDP FLOOD* PADA JARINGAN *INTERNET OF THINGS* (IoT) MENGGUNAKAN ALGORITMA *NAIVE BAYES CLASSIFIER*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer



DISUSUN OLEH :

CHRISTOPER MARLO

09011181823009

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

HALAMAN PENGESAHAN

VISUALISASI DATA SERANGAN *UDP FLOOD* PADA JARINGAN *INTERNET OF THINGS* (IoT) MENGGUNAKAN ALGORITMA *NAIVE BAYES CLASSIFIER*

TUGAS AKHIR

Program Studi Sistem Komputer Jenjang S1

Oleh :

CHRISTOPER MARLO

09011181823009

Palembang, 12 Januari 2023

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

PERSETUJUAN

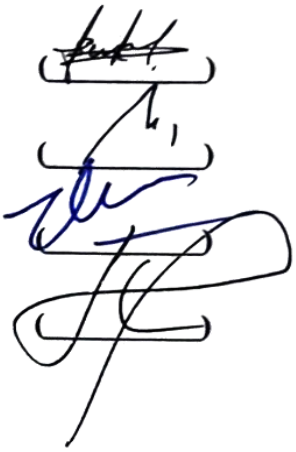
Telah diuji dan lulus pada :

Hari : Rabu

Tanggal : 28 Desember 2022

Tim Penguji :

1. **Ketua** : **Sarmayanta Sembiring, M.T.**
2. **Sekretaris** : **Adi Hermansyah, M.T.**
3. **Pembimbing** : **Deris Stiawan, M.T., Ph.D.**
4. **Penguji** : **Huda Ubaya, M.T.**



Mengetahui, 09/1/23

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Christoper Marlo

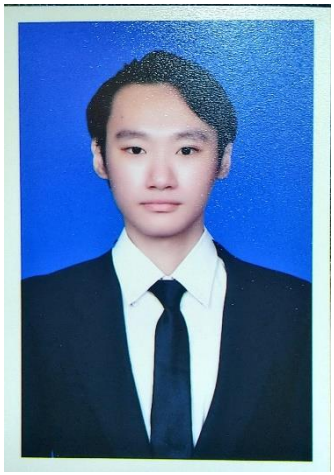
NIM : 09011181823009

Judul : Visualisasi Data Serangan UDP Flood Pada Jaringan Internet Of Things (IoT) Menggunakan Algoritma Naive Bayes Classifier

Hasil Pengecekan Software iThenticate/Turnitin : 15%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya saya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



Palembang, 09 Januari 2023

Christoper Marlo
NIM. 09011181823009

DATA VISUALIZATION OF UDP FLOOD ATTACKS ON INTERNET OF THINGS (IoT) NETWORKS USING THE NAIVE BAYES CLASSIFIER ALGORITHM

Christoper Marlo (09011181823009)

Dept. Of Computer System, Faculty of Computer Science, Sriwijaya University

Email : christopermarlo1379@gmail.com

ABSTRACT

This study focuses on visualize the UDP Flood Attack Pattern on Internet of Things Network Dataset (doi.org/10.5281/zenodo.4436127). The purpose of this study is to obtain a visual form of the dataset classification results using the Naive Bayes Classifier algorithm which shows the difference between UDP Flood attack data and normal data. The method used in this study is the Naive Bayes Classifier as a classifier that applied to datasets. The results from this study showed that the classification carried out using the Naive Bayes Classifier algorithm obtained a classification accuracy rate of 99.80% using the Multinominal Naive Bayes model which applied to the dataset. The classification results are visualized in the form of parallel coordinate graphs which conclude the difference between UDP Flood attack data and normal data is clearly obtained and marked by differences in line colors in the graph produced within this study.

Kata Kunci : *Data Visualization, UDP Flood, Internet of Things (IoT), Naive Bayes Classifier, Parallel Coordinates*

Acknownledged By,

Head of Computer Systems Department	**Supervisor**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

VISUALISASI DATA SERANGAN *UDP FLOOD* PADA JARINGAN *INTERNET OF THINGS* (IoT) MENGGUNAKAN ALGORITMA *NAIVE BAYES CLASSIFIER*

Christoper Marlo (09011181823009)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : christopermarlo1379@gmail.com

ABSTRAK

Penelitian ini melakukan visualisasi pada dataset *UDP Flood Attack Pattern on Internet of Things Network Dataset (doi.org/10.5281/zenodo.4436127)*. Tujuan dari penelitian ini ialah mendapatkan bentuk visual dari hasil klasifikasi dataset menggunakan algoritma *Naive Bayes Classifier* yang menunjukkan perbedaan antara data serangan *UDP Flood* dan data normal. Metode yang digunakan dalam penelitian ini adalah *Naive Bayes Classifier* sebagai pengklasifikasi yang diterapkan pada dataset. Hasil dari penelitian ini menunjukkan bahwa klasifikasi yang dilakukan menggunakan algoritma *Naive Bayes Classifier* didapatkan tingkat akurasi klasifikasi sebesar 99,80% menggunakan model *Multinominal Naive Bayes* yang diterapkan pada dataset. Hasil klasifikasi divisualisasikan dengan bentuk grafik *parallel coordinate* sehingga didapatkan dengan jelas perbedaan antara data serangan *UDP Flood* dan data normal yang ditandai dengan perbedaan warna garis pada grafik yang dihasilkan pada penelitian ini.

Kata Kunci : *Data Visualization, UDP Flood, Internet of Things (IoT), Naive Bayes Classifier, Parallel Coordinates*

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

KATA PENGANTAR

Puji dan syukur saya panjatkan ke hadirat Allah Yang Maha Esa yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penulisan proposal tugas akhir ini yang berjudul "**Visualisasi Data Serangan *UDP FLOOD* Pada Jaringan *Internet Of Things* (IoT) Menggunakan Algoritma *Naive Bayes Classifier***"

Pada penyusunan tugas akhir ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah Yang Maha Esa dan terima kasih kepada yang terhormat :

1. Allah Yang Maha Esa atas rahmat dan kesehatan serta kesempatan yang diberikan kepada penulis dalam penulisan tugas akhir ini.
2. Kepada Orang tua, Saudara, dan Keluarga Besar yang selalu mendoakan dan memberikan motivasi serta dukungan kepada penulis.
3. Bapak Jaidan Jauhari, M.T. 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 Dr. Ir. Bambang Tutuko, M.T. sebagai Pembimbing Akademik Penulis di Jurusan Sistem Komputer.
6. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing Tugas Akhir yang memberikan saran selama proses penulisan Tugas Akhir.
7. Mba Sari dan Mba Renny selaku Admin Jurusan Sistem Komputer yang telah membantu dalam melancarkan proses administrasi.

8. M. Rifqi Abiyyu Ariq dan Budiman Alfian selaku teman seperjuangan dalam penelitian serta membantu dalam masa sulit selama pengerjaan Tugas Akhir.
9. A Josman Pratama dan Ronnie Radhitya Raffi selaku asisten di Center Of Excellence (CoE) Universitas Sriwijaya serta teman dekat dalam masa pengerjaan Tugas Akhir.
10. Teman saya Garinnang Baiduri Salasa, M. Alfat Hayatur Rizon, Arif Tumpal Leonardo Sianturi, M. Dion Iqbal, M. Wahyu Fadli selaku teman yang membantu dan menemani penulis selama pengerjaan Tugas Akhir.
11. Seluruh Staff dan Pegawai Jurusan Sistem Komputer serta Teman Seperjuagan Sistem Komputer 2018 yang telah membersamai.
12. Dan semua pihak yang ikut terlibat serta membantu penulis.

Penulis menyadari bahwa dalam penulisan proposal tugas akhir ini masih jauh dari kata sempurna, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar dapat menjadi lebih baik lagi dikemudian hari.

Akhir kata penulis menyampaikan permohonan maaf bila terdapat perkataan yang tidak berkenan dan berharap semoga proposal tugas akhir ini bermanfaat bagi kita semua, terutama bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumber referensi dalam peningkatan mutu pembelajaran.

Palembang, 09 Januari 2023

Christoper Marlo

NIM. 09011181823009

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Terdapat beberapa cara dalam menyajikan data, diantaranya ialah dengan visualisasi data. Visualisasi Data merupakan penyajian data yang menarik dan mudah untuk dipahami menggunakan berbagai jenis grafik. Oleh karena itu, visualisasi data dapat membantu mempercepat pengambilan keputusan yang tepat. Visualisasi data dapat menggambarkan relasi dan pola antara variabel yang ada dalam data berdasarkan penelitian [1].

Teknologi jaringan seperti IoT tumbuh pada tingkat yang stabil dalam hal pengguna, sistem menengah, dan aplikasi. Statistik terbaru juga menunjukkan bahwa jumlah perangkat yang terhubung akan terus tumbuh menuju beberapa miliar pada tahun 2025 dikutip dari penelitian [2]. Saat ini, sebagian besar pengguna perangkat IoT tidak menyadari kerentanan keamanan perangkat IoT dan bagaimana hal itu dapat mempengaruhi jaringan tempat mereka berada, dalam penelitian [3]. Jaringan IoT dibatasi oleh beberapa faktor baru seperti sejumlah besar perangkat dan objek yang dapat berinteraksi satu sama lain secara kompleks, menggunakan protokol keamanan yang berbeda. *End node* (sensor/perangkat) melekat pada jaringan IoT dan berkomunikasi dengan server data/aplikasi melalui *gateway*. Data yang dikumpulkan biasanya ditransmisikan dari *gateway* ke *server* data/aplikasi menggunakan protokol *File Transfer Protocol* (FTP) berdasarkan penelitian [4].

Seiring dengan peningkatan eksponensial dalam penggunaan Internet dan kemajuan di Internet, ancaman keamanan terutama *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS) juga meningkat secara eksponensial berdasarkan pada penelitian [5]. Serangan DoS mencegah sumber daya (contohnya *server*) dalam jaringan diakses oleh pengguna, baik sementara atau tanpa batas waktu. Serangan DoS dilakukan oleh satu penyerang (*attacker*), sedangkan serangan DDoS dilakukan oleh beberapa penyerang (*attacker*).

Dalam serangan ini, sejumlah besar lalu lintas jaringan yang dihasilkan menghabiskan sumber daya *server* dan mencegah pengguna yang sah mengakses layanannya berdasarkan pada penelitian [6].

Berdasarkan penelitian [7], DoS dan DDoS menjadi tantangan besar dalam sebuah jaringan karena mempengaruhi jaringan dalam berbagai tingkatan. Karena serangan DoS merupakan serangan *one-to-one*, hanya dengan menggunakan satu *compromised host* untuk mempengaruhi *bandwidth* jaringan yang kecil. Karena banyak alat yang tersedia dan sifatnya yang sederhana, *flooding packets* merupakan serangan DoS yang paling umum dan efektif. Seiring berjalannya waktu, *flooding tools* menjadi lebih canggih mengakibatkan *flooding tools* semakin mudah digunakan. Penyerang tanpa banyak pengetahuan tentang pemrograman dapat mengunduh *flooding tools* dan kemudian meluncurkan serangan DoS. *Flooding traffic* dari serangan DoS dapat berasal dari satu sumber atau beberapa sumber.

Penelitian [8] mengatakan bahwa klasifikasi merupakan masalah pembelajaran mesin umum dimana tujuannya adalah untuk menetapkan satu atau beberapa objek ke kelas yang benar. Banyak masalah klasifikasi di dunia nyata diselesaikan dengan menggabungkan *output* dari sekelompok prediktor, masing-masing dari mereka mengusulkan kelas yang mereka pikir sesuai dengan objeknya.

Naive Bayes Classifier adalah pengklasifikasi sederhana berdasarkan nilai-nilai probabilistik yang digunakan dalam teorema Bayes bersama dengan asumsi yang naif. Pengklasifikasi ini mengkonsolidasikan ada atau tidak adanya fitur tertentu yang tidak relevan dengan situasi saat ini. Dengan menggunakan pengaturan *supervised learning*, *Naive Bayes Classifier* dilatih untuk kumpulan data yang kecil sehingga sejumlah besar atribut dapat dideteksi, berdasarkan pada penelitian [9].

1.2 Perumusan Masalah

Penelitian ini dilakukan dengan rumusan masalah sebagai berikut :

1. Bagaimana klasifikasi antara data serangan DoS *UDP Flood* dan data normal pada jaringan *internet of things* (IoT) dengan menggunakan *machine learning* agar mendapatkan hasil prediksi maksimal?

2. Bagaimana hasil visualisasi dari algoritma *naive bayes classifier* yang diterapkan pada *machine learning* dalam visualisasi data?

1.3 Batasan Masalah

Batasan masalah dari tugas akhir ini ialah sebagai berikut :

1. Informasi beserta data yang digunakan pada penelitian ini sepenuhnya berasal dari Comnets Fasilkom Universitas Sriwijaya.

2. Penelitian ini sebatas melakukan visualisasi data serangan DoS *UDP Flood* pada jaringan *Internet of Things* menggunakan *machine learning* dengan menerapkan algoritma *Naive Bayes Classifier*.

3. *Output* yang dihasilkan dari penelitian ini berupa Visualisasi Data serangan DoS *UDP Flood* pada jaringan *Internet of Things* menggunakan *machine learning* dengan menerapkan algoritma *Naive Bayes Classifier*.

1.4 Tujuan

Tujuan dari penulisan tugas akhir ini :

1. Melakukan klasifikasi terhadap data serangan DoS *UDP Flood* dan data normal menggunakan *machine learning* dengan menerapkan algoritma *Naive Bayes Classifier*.

2. Melakukan visualisasi data hasil klasifikasi dengan menerapkan *machine learning* agar mempermudah proses analisis data pada jaringan *Internet of Things*.

1.5 Manfaat

Manfaat dari penulisan tugas akhir ini :

1. Penelitian ini diharapakan dapat menjadi acuan bagi peneliti lain yang membahas mengenai Visualisasi Data serangan DoS *UDP Flood* menggunakan *machine learning* pada jaringan *Internet of Things*.

2. Hasil dari penelitian ini dapat digunakan sebagai bahan informasi dan kajian bagi Fakultas Ilmu Komputer Universitas Sriwijaya dalam bidang Visualisasi Data menggunakan *machine learning*.

1.6 Sistematika Penulisan

Penyusunan penulisan tugas akhir yang disusun pada penelitian ini akan dijelaskan secara sistematis, tugas akhir ini disusun sebagai berikut :

1. BAB I : PENDAHULUAN

   Pada bab ini dijelaskan mengenai latar belakang, rumusan masalah, tujuan, manfaat, serta sistematika penulisan yang digunakan dalam penelitian ini.

2. BAB II : TINJAUAN PUSTAKA

   Bab ini berisikan studi literatur tentang teori-teori yang berkaitan dengan masalah Visualisasi Data menggunakan *machine learning* dengan mengimplementasikan algoritma *Naive Bayes Classifier*.

3. BAB III : METODOLOGI

   Bab ini akan menjelaskan mengenai kerangka kerja, perancangan sistem, langkah kerja dan metodologi yang akan dilakukan dalam proses penelitian ini.

4. BAB IV : ANALIS DAN PEMBAHASAN

   Bab ini berisikan proses, hasil dan analisa pengujian dari penelitian mengenai Visualisasi Data menggunakan *machine learning* dengan mengimplementasikan algoritma *Naive Bayes Classifier* untuk serangan berjenis *Denial of Service* (DoS).

5. BAB V : KESIMPULAN DAN SARAN

   Bab ini berisikan kesimpulan dari hasil penelitian yang diperoleh dan saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] J. R. Castillo and M. J. Flores, “Web-based music genre classification for timeline song visualization and analysis,” *IEEE Access*, vol. 9, pp. 18801–18816, 2021, doi: 10.1109/ACCESS.2021.3053864.

[2] A. O. Sangodoyin, M. O. Akinsolu, P. Pillai, and V. Grout, “Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning,” *IEEE Access*, vol. 9, pp. 122495–122508, 2021, doi: 10.1109/ACCESS.2021.3109490.

[3] R. Paudel, T. Muncy, and W. Eberle, “Detecting DoS Attack in Smart Home IoT Devices Using a Graph-Based Approach,” *Proc. - 2019 IEEE Int. Conf. Big Data, Big Data 2019*, pp. 5249–5258, 2019, doi: 10.1109/BigData47090.2019.9006156.

[4] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, “Investigating Brute Force Attack Patterns in IoT Network,” *J. Electr. Comput. Eng.*, vol. 2019, 2019, doi: 10.1155/2019/4568368.

[5] J. David and C. Thomas, “Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic,” *Comput. Secur.*, vol. 82, pp. 284–295, 2019, doi: 10.1016/j.cose.2019.01.002.

[6] I. Melih Tas, B. G. Unsalver, and S. Baktir, “A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism,” *IEEE Access*, vol. 8, pp. 112574–112584, 2020, doi: 10.1109/ACCESS.2020.3001688.

[7] H. Wang, D. Zhang, and K. G. Shin, “Change-point monitoring for the detection of DoS attacks,” *IEEE Trans. Dependable Secur. Comput.*, vol. 1, no. 4, pp. 193–208, 2004, doi: 10.1109/TDSC.2004.34.

[8] E. Manino, L. Tran-Thanh, and N. R. Jennings, “On the efficiency of data

collection for multiple Naïve Bayes classifiers," *Artif. Intell.*, vol. 275, pp. 356–378, 2019, doi: 10.1016/j.artint.2019.06.010.

[9] K. Wang, "Network data management model based on Naïve Bayes classifier and deep neural networks in heterogeneous wireless networks," *Comput. Electr. Eng.*, vol. 75, pp. 135–145, 2019, doi: 10.1016/j.compeleceng.2019.02.015.

[10] Y. Zhao, W. Cui, S. Geng, B. Bo, Y. Feng, and W. Zhang, "A malware detection method of code texture visualization based on an improved faster RCNN combining transfer learning," *IEEE Access*, vol. 8, pp. 166630–166641, 2020, doi: 10.1109/ACCESS.2020.3022722.

[11] D. Stiawan *et al.*, "Investigating UDP Flood Attack Pattern on Internet of Things Network," 2018, doi: 10.5281/ZENODO.4436127.

[12] C. K. Aridas, S. Karlos, V. G. Kanas, N. Fazakis, and S. B. Kotsiantis, "Uncertainty Based Under-Sampling for Learning Naive Bayes Classifiers under Imbalanced Data Sets," *IEEE Access*, vol. 8, pp. 2122–2133, 2020, doi: 10.1109/ACCESS.2019.2961784.

[13] P. Valdiviezo-Diaz, F. Ortega, E. Cobos, and R. Lara-Cabrera, "A Collaborative Filtering Approach Based on Naïve Bayes Classifier," *IEEE Access*, vol. 7, pp. 108581–108592, 2019, doi: 10.1109/ACCESS.2019.2933048.

[14] M. Ali, A. Alqahtani, M. W. Jones, and X. Xie, "Clustering and Classification for Time Series Data in Visual Analytics: A Survey," *IEEE Access*, vol. 7, pp. 181314–181338, 2019, doi: 10.1109/ACCESS.2019.2958551.

[15] T. Wiktorski, A. Krolak, K. Rosinska, P. Strumillo, and J. C. W. Lin, "Visualization of generic utility of sequential patterns," *IEEE Access*, vol. 8, pp. 78004–78014, 2020, doi: 10.1109/ACCESS.2020.2989165.

[16] Z. Chen, Z. Chen, and A. Delis, "An inline detection and prevention framework for distributed denial of service attacks," *Comput. J.*, vol. 50,

no. 1, pp. 7–40, 2007, doi: 10.1093/comjnl/bxl042.

[17] C. Siaterlis and B. Maglaris, “Detecting DDoS attacks using a multilayer Perceptron classifier,” *Design*, no. March 2005, pp. 1–14, 2004.

[18] A. Furfaro, P. Pace, and A. Parise, “Facing DDoS bandwidth flooding attacks,” *Simul. Model. Pract. Theory*, vol. 98, no. June 2019, p. 101984, 2020, doi: 10.1016/j.simpat.2019.101984.

[19] Z. Xue, J. Wei, and W. Guo, “A Real-Time Naive Bayes Classifier Accelerator on FPGA,” *IEEE Access*, vol. 8, pp. 40755–40766, 2020, doi: 10.1109/ACCESS.2020.2976879.

[20] D. Stiawan *et al.*, “Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network,” *IEEE Access*, vol. 9, pp. 116475–116484, 2021, doi: 10.1109/ACCESS.2021.3105517.

[21] D. Stiawan, S. Sandra, E. Alzahrani, and R. Budiarto, “Comparative analysis of K-Means method and Naïve Bayes method for brute force attack visualization,” *2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017*, pp. 177–182, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905286.

[22] R. F. Malik, E. Pratama, H. Ubaya, R. Zulfahmi, D. Stiawan, and K. Exaudi, “Object Position Estimation Using Naive Bayes Classifier Algorithm,” *Proc. 2018 Int. Conf. Electr. Eng. Comput. Sci. ICECOS 2018*, vol. 17, pp. 39–44, 2019, doi: 10.1109/ICECOS.2018.8605198.

[23] R. Andika, “Pengenalan Pola Serangan Denial of Service (UDP Flood) pada Jaringan Internet of Things (IoT) dengan Algoritma Decision Tree C4.5,” 2018, doi: 10.5281/ZENODO.4436127.

[24] D. Stiawan *et al.*, “UDP Flood Attack Pattern on Internet of Things Network Dataset,” 2018, doi: 10.5281/ZENODO.4436127.

[25] L. Liu, P. Wang, J. Lin, and L. Liu, “Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning,” *IEEE Access*, vol. 9, pp. 7550–7563, 2021, doi: 10.1109/ACCESS.2020.3048198.