VISUALISASI SERANGAN TCP FIN FLOOD PADA JARINGAN IOT MENGGUNAKAN METODE *UNSUPERVISED LEARNING*

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

Anya Nur Defitri

09011182126017

PROGRAM STUDI SISTEM KOMPUTER

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

VISUALISASI SERANGAN TCP FIN FLOOD PADA JARINGAN IOT MENGGUNAKAN METODE *UNSUPERVISED LEARNING*

SKRIPSI

OLEH:

Anya Nur Defitri

09011182126017

PROGRAM STUDI SISTEM KOMPUTER

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

VISUALISASI SERANGAN TCP FIN FLOOD PADA JARINGAN IOT MENGGUNAKAN METODE UNSUPERVISED LEARNING

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

ANYA NUR DEFITRI

09011182126017

Pembimbing 1	**: Prof. Ir.Deris Stiawan, M.T., Ph.D.**
	NIP. 197806172006041002
Pembimbing 2	**: Nurul Afifah, M.Kom**
	NIP. 199211102023212049

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T

196612032006041001

AUTHENTICATION PAGE

FINAL TASK

VISUALIZATION OF TCP FIN FLOOD ATTACK ON IOT NETWORK USING UNSUPERVISED LEARNING METHOD

As one of the requirements for the completion of studies in

the S1 Computer Systems Study Program

By:

ANYA NUR DEFITRI
09011182126017

Supervisor 1	**: Prof. Ir.Deris Stiawan, M.T., Ph.D.**
	NIP. 197806172006041002
Supervisor 2	**: Nurul Afifah, M.Kom**
	NIP. 199211102023212049

Approved by,

Head of Computer Systems Department

Dr. Ir. Sukemi, M.T .
196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at

Tanggal : 11 Juli 2025

Tim Penguji:

1. Ketua : **Dr. Ir. Ahmad Heryanto, M.T.**
2. Penguji : **Ahmad Fali Oklilas, M.T.**
3. Pembimbing I : **Prof. Ir. Deris Stiawan, M.T., Ph.D.**
4. Pembimbing II : **Nurul Afifah, M.Kom**

Mengetahui, 9/8/25

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Anya Nur Defitri

NIM : 09011182126017

Judul : Visualisasi Serangan TCP FIN flood Pada IoT Menggunakan Metode *Unsupervised learning*

Hasil Pengecekan Software iThentivate/Turnitin: 4%

Menyatakan bahwa laporan Tugas Akhir ini sepenuhnya merupakan hasil karya saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Jika ditemukan unsur tersebut, maka saya siap menerima sanksi akademik sesuai dengan ketentuan yang berlaku di Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dengan penuh kesadaran dan tanpa adanya paksaan dari pihak mana pun.

Palembang, 28 Juli 2025

Penulis,

METERAI TEMPEL 10927AMX434865097

Anya Nur Defitri

NIM. 09011182126017

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh,

Puji syukur penulis panjatkan kepada Allah SWT. Atas segala rahmat dan karunia-Nya, yang memberikan kemudahan dan kelancaran dalam penyelesaian tugas akhir ini dengan judul "**Visualisasi Serangan TCP FIN Flood Pada Jaringan IoT Menggunakan Metode *Unsupervised learning***".

Penyusunan Tugas Akhir ini merupakan hasil dari dukungan dan bantuan yang diberikan oleh berbagai pihak. Berkat do'a, motivasi, semangat, dan bimbingan yang diterima, penulis dapat menyelesaikan penelitian ini. Oleh karena itu, penulis menyampaikan rasa terima kasih yang mendalam kepada:

1. Allah SWT. Yang telah melimpahkan rahmat-Nya berupa kesehatan, kemudahan, dan perlindungan, sehingga penulis dapat menyelesaikan penelitian Tugas Akhir ini.
2. Kedua orang tua tercinta yang senantiasa memberikan dukungan moril, materil maupun spiritual dan kasih sayang tanpa henti dalam setiap langkah kehidupan penulis.
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 Universitas Sriwijaya.
5. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D., IPU., ASEAN-Eng., CPENT, selaku pembimbing akademik sekaligus Pembimbing I Tugas Akhir, yang telah meluangkan waktu, memberikan bimbingan, serta motivasi terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini. Semoga segala kebaikan beliau menjadi amal jariyah yang tak pernah putus.
6. Ibu Nurul Afifah, M.Kom., selaku pembimbing II Tugas Akhir, yang tak hanya membimbing, tetapi juga menjadi sumber semangat dan motivasi bagi penulis. Semoga kebaikan beliau menjadi amal jariyah yang mengalir tiada henti.

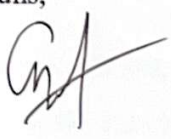
7. Kak Angga Yunanda selaku admin yang telah membantu dalam proses administrasi Tugas Akhir penulis.
8. Kak Septiani Kusuma Ningrum S.Kom., yang telah membantu dalam proses penelitian dan memberikan dukungan selama penyusunan Tugas Akhir ini.
9. Kepada S.A.P, seorang pria yang tetap hadir ketika yang lain menjauh, menjadi sandaran di tengah lelah, penguat saat langkah goyah, dan menghibur kala hati dilanda keresahan. Dalam setiap badai, ia adalah teduh yang menenangkan.
10. Tidak lupa mengucapkan terima kasih kepada diri sendiri, yang telah berjuang dalam diam, menepis lelah yang tak terlihat, dan tetap melangkah meski sering merasa ragu. Untuk setiap air mata yang tak jatuh, untuk keteguhan yang tak selalu dipuji. Terima kasih, telah bertahan sejauh ini.
11. Seluruh pihak yang tidak dapat penulis sebutkan satu per satu, yang telah memberikan dukungan, semangat, dan do'a.
12. Almamater.

Penulis menyadari bahwa laporan ini masih memiliki keterbatasan dan kekurangan. Oleh karena itu, penulis dengan terbuka menerima kritik, saran , dan masukan konstruktif dari para pembaca untuk perbaikan di masa mendatang. Penulis berharap laporan ini dapat memberikan manfaat, khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya. Demikianlah yang dapat penulis sampaikan.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, 28 Juli 2025

Penulis,



Anya Nur Defitri

NIM. 09011182126017

VISUALISASI SERANGAN TCP FIN FLOOD PADA JARINGAN IOT MENGGUNAKAN METODE *UNSUPERVISED LEARNING*

ANYA NUR DEFITRI (09011182126017)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: anyanurdefitri12@gmail.com

ABSTRAK

Seiring berkembangnya *Internet of Things* (IoT), serangan TCP FIN Flood mengancam komunikasi dan sumber daya sistem. Penelitian ini menggunakan dataset node_wifi dari COMNETS Research Labs Universitas Sriwijaya dan menerapkan K-Means serta DBSCAN untuk *cluster*ing dan deteksi anomali pada lalu lintas jaringan. Visualisasi pola serangan dilakukan dengan *Principal Component Analysis* (PCA), yang menunjukkan pola lalu lintas menyimpang, dengan *cluster* terpisah pada K-Means dan titik noise pada DBSCAN. K-Means menghasilkan Silhouette Score 0.8519, namun tidak mendeteksi noise. Sebaliknya, DBSCAN dengan min_samples = 2 dan eps = 10.4621 mendeteksi 4 titik noise dan menghasilkan Calinski-Harabasz Score lebih tinggi (357.67), menunjukkan pemisahan *cluster* lebih baik. Dengan demikian, DBSCAN lebih efektif dalam mendeteksi serangan tersembunyi pada jaringan IoT.

Kata Kunci : TCP FIN Flood, *Internet of Things, Clustering*, K-Means, DBSCAN, *Principal Component Analysis* (PCA), Silhouette Score, Calinski-Harabasz Score

VISUALIZATION OF TCP FIN FLOOD ATTACK ON IOT NETWORK USING UNSUPERVISED LEARNING METHOD

ANYA NUR DEFITRI (09011182126017)

Department of Computer Systems, Faculty of Computer Science
Sriwijaya University
Email: anyanurdefitri12@gmail.com

ABSTRACT

As the Internet of Things (IoT) evolves, TCP FIN Flood attacks threaten communications and system resources. This study uses node_wifi dataset from COMNETS Research Labs, Sriwijaya University and applies K-Means and DBSCAN for clustering and anomaly detection in network traffic. Visualization of attack patterns is done with Principal Component Analysis (PCA), which shows deviant traffic patterns, with separate clusters on K-Means and noise points on DBSCAN. K-Means produces a Silhouette Score of 0.8519, but it does not detect noise. In contrast, a DBSCAN with min_samples = 2 and eps = 10.4621 detected 4 noise points and resulted in a higher Calinski-Harabasz Score (357.67), indicating better cluster separation . Thus, DBSCAN is more effective in detecting hidden attacks on IoT networks.

Keywords *: TCP FIN Flood, Internet of Things, Clustering, K-Means, DBSCAN, Principal Component Analysis (PCA), Silhouette Score, Calinski-Harabasz Score*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) telah menghadirkan paradigma baru di mana jaringan perangkat dan mesin dapat saling berkomunikasi serta bekerja sama melalui koneksi internet [1]. Sistem IoT memiliki kemampuan untuk mengumpulkan data dari objek nyata dalam kehidupan sehari-hari, memproses informasi, dan mengimplementasikannya dalam bentuk tindakan yang dapat ditindaklanjuti. Hal ini menjadikan IoT sebagai aset yang sangat berharga [2]. Menurut penelitian [3], jumlah perangkat IoT diperkirakan akan melebihi 16,44 miliar pada tahun 2025, sementara jumlah perangkat *mobile* diperkirakan melampaui 30,9 miliar.

Perkembangan ini mendorong inovasi dalam berbagai aplikasi generasi mendatang, seperti kota cerdas, layanan kesehatan, rumah pintar, pertanian, serta industri 4.0. IoT juga memungkinkan otomatisasi pengendalian perangkat dengan tujuan meningkatkan kemudahan penggunaan dan memberikan kenyamanan bagi penggunanya [4]. Meskipun IoT menawarkan berbagai manfaat serta pertumbuhan pesat dalam pangsa pasar, aspek keamanannya masih tergolong lemah. Keterbatasan kemampuan komputasi dan ruang penyimpanan pada perangkat IoT menyulitkan implementasi mekanisme perlindungan yang kompleks dan kuat. Oleh karena itu, banyak perangkat IoT menggunakan protokol komunikasi ringan, yang pada akhirnya menyebabkan rendahnya tingkat perlindungan terhadap serangan [5].

Seiring bertambahnya jumlah perangkat yang terhubung, berbagai ancaman keamanan semakin meningkat. Beberapa serangan umum yang mengincar perangkat IoT antara lain serangan *Denial of Service* (DoS), *Distributed Denial of Service* (DDoS), serangan *man-in-the-middle*, dan *code injection* menjadi semakin sering terjadi [6]. Di antara serangan tersebut, *Denial of Service* (DoS) menjadi ancaman yang krusial bagi perangkat IoT karena keterbatasannya dalam kapasitas pemrosesan dan sumber daya [7]. Serangan DoS dilakukan oleh satu atau beberapa perangkat dengan membanjiri jaringan dengan lalu lintas palsu untuk menganggu

ketersediaan layanan. Berbeda dengan DDoS yang melibatkan banyak perangkat, serangan DDoS dapat menyebabkan sistem gagal merespon permintaan sah [8].

Salah satu teknik serangan DoS yang banyak dikaji dalam penelitian adalah TCP SYN flood [9], [10], [11]. Namun, jenis serangan TCP FIN flood masih kurang dieksplorasi. Metode serangan ini bekerja dengan mengirimkan sejumlah besar paket FIN ke server secara berulang, yang bertujuan untuk membebani sistem dan menghabiskan sumber daya seperti memori (*Random Access Memory* atau RAM) dan prosesor. Akibatnya, server tidak lagi memproses permintaan yang sah, sehingga menyebabkan gangguan layanan [12], [13].

Intrusion Detection System (IDS) memiliki peran penting dalam menjaga keamanan jaringan, terutama di lingkungan IoT. Sistem ini dirancang untuk memantau dan menganalisis lalu lintas jaringan guna mengidentifikasi aktivitas mencurigakan atau yang menyimpang dari pola normal [14]. Terdapat tiga pendekatan utama dalam IDS, yaitu berbasis tanda tangan, anomali, dan hibrida [15]. Pendekatan tanda tangan mengenali serangan berdasarkan pola yang telah diketahui, sementara pendekatan anomali mendeteksi penyimpangan dari perilaku normal sehingga lebih efektif dalam mengidentifikasi serangan zero-day. Pendekatan hibrida menggabungkan keduanya untuk meningkatkan akurasi deteksi. Dengan penerapan pendekatan yang tepat, IDS dapat menjadi solusi efektif dalam mendeteksi berbagai jenis serangan.

Salah satu penelitian yang relevan dilakukan oleh [13], kelangkaan dataset nyata dan keterbatasan protokol komunikasi pada dataset sebelumnya yang hanya menggunakan 1 protokol. Karena keterbatasan itu, peneliti membangun sebuah testbed jaringan IoT nyata menggunakan berbagai perangkat. Dataset ini dibangun untuk melatih dan mengevaluasi sistem deteksi intrusi (IDS) yang menerapkan metode *naïve string matching*, terutama dalam jaringan IoT dengan menggunakan dua protokol komunikasi yaitu IEEE 802.11 (WiFi) dan IEEE 802.15.4 (ZigBee). Hasilnya menunjukkan performa akurasi tinggi mencapai 99,92%, presisi 100%, *false positive rate* 0%, dan *false negative* rate hanya 0,089%. Namun, metode ini memiliki keterbatasan dalam mengenali serangan baru yang belum ada dalam database, sehingga membuat IDS rentan terhadap ancaman *zero-day*, yaitu serangan yang belum pernah diketahui atau didokumentasikan sebelumnya.

Lalu lintas jaringan IoT memiliki karakteristik unik yang berbeda dari jaringan tradisional, di mana perangkat IoT cenderung berkomunikasi secara acak dan mengirimkan data dalam jumlah kecil. Pola komunikasi yang tidak teratur ini membuat serangan TCP FIN flood menyerupai lalu lintas normal, sehingga menyulitkan sistem pemantauan berbasis metode konvensional, seperti pendekatan berbasis tanda tangan (*signature-based*) atau aturan (*rule-based*), menjadi kurang efektif dalam mengidentifikasi serangan.[16].

Pendekatan konvensional memiliki keterbatasan dalam menangani pola komunikasi yang tidak teratur mendorong penerapan pendekatan yang modern. Salah satunya adalah pendekatan berbasis *Machine Learning* (ML) mulai banyak diterapkan di beberapa penelitian ([17]), untuk mengatasi keterbatasan konvensional dalam sistem IDS serta kemampuannya dalam mendeteksi pola serangan yang kompleks serta beradaptasi terhadap ancaman baru.

Penelitian yang dilakukan oleh [18], memanfaatkan model *Machine Learning* seperti *Support Vector Machine* (SVM), K-*Nearest Neighbors* (KNN), dan *Random Forest* (RF) untuk mendeteksi serangan pada sistem monitoring IoT di sektor perbankan. Pendekatan ini menggunakan metode *supervised learning*, di mana model dilatih menggunakan data yang telah diberi label antara lalu lintas normal dan serangan. Hasil penelitian ini menunjukkan bahwa SVM mampu mencapai akurasi deteksi hingga 99,5%, mengungguli metode lainnya dalam mengidentifikasi pola serangan kompleks.

Pendekatan supervised telah terbukti memberikan performa deteksi yang tinggi. Namun, metode ini memiliki keterbatasan dalam menghadapi serangan baru, karena bergantung pada data yang telah diberi label [19]. Untuk mengatasi keterbatasan tersebut, pendekatan *unsupervised learning* mulai banyak diteliti karena mampu mengenali pola anomali tanpa memerlukan label. Pendekatan ini dinilai lebih sesuai dengan karakteristik lalu lintas jaringan IoT yang cenderung dinamis dan tidak terstruktur.

Penelitian oleh [20], memperkuat hal ini dengan menunjukkan bahwa algoritma *unsupervised*, seperti *Isolation Forest* dan *Local Outlier Factor* (LOF), memiliki keunggulan dalam mendeteksi serangan yang belum pernah dikenali sebelumnya dibandingkan metode *supervised*. Metode *supervised* menunjukkan

akurasi tinggi untuk serangan yang dikenal, namun performanya turun drastis pada serangan baru, dengan tingkat deteksi kurang dari 50%. Sebaliknya, metode un*supervised learning* mampu mendeteksi serangan tidak dikenal dengan akurasi 70-85%, meski menghasilkan *false positive* yang cukup tinggi, sekitar 30-40%.

Penelitian yang dilakukan oleh [21], menunjukkan efektivitas K-Means dalam mendeteksi serangan ping flood pada jaringan IoT dengan akurasi sangat tinggi, yaitu 99,94%. Namun, penelitian tersebut hanya berfokus pada serangan ping flood (ICMP) pada dataset testbed yang terbatas dan belum membahas visualisasi hasil *Clustering*. Sementara itu, peneliti [15] juga mengevaluasi performa algoritma *unsupervised learning* seperti K-Means++, DBSCAN, LOF, dan *Isolation Forest*. Hasilnya menunjukkan bahwa K-Means++ dan *Isolation Forest* mampu mencapai purity hingga 95% dan akurasi deteksi serangan abnormal sebesar 99%, serta menunjukkan efisiensi komputasi yang tinggi. Namun, penelitian ini memiliki beberapa keterbatasan, yaitu hanya menggunakan dataset BoT-IoT, dan visualisasinya terbatas pada interpretasi *feature importance*, bukan distribusi spasial serangan.

Berdasarkan keterbatasan dalam penelitian-penelitian sebelumnya, terutama terkait kurangnya fokus pada serangan TCP FIN flood dan minimnya eksplorasi visualisasi hasil *cluster*ing, penelitian ini dilakukan untuk mengisi celah tersebut. Penelitian ini mengeksplorasi pendekatan *unsupervised learning* dalam menganalisis lalu lintas jaringan IoT, dengan memanfaatkan algoritma K-Means dan DBSCAN. Tujuannya adalah untuk mengidentifikasi pola lalu lintas anomali dengan visualisasi yang membantu memahami karakteristik serangan TCP FIN flood. Penelitian tugas akhir ini berjudul **"VISUALISASI SERANGAN TCP FIN FLOOD PADA JARINGAN IOT MENGGUNAKAN METODE *UNSUPERVISED LEARNING*"** dan diharapkan dapat menjadi referensi serta kontribusi dalam deteksi serangan yang efisien.

1.2 Rumusan Masalah

Adapun rumusan masalah yang dikaji dalam penelitian ini adalah sebagai berikut.

1. Bagaimana pola lalu lintas serangan TCP FIN flood pada jaringan IoT?

2. Bagaimana performa metode *unsupervised learning* dalam mendeteksi serangan TCP FIN flood pada jaringan IoT ?

1.3 Batasan Masalah

Berdasarkan rumusan masalah dan latar belakang penelitian, maka batasan masalah dalam Tugas Akhir ini ditetapkan sebagai berikut.

1. Penelitian ini difokuskan pada analisis dan deteksi serangan *Denial of Service* (DoS) jenis TCP FIN flood .
2. Dataset yang digunakan dalam penelitian ini merupakan data lalu lintas TCP FIN flood yang diperoleh dari Laboratorium COMNET Universitas Sriwijaya.
3. Penelitian ini membandingkan kinerja algoritma K-Means dan DBSCAN dalam metode *unsupervised learning* untuk mendeteksi pola serangan.

1.4 Tujuan Penelitian

Tujuan dari penulisan Tugas Akhir ini adalah sebagai berikut.

1. Menerapkan metode visualisasi untuk mengidentifikasi dan menganalisis pola lalu lintas jaringan yang mencurigakan guna meningkatkan pemahaman terhadap serangan TCP FIN flood pada *jaringan Internet of Things* (IoT).
2. Menganalisis dan mengevaluasi efektivitas metode *unsupervised learning* dalam mendeteksi serangan TCP FIN flood pada jaringan IoT, serta membandingkan kinerja algoritma K-Means dan DBSCAN.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penulisan Tugas Akhir ini adalah sebagai berikut:

1. Memberikan kontribusi dalam penerapan metode visualisasi guna membantu peneliti, praktisi keamanan jaringan, maupun pengembang sistem dalam memahami pola lalu lintas jaringan yang mencurigakan.
2. Memberikan wawasan mengenai efektivitas metode *unsupervised learning* serta algoritma K-Means dan DBSCAN dalam mendeteksi serangan pada lalu lintas jaring. Hasil dari penelitian ini dapat menjadi

referensi dalam pengembangan sistem deteksi intrusi yang lebih baik dalam menghadapi serangan yang tidak diketahui sebelumnya.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan Tugas Akhir ini terdiri atas beberapa tahapan sebagai berikut.

1. Metode Studi Pustaka (Literatur)

   Pada tahap ini, dilakukan pengumpulan informasi dari berbagai literatur yang relevan mengenai serangan *Denial of Service* (DoS), khususnya jenis TCP FIN flood, serta studi algoritma *unsupervised learning* yang digunakan dalam deteksiintrusi jaringan.

2. Metode Pengumpulan Data

   Pada tahap ini, data dikumpulkan dari dataset lalu lintas jaringan TCP FIN flood yang dikelola oleh COMNETS Research Labs Universitas Sriwijaya, yang dikonversi dari format PCAP menjadi format CSV untuk analisis lebih lanjut.

3. Metode Pengolahan Data

   Metode pengolahan ini merupakan tahapan yang mencakup pembersihan data, ekstraksi fitur, normalisasi data untuk memastikan kualitas data. Selanjutnya, dilakukan reduksi dimensi menggunakan metode *Principal Component Analysis* (PCA) agar data lebih mudah divisualisasikan dan dianalisis oleh algoritma *clustering*.

4. Metode Visualisasi

   Metode visualisasi dilakukan untuk menampilkan hasil pemrosesan dan pola *clustering* dari algoritma yang digunakan. Hasil divisualisasikan menggunakan hasil reduksi PCA untuk menampilkan pola lalu lintas jaringan dan mendeteksi aktivitas mencurigakan.

5. Metode Analisa

   Pada tahap ini, dilakukan evaluasi terhadap performa algoritma K-Means dan DBSCAN berdasarkan metrik evaluasi. Hasil evaluasi digunakan untuk menilai efektivitas masing-masing algoritma dalam mendeteksi serangan.

6. Metode Kesimpulan dan Saran

Metode ini dilakukan setelah menganalisa penelitian secara keseluruhan, dengan tujuan merumuskan kesimpulan dari Tugas Akhir dan memberikan saran yang dapat dimanfaatkan sebagai acuan bagi penelitian selanjutnya.

1.7 Sistematika Penulisan

Berikut ini merupakan sistematika penelitian yang digunakan dalam penulisan Tugas Akhir.

BAB I PENDAHULUAN

Bab ini berisi tentang penjabaran mengenaiLatar belakang penelitian yang dilakukan, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Metodologi Penelitian dan Sistematika Penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini terdapat penelitian terkait, penjelasan mengenai *Internet of Things* (IoT), Serangan *Denial of Service* (DoS), Metode *Unsupervised Learning* dan Algoritma yang digunakan dalam penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menguraikan tahapan penelitian yang mencakup Spesifikasi perangkat yang digunakan, Kerangka kerja penelitian, Persiapan dataset, Flowchart *pre-processing* dan *Modelling*.

BAB IV HASIL DAN ANALISA

Bab ini menyajikan hasil dari penelitian disertai dengan memvisualisasikan serangan dan analisis terhadap kinerja algoritma yang digunakan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari keseluruhan hasil penelitian serta saran yang dapat dijadikan acuan penelitian selanjutnya.

DAFTAR PUSTAKA

[1] I. Lee, “Internet of Things (IoT) cybersecurity: Literature review and iot cyber risk management,” *Futur. Internet*, vol. 12, no. 9, 2020, doi: 10.3390/FI12090157.

[2] R. Kalaria, A. S. M. Kayes, W. Rahayu, E. Pardede, and S. A. Salehi, “IoTPredictor: A security framework for predicting IoT device behaviours and detecting malicious devices against cyber attacks,” *Comput. Secur.*, vol. 146, no. January, p. 104037, 2024, doi: 10.1016/j.cose.2024.104037.

[3] J. E. Z. Macias and S. Trilles, “Machine learning-based prediction model for battery levels in IoT devices using meteorological variables,” *Internet of Things (Netherlands)*, vol. 25, no. December 2023, p. 101109, 2024, doi: 10.1016/j.iot.2024.101109.

[4] B. Kaur *et al.*, “Internet of Things (IoT) security dataset evolution: Challenges and future directions,” *Internet of Things (Netherlands)*, vol. 22, no. October 2022, p. 100780, 2023, doi: 10.1016/j.iot.2023.100780.

[5] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, “FlowGuard: An Intelligent Edge Defense Mechanism against IoT DDoS Attacks,” *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9552–9562, 2020, doi: 10.1109/JIOT.2020.2993782.

[6] M. H. Ali, M. M. Jaber, S. K. Abd, A. Rehman, M. J. Awan, and R. Damaševiˇ, “Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT),” 2022.

[7] B. A. Alabsi, M. Anbar, and S. D. A. Rihan, “Conditional Tabular Generative Adversarial Based Intrusion Detection System for Detecting Ddos and Dos Attacks on the Internet of Things Networks,” *Sensors*, vol. 23, no. 12, 2023, doi: 10.3390/s23125644.

[8] A. Alabdulatif, N. N. Thilakarathne, and M. Aashiq, “Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System,” *Comput. Mater. Contin.*, vol. 80, no. 3, pp. 3655–3683, 2024, doi: 10.32604/cmc.2024.054610.

[9] Y. M. Thant, “IoT Security: Simulation and Analysis of TCP SYN Flooded

DDOS Attack using WireShark," *Trans. Networks Commun.*, vol. 8, no. 3, pp. 16–25, 2020, doi: 10.14738/tnc.83.8389.

[10] M. F. Saiyed and I. Al-Anbagi, "Flow and unified information-based DDoS attack detection system for multi-topology IoT networks," *Internet of Things (Netherlands)*, vol. 24, no. October, p. 100976, 2023, doi: 10.1016/j.iot.2023.100976.

[11] J. R. Sun, C. T. Huang, and M. S. Hwang, "A SYN flooding attack detection approach with hierarchical policies based on self-information," *ETRI J.*, vol. 44, no. 2, pp. 346–354, 2022, doi: 10.4218/etrij.2018-0382.

[12] D. Stiawan, D. Wahyudi, A. Heryanto, F. Muchtar, M. A. Alzahrani, and R. Budiarto, "TCP FIN Flood Attack Pattern Recognition on Internet of Things with Rule Based Signature Analysis," pp. 124–139.

[13] D. Stiawan *et al.*, "The Development of an Internet of Things (IoT) Network Traffic Dataset with Simulated Attack Data," pp. 345–356, doi: 10.53106/160792642023032402013.

[14] V. Christopher *et al.*, "Minority Resampling Boosted Unsupervised Learning with Hyperdimensional Computing for Threat Detection at the Edge of Internet of Things," *IEEE Access*, vol. 9, pp. 126646–126657, 2021, doi: 10.1109/ACCESS.2021.3111053.

[15] G. P. Fernando, A. M. Florina, and C. B. Liliana, "Evaluation of the performance of unsupervised learning algorithms for intrusion detection in unbalanced data environments," *IEEE Access*, vol. 12, no. October, 2024, doi: 10.1109/ACCESS.2024.3516615.

[16] M. Monshizadeh, V. Khatri, R. Kantola, and Z. Yan, "A deep density based and self-determining clustering approach to label unknown traffic," *J. Netw. Comput. Appl.*, vol. 207, no. August, p. 103513, 2022, doi: 10.1016/j.jnca.2022.103513.

[17] K. Kumari and M. Mrunalini, "Detecting Denial of Service attacks using machine learning algorithms," *J. Big Data*, vol. 9, no. 1, 2022, doi: 10.1186/s40537-022-00616-0.

[18] U. Islam *et al.*, "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine

Learning Models," *Sustain.*, vol. 14, no. 14, 2022, doi: 10.3390/su14148374.

[19] M. Snehi and A. Bhandari, "Vulnerability retrospection of security solutions for software-defined Cyber-Physical System against DDoS and IoT-DDoS attacks," *Comput. Sci. Rev.*, vol. 40, p. 100371, 2021, doi: 10.1016/j.cosrev.2021.100371.

[20] T. Zoppi, A. Ceccarelli, T. Puccetti, and A. Bondavalli, "Which algorithm can detect unknown attacks? Comparison of supervised, unsupervised and meta-learning algorithms for intrusion detection," *Comput. Secur.*, vol. 127, p. 103107, 2023, doi: 10.1016/j.cose.2023.103107.

[21] 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.

[22] F. Sun, S. Wang, C. Zhang, and H. Zhang, "Clustering of unknown protocol messages based on format comparison," *Comput. Networks*, vol. 179, no. March, p. 107296, 2020, doi: 10.1016/j.comnet.2020.107296.

[23] L. Yang, L. Liu, Z. Ma, and Y. Ding, "Detection of selective-edge packet attack based on edge reputation in IoT networks," *Comput. Networks*, vol. 188, no. July 2020, p. 107842, 2021, doi: 10.1016/j.comnet.2021.107842.

[24] F. J. Abdullayeva, "Distributed denial of service attack detection in E-government cloud via data clustering," *Array*, vol. 15, no. December 2021, p. 100229, 2022, doi: 10.1016/j.array.2022.100229.

[25] Y. Qu, H. Ma, and Y. Jiang, "CRND : An Unsupervised Learning Method to Detect Network Anomaly," vol. 2022, 2022, doi: 10.1155/2022/9509417.

[26] M. N. Jasim and M. T. Gaata, "K-Means clustering-based semi-supervised for DDoS attacks classification," *Bull. Electr. Eng. Informatics*, vol. 11, no. 6, pp. 3570–3576, 2022, doi: 10.11591/eei.v11i6.4353.

[27] X. Sáez-de-Cámara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, "Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks," *Comput. Secur.*, vol. 131, 2023, doi: 10.1016/j.cose.2023.103299.

[28] L. Lenssen and E. Schubert, "Medoid Silhouette clustering with automatic cluster number selection," *Inf. Syst.*, vol. 120, no. October 2023, p. 102290,

2024, doi: 10.1016/j.is.2023.102290.

[29] R. Efendi, T. Wahyono, and I. R. Widiasari, "DBSCAN SMOTE LSTM: Effective Strategies for Distributed Denial of Service Detection in Imbalanced Network Environments," *Big Data Cogn. Comput.*, vol. 8, no. 9, p. 118, 2024, doi: 10.3390/bdcc8090118.

[30] G. F. Monkam, M. J. De Lucia, and N. D. Bastian, "A topological data analysis approach for detecting data poisoning attacks against machine learning based network intrusion detection systems," *Comput. Secur.*, vol. 144, no. November 2023, p. 103929, 2024, doi: 10.1016/j.cose.2024.103929.

[31] Y. Chen, P. Tan, M. Li, H. Yin, and R. Tang, "K-means clustering method based on nearest-neighbor density matrix for customer electricity behavior analysis," *Int. J. Electr. Power Energy Syst.*, vol. 161, no. August, 2024, doi: 10.1016/j.ijepes.2024.110165.

[32] G. Princz, M. Shaloo, and S. Erol, "Anomaly Detection in Binary Time Series Data: An unsupervised Machine Learning Approach for Condition Monitoring," *Procedia Comput. Sci.*, vol. 232, pp. 1065–1078, 2024, doi: 10.1016/j.procs.2024.01.105.

[33] S. Perumal, P. K. Sujatha, K. S., and M. Krishnan, "Clusters in chaos: A deep unsupervised learning paradigm for network anomaly detection," *J. Netw. Comput. Appl.*, vol. 235, no. August 2024, p. 104083, 2025, doi: 10.1016/j.jnca.2024.104083.

[34] S. A. Sadegh-Zadeh and M. Tajdini, "An unsupervised machine learning approach for cyber threat detection using geographic profiling and Domain Name System data," *Decis. Anal. J.*, vol. 15, no. April, p. 100576, 2025, doi: 10.1016/j.dajour.2025.100576.

[35] M. A. Jabraeil Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, "Towards the Internet of Things: Architectures, Security, and Applications," pp. 9–31, 2020, [Online]. Available: https://doi.org/10.1007/978-3-030-18468-1_2

[36] M. Islam, S. Nooruddin, F. Karray, G. Muhammad, and S. Member, "Internet of Things Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain: A Review," vol. XX, no. Xx, pp. 1–27.

[37] A. Pekar and R. Jozsa, “Evaluating ML-based anomaly detection across datasets of varied integrity: A case study,” *Comput. Networks*, vol. 251, no. June, 2024, doi: 10.1016/j.comnet.2024.110617.

[38] K. P. Sinaga and M. S. Yang, “Unsupervised K-means clustering algorithm,” *IEEE Access*, vol. 8, pp. 80716–80727, 2020, doi: 10.1109/ACCESS.2020.2988796.

[39] M. P. M, C. Dewi, P. S. Emban, G. A. Wijayanti, N. Aulia, and R. Nooraeni, “Comparison of DBSCAN and K-Means Clustering forGrouping the Village Status in Central Java 2020,” *J. Mat. Stat. Komputasi*, vol. 17, no. 3, pp. 394–404, 2021, doi: 10.20956/j.v17i3.11704.

[40] F. D. Wahyuningtyas, A. Arafat, A. Stiawan, and D. Rolliawati, “Komparasi Algoritma Hierarchical, K-Means, dan DBSCAN pada Analisis Data Penjualan Melalui Facebook,” *Explor. J. Sist. Inf. dan Telemat.*, vol. 14, no. 1, p. 7, 2023, doi: 10.36448/jsit.v14i1.2931.