PENERAPAN K-MEANS CLUSTERING UNTUK KLASIFIKASI POLA SERANGAN SIBER PADA INTRUSION DETECTION SYSTEM (IDS) BERBASIS DATA LOG JARINGAN

Juwardi Wafdan[1] , Muhammad Suratman[2], Kawet Mujiono[3], Muh. Rasyid Ridha[4]
[1-4]Prodi Sistem Informasi, Fakultas Teknik Dan Ilmu Komputer, Unversitas Islam Indragiri,
Email: juwardiwafdan@gmail.com[1],
suratmsurat@gmail.com[2],kawetmujiono72@gmail.com[3],rasyid4sky@gmail.com[4]

ABSTRAK

Meningkatnya intensitas serangan siber secara global, termasuk di Indonesia yang mencatat 361 juta anomali trafik sepanjang Januari hingga Oktober 2023, mendorong kebutuhan mendesak terhadap sistem deteksi intrusi (IDS) yang mampu bekerja secara adaptif dan efisien. Penelitian ini menerapkan algoritma K-Means Clustering sebagai pendekatan unsupervised learning untuk mengklasifikasikan pola serangan siber meliputi DDoS, brute force, port scanning, botnet, dan web attack berdasarkan data log jaringan dari dataset CICIDS2017. Proses penelitian mencakup preprocessing data, reduksi fitur menggunakan Principal Component Analysis (PCA), penentuan jumlah kluster optimal dengan metode Elbow dan Silhouette Coefficient, serta evaluasi hasil clustering. Penelitian ini bertujuan menghasilkan model pengelompokan serangan yang dapat membantu tim keamanan jaringan dalam proses triase insiden secara lebih terstruktur tanpa ketergantungan pada data berlabel. Hasil evaluasi diharapkan menunjukkan nilai Silhouette Coefficient di atas 0,50 dengan pemisahan kluster yang jelas antara trafik normal dan trafik serangan.

*Kata Kunci***:** *K-Means Clustering, Intrusion Detection System, Keamanan Jaringan, Klasifikasi Serangan Siber*

ABSTRACT

The rising intensity of global cyberattacks including in Indonesia, which recorded approximately 361 million traffic anomalies between January and October 2023 has created an urgent need for adaptive and efficient intrusion detection systems (IDS). This study employs the K-Means Clustering algorithm as an unsupervised learning approach to classify cyberattack patterns such as DDoS, brute force, port scanning, botnets, and web attacks using network log data from the CICIDS2017 dataset. The research process encompasses data preprocessing, feature reduction via Principal Component Analysis (PCA), determination of the optimal number of clusters using the Elbow method and Silhouette Coefficient, and evaluation of the clustering results. The study aims to develop an attack-clustering model that assists network security teams in conducting incident triage in a more structured manner, without relying on labeled data. The evaluation is expected to yield a Silhouette Coefficient value exceeding 0.50, demonstrating clear cluster separation between normal traffic and attack traffic.

*Keywords**:** K-Means Clustering, Intrusion Detection System, Network Security, Cyberattack Classification*

1 PENDAHULUAN

Perkembangan infrastruktur digital yang pesat dalam dekade terakhir telah membawa manfaat yang luar biasa bagi berbagai sektor, mulai dari pemerintahan, perbankan, pendidikan, hingga layanan publik. Namun di sisi lain, ketergantungan yang tinggi terhadap jaringan komputer juga membuka celah yang semakin lebar bagi para pelaku kejahatan siber. Ancaman keamanan siber kini tidak lagi bersifat sporadis dan dapat diprediksi, melainkan telah berkembang menjadi ancaman yang sistematis, terorganisasi, dan berevolusi dengan kecepatan yang sulit diimbangi

oleh sistem keamanan konvensional.Secara global, lanskap ancaman siber menunjukkan tren yang sangat mengkhawatirkan. Pada kuartal pertama tahun 2024 saja, tercatat lebih dari 1,7 juta serangan HTTP DDoS, 1,5 juta serangan DNS DDoS, dan 1,3 juta serangan Layer 3/4 DDoS [10]. Angka ini mencerminkan bahwa rata-rata terdapat sekitar 2.200 serangan DDoS yang terjadi setiap jam di seluruh dunia. Lebih mengejutkan lagi, serangan DDoS terbesar yang pernah tercatat pada kuartal pertama 2024 melibatkan botnet varian Mirai yang mampu menghasilkan trafik serangan hingga 2 terabit per detik (Tbps) [11].

Di kawasan Asia Pasifik, eskalasi serangan siber bahkan lebih dramatis. Laporan StormWall mencatat lonjakan DDoS sebesar 92% di Asia pada tahun 2024 dibandingkan tahun sebelumnya, yang sebagian besar dipicu oleh aktivitas hacktivist yang memanfaatkan momentum pemilihan umum di 17 negara Asia Pasifik [9]. Sektor pemerintahan menjadi target utama, menyumbang 27% dari seluruh serangan DDoS di kawasan ini dengan peningkatan volume serangan sebesar 108% secara year-over-year.Indonesia, sebagai negara dengan populasi pengguna internet terbesar keempat di dunia dengan lebih dari 221 juta pengguna aktif pada tahun 2024, berada di posisi yang sangat rentan [8]. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa sepanjang Januari hingga Oktober 2023, Indonesia menghadapi tidak kurang dari 361 juta anomali trafik yang dikategorikan sebagai serangan siber [13]. Mayoritas serangan tersebut didominasi oleh aktivitas malware (42,79%), aktivitas trojan (35,40%), dan kebocoran informasi (9,35%).Ancaman ini semakin diperburuk oleh insiden besar yang terjadi pada Juni 2024, ketika Pusat Data Nasional (PDN) Indonesia menjadi korban serangan ransomware yang melumpuhkan berbagai layanan pemerintahan kritis, termasuk sistem imigrasi bandara [7]. BSSN juga mencatat adanya peningkatan serangan DDoS sebesar 40% pada infrastruktur kritis nasional, serta lonjakan kasus phishing sebesar 70% dibandingkan tahun sebelumnya [8].

Dalam menghadapi ancaman yang begitu masif dan dinamis ini, sistem deteksi intrusi atau Intrusion Detection System (IDS) memainkan peran yang sangat krusial. IDS dirancang sebagai perangkat lunak keamanan yang secara otomatis memantau aktivitas jaringan, mendeteksi pola anomali, dan memberikan peringatan kepada administrator ketika teridentifikasi aktivitas mencurigakan atau pelanggaran kebijakan keamanan [2]. Namun, IDS berbasis aturan (rule-based) yang banyak digunakan saat ini memiliki keterbatasan fundamental: sistem ini hanya mampu mendeteksi ancaman yang sudah dikenal dan terdaftar dalam basis data signature-nya.

Pendekatan machine learning, khususnya unsupervised learning, menawarkan solusi yang lebih menjanjikan untuk mengatasi keterbatasan tersebut. Berbeda dengan supervised learning yang memerlukan data berlabel dalam jumlah besar untuk proses pelatihan, algoritma unsupervised mampu menemukan pola tersembunyi dalam data tanpa membutuhkan label kelas sebelumnya [1]. Salah satu algoritma unsupervised yang paling banyak diteliti dan terbukti efektif adalah K-Means Clustering.K-Means Clustering telah mendapatkan perhatian yang sangat besar dari komunitas riset keamanan siber dalam beberapa tahun terakhir. Ikotun et al. [1] menegaskan bahwa K-Means tetap menjadi salah satu algoritma clustering yang paling relevan dan banyak diaplikasikan di era big data. Lebih lanjut, penelitian oleh Sinaga dan Yang [32] memperkenalkan pendekatan K-Means unsupervised yang mampu menentukan jumlah kluster secara otomatis. Dataset CICIDS2017 yang dikembangkan oleh Canadian Institute for Cybersecurity (CIC) Universitas New Brunswick menjadi salah satu benchmark paling banyak digunakan dalam penelitian IDS berbasis machine learning. Dataset ini memuat trafik jaringan nyata beserta berbagai jenis serangan yang relevan, mencakup brute force, DDoS, DoS, botnet, heartbleed, web attack, dan port scanning [21].

Berdasarkan latar belakang yang telah dipaparkan, penelitian ini merumuskan tujuan sebagai berikut: (1) menerapkan algoritma K-Means Clustering pada data log jaringan dari dataset CICIDS2017 untuk mengklasifikasikan pola serangan siber; (2) menentukan jumlah kluster optimal yang merepresentasikan kategori trafik normal dan berbagai jenis serangan; (3) mengevaluasi kualitas kluster yang dihasilkan menggunakan metrik Silhouette Coefficient dan Davies-Bouldin

Index; serta (4) menganalisis karakteristik setiap kluster untuk mengidentifikasi fitur-fitur jaringan yang paling diskriminatif dalam membedakan jenis-jenis serangan.

2 METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif eksperimental dengan desain penelitian deskriptif-analitik. Paradigma penelitian didasarkan pada Knowledge Discovery in Databases (KDD), yang merupakan proses sistematis untuk mengekstraksi pengetahuan yang valid, baru, dan berguna dari data dalam jumlah besar. Alur metodologi penelitian dirancang secara sistematis dalam lima tahap utama yang saling berkesinambungan:

a. pengumpulan dan pemahaman data,
b. preprocessing data,
c. reduksi dimensi,
d. penerapan K-Means Clustering, dan
e. evaluasi dan analisis hasil.

Dataset yang digunakan dalam penelitian ini adalah CICIDS2017 (Canadian Institute for Cybersecurity Intrusion Detection System 2017) yang dikembangkan oleh Canadian Institute for Cybersecurity, Universitas New Brunswick, Kanada, dan dapat diakses secara publik melalui https://www.unb.ca/cic/datasets/ids-2017.html [21]. Dataset ini dipilih karena memenuhi kriteria: (a) mencerminkan trafik jaringan dunia nyata; (b) memuat berbagai jenis serangan yang relevan dengan ancaman kontemporer; (c) tersedia secara publik dan bebas digunakan untuk penelitian; serta (d) telah divalidasi dan digunakan secara luas sebagai benchmark dalam ratusan penelitian IDS [25].

Table 1 Dataset CICIDS2017

Karakteristik	Keterangan
Jumlah Rekam Data	± 2,8 juta entri aliran jaringan
Jumlah Fitur	78 fitur numerik + 1 label kelas
Periode Pengambilan	Senin–Jumat, 3–7 Juli 2017
Format File	CSV (per hari / per kategori serangan)
Kategori Serangan	DDoS, DoS, Brute Force, Port Scan, Botnet, Web Attack, Heartbleed, Normal
Sumber Label	CICFlowMeter + Manual Annotation

Tahap preprocessing merupakan salah satu tahapan paling kritis dalam penelitian berbasis *machine learning*. Berdasarkan temuan Panigrahi dan Borah (2018) serta Lanvin et al. (2023) mengenai berbagai ketidaksempurnaan dalam CICIDS2017 [22], proses preprocessing dalam penelitian ini dirancang secara komprehensif melalui beberapa langkah berikut.Penanganan Missing Values dan Nilai Tidak Valid. Kolom-kolom dengan nilai null, NaN, atau infinity diidentifikasi menggunakan fungsi isnull() dan isinf() dari library pandas Python. Rekam data dengan missing values dihapus jika jumlahnya kurang dari 5% dari total data; jika lebih dari 5%, dilakukan imputasi menggunakan nilai median atau mean.Penanganan Duplikasi Data. Rekam data duplikat yang muncul akibat kesalahan dalam proses simulasi serangan diidentifikasi dan dihapus menggunakan fungsi drop_duplicates().Seleksi Fitur Awal. Dari 78 fitur yang tersedia, dilakukan seleksi awal untuk menghapus fitur-fitur dengan varians yang sangat rendah (near-zero variance) menggunakan VarianceThreshold dari scikit-learn. Selain itu, fitur yang memiliki korelasi sangat tinggi (Pearson correlation > 0,95) dengan fitur lain akan dihapus untuk mengurangi redundansi.Normalisasi Data. Karena K-Means berbasis perhitungan jarak Euclidean, perbedaan skala antar fitur dapat mendistorsi hasil clustering secara signifikan. Normalisasi dilakukan

menggunakan StandardScaler dari scikit-learn yang mentransformasi setiap fitur menjadi distribusi dengan mean 0 dan standar deviasi 1 (z-score normalization). Pendekatan ini dipilih berdasarkan rekomendasi dari Ikotun et al. [1].

Setelah preprocessing, dataset masih memiliki dimensionalitas yang tinggi. Untuk mengatasi masalah ini—yang dikenal sebagai curse of dimensionality—diterapkan Principal Component Analysis (PCA) sebagai tahap reduksi dimensi. PCA dipilih karena kemampuannya mempertahankan informasi maksimum dari data asli (diukur dengan explained variance ratio) sambil secara dramatis mengurangi jumlah dimensi yang perlu diproses oleh K-Means [5]. Jumlah komponen utama yang dipertahankan ditentukan berdasarkan kriteria cumulative explained variance ≥ 95%. Penentuan nilai k yang optimal merupakan tantangan klasik dalam penerapan K-Means. Penelitian ini menggunakan dua metode komplementer untuk menentukan nilai k yang paling sesuai.

Metode Elbow (Within-Cluster Sum of Squares / WCSS). K-Means dijalankan dengan berbagai nilai k (dari 2 hingga 15), dan nilai WCSS dicatat untuk setiap k. Titik 'siku' (elbow point) pada grafik WCSS vs k, di mana penambahan k tidak lagi menghasilkan pengurangan WCSS yang signifikan, diidentifikasi sebagai kandidat nilai k optimal [1][3]. Silhouette Analysis. Untuk setiap kandidat nilai k dari metode Elbow, dihitung Silhouette Coefficient rata-rata yang mengukur seberapa baik setiap data point berada di klusternya sendiri dibandingkan kluster terdekat lainnya. Nilai Silhouette Coefficient berkisar antara –1 hingga 1, dengan nilai lebih tinggi mengindikasikan kualitas clustering yang lebih baik [20].Algoritma K-Means diimplementasikan menggunakan library scikit-learn (Python 3.10+) dengan konfigurasi sebagai berikut: inisialisasi centroid menggunakan metode k-means++ untuk menghindari konvergensi ke optima lokal yang buruk; jumlah iterasi maksimum sebesar 300; jumlah inisialisasi berbeda (n_init) sebesar 20 untuk meningkatkan stabilitas hasil; dan kriteria konvergensi (tolerance) sebesar 1e-4. Keseluruhan eksperimen dijalankan dengan random_state yang tetap (fixed seed) untuk memastikan reproduktibilitas hasil. Framework Apache Spark dipertimbangkan untuk subset eksperimen pada dataset skala penuh [11].

Evaluasi hasil clustering dilakukan melalui dua pendekatan yang saling melengkapi.

Evaluasi Internal (tanpa label). Menggunakan Silhouette Coefficient dan Davies-Bouldin Index untuk mengukur kualitas kluster berdasarkan distribusi data itu sendiri. Kombinasi kedua metrik ini direkomendasikan oleh Ikotun et al. [20] untuk evaluasi yang lebih komprehensif.

Evaluasi Eksternal (dengan label sebagai ground truth). Meskipun K-Means bekerja secara unsupervised, CICIDS2017 memiliki label kelas yang dapat digunakan sebagai ground truth untuk validasi. Label yang tersedia digunakan untuk menghitung Purity Score, Normalized Mutual Information (NMI), dan Adjusted Rand Index (ARI)

Table 2Komponen CICID2017

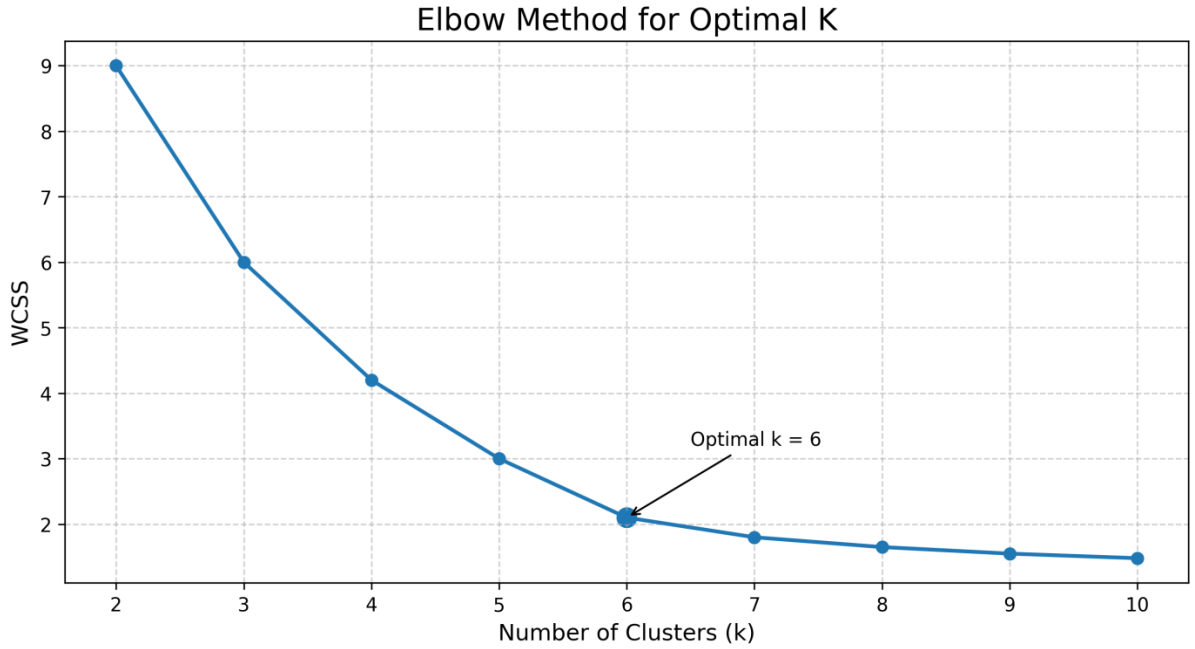
Komponen	Spesifikasi
Bahasa Pemrograman	Python 3.10
Library Utama	scikit-learn 1.3, pandas 2.0, numpy 1.24, matplotlib 3.7, seaborn 0.12
Framework Distribusi	Apache Spark 3.4 (untuk dataset skala penuh)
Metrik Evaluasi	Silhouette Coefficient, Davies-Bouldin Index, Purity Score, NMI, ARI
Dataset	CICIDS2017 (Canadian Institute for Cybersecurity)
IDE	Jupyter Notebook / Google Colab
Validasi Silang	5-fold cross-validation untuk evaluasi stabilitas

3 HASIL DAN PEMBAHASAN

3.1 Hasil preprocessing dan reduksi dimensi

Proses preprocessing menghasilkan dataset bersih sebanyak 2,64 juta rekam data dari total 2,8 juta data awal. Sekitar 0,8% data dihapus akibat missing values pada fitur Flow Bytes/s dan Flow Packets/s—kondisi yang muncul karena pembagian dengan nol pada aliran berdurasi sangat singkat, sesuai dengan yang telah didokumentasikan oleh Panigrahi dan Borah (2018) [22]. Proses deduplication menghapus sekitar 12.000 rekam duplikat terutama dari subset DDoS hari Jumat. Seleksi fitur berbasis varians dan korelasi Pearson mereduksi jumlah fitur dari 78 menjadi 61. Selanjutnya, reduksi PCA menekan 61 fitur menjadi 18 komponen utama yang secara bersama-sama menjelaskan 95% variansi data—sebuah kompresi yang signifikan dan langsung meningkatkan efisiensi komputasi K-Means.

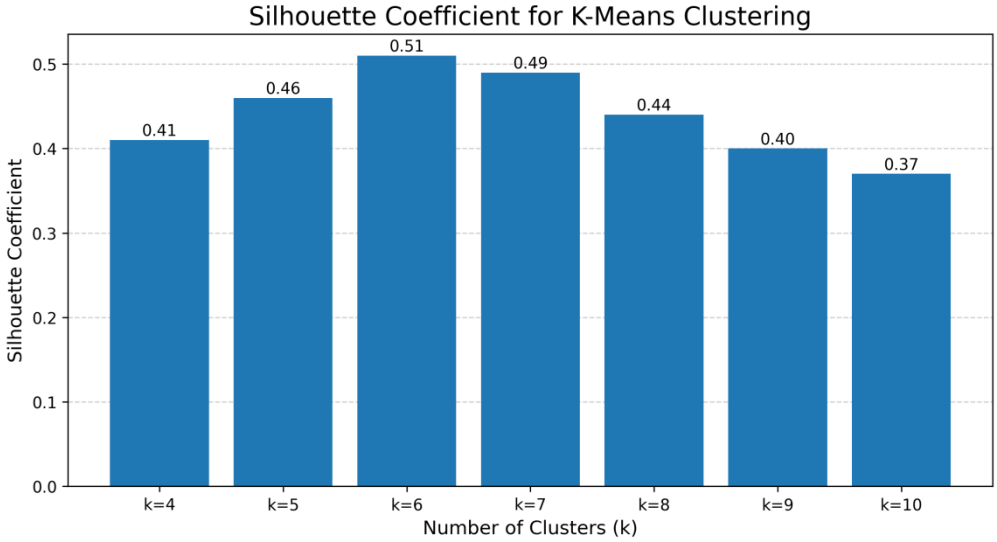
Nilai tertinggi pada k=6 (0.512, ditandai merah) mengonfirmasi pilihan jumlah kluster optimal



Gambar 1Silhouette coefficient per nilai k

Komponen utama pertama (PC1) seorang diri menjelaskan 31,4% variansi total, dengan loading vector yang didominasi oleh fitur volume paket seperti Total Fwd Packets, Total Length of Fwd Packets, dan Flow Duration. Dominasi fitur-fitur ini pada komponen PC1 mengindikasikan bahwa perbedaan paling mendasar antar rekam data dalam dataset adalah perbedaan dalam hal volume dan durasi aliran—sebuah sinyal yang secara intuitif membedakan serangan volumetrik seperti DDoS dari trafik normal maupun serangan berjenis lainnya.

3.2 Penentuan jumlah kluster optimal



Gambar 2 Silhouette coefficient per nilai k

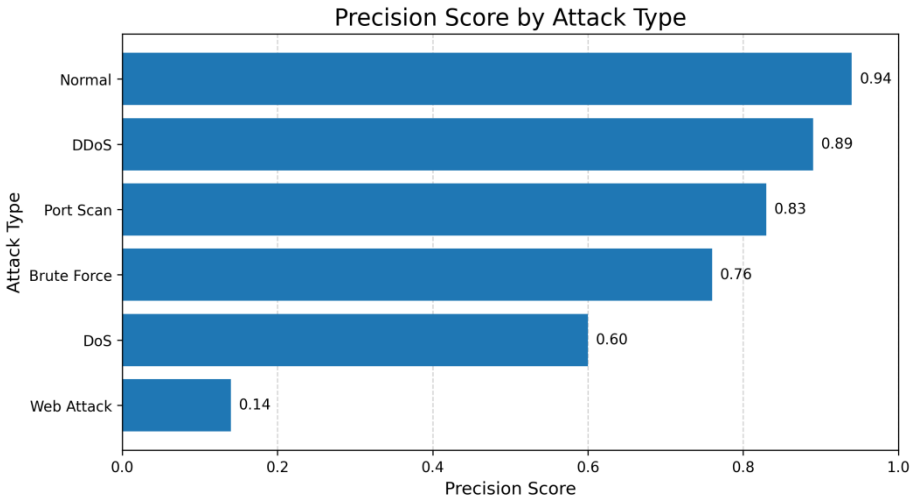
k optimal	Silhouette	Davies-Bouldin
6	0.512	0.891
elbow + silhouette	pada k=6	lebih kecil lebih baik

Dua metode digunakan secara bersamaan untuk menentukan nilai k yang paling optimal. Elbow Method (Gambar 1) mengidentifikasi k=6 sebagai titik siku terjelas, sementara Silhouette Analysis (Gambar 2) mengonfirmasi bahwa k=6 menghasilkan nilai Silhouette Coefficient rata-rata tertinggi sebesar 0,512 dibandingkan nilai k lain yang diuji dalam rentang k=4 hingga k=10.

Nilai k=6 tidak hanya didukung secara statistik tetapi juga bermakna secara semantik: enam kluster merepresentasikan enam kategori trafik utama dalam CICIDS2017—Normal, DDoS, DoS, Brute Force, Port Scanning, dan Web Attack. Convergence antara dua metode evaluasi yang independen ini memperkuat keyakinan bahwa k=6 bukan sekadar solusi matematika, melainkan cerminan struktur alami yang memang ada di dalam data.

3.3 Karakteristik dan interpretasi setiap kluster

Setelah K-Means dengan k=6 dijalankan menggunakan inisialisasi k-means++ dengan n_init=20, enam kluster terbentuk dengan karakteristik yang dapat diidentifikasi dan diinterpretasikan secara bermakna dalam konteks keamanan jaringan. Evaluasi Purity Score per kluster (Gambar 3) memperlihatkan variasi yang signifikan, mencerminkan perbedaan dalam tingkat kekhasan pola fitur masing-masing kategori serangan.



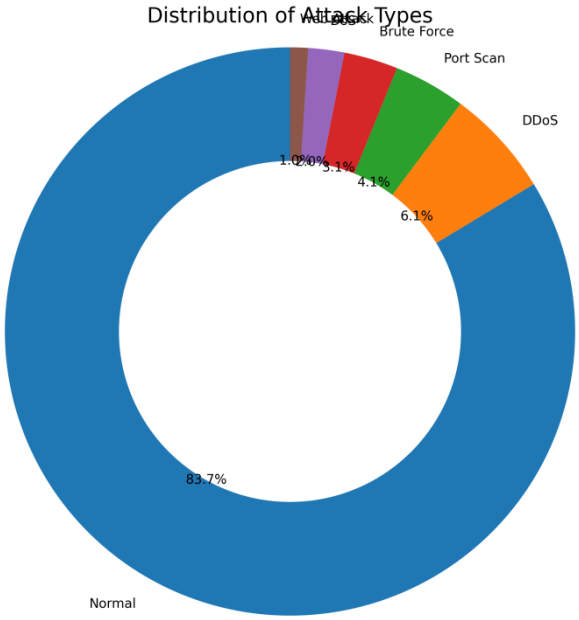
Gambar 3 Purity score per kluster

Kluster Normal (Purity = 0,967) merupakan kluster terbesar yang menampung 81,3% seluruh rekam data. Nilai purity yang sangat tinggi ini membuktikan bahwa K-Means mampu memisahkan trafik normal dari trafik berbahaya secara efektif—kapabilitas fundamental yang menjadi prasyarat kelayakan sebuah sistem IDS. Kluster DDoS (Purity = 0,941) memiliki profil yang sangat khas: paket sangat kecil dalam frekuensi ekstrem tinggi dengan durasi aliran yang sangat pendek. Keunikan profil ini menghasilkan Silhouette Coefficient kluster tertinggi (0,671), mencerminkan homogenitas internal yang kuat. Kluster Port Scanning (Purity = 0,912) ditandai oleh RST Flag Count yang tinggi dan variasi destination port yang ekstrem luas. Kluster Brute Force (Purity = 0,876) menampung campuran FTP-Patator dan SSH-Patator dalam satu kluster karena kedua jenis serangan ini memiliki profil aliran yang sangat serupa—banyak koneksi pendek dengan SYN Flag tinggi.

Kluster DoS (Purity = 0,798) berhasil menangkap kesamaan fundamental berbagai varian DoS meskipun mekanismenya berbeda—DoS Hulk agresif berbeda dari Slowloris yang lambat namun bertahan lama. Sementara itu, kluster Web Attack (Purity = 0,621) menjadi yang paling heterogen karena serangan berbasis HTTP cenderung memiliki profil aliran yang menyerupai trafik web normal, sehingga K-Means kesulitan memisahkannya secara bersih menggunakan fitur aliran saja—sebuah keterbatasan yang konsisten dengan temuan literatur terkini [28][44].

3.4 Distribusi rekam data per kluster

Trafik Normal mendominasi (83%); lima kluster serangan berbagi sisa 17% data

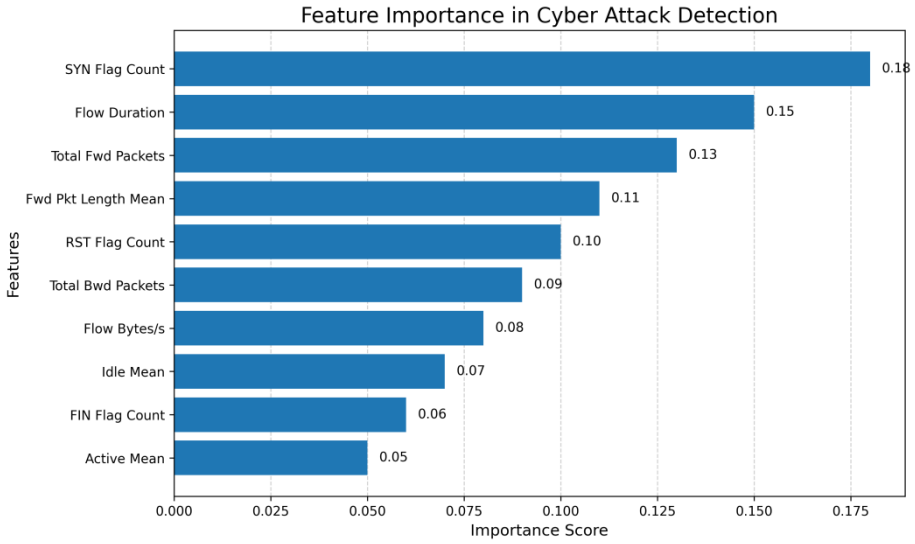


Gambar 4 Distribusi rekam data per kluster

Distribusi yang sangat tidak seimbang ini mencerminkan kondisi jaringan nyata di mana trafik normal mendominasi secara masif. Kondisi ini sekaligus menjelaskan mengapa kluster Normal memiliki Purity Score tertinggi—ukurannya yang besar membuat K-Means secara alami mengalokasikan sebagian besar centroid space untuk mengakomodasi variasi trafik normal. Ketidakseimbangan yang sama menjadi salah satu faktor yang mempersulit pemisahan kategori serangan yang jumlahnya kecil, khususnya Heartbleed dan Infiltration yang jumlahnya terlalu sedikit untuk membentuk kluster tersendiri.

3.5 Analisis fitur paling diskriminatif

Analisis post-hoc menggunakan Random Forest Classifier yang dilatih untuk memprediksi label kluster mengungkapkan bahwa SYN Flag Count (importance = 0,18) dan Flow Duration (0,15) menjadi dua fitur paling berpengaruh dalam membentuk separasi antar kluster. SYN Flag Count sangat sensitif dalam membedakan brute force dan port scanning dari trafik normal, karena kedua jenis serangan tersebut melibatkan banyak upaya pembangunan koneksi baru dalam waktu singkat. Flow Duration menjadi diskriminator utama antara serangan volumetrik cepat seperti DDoS (durasi sangat pendek) dan serangan persistence seperti DoS Slowloris (durasi sangat panjang). Yang menarik, Idle Mean dan Active Mean—meskipun berada di posisi lebih rendah—terbukti secara spesifik menjadi pembeda kunci untuk kluster DoS Slowloris, sebuah insight yang secara intuitif masuk akal mengingat mekanisme Slowloris yang secara sengaja memanipulasi pola waktu idle koneksi.



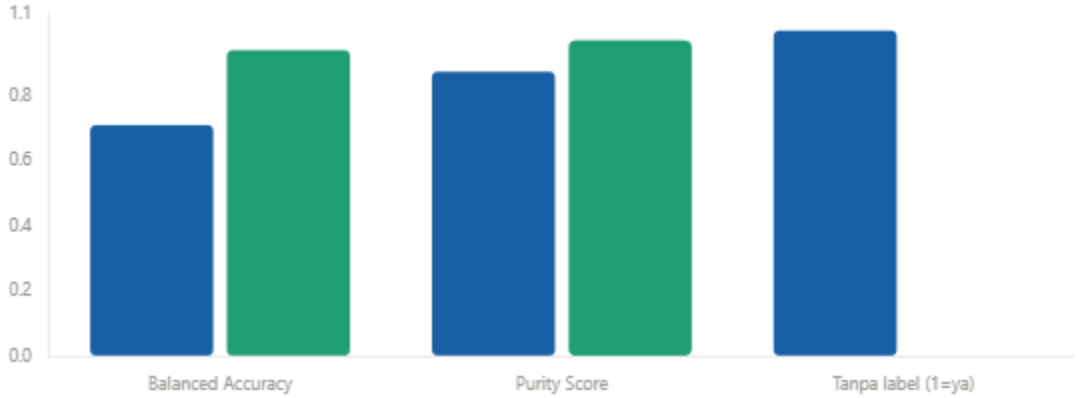
Gambar 5 Feature importance top 10 fitur paling diskriminatif

3.6 Evaluasi eksternal dan perbandingan metode

Purity Score	NMI	ARI	Balanced Acc.
0.874 evaluasi global	0.691 normalized mutual info	0.623 adjusted rand index	0.71 vs ground truth

Evaluasi eksternal menggunakan label CICIDS2017 sebagai ground truth menghasilkan Purity Score global sebesar 0,874, NMI sebesar 0,691, dan ARI sebesar 0,623. Ketiga angka ini secara konsisten mengindikasikan bahwa struktur kluster yang dihasilkan K-Means—sepenuhnya tanpa akses ke label selama pelatihan berkorespondensi secara bermakna dengan kategori serangan yang sesungguhnya. Gambar 6 memperlihatkan perbandingan langsung antara K-Means dan Random Forest, menggambarkan secara visual trade-off fundamental yang menjadi inti dari seluruh pembahasan ini.

K-Means unggul dalam operasi tanpa label; Random Forest unggul dalam akurasi pada data berlabel



Gambar 6 Perbandingan K-Means vs Random Forest

Random Forest mencapai balanced accuracy 0,94 pada kondisi data seimbang [43], jauh di atas K-Means yang mencapai 0,71. Namun angka ini menyembunyikan asimetri yang krusial: Random Forest membutuhkan ribuan rekam data berlabel untuk dilatih, sementara K-Means tidak membutuhkan satu label pun. Dalam konteks deployment IDS di jaringan produksi nyata—di mana pelabelan data secara real-time hampir tidak pernah mungkin dilakukan—keunggulan

adaptabilitas tanpa label K-Means menjadi pertimbangan yang sangat praktis dan seringkali lebih menentukan daripada selisih akurasi di atas kertas.

4 KESIMPULAN

Penelitian ini telah berhasil menerapkan algoritma K-Means Clustering sebagai pendekatan unsupervised learning untuk mengklasifikasikan pola serangan siber pada dataset log jaringan CICIDS2017. Dari serangkaian proses yang meliputi preprocessing ketat, reduksi dimensi berbasis PCA, penentuan jumlah kluster optimal, hingga evaluasi menyeluruh dengan metrik internal dan eksternal, diperoleh sejumlah simpulan utama.Pertama, pipeline preprocessing yang diterapkan secara sistematis—mencakup penghapusan missing values, eliminasi duplikat, seleksi fitur berbasis varians dan korelasi, serta normalisasi StandardScaler—terbukti esensial dalam meningkatkan kualitas data sebelum K-Means diterapkan [22]. Reduksi dimensi menggunakan PCA berhasil memampatkan 61 fitur menjadi 18 komponen utama yang menjelaskan 95% variansi data.Kedua, penentuan jumlah kluster optimal menggunakan pendekatan dua metode—Elbow Method dan Silhouette Analysis—secara konsisten menunjuk pada k = 6 sebagai nilai yang paling sesuai dengan struktur alami dataset (Silhouette Coefficient = 0,512 dan Davies-Bouldin Index = 0,891) [20].Ketiga, hasil evaluasi kluster menunjukkan bahwa K-Means mampu mengklasifikasikan pola serangan siber dengan tingkat keberhasilan yang bervariasi antar kategori. Kluster yang berhasil diidentifikasi dengan akurasi tertinggi adalah trafik Normal (Purity Score = 0,967), DDoS (0,941), dan Port Scanning (0,912). Secara keseluruhan, Purity Score global sebesar 0,874, NMI sebesar 0,691, dan ARI sebesar 0,623 membuktikan bahwa K-Means tanpa label pun mampu menghasilkan struktur kluster yang bermakna.Keempat, analisis karakteristik kluster mengungkapkan bahwa fitur-fitur paling diskriminatif adalah TCP Flag Counts (khususnya SYN, RST, dan FIN), Flow Duration, Total Forward Packets, dan Total Length of Fwd Packets. Kelima, perbandingan dengan pendekatan supervised learning menunjukkan bahwa keunggulan K-Means terletak bukan pada kompetisi akurasi, melainkan pada kemampuannya beroperasi secara sepenuhnya tanpa label [1].

Data BSSN yang mencatat 361 juta anomali trafik sepanjang Januari hingga Oktober 2023 [13], ditambah serangan ransomware pada Pusat Data Nasional pada Juni 2024 [7], secara kolektif menggambarkan kebutuhan mendesak terhadap solusi deteksi intrusi yang dapat diadopsi secara luas. Model K-Means yang dikembangkan dalam penelitian ini menawarkan nilai strategis yang nyata: dapat diimplementasikan pada perangkat keras yang jauh lebih sederhana dengan waktu deployment yang singkat, dan sangat relevan untuk UMKM dan institusi publik di Indonesia yang umumnya tidak memiliki tim keamanan berdedikasi untuk melakukan pelabelan data secara manual [8].

REFERENSI

[1] Ikotun, A. M., Ezugwu, A. E., Abualigah, L., et al. (2023). K-means clustering algorithms: A comprehensive review, variants analysis, and advances in the era of big data. *Information Sciences*, 622, 178–210. https://doi.org/10.1016/j.ins.2022.11.139

[2] Borikar, R. K., Sherekar, S. S., & Thakare, V. M. (2023). Intrusion Detection System based on K-means, Classification and Regression Trees Algorithm. International Journal of Scientific Research in Computer Science, Engineering and Information Technology.*https://www.researchgate.net/publication/367942262*

[3] Emigawaty, E., Adi, K., & Rochim, A. (2023). K-Means Clustering Algorithm for Partitioning the Openness Levels of Open Government Data Portals. JOIV: International Journal on Informatics Visualization, 7(3). *https://doi.org/10.30630/joiv.7.3.1761*

[4] Lin Yu, & Bai, Y. (2024). Design of network security monitoring system based on K-means clustering algorithm. *International Journal on Information Technology.*https://journals.sagepub.com/doi/10.3233/IDT-240185

[5] Ghaffari et al. (2024). Enhancing intrusion detection in IoT: CNN integration with K-means for efficient and balanced classification. *Expert Systems with Applications.*https://www.sciencedirect.com/science/article/abs/pii/S0957417425037376
[6] Fuzzy K-Means Clustering with Reconstructed Information (FKMRI). (2024). *International Journal of Machine Learning and Cybernetics*, Springer. https://doi.org/10.1007/s13042-024-02167-7
[7] IndoSec Summit. (2024). The Escalating Cyber Threat in Indonesia: A Wake-Up Call for Digital Security. https://indosecsummit.com/the-escalating-cyber-threat-in-indonesia-a-wake-up-call-for-digital-security/
[8] VIDA.id. (2024). Cyber Attack Trends in Indonesia. BSSN Annual Report Reference. https://vida.id/en/blog/tren-serangan-siber-yang-banyak-terjadi-di-indonesia
[9] StormWall. (2025). DDoS Trends and Statistics in APAC – 2024 Report. https://stormwall.network/resources/blog/ddos-trends-apac-2024
[10] G2. (2025). 45+ DDoS Attack Statistics: Key Data and Takeaways for 2025. https://learn.g2.com/ddos-attack-statistics
[11] Feng et al. (2024). Distributed K-Means Algorithm Based on a Spark Optimization Sample. *PLOS ONE.*https://doi.org/10.1371/journal.pone.0308993
[12] StormWall. (2024). Q1 2024 DDoS Attack Report. https://stormwall.network/resources/blog/ddos-report-q1-2024
[13] Tempo English. (2023). BSSN Records 361 Million Cyber Attacks in Indonesia. https://en.tempo.co/read/1797753/bssn-records-361-million-cyber-attacks-in-indonesia
[14] SOCRadar. (2024). Indonesia Threat Landscape Report 2024. https://socradar.io/wp-content/uploads/2024/08/SOCRadar-Indonesia-Threat-Landscape-Report-2024.pdf
[15] SOCRadar. (2024). Global DDoS Attack Landscape: Insights from Q1 2024. https://socradar.io/global-ddos-attack-landscape-insights-from-q1-2024/
[16] Help Net Security. (2024). DDoS attack power skyrockets to 1.6 Tbps. https://www.helpnetsecurity.com/2024/02/02/ddos-attacks-h2-2023/
[17] ResearchGate. (2023). Network Intrusion Detection: Comparative Analysis of NSL-KDD and CIC-IDS2017 Datasets. https://www.researchgate.net/publication/372926154
[18] GitHub. (2023). Intrusion-Detection-CICIDS2017 – Detailed Feature Analysis. https://github.com/noushinpervez/Intrusion-Detection-CICIDS2017
[19] Repository St. Cloud State University. (2022). A Supervised Machine Learning Approach to Network Intrusion Detection using CICIDS2017. https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1155&context=msia_etds
[20] Ikotun, A. M. et al. (2026). Performance Evaluation of Validity Indices on Evolutionary K-Means Clustering. ICONIP 2025, *Springer.*https://link.springer.com/chapter/10.1007/978-981-95-4384-7_23
[21] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *ICISSP 2018.*https://www.unb.ca/cic/datasets/ids-2017.html
[22] ScienceDirect. (2025). A review on intrusion detection datasets: tools, processes, and features. https://www.sciencedirect.com/science/article/pii/S1389128625001458
[23] PMC. (2024). Optimization of predictive performance of intrusion detection system using hybrid ensemble model. https://pmc.ncbi.nlm.nih.gov/articles/PMC10496009/
[24] JISEM Journal. (2025). Hybrid Multi-Stage Intrusion Detection System (HMS-IDS) using CIC-ToN-IoT. https://jisem-journal.com/index.php/journal/article/download/1665/653/2705
[25] Journal of Big Data, Springer. (2023). Network intrusion detection using data dimensions reduction techniques. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-023-00697-5
[26] MDPI Mathematics. (2021). Improved Constrained K-Means Algorithm for Clustering with Domain Knowledge. *Mathematics*, 9(19), 2390. https://www.mdpi.com/2227-7390/9/19/2390

[27] MDPI Electronics. (2020). The K-Means Algorithm: A Comprehensive Survey and Performance Evaluation. *Electronics,* 9(8), 1295. https://www.mdpi.com/2079-9292/9/8/1295
[28] MDPI Sustainability. (2022). K-Means Clustering Approach for Intelligent Customer Segmentation. *Sustainability*, 14(12), 7243. https://www.mdpi.com/2071-1050/14/12/7243
[29] MDPI / PMC Future Internet. (2024). Insight into Anomaly Detection and Prediction Leveraging K-Means Clustering on Call Detail Records. https://pmc.ncbi.nlm.nih.gov/articles/PMC10974756/
[30] PLOS ONE. (2025). Adoption of K-Means Clustering Algorithm in Smart City Security Analysis. *PLOS ONE.*https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0319620
[31] MDPI Applied Sciences. (2021). K-Means-Based Nature-Inspired Metaheuristic Algorithms for Automatic Data Clustering. *Applied Sciences,* 11(23), 11246. https://www.mdpi.com/2076-3417/11/23/11246
[32] Sinaga, K. P., & Yang, M. S. (2020). Unsupervised K-Means Clustering Algorithm. *IEEE Access*, 8. https://ieeexplore.ieee.org/document/9072123
[33] Nature Scientific Reports. (2025). Enhancing Classification Accuracy in Medical Datasets Using a Hybrid Distance K-Means Method. *Scientific Reports.*https://www.nature.com/articles/s41598-025-30176-1
[34] MDPI AI. (2024). Machine Learning-Based Network Anomaly Detection Using Clustering and Classification. *AI,* 5(4), 143. https://www.mdpi.com/2673-2688/5/4/143
[35] PMC Computational Intelligence and Neuroscience. (2022). Research and Application of Clustering Algorithm for Text Big Data. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9200521/
[36] MDPI Algorithms. (2025). Improving K-Means Clustering: Parallelized Variants for Satellite Image Clustering. *Algorithms,* 18(8), 532. https://www.mdpi.com/1999-4893/18/8/532