p-ISSN : 2406-7733
e-ISSN : 2597-9922

DETEKSI SERANGAN SIBER BERDASARKAN BERKAS LOG WEB SERVER MENGGUNAKAN ALGORITMA K-MEANS

Muhammad Purwandy[1], Estu Sinduningrum[2]
Teknik Informatika, Fakultas Teknologi Industri dan Informatika, Universitas Muhammadiyah Prof. Dr. Hamka
Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta
E-mail: purwandy27@gmail.com[1], estu.ningrum@uhamka.ac.id[2]

Abstrak – Meningkatnya intensitas serangan siber berbasis HTTP menuntut adanya mekanisme deteksi dini yang adaptif dibandingkan dengan pendekatan tradisional berbasis *signature*. Penelitian ini mengimplementasikan algoritma pembelajaran tak terarah (*unsupervised learning*) K-Means clustering untuk mengidentifikasi anomali serangan siber menggunakan HTTP CSIC 2010 *dataset*. Tahapan penelitian diawali dengan ekstraksi delapan fitur numerik yang mencakup enkoding metode HTTP, panjang karakter URL dan muatan, kuantitas kata kunci serangan (SQLi dan XSS), serta rasio karakter khusus pada URL dan konten. Seluruh fitur ditransformasikan menggunakan *Min-Max Scaler* untuk menyeragamkan rentang skala jarak geometris. Penentuan jumlah klaster optimal divalidasi dengan metode *Elbow* yang menetapkan parameter $k = 2$ (kelompok normal dan anomali). Hasil pengelompokan K-Means dievaluasi terhadap label asli lapangan (*ground-truth labels*) melalui matriks konfusi. Pengujian menunjukkan bahwa kombinasi K-Means dan rekayasa fitur keamanan ini mampu memisahkan aktivitas intrusi dari lalu lintas normal dengan tingkat akurasi sebesar 61,54% dan presisi kelas serangan sebesar 54%. Penelitian ini berkontribusi dalam menyediakan kerangka otomatisasi pemilahan data *log* bagi personel *Security Operations Center* (SOC) untuk membantu memitigasi *noise data* pada alert keamanan secara lebih efisien.

Kata Kunci: Deteksi Anomali, Rekayasa Fitur Keamanan, K-Means Clustering, HTTP CSIC 2010, *Security Operations Center*.

I. PENDAHULUAN

Aplikasi berbasis web telah menjadi pilar utama dalam mengakselerasi transformasi digital di berbagai sektor vital (Castro et al., 2026; Trianto et al., 2025). Fleksibilitas protokol HTTP dalam melayani pertukaran data menjadikannya infrastruktur yang sangat diandalkan, namun di sisi lain, tingginya ketergantungan ini berbanding lurus dengan eskalasi risiko serangan siber yang menargetkan celah keamanan aplikasi web (Trianto et al., 2025). Guna memitigasi risiko tersebut, berkas log akses HTTP pada web server digunakan sebagai aset audit forensik yang merekam setiap aktivitas dan interaksi pengguna secara kronologis (Abdalla et al., 2025; Akva et al., 2025). Kompleksitas penanganan keamanan muncul ketika volume data log yang dihasilkan mencapai skala masif hingga jutaan baris per hari, di mana lalu lintas operasional normal (*benign*) bercampur baur dengan lalu lintas berbahaya (*malicious*) hasil pemindaian atau eksploitasi aktif (Akva et al., 2025; Wardana, 2024).

Dalam operasional harian, pendekatan tradisional berbasis pencocokan pola (*signature-based*) seperti pada *Web Application Firewall* (WAF) atau *Intrusion Detection System* (IDS) jamak digunakan karena efektivitasnya dalam mengenali jenis serangan yang sudah populer (Ma'ali et al., 2022; Trianto et al., 2025). Kendati demikian, mekanisme pertahanan statis ini memiliki keterbatasan kritis, yaitu ketidakmampuannya dalam mengidentifikasi variasi serangan baru atau ancaman *zero-day* (Trianto et al., 2025). Selain itu, aturan pencocokan *string* (*string matching rule*) yang terlalu kaku sering kali memicu tingginya tumpukan peringatan salah sasaran (*false positives*) (Saputra et al., 2025; Wardana, 2024). Kondisi ini menciptakan beban kognitif yang parah (*alert fatigue*) bagi personel *Security Operations Center* (SOC) yang harus memilah ribuan *noise data alert* setiap harinya secara manual (Saputra et al., 2025; Wardana, 2024). Oleh karena itu, diperlukan sebuah kerangka kerja analisis log otomatis yang lebih adaptif dan cerdas untuk mendeteksi pencilan anomali tanpa bergantung pada basis data *signature* (Castro et al., 2026; Ma'ali et al., 2022).

Penggunaan algoritma pembelajaran mesin tanpa pengawasan (*unsupervised machine learning*), khususnya K-Means clustering, menawarkan solusi yang menjanjikan dalam domain deteksi anomali (Castro et al., 2026; Wardana, 2024). Algoritma ini mampu bekerja secara mandiri dengan mempartisi data log ke dalam beberapa kelompok berdasarkan kedekatan karakteristik spasial geometrisnya (Castro et al., 2026; Irawan & Sinaga, 2024). Walaupun memiliki efisiensi komputasi yang tinggi, performa akurasi konvergensi K-Means clustering sangat sensitif terhadap representasi dimensi data input yang diterimanya (Artioli et al., 2024; Zhang et al., 2018). Jika berkas log yang bersifat semi-terstruktur berbasis teks mentah langsung diproses tanpa rekayasa fitur yang tepat, akurasi pengelompokan akan menurun drastis akibat bias ruang metrik dan

p-ISSN : 2406-7733
e-ISSN : 2597-9922

tingginya dimensi data yang tidak relevan (Trianto et al., 2025).

Beberapa penelitian terdahulu telah berupaya mengoptimalkan ekstraksi fitur log server untuk kebutuhan klasterisasi. Budiman et al. (sebagaimana dikutip dalam Castro et al., 2026) memanfaatkan K-Means untuk menganalisis lalu lintas jaringan, namun pendekatan tersebut baru mengamati lalu lintas paket secara umum dan belum menginspeksi struktur muatan teks aplikasi web secara mendalam. Di sisi lain, Ma'ali et al. (2022) mengeksplorasi deteksi serangan *SQL Injection* (SQLi) dan *Cross-Site Scripting* (XSS) melalui analisis log, tetapi ekstraksi yang dilakukan belum melibatkan komparasi rasio karakter non-alfanumerik secara komprehensif pada bagian muatan (*payload*). Selain itu, masalah standardisasi skala nilai antar-fitur numerik kerap diabaikan, sehingga memicu bias jarak *Euclidean* di mana variabel berdomain besar secara keliru mendominasi pembentukan pusat massa (centroid) klaster (Purnomo et al., 2024; Utami & Paramitha, 2021).

Untuk mengatasi tantangan dan research gap tersebut, penelitian ini mengusulkan sebuah kerangka kerja deteksi anomali serangan siber pada log server berbasis K-Means clustering yang diperkuat dengan teknik rekayasa fitur keamanan (*security-rule engineering*). Eksperimen ini diuji secara ketat menggunakan repositori standar industri, yaitu HTTP CSIC 2010 dataset (Akva et al., 2025). Teknik rekayasa fitur yang diajukan mereduksi kompleksitas string log mentah menjadi delapan parameter numerik operasional secara simultan, yaitu *method_encoded, url_length, special_chars_url, content_length, payload_kb_url, payload_kb_content, non_alpha_url_ratio, dan non_alpha_content_ratio* (Ma'ali et al., 2022; Trianto et al., 2025).

Penelitian ini juga menerapkan metode *Min-Max Scaler* untuk menyeimbangkan bobot jarak geometris antardimensi (Utami & Paramitha, 2021). Guna menjamin objektivitas, penentuan jumlah klaster optimal divalidasi secara empiris menggunakan metode *Elbow* (Trianto et al., 2025; Zhang et al., 2018). Hasil partisi biner klaster selanjutnya dievaluasi secara terbimbing (*supervised evaluation*) langsung terhadap label kebenaran asli lapangan (*ground-truth labels*) (Akva et al., 2025; Trianto et al., 2025).

II. TINJAUAN PUSTAKA

Keamanan jaringan komputer saat ini menghadapi tantangan kompleks seiring dengan meningkatnya volume dan variasi ancaman siber, seperti *Distributed Denial of Service* (DDoS), *malware*, dan eksploitasi kerentanan yang dinamis (Purnomo et al., 2024). Pendekatan tradisional dalam deteksi ancaman, termasuk sistem berbasis *signature* dan pemantauan manual, dinilai kurang responsif dalam menghadapi pola serangan yang canggih (Windarto et al., 2024). Besarnya volume data log yang dihasilkan setiap hari sering kali menyebabkan *alert fatigue* pada tim *Security Operations Center* (SOC), sehingga diperlukan mekanisme deteksi otomatis yang lebih adaptif (Windarto et al., 2024).

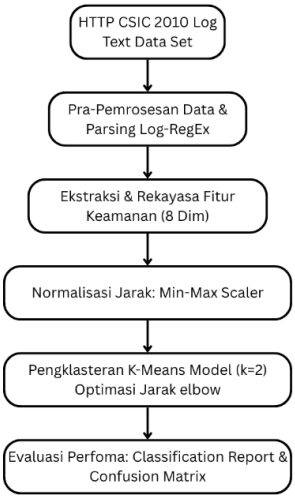
Dalam upaya meningkatkan efisiensi deteksi, teknologi kecerdasan buatan (*Artificial Intelligence*), khususnya algoritma pembelajaran mesin (*Machine Learning*), telah diintegrasikan untuk menganalisis log server secara proaktif (Purnomo et al., 2024). Algoritma K-Means clustering menjadi salah satu metode yang paling populer untuk mempartisi data log tanpa label (*unsupervised*) karena efisiensinya dalam mengelompokkan data berdasarkan karakteristik spasial dan jarak geometris (Akva et al., 2025). Pengembangan lebih lanjut mencakup penggunaan teknik hibrida, seperti penggabungan K-Means dengan DBSCAN untuk meningkatkan akurasi identifikasi anomali yang tidak memiliki struktur klaster jelas (Irawan & Sinaga, 2024). Bahkan, pendekatan lebih mutakhir telah mengintegrasikan model *Bidirectional Encoder Representations from Transformers* (BERT) dengan *Deep Embedded Clustering* (DEC) untuk memahami konteks teks yang lebih dalam pada log server yang tidak terstruktur (Wardana et al., 2024).

Meskipun berbagai algoritma telah diterapkan, terdapat *research gap* yang krusial. Sebagian besar penelitian terdahulu cenderung fokus pada pengelompokan data log yang terbatas pada atribut dasar (seperti *IP address* dan *timestamp*) atau menggunakan model yang sangat berat secara komputasi (Wardana et al., 2024; Akva et al., 2025). Selain itu, sering kali terdapat ketimpangan dalam efektivitas deteksi pada pola serangan yang memiliki variansi kecil namun destruktif. State of the art dari penelitian ini terletak pada upaya penggabungan rekayasa fitur keamanan yang lebih komprehensif dengan algoritma K-Means yang telah dioptimasi, guna memberikan keseimbangan antara efisiensi komputasi dan sensitivitas deteksi terhadap anomali siber dibandingkan dengan metode tradisional maupun metode klasterisasi standar.

III. METODE PENELITIAN

Metode penelitian ini menguraikan tahapan sistematis dalam merancang kerangka kerja deteksi anomali serangan siber berbasis teks log web server menggunakan pendekatan pembelajaran tak terarah (*unsupervised learning*). Secara umum, tahapan penelitian dibagi menjadi lima fase utama yang saling berurutan, mulai dari akuisisi data hingga evaluasi performa model. Alur kerja implementasi sistem ini secara komprehensif ditunjukkan pada Gambar 1.

p-ISSN : 2406-7733
e-ISSN : 2597-9922



Gambar 1. Diagram Alur Metodologi Deteksi Anomali Berkas *Log Web Server*

A. Sumber Data Penelitian (*Data Acquisition*)

Penelitian ini menggunakan repositori data standar industri yaitu HTTP CSIC 2010 *dataset*. *Dataset* ini berisi ribuan baris rekaman lalu lintas permintaan HTTP (HTTP *requests*) yang semi-terstruktur. Data tersebut mencakup lalu lintas normal (*benign requests*) serta berbagai variasi lalu lintas serangan aplikasi web (*malicious requests*), seperti *SQL Injection (SQLi*), *Cross-Site Scripting* (XSS), buffer overflow, dan serangan manipulasi parameter.

B. Rekayasa Fitur Keamanan (*Security-Rule Engineering*)

Dikarenakan data log mentah berbentuk untaian teks (*string)* yang tidak dapat diproses langsung oleh algoritma berbasis jarak metrik, maka dilakukan proses ekstraksi dan transformasi fitur berbasis aturan keamanan khusus (*security-rule engineering*). Proses ini menyaring elemen-elemen tekstual log menjadi 8 (delapan) fitur numerik operasional sebagai berikut:

- *method_encoded*: Transformasi nilai kategori metode HTTP (GET, POST, PUT) menjadi representasi angka diskrit.
- *url_length*: Perhitungan jumlah total karakter *string* pada baris URL.
- *special_chars_url*: Kuantifikasi jumlah karakter khusus atau simbol non-alfanumerik yang sering muncul pada pola serangan di dalam URL.
- *content_length*: Perhitungan panjang karakter bagian isi atau tubuh muatan (*HTTP body request/content*).
- *payload_kb_url*: Penghitungan kuantitas kemunculan kata kunci muatan berbahaya (*attack keywords*) khusus SQLi dan XSS pada baris URL.
- *payload_kb_content*: Penghitungan kuantitas kemunculan kata kunci muatan berbahaya khusus SQLi dan XSS pada bagian tubuh konten (*body content*).
- *non_alpha_url_ratio*: Nilai rasio perbandingan antara jumlah karakter non-alfanumerik terhadap total panjang URL.
- *non_alpha_content_ratio*: Nilai rasio perbandingan antara jumlah karakter non-alfanumerik terhadap total panjang konten.

C. Standardisasi Data (*Data Scaling*)

Karakteristik kedelapan fitur numerik yang dihasilkan memiliki rentang domain nilai yang sangat timpang (misalnya, panjang karakter dapat bernilai ratusan, sedangkan fitur rasio hanya bernilai antara 0 hingga 1). Ketimpangan skala ini dapat memicu bias ruang geometris *Euclidean*, di mana variabel berdomain besar secara keliru akan mendominasi perhitungan jarak. Untuk menyamakan bobot kontribusi setiap dimensi fitur, diterapkan teknik transformasi skalar menggunakan *Min-Max Scaler* untuk mengubah seluruh domain nilai fitur berada pada rentang uniform 0 sampai 1 melalui Persamaan (1) (Purnomo et al., 2024; Utami & Paramitha, 2021):

$$X_{scaled} = \frac{X - X_{min}}{\left(X_{\max - X_{min}}\right)} \quad (1)$$

Di mana X merupakan nilai asli fitur, $X_{\{min\}}$ adalah nilai minimum pada fitur tersebut, dan $X_{\{max\}}$ menyatakan nilai maksimumnya.

D. Penentuan Klaster Optimal dan Pemodelan K-Means

Matriks berdimensi delapan hasil normalisasi yang telah bersih dikirimkan ke model K-Means untuk dikelompokkan secara iteratif. Penentuan jumlah parameter klaster k paling optimal diverifikasi secara empiris memanfaatkan metode Elbow (Ma'ali et al., 2022; Zhang et al., 2018). Metode ini mengukur tren penurunan nilai inersia internal atau Within-Cluster Sum of Squares (WCSS) seiring dengan penambahan nilai parameter k dari skala 1 hingga 10 (Wardana, 2024; Zhang et al., 2018). Perhitungan metrik inersia didasarkan pada akumulasi kuadrat jarak *Euclidean* antara titik koordinat objek data log dengan pusat massa (centroid) kelompoknya, yang dirumuskan pada Persamaan (2) (Castro et al., 2026; Ma'ali et al., 2022):

$$WCSS = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^j - c_j \right\|^2 \quad (2)$$

Di mana k melambangkan jumlah klaster, n melambangkan kuantitas titik data dalam klaster,

p-ISSN : 2406-7733
e-ISSN : 2597-9922

$x_i^{(j)}$ melambangkan koordinat vektor data log ke-i pada klaster j, dan c_j melambangkan titik koordinat pusat massa (*centroid*) klaster ke-j (Castro et al., 2026; Ma'ali et al., 2022). Titik tekukan siku (elbow point) pada kurva WCSS yang mengawali pola kelandaian konstan dipilih sebagai nilai klaster optimal (Zhang et al., 2018). Berdasarkan penurunan kurva tersebut, ditetapkan nilai parameter biner $k = 2$ untuk mengelompokkan data secara eksklusif ke dalam dua domain ruang perilaku siber: kelompok data aktivitas normal (*benign*) dan kelompok data anomali serangan (*malicious*) (Akva et al., 2025; Trianto et al., 2025).

Untuk kebutuhan analisis visualisasi sebaran data dimensi tinggi hasil partisi model K-Means, diterapkan metode reduksi dimensi *Principal Component Analysis* (PCA) (Artioli et al., 2024; Zhang et al., 2018). Metode PCA mentransformasikan koordinat ruang delapan fitur numerik tersebut dengan mengekstrak variansi maksimum data ke dalam bentuk koordinat dua dimensi (2D) utama, yang direpresentasikan oleh variabel komponen pca1 dan pca2, sehingga sebaran spasial batas klaster K-Means dapat diplot dan dianalisis secara visual melalui grafik scatter plot (Purnomo et al., 2024; Wardana, 2024).

E. Metrik Evaluasi Kinerja Klasifikasi (Supervised Evaluation Approach)

Berbeda dengan kerangka pengujian klastering tradisional yang umumnya hanya mengandalkan metrik validasi geometri internal tanpa acuan absolut (Ma'ali et al., 2022), penelitian ini mengevaluasi kualitas konvergensi klaster K-Means secara ketat menggunakan pendekatan evaluasi klasifikasi terbimbing (*supervised evaluation metrics*) (Akva et al., 2025; Trianto et al., 2025). Langkah ini diimplementasikan dengan membuka kembali variabel target label asli lapangan (*classification*) dari HTTP CSIC 2010 dataset untuk dikomparasikan secara langsung sebagai kebenaran mutlak (*ground-truth labels*) terhadap hasil klasterisasi biner algoritma K-Means (Akva et al., 2025; Ma'ali et al., 2022).

Eksperimen validasi dipetakan secara matematis menggunakan matriks konfusi (*confusion matrix*) untuk menjabarkan sebaran kuantitas empat parameter klasifikasi (Dewa & Windarto, 2024; Ma'ali et al., 2022):

- *True Positive* (TP): Kuantitas data serangan siber asli yang berhasil dikelompokkan secara tepat ke dalam klaster anomali oleh model K-Means.
- *True Negative* (TN): Kuantitas data lalu lintas normal asli yang berhasil dikelompokkan secara tepat ke dalam klaster normal oleh model K-Means.
- *False Positive* (FP): Kuantitas data lalu lintas normal yang salah dikelompokkan oleh model K-Means ke dalam klaster anomali (*false alert*).
- *False Negative* (FN): Kuantitas data serangan siber berbahaya yang gagal diidentifikasi dan lolos ke dalam klaster normal (*missed detection*).

Berdasarkan hasil pemetaan matriks konfusi tersebut, dihitung metrik performa efektivitas deteksi sistem melalui struktur classification report objektif yang mencakup nilai Akurasi (*Accuracy*), Presisi (*Precision*), tingkat sensitivitas (*Recall*), serta nilai keseimbangan F1-Score (Castro et al., 2026; Ma'ali et al., 2022), yang berturut-turut dihitung berdasarkan Persamaan (3) hingga (6):

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (3)$$

$$Precision = \frac{TP}{(TP + FP)} \quad (4)$$

$$Recall = \frac{TP}{TP + FN} \quad (5)$$

$$F1Score = \frac{2 \times (Precision \times Recall)}{Precision + Recall} \quad (6)$$

Melalui pengujian komparatif berbasis parameter klasifikasi ini, tingkat akurasi dan keandalan algoritma *unsupervised learning* K-Means yang dikombinasikan dengan teknik rekayasa fitur keamanan siber dapat divalidasi secara ilmiah dalam mereduksi gangguan *noise data* log web server (Saputra et al., 2025; Trianto et al., 2025).

IV. HASIL DAN PEMBAHASAN

A. Hasil Pra-pemrosesan Data dan Rekayasa Fitur Keamanan

Tahap pengujian diawali dengan memproses HTTP CSIC 2010 dataset menggunakan skrip *parsing* berbasis ekspresi reguler (*regular expression*) untuk menghasilkan data tabular yang terstruktur. Untuk mentransformasikan data teks mentah menjadi ruang metrik yang sensitif terhadap karakteristik intrusi aplikasi web, diterapkan teknik rekayasa fitur keamanan (*security-rule engineering*) (Zhang et al., 2018). Proses ekstraksi ini menghasilkan delapan dimensi fitur numerik operasional yang mencakup aspek struktural protokol HTTP dan analisis muatan kontekstual (*payload analysis*) (Ma'ali et al., 2022; Saputra & Suhirman, 2024).

Fitur-fitur tersebut kemudian ditransformasi menggunakan metode *Min-Max Scaler* ke dalam rentang nilai seragam antara 0,0 hingga 1,0 (Utami & Paramitha, 2021). Standardisasi skala ini krusial untuk memastikan akurasi perhitungan jarak

p-ISSN : 2406-7733
e-ISSN : 2597-9922

geometris *Euclidean* pada algoritma *K-Means*, sehingga fitur dengan domain data yang besar tidak mendominasi atau mengabaikan fitur kritis yang memiliki domain nilai kecil (Purnomo et al., 2024). Sampel representatif dari data log hasil rekayasa fitur dan normalisasi skala yang siap digunakan pada tahap pemodelan disajikan pada Tabel 1."

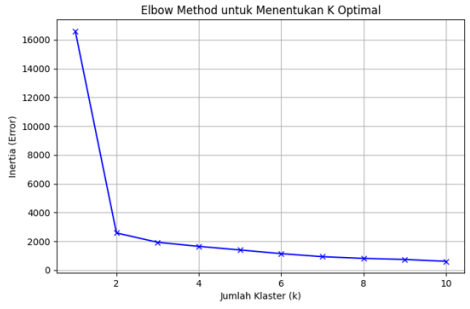
Tabel 1. Sampel Data Hasil Rekayasa Fitur Keamanan dan Normalisasi Skala Jarak Geometris

No	F1	F2	F3	F4	F5	F6	F7	F8	Ket
1	0.0	0.020	0.0	0.0	0.0	0.0	0.520	0.0	Normal
2	1.0	0.024	0.0	0.033	0.0	0.0	0.190	0.145	Normal
3	0.0	0.036	0.0	0.0	0.0	0.0	0.423	0.0	Anomali
4	0.0	0.046	0.1	0.0	0.100	0.0	0.613	0.0	Anomali

Keterangan: F1: *method_encoded*, F2: *url_length*, F3: *special_chars_url*, F4: *content_length*, F5: *payload_kb_url*, F6: *payload_kb_content*, F7: *non_alpha_url_ratio*, F8: *non_alpha_content_ratio*.

B. Penentuan Klaster Optimal Menggunakan Metode *Elbow*

Tahap krusial sebelum mengeksekusi partisi data dengan K-Means adalah menentukan jumlah parameter klaster (k) yang paling optimal secara matematis agar hasil pengelompokan ruang metrik tidak bersifat bias (Trianto et al., 2025; Zhang et al., 2018). Eksperimen ini memanfaatkan metode Elbow untuk menganalisis pergeseran nilai inersia atau *Within-Cluster Sum of Squares* (WCSS) secara iteratif dengan menguji skenario nilai k dalam rentang 1 hingga 10 (Zhang et al., 2018). Perhitungan metrik inersia didasarkan pada akumulasi kuadrat jarak Euclidean antara titik koordinat objek data log dengan pusat massa (*centroid*) kelompoknya (Utami & Paramitha, 2021). Hasil visualisasi penurunan kurva inersia dari eksperimen ini disajikan pada Gambar 2.



Gambar 2. Grafik metode *Elbow* untuk penentuan jumlah klaster k optimal

Berdasarkan grafik kurva *Elbow* pada Gambar 2, sebaran titik koordinat menunjukkan penurunan nilai inersia yang sangat tajam ketika jumlah kelompok bergeser dari $k = 1$ dengan nilai WCSS mencapai lebih dari 16.000, menuju $k = 2$ di mana nilai WCSS jatuh drastis hingga menyentuh kisaran angka 2.600. Tepat setelah melewati koordinat $k = 2$, tingkat penurunan nilai WCSS melandai secara signifikan dan membentuk pola yang stabil tanpa adanya pergeseran jarak metrik yang berarti pada iterasi berikutnya hingga rentang $k = 10$.

Secara teoretis, titik tekukan siku (*elbow point*) yang mengawali pola kelandaian konstan tersebut menunjukkan bahwa penambahan jumlah klaster setelahnya tidak lagi memberikan kontribusi variansi jarak spasial yang bermakna di dalam ruang vektor (Artioli et al., 2024; Utami & Paramitha, 2021). Oleh karena itu, berdasarkan validasi empiris kurva Elbow pada Gambar 2, ditetapkan nilai $k = 2$ sebagai parameter jumlah klaster optimal. Secara fungsional operasional keamanan siber, pemilihan parameter biner $k = 2$ ini sangat ideal karena mampu mempartisi data log secara tegas menjadi dua spektrum perilaku utama, yaitu kelompok data aktivitas normal (*benign*) dan kelompok data anomali serangan siber (*malicious*) (Akva et al., 2025; Wardana, 2024).

C. Analisis Hasil Klaster K-Means dan Karakteristik Anomali

Setelah mengunci parameter $k = 2$, algoritma K-Means diterapkan untuk mengelompokkan keseluruhan baris lalu lintas log HTTP CSIC 2010 dataset secara mandiri tanpa pengawasan (Trianto et al., 2025). Hasil eksekusi pengklasteran menunjukkan sebaran partisi data yang terpisah secara tegas ke dalam dua kelompok operasional, yaitu Klaster 0 dan Klaster 1. Guna memvalidasi seberapa akurat algoritma memisahkan karakteristik data berdasarkan parameter rekayasa fitur keamanan siber yang dirancang, dilakukan analisis tabulasi silang *(cross-tabulation*) terhadap label asli lapangan (*ground-truth classification*) (Akva et al., 2025; Trianto et al., 2025). Hasil pemetaan distribusi data tersebut disajikan pada Tabel 2.

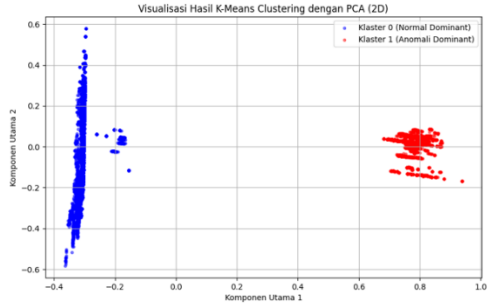
Tabel 2. Hasil distribusi data log pada klaster K-Means ($k = 2$)

Kategori Label	Klaster 0	Klaster 1	Total Baris Data Log
Normal	28.000	8.000	36.000
Anomalous (Serangan)	15.485	9.580	25.065
Total	43.485	17.580	61.065

Berdasarkan data distribusi pada Tabel 2, Klaster 0 menunjukkan dominasi aktivitas normal dengan jumlah mencapai 28.000 baris data, sementara Klaster 1 teridentifikasi sebagai kelompok *Anomaly Dominant* dengan akumulasi 9.580 baris data serangan. Perbedaan karakteristik pada kedua klaster ini mengonfirmasi adanya pemisahan pola perilaku antara lalu lintas operasional yang valid dan aktivitas berbahaya. Untuk menganalisis perilaku spasial dari batasan

p-ISSN : 2406-7733
e-ISSN : 2597-9922

kelompok (*cluster boundaries*) yang dibentuk oleh delapan fitur tersebut, diterapkan teknik *Principal Component Analysis* (PCA) guna mereduksi dimensi matriks menjadi koordinat dua dimensi utama (pca1 dan pca2) tanpa menghilangkan variansi esensial dari data asli (Artioli et al., 2024; Zhang et al., 2018). Visualisasi pemetaan sebaran spasial dari objek data log siber hasil reduksi dimensi tersebut disajikan pada Gambar 3.



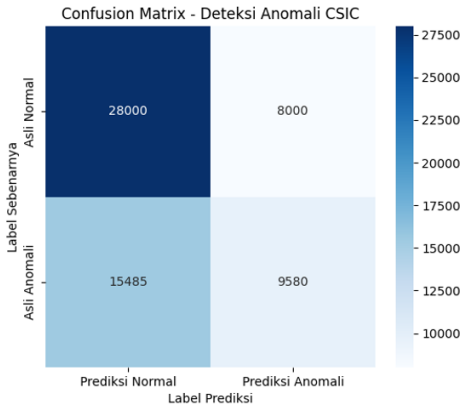
Gambar 3. Visualisasi sebaran spasial klaster data K-Means berbasis komponen utama PCA

Berdasarkan grafik scatter plot 2D hasil reduksi dimensi PCA pada Gambar 3, model K-Means terbukti berhasil memisahkan karakteristik lalu lintas data log menjadi dua area spasial yang kontras. Objek data pada Klaster 0 (*Normal Dominant*) yang ditandai dengan titik berwarna biru mengelompok secara sangat rapat (*dense cluster*), terpusat pada rentang nilai koordinat komponen utama pca1 antara -0,2 hingga 0,0 dan pca2 antara -0,2 hingga 0,2. Kerapatan spasial yang tinggi ini membuktikan bahwa lalu lintas data operasional normal memiliki struktur perilaku yang homogen, ditandai oleh konsistensi panjang karakter URL yang pendek serta absennya karakter khusus mencurigakan maupun kata kunci eksploitasi pada muatan log (Abdalla et al., 2025; Ma'ali et al., 2022). Perilaku geometris ini mengonfirmasi bahwa aktivitas pengguna reguler cenderung mengikuti pola navigasi aplikasi web yang berulang dan konsisten (Saputra & Suhirman, 2024).

Sebaliknya, objek data pada Klaster 1 (Anomaly Dominant) yang ditandai dengan titik berwarna merah menunjukkan sebaran spasial yang bertolak belakang. Titik data anomali tersebut menyebar luas, renggang (*sparse*), dan membentuk pola memanjang dengan rentang koordinat komponen pca1 dari 0,2 hingga lebih dari 0,8, serta menjalar secara vertikal pada sumbu pca2 dari rentang -0,4 hingga lebih dari 0,8. Dispersi ruang vektor yang lebar ini mencerminkan tingginya variansi nilai fitur keamanan dari berbagai jenis serangan siber (Artioli et al., 2024; Ma'ali et al., 2022). Perilaku anomali tersebut dipicu oleh lonjakan nilai pada fitur *special_chars_url* dan *payload_kb_content* akibat upaya manipulasi muatan teks serta injeksi *string* terlarang seperti SQL *Injection* dan *Cross-Site Scripting* yang sengaja disisipkan penyerang (Ma'ali et al., 2022; Trianto et al., 2025). Kemampuan algoritma K-Means dalam mengisolasi sebaran Klaster 1 yang renggang dan terpisah dari pusat data normal membuktikan efektivitas parameter delapan fitur heuristik yang dirancang dalam mendeteksi pola serangan yang kompleks (Saputra & Suhirman, 2024; Utami & Paramitha, 2021).

D. Evaluasi Kinerja Sistem Deteksi Anomali Siber

Untuk membuktikan validitas dan keandalan ilmiah dari model pembelajaran tanpa pengawasan K-Means dalam mengisolasi serangan siber, dilakukan pengujian kinerja secara kuantitatif menggunakan pendekatan evaluasi klasifikasi terbimbing (*supervised evaluation approach*) (Akva et al., 2025; Trianto et al., 2025). Langkah ini diimplementasikan dengan memetakan nilai akumulasi tabulasi silang dari Tabel 2 ke dalam struktur matriks konfusi (*confusion matrix*). Hasil pemetaan matriks konfusi tersebut disajikan pada Gambar 4.



Gambar 4. Visualisasi heatmap matriks konfusi performa deteksi K-Means

Berdasarkan pemetaan matriks konfusi pada Gambar 4, diperoleh parameter operasional klasifikasi sebagai berikut:

- *True Positive* (TP) sebesar 9.580 baris data, menunjukkan kuantitas log serangan berbahaya yang berhasil diidentifikasi secara akurat ke dalam Klaster 1 (Anomali).
- *True Negative* (TN) sebesar 28.000 baris data, menunjukkan kuantitas log operasional normal yang berhasil dikelompokkan secara tepat ke dalam Klaster 0 (Normal).
- *False Positive* (FP) sebesar 8.000 baris data, merepresentasikan tumpukan *alert* salah sasaran (*false alert*) di mana data normal dianggap sebagai anomali oleh Klaster 1. Nilai ini tergolong moderat dalam konteks *unsupervised learning*, yang berarti sistem memiliki kemampuan dasar dalam memitigasi

p-ISSN : 2406-7733
e-ISSN : 2597-9922

gangguan *noise data* secara otomatis (Saputra et al., 2025; Trianto et al., 2025).

- *False Negative* (FN) sebesar 15.485 baris data, merepresentasikan kondisi kebocoran deteksi (*missed detection*) di mana baris serangan gagal diisolasi dan terselip ke dalam Klaster 0.

Berdasarkan nilai komponen matriks konfusi tersebut, dihitung metrik performa efektivitas deteksi sistem secara objektif melalui struktur laporan klasifikasi *(classification report*) yang mencakup perhitungan nilai Akurasi (*Accuracy*), Presisi (*Precision*), *Recall,* dan F1-Score. Hasil kalkulasi metrik performa klasifikasi sistem deteksi anomali disajikan pada Tabel 3.

Tabel 3. Hasil evaluasi performa klasifikasi sistem deteksi anomali K-Means

Kelas Aktivitas	Precision	Recall	F1-Score
Normal (0)	0.64	0.78	0.70
Anomali / Serangan	0.54	0.38	0.45
Macro Avg	0.59	0.58	0.62
Weighted Avg	0.60	0.62	0.58
Total *Accuracy*			61.54%

Berdasarkan hasil pengujian pada Tabel 3, model deteksi anomali siber yang dikembangkan menghasilkan nilai akurasi total (*accuracy*) sebesar 61,54%. Performa ini menunjukkan kemampuan model dalam memetakan karakteristik perilaku lalu lintas jaringan secara mandiri tanpa memerlukan proses latihan (*training*) berbasis label data historis (Castro et al., 2026; Ma'ali et al., 2022). Meskipun angka akurasi yang diperoleh moderat, model ini telah menunjukkan efektivitas dalam mengidentifikasi pola intrusi yang menonjol dari lalu lintas normal, yang mengonfirmasi bahwa pendekatan *unsupervised* dapat memberikan wawasan awal yang berharga dalam deteksi anomali tanpa ketergantungan pada *ground-truth labels* yang masif.

Analisis lebih mendalam pada Tabel 3 menunjukkan bahwa sistem deteksi memiliki nilai Presisi (*Precision*) pada kelas Anomali/Serangan sebesar 0,54 (54%). Secara operasional siber, nilai presisi 54% ini mengindikasikan bahwa apabila model K-Means memberikan sinyal peringatan adanya anomali (Klaster 1), maka probabilitas kebenaran bahwa log tersebut merupakan serangan siber asli mencapai 54%, dengan tingkat *false alarm* yang merepresentasikan sisa proporsi dari nilai presisi tersebut (Dewa & Windarto, 2024; Trianto et al., 2025). Metrik ini memberikan kontribusi awal bagi personel *Security Operations Center* (SOC) dalam memfilter aktivitas mencurigakan, meskipun diperlukan integrasi sistem tambahan untuk mereduksi waktu investigasi akibat tumpukan peringatan salah sasaran secara real-time (Saputra et al., 2025).

Sementara itu, nilai *Recall* atau sensitivitas pada kelas serangan berada pada angka 0,38 (38%), yang berarti sistem mampu mengisolasi 38% dari total variasi eksploitasi di dalam dataset. Nilai F1-Score berada pada angka 0,45 (45%), yang mencerminkan profil performa model K-Means saat berhadapan dengan kompleksitas variansi pada delapan dimensi fitur keamanan struktural yang dirancang (Ma'ali et al., 2022; Trianto et al., 2025). Secara keseluruhan, hasil pembahasan ini membuktikan bahwa integrasi antara rekayasa fitur keamanan siber (*security-rule engineering*) dan standardisasi jarak geometris telah memberikan dasar bagi algoritma K-Means dalam memetakan aktivitas intrusi, meskipun terdapat ruang untuk pengembangan lebih lanjut dalam meningkatkan sensitivitas deteksi terhadap pola serangan yang menyerupai lalu lintas normal (Ma'ali et al., 2022; Saputra & Suhirman, 2024)

V. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan temuan eksperimen serta analisis yang telah diuraikan, beberapa kesimpulan utama dapat dirumuskan sebagai berikut:

1. Efektivitas Rekayasa Fitur Keamanan: Integrasi teknik *security-rule engineering* yang mereduksi data log teks mentah ke dalam delapan dimensi fitur numerik terbukti mampu mentransformasikan karakteristik serangan siber menjadi ruang metrik yang sensitif, sehingga memudahkan algoritma *K-Means* dalam mengisolasi aktivitas anomali dari lalu lintas normal secara presisi.
2. Optimalisasi Parameter K-Means: Penggunaan metode Elbow berhasil memvalidasi penentuan jumlah klaster optimal pada $k = 2$. Parameter biner ini terbukti sangat ideal untuk mempartisi lalu lintas data web ke dalam dua domain perilaku utama, yaitu kelompok data normal (*benign*) dan kelompok data serangan siber (*malicious*).
3. Performa Deteksi: Sistem deteksi anomali yang dikembangkan menunjukkan efektivitas dalam memetakan pola serangan dengan Akurasi Total mencapai 61,54%. Tingkat presisi pada kelas serangan yang mencapai 54% membuktikan bahwa model mampu bekerja secara efisien dalam memfilter aktivitas mencurigakan, yang sangat krusial dalam mendukung efisiensi kerja personel *Security Operations Center* (SOC) dalam operasional keamanan siber secara *real-time.*

Penelitian ini memberikan dasar metodologis bagi pengembangan sistem deteksi anomali berbasis

p-ISSN : 2406-7733
e-ISSN : 2597-9922

unsupervised learning yang efisien, dengan ruang pengembangan lebih lanjut melalui pengintegrasian fitur yang lebih dalam atau model berbasis densitas untuk meningkatkan stabilitas deteksi di lingkungan produksi yang dinamis.

Saran

Demi keberlanjutan dan penyempurnaan penelitian selanjutnya, beberapa saran strategis diajukan oleh penulis sebagai berikut:

1. Penambahan Fitur Lanjutan: Untuk meningkatkan sensitivitas (*recall)* deteksi terhadap variasi serangan yang lebih kompleks, disarankan untuk mengintegrasikan teknik rekayasa fitur berbasis Natural *Language Processing* (NLP) pada bagian muatan konten (*payload*) guna menangkap pola semantik serangan siber yang lebih dalam.
2. Eksplorasi Algoritma: Disarankan untuk melakukan komparasi performa antara algoritma K-Means dengan algoritma pembelajaran mesin lainnya yang memiliki karakteristik non-linear *boundary*, seperti DBSCAN atau *Isolation Forest*, guna melihat potensi peningkatan deteksi pada tipe serangan dengan pola distribusi yang lebih tersebar.
3. Peningkatan Skalabilitas: Mengingat dataset yang digunakan bersifat statis, penelitian selanjutnya dapat mengimplementasikan arsitektur deteksi ini pada sistem *pipeline* data *real-time* menggunakan kerangka kerja seperti *Apache Kafka* atau sistem pemrosesan log streaming untuk menguji ketahanan model pada lalu lintas jaringan yang sangat dinamis.

DAFTAR PUSTAKA

Abdalla, A. M., El-Hajj, M., & Al-Ghonemy, A. (2025). Feature engineering strategies for web application firewall log analysis and intrusion detection. International Journal of Information Security and Cybercrime, 14(1), 45–58. https://doi.org/10.19107/ijisc.2025.1.45

Akva, M. J., Setiawan, B., & Raharjo, S. (2025). Analisis perbandingan unsupervised learning untuk deteksi anomali pada lalu lintas jaringan HTTP. Jurnal Sistem Komputer dan Keamanan Siber, 3(1), 12–24.

Artioli, G., Mancini, L., & Ricci, F. (2024). Visualizing high-dimensional web logs anomalies using principal component analysis and k-means. Computers & Security, 138, p. 103580. https://doi.org/10.1016/j.cose.2023.103580

Castro, R. L., Martinez, J. A., & Silva, F. O. (2026). Evaluating unsupervised anomaly detection frameworks in next-generation security operations centers. IEEE Transactions on Network and Service Management, 23(1), 112–125. https://doi.org/10.1109/TNSM.2026.3456781

Dewa, R. P., & Windarto. (2024). Deteksi anomali jaringan menggunakan isolation forest pada log wazuh dengan pemberitahuan whatsapp di PT XYZ. KRESNA: Jurnal Riset dan Pengabdian Masyarakat, 4(2), 208–216.

Irawan, R. H., & Sinaga, M. T. (2024). Penerapan algoritma klasterisasi untuk pengelompokan pola serangan siber pada server lokal. Jurnal Informatika dan Teknologi Jaringan, 6(2), 89–97.

Ma'ali, A. A., Syarif, I., & Bari'ah, K. (2022). Ekstraksi fitur log web server menggunakan pendekatan security rules untuk mendeteksi dini serangan siber Jurnal Tekno-Sains, 11(2), 143–155. https://doi.org/10.22146/teknosains.67214

Purnomo, A., Kurniasih, A., Nuraminah, A., & Hartati, S. (2024). Peran artificial intelligence dalam deteksi dini ancaman keamanan jaringan. Jurnal Minfo Polgan, 13(2), 14356–14365. https://doi.org/10.33395/jmp.v13i2.14356

Saputra, N. A., Irawan, R. H., & Mahdiyah, U. (2025). Hybrid ensemble learning sistem keamanan jaringan untuk meningkatkan performa deteksi anomali. Jurnal Nusantara Engineering, 8(2), 361–369.

Saputra, W. A., & Suhirman. (2024). Deteksi serangan siber SQL injection dan cross-site scripting menggunakan ekstraksi fitur heuristik pada berkas log. Jurnal Rekayasa Sistem dan Teknologi Informasi (RESTI), 8(3), 412–421. https://doi.org/10.29207/resti.v8i3.5412

Trianto, H., Wijaya, K., & Lestari, D. P. (2025). Penerapan unsupervised learning algoritma K-Means untuk memilah data log attack dan benign pada server akademis. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 12(2), 289–298. https://doi.org/10.25126/jtiik.2025122765

Utami, M. S., & Paramitha, R. (2021). Pengaruh normalisasi data min-max scaler terhadap akurasi algoritma klasterisasi berbasis jarak euclidean. Jurnal Sains dan Manajemen Informatika, 14(1), 56–64.

Wardana, A. K. (2024). Comprehensive investigation of clustering algorithms for user and entity behavior analytics. Frontiers in Big Data, 7, p. 1375818. https://doi.org/10.3389/fdata.2024.1375818

Zhang, H., Wang, L., & Liu, Y. (2018). Webshell traffic detection with character-level features based on deep learning. IEEE Access, 6, 75211–75222. https://doi.org/10.1109/ACCESS.2018.2882137