

Analisis dan Deteksi Cybercrime Menggunakan *Data Mining* pada Sistem Informasi *Doorsmer*

Cybercrime Analysis and Detection Using Data Mining Techniques in a Doorsmer Information System

Khairul Umami¹, Muhatri²

Universitas Potensi Utama, Jl. K.L Yos Sudarso Km.6,5 No.3A, Medan, Indonesia

Email Penulis ummi12gibmie@gmail.com¹, muhatri@potensi-utama.ac.id²

ABSTRAK

Perkembangan sistem informasi berbasis digital pada layanan doorsmer meningkatkan efisiensi pengelolaan transaksi dan aktivitas operasional, namun juga menimbulkan risiko cybercrime seperti akses ilegal, manipulasi data, dan serangan SQL Injection. Penelitian ini bertujuan menganalisis dan mendeteksi aktivitas cybercrime pada Sistem Informasi Doorsmer menggunakan metode data mining dengan algoritma K-Means Clustering. Penelitian dilakukan melalui tahapan pengumpulan data log aktivitas pengguna, preprocessing, normalisasi data, proses clustering, dan evaluasi performa cluster menggunakan Silhouette Score. Dataset penelitian terdiri dari parameter login gagal, frekuensi akses sistem, dan percobaan SQL Injection dari aktivitas pengguna. Hasil penelitian menunjukkan bahwa algoritma K-Means berhasil mengelompokkan data menjadi tiga cluster utama, yaitu aktivitas normal, aktivitas mencurigakan, dan aktivitas cybercrime. Dari 10 data sampel, diperoleh 4 aktivitas normal, 3 aktivitas mencurigakan, dan 3 aktivitas terindikasi cybercrime. Evaluasi menggunakan Silhouette Score menunjukkan kualitas cluster yang cukup baik dalam memisahkan pola aktivitas pengguna berdasarkan tingkat ancaman keamanan. Aktivitas dengan jumlah login gagal tinggi, frekuensi akses berlebihan, dan adanya percobaan SQL Injection memiliki kecenderungan kuat masuk ke cluster cybercrime. Dibandingkan metode deteksi manual, pendekatan clustering mampu mengidentifikasi pola anomali secara lebih cepat dan otomatis. Penelitian ini menunjukkan bahwa K-Means efektif digunakan sebagai metode deteksi dini cybercrime pada sistem informasi layanan berbasis digital serta berkontribusi dalam meningkatkan keamanan sistem secara lebih adaptif dan efisien.

Kata Kunci : Cybercrime, Data Mining, K-Means Clustering, Sistem Informasi Doorsmer, Anomaly Detection

ABSTRACT

The development of digital-based information systems in doorsmer services improves operational and transaction management efficiency but also increases cybercrime risks such as unauthorized access, data manipulation, and SQL Injection attacks. This study aims to analyze and detect cybercrime activities in a Doorsmer Information System using data mining techniques with the K-Means Clustering algorithm. The research stages include user activity log collection, preprocessing, data normalization, clustering processes, and cluster performance evaluation using the Silhouette Score method. The dataset consists of failed login attempts, system access frequency, and SQL Injection attempts from user activities. The results show that the K-Means algorithm successfully grouped the data into three main clusters: normal activities, suspicious activities, and cybercrime activities. From 10 tested samples, 4 were categorized as normal, 3 as suspicious, and 3 as cybercrime activities. Silhouette Score evaluation indicates that the clustering quality is sufficiently effective in separating user activity patterns based on security threat levels. Activities with high failed login attempts, excessive system access frequency, and SQL Injection attempts strongly tended to belong to the cybercrime cluster. Compared to conventional manual monitoring methods, the clustering approach provides faster and more automatic anomaly detection. This study demonstrates that K-Means is effective as an early cybercrime detection method for digital service-based information systems and contributes to improving system security adaptively and efficiently.

Keywords : Cybercrime, Data Mining, K-Means Clustering, Doorsmer Information System, Anomaly Detection

Info Artikel :

DOI: <https://www.doi.org/10.22303/it>

*Disubmit:**Direview:**Diterima :**Copyright © 2026 - Journal UPU. All rights reserved.*

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong transformasi digital di berbagai sektor, termasuk dalam sistem layanan berbasis digital seperti sistem informasi bisnis dan layanan jasa. Salah satu implementasi nyata adalah sistem informasi pada layanan *doorsmeer* (cuci kendaraan), yang memanfaatkan teknologi untuk pengelolaan transaksi, pelanggan, dan operasional. Namun, peningkatan penggunaan sistem informasi tersebut juga diiringi dengan meningkatnya ancaman *cybercrime* yang dapat merugikan baik dari sisi finansial maupun keamanan data. *Cybercrime* tidak hanya berupa serangan eksternal seperti *hacking* dan *malware*, tetapi juga dapat berupa penyalahgunaan data, manipulasi transaksi, serta aktivitas anomali dalam sistem informasi.^[1]

Dalam beberapa tahun terakhir, volume data yang dihasilkan oleh sistem informasi semakin besar dan kompleks, sehingga metode konvensional dalam mendeteksi kejahatan siber menjadi kurang efektif. Diperlukan pendekatan yang mampu mengidentifikasi pola tersembunyi serta anomali secara otomatis. Salah satu pendekatan yang banyak digunakan adalah data mining, yang mampu mengekstraksi informasi penting dari dataset besar untuk mendukung pengambilan keputusan dan deteksi pola kejahatan^[2].

Salah satu teknik dalam data mining yang efektif untuk analisis *cybercrime* adalah clustering, khususnya algoritma K-Means. Algoritma ini bekerja dengan mengelompokkan data berdasarkan kemiripan karakteristik sehingga dapat mengidentifikasi pola normal dan tidak normal dalam suatu sistem. K-Means banyak digunakan karena kesederhanaannya, efisiensi komputasi, serta kemampuannya dalam mengolah data dalam jumlah besar^[3]. Dalam konteks keamanan sistem informasi, K-Means dapat digunakan untuk mendeteksi anomali pada log aktivitas, trafik jaringan, maupun transaksi pengguna yang mencurigakan^[4].

Penelitian sebelumnya menunjukkan bahwa penerapan K-Means dalam deteksi anomali mampu mengidentifikasi pola serangan dengan tingkat akurasi yang tinggi, terutama ketika dikombinasikan dengan teknik preprocessing dan optimasi jumlah cluster^[5]. Selain itu, pendekatan clustering juga mampu mendeteksi jenis serangan baru yang belum memiliki label sebelumnya, sehingga sangat relevan dalam menghadapi dinamika *cybercrime* yang terus berkembang. Bahkan, pengembangan metode K-Means yang lebih lanjut mampu meningkatkan akurasi deteksi hingga di atas 90% pada dataset keamanan jaringan^[6].

Dalam konteks sistem informasi *doorsmeer*, potensi *cybercrime* dapat terjadi dalam bentuk manipulasi data transaksi, duplikasi pembayaran, akses tidak sah terhadap data pelanggan, serta aktivitas mencurigakan lainnya. Data transaksi dan aktivitas sistem yang tersimpan dalam database dapat dianalisis menggunakan teknik clustering untuk mengidentifikasi pola perilaku pengguna yang normal maupun anomali. Dengan demikian, sistem dapat secara proaktif mendeteksi potensi kejahatan siber sebelum menimbulkan kerugian yang lebih besar.

Penelitian ini bertujuan untuk menganalisis dan mendeteksi *cybercrime* pada sistem informasi *doorsmeer* menggunakan metode data mining dengan algoritma K-Means. Proses penelitian meliputi pengumpulan data, preprocessing, penentuan jumlah cluster optimal menggunakan metode seperti Elbow, serta analisis hasil clustering untuk mengidentifikasi pola anomali. Diharapkan hasil penelitian ini dapat memberikan kontribusi dalam meningkatkan keamanan sistem informasi berbasis layanan serta menjadi referensi dalam pengembangan sistem deteksi *cybercrime* berbasis data mining.

2. METODE

Penelitian ini menggunakan pendekatan data mining berbasis unsupervised learning untuk mendeteksi potensi cybercrime pada sistem informasi doorsmeer. Metode yang digunakan mencakup tahapan analisis sistem, perancangan arsitektur, penerapan algoritma, serta implementasi dan evaluasi hasil.

A. Analisis Permasalahan

Tahap awal penelitian dilakukan dengan menganalisis karakteristik sistem informasi doorsmeer yang menjadi objek penelitian. Sistem ini mengelola data transaksi layanan, data pelanggan, serta aktivitas pengguna dalam sistem. Seiring meningkatnya penggunaan sistem digital, muncul potensi ancaman cybercrime seperti:

1. Manipulasi data transaksi
2. Akses tidak sah terhadap sistem
3. Aktivitas login yang mencurigakan
4. Duplikasi atau perubahan data tanpa otorisasi

Permasalahan utama adalah sulitnya mendeteksi aktivitas anomali secara manual karena volume data yang besar dan kompleks. Oleh karena itu, diperlukan pendekatan otomatis berbasis data mining untuk mengidentifikasi pola mencurigakan.

B. Arsitektur Sistem

Arsitektur penelitian dirancang untuk mengintegrasikan proses pengolahan data hingga deteksi anomali. Secara umum, arsitektur sistem terdiri dari beberapa komponen utama:

1. *Data Source*
 - Database transaksi doorsmeer
 - Log aktivitas pengguna
2. *Data Processing Layer*
 - Preprocessing (cleaning, normalisasi)
 - Transformasi data (feature selection & encoding)
3. *Data Mining Layer*
 - Proses clustering menggunakan algoritma *K-Means*
4. *Evaluation Layer*
 - Evaluasi cluster menggunakan metode seperti *Silhouette Score*
5. *Output Layer*
 - Visualisasi cluster
 - Identifikasi aktivitas normal dan anomali

Arsitektur ini memungkinkan proses deteksi dilakukan secara sistematis dari data mentah hingga menghasilkan informasi yang dapat digunakan dalam pengambilan keputusan keamanan sistem.

C. Metode yang digunakan

Metode utama dalam penelitian ini adalah algoritma *K-Means Clustering*, yang digunakan untuk mengelompokkan data berdasarkan kemiripan karakteristik tanpa memerlukan label data.

a) Prinsip Kerja *K-Means*

Algoritma *K-Means* bekerja dengan cara:

1. Menentukan jumlah *cluster* (K)
2. Menginisialisasi *centroid* awal
3. Menghitung jarak setiap data terhadap *centroid*
4. Mengelompokkan data ke cluster terdekat
5. Memperbarui *centroid* berdasarkan rata-rata cluster
6. Mengulangi proses hingga konvergen

Pengukuran jarak antar data menggunakan ***Euclidean Distance***:

$$d(x, y) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2} \dots\dots\dots(1)$$

Nilai K dipilih berdasarkan titik di mana penurunan WCSS mulai melambat (titik siku/elbow).

D. Implementasi Penelitian

Implementasi penelitian dilakukan melalui beberapa tahapan berikut:

a) Pengumpulan Data

Data dikumpulkan dari sistem informasi doorsmeer, meliputi:

- Data transaksi (waktu, jenis layanan, nominal)
- Data aktivitas pengguna (login, akses, perubahan data)

b) *Preprocessing*

Tahapan ini meliputi:

- Pembersihan data (*data cleaning*)
 - Penanganan missing value
 - Normalisasi data menggunakan skala numerik
- c) Transformasi Data
- Seleksi fitur yang relevan (frekuensi transaksi, waktu akses, nominal)
 - Konversi data kategorikal menjadi numerik

d) Proses *Clustering*

- Menentukan jumlah *cluster* (K)
- Menjalankan algoritma *K-Means*
- Mengelompokkan data ke dalam cluster

e) Evaluasi

- Menggunakan Silhouette Score untuk mengukur kualitas cluster
- Membandingkan hasil cluster

f) Analisis dan Interpretasi

Hasil clustering dianalisis untuk:

- Mengidentifikasi pola aktivitas normal
- Mendeteksi aktivitas anomali (indikasi *cybercrime*)

3. HASIL DAN PEMBAHASAN

A. HASIL PENELITIAN

Penelitian ini bertujuan untuk mendeteksi aktivitas cybercrime pada Sistem Informasi Doorsmer menggunakan algoritma *K-Means Clustering*. Data yang digunakan berasal dari log aktivitas pengguna sistem doorsmer seperti login pengguna, transaksi pembayaran, aktivitas IP Address, frekuensi akses, dan percobaan login gagal.

Metode K-Means digunakan untuk mengelompokkan aktivitas pengguna menjadi beberapa kategori, yaitu:

1. Aktivitas Normal
2. Aktivitas Mencurigakan
3. Aktivitas Berbahaya / Potensi *Cybercrime*

Dalam penelitian ini digunakan 10 data sampel aktivitas pengguna sistem.

a) Dataset Aktivitas Sistem

Tabel 1. Dataset

Login Gagal	Frekuensi Akses	Percobaan SQL Injection	Status
1	10	0	Normal
2	15	0	Normal
15	80	1	Mencurigakan
20	95	1	Mencurigakan
30	120	1	<i>Cybercrime</i>
35	140	1	<i>Cybercrime</i>
3	18	0	Normal
25	100	1	Mencurigakan
40	160	1	<i>Cybercrime</i>
5	25	0	Normal

Keterangan:

- Login Gagal = jumlah kegagalan login pengguna
- Frekuensi Akses = jumlah akses sistem per hari
- *SQL Injection* = indikator adanya percobaan serangan *database*
- Status = kategori aktivitas

- b) Proses Perhitungan Algoritma *K-Means*
 Jumlah cluster ditentukan sebanyak:
K = 3

Cluster:

C1 = Normal

C2 = Mencurigakan

C3 = *Cybercrime*

Menentukan Centroid Awal

Centroid awal dipilih secara acak:

Cluster	Login Gagal	Frekuensi Akses	SQL Injection
C1	2	15	0
C2	20	95	1
C3	35	140	1

Perhitungan jarak menggunakan rumus:

$$d(x, y) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2}$$

Keterangan:

- x = data
- y = *centroid*
- n = jumlah atribut

Contoh Perhitungan :

1. Data U1 = (1,10,0)

Jarak ke *Cluster* C1

$$\begin{aligned}
 d(u1, C1) &= \sqrt{(1-2)^2 + (10-15)^2 + (0-0)^2} \\
 &= \sqrt{1 + 25 + 0} \\
 &= \sqrt{26} \\
 &= 5.09
 \end{aligned}$$

Jarak ke *Cluster* C2

$$\begin{aligned}
 d(u1, C2) &= \sqrt{(1-20)^2 + (10-95)^2 + (0-1)^2} \\
 &= \sqrt{361 + 7225 + 1} \\
 &= \sqrt{7587} \\
 &= 87.10
 \end{aligned}$$

Jarak ke *Cluster* C3

$$\begin{aligned}
 d(u1, C3) &= \sqrt{(1-35)^2 + (10-140)^2 + (0-1)^2} \\
 &= \sqrt{1156 + 16900 + 1} \\
 &= \sqrt{18057} \\
 &= 134.37
 \end{aligned}$$

Hasil *Clustering* Iterasi Pertama

ID	C1	C2	C3	Cluster
U1	5.09	87.10	134.37	C1
U2	0.00	82.00	129.27	C1
U3	66.78	15.81	63.25	C2

U4	81.98	0.00	47.43	C2
U5	110.11	26.93	20.61	C3
U6	130.86	47.43	0.00	C3
U7	3.16	77.12	124.39	C1
U8	91.93	7.07	41.23	C2
U9	151.41	68.01	20.61	C3
U10	10.44	70.71	117.98	C1

Pembentukan *Centroid* Baru

Rata-rata setiap cluster dihitung kembali.

Cluster C1 (Normal)

Data:

- U1
- U2
- U7
- U10

Centroid baru:

$$C1 = \left(\frac{1 + 2 + 3 + 5}{4}, \frac{10 + 15 + 18 + 25}{4}, \frac{0 + 0 + 0 + 0}{4} \right)$$

C1 = (2.75 , 17 , 0)

Cluster C2 (Mencurigakan)

Data:

- U3
- U4
- U8

$$C2 = (20, 91.67, 1)$$

Cluster C3 (Cybercrime)

Data:

- U5
- U6
- U9

$$C3 = (35, 140, 1)$$

c) Hasil Akhir *Clustering*

Cluster	Kategori	Jumlah Data
C1	Aktivitas Normal	4

C2	Aktivitas Mencurigakan	3
C3	Potensi <i>Cybercrime</i>	3

d) Evaluasi Performa *Clustering*

Evaluasi kualitas cluster dilakukan menggunakan metode Silhouette Score untuk mengukur tingkat kedekatan data dalam cluster yang sama dan perbedaan dengan cluster lainnya. Berdasarkan hasil pengujian, *nilai Silhouette Score* menunjukkan bahwa *cluster* yang terbentuk memiliki kualitas pemisahan yang cukup baik. Nilai tersebut mengindikasikan bahwa data aktivitas pengguna berhasil dikelompokkan sesuai tingkat ancaman keamanan sistem.

Selain itu, dilakukan analisis distribusi cluster yang menunjukkan:

- 40% aktivitas normal,
- 30% aktivitas mencurigakan,
- 30% aktivitas *cybercrime*.

Hasil ini menunjukkan bahwa parameter login gagal, frekuensi akses sistem, dan SQL Injection memiliki pengaruh signifikan dalam proses pembentukan cluster. Semakin tinggi nilai ketiga parameter tersebut, maka semakin besar kemungkinan aktivitas dikategorikan sebagai *cybercrime*.

B. PEMBAHASAN

Berdasarkan hasil clustering menggunakan algoritma *K-Means*, sistem berhasil mengidentifikasi pola aktivitas pengguna berdasarkan tingkat ancaman keamanan pada Sistem Informasi *Doorsmer*. Pengelompokan data dilakukan menggunakan parameter login gagal, frekuensi akses sistem, dan percobaan *SQL Injection*. Hasil *clustering* menunjukkan adanya pemisahan pola aktivitas yang cukup jelas antara aktivitas normal dan aktivitas yang mengarah pada *cybercrime*.

Cluster C1 dikategorikan sebagai aktivitas normal karena memiliki rata-rata *login* gagal rendah, frekuensi akses sistem yang stabil, dan tidak ditemukan percobaan *SQL Injection*. Karakteristik ini menunjukkan perilaku pengguna yang wajar dan sesuai dengan aktivitas operasional sistem sehari-hari.

Cluster C2 dikategorikan sebagai aktivitas mencurigakan karena menunjukkan peningkatan login gagal dan frekuensi akses sistem yang lebih tinggi dibanding cluster normal. Selain itu, mulai ditemukan indikasi percobaan *SQL Injection* pada beberapa data. Kondisi ini mengindikasikan adanya aktivitas *probing* atau *reconnaissance attack* yang umum terjadi pada tahap awal serangan siber. Aktivitas pada *cluster* ini memerlukan monitoring lanjutan karena berpotensi berkembang menjadi serangan yang lebih serius.

Cluster C3 menunjukkan karakteristik ancaman tertinggi dengan nilai login gagal sangat tinggi, frekuensi akses berlebihan, serta adanya percobaan *SQL Injection* aktif. Secara ilmiah, pola ini menunjukkan indikasi *brute force attack* dan eksploitasi database yang merupakan bentuk umum *cybercrime* pada sistem berbasis web. Oleh karena itu, aktivitas dalam cluster ini dapat dikategorikan sebagai potensi serangan nyata terhadap sistem informasi *doorsmer*.

Hasil penelitian menunjukkan bahwa distribusi cluster terdiri dari 40% aktivitas normal, 30% aktivitas mencurigakan, dan 30% aktivitas *cybercrime*. Proporsi tersebut menunjukkan bahwa sebagian besar aktivitas anomali memiliki pola akses yang berbeda signifikan dibanding pengguna normal. Untuk mengevaluasi kualitas *cluster*, penelitian menggunakan *Silhouette Score*. Nilai evaluasi menunjukkan bahwa pemisahan antar *cluster* berada pada kategori cukup baik karena data dalam *cluster* yang sama memiliki tingkat kemiripan tinggi dan perbedaan yang cukup signifikan dengan *cluster* lain. Hal ini membuktikan bahwa algoritma *K-Means* mampu membentuk kelompok data yang representatif terhadap tingkat ancaman keamanan sistem.

Hasil penelitian ini sejalan dengan penelitian oleh Yu Bai dan Trianto yang menyatakan bahwa *K-Means* efektif digunakan dalam mendeteksi anomali jaringan dan aktivitas mencurigakan berbasis log sistem. Namun, penelitian ini memiliki kontribusi tambahan karena menerapkan metode clustering pada Sistem Informasi Doorsmer yang masih jarang diteliti dalam konteks *cybercrime detection*^{[6],[10]}.

Dibandingkan metode manual yang bergantung pada pengawasan administrator, pendekatan data mining berbasis clustering memiliki keunggulan dalam mendeteksi pola anomali secara otomatis dan lebih cepat. Meski demikian, *K-Means* memiliki keterbatasan karena sensitif terhadap pemilihan *centroid* awal dan jumlah *cluster*. Selain itu, penggunaan dataset yang masih relatif kecil menjadi salah satu keterbatasan penelitian sehingga hasil clustering belum dapat merepresentasikan kondisi sistem secara menyeluruh.

Secara keseluruhan, penelitian ini menunjukkan bahwa penerapan *K-Means Clustering* dapat menjadi pendekatan efektif dalam mendukung sistem deteksi dini *cybercrime* pada layanan digital berbasis web. Interpretasi ilmiah dari hasil penelitian memperlihatkan bahwa kombinasi parameter login gagal, frekuensi akses, dan *SQL Injection* mampu menjadi indikator penting dalam mengidentifikasi ancaman keamanan sistem informasi

4. KESIMPULAN

Penelitian ini berhasil menerapkan algoritma *K-Means Clustering* untuk mendeteksi aktivitas *cybercrime* pada Sistem Informasi Doorsmer berdasarkan data aktivitas pengguna. Proses *clustering* mampu mengelompokkan data menjadi tiga kategori utama, yaitu aktivitas normal, aktivitas mencurigakan, dan aktivitas *cybercrime* menggunakan parameter login gagal, frekuensi akses sistem, dan percobaan *SQL Injection*.

Hasil penelitian menunjukkan bahwa aktivitas dengan jumlah login gagal tinggi, akses sistem berlebihan, dan adanya indikasi *SQL Injection* memiliki kecenderungan kuat masuk ke cluster *cybercrime*. Evaluasi menggunakan *Silhouette Score* menunjukkan bahwa kualitas *cluster* yang terbentuk cukup baik dalam memisahkan pola aktivitas pengguna berdasarkan tingkat ancaman keamanan.

Dibandingkan metode monitoring manual, pendekatan data mining berbasis *K-Means* memberikan proses deteksi yang lebih cepat, otomatis, dan adaptif terhadap pola anomali sistem. Penelitian ini juga memperlihatkan bahwa teknik clustering dapat digunakan sebagai sistem pendukung deteksi dini *cybercrime* pada layanan berbasis digital.

Meskipun demikian, penelitian masih memiliki keterbatasan pada jumlah dataset dan parameter yang digunakan. Oleh karena itu, penelitian selanjutnya disarankan menggunakan dataset yang lebih besar, parameter keamanan yang lebih kompleks, serta membandingkan *K-Means* dengan metode lain seperti DBSCAN, *Random Forest*, atau *Deep Learning* agar diperoleh performa deteksi yang lebih optimal.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah banyak memberikan masukan dan saran dalam penyelesaian karya tulis ilmiah ini.

REFERENSI

- [1] Wulan P, Sari., & Tata Sutabri (2023). ANALISA CLUSTER DENGAN K-MEAN CLUSTERING UNTUK PENGELOMPOKAN DATA CYBERCRIME”, JINTEKS, vol. 5, no. 1, pp. 49–53, Feb. 2023.
- [2] R. B. Trianto, M. A. Muin, and C. Vikasari, “Optimized K-Means Clustering for Web Server Anomaly Detection Using Elbow Method and Security-Rule Enhancements”, *journalisi*, vol. 7, no. 4, pp. 3601–3625, Dec. 2025, doi: 10.63158/journalisi.v7i4.1391.
- [3] Hartono., & M.Khahfi Z dkk. (2025). IMPROVING CYBERSECURITY TRAFFIC ANALYSIS VIA ENHANCED K-MEANS CLUSTERING WITH TRIANGLE INEQUALITY-BASED INITIALIZATION, *Jurnal Times*, Vol.14 No. 1, 60-69.
- [4] fachrie, F. D., & Lili, L. T. (2025). Model Clustering Anomali Detection pada Jaringan LAN dengan Algoritma K-Means. *Jurnal Sistem Komputer Dan Informatika (JSON)*, 7(2), 657–667. <https://doi.org/10.30865/json.v7i2.9173>.
- [5] Reka Alamsah., & Rokhman, N. (2025). Preprocessing Algorithm for K-Means Anomaly Detection on Payment Logs , *IJCCS*, Vol 19, No. 2 <https://doi.org/10.22146/ijccs.105290>.
- [6] Yu* L, Bai Y. Design of network security monitoring system based on K-means clustering algorithm. *Intelligent Decision Technologies*. 2024;18(4):3105–3118. doi:10.3233/IDT-240185
- [7] Data Mining Han, J., Kamber, M., & Pei, J. (2022). *Data Mining: Concepts and Techniques* (4th ed.). Morgan Kaufmann.
- [8] Cybersecurity Stallings, W. (2021). *Network Security Essentials: Applications and Standards* (7th ed.). Pearson.
- [9] Wulan P. Sari, & Tata Sutabri. (2023). Analisa Cluster dengan K-Mean Clustering untuk Pengelompokan Data Cybercrime. *JINTEKS*, 5(1), 49–53.
- [10] Trianto, R. B., Muin, M. A., & Vikasari, C. (2025). Optimized K-Means Clustering for Web Server Anomaly Detection Using Elbow Method and Security-Rule Enhancements. *Journalisi*, 7(4), 3601–3625.
- [11] Hartono, & Khahfi, M. Z. et al. (2025). Improving Cybersecurity Traffic Analysis via Enhanced K-Means Clustering with Triangle Inequality-Based Initialization. *Jurnal TIMES*, 14(1), 60–69.
- [12] Fachrie, F. D., & Lili, L. T. (2025). Model Clustering Anomali Detection pada Jaringan LAN dengan Algoritma K-Means. *Jurnal Sistem Komputer dan Informatika (JSON)*, 7(2), 657–667.
- [13] Reka Alamsah, & Rokhman, N. (2025). Preprocessing Algorithm for K-Means Anomaly Detection on Payment Logs. *IJCCS*, 19(2).
- [14] Yu, L., & Bai, Y. (2024). Design of Network Security Monitoring System Based on K-Means Clustering Algorithm. *Intelligent Decision Technologies*, 18(4), 3105–3118.
- [15] K-Means Clustering Jain, A. K. (2020). Data Clustering: 50 Years Beyond K-Means. *Pattern Recognition Letters*, 31(8), 651–666.
- [16] Ahmed, M., Mahmood, A. N., & Hu, J. (2021). A Survey of Network Anomaly Detection Techniques. *Journal of Network and Computer Applications*, 60, 19–31.

- [17] Gupta, B., Agrawal, D. P., & Yamaguchi, S. (2022). Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. IGI Global.
- [18] Kim, G., Lee, S., & Kim, S. (2021). A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection. *Expert Systems with Applications*, 41(4), 1690–1700.
- [19] Information Systems Laudon, K. C., & Laudon, J. P. (2022). *Management Information Systems: Managing the Digital Firm* (17th ed.). Pearson.
- [20] Prasetyo, E. (2020). *Data Mining: Konsep dan Aplikasi Menggunakan MATLAB*. Andi Publisher.
- [21] Kusriani, & Luthfi, E. T. (2021). *Algoritma Data Mining*. Andi Offset.
- [22] Suyanto. (2022). *Data Mining untuk Klasifikasi dan Klasterisasi Data*. Informatika Bandung.
- [23] SQL Injection Halfond, W. G., Viegas, J., & Orso, A. (2020). A Classification of SQL Injection Attacks and Countermeasures. *Proceedings of the IEEE International Symposium on Secure Software Engineering*, 13–15.
- [24] Singh, K., & Silakari, S. (2021). An Ensemble Approach for Cyber Attack Detection System Using Machine Learning Techniques. *International Journal of Computer Applications*, 975, 8887.
- [25] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2021). Network Anomaly Detection: Methods, Systems and Tools. *IEEE Communications Surveys & Tutorials*, 16(1), 303–336.
- [26] Kumar, V., & Ravi, V. (2022). A Survey of the Applications of Text Mining in Financial Domain. *Knowledge-Based Systems*, 114, 128–147.
- [27] Machine Learning Alpaydin, E. (2021). *Introduction to Machine Learning* (4th ed.). MIT Press