

INTEGRASI AUDIT *TRAIL* DAN TEKNIK *CLUSTERING* UNTUK SEGMENTASI DAN KATEGORISASI AKTIVITAS LOG

Candra Heru Saputra^{*1}, Suhirman²

^{1,2}Universitas Teknologi Yogyakarta, Yogyakarta
Email: ¹CandraHeru.6230211005@student.uty.ac.id, ²suhirman@uty.ac.id
^{*}Penulis Korespondensi

(Naskah masuk: 20 November 2023, diterima untuk diterbitkan: 15 Januari 2024)

Abstrak

Dengan berkembangnya teknologi, organisasi dan perusahaan kini mengumpulkan data dalam jumlah yang sangat besar, yang tercatat dalam log sistem untuk tujuan audit keamanan, pemantauan, dan investigasi forensik. Namun, tantangan utama muncul saat analisis keamanan harus menangani volume data log yang besar, yang seringkali membuat sulit untuk mengidentifikasi aktivitas mencurigakan atau abnormal. Dalam upaya mengatasi tantangan analisis log yang berskala besar dalam sistem informasi, penelitian ini bertujuan untuk mengintegrasikan teknik audit *trail* dengan metode *clustering*, khususnya menggunakan *K-Means*, untuk segmentasi dan kategorisasi aktivitas log. Penelitian ini mencari pendekatan yang dapat meningkatkan efisiensi dalam menelusuri dan menganalisis log aktivitas dengan mengelompokkan data log yang serupa. Metode yang digunakan mencakup desain eksperimental, pengumpulan data audit *trail* yang komprehensif, preprocessing data, implementasi algoritma *K-Means*, dan evaluasi hasil *clustering*. Hasil penelitian mengindikasikan bahwa penerapan *K-Means* pada audit *trail* memungkinkan identifikasi pola aktivitas yang signifikan, memudahkan deteksi anomali dengan cepat, dan menyederhanakan proses audit keamanan data, yang mengarah pada pemahaman yang lebih baik dalam pengelolaan risiko keamanan informasi.

Kata kunci: Audit Trail, Clustering, K-Means, Analisis Log

INTEGRATION OF AUDIT TRAIL AND CLUSTERING TECHNIQUES FOR SEGMENTATION AND CATEGORIZATION OF LOG ACTIVITIES

Abstract

With the advancement of technology, organizations and companies are now accumulating a vast amount of data, which is recorded in system logs for security auditing, monitoring, and forensic investigation purposes. However, a major challenge arises when security analysts have to deal with large volumes of log data, often making it difficult to identify suspicious or abnormal activities. In an effort to overcome the challenges of large-scale log analysis in information systems, this study aims to integrate audit trail techniques with clustering methods, specifically using *K-Means*, for segmentation and categorization of log activities. This research seeks an approach to enhance efficiency in tracing and analyzing activity logs by grouping similar log data. The methods employed include experimental design, comprehensive collection of audit trail data, data preprocessing, implementation of the *K-Means* algorithm, and evaluation of the clustering results. The findings indicate that the application of *K-Means* to audit trails enables the identification of significant activity patterns, facilitates rapid anomaly detection, and simplifies the data security audit process, leading to a better understanding of information security risk management.

Keywords: Audit Trail, Clustering, K-Means, Log Analysis

1. PENDAHULUAN

Di era digital saat ini, pengelolaan log aktivitas sistem menjadi komponen krusial dalam memastikan keamanan dan integritas data. Organisasi dan perusahaan menghasilkan jumlah data yang sangat besar setiap hari, yang dicatat dalam log sistem untuk audit keamanan, pemantauan, dan analisis forensik.

Chen et al. (2022) menyatakan bahwa log ini telah berkembang menjadi aset krusial dalam menjamin keandalan dan kesinambungan berbagai sistem perangkat lunak.

Log adalah elemen penting dalam sistem bisnis korporat masa kini, memberikan berbagai keuntungan seperti transparansi dan integritas data, serta melindungi informasi sensitif dengan

menyediakan struktur pendukung berupa bukti informasi (Regueiro et al., 2021).

Audit *trail*, yang terdiri dari catatan rinci tentang berbagai kegiatan yang terjadi dalam sistem, memiliki peranan krusial dalam memastikan kemungkinan pelacakan dan pemeriksaan atas setiap kejadian di dalam sistem. Hal ini sejalan dengan peraturan pemerintah Indonesia, seperti PP No. 71 tahun 2019 tentang penyelenggaraan sistem dan transaksi elektronik, serta POJK No. 38/POJK.03/2016 tentang penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum, yang keduanya menyoroti pentingnya audit *trail* dalam pengelolaan dan operasional sistem informasi.

Audit *trail* juga memberikan sumbangan yang signifikan pada audit keuangan di sektor perbankan. Fungsi audit *trail* tidak hanya terbatas pada validasi sumber dari entri keuangan atau transaksi perdagangan, tetapi juga berperan sebagai pelindung bagi bisnis dari tanggung jawab hukum, membantu dalam pemantauan data untuk mengidentifikasi pelanggaran keamanan, memastikan penerapan protokol yang tepat, dan menjadi bukti kepatuhan (Bana, 2020).

Namun, ketika menghadapi volume data log yang sangat besar, analis keamanan sering kali mengalami kesulitan dalam mengidentifikasi perilaku yang tidak biasa atau mencurigakan. Situasi ini menjadi tantangan karena data yang berlimpah dapat menyembunyikan indikasi adanya gangguan keamanan atau aktivitas ilegal. Perilaku yang tidak biasa ini penting untuk dikenali karena mereka bisa menjadi tanda-tanda dari masalah keamanan yang serius, seperti pelanggaran data atau serangan siber.

Menanggapi tantangan ini, penelitian ini dirancang untuk mengembangkan sebuah metodologi baru dengan menggabungkan teknik *clustering*, khususnya algoritma *K-Means*, ke dalam sistem audit *trail*. Algoritma *K-Means* merupakan salah satu metode *clustering* yang paling populer dan sering digunakan dalam berbagai studi dan aplikasi (Henriques et al., 2020; Istianto & Uyun, 2021; Sinaga & Yang, 2020). *Clustering* sendiri merupakan sebuah teknologi pembelajaran mesin tanpa pengawasan yang mengelompokkan data berdasarkan tingkat kemiripannya, seperti diuraikan oleh Zhang et al. (2023) dan Rodriguez et al. (2019).

Tujuan penelitian ini adalah untuk menciptakan proses yang lebih efisien dalam menganalisis log aktivitas yang besar, dengan mengelompokkan data berdasarkan kesamaan karakteristiknya, sehingga memudahkan pemahaman yang lebih baik tentang perilaku dalam sistem dan memungkinkan deteksi anomali dengan lebih cepat.

Selain itu, tujuan lain dari penelitian ini adalah untuk mengeksplorasi bagaimana teknik *clustering* dapat diaplikasikan dalam konteks keamanan siber untuk mempercepat proses identifikasi insiden. Dengan membedakan antara aktivitas normal dan

mencurigakan melalui pola yang dihasilkan oleh *clustering*, organisasi dapat lebih cepat merespons potensi ancaman keamanan. Hal ini sangat penting dalam lingkungan bisnis saat ini di mana waktu untuk mendeteksi dan merespons insiden keamanan dapat memiliki dampak signifikan terhadap kerugian finansial dan reputasi.

Manfaat praktis dari penelitian ini terletak pada potensinya untuk meningkatkan proses audit internal perusahaan. Dengan mengaplikasikan hasil penelitian dalam sistem audit *trail*, analis keamanan dapat mengurangi waktu yang diperlukan untuk menyaring dan menganalisis log aktivitas. Sehingga sumber daya dapat dialihkan dari tugas-tugas rutin dan repetitif untuk fokus pada kegiatan yang memerlukan penilaian manusia dan analisis yang lebih mendalam.

Dari segi teoritis, penelitian ini bertujuan untuk memberikan sumbangan kepada korpus literatur di bidang data mining dan keamanan informasi. Selain itu penelitian ini diharapkan dapat menjadi dasar bagi pengembangan teknologi audit *trail* dan sistem pemantauan keamanan informasi yang lebih canggih. Dengan memahami lebih dalam tentang bagaimana *clustering* dapat diintegrasikan dalam audit *trail*, *programmer* dapat merancang alat dan sistem yang lebih adaptif dan responsif terhadap ancaman keamanan yang terus berkembang, memberikan landasan untuk inovasi teknologi ke depannya.

2. METODE PENELITIAN

Penelitian ini dirancang untuk menjawab tantangan dalam analisis log aktivitas dalam sistem informasi dengan menerapkan algoritma *clustering*. Dalam rangka menjaga kerahasiaan dan integritas data, penelitian ini menggunakan data log yang disintesis berdasarkan kejadian nyata. Data sintesis ini dibuat untuk merefleksikan karakteristik dan pola yang serupa dengan apa yang dapat ditemukan dalam log aktivitas sebenarnya, namun tanpa mengandung informasi yang sensitif atau pribadi.

Proses pembuatan data sintesis ini melibatkan pengembangan skenario yang realistis berdasarkan log aktivitas dari berbagai sistem informasi yang sudah ada. Setiap skenario dibuat dengan mempertimbangkan berbagai variabel, seperti jenis aktivitas, frekuensi, volume, dan pola yang dapat menandai perilaku normal atau anomali. Dengan pendekatan ini, data yang dihasilkan menyediakan dasar yang kokoh untuk eksperimen tanpa mengorbankan kerahasiaan data aktual.

Setelah pembuatan data sintesis selesai, langkah berikutnya adalah *preprocessing*. Proses ini meliputi normalisasi, transformasi, dan pembersihan data, yang bertujuan untuk memastikan bahwa setiap entri log siap untuk analisis dan bebas dari *distorsi* yang dapat mempengaruhi hasil *clustering*. Langkah ini penting karena kualitas data input secara langsung mempengaruhi validitas output *clustering*.

Setelah memastikan bahwa *preprocessing* data telah dilakukan dengan baik, fokus selanjutnya adalah

pemilihan algoritma *clustering* yang tepat. Dalam penelitian ini, algoritma *K-Means* menjadi pilihan yang cocok karena memiliki tingkat efektivitas dan efisiensi yang tinggi dalam mengelompokkan dataset besar menjadi beberapa kelompok berdasarkan kedekatan fitur-fiturnya (Ali et al., 2022). Algoritma *K-Means* ini bekerja dengan cara menginisiasi k buah *centroid* (pusat kluster), kemudian mengalokasikan setiap titik data ke *centroid* terdekat berdasarkan jarak. Proses ini diulangi secara iteratif hingga posisi *centroid* stabil dan tidak mengalami perubahan yang signifikan.

Rumus yang digunakan dalam *K-Means* untuk mengukur jarak antara titik data dan *centroid* adalah *Euclidean Distance*, sebagaimana yang ditampilkan pada rumus (1) berikut:

$$d(p, q) = \sqrt{\sum_{k=1}^n (p_k - q_k)^2} \quad (1)$$

dimana p dan q masing-masing merupakan titik data dan *centroid*, dan n adalah jumlah dimensi. Dengan menggunakan *Euclidean Distance*, *K-Means* mampu mengidentifikasi kluster berdasarkan kedekatan spasial, yang menjadikannya metode yang baik untuk banyak skenario analisis data

Penentuan jumlah *centroid* atau *cluster* yang optimal merupakan salah satu aspek penting dalam eksperimen ini. Untuk tujuan ini, peneliti menggunakan metode *Elbow* dan analisis *Silhouette Score*. Hasil penelitian menunjukkan bahwa penerapan algoritma *K-Means* dengan optimasi *Elbow* dan *Silhouette* dapat menghasilkan *cluster* yang relevan (Lashiyanti et al., 2023; Sholeh & Aeni, 2023; Sutomo et al., 2023).

Proses evaluasi hasil *clustering* melibatkan pemeriksaan terhadap kohesi dan pemisahan antar-*cluster* untuk memastikan bahwa pengelompokan yang dihasilkan signifikan dan representatif terhadap pola dalam data log. Evaluasi ini juga menguji *robustness* dari model *clustering* dengan menerapkannya pada berbagai skenario data sintetis untuk menguji konsistensi hasil.

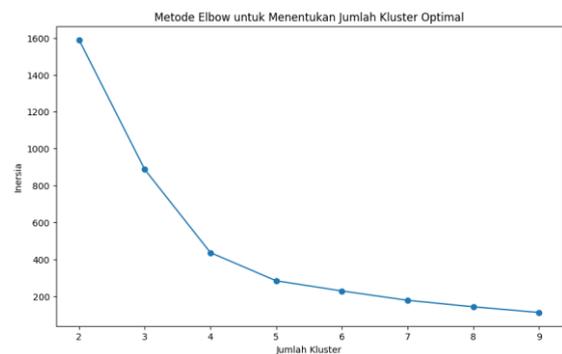
Teknik validasi eksternal, seperti perbandingan dengan insiden keamanan yang sudah diketahui, tidak diterapkan secara langsung mengingat sifat data sintetis. Sebagai gantinya, penelitian ini menggunakan simulasi berbasis skenario untuk memvalidasi hasil *clustering*, dengan asumsi bahwa skenario yang dikembangkan mencerminkan kejadian nyata dengan cukup akurat.

Seluruh proses dari pengembangan data sintetis hingga analisis hasil *clustering* diarahkan untuk menghasilkan rekomendasi yang praktis dan dapat diaplikasikan dalam pengaturan keamanan data nyata. Rekomendasi ini diharapkan dapat memberikan wawasan baru untuk pengembangan sistem audit *trail* dan meningkatkan keamanan informasi dengan memanfaatkan teknik data mining.

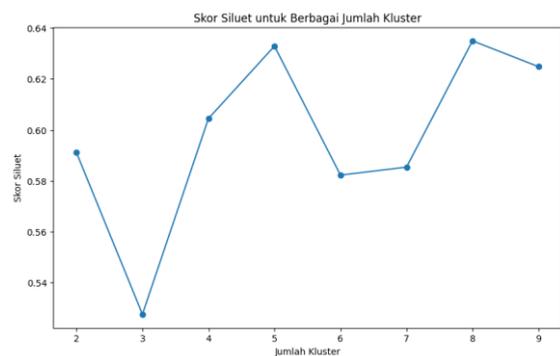
3. HASIL DAN PEMBAHASAN

Proses analisis dimulai dengan penentuan jumlah kluster optimal. Metode *Elbow* digunakan untuk mengestimasi jumlah kluster yang paling ideal dan cocok dengan dataset (Fabrianto et al., 2021). Berdasarkan grafik *Elbow* yang dapat dilihat pada Gambar 1, terlihat bahwa titik siku terindikasi pada kisaran 4 hingga 5 kluster, di mana penurunan inerti mulai stabil dan kurva mereda. Namun, untuk memperoleh validasi tambahan, dilakukan pula analisis Skor *Silhouette*.

Skor *Silhouette* memberikan perspektif tentang sejauh mana data dipisahkan dalam pembentukan kluster. Hasil analisis pada Gambar 2 menunjukkan bahwa nilai Skor *Silhouette* tertinggi dicapai untuk jumlah kluster 5 dan 8, yang mengindikasikan pemisahan yang baik antar kluster dan kohesi dalam kluster. Dengan pertimbangan ini, dipilih jumlah kluster 5 sebagai jumlah kluster yang optimal untuk analisis lebih lanjut.



Gambar 1. Grafik *Elbow*



Gambar 2. Grafik Skor *Silhouette*

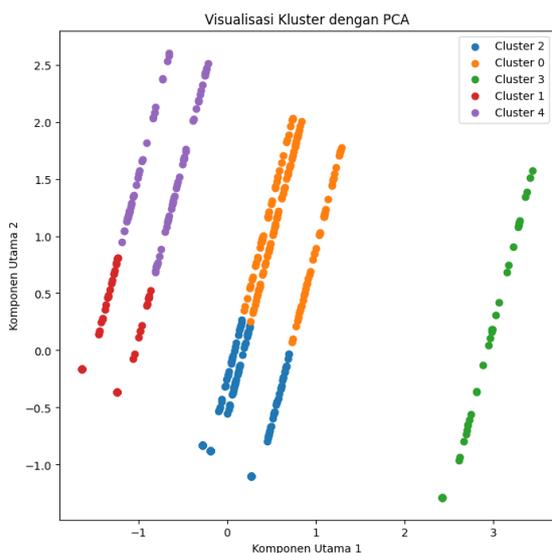
Setelah menentukan jumlah kluster optimal, algoritma *K-means* diterapkan pada data yang telah dinormalisasi. Hasil klusterisasi menunjukkan pembagian data ke dalam lima kluster yang berbeda, dengan karakteristik dan jumlah anggota kluster yang variatif. Proses ini mengungkapkan adanya variasi dalam pola aktivitas log, yang menunjukkan adanya beragam jenis transaksi dalam log sistem.

Visualisasi hasil kluster dengan menggunakan teknik PCA menyediakan representasi visual dari segmentasi kluster. Dalam ruang dua dimensi yang dihasilkan oleh PCA, kluster-kluster terlihat jelas

terpisah satu sama lain seperti pada Gambar 3. Komponen Utama 1 dan Komponen Utama 2 menangkap variabilitas terbesar dalam dataset dan memperlihatkan pemisahan antar kluster yang signifikan.

Dalam analisis, ditemukan bahwa beberapa kluster memiliki jumlah data yang sedikit. Ini menimbulkan pertanyaan tentang keberadaan aktivitas anomali atau outlier dalam sistem. Pembahasan mendalam tentang kluster ini mengungkapkan bahwa walaupun jumlahnya sedikit, kluster tersebut mungkin sangat signifikan, menunjukkan pola transaksi yang tidak umum yang bisa menjadi fokus untuk audit keamanan lebih lanjut.

Temuan dari analisis klusterisasi ini memberikan wawasan baru mengenai aktivitas log sistem. Potensi aplikasi hasil ini sangat luas, mulai dari peningkatan prosedur audit *trail* hingga peningkatan mekanisme deteksi penipuan. Hasil ini juga memberikan dasar untuk mengembangkan sistem pemantauan yang lebih cerdas yang dapat secara otomatis mengkategorikan dan menandai aktivitas yang mencurigakan.



Gambar 3. Grafik Visualisasi Kluster PCA

Hasil *clustering* menunjukkan bahwa aktivitas log yang disintesis dapat dikelompokkan menjadi *cluster* yang memiliki karakteristik internal yang kohesif dan terpisah dengan baik satu sama lain. Hal ini mengindikasikan bahwa model *clustering* mampu mendeteksi pola yang konsisten dalam data, yang merupakan indikator baik bahwa metode ini dapat diterapkan pada data nyata dengan efektivitas yang serupa.

Pembahasan lebih dalam mengungkapkan bahwa data sintetis, meskipun tidak mengandung informasi nyata, memang menyediakan wawasan yang berguna tentang kinerja algoritma *clustering* dalam konteks audit *trail*. Namun, penting untuk dicatat bahwa data sintetis mungkin tidak sepenuhnya menangkap semua nuansa dari perilaku pengguna

atau ancaman yang mungkin terjadi dalam lingkungan nyata.

Penelitian ini juga mengakui batasan penelitian dan menyediakan rekomendasi untuk penggunaan teknik ini dalam praktik. Salah satu batasan utama adalah ketergantungan pada keakuratan data sintetis dalam meniru perilaku log nyata. Oleh karena itu, di masa depan, kolaborasi dengan organisasi untuk mendapatkan akses ke log anonim atau semi-anonim dapat membantu dalam menguji metodologi ini dengan data yang lebih representatif.

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Penelitian ini telah berhasil mengembangkan dan menguji pendekatan integratif yang menggunakan algoritma *K-Means clustering* untuk memproses dan menganalisis audit *trail* dengan menggunakan data log sintetis. Berdasarkan hasil yang diperoleh, dapat diambil kesimpulan sebagai berikut:

- Algoritma *K-Means* berhasil diimplementasikan pada data log sintetis, dan proses *clustering* berhasil mengidentifikasi kelompok-kelompok aktivitas dengan karakteristik yang serupa. Hal ini menunjukkan bahwa *clustering* dapat menjadi alat yang efektif untuk mempermudah segmentasi dan kategorisasi dalam jumlah data yang besar.
- Pembuatan data sintetis yang mendekati kejadian nyata menunjukkan potensinya sebagai alternatif untuk penelitian yang tidak dapat mengakses data nyata karena batasan privasi atau keamanan.
- Evaluasi *cluster* menunjukkan bahwa algoritma *clustering* mampu mendeteksi pola dalam log aktivitas yang dapat menandakan perilaku normal atau anomali, membuka jalan untuk aplikasi dalam sistem deteksi ancaman.
- Hasil penelitian ini memberikan bukti awal yang mendukung potensi penerapan teknik data mining dalam keamanan informasi dan manajemen audit *trail*.

4.2. Saran

Berdasarkan temuan dan pembahasan dari penelitian ini, beberapa saran untuk penelitian selanjutnya serta untuk praktik keamanan informasi adalah sebagai berikut:

- Validasi dengan data sebenarnya
Untuk mengkonfirmasi efektivitas pendekatan ini, penelitian selanjutnya harus dilakukan dengan menggunakan data log nyata yang telah

- di-anonimisasi untuk memastikan privasi dan keamanan data.
- b. Pengujian dengan berbagai algoritma
Selain *K-Means*, algoritma *clustering* lain seperti DBSCAN atau algoritma berbasis hierarki dapat diuji untuk menentukan pendekatan mana yang paling efektif dalam berbagai skenario audit *trail*.
 - c. Penerapan pembelajaran mesin lanjutan
Penerapan teknik pembelajaran mesin yang lebih canggih, seperti pembelajaran mendalam (*deep learning*), dapat dijajaki untuk memahami apakah ini dapat lebih meningkatkan proses audit *trail*.
 - d. Pengembangan aplikasi analisis log
Terdapat peluang untuk mengembangkan aplikasi analisis log yang memanfaatkan hasil penelitian ini untuk mempermudah analisis keamanan dalam memantau dan menganalisis audit *trail*.
 - e. Peningkatan pada data sintesis
Kedepannya, penelitian bisa mencakup peningkatan proses pembuatan data sintesis untuk lebih mendekati kompleksitas dan variabilitas data log sebenarnya.

Kesimpulan dan saran yang dihasilkan dari penelitian ini diharapkan dapat memberikan nilai tambah bagi komunitas ilmiah dan praktisi dalam bidang keamanan informasi, serta menjadi dasar bagi inovasi lebih lanjut dalam teknologi audit trail dan analisis keamanan data.

DAFTAR PUSTAKA

- ALI, I., UR REHMAN, A., KHAN, D. M., KHAN, Z., SHAFIQ, M., & CHOI, J. G. (2022). Model Selection Using K-Means Clustering Algorithm for the Symmetrical Segmentation of Remote Sensing Datasets. *Symmetry*, *14*(6). <https://doi.org/10.3390/sym14061149>
- BANA, J. O. (2020). *Impact of Audit Trails on the Financial Audit of Nigerian Banking Sector*.
- CHEN, Z., LIU, J., GU, W., SU, Y., & LYU, M. R. (2022). *Experience Report: Deep Learning-based System Log Analysis for Anomaly Detection*. <http://arxiv.org/abs/2107.05908>
- FABRIANTO, L., RIZA, F., & FAIZAH, N. M. (2021). *Korelasi Antara Profil Dan Nilai Akademis Siswa Dengan Menggunakan Algoritma K-Means*. <https://doi.org/10.25126/Jtiik.202183034>
- HENRIQUES, J., CALDEIRA, F., CRUZ, T., & SIMÕES, P. (2020). Combining k-means and xgboost models for anomaly detection using log datasets. *Electronics (Switzerland)*, *9*(7), 1–17. <https://doi.org/10.3390/electronics9071164>
- ISTIANTO, Y., & UYUN, S. (2021). *Klasifikasi Kebutuhan Jumlah Produk Makanan Customer Menggunakan K-Means Clustering Dengan Optimasi Pusat Awal Cluster Algoritma Genetika Classification Of Needs For The Number Of Customer Food Products Using K-Means Clustering With Optimization Initial Cluster Center Genetic Algorithm*. *8*(5), 861–870. <https://doi.org/10.25126/jtiik.202182990>
- LASHIYANTI, A. R., RASYID MUNTHE, I., NASUTION, F. A., & KORESPONDENSI, E. P. (2023). Optimisasi Klasterisasi Nilai Ujian Nasional dengan Pendekatan Algoritma K-Means, Elbow, dan Silhouette. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, *6*(1), 14–20.
- REGUEIRO, C., SECO, I., GUTIÉRREZ-AGÜERO, I., URQUIZU, B., & MANSELL, J. (2021). A blockchain-based audit trail mechanism: Design and implementation. *Algorithms*, *14*(12). <https://doi.org/10.3390/a14120341>
- REPUBLIK INDONESIA. (2016). *Peraturan Otoritas Jasa Keuangan Nomor 38 /Pojk.03/2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum*.
- REPUBLIK INDONESIA. (2019). *PERATURAN PEMERINTAH REPUBLIK INDONESIA NOMOR 71 TAHUN 2019 TENTANG PENYELENGGARAAN SISTEM DAN TRANSAKSI ELEKTRONIK*.
- RODRIGUEZ, M. Z., COMIN, C. H., CASANOVA, D., BRUNO, O. M., AMANCIO, D. R., COSTA, L. DA F., & RODRIGUES, F. A. (2019). Clustering algorithms: A comparative approach. *PLoS ONE*, *14*(1). <https://doi.org/10.1371/journal.pone.0210236>
- SHOLEH, M., & AENI, K. (2023). *Perbandingan Evaluasi Metode Davies Bouldin, Elbow Dan Silhouette Pada Model Clustering Dengan Menggunakan Algoritma K Means*. <https://archive.ics.uci.edu/ml/datasets/Trave>
- SINAGA, K. P., & YANG, M. S. (2020). Unsupervised K-means clustering algorithm. *IEEE Access*, *8*, 80716–80727. <https://doi.org/10.1109/ACCESS.2020.2988796>
- SUTOMO, F., MUAAFII, D. A., NAUFALDI, D., RASYID, A., KURNIAWAN, Y. I., AFUAN, L., CAHYONO, T., MARYANTO, E., & ISKANDAR, D. (2023). Optimization Of The K-Nearest Neighbors Algorithm Using The Elbow Method On Stroke Prediction. *Jurnal Teknik Informatika (JUTIF)*, *4*(1). <https://doi.org/10.20884/1.jutif.2023.4.1.839>

ZHANG, C., HUANG, W., NIU, T., LIU, Z., LI, G., & CAO, D. (2023). Review of Clustering Technology and Its Application in Coordinating Vehicle Subsystems. *Automotive Innovation*, 6(1), 89–115. <https://doi.org/10.1007/s42154-022-00205-0>