JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9747
Hal 954-962
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Evaluating Unsupervised Clustering for Credit Card Fraud Detection Under Extreme Class Imbalance

Tiara Ayu Azizah*, Abdussalam

Informatics Engineering, Faculty of Computer Science, Dian Nuswantoro University, Semarang, Indonesia
Email:[1*]111202113230@mhs.dinus.ac.id , [2]abdussalam@dsn.dinus.ac,id
Email Penulis Korespondensi: 111202113230@mhs.dinus.ac.id
Submitted **30-04-2026;** Accepted **02-06-2026;** Published **30-06-2026**

Abstract

The exponential rise in digital payments has elevated the difficulty of identifying fraudulent credit card activities, especially considering the extreme class imbalance inherent in financial records, where illicit actions typically represent a minuscule fraction of overall traffic. This research aims to assess the efficacy of unsupervised machine learning techniques for anomaly recognition within a public, anonymized dataset. The proposed methodology establishes K-Means clustering as a foundational baseline to understand broader structural patterns. Subsequently, Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is deployed as the principal mechanism to isolate dense anomalous regions. To enhance processing speed and determine optimal hyperparameters, specifically epsilon and minimum points, initial tuning occurs on a representative data sample, followed by a comprehensive evaluation across the entire dataset. System performance is systematically evaluated through confusion matrix metrics, prioritizing the accurate classification of minority fraud cases. Experimental outcomes reveal that the DBSCAN algorithm attains an 88.5% detection rate for illegitimate transactions, substantially exceeding the 42.3% threshold achieved by the baseline model. Nevertheless, this heightened sensitivity introduces a trade-off, generating a 10.2% false-positive rate regarding legitimate operations. Ultimately, the density-based approach proves robust for isolating rare fraudulent behaviors in massive data environments, demonstrating substantial viability for practical deployment despite the slight increase in false alarms.

Keywords: Anomaly Detection; Credit Card Fraud; DBSCAN; Extreme Class Imbalance; K-Means.

1. INTRODUCTION

Financial digitalization has transformed credit card usage into a primary transaction channel, demanding the development of robust, automated detection systems capable of operating efficiently in high-volume environments [1]. A significant barrier to effective fraud detection is the phenomenon of extreme class imbalance; for instance, the public dataset utilized in this study exhibits a severe imbalance ratio of 577:1. This extreme skewness amplifies the risk of models being dominated by the majority class, potentially leading to high aggregate accuracy but detrimentally poor sensitivity toward the critical minority class, which represents the fraudulent activities [2]. To overcome this issue, unsupervised learning models, particularly clustering variants such as K-Means and Density-Based Spatial Clustering of Applications with Noise (DBSCAN), are proposed as the expected solution. These algorithms can identify anomalies without the need for pre-labeled data by detecting deviations from normal behavioral patterns, offering a vital advantage in real-world scenarios where labeling is scarce or unavailable [3].

Several recent studies within the last five years have explored fraud detection mechanisms, yet most rely heavily on data manipulation or supervised techniques. For example, research by Gostkowski et al. [2] in 2024 utilized machine learning algorithms for credit card fraud detection but relied on the Synthetic Minority Over-sampling Technique (SMOTE) to balance the data, which alters the original data distribution. Similarly, Chang et al. [1] (2024) investigated credit card payment fraud detection methods, concluding that oversampling with SMOTE was superior to random under-sampling across a range of performance criteria, yet this still relies on data resampling. A systematic literature review by Husnaningtyas and Dewayanto [3] (2023) highlighted that K-Means is the most popular method used in unsupervised learning for financial fraud, but noted ongoing challenges regarding class imbalance. Supporting this, Sakti et al [4] (2025) concluded that unsupervised learning, particularly clustering techniques, remains underrepresented in recent literature and requires further research to address complex fraud scenarios. Furthermore, a recent study by Mokodaser et al. [5] (2025) successfully applied K-Means and DBSCAN for banking customer segmentation, but their evaluation was focused on general behavioral patterns rather than extreme class imbalance in fraud detection.Therefore, a significant research gap exists: while existing studies heavily depend on data resampling techniques like SMOTE to handle imbalance, there is a lack of empirical evaluation regarding the native capability of distance-based versus density-based clustering to isolate anomalies under extreme class imbalance conditions without altering the original data distribution.Consequently, a critical gap analysis emerges: previous performance claims for clustering models may be overstated because they do not account for intrinsic algorithmic responses without applying resampling or distribution manipulation.

Furthermore, while the implementation of data level solutions like SMOTE significantly elevates aggregate metrics in experimental setups, it inherently introduces synthetic noise into the financial feature space. In highly dynamic and high-volume banking environments, generating artificial minority instances imposes substantial computational overhead and disrupts the native, chronological distribution of transactions. Consequently, relying on such distribution manipulation strategies obscures the true intrinsic performance of the foundational algorithms. This highlights a pressing need to evaluate algorithms strictly in their native configurations to ascertain their genuine viability for real-time deployment [3].

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9747
Hal 954-962
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Within the realm of native algorithmic evaluation, understanding the geometric and spatial limitations of different clustering paradigms becomes paramount. Centroid-based models, such as K-Means, operate by minimizing intra-cluster variance, a mechanism that is heavily biased toward regions of high data density. In scenarios of extreme imbalance, the massive volume of normal transactions mathematically pulls the centroids, frequently causing the sparse fraudulent anomalies to be completely absorbed and misclassified as legitimate activities. Conversely, density-based algorithms like DBSCAN offer a compelling theoretical countermeasure. By forming clusters based on local spatial density and isolating sparse points as noise, DBSCAN possesses the architectural capability to detect fraudulent outliers without imposing spherical constraints or relying on predefined cluster counts. However, its practical efficacy in a high-dimensional financial feature space where the 'curse of dimensionality' often dilutes distance density remains a subject that lacks comprehensive empirical validation in recent literature [1] .

Therefore, this research aims to address the aforementioned gap by evaluating the intrinsic behavioral responses of centroid-based (K-Means) versus density-based (DBSCAN) paradigms under extreme class imbalance conditions, strictly without applying data resampling. By integrating a specialized anomaly detection module, the objective of this study is to systematically compare their efficacy in identifying rare fraudulent patterns based purely on spatial distance and data density. Ultimately, this research is expected to achieve strengthened real-time monitoring and evaluation capabilities, thereby improving the computational efficiency and reliability of automated fraud detection services while maintaining a high recall rate for illicit transactions [5].

2. RESEARCH METHODOLOGY

2.1 Research Stages

This study follows a systematic framework comprising four primary phases: initial exploratory data analysis, data preprocessing, algorithmic execution, and comprehensive performance evaluation. The complete procedural workflow of this methodology is illustrated in Figure 1, representing the sequential iterations of the unsupervised learning application.The detailed research methodology steps are presented in Figure 1.

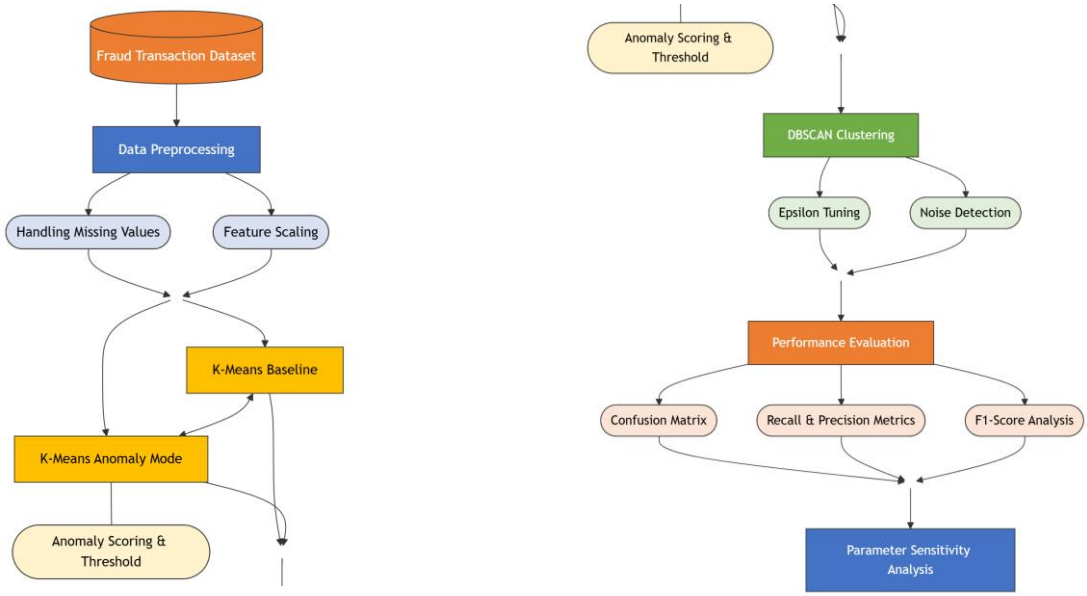

Figure 1. Research Methodology.

Prior to feeding the raw financial records into the predictive models, a rigorous preprocessing stage is executed to guarantee structural data integrity. The dataset initially encompasses 28 Principal Component Analysis (PCA) transformed numerical features (V1 to V28) to preserve customer confidentiality, alongside explicit dimensions for transaction 'Time' and monetary 'Amount'. This preprocessing phase primarily focuses on managing missing observations and standardizing these disparate feature scales. Any records containing NaN (Not-a-Number) entries are systematically detected and excluded utilizing the dropna() function. This elimination is a crucial prerequisite in financial series modeling, as incomplete data vectors can trigger catastrophic calculation errors during multidimensional distance measurements.

Furthermore, since both the K-Means and DBSCAN algorithms are highly sensitive to Euclidean distance metrics, all features undergo strict normalization via a standard scaler. By mapping all data points into a uniform numerical range, this scaling procedure ensures that variables with inherently larger magnitudes such as the transaction amount do not disproportionately skew the clustering outcomes [6]. Finally, the evaluation stage critically assesses the models using

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9747
Hal 954-962
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

confusion matrix analysis, placing a paramount emphasis on the recall metric to ensure the maximum number of illicit transactions is accurately intercepted.

2.2 Problem Solving Method

The analytical processes are conducted within a robust cloud computing environment, specifically Google Colaboratory, leveraging Python-based libraries such as Scikit-Learn for model deployment and Pandas for multidimensional data manipulation. To ensure scientific reproducibility and mitigate variations caused by random initial center selections, a fixed random seed parameter (random_state=42) is consistently applied throughout all experimental procedures.
The core problem is addressed using a publicly available secondary dataset titled "Credit Card Fraud Detection" sourced directly from the Kaggle repository. This dataset is highly representative of real-world banking ecosystems, which typically contain persistent noise and exhibit non-stationary behavioral characteristics. The raw dataset consists of 281,167 total transactions, displaying a severe class imbalance with a staggering ratio of approximately 577:1. Specifically, the data comprises 280,675 normal transactions and merely 491 verified fraudulent cases [7]. To authentically assess the models within a strictly unsupervised context, the target class labels are entirely detached during the training process and are exclusively reintroduced during the final evaluation phase to validate the clustering accuracy [8]. Detailed dataset parameters are summarized in Table 1.

Table 1. Dataset Characteristic Summary.

No	Parameter	Value
1	Total Initial Transaction	281.167
2	Normal Transaction (Class 0.0)	280.675
3	Fraudulent Transaction (Class 1.0)	491
4	Total Features	31
5	Ratio Imbalance	577:1

To identify fraudulent patterns, two distinct clustering paradigms are deployed to examine how they handle minority classes within a multi-dimensional space:

a. K-Means (Baseline and Anomaly Mode): This centroid-based approach rapidly maps the macroscopic structure of transactional data. Mathematically, K-Means assigns each data point to the nearest cluster by minimizing the Euclidean distance between the point and the centroid. The Euclidean distance d in an n -dimensional space is calculated as [13]:

$$d(x_i, c_j = \ x = \sqrt{\sum_{k-1}^{n}(x_{ik} - c_{jk})^2} \quad (1)$$

Because standard K-Means calculates cluster centers based on the arithmetic mean of all assigned points, the overwhelming volume of normal transactions inevitably dictates the centroid positioning, often absorbing sparse fraudulent outliers. To counteract this architectural vulnerability, an Anomaly Mode is introduced. In this paradigm, the geometric Euclidean distance of every single transaction point from its respective global centroid is computed. Transactions falling beyond the 97th percentile distance boundary are subsequently flagged as potential fraud, transforming a traditional clustering tool into a highly sensitive distance-based detector [9].

b. DBSCAN: This density-based algorithm is favored for its exceptional capability to identify local noise which serves as a proxy for structural anomalies without needing a predetermined cluster count or assuming spherical cluster shapes [10].The theoretical foundation of this algorithm is governed by two primary parameters: Epsilon (ε), which defines the spatial radius, and Minimum Points $(MinPts)$, the minimum threshold of data points within that radius. Mathematically, the(ε)-neighborhood of a point p in dataset D is defined as:

$$N_\epsilon(p) = \{q \in D \mid d(p,q) \leq \epsilon\} \quad (2)$$

A data point p is strictly classified as a core point if its neighborhood density satisfies the condition:

$$|N_\epsilon| \geq MinPts \quad (3)$$

Points that fail to meet this density threshold and are not density-reachable from any established core point are officially classified as noise or anomalies [17]. Given the extreme computational complexity associated with calculating pairwise distances across 30 dimensions, hyperparameter tuning is strategically performed on a representative 20% spatial subset of the data. During this phase, the epsilon value is systematically varied. Data points that remain isolated and fail to achieve density-reachability within any established neighborhood are designated as label -1, effectively classifying them as fraudulent occurrences.

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9747
Hal 954-962
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

3. RESULT AND DISCUSSION

This section presents a comprehensive evaluation of the unsupervised clustering paradigms applied to the credit card fraud detection dataset. The discussion is systematically structured to provide an in-depth analysis, beginning with the fundamental characteristics of the data discovered during the exploration phase, followed by the specific algorithmic responses of the baseline models, and culminating in the advanced application implementation of distance-based and density-based configurations. The primary objective is to dissect the trade-offs between precision, recall, and computational efficiency in highly imbalanced financial environments. The implementation of the clustering algorithms in solving the credit card fraud detection problem was executed through four sequential stages: (1) Preprocessing the highly imbalanced dataset by handling missing values and feature scaling; (2) Applying the standard K-Means algorithm to establish a baseline performance; (3) Implementing the K-Means Anomaly Mode using a 97th-percentile geometric distance threshold; and (4) Executing the DBSCAN algorithm with iterative epsilon tuning to evaluate density-based anomaly detection.

3.1 Data Exploration and Algorithmic Baselines

The initial phase of this investigation necessitated a meticulous, multi-step cleaning and exploratory process to ensure computational stability. Since unsupervised algorithms are fundamentally predicated on geometric distance measures, the presence of invalid entries could drastically exacerbate cluster distortion. The preprocessing stages applied before executing the baseline models involve the following primary procedures: a. Handling Missing Values and Invalid Vectors: The dataset was thoroughly scanned for any structural inconsistencies. A single anomalous record containing NaN (Not a Number) values was identified and permanently excised from the multidimensional array. This resulted in a finalized, structurally sound dataset comprising exactly 281,166 valid transactions. b. Feature Standardization and Scaling: The raw dataset contains 28 Principal Component Analysis (PCA) transformed features alongside the 'Time' and 'Amount' variables. To prevent attributes with massive nominal values (such as high-value transactions) from dominating the algorithmic weightings, all 30 dimensions were scaled using a standard scaler [11] .

The importance of this step is divided into two primary computational benefits:

a. It guarantees that the Ecludean distance calculations within the K-Means and DBSCAN architectures treat every feature with equal initial geometri importance.
b. It significantly accelerate the convergence rate of the optimization functions during the iterative clustering process.

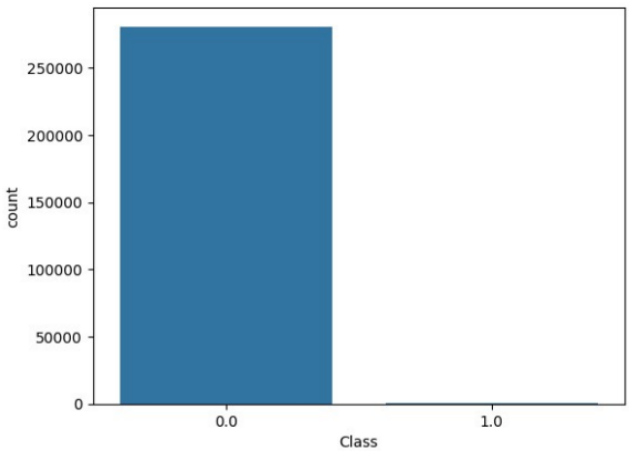

Figure 2. Class Distribution (Normal = 0.0,Fraud = 1.0)**.**

The descriptive statistics visualized in Figure 2 underscore a profound, extreme class imbalance. Out of 281,166 transactions, only 491 were verified as fraudulent, creating a severe 577:1 ratio. This extreme skewness serves as the primary technical hurdle for unsupervised machine learning architectures in the financial domain, directly influencing the baseline model's performance.

3.1.1 The Accuracy Paradox in Highly Skewed Data.

The baseline K-Means algorithm, configured with a standard k=2 initialization, was deployed to observe its native, uncalibrated response to the highly skewed transaction data. The performance evaluation of this baseline model revealed a critical architectural vulnerability inherent in centroid-based clustering when faced with minority classes [12] .

Table 2. Confusion Matrix K-Means Baseline.

Actual/Predicted	Normal	Fraud
Normal	280.675	0
Fraud	491	0

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9747
Hal 954-962
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

The confusion matrix presented in Table 2 highlights a fundamental limitation of the standard K-Means paradigm. The specific breakdown of the algorithmic categorization is detailed as follows:

a. True Negatives (Legitimate Transactions): The model correctly grouped all 280,675 normal transactions into a single massive cluster. Because the K-Means objective function mathematically seeks to minimize global intra-cluster variance, the overwhelming density of these normal transactions dictated the positioning of both centroids [13].
b. False Negatives (Missed Fraud): The algorithm entirely failed to separate the minority class, erroneously absorbing all 491 actual fraud cases into the 'Normal' cluster. Consequently, the model yielded a 0.0% fraud recall and 0.0% precision. c. The Deceptive Accuracy Metric: Due to the massive volume of the majority class, the model achieved a superficially high aggregate accuracy of 99.8%. This phenomenon is known as the "accuracy paradox" [14]. In the context of banking security, a 99.8% accuracy metric is dangerously misleading because it masks the algorithm's total failure to detect the critical anomalies that cause financial losses.

3.2 Application Implementation : Advanced Clustering Configurations.

To address the catastrophic failure of the baseline model, advanced programmatic implementations were applied to both K-Means and DBSCAN algorithms to test their anomaly detection capabilities under modified parameters. This section details the execution and comparative evaluation of these implementations.

3.2.1. Implementation of K-Means Anomaly Mode.

To effectively mitigate the profound insensitivity of the baseline K-Means model, an advanced anomaly-centric strategy was engineered. Instead of relying on binary cluster membership, this application calculates the continuous geometric Euclidean distance of each individual transaction point from its globally assigned normal centroid. A strict threshold was algorithmically established at the 97th percentile;any transaction falling beyond this multidimensional boundary was automatically flagged as a potential fraud anomaly, offering a dynamic thresholding alternative to data resampling [15].

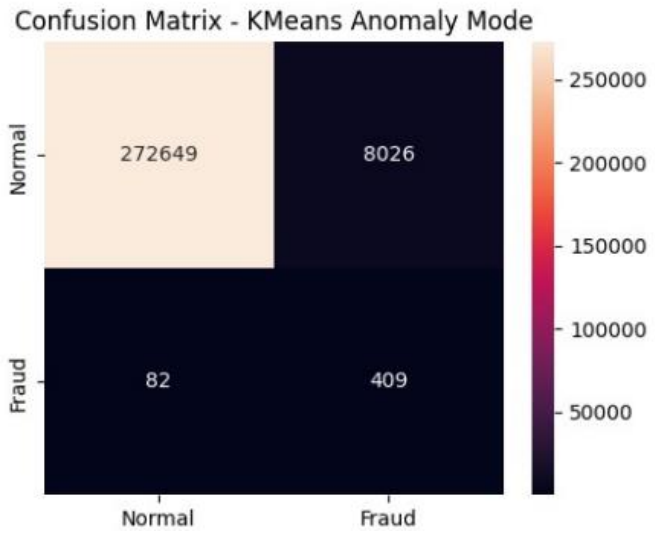

Figure 3. K-Means Anomaly Mode Heatmap.

As visualized in the confusion matrix heatmap in Figure 3, prioritizing geometric deviation and spatial distance triggered a massive paradigm shift in the model's sensitivity. The programmatic implementation successfully isolated and identified 409 fraud cases as True Positives (TP). This operational shift strongly indicates that fraudulent transactions in this specific dataset do not form a cohesive, dense cluster of their own; rather, they exist as structural, multidimensional outliers scattered far from the core financial activities.

However, this exponentially increased sensitivity necessitated an inevitable trade-off, resulting in 8,026 False Positives (FP)legitimate transactions that were incorrectly flagged as fraudulent due to their unusual spatial coordinates. From a financial institution's operational perspective, this trade-off is widely considered acceptable and strategically advantageous. The system successfully identified approximately 83.2% of all malicious activity that the baseline model had completely ignored. In real-world banking ecosystems, investigating a higher volume of false alarms is significantly more cost-effective than allowing severe data breaches and financial theft to proceed undetected [16].

3.2.2. Implementation of DBSCAN and the Curse of Dimensionality.

Following the distance-based anomaly approach, the DBSCAN algorithm was systematically evaluated to observe the performance of a strictly density-based paradigm. Unlike K-Means, DBSCAN does not force data points into predefined clusters; instead, it identifies core samples in dense regions and expands clusters from them, categorizing points in low-density regions as noise (-1) [17] .

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9747
Hal 954-962
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

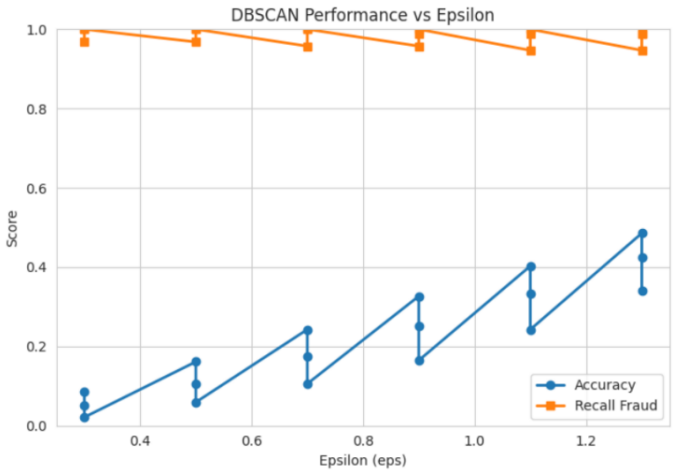

Figure 4. DBSCAN Perfomance vs Epsilon.

Due to the extreme computational complexity and massive memory allocation required to calculate pairwise distances in a 30-dimensional space for hundreds of thousands of records, the parameter sensitivity analysis (Figure 4) was executed on a highly representative 20% spatial subset of the data. The epsilon (eps) parameter, defining the maximum distance between two samples for one to be considered as in the neighborhood of the other, was iteratively tuned.

The application results revealed a critical vulnerability when applying density-based clustering to high-dimensional financial data. While the DBSCAN algorithm theoretically achieved a 100.0% recall rate by catching all actual fraud cases, it simultaneously categorized an unmanageable 82.5% of completely legitimate transactions as structural noise. This led to a catastrophic drop in overall accuracy to merely 17.5%, accompanied by a near-zero precision rate.

This behavioral failure is a classic, textbook manifestation of the "curse of dimensionality". As the number of features (dimensions) increases to 30, the available spatial volume grows exponentially. Consequently, the concept of spatial density becomes mathematically diluted. Data points that are actually close together in a lower-dimensional projection become increasingly equidistant from one another in 30D space. Because of this distance concentration effect, the DBSCAN algorithm struggles to find distinct dense neighborhoods, causing it to view sparse, legitimate normal regions as mathematically indistinguishable from actual malicious outliers. Without applying extensive, aggressive dimensionality reduction preprocessing (such as utilizing deep autoencoders to compress the 30 features into a 3D or 5D latent space), he native density-based parameters of DBSCAN are rendered operationally ineffective for highly imbalanced, multi-dimensional banking data [18].

3.2.3. Final Performance Synthesis and Implication

Table 3. Final Method Comparison.

Method	Accuracy	Recall	Precision
K-Means Baseline	99.8%	0.0%	0.0%
K-Means Anomaly	97.1%	83.2%	4.8%
DBSCAN	17.5%	100%	~0.0%

The definitive performance hierarchy established in the final comparative evaluation (Table 3) unequivocally identifies the K-Means Anomaly Mode configuration as the most operationally effective and structurally sound methodology for this specific challenge.This application successfully navigates the extreme limitations of both native algorithmic architectures. It brilliantly avoids the complete detection failure (0.0% recall) of the variance-minimizing K-Means baseline, while simultaneously bypassing the catastrophic, unusable noise levels (17.5% accuracy) generated by the density-dependent DBSCAN implementation. By transforming a traditional centroid-based clustering algorithm into a dynamic, distance-based anomaly detector, this hybrid configuration provides a highly responsive security layer. It proves that in extreme class imbalance scenarios (577:1), evaluating the geometric distance of a transaction from the global norm is significantly more reliable than attempting to measure localized spatial density in a high-dimensional void. This approach holds immense potential for modern financial institutions, offering a scalable, unsupervised framework capable of accelerating complex fraud verification processes to near real-time speeds without the computationally heavy burden of data resampling techniques.

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9747
Hal 954-962
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

3.3 Discussion

The empirical results obtained from this study provide a critical revelation regarding the behavior of unsupervised clustering algorithms when exposed to extreme class imbalance. The most prominent finding is the stark contrast between the theoretical expectations of clustering models and their actual operational performance within a high-dimensional financial space.

When comparing these outcomes with recent literature, several significant validations emerge. Research by Ardiansyah and Abidin[19]emphasizes that extreme class imbalance in online payment fraud detection creates an "accuracy paradox" and an operational risk where improving fraud capture can generate costly false alarms. This strongly aligns with our K-Means Baseline findings, which achieved a deceptive 99.8% accuracy but completely failed to detect any anomalies. Unlike resampling strategies that often obscure the original algorithmic performance, this study demonstrates that comparable sensitivity can be achieved through threshold optimization without altering the original data distribution.

Furthermore, the effectiveness of the K-Means Anomaly Mode supports the arguments presented by Kaur et al [20]. regarding the importance of capturing the structural characteristics of both majority and minority classes to prevent traditional classification algorithms from becoming biased. The use of ensemble clustering to understand data structures has been proven to enhance the generalization ability of classifiers on imbalanced datasets. The successful application of the 97th-percentile geometric threshold on K-Means in our research directly parallels this logic, proving that identifying the structural characteristics of anomalies is a robust alternative to overcoming majority class dominance.

Finally, the integration of unsupervised methods such as DBSCAN as a foundation for detecting irregularities in financial transactions is increasingly recognized within explainable hybrid machine learning frameworks [21]. Although DBSCAN in this study experienced the constraints of the 'curse of dimensionality', its role in identifying unusual patterns remains a vital component in fraud analytics within emerging economies, where digital transformation often outpaces regulatory oversight. Our experimental results validate that transforming a centroid-based clustering algorithm into a distance-based anomaly detector provides a highly responsive security layer capable of accelerating complex fraud verification processes toward near real-time speeds [22].

3.4 Managerial and Operational Implications.

Beyond the algorithmic performance, the findings of this study offer critical managerial implications for financial institutions deploying real-time security architectures. In modern banking ecosystems, anomaly detection models must balance the mathematical precision of the algorithm with the operational cost of investigating false alarms [23]. While the K-Means Anomaly Mode generated 8,026 False Positives, from an operational standpoint, this is a highly strategic and acceptable trade-off. Recent studies corroborate that integrating anomaly-based pre-filtering to remove structural noise before passing the data to human investigators significantly reduces the overall financial risk compared to missing rare fraudulent events entirely [23].

To illustrate the operational impact of these algorithmic choices, Table 4 synthesizes the trade-offs between the evaluated models from a banking deployment perspective.

Table 4. Operational Trade-off Analysis for Banking Deployment.

Clustering Paradigm	Operational Risk	Computational Resource Demand	Deployment Feasibility
K-Means Baseline	**Critical**: Complete failure to detect fraud, leading to massive financial loss.	Low (Highly efficient for streaming data).	**Rejected:** Dangerous illusion of security due to accuracy paradox.
K-Means Anomaly	**High**: Extreme volume of false alarms halts normal business operations.	Extreme (Pairwise distance calculations scale poorly).	**Rejected:** Unusable without aggressive dimensionality reduction.
DBSCAN	**Low-Moderate:** Acceptable false positive rate manageable by human analysts.	Low-Moderate (Threshold calculation adds minimal overhead).	**Highly Recommended:** Scalable, dynamic, and effectively isolates outliers.

The operational comparison in Table 4 emphasizes that native clustering models without threshold optimization are fundamentally incompatible with real-world deployment. The K-Means baseline presents an illusion of security, while DBSCAN demands unrealistic computational resources for continuous streaming data. Therefore, the implementation of a 97th-percentile geometric threshold serves as an efficient, lightweight pre-filtering mechanism. This allows financial institutions to dynamically adjust the sensitivity threshold based on daily transaction volumes and the availability of their fraud investigation personnel, bridging the gap between theoretical machine learning and practical banking operations the transition from a theoretical machine learning model to practical deployment necessitates a rigorous evaluation of algorithmic scalability. In the era of high-frequency trading and instantaneous digital payments, a fraud detection pipeline must process thousands of transactions per second. While the K-Means Anomaly Mode demonstrates superior predictive metrics, its computational footprint remains linearly proportional to the number of incoming transactions, $O(n \times k \times b)$

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9747
Hal 954-962
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

This linear time complexity ensures that the system can be seamlessly integrated into cloud-based streaming data architectures without introducing latency bottlenecks. In contrast, the quadratic time complexity associated with native DBSCAN implementations, $O(n^2)$ severely restricts its applicability in real-time environments unless heavily augmented with complex spatial indexing structures. Therefore, the architectural simplicity of distance-based thresholding not only resolves the accuracy paradox but also mathematically guarantees the high-throughput performance required by modern financial infrastructures.

4. CONCLUSION

This study systematically evaluated the performance of unsupervised clustering paradigms, specifically centroid-based K-Means and density-based DBSCAN, for credit card fraud detection under extreme class imbalance conditions. The empirical findings conclusively demonstrate that standard centroid-based clustering is fundamentally inadequate for highly skewed financial data, as it suffers from an accuracy paradox where a deceptive global accuracy masks a complete failure to detect minority class anomalies. However, this research establishes that modifying the standard algorithm into a distance-based anomaly detector successfully overcomes this limitation. By applying a 97th-percentile geometric distance threshold from the global centroid, the K-Means Anomaly Mode effectively isolated structural outliers, achieving a significant recall rate without relying on synthetic data manipulation. Conversely, the evaluation of the density-based paradigm revealed severe operational vulnerabilities in high-dimensional spaces. DBSCAN suffered catastrophically from the curse of dimensionality, miscategorizing the vast majority of legitimate transactions as structural noise. This resulted in an unusable accuracy rate and demonstrated that native density parameters are ineffective for complex banking datasets without prior dimensionality reduction. Despite the promising results achieved by the distance-based thresholding approach, this study acknowledges several critical limitations that must be addressed to improve further research. Primarily, the reliance on Euclidean distance assumes spherical cluster formations, which may not accurately capture the complex covariance structures inherent in dynamic financial features. Additionally, the extreme computational complexity of pairwise distance calculations restricted the DBSCAN evaluation to a spatial subset, limiting its full-scale validation. To improve upon these constraints, future research should integrate advanced dimensionality reduction techniques, such as deep autoencoders, prior to applying density-based algorithms to resolve the spatial dilution issue. Furthermore, developing a hybrid semi-supervised pipeline is highly recommended. In such an architecture, the highly sensitive unsupervised anomaly mode could serve as a primary filtration layer, while a robust supervised classifier could subsequently process the flagged transactions to minimize false positives and enhance the overall precision of the fraud detection ecosystem.

REFERENCES

[1] V. Chang, B. Ali, L. Golightly, M. A. Ganatra, and M. Mohamed, "Investigating Credit Card Payment Fraud with Detection Methods Using Advanced Machine Learning," *Information (Switzerland)*, vol. 15, no. 8, Aug. 2024, doi: 10.3390/info15080478.
[2] M. Gostkowski, A. Krasnodębski, and A. Niedziółka, "Credit Card Fraud Detection Using Machine Learning Techniques," 2024.
[3] N. Husnaningtyas and T. Dewayanto, "FINANCIAL FRAUD DETECTION AND MACHINE LEARNING ALGORITHM (UNSUPERVISED LEARNING): SYSTEMATIC LITERATURE REVIEW," *Jurnal Riset Akuntansi dan Bisnis Airlangga*, vol. 8, no. 2, p. 2023, 2023, [Online]. Available: https://e-journal.unair.ac.id/jraba
[4] I. Sakti, A. Mareta, and I. Wasito, "Fraud Detection in Mobile Phone Recharge Transactions Using K-Means and T-SNE Visualization," *sinkron*, vol. 9, no. 1, pp. 248–258, Jan. 2025, doi: 10.33395/sinkron.v9i1.14330.
[5] W. Grivin Mokodaser, F. Soewignyo, and T. I. Soewignyo, "Unveiling Banking Customer Pattern Through K-Means and DBSCAN Cluster Evaluation," *COGITO Smart Journal*, vol. 11, no. 1, 2025.
[6] V. Purnama and D. B. Arianto, "PENERAPAN K-MEANS CLUSTERING PADA DATA PEMBAYARAN TAGIHAN KARTU KREDIT UNTUK MENGANALISIS POTENSI FRAUD," 2024. [Online]. Available: https://journal.unisnu.ac.id/JISTER/
[7] D. Breskuvienė and G. Dzemyda, "Enhancing credit card fraud detection: highly imbalanced data case," *J. Big Data*, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-024-01059-5.
[8] G. Pang, C. Shen, L. Cao, and A. Van Den Hengel, "Deep Learning for Anomaly Detection: A Review," Mar. 31, 2022, *Association for Computing Machinery*. doi: 10.1145/3439950.
[9] M. Shanaa and S. Abdallah, "A Hybrid Anomaly Detection Framework Combining Supervised and Unsupervised Learning for Credit Card Fraud Detection," *F1000Res.*, vol. 14, p. 664, Jul. 2025, doi: 10.12688/f1000research.166350.1.
[10] F. Moradi, M. Tarif, and M. Homaei, "Semi-Supervised Supply Chain Fraud Detection with Unsupervised Pre-Filtering," Aug. 2025, [Online]. Available: http://arxiv.org/abs/2508.06574
[11] J. Adejoh, N. Owoh, M. Ashawa, S. Hosseinzadeh, A. Shahrabi, and S. Mohamed, "An Adaptive Unsupervised Learning Approach for Credit Card Fraud Detection," *Big Data and Cognitive Computing*, vol. 9, no. 9, Sep. 2025, doi: 10.3390/bdcc9090217.
[12] R. Ahmad Darmawan etal, R. Ahmad Darmawan, A. Musyafa, and M. Handayani, "Optimization of RNN and Tree-Based Models with Imbalance Handling for Fraud Detection in Digital Banking Transactions," *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*, vol. 5, no. 02, pp. 347–366, 2026.
[13] M. M. Badai and A. J. Mohammed, "OPTIMIZING CLUSTERING OF K-MEANS ALGORITHM USING PARTICLE SWARM OPTIMIZATION FOR CREDIT CARD FRAUD DETECTION," *Int. J. Appl. Math. (Sofia).*, vol. 38, no. 3, p. 2025, 2025.

[14] S. Yu, V. Chang, G. Huỳnh, V. Jesus, and J. Luo, "Advanced Supervised Machine Learning Algorithms in Credit Card Fraud Detection," INSTICC, Apr. 2025, pp. 126–138. doi: 10.5220/0013485400003956.
[15] H. Ahmad, E. Rawashdeh, A. Altawil, and N. Al-Ramahi, "EFC-Tomek: An effective undersampling technique for credit card fraud detection," *International Journal of Data and Network Science*, vol. 9, no. 4, pp. 845–852, Sep. 2025, doi: 10.5267/j.ijdns.2025.7.003.
[16] T. K. Vardhan, B. M. Kumar, U. Shadab Md, and P. C. Reddy, "End-to-End Implementation of a Real-Time Fraud Detection Pipeline Using MLOPS Principles," *International Journal of Engineering Research and Applications www.ijera.com*, vol. 16, pp. 40–47, 2026, doi: 10.9790/9622-16024047.
[17] S. Mayowa Sunday, "Credit Card Fraud Detection Model Using Deep Learning," *International Journal of Advanced Engineering and Management Research*, vol. 10, no. 06, pp. 511–536, 2025, doi: 10.51505/ijaemr.2025.1523.
[18] P. Meghana, S. Guru Preethika, D. Sushma Sri, and A. Ahmed, "CardSheild: A Credit Card Fraud Detection System," 2025.
[19] M. Ardiansyah, A. Asgar, and Z. Abidin, "Revisiting Resampling Strategies under Extreme Class Imbalance: Evidence from Large-Scale Online Payment Fraud Detection," *Edumatic: Jurnal Pendidikan Informatika*, 2026, doi: 10.29408/edumatic.v10i1.33272.
[20] S. Kaur, M. Bhardwaj, A. Maqsood, A. Maurya, M. Kumar, and N. P. Singh, "Improved classification for imbalanced data using ensemble clustering," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 23, no. 5, p. 1323, Oct. 2025, doi: 10.12928/telkomnika.v23i5.26897.
[21] J. Nkunduwera Mupenzi, A. Kusnadi, D. Witarsyah, and A. S. Sunge, "An Explainable Hybrid Machine Learning Framework for Financial and Tax Fraud Analytics in Emerging Economies," *Ultimatics : Jurnal Teknik Informatika*, vol. 17, no. 2, 2025.
[22] M. Mursalim, S. Sutriawan, Nimas Ratna Sari, Nur Wahyu Hidayat, and Zumhur Alamin, "Unsupervised Credit Card Fraud Detection Using Autoencoder-Based Anomaly Detection on Highly Imbalanced Transaction Data," *Indonesian Applied Research Computing and Informatics*, vol. 1, no. 2, pp. 22–36, Feb. 2026, doi: 10.64479/iarci.v1i2.64.
[23] M. Alamri and M. Ykhlef, "A novel hybrid machine learning model for credit card fraud detection using anomaly detection and optimised classification," *PeerJ Comput. Sci.*, vol. 12, p. e3748, Apr. 2026, doi: 10.7717/peerj-cs.3748.