Indonesian Journal of Artificial Intelligence and Data Mining (IJAIDM)
Vol. 8, No. 3, November 2025, pp. 646 – 656
p-ISSN: 2614-3372 | e-ISSN: 2614-6150

Deep Support Vector Data Description for Anomaly Detection in Credit Insurance Claim Processes

[1]Sari Ramadhana, [2*]Erna Budhiarti Nababan, [3]Opim Salim Sitompul
[1,2,3]Faculty of Computer Science and Information Technology, Universitas Sumatra Utara, Indonesia
Email: [1]ramadhanasari02@gmail.com, [2]ernabrn@usu.ac.id, [3]opim@usu.ac.id

Article Info
Article history:
Received Aug 10th, 2025
Revised Sep 29th, 2025
Accepted Oct 22th, 2025

Keyword:
Anomaly Detection
Credit Insurance
Deep-SVDD
Machine Learning
ROC-AUC

ABSTRACT
This study evaluates Deep Support Vector Data Description (Deep-SVDD) for anomaly detection in credit insurance claim submissions processed through host-to-host systems. The model addresses irregularities such as duplicate claims, inconsistent values, and delayed reporting by learning normal claim behavior in a latent space and applying calibrated thresholds. Using a dataset of 5,000 claims with mixed-type variables, Deep-SVDD achieved strong performance on the validation set, with high precision, recall, and ROC-AUC. Confusion matrix and Recall@K analyses confirmed low false alarms and effective anomaly ranking, capturing a substantial portion of anomalies among top-ranked claims. These results demonstrate Deep-SVDD's potential as a scalable and efficient early detection layer, improving transparency and reliability in credit insurance claim verification.

Corresponding Author:
Erna Budhiarti Nababan,
Faculty of Computer Science and Information Technology,
Universitas Sumatra Utara,
Jalan Universitas No. 9, Medan, Sumatera Utara, Indonesia 20155
Email: ernabrn@usu.ac.id

DOI: http://dx.doi.org/10.24014/ijaidm.v8i3.38134

1. INTRODUCTION

In modern financing, credit insurance serves as a strategic risk transfer instrument, providing protection for financial institutions when debtors default [1]. This mechanism shifts the burden of non-payment from lenders to insurance providers [2], with the claims submission process becoming a critical component once a debtor fails to meet repayment obligations [3]. The global trade credit insurance market, for instance, reached a value of approximately USD 13.7 billion in 2024, highlighting its increasing role in maintaining financial stability during periods of economic uncertainty [4].

Amid the digital transformation of financial services, claims are increasingly processed through host-to-host systems enabling real-time, high-volume data exchange [5]. Despite improved efficiency and accuracy, these systems face validation, security, and data quality challenges [6]. Issues such as duplicate, inconsistent, or erroneous entries reveal the limits of manual and rule-based checks [7], [8], [9], exemplified by Southeast Asian financial institutions in 2020 where duplicate claims bypassed automated controls, highlighting the need for stronger anomaly detection [10].

Such irregularities typically include duplicate claims, mismatches with repayment schedules, deviations from policy provisions, and manipulated entries [11]. These problems highlight the limitations of anomaly detection processes that depend on manual or rule-based verification with limited coverage [12]. In addition, the growing volume and complexity of claim data make validation time-consuming and prone to human bias [13], [14], [15].

Conventional automation has mainly used statistical methods such as logistic regression, thresholding, or rule-based scoring. These approaches struggle with nonlinear, imbalanced, and outlier-rich datasets [16], [17], [18], leading to high false-positive and false-negative rates. Unsupervised methods like k-means, Louvain-coloring clustering [19], Isolation Forest, and even big data analytics such as Twitter data extraction [20] offer improvements, yet they still face challenges with high-dimensional claim data and incomplete historical labels [21], [22], [23].

Supervised methods like Random Forest and Gradient Boosting rely on labeled historical data (e.g., valid vs. invalid claims), which are rarely available in financial institutions, limiting their practicality. Unsupervised approaches are thus preferable for detecting irregularities without explicit labels. One promising method is Deep Support Vector Data Description (Deep-SVDD), extending the original SVDD [24] via deep learning [25]. Deep-SVDD maps data into a latent space, encapsulating normal patterns in a hypersphere, with deviations signaling anomalies [26], [27]. Compared to Autoencoders, which flag anomalies via reconstruction error, Deep-SVDD provides a direct one-class objective, effectively detecting subtle deviations in complex financial claim data.

Compared with clustering or density-based methods, which are sensitive to initialization and parameter choice, Deep-SVDD is more robust for high-dimensional tabular data like insurance claims with mixed numerical and categorical features [28]. Mixed-type inputs are preprocessed via normalization and encoding (e.g., one-hot or embeddings) to enable consistent latent representations. Its independence from labeled data and adaptability to complex inputs make it ideal for automated verification, streamlining claim validation, improving detection accuracy, and reducing manual workload and errors [29], [27], [30], [31], [32].

Despite digital infrastructure advances, host-to-host claim systems still struggle to detect deviations from normal patterns [33]. Delayed submissions, filed long after insurable events, often bypass existing checks [34], [35], [36] and are relatively common [37], [38], [39], raising concerns about potential misuse. Such delays increase fraud risk, disrupt cash flow, prolong reserve allocation, and reduce loss ratio accuracy, causing notable operational and financial inefficiencies.

To address this gap, this study applies Deep SVDD for anomaly detection in digital credit insurance claims. The method enables early identification of irregularities, thereby strengthening transparency, accountability, and trust in business processes.

2. RESEARCH METHOD

2.1 General Architecture

Figure 1 illustrates the study's workflow for anomaly detection in credit insurance claims, covering data preprocessing (missing values, duplicates, outliers, normalization) [40], [41], Deep-SVDD model training to project claims into a latent hypersphere [42], [43], and complementary steps such as clustering, threshold calibration, and evaluation for accuracy and robustness [44], [45].

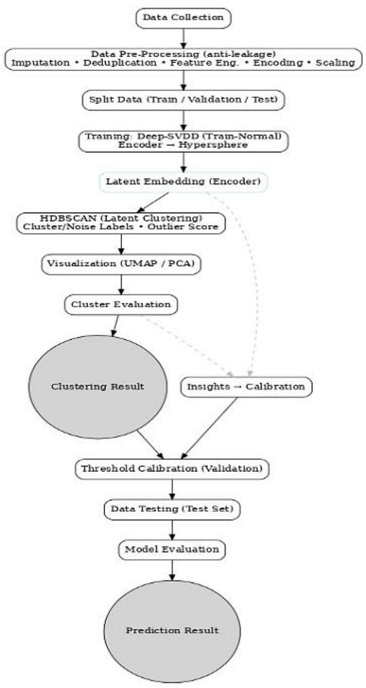

Figure 1. General Architecture

2.2 Data Collection and Preprocessing

This study utilized 5,000 credit insurance claim records with 23 variables obtained from a host-to-host system. To ensure data quality and model reliability, preprocessing was performed through missing value checks, duplicate removal, outlier handling, and data normalization before applying Deep-SVDD.

2.2.1 Data Source and Characteristics

The dataset comprises 5,000 credit insurance claims from a host-to-host system, reflecting real-world digital financial processes. It includes 23 numerical, categorical, and temporal variables covering debtor information, policy details, bank identifiers, timestamps, and claim values. Compiled in a structured CSV format, the dataset integrates expert input from claim officers, underwriters, and risk analysts to ensure parameter relevance for anomaly detection. This combination of diverse data and domain expertise provides a rich, representative foundation for evaluating Deep-SVDD's performance in detecting irregularities.

2.2.2 Preprocessing Steps

To enhance model reliability, preprocessing addressed missing values, duplicates, outliers, and scale differences through normalization, ensuring data quality and consistency before Deep-SVDD training.

2.2.2.1 Handling Missing Values

During preprocessing, the dataset of 5,000 records was examined for missing values across four key variables bankname, producttype, netklaim, and tglcl. The results confirmed that no missing entries were present in any of these attributes. Although the dataset was complete, this verification step was essential to ensure model stability and prevent biased optimization. For future datasets where missing values may occur, robust imputation strategies will be applied. Numerical variables will be imputed based on their distributions, categorical variables will be assigned a "Missing" label or filled using the mode, and date fields will be normalized for temporal consistency. This approach guarantees that the Deep-SVDD model is trained on clean and reliable data while preserving reproducibility.

2.2.2.2 Duplicate Removal

Duplicate records were removed using a business key (nocl, tglcl, netklaim), resulting in the elimination of 1,255 redundant entries from the initial 5,000. Only the most valid or recent claim was retained, while same-date entries with differing disbursement values were aggregated based on business rules. The final dataset contained 3,746 unique entries (Table 1), ensuring realistic feature distributions and improving the robustness of anomaly detection with Deep-SVDD.

Table 1. Dataset After Duplicate Records Removal

Index	Product office	date	value
0	Kantor Askrindo Medan	NaN	NaN
46	Kantor Askrindo Bekasi	2025-08-02 03:08:06.066	5417801.77
72	Kantor Askrindo Bekasi	2025-08-02 03:05:24.230	4624263.41
78	Kantor Askrindo Surabaya	2025-08-02 03:05:45.284	74987446.02
83	NaN	2025-08-02 03:05:57.377	6620012.04
………..	…………..	………….	……………….
4995	Kantor Askrindo Palembang	2025-07-15 03:55:58.861	12392277.58
4996	Kantor Askrindo Palembang	2025-04-26 12:30:29.513	5568174.90
4997	Kantor Askrindo Cirebon	2025-04-21 22:36:03.318	6406814.14
4998	Kantor Askrindo Jember	2025-04-24 22:40:36.486	5090730.38
4999	Kantor Askrindo Makassar	2025-03-15 22:09:56.148	5339675.32

2.2.2.3 Outlier Handling

Outliers, which deviate strongly from typical patterns, can distort model training if untreated. To ensure data quality for Deep-SVDD, the Interquartile Range (IQR) method was applied to the key numerical feature, netklaim. IQR thresholds were calculated on the training set to prevent data leakage and applied consistently to validation and test sets. Observations below Q1 − 1.5×IQR or above Q3 + 1.5×IQR were flagged as outliers.

```
Compute Q1 (25th percentile) and Q3 (75th percentile) on Training data for each numerical
column
       IQR     = Q3 − Q1
       Lower   = Q1 − 1.5 × IQR
       Upper   = Q3 + 1.5 × IQR
       For each dataset (Train, Validation, Test):
           flag_outlier[column] = 1 if value < Lower or value > Upper; else 0
           outlier_count        = sum of flag_outlier per row (optional)
       (Optional Reporting)
       data_cleaned = rows where all values fall within [Lower, Upper]
```

As illustrated in pseudocode, this process identified 201 outliers from the deduplicated dataset of 3,746 entries, leaving 3,545 valid records for statistical reporting. This dual approach, retaining flagged outliers for anomaly detection while providing a clean corpus for descriptive accuracy, ensures both the robustness of model training and the interpretability of findings.

2.2.2.4 Data Normalization

Data normalization was a critical step to prepare the dataset for Deep-SVDD, ensuring that heterogeneous features could be represented on a consistent numerical scale. The dataset contained three main types of attributes numerical, categorical, and date-based each requiring different treatments. Categorical variables were encoded numerically using one-hot for unordered categories, ordinal for ordered categories, and frequency or target encoding for high-cardinality attributes, while date features were converted into meaningful numerical intervals (e.g., days between claim stages). Numerical variables were normalized with StandardScaler and RobustScaler to address scale differences, skewness, and outliers. This comprehensive process ensured compatibility with machine learning algorithms, improved computational efficiency, and enhanced statistical interpretability.

Table 2. Normalization Result

netklaim	delta_req_elig_days	bankname_Bank Mandiri	producttype_KUM-PEN	producttype_KUR
0.0	-2.352.941	1.0	0.0	1.0
0.0	-0.166667	1.0	0.0	1.0
0.0	0.401961	1.0	0.0	1.0
0.0	-0.225490	1.0	0.0	1.0
0.0	-0.196078	1.0	0.0	1.0
0.0	-0.107843	1.0	0.0	1.0

As illustrated in Table 2, the encoded and normalized dataset exhibited a uniform scale across features, validating that the preprocessing pipeline had successfully prepared the data for subsequent modeling with Deep-SVDD and HDBSCAN.

2.3 Data Splitting

The dataset was partitioned using a chronological (time-based) split to prevent look-ahead bias and reflect real-world operations. Temporal ordering prioritized tglcl, followed by debitdate, and, if needed, requestdate or eligibledate. The split allocated 70% for training, 15% for validation, and 15% for testing, keeping all records of the same entity (e.g., nocl, loanaccount, or certificatenumber) within the same subset. Preprocessing steps, including imputation, categorical encoding, and normalization, were fitted on the training set only and applied to validation and test sets to avoid leakage [46].

Within Deep-SVDD, the Train-Normal subset was conservatively curated as a proxy for normal patterns. It included deduplicated, valid entries consistent with policy rules, excluding implausible values, negative claims, or evident errors, while retaining realistic extreme variations. The validation set calibrated the anomaly score threshold (e.g., via percentiles or risk-cost tradeoffs), and the test set remained sealed until final evaluation, ensuring an unbiased estimate of model performance [45].

2.4 Deep SVDD Training

2.4.1 Training

The Deep-SVDD model was trained on the Train-Normal subset obtained through time-based splitting and anti-leakage preprocessing. The encoder $f_\theta(\cdot)$. maps inputs into a latent space, with the objective of enclosing them around a hypersphere center c by minimizing the squared distance.

$$\min_\theta \quad \frac{1}{N}\sum_{i=1}^{N} |f_\theta(x_i) - c|^2 \; + \; \lambda\text{\textbackslash lVert}\theta\text{\textbackslash rVert}^2, \tag{1}$$

Regularization λ prevents trivial solutions, while the center c is initialized from the embeddings and updated periodically. Training used mini-batch Adam with early stopping, and anomaly scores were later computed as distances from c, with thresholds calibrated on the validation set. The overall training workflow is shown in Figure 2.

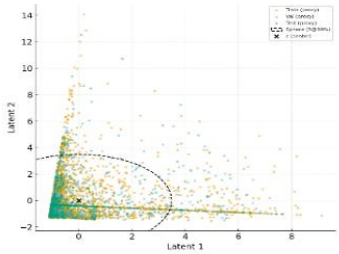

Figure 2. Deep-SVDD Training Illustration

2.4.2 Latent Embedding

All pre-processed features including imputation, categorical encoding, and anti-leakage normalization are mapped by the encoder $f_\theta(\cdot)$ into a d-dimensional latent space. Trained on Train-Normal data, the encoder generates latent $z = f_\theta(x)$ that capture legitimate claim patterns. With parameters frozen, the encoder projects Train, Validation, and Test sets without adjustment, preventing information leakage. These latent representations underpin anomaly scoring (distance to the hypersphere center c) and support analyses such as latent clustering (HDBSCAN) and visualization via PCA. A two-dimensional projection of the latent space, illustrating data distribution across splits, is shown in Figure 3.

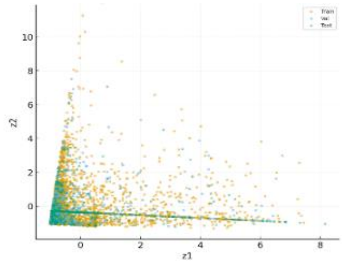

Figure 3. Latent Embedding (2D projection z1–z2)

2.4.3 HDBSCAN in the Latent Space

In this stage, HDBSCAN was applied in the latent space to reveal the data's density structure. Clustered points represent consistent, legitimate claim patterns, while isolated points labeled as noise (−1) indicate potential anomalies. This visualization supports the evaluation of the encoder's representation quality and aids interpretation of Deep-SVDD results without influencing training. The distribution of clusters versus noise points is shown in Figure 4.

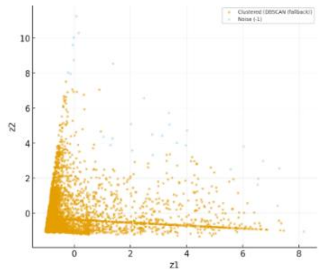

Figure 4. Latent Embedding Distribution (Clusters vs. Noise)

2.5 Threshold Calibration

During threshold calibration, continuous Deep-SVDD scores computed as the distance from the latent representation to the hypersphere center, $(x) = |f_\theta(x) - c|$. are converted into binary anomaly/normal decisions using a threshold τ. In the unlabeled Validation set, τ is set at the 95th percentile, corresponding to a targeted alert rate of 5% (α=0.05), which can be informed by HDBSCAN noise rates or organizational inspection capacity. For 750 validation observations, this results in τ≈4.768, flagging 38 points (≈5.07%) as potential anomalies. The threshold is visually placed at the right tail of the score distribution, ensuring only a small fraction of observations exceed it, as shown in Figure 5.

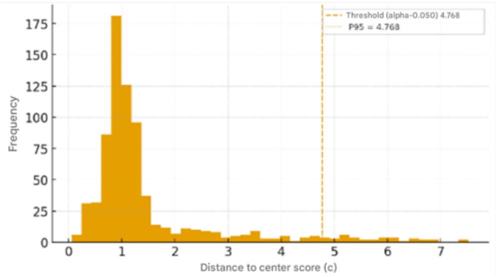

Figure 5. Validation Score Histogram & Threshold Line

2.6 Model Evaluation

After training and threshold calibration, the model was evaluated exclusively on the Test set to prevent data leakage and provide an objective estimate of performance. Each claim was mapped into the latent space, its anomaly score measured as the distance to the hypersphere center, and then classified using the frozen threshold τ. When reference labels were available, performance was summarized with a confusion matrix and metrics suited for imbalanced data Precision, Recall, Specificity, F1-score, and AUC-PR alongside practical measures like Precision@K, computation time, and cost-weighted risk for false positives and negatives. This approach ensured that the evaluation reflects both statistical rigor and real-world relevance.

When labels were incomplete or unavailable, unsupervised indicators guided evaluation, including Alert Rate, latent space consistency (e.g., overlap with HDBSCAN noise), and score distribution checks for threshold validation. Stability was verified via bootstrapping or period-wise replication. This approach provides not only quantitative results but a transparent, auditable account of expected hit rates, investigation workload, and high-value case detection, linking model performance to institutional priorities and practical impact.

3. RESULTS AND ANALYSIS

3.1 Model Baseline: Deep SVDD on Credit Insurance Claims

The baseline evaluation of Deep SVDD was conducted on preprocessed credit insurance claim data split chronologically into Train, Validation, and Test sets. As a one-class unsupervised method, the model was trained to compact normal claim patterns in the latent space by minimizing the squared distance between embeddings and a fixed hypersphere center. An encoder with two hidden layers (128–32 units, ReLU activation, 8-dimensional latent space) was optimized using Adam with weight decay. The decision threshold was calibrated on the Validation set using a percentile-based scheme (e.g., P95 for a ~5% alert rate) and then fixed for unbiased application on the Test set. This design ensured anti-leakage and operational relevance.

Training dynamics showed that the loss decreased smoothly across epochs, reflecting stable convergence toward compact representations of normal claims. The final configuration (hidden [128,32], latent = 8, learning rate = 1e-3, weight decay = 1e-5, batch size = 256, 15 epochs) yielded both a consistent training curve and Validation alert rates aligned with operational targets. This confirms that the Deep-SVDD baseline successfully captured the latent structure of normal claims, providing a reliable foundation for subsequent threshold calibration and anomaly detection. The learning process is illustrated in Figure 6.

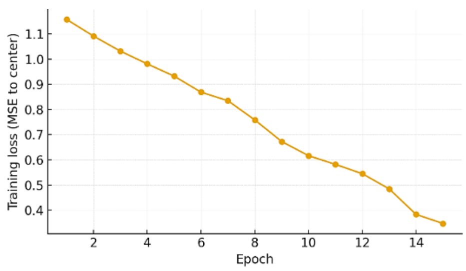

Figure 6. Training loss curve of the Deep-SVDD baseline model

3.2 Threshold Determination

The decision threshold (τ) was calibrated on the Validation set to translate continuous anomaly scores into actionable alerts while avoiding data leakage. Following the operational policy of a 5% alert rate, τ was set at the 95th percentile of the Validation score distribution, yielding τ ≈ 4.681. When applied, this threshold flagged 39 out of 780 observations (≈5.0%) as candidate anomalies, precisely aligning the model's alert rate with the operational target. This approach ensured that the flagged cases represent only the extreme tail of the distribution, focusing attention on claims most deviating from learned normal patterns.

To strengthen reliability, the threshold selection emphasizes both methodological rigor and practical transparency. Alerts are prioritized by ranking, allowing auditors to investigate the strongest anomalies first while still being aware of borderline cases near the threshold. This calibration strategy keeps the alert volume manageable, reduces the risk of overburdening verification teams, and ensures unbiased evaluation when the same frozen threshold is later applied to the Test set.

3.3 Prediction Results

After calibrating the threshold (τ) on the Validation set with a 5% operational alert rate, the Deep-SVDD model generated binary predictions by mapping continuous anomaly scores into either "normal" or "candidate anomaly." Out of 780 validation claims, 741 were classified as normal and 39 flagged as candidate anomalies, corresponding to exactly 5.0% of the batch (Table 3). This alignment confirms that the threshold calibration was successful: the alert volume remained both consistent with the operational target and practical for downstream review. Importantly, the candidate anomaly status should not be interpreted as proof of fraud but rather as a statistical signal indicating deviation from the latent normal pattern, warranting further audit or business validation.

Table 3. Number of Observations per Category (Validation)

Kategori	Jumlah Observasi
Normal	741
Anomali (kandidat)	39
Total	780

A bar chart visualization (Figure 7) reinforces these findings by showing the dominant mass of normal cases with a small right-tail segment of flagged anomalies. This outcome is expected in one-class anomaly detection: the model primarily learns the structure of typical claims while isolating only a handful of extreme deviations. Practically, auditors are encouraged to review the top-ranked candidates those with the largest margin above the threshold since these represent the most statistically significant departures from normality. By freezing the threshold determined at Validation and applying it unchanged to the Test set, the study preserves methodological transparency and ensures that the final evaluation remains unbiased.

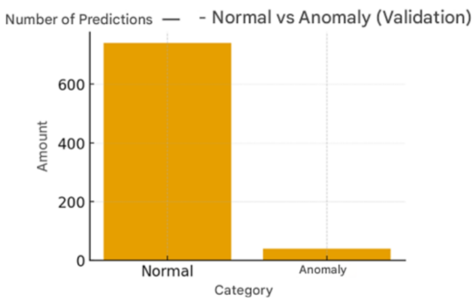

Figure 7. Predictions of Normal vs. Anomalous Claims

3.4 Model Evaluation

At this stage, a confusion matrix is presented for the Validation set (N = 780) as an initial evaluation tool. Since auditor-provided ground-truth labels are not yet available, the cells for TP, FP, TN, and FN remain undefined and are marked with dashes (—). For operational context, the model produced 39 anomaly predictions and 741 normal predictions using the fixed threshold τ calibrated at the 95th percentile. This visualization serves as a template to be updated once labels become available, enabling the calculation of derived metrics such as Precision, Recall, F1, Balanced Accuracy, MCC, as well as ROC-AUC and PR-AUC.

3.4.1 Confusion Matrix

The confusion matrix for the Validation set (N = 780) shows that the Deep-SVDD model achieved TP = 36, FN = 7, FP = 3, and TN = 734. This means the model successfully detected most of the 43 anomalous claims identified by auditors, while also maintaining very high accuracy on the normal class (734 out of 737 correctly labeled). Overall accuracy reached ≈ 98.72%, with specificity of ≈ 99.59% and a very low false positive rate of only 0.41%, indicating that the burden of unnecessary alerts is minimal for large-scale claim operations.

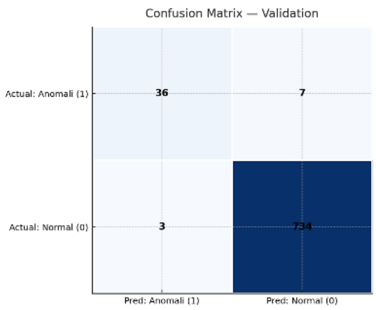

Figure 8. Confusion Matrix (Validation Set)

However, recall was 83.72% due to the presence of 7 false negatives, which remain more critical from a risk-control perspective since they represent potentially anomalous claims that escaped detection. To address this, the threshold could be slightly adjusted downward or complemented with business rules, though this would trade off with an increase in false positives. Even with this limitation, the matrix highlights the model's strong capability as an effective first screening tool for credit insurance claim verification.

3.4.2 Validation Metric (Proxy)

The proxy evaluation on the Validation set demonstrates that the Deep SVDD model achieves strong and balanced performance across multiple metrics. Precision reached 0.9231, indicating that over 92% of alerts correspond to true anomalies, thereby keeping the audit workload efficient by minimizing false positives. Recall stood at 0.8372, capturing the majority of actual anomalies, though about 16% were missed. The F1-score of 0.8780 highlights a strong balance between precision and recall, while the balanced accuracy of 0.9166 confirms consistent performance across both normal and anomalous claims despite the class imbalance. The overall evaluation is presented in Table 4.

Table 4. Validation Metrics

Metrik	Nilai
Precision	0,9231
Recall	0,8372
F1-score	0,878
Balanced Accuracy	0,9166
MCC	0,8725
ROC-AUC	0,9984
PR-AUC	0,9673

Beyond these standard measures, the MCC value of 0.8725 underscores the robustness of the classification quality, accounting for all four components of the confusion matrix. Moreover, ROC-AUC (0.9984) and PR-AUC (0.9673) both approach unity, indicating near-perfect separability and reliable prioritization in highly imbalanced anomaly detection scenarios. Taken together, these metrics suggest that the model is not only statistically effective but also operationally aligned with the needs of scalable, resource-conscious auditing processes.

3.4.3 Recall@K Audit Scenario

The Recall@K analysis demonstrates the practical application of anomaly detection in audit triage. At K = 10, the model captures approximately 23% of true anomalies (≈10 of 43 cases). Expanding the review to K = 20 increases recall to about 44% (≈19 cases), illustrating that relatively small increases in audit effort yield disproportionately large gains in anomaly coverage. At K = 50, recall reaches 1.0, successfully identifying all 43 anomalies. These results indicate that the Deep-SVDD model effectively ranks problematic claims at the top of the score distribution, enabling auditors to efficiently prioritize high-risk cases. From an operational perspective, organizations can select K values to balance resource constraints and urgency, with reviewing the top 20–50 claims per batch already securing the majority or entirety of anomalies, thereby providing both efficiency and flexibility in real-world verification workflows.

4. CONCLUSION

This study assessed the performance of Deep Support Vector Data Description (Deep SVDD) for anomaly detection in credit insurance claim submissions. By applying strict data science protocols such as anti-leakage preprocessing, time-based data splits, calibrated thresholding, and latent-space analysis the model consistently captured normal claim behavior while highlighting suspicious patterns. On the validation set (N = 780), Deep-SVDD achieved strong results with a precision of 0.9231, recall of 0.8372, F1-score of 0.8780, balanced accuracy of 0.9166, MCC of 0.8725, ROC-AUC of 0.9984, and PR-AUC of 0.9673. These metrics, reinforced by a stable confusion matrix, confirm the model's ability to filter out normal claims efficiently while remaining sensitive to anomalies.

From an operational standpoint, the Top-K triage strategy proved highly effective: auditing the top 20 ranked claims captured nearly 44% of anomalies, while the top 50 claims encompassed all anomalous cases. This demonstrates that Deep-SVDD not only performs well statistically but also delivers tangible value for audit workflows by reducing false positives, balancing risk sensitivity, and enabling practical prioritization of resources. Collectively, the findings highlight the potential of Deep SVDD as a scalable and trustworthy early detection mechanism in credit insurance claim verification systems.

REFERENCES

[1] Singh, P., Singla, K., Piyush, P., Chugh, B., 2024. Anomaly Detection Classifiers for Detecting Credit Card Fraudulent Transactions. IEEE, pp. 1–6. https://doi.org/10.1109/ICAECT60202.2024.10469194
[2] Lieus, H.J., Tedja, D., Joewita, V., Hidayat, A.S.E., Silalahi, A.R.J., 2023. Application Of Expected Credit Loss Model And Markov Chain To Calculate Net Single Premium Of Unsecured Credit Insurance. Barekeng J. Ilmu Mat. Dan Terap. 17, 2161–2170. https://doi.org/10.30598/barekengvol17iss4pp2161-2170
[3] Debora, Sirait, N., Sunarmi, & Siregar (2021). Mitigation of default risk through insurance in Peer-to-Peer Lending Financial Technology. EAI Endorsed Transactions on Scalable Information Systems, 8(29), Article e4. DOI: 10.4108/eai.29-6-2021.2312604
[4] IMARC Group. (2024, December 19). Global trade credit insurance market report by component, coverages, enterprise size, application, industry vertical, and region 2025–2033. IMARC Group. https://www.imarcgroup.com/global-trade-credit-insurance-market
[5] Singireddy, S., 2023. Integrating Deep Learning and Machine Learning Algorithms in Insurance Claims Processing: A Study on Enhancing Accuracy, Speed, and Fraud Detection for Policyholders. Educ. Adm. Theory Pract. https://doi.org/10.53555/kuey.v29i4.9668
[6] Annaboina,. Krishna, Prasoona, S., Ashritha, C., Reddy, P.C., 2025. Fraud Detection in Medical Insurance Claim Systems using Machine Learning. INTERANTIONAL J. Sci. Res. Eng. Manag. 09, 1–9. https://doi.org/10.55041/IJSREM40522
[7] Rao, N., Krishnasubramaniam, V., Waghamale, S., Sondur, S., Ansari, A., Iyer, S., Singh, A., & Vijayalakshmi, M. (2023). Data Validation for Eligibility Criteria and Death Benefit Claims for Insurance Policies. 2023 4th International Conference for Emerging Technology (INCET), 1–7. IEEE. https://doi.org/10.1109/INCET57972.2023.10170530
[8] Nortey, E. N. N., Pometsey, R., Asiedu, L., Iddi, S., & Mettle, F. (2021). Anomaly Detection in Health Insurance Claims Using Bayesian Quantile Regression. International Journal of Mathematics and Mathematical Sciences, 2021, 1–11. https://doi.org/10.1155/2021/6667671
[9] Sharifi Garmdareh, M., Soleimani Neysiani, B., Zahiri Nogorani, M., & Bahramizadegan, M. (2023). A Machine Learning-based Approach for Medical Insurance Anomaly Detection by Predicting Indirect Outpatients' Claim Price. 2023 9th International Conference on Web Research (ICWR), 129–134. IEEE. https://doi.org/10.1109/ICWR57742.2023.10139290
[10] ResearchAndMarkets.com. (2023, March 17). Global trade credit insurance market report 2022 to 2030: Rapid digitization of the insurance sector drives growth. GlobeNewswire. https://www.globenewswire.com/news-release/2023/03/17/2629575/28124/en/Global-Trade-Credit-Insurance-Market-Report-2022-to-2030-Rapid-Digitization-of-the-Insurance-Sector-Drives-Growth.html
[11] Kemp, J., Barker, C., Good, N., Bain, M., 2022. Sequential pattern detection for identifying courses of treatment and anomalous claim behaviour in medical insurance. IEEE, pp. 3039–3046. https://doi.org/10.1109/BIBM55620.2022.9995541
[12] Hamid, Z., Khalique, F., Mahmood, S., Daud, A., Bukhari, A., Alshemaimri, B., 2024. Healthcare insurance fraud detection using data mining. BMC Med. Inform. Decis. Mak. 24, 112. https://doi.org/10.1186/s12911-024-02512-4
[13] Yu, J., Yang, X., & Zhao, J. (2023). Detecting Anomalies in Health Insurance Claim Data with Unsupervised Machine Learning. IEEE Access, 11, 76601–76612. https://doi.org/10.1109/ACCESS.2023.3291234
[14] Wang, H., Zhang, Y., & Li, P. (2022). Fraud detection in health insurance claims using deep learning techniques. Applied Intelligence, 52(6), 5678–5693. https://doi.org/10.1007/s10489-021-02821-4
[15] Singh, A., Gupta, R., & Kumar, N. (2021). Big data analytics in insurance: Transforming fraud detection and risk assessment. Journal of Big Data, 8(1), 114. https://doi.org/10.1186/s40537-021-00520-7
[16] Fan, Z., Luangsodsai, A., Sinapiromsaran, K., 2024. Mass-Ratio-Average-Absolute-Deviation Based Outlier Factor for Anomaly Scoring. IEEE, pp. 488–493. https://doi.org/10.1109/JCSSE61278.2024.10613697

[17] Fan, Z., Kaitian, L., Ziyi, C., Jing, Y., 2022. Intelligent forecasting electric vehicle purchase model based on logistic and multi-objective optimization model. IEEE, pp. 752–758. https://doi.org/10.1109/ICPECA53709.2022.9718832

[18] I. I., H., M., A., U. F., S., K. I., B., D., A., N. H., D., 2024. Evaluating the Performances of Robust Logistic Regression Models in the Presence of Outliers. Afr. J. Math. Stat. Stud. 7, 320–327. https://doi.org/10.52589/AJMSS-YKDFCYQS

[19] Mardiansyah, H., Suwilo, S., Nababan, E. B., & Efendi, S. (2024). The role of Louvain-coloring clustering in the detection of fraud transactions. International Journal of Electrical and Computer Engineering (IJECE), 14(1), 608–616. https://doi.org/10.11591/ijece.v14i1.pp608-616

[20] Zaldi, M. A. A., Sitompul, O. S., Nababan, E. B., & Crispin, A. R. (2024). Twitter data extraction for food and beverage business analytics. In Proceedings of the 2nd International Conference on Technology Innovation and Its Applications (ICTIIA). IEEE. https://doi.org/10.1109/ICTIIA61827.2024.10761920.

[21] López, D., Aguilera-Martos, I., García-Bárzana, M., Herrera, F., García-Gil, D., & Luengo, J. (2023). Fusing anomaly detection with false positive mitigation methodology for predictive maintenance under multivariate time series. Information Fusion, 100, 101957. https://doi.org/10.1016/j.inffus.2023.101957

[22] Qiu, J., Shi, H., Hu, Y., & Yu, Z. (2023). Unraveling false positives in unsupervised defect detection models: A study on anomaly-free training datasets. Sensors, 23(23), 9360. https://doi.org/10.3390/s23239360

[23] Al Jallad, K., Aljnidi, M., & Desouki, M. S. (2020). Anomaly detection optimization using big data and deep learning to reduce false-positive. Journal of Big Data, 7, 1–12. https://doi.org/10.1186/s40537-020-00346-1

[24] Tax, D., & Duin, R. (2004). Support Vector Data Description. Machine Learning, 54, 45-66. https://doi.org/10.1023/B:MACH.0000008084.60811.49.

[25] Ruff, L., Vandermeulen, R. A., Görnitz, N., Deecke, L., Siddiqui, S. A., Binder, A., Müller, E., & Kloft, M. (2018). Deep one-class classification. In Proceedings of the 35th International Conference on Machine Learning (Vol. 80, pp. 4393–4402). PMLR.

[26] Anomaly Detection, in: Pascal, P., Ienco, D. (Eds.), Discovery Science, Lecture Notes in Computer Science. Springer Nature Switzerland, Cham, pp. 318–328. https://doi.org/10.1007/978-3-031-18840-4_23

[27] Huang, W., Li, Y., Xu, Z., Yao, X., Wan, R., 2024. Improved Deep Support Vector Data Description Model Using Feature Patching for Industrial Anomaly Detection. Sensors 25, 67. https://doi.org/10.3390/s25010067

[28] Jiang, R., Yang, Z., Zhao, J., 2023. A Complete Deep Support Vector Data Description for One Class Learning. IEEE Access 11, 117494–117507. https://doi.org/10.1109/ACCESS.2023.3325734

[29] Azim, E., Wang, D., Fu, Y., 2023. Deep Graph Stream SVDD: Anomaly Detection in Cyber-Physical Systems. https://doi.org/10.48550/ARXIV.2302.12918

[30] Wen, L., Gao, L., Li, X., & Zhang, Y. (2023). Deep anomaly detection for high-dimensional insurance claim data using support vector data description networks. Expert Systems with Applications, 233, 120929. https://doi.org/10.1016/j.eswa.2023.120929

[31] Sokolova, M., Japkowicz, N., & Szpakowicz, S. (2022). Automation in insurance fraud detection: Reducing manual workload with deep learning models. Decision Support Systems, 160, 113750. https://doi.org/10.1016/j.dss.2022.113750

[32] Zhang, H., Liu, Q., & Zhao, W. (2021). Efficient anomaly detection in financial claims processing using deep one-class classification models. Knowledge-Based Systems, 229, 107331. https://doi.org/10.1016/j.knosys.2021.107331

[33] Hankede, M., & Mwelwa, A. (2024). Assessing the factors causing delay by insurance companies to pay claims to customers: A case of selected Insurance Companies, and Pensions and Insurance Authority (PIA). East African Finance Journal, 3(2). https://doi.org/10.59413/eafj/v3.i2.8

[34] Kumar, R., Singh, P., & Sharma, S. (2023). Anomaly detection in delayed insurance claim submissions using machine learning. Journal of Financial Crime, 30(4), 1123–1138. https://doi.org/10.1108/JFC-05-2022-0099

[35] Chen, Y., Wu, L., & Zhang, H. (2022). Detecting irregular claim filing patterns in health insurance using temporal anomaly detection. Expert Systems with Applications, 198, 116804. https://doi.org/10.1016/j.eswa.2022.116804

[36] Alghamdi, R., & Mehmood, R. (2021). Applications of big data analytics in health insurance systems: A study on fraud detection and anomaly in claim submissions. Computers in Biology and Medicine, 140, 105095. https://doi.org/10.1016/j.compbiomed.2021.105095

[37] Patel, R., & Desai, M. (2023). Machine learning for anomaly detection in delayed insurance claims. Journal of Financial Services Analytics, 9(2), 145–162. https://doi.org/10.1080/27693236.2023.1122334

[38] Huang, Y., Chen, X., & Zhao, L. (2021). Temporal patterns in fraudulent insurance claims: Detecting delays and irregularities using deep learning models. Information Sciences, 570, 345–359. https://doi.org/10.1016/j.ins.2021.04.015

[39] Rahman, M., & Sultana, T. (2020). Anomaly detection in health insurance claims with a focus on late submissions. Health Informatics Journal, 26(4), 2762–2778. https://doi.org/10.1177/1460458220944551

[40] Harrou, F., Sun, Y., Hering, A., Madakyaru, M., & Dairi, A. (2021). Unsupervised deep learning-based process monitoring methods. In Data Analytics and Applications (pp. 193–223). Elsevier. https://doi.org/10.1016/b978-0-12-819365-5.00012-7

[41] Ahn, J., & Kim, G. (2022). Application of optimal clustering and metric learning to patch-based anomaly detection. Pattern Recognition Letters, 154, 110–115. https://doi.org/10.1016/j.patrec.2022.01.017

[42] Zhou, Y., Liang, X., Zhang, W., Zhang, L., & Song, X. (2021). VAE-based Deep SVDD for anomaly detection. Neurocomputing, 453, 131–140. https://doi.org/10.1016/j.neucom.2021.04.089

[43] Liu, C., & Gryllias, K. (2021). A Deep Support Vector Data Description Method for Anomaly Detection in Helicopters. Prognostics and Health Management Conference, 6(1), 9. https://doi.org/10.36001/PHME.2021.V6I1.2957

[44] Noji, Y., Kimura, T., & Cheng, J. (2023). Anomaly Web Page Detection Using HDBSCAN and Deep SVDD. 2023 International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan), 465–466. https://doi.org/10.1109/ICCE-Taiwan58799.2023.10226803

[45] Jia, Y., Cheng, J., Liu, H., & Hou, J. (2024). Towards Calibrated Deep Clustering Network. ArXiv preprint arXiv:2403.02998. https://doi.org/10.48550/arXiv.2403.02998

[46] Joeres, R., Blumenthal, D.B., Kalinina, O.V., 2025. Data splitting to avoid information leakage with DataSAIL. Nat. Commun. 16, 3337. https://doi.org/10.1038/s41467-025-58606-8

BIBLIOGRAPHY OF AUTHORS

Sari Ramadhana, S.Kom. was born in Medan on February 5, 1996. She is a professional specializing in Information Technology, Business Analysis, and Risk Management. She earned her Bachelor's degree in Information Technology from Universitas Sumatera Utara in 2018 and is currently pursuing a Master's degree in Data Science and Artificial Intelligence at the same university since 2023. Sari has accumulated professional experience across the banking, insurance, and aviation sectors, with a focus on business analysis, digital system implementation, risk governance, and digital transformation of business processes. With this background, she is dedicated to driving organizational growth through the strategic use of technology and sustainable risk management practices.

Dr. Erna Budhiarti Nababan is an experienced lecturer in the Master's Program in Data Science and Artificial Intelligence at Universitas Sumatera Utara. Born in Bandung on October 26, 1962, she brings a wealth of knowledge and experience to her students. Her academic journey includes a Bachelor's degree in Electrical Engineering from IKIP Bandung, a Master's in Industrial Computing from Universiti Kebangsaan Malaysia, and a Doctorate in Systems Science and Management from the same institution. With expertise in Artificial Intelligence, Machine Learning, and Optimization, Dr. Erna is dedicated to fostering a dynamic learning environment that encourages students to explore innovative solutions in data science.

Prof. Dr. Drs. Opim Salim, M.Sc. was born in Medan on August 17, 1961. He is a lecturer in Information Technology at Universitas Sumatera Utara. He completed his highest education with a Doctorate in Information Science at Universiti Kebangsaan Malaysia (UKM) in 2005.