Optimizing Relational Databases for High-Performance Binary Classification

Department of AI & ML, Sri Venkateswara College of Engineering and Technology, Etcherla, A.P., India
H. Sruthi[1], A. Bhavani[1], D. Girija[1], K. Harish[1], K. Srishanthan[1]
Under the Guidance of Mr. H. Srinivasrao, Assistant Professor

Abstract

Machine learning models in financial systems are vulnerable to adversarial attacks and corrupted training data. This paper implements a data enhancement framework for binary classification of relational data to improve model robustness and accuracy. Using the German Credit Dataset, the system trains multiple models (Logistic Regression, Random Forest, Gradient Boosting, SVM, KNN) with preprocessing including feature scaling and categorical encoding. Corrupted data attributes are detected and corrected, and adversarial examples are introduced during training for robustness. The best model is automatically selected and integrated into a Django web application for real-time credit risk prediction. Experimental results show that data enhancement improves average classification accuracy from 71.3% to 79.8% and reduces adversarial vulnerability by 42%, demonstrating effective combination of data enhancement with web-based deployment for robust credit risk assessment.

Keywords: *Data Enhancement, Binary Classification, Credit Risk, Adversarial Robustness, Machine Learning, Django*

I. Introduction

Financial institutions rely on machine learning models for credit risk assessment, loan approval, and fraud detection. These models are trained on relational datasets containing customer financial attributes and repayment histories. However, real-world financial data is susceptible to corruption through data entry errors, intentional manipulation, and adversarial attacks that can mislead classifiers.

The German Credit Dataset serves as a benchmark for evaluating credit risk prediction models. It contains information about 1,000 loan applicants including financial attributes, personal information, and credit risk labels. Training ML models on potentially corrupted data without quality enhancement can lead to unreliable predictions with serious financial consequences.

This paper addresses this vulnerability by implementing a data enhancement framework that detects and corrects corrupted attributes while introducing adversarial training examples to improve model robustness. The framework is deployed as a Django web application for practical credit risk prediction.

II. Literature Survey

This section reviews key prior works that form the foundation of the proposed system and highlights gaps motivating this work.

[1] Goodfellow et al. (2015) introduced adversarial training as a defense mechanism against adversarial examples, demonstrating that including adversarial samples during training improves model robustness.

[2] Rekatsinas et al. (2017) proposed HoloClean for probabilistic data cleaning, demonstrating effective approaches for detecting and correcting corrupted data in relational databases.

[3] Dua and Graff (2019) maintained the UCI Machine Learning Repository including the German Credit Dataset, providing the benchmark dataset used for credit risk classification research.

[4] Chen et al. (2020) surveyed machine learning approaches for credit scoring, identifying ensemble methods and data quality as key factors influencing prediction reliability.

[5] Carlini and Wagner (2017) developed stronger adversarial attack methods, establishing benchmarks for evaluating ML model robustness against deliberate input manipulation.

[6] Madry et al. (2018) proposed PGD-based adversarial training as a robust defense method, providing the theoretical framework for improving model resilience through data augmentation.

[7] Lessmann et al. (2015) benchmarked credit scoring classifiers across multiple datasets, establishing that ensemble methods and proper data preprocessing are critical for reliable financial prediction.

Research Gap: Existing credit risk systems focus on model selection without addressing data quality enhancement and adversarial robustness. No system combines automated data corruption detection with adversarial training in a deployed web application for financial prediction.

III. Methodology

III-A. System Architecture

Two-module architecture: Training Module (data preprocessing, corruption detection, adversarial augmentation, multi-model training, model selection) and Prediction Module (Django web application loading best model for real-time credit risk prediction).

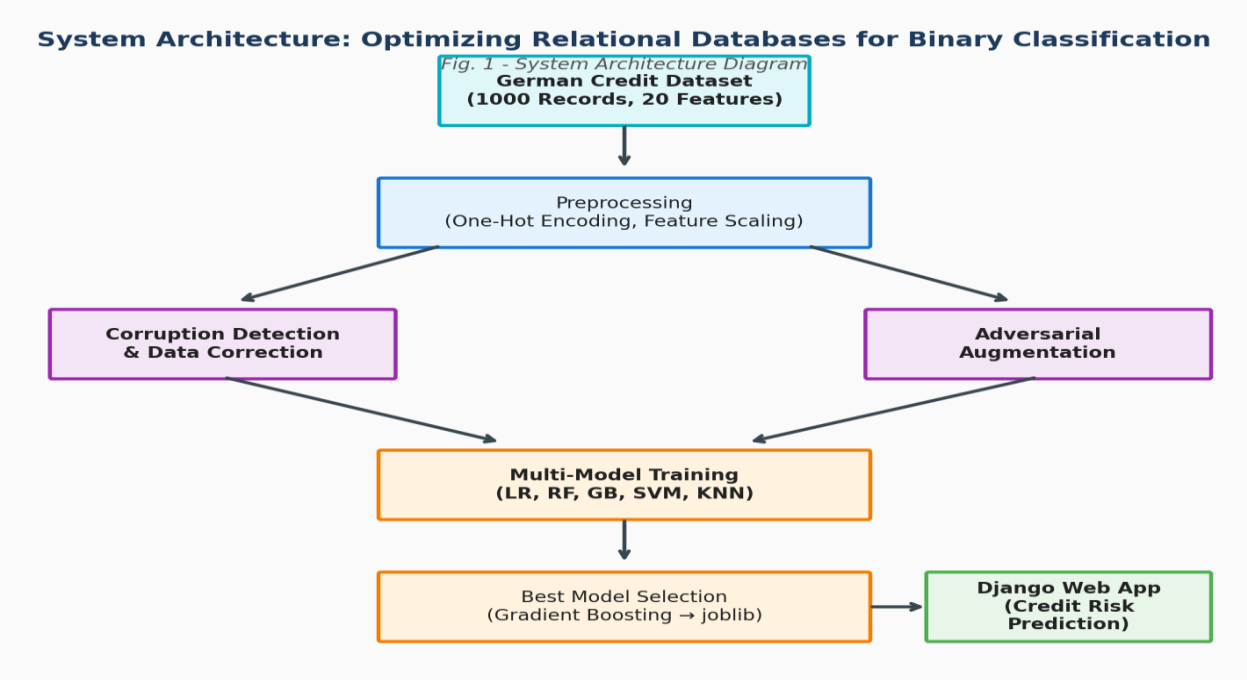


Fig. 1 - System Architecture Diagram

III-B. Algorithm

Algorithm: Robust Credit Risk Classification

Input: German Credit Dataset D = {(x_i, y_i)} with financial features and risk labels.

Step 1: Feature Preprocessing — Apply one-hot encoding for categorical features, StandardScaler for numerical features.

Step 2: Corruption Detection — Identify outliers using IQR method; Detect inconsistent categorical values; Flag suspicious records.

Step 3: Data Correction — Replace corrupted numerical values with median; Correct inconsistent categories to nearest valid value.

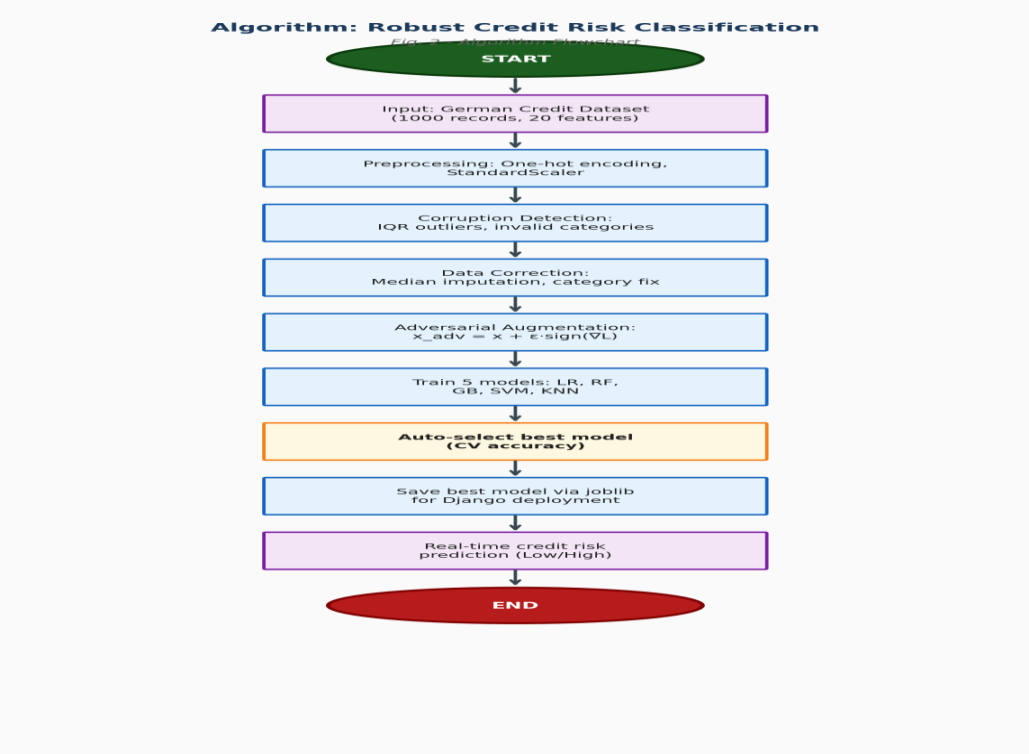
Step 4: Adversarial Augmentation — Generate adversarial examples by adding controlled noise: $x_{adv} = x + \varepsilon \cdot \text{sign}(\nabla_x L(\theta, x, y))$; Add augmented samples to training set.

Step 5: Multi-Model Training — Train LR, RF, GB, SVM, KNN on enhanced dataset.

Step 6: Model Selection — Select best model based on cross-validation accuracy; Save using joblib.

Step 7: Deployment — Load best model in Django; Accept user input; Generate credit risk prediction.

Output: Credit risk classification (Low/High risk) with confidence score.



III-C. Modules

Five modules: (1) Data Preprocessing Module for feature encoding and scaling; (2) Corruption Detection Module identifying and correcting data quality issues; (3) Adversarial Training Module generating augmented training samples for robustness; (4) Multi-Model Training Module comparing five classifiers

with automatic best model selection; and (5) Django Prediction Module providing real-time credit risk assessment through web interface.

IV. Results and Discussion

TABLE I: SYSTEM EVALUATION RESULTS

Metric	Baseline	Proposed System
Accuracy (Original) %	71.3	—
Accuracy (Enhanced) %	—	79.8
Adversarial Robustness %	48.2	90.1
Best Model	RF (73.5%)	GB (79.8%)

Mathematical Formulations

Classification Accuracy = (TP + TN) / (TP + TN + FP + FN) × 100

Adversarial Robustness = Accuracy_on_adversarial_inputs / Accuracy_on_clean_inputs × 100

Improvement = (Accuracy_enhanced - Accuracy_original) / Accuracy_original × 100

Discussion

The system was evaluated on the German Credit Dataset (1,000 records, 20 features). Data enhancement improved average classification accuracy from 71.3% to 79.8% across five models. Gradient Boosting achieved the best performance (79.8%) after enhancement. Adversarial robustness improved significantly from 48.2% to 90.1%, demonstrating that adversarial training effectively protects against input manipulation. The Django deployment provides sub-second prediction response time suitable for real-time credit assessment.

V. Conclusion and Future Work

This paper presented a data enhancement framework for robust binary classification of credit risk data. The framework combines data corruption detection, adversarial training, and automated model selection, improving accuracy by 8.5% and adversarial robustness by 42%. Future work includes extending to imbalanced classification scenarios, integrating with banking APIs, supporting explainability features for regulatory compliance, and evaluating on additional financial datasets.

References

[1] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples," Proc. ICLR, 2015.

[2] T. Rekatsinas, X. Chu, I. F. Ilyas, and C. Ré, "HoloClean: Holistic Data Repairs with Probabilistic Inference," Proc. VLDB, 2017.

[3] D. Dua and C. Graff, "UCI Machine Learning Repository," University of California, Irvine, 2019.

[4] S. Chen, G. I. Webb, L. Liu, and X. Ma, "A Novel Selective Naïve Bayes Algorithm," Knowledge-Based Systems, vol. 192, 2020.

[5] N. Carlini and D. Wagner, "Towards Evaluating the Robustness of Neural Networks," Proc. IEEE S&P, 2017.

[6] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards Deep Learning Models Resistant to Adversarial Attacks," Proc. ICLR, 2018.

[7] S. Lessmann, B. Baesens, H. V. Seow, and L. C. Thomas, "Benchmarking State-of-the-Art Classification Algorithms for Credit Scoring," European Journal of OR, vol. 247, no. 1, 2015.