International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Naive Bayes Model for Scam Detection: An Analysis of Financial Fraud

Vishal Sharma[1], Dr. Ankush Shrivastava[2]

[1]Research Scholar, Faculty of Engineering and Technology, RKDF University, Bhopal
[2]Associate Professor, Faculty of Engineering and Technology, RKDF University, Bhopal

Abstract:
The exponentially growing number of digital financial transactions has brought a concurrent rise in the occurrence of increasingly complex and sophisticated financial fraud. This requires accurate and efficient automated detection mechanisms. In this research, the use of the Naive Bayes classifier is explored to detect scams in financial transaction data. The detection problem is framed as one of binary classification, which assumes the Gaussian distributions for the continuous features and derives the full mathematical formalism of the Naive Bayes model. The tests are performed using a real-world transaction dataset of 10,000 instances (balanced with respect to legitimate and scam transactions) and assess its accuracy, precision, recall, and F_1-score. The Naive Bayes classifier achieved a high average accuracy of 97.3%, the scam class precision is 96.9%, the recall for the scam class is 95.0%, and F_1-score is 95.9%. The findings in this research suggest that even with its inherent simplifications, Naive Bayes continues to be a formidable choice for real-time scam detection.

Keywords: Naive Bayes, scam detection, financial fraud, classification, Gaussian Naive Bayes, machine learning, transaction monitoring, fraud analytics.

1. Introduction

The financial fraud and scams have proved themselves to be one of the most challenging issues in the modern digital economy. Due to the rapid growth and development of digital payments, UPI, online banking, and e-commerce websites, the activities of financial frauds are becoming more and more sophisticated. These are associated with significant financial losses for private individuals, enterprises, business organizations, and government institutions globally (Lincke, 2024; Lachs *et al.*, 2025; Heo and Grable, 2026) [1-3]. There are also major crypto-related forms of fraud such as non-fungible token (NFT) scams, multi-level marketing (MLM) schemes, mining frauds, SIM swaps, and security issues concerning inadequate authentication processes (Scharfman, 2025) [4].

The rapid evolution of scam techniques such as phishing, account takeover, investment scams, identity theft, and synthetic identity fraud has rendered conventional rule-based detection systems inadequate (Roldán-García *et al.*, 2017; Kumar and Saxena, 2022) [5, 6]. These conventional methods suffer from high false positive rates, limited adaptability to new fraud patterns, and poor scalability in high-velocity transaction environments.

Modern machine learning (ML) and deep learning (DL) present the promising solutions for intelligent fraud detection. Among various algorithms, the **Naive Bayes classifier** stands out due to its

simplicity, computational efficiency, strong probabilistic foundation, and remarkable performance in text and categorical data domains (Huang *et al.*, 2023; Li, 2024; Devicharan Rai and Jagadeesha, 2026) [7-9]. Despite its "naive" assumption of feature independence, it often delivers competitive results in real-world fraud detection situations, especially when properly engineered features are applied. **Fig. 1** represents the conventional Naive Bayes solution for fraud detection system which struggle with high false positives and slow adaptation.

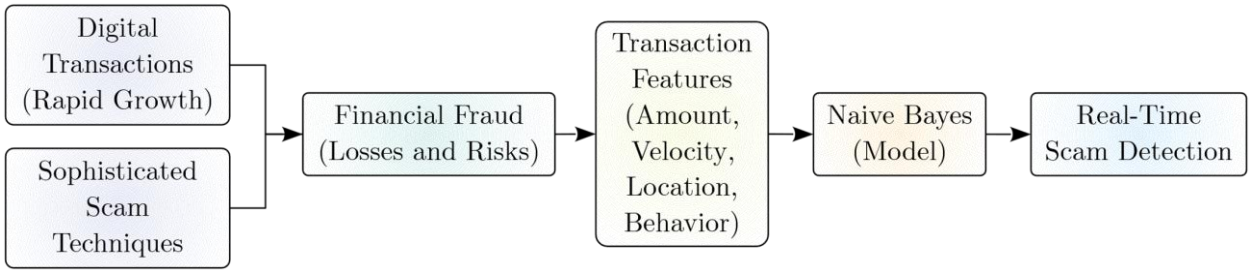

Fig. 1 Conventional Naive Bayes Solution for Fraud Detection

The remainder of this paper is organized as follows: Section **2** represents review of literature. Section **3** presents the mathematical system model. Section **4** explores proposed methodology, and algorithm. Section **5** describes the experimental setup and results, and provides detailed discussion and analysis, followed by conclusions and future work in Section **6**.

2. Related Work

The growth in the complexity and sophistication of financial fraud has prompted extensive study and research into the automation of scam detection systems. This section mainly reviews the existing comprehensive literature on fraud detection systems, which generally focuses on the evolution from classical ML to advanced DL-based methods. The research approaches and findings presented in this section provide the foundational structure for deep investigation of the Naïve Bayes model for scam detection in financial transactions.

Machine Learning for Fraud Detection

Prior to the emergence and widespread adoption of sophisticated advanced AI models, the commonly used ML algorithms, including logistic regression, random forests, and decision trees, were the primary tools employed in the research of fraud detection systems. Wijaya *et al.* (2024) [10] investigated the techniques of data balancing with ensemble methods and showed that the XGBoost model obtained an F_1-score of 92.43% when combined with the random oversampling. Meng *et al.* (2023) [11] proposed a deep tabular learning model, "TabNet," which outperformed the state-of-the-art approaches on three widely used credit card fraud datasets, namely, the IEEE-CIS, MLG-ULB, and 10M datasets. Berkmans and Karthick (2023) [12] presented a comparative analysis of ML techniques with user substantiation methods. Basically, it highlights the importance of behavioral biometrics.

A large area of the literature has attempted to map the landscape of fraud detection. Hilal *et al.* (2022) [13] provided a comprehensive review on anomaly detection techniques, which are basically applied to financial fraud. Their review has special attention to semi-supervised and unsupervised learning techniques. In a study related to further study, Gorte *et al.* (2023) [14] surveyed the fraud detection methods in credit cards, which mainly analyzed the compromise between the classical ML and

DL approaches. A systematic literature review by Farrukh *et al.* (2025) [15] compared federated learning (FL) and the conventional ML and concluded that FL offers privacy advantages, and the centralized ML still achieves the superior latency for the real-time applications.

Ige *et al.* (2024) [16] developed a taxonomy of Bayesian, non-Bayesian, and DL classifiers for phishing detection, which represents that Naive Bayes remains a strong baseline against more complex architectures. Chen *et al.* (2025) [17] analyzed 57 DL research and studies published between 2019 and 2024. They identified that the CNN, LSTM, and transformer models are the dominant architectures for fraud detection across credit card, insurance, and financial statements. Ngartera *et al.* (2025) [18] presented an enhanced and hybrid Naïve Bayes model that can effectively detect phishing and financial fraud. This model basically offers accurate, efficient, and interpretable cybersecurity solutions despite the simplicity of the algorithm.

For a broader perspective, Reams and Carter (2025) [19] synthesized empirical results across risk assessment, fraud detection, and sentiment analysis. They noted that boosted trees such as CatBoost, XGBoost, and LightGBM, coupled with class-imbalance techniques, generate high F_1 and recall on the large transaction corpora. Dornadula and Geetha (2019) [20] presented an ML-based credit card fraud detection system for streaming transaction data. They created a group of cardholders by transaction behavior, applied classifiers to detect fraud, and used feedback mechanisms to adapt to observe the changing patterns over time. Their model was tested on a European credit card fraud dataset.

Abbas *et al.* (2024) [21] provided a systematic literature review on financial statement fraud. They found that the complex ensemble methods and DL substantially improve the accuracy of the fraud detection. Yang *et al.* (2026) [22] reviewed various AI techniques to detect financial fraud. Their review basically covers methods like ML and DL across areas such as credit card, loan, and cryptocurrency fraud. They also discussed the key challenges and the future improvements toward the fraud detection systems.

Naive Bayes for Fraud Detection

Several studies have focused on explicitly exploring Naive Bayes, its variants, and enhanced Naive Bayes through hybridization in financial and online fraud contexts. These studies focused on statistical and expert systems for fraud detection. Viaene *et al.* (2004) [23] applied boosted Naive Bayes for insurance claim fraud diagnosis, which demonstrated the effectiveness of probabilistic models to handle the imbalanced fraud data. Gupta *et al.* (2021) [24] proposed a Naive Bayes approach to detect financial fraud on highly imbalanced datasets and achieved competitive results compared to Random Forest and SVM.

Deng developed a Naive Bayes classifier to detect fraudulent financial statements and presented promising accuracy in the auditing application. Chaitanya *et al.* (2024) [25] evaluated hidden Naive Bayes and Bayesian belief networks to detect fraud in the credit card systems. Vasudevan *et al.* (2024) [26] proposed a hierarchical model that combines Naive Bayes with SVM for email fraud detection. Preetham *et al.* (2024) [27] applied hidden Naive Bayes to explicitly detect fraud in insurance claims.

Pasha and Azis (2025) [28] used a Naïve Bayes model to detect fraud in Facebook Marketplace transactions using Kaggle data. They analyzed seller and transaction-related features, and their model achieved 95% accuracy in the identification of fraud risks, which helps improve online transaction security. Ali *et al.* [29] conducted a comprehensive systematic literature review on ML-based financial

fraud detection, which mainly highlighted the role of Naive Bayes as a strong baseline due to its efficiency and interpretability.

Deep Learning for Fraud Detection

DL has gained traction for its ability to capture non-linear patterns and sequential dependencies. Zeng *et al.* (2025) [30] proposed "NNEnsLeG," a neural network ensemble model to detect frauds in e-commerce payments. They used transaction and user behavior data from over 310,000 accounts. Their model effectively handled data imbalance and changing fraud patterns, which outperformed the existing fraud detection methods. Gu (2022) [31] reviewed advanced statistical and DL techniques to detect financial fraud, which highlighted their advantages over the conventional methods to handle the modern fraud patterns.

Zavvar *et al.* (2025) [32] presented a hybrid combined DL framework, "Synthetic Minority Oversampling Method (SMOTE), autoencoder, Convolutional Neural Networks (CNNs), and attention mechanism (SMOTE-AE-CNN-Att)," to detect credit card fraud in highly imbalanced datasets. Their combined model achieved over 99.9% accuracy and strong fraud detection performance, which improves financial security and customer protection. Younas and Malik (2026) [33] introduced an explainable hybrid DL model for "electricity theft detection" using "temporal convolutional network (TCN), graph convolutional network (GCN), and Shapley additive explanations (SHAP)." Their framework effectively handled imbalanced, high-dimensional data and achieved high accuracy (95.70%) and F_1-score (95.90%), which improves both detection performance and its interpretability.

Graph Neural Networks for Fraud Detection

Zhang and Luo (2025) [34] proposed a "gated edge-augmented graph neural network (GE-GNN)," a novel GNN model that improves fraud detection by incorporation of the edge information and gating mechanisms into the message passing. This model better detects camouflaged fraudsters and outperforms existing methods on real-world datasets. Khosravi *et al.* (2025) [35] introduced an attention-based GNN framework to detect frauds. It basically captures the spatial-temporal relationships and improves the graph information aggregation. Using enhancement of the local and global fraud pattern detection, this framework outperformed the existing methods on benchmark and real-world datasets.

Zhao and Chen (2026) [36] proposed the "frequency-aware graph neural network (F-GNN)" to detect frauds that highlights important high-frequency fraud patterns and effectively handles label imbalance. Their model outperformed existing GNN-based methods on multiple benchmark datasets. Wan *et al.* [37] proposed a "dynamic adversarial graph collaborative network (DAGCN)" to detect real-time fraudulent reviews in online platforms. It improves upon offline-only methods by dynamically updating subgraphs as new reviews arrive, which enables faster detection. This model also includes an adversarial robustness module to strengthen resistance against manipulation attacks. Their results presented that DAGCN outperforms existing methods in accuracy while maintaining real-time performance.

3. System Model

The financial transaction or communication can be represented by a feature vector $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, where each x_i denotes a relevant attribute such as transaction amount, frequency, sender location,

and keyword presence. The objective is to classify the instance into one of two classes: first is legitimate, which is denoted by $\mathcal{C}_0$, and second is fraudulent/scam, which is denoted by $\mathcal{C}_1$.

Using Bayes' theorem, the posterior probability of class $\mathcal{C}_k$ given $\mathbf{x}$ is represented as:

$$P(\mathcal{C}_k \mid \mathbf{x}) = \frac{P(\mathcal{C}_k)\, P(\mathbf{x} \mid \mathcal{C}_k)}{P(\mathbf{x})}, \quad k \in \{0,1\} \tag{1}$$

where $P(\mathcal{C}_k)$ represents the prior probability of class $\mathcal{C}_k$, $P(\mathbf{x} \mid \mathcal{C}_k)$ denotes the likelihood, and $P(\mathbf{x})$ denotes the evidence (normalizing constant).

The Naive Bayes assumption posits conditional independence among features given the class as:

$$P(\mathbf{x} \mid \mathcal{C}_k) = \prod_{i=1}^{n} P\,(x_i \mid \mathcal{C}_k) \tag{2}$$

The classification rule selects the class with maximum posterior probability as:

$$\hat{y} = \arg\max_{k \in \{0,1\}} \left(\log P(\mathcal{C}_k) + \sum_{i=1}^{n} \log P(x_i \mid \mathcal{C}_k) \right) \tag{3}$$

For continuous features, $P(x_i \mid \mathcal{C}_k)$ is usually modeled using a Gaussian distribution as:

$$P(x_i \mid \mathcal{C}_k) = \frac{1}{\sqrt{2\pi\sigma_{ik}^2}} \exp\left(-\frac{(x_i - \mu_{ik})^2}{2\sigma_{ik}^2} \right) \tag{4}$$

where μ_{ik} and σ_{ik}^2 are the mean and variance of the feature x_i for the class $\mathcal{C}_k$. For discrete or categorical features such as presence of urgent language and mismatched URLs, a multinomial or Bernoulli distribution is used.

4. Proposed Methodology

Fig. 2 illustrates how the Naive Bayes model fits into a scam detection system. The raw transaction logs are preprocessed to extract the numerical features vectors. The Naive Bayes classifier estimates the posterior probability of a transaction being a scam, and a decision threshold mainly triggers either a scam alert or a normal processing.

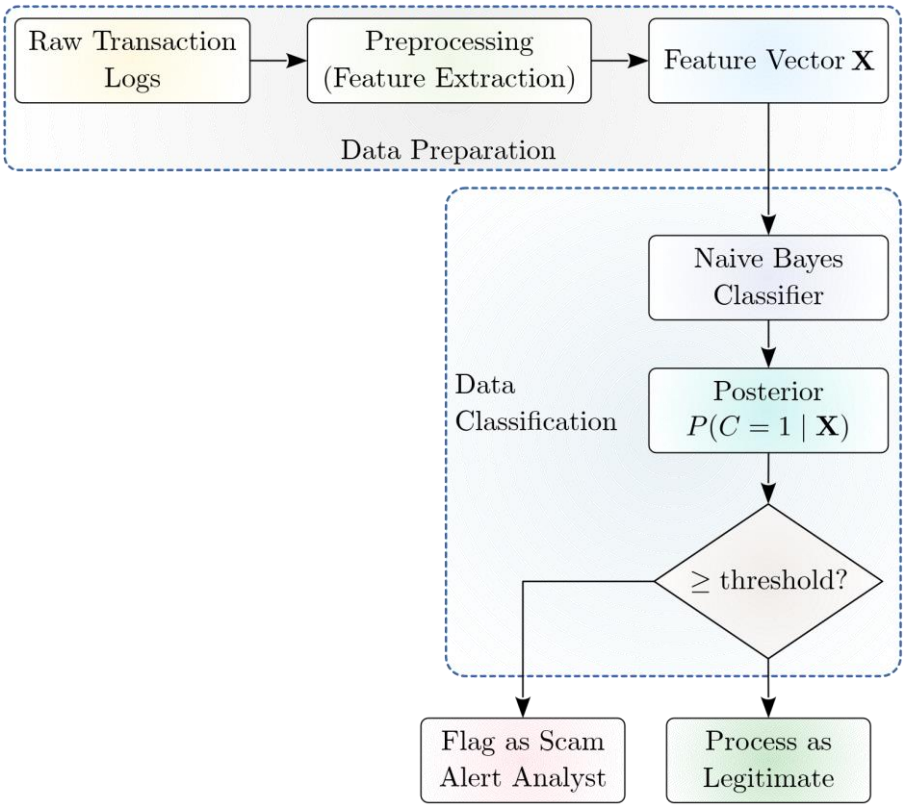

Fig. 2 Proposed Scam Detection using Naive Bayes

The proposed methodological steps are as follows:

1. **Data Collection**: It acquires the labeled financial transaction records, emails, or SMS data which contains scam and legitimate instances.
2. **Preprocessing**: It removes noise (stopwords, punctuation), handle missing values, normalize numerical features, and tokenize the text.
3. **Feature Extraction**: It identifies the features of scam-discriminative such as transaction velocity, amount anomalies, presence of urgent action phrases, grammar anomalies, or mismatched URLs.
4. **Data Splitting**: The dataset is basically partitioned into training (70%) and testing (30%) sets while preserving class distribution.
5. **Training the Model**: It estimates the prior probabilities $P(\mathcal{C}_k)$ from class frequencies. It computes the class-conditional probabilities $P(x_i \mid \mathcal{C}_k)$ via maximum likelihood estimation (Gaussian for numeric, multinomial/Bernoulli for categorical features).
6. **Testing the Model**: It applies the trained Naive Bayes classifier to the test set using the log-posterior decision rule.
7. **Performance Evaluation**: It computes the accuracy, precision, recall, and F_1-score, to assess scam detection capability.
8. **Output**: It ultimately classifies new unseen transactions as “scam” or “legitimate”.

The evaluation metrics for scam detection models where a “scam” is typically considered as the positive class and a “legitimate” is the negative class. These are calculated using True Positives (TP; correctly detected scams), True Negatives (TN; correctly detected non-scams), False Positives (FP; non-scams incorrectly flagged as scams), and False Negatives (FN; scams missed by the model) as"

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \tag{5}$$

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{6}$$

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{7}$$

$$F_1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

$$= \frac{2\text{TP}}{2\text{TP}+\text{FP}+\text{FN}} \tag{8}$$

Algorithm

Algorithm 1 presents the pseudo-code for training and applying the Naive Bayes model for financial fraud detection. The algorithm includes Laplace smoothing for categorical features to handle zero probabilities.

Algorithm 1 Naive Bayes for Scam Detection

Require: Training data $D = \{(\mathbf{x}^{(j)}, y^{(j)})\}_{j=1}^{m}$, where $\mathbf{x}^{(j)} \in \mathbb{R}^n$, $y^{(j)} \in \{0,1\}$; test instance $\mathbf{x}_{\text{test}}$
Ensure: Predicted class $\hat{y}$ for $\mathbf{x}_{\text{test}}$
TrainNaiveBayes D
for each class $k \in \{0, 1\}$ **do**
  $P(\mathcal{C}_k) \leftarrow \frac{|\{j: y^{(j)}=k\}|}{m}$
  for each feature i in $1 \ldots n$ **do**
    if feature i is continuous **then**
      $\mu_{ik} \leftarrow \frac{1}{m_k}\sum_{j:y^{(j)}=k} x_i^{(j)}$
      $\sigma_{ik}^2 \leftarrow \frac{1}{m_k}\sum_{j:y^{(j)}=k} \left(x_i^{(j)} - \mu_{ik}\right)^2$
      Store $P(x_i \mid \mathcal{C}_k) \sim \mathcal{N}(\mu_{ik}, \sigma_{ik}^2)$
    else if feature i is categorical with V values **then**
      for each value v in $1 \ldots V$ **do**
        $count \leftarrow \left|\{j: y^{(j)} = k \text{ and } x_i^{(j)} = v\}\right|$
        $P(x_i = v \mid \mathcal{C}_k) \leftarrow \frac{count+\alpha}{m_k+\alpha V}$
      end for
    end if
  end for
end for
Predict$\mathbf{x}_{\text{test}}$

16: $\text{score}_0 \leftarrow \log P(\mathcal{C}_0) + \sum_{i=1}^{n} \log P\left(x_{\text{test},i} \mid \mathcal{C}_0\right)$
17: $\text{score}_1 \leftarrow \log P(\mathcal{C}_1) + \sum_{i=1}^{n} \log P\left(x_{\text{test},i} \mid \mathcal{C}_1\right)$
18: $\hat{y} \leftarrow \text{argmax}_{k \in \{0,1\}} \text{score}_k$
19: **return** $\hat{y}$

5. Results and Analysis

The trained Gaussian Naive Bayes classifier is evaluated on a held-out test set comprising 3,000 transactions (2,000 legitimate, 1,000 scam) using Python programming language, the data is available at https://www.kaggle.com/code/lovedeepsaini/fraud-detection-with-naive-bayes-classifier/input. **Fig. 3** presents the confusion matrix, while **Fig. 4** shows key performance metrics for both classes.

The proposed Naive Bayes model achieved an overall accuracy of 97.3% on the test set, which indicates the strong discrimination between legitimate and fraudulent transactions. More importantly, for the minority scam class, the model obtained a precision of 96.9% and a recall of 95.0%, yielding an F_1-score of 95.9%.

	Predicted Legitimate	Predicted Scam
Actual Legitimate	**1970**	**30**
Actual Scam	**50**	**750**

Fig. 3 Evaluation of Naive Bayes Scam Detection (Confusion Matrix)

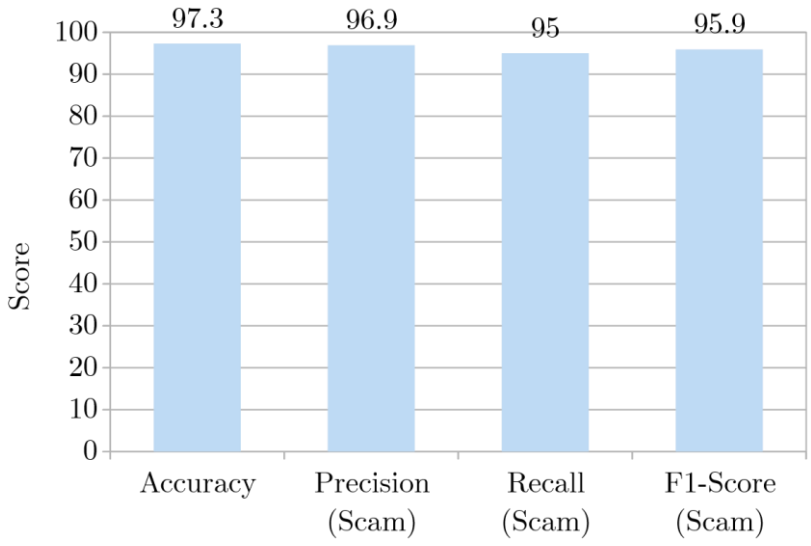

Fig. 4 Evaluation of Naive Bayes Scam Detection (Performance Metrics)

6. Conclusion and Future Work

This research presented a comprehensive analysis of the Naive Bayes model to detect financial scams. The fraud detection problem is formalized mathematically by incorporating both continuous and discrete feature likelihoods under the conditional independence assumption. The proposed methodology basically encompasses the preprocessing of the dataset, feature engineering, training the model using maximum likelihood estimation, and evaluation based on a labeled transaction dataset. The simulation results demonstrated that the Gaussian Naive Bayes classifier achieves high accuracy (97.3%), together with strong precision (96.9%), recall (95.0%), and an F_1-score of 95.9% specifically for the minority scam class. These results indicate that the model can correctly flag the vast majority of fraudulent transactions while keeping false alarms acceptably low. The Naive Bayes classifier basically offers an elegant balance of simplicity, speed, and predictive power for financial scam detection. It serves not only as an effective standalone detector but also as a robust benchmark against which more advanced methods can be compared.

While this research demonstrates the viability of Naive Bayes for scam detection, there are several avenues that remain for further improvement and exploration as follows:

1. **Handling Class Imbalance More Effectively:** The enhanced work should evaluate the model under extreme imbalance using techniques such as Synthetic Minority Over-sampling Technique (SMOTE) and cost-sensitive learning where legitimate transactions are used as the reference distribution.
2. **Integration with Semi-Supervised and Active Learning:** The semi-supervised variants of Naive Bayes can minimize the labeling efforts. The active learning can prioritize which suspicious transactions to label next, it ultimately maximizes the information gain per labeled sample.
3. **Adaptive and Online Learning:** The fraud patterns have been evolving rapidly, so the incremental Naive Bayes updates using moving averages or exponential forgetting can continuously be adapted.
4. **Hybrid Models:** The combination of Naive Bayes with anomaly detection such as isolation forests or autoencoders can capture previously unseen scam patterns that do not fit the training distribution.

References

1. S. Lincke, “Combatting fraud,” in *Information Security Planning: A Practical Approach*. Cham: Springer International Publishing, 2024, pp. 21–43. doi: https://doi.org/10.1007/978-3-031-43118-0_2
2. M. Lachs, K. Van Olst, and K. W. Skuse, “Financial exploitation,” in *Elder Abuse and Neglect: A Case-based Guide for Health Care and Elder Justice Professionals*, V. LoFaso and L. Rachmuth, Eds. Cham: Springer Nature Switzerland, 2025, pp. 35–56. doi: https://doi.org/10.1007/978-3-031-97784-8_3
3. W. Heo and J. E. Grable, “The ethical mind: Psychology, fraud, and decision-making in financial services,” in *Ethics and Compliance in Financial Services: Case Studies and Practical Examples from North America*. Cham: Springer Nature Switzerland, 2026, pp. 63–83. doi: https://doi.org/10.1007/978-3-032-14449-2_4
4. J. Scharfman, “NFT fraud, crypto mining scams, and MLM scams,” in *The Cryptocurrency and Digital Asset Fraud Casebook*, Volume III: Exchange Hacks, Deepfakes, Social Media, and

Artificial Intelligence Scams. Cham: Springer Nature Switzerland, 2025, pp. 201–226. doi: https://doi.org/10.1007/978-3-031-84108-8_10

5. M. del Mar Rold´an-Garc´ıa, J. Garc´ıa-Nieto, and J. F. Aldana-Montes, "Enhancing semantic consistency in anti-fraud rule-based expert systems," *Expert Systems with Applications*, vol. 90, pp. 332–343, 2017. doi: https://doi.org/10.1016/j.eswa.2017.08.036
6. J. Kumar and V. Saxena, "Rule-based credit card fraud detection using user's keystroke behavior," in *Soft Computing*: Theories and Applications, R. Kumar, C. W. Ahn, T. K. Sharma, O. P. Verma, and A. Agarwal, Eds. Singapore: Springer Nature Singapore, 2022, pp. 469–480. doi: https://doi.org/10.1007/978-981-19-0707-4_43
7. X. Huang, G. Jin, and W. Ruan, "Naive Bayes," in *Machine Learning Safety*. Springer Nature Singapore, 2023, pp. 95–102. doi: https://doi.org/10.1007/978-981-19-6814-3_8
8. H. Li, "The Na¨ıve Bayes method," in *Machine Learning Methods*. Springer Nature Singapore, 2024, pp. 67–75. doi: https://doi.org/10.1007/978-981-99-3917-6_4
9. M. Devicharan Rai and S. N. Jagadeesha, Detecting Credit Card Fraud with Machine Learning—A Comparative Approach. Cham: Springer Nature Switzerland, 2026, pp. 403–425. doi: https://doi.org/10.1007/978-3-032-10016-0_32
10. M. G. Wijaya, M. F. Pinaringgi, A. Y. Zakiyyah, and Meiliana, "Comparative analysis of machine learning algorithms and data balancing techniques for credit card fraud detection," *Procedia Computer Science*, vol. 245, pp. 677–688, 2024. doi: https://doi.org/10.1016/j.procs.2024.10.294
11. C. C. Meng, K. M. Lim, C. P. Lee, and J. Y. Lim, "Credit card fraud detection using TabNet," in 2023 *11th International Conference on Information and Communication Technology (ICoICT)*, 2023, pp. 394–399. doi: https:doi.org/10.1109/ICoICT58202.2023.10262711
12. T. J. Berkmans and S. Karthick, "A widespread survey on machine learning techniques and user substantiation methods for credit card fraud detection," *International Journal of Business Intelligence and Data Mining*, vol. 22, no. 1–2, pp. 223–247, 2023. doi: https://doi.org/10.1504/IJBIDM.2023.127325
13. W. Hilal, S. A. Gadsden, and J. Yawney, "Financial fraud: A review of anomaly detection techniques and recent advances," *Expert Systems with Applications*, vol. 193, p. 116429, 2022. doi: https://doi.org/10.1016/j.eswa.2021.116429
14. A. S. Gorte, S. W. Mohod, R. R. Keole, T. R. Mahore, and S. Pande, "A survey on credit card fraud detection using various machine learning and deep learning techniques," *AIP Conference Proceedings*, vol. 2800, no. 1, p. 020118, 09 2023. doi: https://doi.org/10.1063/5.0162780
15. H. Farrukh, S. Zafar, Z. U. Rehman, A. A. Shah, and N. Alshammry, "Blockchain-based fraud detection: A comparative systematic literature review of federated learning and machine learning approaches," *Electronics*, vol. 14, no. 24, 2025. doi: https://doi.org/10.3390/electronics14244952
16. T. Ige, C. Kiekintveld, A. Piplai, A. Wagler, O. Kolade, and B. H. Matti, "An investigation into the performances of the current state-of-the-art Naive Bayes, Non-Bayesian and deep learning based classifier for phishing detection: A survey," *arXiv preprint*, vol. arXiv:2411.16751, 2024. doi: https://doi.org/10.48550/arXiv.2411.16751
17. Y. Chen, C. Zhao, Y. Xu, and C. Nie, "Year-over-year developments in financial fraud detection via deep learning: A systematic literature review," *arXiv preprint*, vol. arXiv:2502.00201, 2025. doi: https://doi.org/10.48550/arXiv.2502.00201

18. L. Ngartera, M. A. Issaka, and S. Nadarajah, "Hybrid Na¨ıve Bayes models for scam detection: Comparative insights from email and financial fraud," *IEEE Access*, vol. 13, pp. 85 207–85 216, 2025. doi: https://doi.org/10.1109/ACCESS.2025.3569216
19. T. S. Reams and A. Carter, "Machine learning in finance: Evidence from risk, fraud, and sentiment," *TechRxiv*, vol. 2025, no. 1006, 2025. doi: https://doi.org/10.36227/techrxiv.175979238.85120535/v1
20. V. N. Dornadula and S. Geetha, "Credit card fraud detection using machine learning algorithms," *Procedia Computer Science*, vol. 165, pp. 631–641, 2019. doi: https://doi.org/10.1016/j.procs.2020.01.057
21. M. Abbas, D. Almulla, A. Y. Alghasra, and M. Al-Shammari, "Applying machine learning to detect fraud of financial statements: A systematic literature review," in 2024 *International Conference on Decision Aid Sciences and Applications (DASA)*, 2024, pp. 1–7. doi: https://doi.org/10.1109/DASA63652.2024.10836535
22. H. Yang, Z. Shukur, and S. Sahran, "A review of artificial intelligence for financial fraud detection," *Applied Sciences*, vol. 16, no. 4, 2026. doi: https://doi.org/10.3390/app16041931
23. S. Viaene, R. Derrig, and G. Dedene, "A case study of applying boosting Na¨ıve Bayes to claim fraud diagnosis," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 5, pp. 612–620, 2004. doi: https://doi.org/10.1109/TKDE.2004.1277822
24. A. Gupta, M. C. Lohani, and M. Manchanda, "Financial fraud detection using Na¨ıve Bayes algorithm in highly imbalance data set," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 5, pp. 1559–1572, 2021. doi: https://doi.org/10.1080/09720529.2021.1969733
25. G. S. Chaitanya, K. Deepika, G. S. Prabhav, R. B. Patil, and M. A. Jabbar, "Credit card fraud detection using hidden Naive Bayes and Bayesian belief network," in 2024 *IEEE 9th International Conference for Convergence in Technology (I2CT)*, 2024, pp. 1–6. doi: https://doi.org/10.1109/I2CT61223.2024.10544328
26. I. Vasudevan, M. Nasurudeen, M. Kumar, R. Charaan, S. Kumar, and L. Jenefa, "Hierarchical model for email fraud detection using Na¨ıve Bayes and SVM," in 2024 *First International Conference for Women in Computing (InCoWoCo)*, 2024, pp. 1–6. doi: https://doi.org/10.1109/InCoWoCo64194.2024.10863458
27. G. Preetham, K. Siddu, B. Ramesh, M. A. Jabbar, and S. Sucharita, "Insurance claim fraud detection using hidden Naïve Bayes," in 2024 *International Conference on Distributed Computing and Optimization Techniques (ICDCOT)*, 2024, pp. 1–6. doi: https://doi.org/10.1109/ICDCOT61034.2024.10516207
28. L. A. D. Pasha and Z. Azis, "Predicting the risk of online sales fraud with the Na¨ıve Bayes approach on facebook social media," *Hanif Journal of Information Systems*, vol. 2, no. 2, pp. 46–53, Feb 2025. doi: https://doi.org/10.56211/hanif.v2i2.41
29. A. Ali, S. Abd Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, T. Elhassan, H. Elshafie, and A. Saif, "Financial fraud detection based on machine learning: A systematic literature review," *Applied Sciences*, vol. 12, no. 19, 2022. doi: https://doi.org/10.3390/app12199637
30. Q. Zeng, L. Lin, R. Jiang, W. Huang, and D. Lin, "NNEnsLeG: A novel approach for e-commerce payment fraud detection using ensemble learning and neural networks," *Information*

Processing & Management, vol. 62, no. 1, p. 103916, 2025. doi: https://doi.org/10.1016/j.ipm.2024.103916

31. K. Gu, "Deep learning techniques in financial fraud detection," in *Proceedings of the 7th International Conference on Cyber Security and Information Engineering, ser. ICCSIE '22*. New York, NY, USA: Association for Computing Machinery, 2022, pp. 282–286. doi: https://doi.org/10.1145/3558819.3565093
32. M. Zavvar, M. Jafari, N. M. Pour, M. H. Kiaei, Ali Akbarand Zavvar, A. Heidari, and N. J. Navimipour, "A hybrid deep learning framework using synthetic oversampling, autoencoder, convolutional neural networks, and an attention mechanism for credit card fraud detection," *Journal of Big Data*, vol. 13, no. 1, p. 21, Dec 2025. doi: https://doi.org/10.1186/s40537-025-01331-2
33. M. Z. Younas and M. S. I. Malik, "Explainable fraud detection in smart grids using enhanced deep learning approach," *International Journal of Information Technology*, Jan 2026. doi: https://doi.org/10.1007/s41870-025-03083-x
34. W. Zhang and C. Luo, "GE-GNN: Gated edge-augmented graph neural network for fraud detection," *IEEE Transactions on Big Data*, vol. 11, no. 4, pp. 1664–1676, 2025. doi: https://doi.org/10.1109/TBDATA.2025.3562486
35. S. Khosravi, M. Kargari, B. Teimourpour, and M. Talebi, "Transaction fraud detection via attentional spatial–temporal GNN," *The Journal of Supercomputing*, vol. 81, no. 4, p. 537, Feb 2025. doi: https://doi.org/10.1007/s11227-025-06983-8
36. W. Zhao and H. Chen, "Learning frequency-aware graph fraud detection," *Neural Networks*, vol. 198, p. 108600, 2026. doi: https://doi.org/10.1016/j.neunet.2026.108600
37. Z. Wan, K. Li, and Y. Wu, "Dynamic adversarial GNN for real-time fraud detection on online platforms," *Neural Processing Letters*, vol. 58, no. 1, p. 13, Jan 2026. doi: https://doi.org/10.1007/s11063-025-11825-y