*Conference Name: International Conference on Business, Economics, Law, Language & Psychology, 21-22 June 2025, Berlin*
*Conference Dates: 21-Jun- 2025 to 22-Jun- 2025*
*Conference Venue: Online LIVE on Zoom*
*Appears in: PEOPLE: International Journal of Social Sciences (ISSN 2454-5899)*
*Publication year: 2025*

*Abu-Amara et.al, 2025*

*Volume 2025, pp.291-305*

*DOI- https://doi.org/10.20319/icssh.2025.291305*

*This paper can be cited as: Abu-Amara, F., Alhammadi, M., Alhashmi, Z.(2025). Enhancing E-Commerce Security: A Novel Approach To Credit Card Fraud Detection. International Conference on Business, Economics, Law, Language & Psychology, 21-22 June 2025, Berlin, Proceedings of Social Science and Humanities Research Association (SSHRA), 2025, 291-305*

# ENHANCING E-COMMERCE SECURITY: A NOVEL APPROACH TO CREDIT CARD FRAUD DETECTION

**Fadi Abu-Amara**
*Cybersecurity Program, Shenandoah University, Winchester, VA, USA*
*fadi.abuamara@su.edu*

**Mariam Alhammadi**
*Computer and Information Sciences Department, Higher Colleges of Technology, Abu Dhabi, UAE*

**Zainab Alhashmi**
*Computer and Information Sciences Department, Higher Colleges of Technology, Abu Dhabi, UAE*

---

## Abstract

*Credit card fraud presents a risk to businesses and their clients. To combat security breaches, organizations implement different administrative and technical security controls to protect their data. With the increasing use of online transactions, organizations implement fraud detection systems. In this paper, we propose a novel credit card fraud detection system that integrates K-Nearest Neighbors and Naive Bayes machine learning algorithms. It educates employees on adherence to company guidelines and enhances their ability to handle cyber threats. The proposed system examines online transactions and notifies administrators of suspicious transactions to act. The system is trained and tested on a dataset of 188 transactions. It achieved 94.3% accuracy, 94.4% sensitivity, and 94.1% specificity. The research findings demonstrate effectiveness of the proposed system in improving e-commerce security and safeguarding businesses and customers from this*

*risk.*

**Keywords:**

Credit Card Fraud Detection, K-Nearest Neighbors (KNN), Naive Bayes Classifier (NB), E-Commerce Security, Machine Learning, Fraud Detection System

## 1. INTRODUCTION

Credit card fraud is an issue that affects people worldwide each year [1]. In 2023, the global card fraud losses exceeded $35 billion, according to the Nilson's Report [2]. Credit card fraud negatively impacts an organization’s reputation due to its inability to protect its customer data. This fraud also may result in legal consequences from the affected customers and financial losses.

Over time, there has been an increase in credit card fraud due to the growth in online shopping and remote transactions [3]. This increase in fraudulent activities has led to a greater need for effective credit card fraud detection systems. These systems monitor normal network activities and online transactions to establish a baseline. Then, detect any suspicious behavior, unusual transactions, or security protocol breaches. They also alert the security team of detected suspicious activities.

Any credit card fraud detection system should minimize financial losses, detect suspicious activities and transactions, and alert administrators. Our proposed system has these features in addition to educating users in recognizing and reporting suspicious transactions. These capabilities aid organizations in protecting their public image and reputation.

There were several credit card fraud detection techniques and models reported in the literature. In the Background section, a number of the proposed methods are reviewed. These methods include Naive Bayes, K-Nearest Neighbor, Support Vector Machines, Bagging Ensemble, Hadoop MapReduce, and Artificial Immune Recognition System, to list a few. All these methods have their advantages and limitations.

In this research work, we propose a hybrid machine learning method that integrates the K-Nearest Neighbor and Naive Bayes classifiers for credit card fraud detection. The proposed method analyzes transaction patterns and generate an alert for any suspicious activity. This empowers the responsible entity to take actions in the real-time. The proposed detection system is trained on 168 transactions and tested on 20 transactions. The accuracy, sensitivity and specificity are used to measure performance of the proposed method. The experimental results indicate that this method is effective in enhancing e-commerce security and mitigating the financial credit card fraud losses. Furthermore, our proposed tool can be used by enterprises and individuals.

The rest of this paper is organized as follows. Section 2 explores the technical

background. The proposed fraud detection system is explored in Section 3. Section 4 discusses experimental results, while Section 5 concludes the paper.

## 2. BACKGROUND

Credit card fraud is one of the most prevalent types of fraud in the present world where technology has advanced a lot, and it impacts many consumers and businesses globally. Scammers use different techniques to get around the security measures and gather credit card details that are then used to make unauthorized purchases and cause financial damages to the victims. Traditional fraud detection methods become ineffectual as attackers of credit card fraud keep on evolving their tactics. Therefore, there is a growing need for enhanced and effective fraud detection systems.

To improve information safety, financial institutions employ efficient credit card fraud detection tools. These tools protect consumers and employees from fraudulent activities. Any used tool should accurately identify fraudulent activities and generate real-time alerts. This improves customers trust in the online trading website and preserves its reputation.

In [1], the credit fraud detection performance of different supervised machine learning models, such as logistic regression, support vector machines, and decision trees, and unsupervised machine learning models, such as clustering and anomaly detection, was analyzed. These methods exhibited better detection accuracy than traditional rule-based methods. However, they require training on a large number of labeled data, had challenges in dealing with imbalanced data, the need for continuous retraining. In another survey paper, the authors found that the ensemble and deep learning methods can be efficiently used for credit card fraud detection, since they can capture complex patterns [3]. However, they face challenges in case of rare fraudulent transactions and the need for continuous retraining.

In [5], the Synthetic Minority Oversampling Technique (SMOTE) was combined with deep learning for credit card fraud detection. The proposed method overcome class imbalance problem through creating fake data points of the minority class that represent fraudulent transactions. However, the generation of synthetic data introduces overtraining and computational cost. In [6], an ensemble-based machine learning model was proposed to detect fraudulent credit card activities. The hybrid model employed Support Vector Machine, K-Nearest Neighbor, Random Forest, Bagging, and Boosting

classifiers. Under sampling and smote method were combined to overcome class imbalance. However, the proposed method was trained on a specific dataset.

Various explainable AI (XAI) methods, such as SHapley Additive exPlanations and Local Interpretable Model-agnostic Explanations, used to increase transparency of the deep learning models for credit card fraud detection [7]. However, these methods are computationally expensive with increased difficulty of interpreting explanations for highly complex models. In [8], the Generative Adversarial Networks (GAN) was used to overcome data imbalance that resulted from having fewer fraudulent transactions than the legitimate ones. The generated fraudulent transactions improved training the fraud detection model. However, the training process is complex and there is a need for manual evaluation of the generated synthetic data.

Another work proposed a credit card fraud detection system that integrated streaming analytics and machine learning [9]. The proposed system integrated Apache Kafka, Apache Spark, and Random Forests for data ingestion, data processing, and fraud detection. The study used only one database and lacked comparison with relevant algorithms. In [10], a credit card fraud detection system used the k-Nearest Neighbors classifier. The system used transaction amount and the location of the transaction as indicators of fraud.

Another work reviewed 75 articles that used deep learning models in credit card fraud detection based on user's behavior [11]. The explored machine learning models used behavioral biometrics, such as location, amount, and time, and anomaly detection to flag fraudulent activities. The survey paper concluded that the existing techniques are not sufficient to deal with the ever-increasing frauds. In [12], a hybrid model was proposed that combined autoencoder method for feature learning, classification model for fraud identification, and secure aggregation for data privacy. The federated model was used in multiple banks to mitigate credit card fraud detection. The model trained on artificial scenarios and assumed all banks have similar data distribution.

A blockchain-based model integrated with machine learning was proposed to detect fraudulent credit card activities [13]. Transparency and security of online transactions were improved. However, the proposed model is limited in handling increased transaction scalability and associated with implementation costs. In [14], a hybrid model was proposed for credit card fraud detection that integrated two deep learning models:

LightGBM and AdaBoost. However, it was limited to a specific data set. In [15], different supervised learning algorithms, such as Logistic Regression, Support Vector Machines, and Random Forest, were employed to identify fraudulent transactions. The Random Forest model had the highest credit card fraud detection accuracy. It suggested considered other data such as credit history and behavioral data to improve detection accuracy.

## 3. PROPOSED FRAUD DETECTION METHOD

In this section, the proposed credit card fraud detection method is explored. It integrates the K- Nearest Neighbors (KNN) and Naive Bayes (NB) Classifiers to exploit their strengths and compensate for their weaknesses. This integration aims at developing a robust credit card fraud detection method.

### 3.1. K-Nearest Neighbors Algorithm

The KNN algorithm is used in many applications, including classification and regression. In this research work, we used the KNN to classify online transactions into normal or fraud. During the supervised training phase, the KNN is trained to recognize normal and fraudulent transactions. During the testing phase, the KNN calculates the distance between a suspected transaction and all previously labelled transactions. This results in identifying the K nearest neighbors to that transaction. Based on the category of the nearest neighbors, the transaction is classified. Figure 1 shows the steps the KNN follow in classifying a transaction as normal or fraudulent.

### 3.2. Naive Bayes Classifier (NB)

The Naive Bayes Classifier (NB) is a machine learning method that is used in binary and multi- class classification applications. In this research work, we used the NB for binary classification of a transaction into normal or fraudulent. NB extracts features from a transaction, such as time, amount, and location, and then calculates the probability of that transaction falling into each class. Finally, the transaction is categorized into the class with the maximum probability.

Figure 2 shows the steps the Naïve Bayes follow in classifying a transaction as normal or fraudulent. First, it gathers customer details, payment information, order details, and device information for the corresponding transaction. Next, it breaks down the corresponding transaction into tokens (individual components) for further analysis. Then,

it converts a few variables, such as country, into numerical values. It also combines some features. For example, it calculates total order value. It also normalizes numerical features into a common scale. The next step includes utilizing the database of historical transactions to calculate the probability of each extracted feature. Finally, it assigns risk scores for each feature.

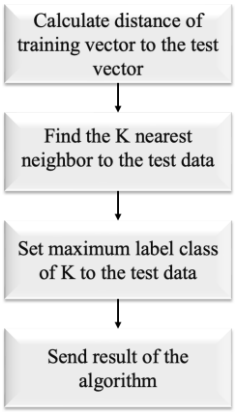


**Fig. 1** *K-Nearest Algorithm*

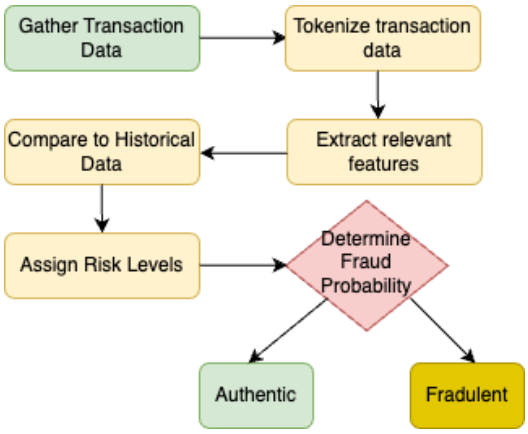


**Fig. 2** *Naive Bayes Classifier*

### 3.3. Combining KNN and NB

The KNN excels at handling noisy data, and it doesn't require any explicit model training. However, KNN exhibits slow performance when dealing with large datasets. On the other hand, the NB performs well with large datasets. However, its classification performance is affected by feature redundancy and noisy features.

To overcome the limitations of KNN and NB, the proposed credit card fraud detection method integrates the KNN and NB to improve the detection accuracy. The KNN excels in capturing data local trends, while NB provides a general view of the data. The

hybrid model produces its final classification using a voting strategy of the outputs of KNN and BN. This integrates benefits of KNN and BN and offsets their limitations, which results a more stable and accurate credit card fraud detection. If the two classifiers produce different classification results, the transaction is marked as suspicious, and the administrator is notified.

### 3.4. User login and Purchase

Figure 3 shows the user's login, authentication, and purchase processes. If the user doesn't have an account, they are asked to sign up with a strong password. Next, the user logins to the system. After that, a passcode is sent to the user's email address. Once the user passes the two-factor authentication step, they are allowed to visit the website. The user browses the current products and add a few to the cart. During the checkout process, the user is asked to enter their credit card details.

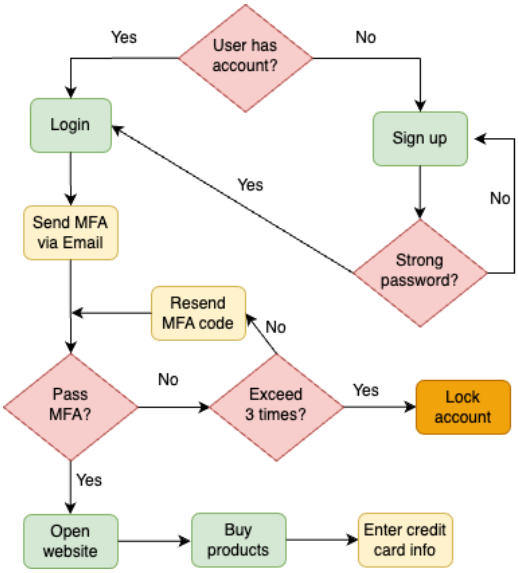


**Fig. 3** *User login, authentication, and purchase*

Figure 4 shows the proposed credit card fraudulent detection system. After the system received the transaction payment details, it sends the details to the K-nearest Neighbor and Naïve Bayes classifiers. The hybrid model produces its final classification using a voting strategy of the outputs of KNN and BN. Based on the result, the transaction is either approved or denied. If denied, the system administrator is alerted to this fraudulent transaction.

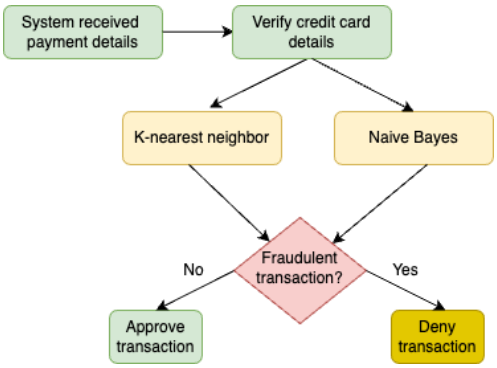

**Fig. 4** *Proposed credit card fraud detection system*

## 4. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, the used dataset is explored. The used metrics to assess performance of the credit card fraud detection system is also discussed. Next, the experimental results are presented and analyzed.

Dataset in this research project, a dataset that consists of 188 credit card transactions is used. For the training phase, 168 transactions are used. For the testing phase, 20 transactions are used.

### 4.1. Implementation

To develop the proposed credit card fraud detection model, we used C# and Microsoft Visual Studio. It runs on any web browser on PC-based machines. We used MySQL to store transaction and fraud detection details.

Figure 5 shows the user registration page. Figure 6 shows sample products to review, while Figure 7 shows the checkout process.

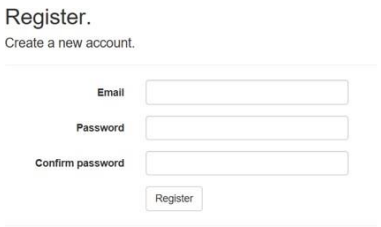


**Fig. 5** *User registration page*

### 4.2. Evaluation Metrics

To evaluate the fraud detection performance of the proposed model, we used accuracy, sensitivity, and specificity. Accuracy is used to assess the proposed model's total effectiveness in classifying online transactions into either authentic or fraudulent. Sensitivity is used to assess the true positive rate of our proposed model. In other words, it is used to estimate the model's ability to correctly identify fraudulent transactions. Specificity is used to assess the true negative rate of the proposed model. In other words, it

is used to estimate the model's ability to correctly identify authentic transactions.

### 4.3. Experimental Results

20 online transactions are used to test the proposed credit card fraud detection model. The experimental results indicate 94.28% accuracy, 94.44% sensitivity, and 94.12% specificity. These results indicate a high accuracy level in detecting fraudulent credit card transaction. In addition, the proposed model proactively alert administrators about the detected fraudulent transactions. The proposed model also exhibits low false positive and false negative rates.

### 4.4. Discussion

The proposed system exhibited high accuracy, specificity, and sensitivity. It incorrectly classified a fraudulent transaction as authentic. It also incorrectly classified an authentic transaction as fraudulent. The achieved high detection performance emphasizes the effectiveness of integrating the K-Nearest Neighbor with Naïve Bayes. The KNN excels at capturing local patterns while the NB can learn general patterns from training data and apply them to new transactions. Therefore, both classifiers complement each other, which leads to improved fraud detection performance

There are sectors, such as e-commerce banks, credit unions, insurance companies, telecommunications, government agencies, health care, and retail, that can utilize the proposed credit card fraud detection system to identify fraudulent transactions. Through reducing the rate of false alerts, organizations can avoid unnecessary failed authorizations, blocked payments, and customer frustration.

In summary, the experimental results and discussion detailed in the preceding analysis clearly demonstrate strengths of the proposed credit card fraud detection model. The achieved high detection performance underlines the potential for improving e-commerce security, protecting businesses, and users from financial losses.

## 5. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a hybrid credit card fraud detection method that integrated two machine learning models: K-Nearest Neighbors and Naive Bayes Classifier. Experimental results exhibited high accuracy, sensitivity, and specificity in detecting fraudulent credit card transactions.

The K-Nearest Neighbors algorithm captures data local patterns, while the Naive Bayes algorithm provide a global data perspective. Therefore, the hybrid method utilizes the complementary strengths of both algorithms. This results in a more accurate detection

of fraudulent transactions.

As a future work, we plan to improve the detection performance through integrating other machine learning algorithms, such as Support Vector Machines, Random Forest, and Decision Trees. We also plan to expand the training and testing dataset to improve the system's ability to generalize to new fraudulent patterns. Finally, we plan to integrate predictive analytics to improve the identification of emerging fraud patterns.

# References


Bhasin, M. L. (2023). Credit Card Fraud Detection Using Machine Learning Algorithms: A Review.

*International Journal of Advanced Computer Science and Applications*, 14(1).

Nilson Report (2024). *The Nilson Report*, Issue 1229. Website: https://nilsonreport.com/newsletters/1229/

de Moura, J. M., Santos, A. T., & Lastres, O. (2023). Credit card fraud detection: a comprehensive survey of techniques and challenges. *Artificial Intelligence Review*, 1-53.

Bhatia, M. S., & Goyal, P. (2021). Credit card fraud detection: A systematic review of machine learning techniques. *Journal of Emerging Technologies and Innovative Research*, *8*(1), 627-634.

Shaghayegh Hajian, Mohsen Rabbani, Shahaboddin Shamshirband. Credit Card Fraud Detection Based on Synthetic Minority Oversampling Technique and Deep Learning. Neural Computing and Applications. 2023.

Arun, A. K., Varatharajan, R., & Surendran, M. (2023). Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach. Electronics, 12(11), 2409.

Marín, D., Ramírez, S., & Sotoca, J. M. (2022). Explainable AI for Credit Card Fraud Detection: A Comparative Study. Applied Sciences, 12(11), 5545.

Zhang, X., Wang, Y., Zhou, Y., Liu, Y., & Zhang, S. (2021). Credit Card Fraud Detection Based on Generative Adversarial Networks. IEEE Access, 9, 149299-149309.

Fernando, A. D. S. L., & Arachchige, K. K. W. (2021). Real-time Credit Card Fraud Detection Using Streaming Analytics and Machine Learning. International Journal of Advanced Computer Science and Applications, 12(11).

Auwal, M. A. H. A., & Yau, A. S. (2022). Credit Card Fraud Detection Using Transaction Amount and Location Information. Journal of Theoretical and Applied Information Technology, 100(12), 3391- 3401.

Alzahrani, A. A. A., Aljuaid, M., & Alshammari, A. K. (2022). Credit Card Fraud Detection Based on User Behavior: A Systematic Literature Review. IEEE Access, 10, 49143-49163.

Liu, J., Chen, M., Li, J., & Huang, H. (2023). Federated Learning for Credit Card Fraud Detection: A Collaborative Approach. IEEE Transactions on Network Science and Engineering, 10(3), 1820-1832.

Omar, A. A., Alharbi, A., & Alghanmi, W. M. (2023). Blockchain-Based Secure Credit Card Transaction System for Fraud Detection. Sustainability, 15(11), 8866.

Kumar, S., Sharma, S., & Singh, S. K. (2022). A Hybrid Model for Credit Card Fraud Detection Using Machine Learning and Deep Learning Techniques. International Journal of Information Technology, 14(3), 1091-1100.

Bhattacharyya, R., Ghosh, S., & Das, A. K. (2021). Detecting Application Fraud in Credit Card Applications Using Machine Learning. Expert Systems with Applications, 166, 114077.