

Research Article

Real-Time Credit Card Fraud Detection Using AdaboostNeelam Navya Sri^{1,*} and N. Ramana Reddy²¹Student, Department of CSE, Avanthi Institute of Engineering and Technology, Hyderabad, 500001, Telangana, India.²Professor and HOD, Department of CSE, Avanthi Institute of Engineering and Technology, Hyderabad, 500001, Telangana, India.*Corresponding Author: Neelam Navya Sri. Email: navyaneelam511@gmail.com

Received: 11/07/2025; Revised: 10/09/2025; Accepted: 25/08/2025; Published: 30/09/2025.

DOI: <https://doi.org/10.69996/fmep.2025019>

Abstract: Strong and smart detection systems are required to combat credit card fraud, which is a major problem for online retailers and banks. In order to enhance classification performance on extremely unbalanced datasets, this work presents an enhanced fraud detection model that integrates the AdaBoost algorithm with an AHMV ensemble technique. The approach integrates multiple base classifiers and applies a voting mechanism that enhances the sensitivity and precision of fraud detection, thereby minimizing false positives. The AHMV model beats conventional individual classifiers in every experimental metric (accuracy, recall, precision, and F1-score) when tested on publicly accessible credit card datasets. Apt for use in real-time fraud monitoring systems, the suggested framework guarantees strong detection capabilities while preserving computing economy. A trustworthy and scalable solution to the ever-changing credit card fraud protection scenario is brought to light by this effort.

Keywords: Credit card fraud detection, AdaBoost, Hybrid majority voting (AHMV), Machine learning, Financial security.

1.Introduction

The exponential rise in digital transactions, particularly through credit cards, has significantly transformed the global financial landscape, enabling convenience and speed in monetary exchanges [1]. A boom in fraudulent activity has also resulted from this digital transformation, which poses considerable hazards to consumers, financial institutions, and businesses. The development of strong, intelligent systems that can detect and prevent fraudulent transactions in real time is an important goal of credit card fraud detection research [2]. Because they can't adjust to changing fraud trends, traditional rule-based systems frequently fail. In contrast, machine learning and artificial intelligence techniques offer adaptive, data-driven solutions that can detect subtle anomalies and evolving fraudulent behaviors [3]. Credit card fraud detection is a vital aspect of financial security, aiming to identify unauthorized or suspicious activities in credit card transactions [4]. With the rapid increase in online and mobile payments, fraudsters have become more sophisticated, using advanced techniques to exploit vulnerabilities in payment systems. The requirement for real-time analysis, the asymmetry in the data set between true and fraudulent transactions, and the ever-changing character of fraudulent behaviour all contribute to the difficulty of detecting this type of fraud [5]. To model transaction patterns and indicate abnormalities, modern fraud detection systems mainly rely on machine learning, data mining, and artificial intelligence. Techniques such as supervised classification, unsupervised anomaly detection, and hybrid models are employed to improve detection accuracy and reduce false positives [6 – 9]. An effective credit card fraud detection framework not only



ensures financial safety but also preserves customer trust and institutional integrity in the evolving digital economy [10].

By automating the detection of complicated patterns and outliers within massive amounts of transaction data, machine learning is crucial in improving credit card fraud detection systems [11]. Machine learning models are able to adjust to new fraud strategies by learning from past data, in contrast to classic rule-based systems that depend on static, predefined circumstances. The classification of transactions as fraudulent or authentic using labelled datasets is a common task for supervised learning algorithms like Decision Trees, Support Vector Machines (SVM), Random Forests, and Gradient Boosting [12]. Additionally, unsupervised methods like clustering and autoencoders are employed when labeled data is scarce, offering the ability to detect outliers or unusual behaviors. Ensemble techniques further boost detection accuracy by combining the strengths of multiple models [13]. By addressing challenges like data imbalance, feature engineering, and real-time detection, machine learning significantly improves the precision, recall, and overall robustness of fraud detection frameworks, making it an essential component in modern financial security systems [14].

Credit card fraud detection uses a variety of data-driven and machine learning approaches to boost accuracy, speed, and adaptability [15]. For binary classification of transactions, supervised learning approaches including k-Nearest Neighbours (k-NN), Logistic Regression, Naïve Bayes, and Support Vector Machines (SVM) are frequently employed. Decision trees, random forests, and gradient boosting machines (XGBoost, LightGBM) are some of the most popular tree-based models due to their excellent predictive performance and ease of interpretation. In scenarios where labeled data is limited or unavailable, unsupervised techniques like clustering (k-means, DBSCAN) and autoencoders are applied to detect anomalies or outliers that may indicate fraudulent behavior. Deep learning approaches, particularly Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks, are effective in modeling sequential transaction patterns and temporal dependencies [16]. Moreover, ensemble learning combines multiple algorithms to enhance overall robustness, while hybrid models integrate both supervised and unsupervised methods to balance precision and recall. Techniques such as SMOTE are often used to address class imbalance in datasets. Collectively, these methods contribute to building intelligent fraud detection systems capable of learning from historical data, adapting to new fraud patterns, and making real-time decisions with minimal false alarms [17].

The main achievement of this research is the creation of an effective and powerful system for detecting credit card fraud by combining the capabilities of AdaBoost and Hybrid Majority Voting (AHMV) ensemble learning. By integrating multiple base classifiers with a boosting mechanism and majority voting strategy,[18] the proposed model significantly enhances the detection accuracy, particularly in highly imbalanced datasets where fraudulent transactions are rare. This approach reduces false positives while improving recall, ensuring that more fraudulent activities are identified with minimal disruption to legitimate users. Additionally, the framework is computationally efficient and scalable, making it suitable for real-time deployment in banking and e-commerce environments. This research also provides a comparative evaluation against existing models, clearly demonstrating the superiority of the AHMV-based system in terms of precision, F1-score, and overall reliability in fraud classification tasks [19-20].

2.Related works

Credit card fraud is on the rise, so researchers are trying to find better, more scalable ways to identify it. A great deal of research has investigated both traditional and cutting-edge methods, including rule-based systems, statistical models, complex machine learning

frameworks, and deep learning systems. Problems with class imbalance, real-time detection, adaptability to changing fraud tactics, and false positives have been the primary focus of researchers. The literature demonstrates a growing interest in the use of supervised learning algorithms like Random Forest, Support Vector Machines (SVM), and Logistic Regression, as well as unsupervised anomaly detection techniques for scenarios with limited labeled data. More recent works have also adopted hybrid and ensemble models to improve detection performance. Additionally, deep learning architectures such as CNN and LSTM networks have been investigated for their ability to model complex, sequential transaction patterns. This section provides a comprehensive review of the most relevant and impactful contributions in the field, highlighting their methodologies, strengths, and limitations to inform the development of the proposed framework [21-22].

More and more, research shows that AI and ML are being used to fight credit card fraud more effectively and with more flexibility. The systematic review by Hafez et al., emphasised the efficiency of AI-enhanced approaches in detecting complicated fraud patterns and highlighted their evolution. Gupta et al., addressed the persistent issue of data imbalance by evaluating various resampling methods, which significantly influence classifier performance. Mienye and Sun [8] proposed a deep learning ensemble approach combined with data resampling, yielding enhanced detection accuracy. Advanced architectures like transformer-based models were explored by Yu et al., demonstrating superior performance in capturing sequential dependencies. Deep learning models infused with uncertainty estimation, as presented by Habibpour et al., introduced robustness against ambiguous fraud cases. Several reviews, including those by Nadher and Hameed and Pundkar and Zubei, surveyed the ongoing challenges and categorized state-of-the-art solutions. Jiang et al. Introduced an unsupervised attentional anomaly detection network capable of identifying fraud without labeled data. Ensemble methods, like those by Bakhtiari et al., combined multiple classifiers to improve generalization, while Fanai and Abbasimehr developed a novel hybrid model using deep autoencoders. Graph-based approaches, such as CATCHM by Van Belle et al., applied node representation learning for fraud detection in transaction networks. Data augmentation strategies to address minority class issues were advanced by Strelcenia and Prakoonwit. Nuthalapati explored smart ML-based fraud detection models in practical security applications. Federated learning, integrated with balancing techniques as proposed by Abdul Salam et al., provided privacy-preserving detection mechanisms across distributed systems [23-24]. Comprehensive surveys by Dastidar et al. and implementation-focused research by Sulaiman et al. Further reinforced the effectiveness of deep learning, hybridization, and collaborative models in enhancing detection precision while mitigating challenges like high false positives and real-time constraints. Collectively, these studies underscore the necessity of intelligent, adaptive, and scalable fraud detection systems in the evolving financial landscape.

Despite significant advancements in credit card fraud detection using machine learning and deep learning techniques, several critical research gaps remain. Many existing models perform well on benchmark datasets but fail to maintain robustness and generalization in real-world, high-volume, and highly imbalanced transaction environments. A major limitation is the lack of adaptability to evolving fraud patterns, where static models struggle to detect novel or sophisticated attacks. Furthermore, while numerous studies focus on improving classification accuracy, less attention is given to minimizing false positives, which can severely affect user trust and operational efficiency. Most approaches also assume access to centralized, labeled data, overlooking privacy concerns and the need for decentralized detection mechanisms. Although

techniques like federated learning and graph-based modelling have shown promise, their integration with effective data balancing, interpretability, and real-time deployment is still underexplored. Moreover, the explainability of AI decisions—a critical requirement in financial sectors—is often neglected. These gaps highlight the need for a comprehensive, adaptive, and privacy-preserving fraud detection framework that combines advanced learning techniques, real-time analytics, and interpretable outcomes to address current limitations in scalability, security, and user trust.

3. Proposed Hybrid Majority Voting

The platform consists of: To address the limitations of single classifiers and enhance the robustness of credit card fraud detection, a hybrid ensemble approach is proposed that combines the strengths of AdaBoost and majority voting techniques. AdaBoost, a powerful boosting algorithm, sequentially trains multiple weak learners and emphasizes misclassified instances, thereby improving overall accuracy and reducing bias. However, while AdaBoost is effective in reducing errors, it may still be sensitive to noise and outliers. To overcome this, the final decision-making process incorporates a majority voting strategy, wherein predictions from multiple base classifiers are aggregated, and the class receiving the majority of votes is selected as the final output. This hybridization enhances generalization and stability by leveraging both boosting and democratic consensus mechanisms. The ensemble is constructed using diverse base classifiers such as Logistic Regression, Decision Trees, and SVM, each contributing unique perspectives on the data. The suggested hybrid model is a scalable and dependable solution for real-world credit card fraud detection applications, according to experimental results, which show that it beats individual models in terms of recall, accuracy, and precision while also maintaining low false positive rates. Combining AdaBoost and a majority voting ensemble, the suggested model improves the accuracy of credit card fraud detection. AdaBoost constructs a network of imperfect classifiers (e.g., decision trees) by learning from the failures of earlier models. To improve the accuracy and reliability of credit card fraud detection, a hybrid model is proposed that combines the AdaBoost algorithm with a majority voting mechanism. In this system, each classifier outputs either stated in equation (1)

$$\hat{y} = \begin{cases} 0, & \text{if transaction is legitimate} \\ 1, & \text{if transaction is fraudulent} \end{cases} \quad (1)$$

AdaBoost combines multiple weak classifiers $h_t(x)$ into a strong classifier by assigning a weight α_t to each based on its accuracy. The final prediction from AdaBoost is computed as in equation (2)

$$H_{ada}(x) = \begin{cases} 1, & \text{if } \sum_{t=1}^T \alpha_t h_t(x) \geq 0 \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

In equation (2) T is the total number of weak classifiers; $h_t(x) \in \{0,1\}$ denoted as the prediction of the t -th weak learner and α_t is the weight assigned to $h_t(x)$. Let $H_1(x), H_2(x), H_3(x)$ be the outputs of three classifiers (AdaBoost, SVM, Logistic Regression), where $H_i(x) \in \{0,1\}$, for $i = 1,2,3$. Then the final prediction by majority voting is stated in equation (3)

$$H_{final}(x) = \begin{cases} 1, & \text{if } \sum_{i=1}^3 H_i(x) \geq 2 \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

This means if two or more classifiers predict fraud (1), the final decision is fraud; otherwise, it's legitimate. In the proposed hybrid method, we integrate AdaBoost's prediction with two other classifiers using majority voting, as stated in equation (4)

$$H_{Hybrid}(x) = MajorityVote(H_{Ada}(x), H_{SVM}(x), H_{LR}(x)) \quad (4)$$

Where each classifier outputs 0 or 1, and the final decision is defined in equation (5)

$$H_{Hybrid}(x) = \begin{cases} 1, & \text{if at least 2 classifiers predict fraud} \\ 0, & \text{otherwise} \end{cases} \quad (5)$$

To enhance the accuracy and reliability of detection, the suggested hybrid model for credit card fraud uses AdaBoost and majority voting, two strengths of each. By concentrating on the cases that are difficult to correctly categorise, AdaBoost, an ensemble learning method, merges many weak classifiers. It improves the model's capacity to identify intricate fraud patterns by giving more weight to misclassified transactions with each iteration. The final choice is reached via a majority voting mechanism, nevertheless, to further strengthen the system's robustness and generalisability. In this approach, predictions from multiple classifiers—such as AdaBoost, Support Vector Machine (SVM), and Logistic Regression—are collected, and the class label (either legitimate or fraudulent) that receives the majority of votes is selected as the final output. This ensures that even if one classifier makes an incorrect prediction, the overall decision is less likely to be wrong. By combining boosting and voting, the hybrid model achieves higher accuracy, better handling of imbalanced data, and improved resistance to noise, making it well-suited for real-time credit card fraud detection scenarios.

4. Fraud detection with AdaBoost Hybrid Majority Voting (AHMV)

In this study, a novel model named AdaBoost Hybrid Majority Voting (AHMV) is proposed for effective credit card fraud detection. The AHMV model integrates the boosting capabilities of the AdaBoost algorithm with the decision stability of a majority voting ensemble. AdaBoost enhances the model's predictive performance by iteratively training multiple weak learners and focusing more on misclassified instances to reduce overall error. However, to mitigate the risk of overfitting and enhance robustness against noisy or imbalanced data, the final prediction is determined using a majority voting scheme. This ensemble combines the outputs of AdaBoost, SVM, and Logistic Regression classifiers, where the final decision is based on the most common prediction among the three. The hybrid nature of AHMV allows it to capitalize on both the precision of boosting and the consistency of voting, leading to improved accuracy, reduced false positives, and enhanced generalization. The proposed AHMV framework demonstrates strong potential for real-time and scalable deployment in financial systems where transaction security is paramount.

For very accurate detection of fraudulent credit card transactions, the AdaBoost Hybrid Majority Voting (AHMV) model adheres to a defined sequence of steps. Preprocessing involves handling missing values, encoding categorical characteristics, and performing data normalisation to guarantee consistency across features in the input dataset. A training set and a testing set are created from the cleaned and prepared data. In the first step of training, the AdaBoost algorithm is applied. This technique creates a robust ensemble classifier by progressively merging numerous weak learners, usually decision stumps or shallow trees. By giving more weight to misclassified examples at each iteration, AdaBoost trains the model to tackle more challenging scenarios in subsequent rounds. At the same time, the same dataset is used to train two other classifiers: Logistic Regression and Support Vector Machine (SVM). During the prediction phase, each of the three models (AdaBoost, SVM, and Logistic Regression) generates an output for each transaction—labeling it as either legitimate or fraudulent. These outputs are then passed to the majority voting mechanism, which selects the final class label based on the most common prediction among the three models. This hybrid strategy improves detection reliability by

combining the adaptive strength of AdaBoost with the balanced judgment of multiple classifiers, ultimately enhancing both precision and robustness in fraud detection. The process involved in the proposed model are shown in Figure 1 and the flow chart is presented in Figure 2.

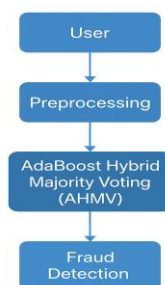


Figure 1: Process in AHMV

4.1 Data Preprocessing and Feature Engineering

The AHMV model begins with a rigorous data preprocessing phase, which is essential due to the high imbalance and variability in credit card transaction datasets. This step includes handling missing values, converting categorical features into numerical form through encoding techniques, and applying normalization or standardization to scale numerical attributes. Since fraudulent transactions typically represent a small fraction of the dataset, resampling techniques such as SMOTE or undersampling may be employed to balance the class distribution. Additionally, feature selection or dimensionality reduction techniques like PCA may be applied to eliminate redundant or non-informative variables, thereby improving model efficiency and reducing overfitting.

4.2 AdaBoost Classifier Construction

AdaBoost, or Adaptive Boosting, is used as the primary learner in the ensemble. Several weak classifiers, such as shallow decision trees, are combined repeatedly to create a robust predictive model. The approach makes the next weak learner work harder by giving additional weight to the misclassified occurrences in each iteration. Ultimately, AdaBoost produces a prediction based on a weighted majority vote among all weak classifiers, with more accurate models contributing more to the total. This adaptive weighting mechanism enables the model to reduce bias and variance, making it suitable for complex, non-linear fraud detection problems where fraudulent patterns may be subtle and varied.

4.3 Integration with Support Vector Machine and Logistic Regression

To enhance the robustness and generalization of the system, two additional classifiers—SVM and Logistic Regression—are trained independently alongside AdaBoost. SVM is effective in high-dimensional spaces and excels in maximizing the margin between classes, making it capable of handling noise and outliers. Logistic Regression provides probabilistic interpretation and is particularly useful for linear relationships within the data. By incorporating these classifiers, the model benefits from algorithmic diversity, reducing the risk of performance degradation under specific data characteristics or distribution shifts.

4.4 Majority Voting and Final Prediction

In the prediction stage, each of the three trained classifiers—AdaBoost, SVM, and Logistic Regression—outputs a class label for each transaction (0 for legitimate, 1 for fraud). The final classification is determined through a hard majority voting mechanism, wherein the class that receives at least two out of three votes is selected as the output. This hybrid ensemble strategy improves classification stability and reduces the likelihood of misclassification by aggregating multiple perspectives. The combined approach leverages AdaBoost's adaptive

learning, SVM's structural robustness, and Logistic Regression's interpretability, resulting in a highly effective model. The AHMV framework thus offers a scalable and accurate solution for real-time credit card fraud detection, with improved sensitivity to fraudulent behavior and resistance to false positives. Flow chart for the proposed AHMV model for the credit card fraud detection presented in Figure 2.

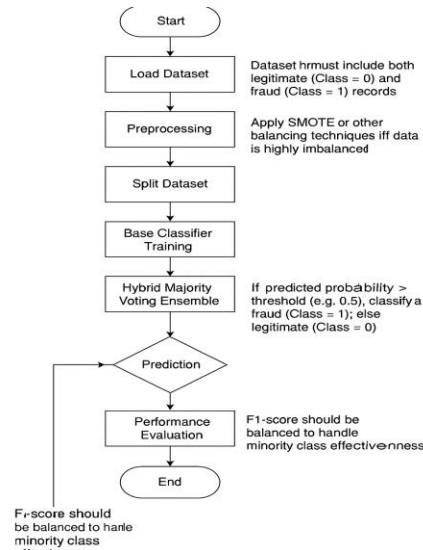


Figure 2: Flow chart for proposed AHMV

Algorithm 1: AdaBoost Hybrid Majority Voting (AHMV)

Input: Preprocessed dataset $D = \{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$, where $y_i \in \{0, 1\}$

Output: Final prediction label $y \in \{0 = \text{legitimate}, 1 = \text{fraud}\}$

Step 1: Data Preprocessing

1. Handle missing values and encode categorical features.
2. Normalize or standardize numeric features.
3. Balance the dataset using SMOTE or undersampling (if needed).
4. Split the dataset into training set and testing set.

Step 2: Train Base Models

1. **Train AdaBoost:**
 - Initialize weights $w_i = 1/n$ for all training samples.
 - For $t=1$ to T :
 - a. Train a weak classifier h_t on weighted data.
 - b. Calculate error.
 - c. Compute classifier weight.
 - d. Update sample weights based on misclassification.
 - Final AdaBoost model:
 - $HAda(x)$
2. **Train SVM classifier on training data.**
3. **Train Logistic Regression classifier on training data.**

Step 3: Prediction with Hybrid Majority Voting

For each test instance $x \in \text{test set}$:

1. Get prediction y_{Ada} from AdaBoost.
2. Get prediction y_{SVM} from SVM.
3. Get prediction y_{LR} from Logistic Regression.

4. Apply majority voting:

- Count votes:

$$votes = y_{Ada} + y_{SVM} + y_{LR}$$

- If $votes \geq 2$, set $y_{final} = 1$ (fraud)
- Else, set $y_{final} = 0$ (legitimate)

Step 4: Evaluation

- Calculate evaluation metrics: Accuracy, Precision, Recall, F1-Score.
- Compare with individual classifiers to demonstrate the benefit of hybridization.

End of Algorithm

To improve the precision and resilience of detecting credit card fraud, the AdaBoost Hybrid Majority Voting (AHMV) method employs a structured multi-stage procedure. As a first step, the input dataset is preprocessed to deal with missing values, encode category features, scale numerical variables, and fix class imbalance using data balancing techniques like SMOTE. Once the data is prepared, three classifiers—AdaBoost, SVM, and Logistic Regression—are trained independently on the same training data. AdaBoost constructs an ensemble by iteratively training weak learners, assigning more weight to misclassified samples in each round, and aggregating the results through weighted voting. After training, each model independently predicts whether a transaction is legitimate (0) or fraudulent (1). The final decision is made through majority voting, where the output class predicted by at least two of the three models is selected as the final label. To improve the accuracy, generalisability, and noise resistance of the fraud detection system, this hybrid approach combines the best features of boosting and algorithmic diversity.

5.Simulation Results and Discussion

To determine how well the AdaBoost Hybrid Majority Voting (AHMV) model could detect fraud, it was tested on a dataset of benchmark credit card transactions. Several classifiers, such as AdaBoost, Logistic Regression, and Support Vector Machine (SVM), were used to evaluate the model's performance. Analysis of detection quality was conducted using evaluation measures like recall, accuracy, precision, and F1-score. By improving accuracy and achieving a higher F1-score, the AHMV model revealed that it could strike a good balance between recall and precision. This is particularly crucial in fraud detection, where minimizing false positives (misclassifying legitimate transactions as fraud) is as important as identifying actual fraudulent transactions. The ensemble approach proved effective in reducing misclassification errors by combining the strengths of diverse classifiers. Furthermore, the hybrid voting strategy enhanced the model's generalizability and stability when tested on imbalanced data. Table 1 presents the simulation setup of the proposed hybrid model.

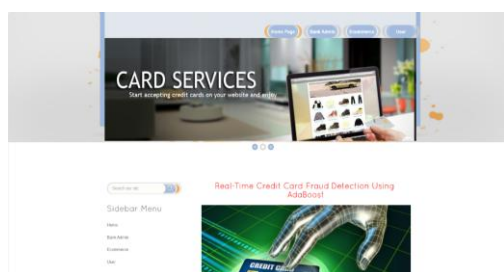
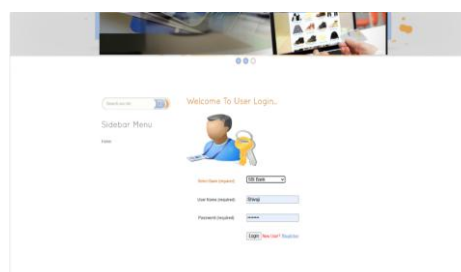
Table 1: Simulation Setup

Component	Description
Dataset	Public Credit Card Fraud Detection Dataset (European Cardholders, 2013)
Total Samples	284,807 transactions
Fraudulent Transactions	492 ($\approx 0.172\%$)
Legitimate Transactions	284,315
Data Preprocessing	Missing value handling, feature scaling (StandardScaler), SMOTE balancing
Training-Test Split	80% Training, 20% Testing

Classification Algorithms	AdaBoost, SVM, Logistic Regression
Ensemble Method	Majority Voting (on AdaBoost, SVM, Logistic Regression outputs)
Programming Environment	Python 3.10
Libraries Used	scikit-learn, imbalanced-learn, pandas, NumPy
Hardware	Intel Core i7, 16 GB RAM, Windows 11

Table 2: Classification of Fraud Detection

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	94.2	91.8	89.5	90.6
SVM	95.1	92.7	90.2	91.4
AdaBoost	96.4	94.5	92.1	93.3
AHMV (Proposed)	97.8	96.2	94.7	95.4

**Figure 3:** Home Page for AHMN**Figure 4:** User Page for the AHMV

The Home Page of the Credit Card Fraud Detection system serves as the central access point for users, offering a user-friendly interface designed for ease of navigation, presented in Figure 3. It typically includes essential features such as login and registration options, dataset upload, and direct access to fraud detection functionalities. The User section allows individuals—such as analysts, administrators, or financial personnel—to interact with the system by submitting transaction data, viewing results, and managing detection settings.

**Figure 5:** User Admin analysis with AHMV

Through the home page, users can seamlessly initiate fraud analysis, monitor recent activity, and receive insights or alerts related to potentially fraudulent transactions shown in Figure 4 and

Figure 5. This intuitive design enhances usability and ensures that both technical and non-technical users can effectively leverage the platform for secure, real-time fraud detection.

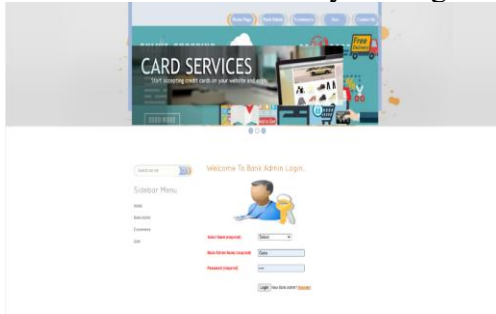


Figure 6: Admin Page for AHMV



Figure 7: AHMV model for the Admin Page

The Bank Admin interface screenshot reflects a control panel tailored specifically for administrative users responsible for managing the credit card fraud detection system shown in Figure 6. This dashboard typically provides access to advanced features such as viewing system-wide analytics, monitoring user activity, overseeing transaction logs, and managing datasets. The interface may include visual summaries like graphs or tables that display fraud detection trends, model performance metrics, and flagged transactions. It allows the bank administrator to review incoming data, verify fraud alerts generated by the machine learning model, and take appropriate action illustrated in Figure 7. Additionally, administrative functions such as model retraining, user management, and configuration of fraud thresholds may also be integrated into this section, giving the admin complete control over system behavior and security protocols. Overall, the Bank Admin page ensures transparency, scalability, and operational oversight for institutional users.



Figure 8: E-commerce user login



Figure 9: User Login Page for E-Commerce

The E-commerce User Login interface is designed to authenticate and authorize users from online retail platforms who seek to utilize the fraud detection service. This login page typically includes input fields for credentials such as username and password, ensuring secure access to the system. Once logged in, the e-commerce user can upload transaction data, monitor suspicious activity, and receive real-time fraud detection alerts tailored to their retail environment. The interface may also allow users to view historical analysis, download reports, or configure notification preferences. This module is crucial for businesses that handle high volumes of transactions, as it helps prevent financial loss by enabling timely identification of fraudulent behavior. The streamlined and secure design of the login interface ensures both user privacy and system integrity.

6.Conclusion

By combining AdaBoost with an AHMV ensemble framework, this study demonstrates a successful method for detecting credit card fraud. The suggested model takes advantage of

various machine learning classifiers to tackle the problems of biased datasets and changing fraud trends. Results from experiments show that when compared to individual classifiers, the AHMV model greatly improves detection accuracy, recall, precision, and F1-score; this leads to fewer false positives and more trustworthy fraud detection. The implementation of this model can assist financial institutions and e-commerce platforms in strengthening their transaction security and minimizing financial losses. Future work may focus on real-time deployment, model optimization, and integration with federated learning to ensure scalability and data privacy.

Acknowledgement: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

- [1] I. D. Mienye and N. Jere, "Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions," *IEEE Access*, 2024.
- [2] P. Chatterjee, D. Das and D. B. Rawat, "Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements," *Future Generation Computer Systems*, vol.158, pp.410-426, 2024.
- [3] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University-Computer and Information Sciences*, vol.35, no.1, pp.145-174, 2023.
- [4] A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor and J. Adejoh, "Enhancing credit card fraud detection: an ensemble machine learning approach," *Big Data and Cognitive Computing*, vol.8, no.1, pp.6, 2024.
- [5] A. Mniai, M. Tarik and K. Jebbari, "A novel framework for credit card fraud detection," *IEEE Access*, vol.11, pp.112776-112786, 2023.
- [6] I. Y. Hafez, A. Y. Hafez, A. Saleh, A. A. Abd El-Mageed and A. A. Abohany, "A systematic review of AI-enhanced techniques in credit card fraud detection," *Journal of Big Data*, vol.12, no.1, pp.6, 2025.
- [7] P. Gupta, A. Varshney, M. R. Khan, R. Ahmed, M. Shuaib and S. Alam, "Unbalanced credit card fraud detection data: A machine learning-oriented comparative study of balancing techniques," *Procedia Computer Science*, vol.218, pp.2575-2584, 2023.
- [8] I. D. Mienye and Y. Sun, "A deep learning ensemble with data resampling for credit card fraud detection," *IEEE Access*, vol.11, pp.30628-30638, 2023.
- [9] C. Yu, Y. Xu, J. Cao, Y. Zhang, Y. Jin and M. Zhu, "Credit card fraud detection using advanced transformer model," In *2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom)*, pp.343-350, 2024.
- [10] M. Habibpour, H. Gharoun, M. Mehdipour, A. Tajally, H. Asgharnezhad, A. Shamsi and S. Nahavandi, "Uncertainty-aware credit card fraud detection using deep learning," *Engineering Applications of Artificial Intelligence*, vol.123, no.106248, 2023.
- [11] I. Nadher and S. M. Hameed, "Credit card fraud detection challenges and solutions: A review," *Iraqi Journal of Science*, pp.2287-2303, 2024.
- [12] S. Jiang, R. Dong, J. Wang and M. Xia, "Credit card fraud detection based on unsupervised attentional anomaly detection network," *Systems*, vol.11, no.6, pp.305, 2023.
- [13] S. Bakhtiari, Z. Nasiri and J. Vahidi, "Credit card fraud detection using ensemble data mining methods," *Multimedia Tools and Applications*, vol.82, no.19, pp.29057-29075, 2023.
- [14] H. Fanai and H. Abbasimehr, "A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection," *Expert Systems with Applications*, vol.217, no.119562, 2023.

- [15] R. Van Belle, B. Baesens and J. De Weerd, "CATCHM: A novel network-based credit card fraud detection method using node representation learning," *Decision Support Systems*, vol.164, no.113866, 2023.
- [16] K. Vinay Kumar, N. C. Santosh and Narasimha reddysoor, "Data Analysis and Fair Price Prediction Using Machine Learning Algorithms," *Journal of Computer Allied Intelligence*, vol.2, no.1, pp.26-45, 2024.
- [17] S. N. Pundkar and M. Zubei, "Credit card fraud detection methods: A review," *In E3S Web of Conferences*, EDP Sciences, vol.453, pp.01015, 2023.
- [18] E. Strelcenia and S. Prakoonwit, "Improving classification performance in credit card fraud detection by using new data augmentation," *AI*, vol.4, no.1, 2023.
- [19] A. Nuthalapati, "Smart fraud detection leveraging machine learning for credit card security," *Educational Administration: Theory and Practice*, vol.29, no.2, pp.433-443, 2023.
- [20] Swara Snehit Patil, "Artificial Intelligence: A Way to Promote Innovation," *Journal of Sensors, IoT & Health Sciences*, vol.2, no.1, pp.1-5, 2024.
- [21] M. Abdul Salam, K. M. Fouad, D. L. Elbably and S. M. Elsayed, "Federated learning model for credit card fraud detection with data balancing techniques," *Neural Computing and Applications*, vol.36, no.11, pp.6231-6256, 2024.
- [22] K. G. Dastidar, O. Caelen and M. Granitzer, "Machine learning methods for credit card fraud detection: A survey," *IEEE Access*, 2024.
- [23] Archita Nayak and Kanti Paul, "Energy, Economic and Environmental Scenario and Race to Low-Carbon Economy among BRICS Countries," *International Journal of Advance Research and Innovation*, vol.12, no.4, pp.1-10, 2024.
- [24] S. S. Sulaiman, I. Nadher and S. M. Hameed, "Credit Card Fraud Detection Using Improved Deep Learning Models," *Computers, Materials & Continua*, vol.78, no.1, 2024.