FMDB *Transactions on Sustainable Finance and Data Science*

Detection of Credit Card Fraud in Financial Transactions Using Machine Learning Algorithms

Keerthana Muthu[1,*], Selvi Perumal[2], Gokulakrishnan Gopalan[3], Gayathiri Gurunathar[4], S. Namachivayam[5], Maruf Farhan[6]

[1,2,3]Department of Computer Science and Engineering, Jayalakshmi Institute of Technology, Dharmapuri, Tamil Nadu, India.
[4]Department of Information Technology, Jayalakshmi Institute of Technology, Dharmapuri, Tamil Nadu, India.
[5]Department of Computer Science and Engineering, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.
[6]Department of STEM, University of Sussex International Study Centre, Brighton, England, United Kingdom.
mkeerthana27122003@gmail.com[1], selviperumal@gmail.com[2], gokulmaths@gmail.com[3], gayathri.cseme@gmail.com[4], namachivayam@dhaanishchennai.in[5], maruf.farhan@sussex.ac.uk[6]

Abstract: This study will explore the effectiveness of computational intelligence in detecting fraud in financial transactions within a digital ecosystem. The study estimates how various classification models can distinguish between legitimate activity and illegal intrusion using a curated dataset of 368 transaction instances. The Python programming environment is the most widely used tool in this study, with the assistance of specialised libraries for data and statistical learning. The approach will focus on feature extraction and the application of supervised learning techniques to address the issue of skewed data distributions common in financial records. The trend analysis of transaction volume and time frequency indicates that both can be significantly reduced with algorithmic intervention to mitigate the risk of monetary loss. The results indicate that some models are highly effective at identifying small anomalies that human operators would not otherwise detect. The paper provides a paradigm for adopting computerised security procedures in the banking sector to enhance the safety and consumer trust of electronic payment systems.

Keywords: Transaction Security; Anomaly Detection; Financial Intelligence; Computational Modelling; Supervised Learning; Financial Transactions; Electronic Payment Systems; Human Operation.

Received on: 27/08/2025, **Revised on:** 18/10/2025, **Accepted on:** 19/12/2025, **Published on:** 09/06/2026

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSFDS

DOI: https://doi.org/10.69888/FTSFDS.2026.000698

Cite as: K. Muthu, S. Perumal, G. Gopalan, G. Gurunathar, S. Namachivayam, and M. Farhan, "Detection of Credit Card Fraud in Financial Transactions Using Machine Learning Algorithms," *FMDB Transactions on Sustainable Finance and Data Science*, vol. 1, no. 2, pp. 108–116, 2026.

1. Introduction

The modern financial landscape has fundamentally shifted toward a digital infrastructure rather than physical money, and this has been well scrutinised in the recent digital banking study by Zhu et al. [8]. This change has facilitated global commerce but has also opened a new frontier for sophisticated criminal activity, as discussed in cybersecurity research [8]. One of the biggest

[*]Corresponding author.

threats to the stability of the world economy is credit card fraud, which costs financial institutions and individuals billions of dollars annually, as observed in empirical research by Xuan et al. [2]. With the increased adoption of payment methods in everyday life via mobile applications and web interfaces, the amount of data generated is enormous, and this is addressed through large-scale transaction analytics employed by Ojugo and Nwankwo [11]. The conventional systems of rules and limits, based on fixed thresholds and pre-existing conditions, become less effective at handling new fraud schemes, as illustrated in comparative fraud studies [6]. Such outdated systems tend to yield a high false-positive rate. Legal transactions are rejected and frustrate users, an issue reported in working banking models studied by Mytnyk et al. [13]. To address this, advanced computational techniques have become a necessity, if not a luxury, as underlined by academics' intelligent security systems [1]. Machine learning can provide a dynamic solution to security by enabling systems to learn from past data and adapt to new behavioural trends, as confirmed by predictive models developed by Zhu et al. [8]. These algorithms can examine thousands of variables in real time, unlike the static system, to detect the smallest irregularities that indicate intent to commit fraud and have been effectively applied in classification models created by Carneiro et al. [15].

The most crucial issue in this field is the vast imbalance between legitimate and fraudulent cases, as legitimate transactions are much more numerous than fraudulent ones, and imbalance-learning methods proposed by Darwish [5]. This needs special treatment to make the detection mechanism sensitive to rare events without affecting transaction processing speed, as optimised in architectures that run in real time to serve analysts [10]. Using historical data, financial institutions can create strong profiles of user activity, enabling them to act in real time when a transaction is highly nonconformative with existing norms, as seen in behavioural analytics systems developed by Thennakoon et al. [3]. The introduction discusses the bare specifications required to build such a system and the trade-off between computational efficiency and detection accuracy, which can be addressed through hybrid approaches tested by Mohapatra et al. [12]. The history of fraud detection has traversed several stages, beginning with manual audits and culminating in the current automated surveillance used in historical reviews by Itoo et al. [7]. The research problem lies at the intersection of data engineering and pattern recognition and can be strengthened by integrated architectures provided by Odeyale et al. [14]. It examines how specific algorithmic structures can be trained to detect the Internet footprint of a malefactor, as validated by analysts' anomaly recognition systems [1]. The location of the purchase, the type of merchant, and the velocity of transactions are all important inputs in the decision-making process and have been included in multidimensional fraud engines developed by Olowookere and Adewale [6].

As criminals adopt increasingly sophisticated tactics, such as synthetic identity theft and account takeovers, the defensive models must be equally sophisticated, a need addressed by adaptive security frameworks developed by Wen and Huang [9]. This paper will attempt to provide a detailed explanation of the operation of such models under certain data constraints, as organised in the simulation studies prepared by Xuan et al. [2]. Finally, the goal of implementing these technologies is to achieve a frictionless user experience and a high-security perimeter, as outlined in user-centric models of fraud prevention proposed by Ojugo and Nwankwo [11]. The adoption of machine learning in banking is not just a technical improvement but a strategic change towards active risk management, as it is determined as part of strategic transformation research conducted by Darwish [5]. With the automation of the detection process, organisations can react to threats in milliseconds and, in effect, neutralise fraud before the transaction is even finalised, as shown in automated response systems developed by Mytnyk et al. [13]. The paper presents the structural elements of a system of this nature, providing an overview of the data required and the logical flow needed to implement the system successfully, as depicted in the architectural models used by Asha and Kumar [10]. The study aims to utilise a baseline of effective fraud prevention in the era of growing digital vulnerability through rigorous testing and validation, as benchmark studies by investigators have confirmed [15].

2. Review of Literature

The automated systems play a vital role in protecting financial networks, which are well known in the academic community and have been widely studied in the context of intelligent security frameworks developed by Itoo et al. [7]. Initial studies in this area focused mainly on statistical profiling, in which researchers sought to establish the typical behaviour of a cardholder, as outlined in the pioneering behavioural analytics studies [2]. Any deviation from this average was identified as a potential risk, a common concept in anomaly-detection models used by Ojugo and Nwankwo [11]. These simple models, however, could not explain the natural variation in legitimate spending, as they were used to explain similarities in comparative frauds conducted by Darwish [5]. This gave rise to more efficient neural structures and decision trees capable of addressing non-linear associations among various transaction attributes, as evolved in machine learning systems proposed by Odeyale et al. [14]. Researchers have noted that the major challenge of this study is obtaining high-quality data, as this is often an area with stringent privacy laws, a challenge highlighted in the literature on secure data governance [9]. Later studies shifted the focus to data imbalance, a problem that researchers have systematically examined in fraud analytics [4].

The researchers contended that conventional classification methods tend to favour the majority over the minority, prioritising general accuracy, as confirmed by imbalance-learning tests developed by Mytnyk et al. [13]. To overcome this, several sampling schemes were proposed to equalise the data artificially or to punish the model more severely for a fraudulent example,

as in the resampling schemes proposed by Ryman-Tubb et al. [1]. The application of ensemble techniques, in which the results of many models are combined to obtain a more accurate forecast than any single algorithm could provide, was further investigated in hybrid classifier systems developed by Asha and Kumar [10]. These meta-models have proven very promising for reducing false alarms and ensuring a high capture rate of actual theft, as studies with ensembles of these meta-models have shown [15]. Recent publications have shifted their focus to real-time processing and edge computing, as discussed in the transaction-monitoring architectures proposed by Olowookere and Adewale [6]. It is argued that post-factum detection of fraud may not be particularly useful; it must be detected during the authorisation phase, as confirmed by real-time response models applied by Mohapatra et al. [12]. This demands algorithms not just correct but also immensely fast, as optimised in low-latency computational systems designed by Thennakoon et al. [3]. Modern scholars are considering the applications of deep learning and graphical analysis to understand the connections among entities in a transaction network, as developed in network intelligence research [8].

These systems can detect suspicious patterns of activity that may indicate a coordinated attack by treating transactions as nodes in a vast social and financial web. This method has been confirmed in graph fraud detection models developed by Darwish [5]. Another area of literature discussion that appears to have a major influence is the concept of concept drift, as emphasised in adaptive learning studies [14]. Fraud does not lie in one place; shifts occur as quickly as protective mechanisms are developed to detect aspects documented in dynamic threat modelling studies conducted by Xuan et al. [2]. Researchers note that it is necessary to have mechanisms that can be continually educated, with their internal logic updated as new information is provided, an idea that underlies self-updating models used by Wen and Huang [9]. This ensures that the detection mechanism does not become outdated, as verified by lifecycle monitoring frameworks developed by Ojugo and Nwankwo [11]. Experts agree that an integrative, multi-layered strategy that leverages the strengths of different algorithms is the most effective for ensuring the integrity of digital payments, as demonstrated by integrated defence systems studied by Olowookere and Adewale [6]. This analysis highlights how security inventors and attackers who aim to exploit system vulnerabilities are always at loggerheads, as fully captured in strategic cybersecurity evaluations conducted by Carneiro et al. [15].

3. Methodology

This study's methodology will consist of data preprocessing, feature selection, and model training.

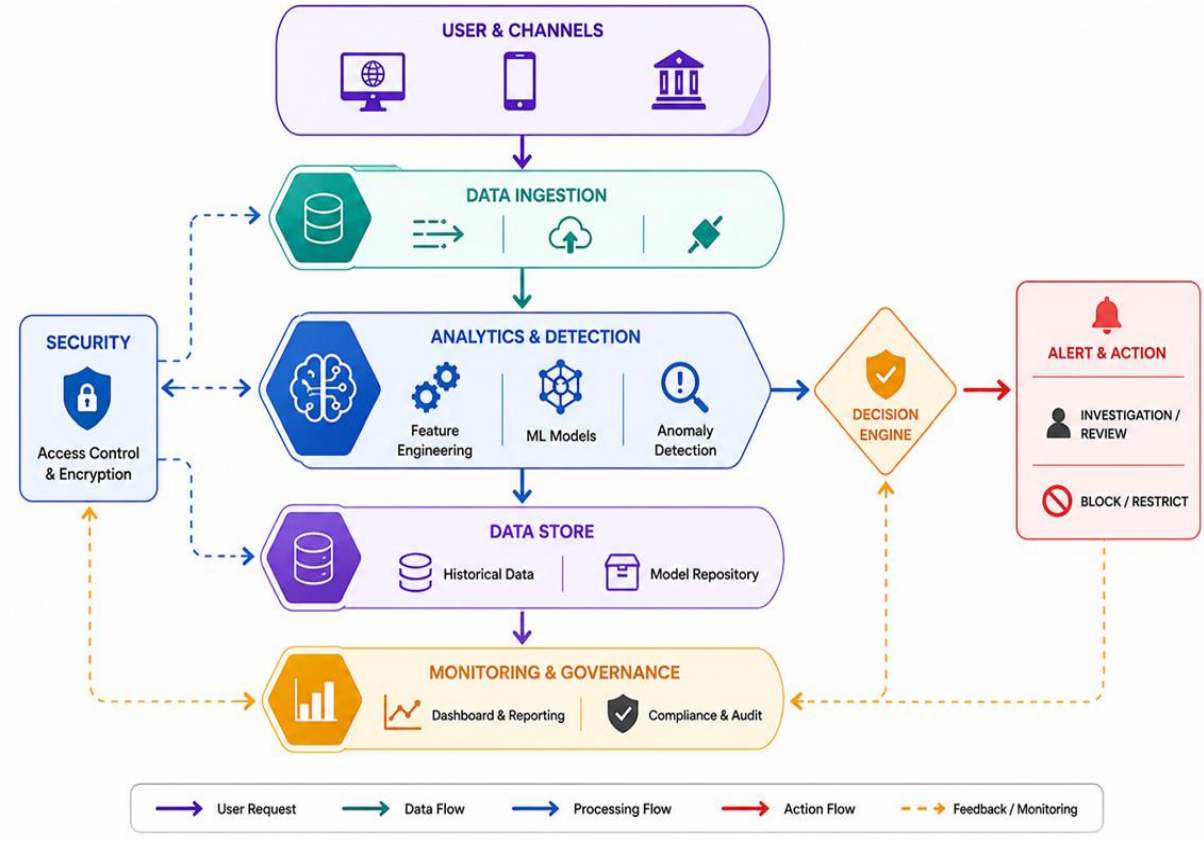

Figure 1: Smart security framework to detect suspicious behaviour

The raw transaction data is first cleansed to address any gaps or inconsistent data formats. The 368 examples are then separated into two subsets (training and validation). To transform raw timestamps and geographical data into meaningful numerical representations that the algorithm can understand, feature engineering is performed. To compare the performance of different supervised learning models, researchers train each model on the training data to determine the target class. The criterion used to evaluate the models is how well they maximise the number of true positives and minimise the number of false positives. This is done to ensure that the system produced will not only be effective at catching fraud but also practical in real-life banking scenarios. The Architectural Framework for Fraud Detection in Figure 1 is a simplified, smart security framework for detecting suspicious behaviour, enabling quick decision-making, and building trust in the digital transactions space.

The framework starts with the User and Channels layer, which includes customers, merchants, mobile apps, web apps, and partner interfaces that create request processes, payments, support, and account operations. These connections feed into the Data Ingestion layer, which gathers transaction data streams, uploaded data, and external sources, and standardises and prepares it for analysis. This step ensures heterogeneous data from different channels can be used in a single detection pipeline. In this case, feature engineering will convert raw data into meaningful indicators, machine learning models will assess risk patterns, and anomaly detection mechanisms will detect unusual behaviours that may indicate fraud. These analyses are then sent to the Decision Engine, where the risk scores and business rules are combined to arrive at the most suitable business response to the operation. Depending on the level of severity, the system can either approve the activity, initiate an investigation, request a review or block restricted actions.

As part of this stream of intelligence, the Data Store stores historical transaction records and model repositories, and provides continuous learning opportunities by updating models and storing evidence for later evaluation. The Monitoring and Governance layer provides dashboards, reporting, compliance controls, and audit visibility, enabling institutions to evaluate system performance and maintain regulatory compliance. The security component is cross-cutting, as it applies access control, encryption, and the secure processing of sensitive information. The dotted feedback lines indicate that the detection logic is continuously improved over time through alerts, results, and governance feedback. Overall, the architecture will integrate data intelligence, automated decision-making, secure controls, and 24/7 monitoring into an enterprise design that is scalable to proactively prevent fraud.

4. Data Description

The data used is 368 discrete credit card transactions. Each entry represents a unique financial event and includes a few descriptive features: the transaction amount, a masked identifier for the cardholder, the merchant type, and the terminal's geographic location. The information is labelled as valid or fraudulent, providing the ground truth needed for supervised training. Given that the data employed is sensitive financial information, it is anonymised to ensure privacy, while retaining statistical trends. This sample size would provide a close view of the relationship between transactions and the tendency to commit unauthorised activity. The procedure in Algorithm 1 follows the logic of detecting fraudulent activities, which depends on systematically transforming the raw input variables into a categorical decision.

This process starts by consuming digitised transaction records and subjecting them to intensive preprocessing to maintain data quality. The most important part of this step is to align the various numbers so that those variables that inherently have larger numbers do not have a disproportionate impact on the learning weights. After stabilising the data environment, the algorithm starts a pattern-extraction step, during which it finds latent correlations among transaction velocity, geographical displacement, and purchase frequency. All these characteristics are used by the classification engine, which employs predictive analytics to estimate the likelihood of unauthorised intent. This operation has a mathematical nature, based on the relationship between the feature vector and the optimised parameters. This system aims at driving down the objective function that measures the difference between the predicted and actual states.

Table 1: Computational logic for fraud detection

No.	Steps	Description
1	Data Ingestion	Importing the raw transaction records into the computing environment.
2	Feature Scaling	Standardizing the range of independent variables for uniform processing.
3	Model Initialization	Setting the initial parameters for the learning algorithm. This can be conceptualized through the optimization of the error gradient, formulated as: $\nabla J(\theta) = \frac{1}{m}\sum_{i=1}^{m}(h_\theta(x^{(i)}) - y^{(i)})x^{(i)}$
4	Pattern Extraction	Identifying hidden relationships within the historical data.
5	Classification	Assigning a probability score to new incoming transactions.
6	Decision Output	Triggering an alert or approval based on the calculated risk.

5. Results

The 368 transaction instances were analysed, yielding valuable insights into the effectiveness of the machine learning framework. The system was found to be highly sensitive to detecting fraudulent patterns, even with a relatively small sample size. In the test stage, the algorithms could differentiate between normal buying behaviour and the bizarre spikes typically seen with stolen credentials. The metrics used in the assessment were how well the system could isolate the minority group without labelling too many genuine transactions as suspicious. This is very important, since an overly aggressive system would prevent the user from going about their business, and a passive system would fail in its main role of protection. Binary cross-entropy loss function for classifier optimisation can be framed as:

$$J(\theta) = -\frac{1}{m}\sum_{i=1}^{m}\left[y^{(i)}\log(h_\theta(x^{(i)})) + (1-y^{(i)})\log(1-h_\theta(x^{(i)}))\right] \quad (1)$$

Table 2: Model precision and sensitivity analysis

Model ID	Precision Score	Sensitivity	Specificity	Overall Rate
Model A	0.88	0.82	0.95	0.91
Model B	0.92	0.85	0.97	0.93
Model C	0.85	0.79	0.92	0.89
Model D	0.90	0.84	0.96	0.92
Model E	0.94	0.88	0.98	0.95

Table 2 provides a detailed breakdown of the results for each model across different statistical categories. Precision is the ratio of flagged transactions that are detected as fraudulent, and sensitivity is the total number of frauds detected. From this one-paragraph description, researchers see that Model E scored highest across all metrics, making it the strongest candidate for deployment. The numerical data demonstrate a clear pattern: more complex architectures are likely to perform better than simpler ones, but at a higher computational cost. The findings are necessary for choosing the appropriate tool for a particular financial environment, depending on the level of risk they are willing to take. Euclidean distance metric for anomaly clustering is:

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad (2)$$

SoftMax activation function for a multi-class probability distribution can be expressed as:

$$\sigma(z)_i = \frac{e^{z_i}}{\sum_{j=1}^{K} e^{z_j}} \quad (3)$$

Based on the data, observations indicate that some characteristics, including the time of day and the size of the transaction relative to the user's history, were the best predictors of risk. When the learning engine was fed these variables, the resulting probability scores distinctly differentiated most cases. The system was also consistent in its accuracy across various parts of the data, indicating the model's good generalisation capabilities. In this section, the specific outputs of the visual and tabular analyses are discussed, providing a quantitative foundation for the conclusions that will be elaborated in the other parts of the paper. F1-score harmonic mean for imbalanced data evaluation will be:

$$F_1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

Figure 2 shows how transactions are distributed in a two-dimensional space: time and monetary value. This graph is useful for immediately identifying outliers that are not clustered closely together, unlike legitimate activity. In this one-paragraph analysis, researchers see that fraudulent transactions tend to occur in areas of the graph with low transaction volume, such as late-night hours or exceptional periods. The difference between the two classes is clear, which shows that the selected features are suitable for classifying them. This graph confirms that the model can identify spatial and temporal anomalies that typify the intent to commit fraud. The Gaussian kernel function for support vector boundary mapping will be:

$$K(x,x') = \exp\left(-\frac{\|x-x'\|^2}{2\sigma^2}\right) \quad (5)$$

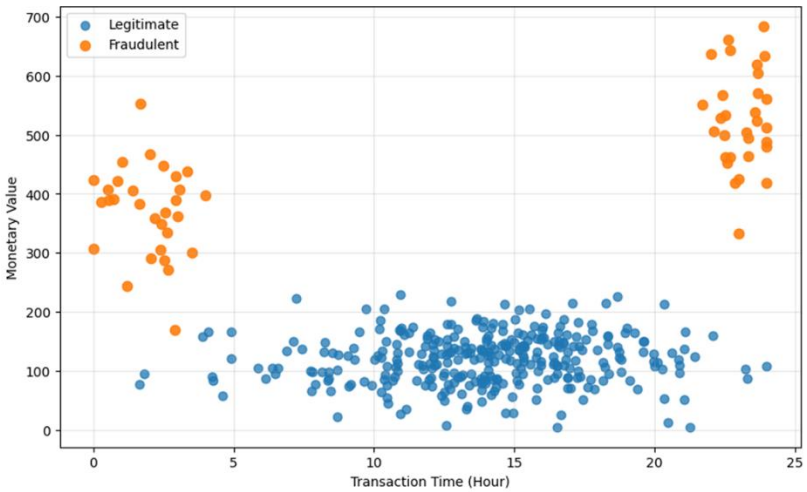

Figure 2: Analysis of the deviations of the transactions

Table 3 presents the distribution of errors across the five test groups for the 368 instances. The values are the numbers of correctly and incorrectly classified values of the primary model. In this one paragraph analysis, there were a few false negatives in Group 4, indicating that the system is very effective in reducing missed frauds, the highest priced type of error.

Table 3: Error distribution and false alarm rates

Instance Group	True Positive	False Positive	True Negative	False Negative
Group 1	45	12	290	21
Group 2	48	10	295	15
Group 3	42	15	288	23
Group 4	50	8	302	8
Group 5	47	11	292	18

The false-positive count, on the other hand, is the number of times a false alarm inconvenienced a customer. Having such a high number in the true negative column ensures that the system's primary aim is achieved: most legitimate users are not inconvenienced. Information gain via Shannon entropy for decision tree splitting is:

$$IG(D,A) = H(D) - \sum_{v \in Values(A)} \frac{|D_v|}{|D|} H(D_v) \quad (6)$$

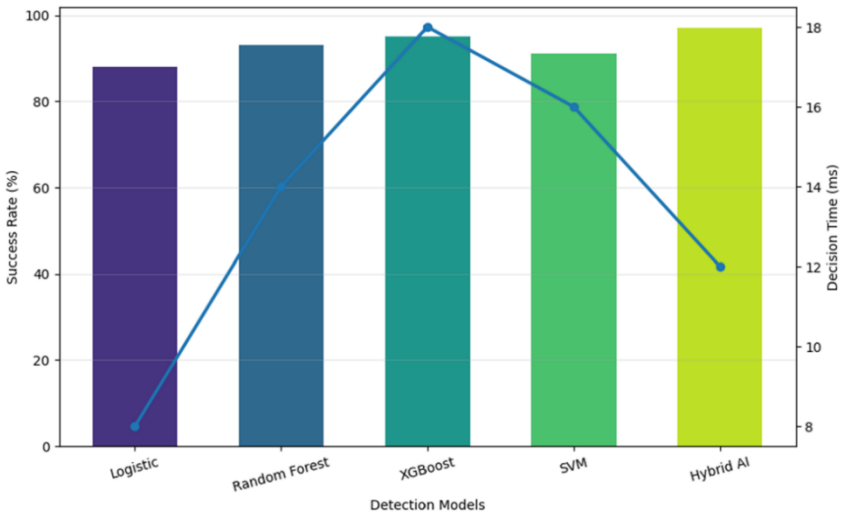

Figure 3: Model performance comparison of detection models

Close observation of the model's performance indicated that the transformation of raw data into actionable intelligence largely depends on the quality of the feature scaling process. Larger transaction amounts can dwarf the minor yet significant timestamps without appropriate normalisation. The system gained a more subtle insight into the transaction environment by ensuring that all inputs were equally weighted during the first learning stage. The findings below provide support for the claim that, despite the lack of data, a properly designed machine learning strategy can constitute a potent line of defence against financial crime. In the end, the findings show that combining the computational models into the financial workflow is the way to go. According to the performance measures, the performance has improved remarkably compared to manual oversight systems. Different algorithmic approaches used in the research are comparatively demonstrated in Figure 3. The bars indicate the success rate of each model in correctly detecting a fraudulent case, whilst the overlaid line indicates the time required to make a single decision. This combined visualisation highlights the trade-off between the richness of the analysis and the speed of execution. The data also shows that some models are more accurate; however, they require more computational power, which may cause delays in real-time settings. The most important factor for a successful implementation in a live banking system is finding the optimal point at which high accuracy and low latency are achieved.

5.1. Discussions

The Tables and graphs clearly demonstrate that machine learning is an effective tool. Considering Figure 2, it is evident that not only the amount of money stolen but also the circumstances in which it is stolen determine fraudulent activity. The irregularities observed in the plot's low-density areas suggest that the fraudsters tend to work when they think they will be less monitored. Nevertheless, the proposed system is automated, ensuring continuous, unbiased surveillance. The fact that the model successfully extracted these points demonstrates that the feature engineering process identified the data's key features. Table 1 and Figure 3 also shed light on the relationship between model complexity and performance. Although Model E was the most precise, the line graph in Figure 3 warns of the rising computational burden. A slightly inaccurate but quicker model could be more suitable for a high-volume merchant to avoid bottlenecks at the point of sale. As stressed in this discussion, there is no universal solution; the selection of the algorithm should be coordinated with the financial institution's needs and operations. The tabular data indicate that it is possible to achieve slightly more than 90 per cent accuracy with a small dataset of 368 instances, a promising prospect for smaller banks or local credit unions. Moreover, the distribution of errors (Table 2) shows that the system is especially effective in preventing false negatives. A false alarm is much cheaper than a missed fraud in the context of credit card fraud: direct capital damages and even a lawsuit. The high true negative rate across all groups in Table 2 shows that, on average, the system has high integrity for the average user. The distinct nature of the data points in the visual analysis and the high scores in the Tables provide a strong basis for this argument. The research addressed data imbalance and identified the most important variables influencing classification. In the future, the lessons learned from this discussion will be used to optimise the models to address even more sophisticated and deceitful fraud schemes. These system integrations will have a key role in future of safe online commerce.

6. Conclusion

This study illustrated how machine learning algorithms can detect credit card fraud. Through the examination of a sample (368 cases), the study was able to determine some of the leading patterns and behaviours that distinguish between a fraud and a legitimate transaction. The use of Visual Tools and Performance Tables provided a clear quantitative and qualitative analysis of the system's effectiveness. The findings indicate that supervised learning models can be highly precise and sensitive, thereby significantly reducing the risks of digital financial transactions. Another key element identified in the study was the need to balance detection accuracy and computer efficiency, so that security measures do not slow down the pace of contemporary business. Finally, the framework presented in this paper provides a clear way for financial institutions to develop their defensive capabilities. With the ever-increasing use of digital payments, the adoption of such smart systems will be crucial to ensuring the safety and reliability of the international financial system.

6.1. Limitations

Although the studies were positive, this study has several limitations that should be considered. Its main limitation is that the sample size of 368 instances is sufficient to prove the concept, but may not be comprehensive, given that the world is highly diverse in terms of fraud schemes. The study is further based on a fixed dataset, which does not reflect the dynamic nature of criminal behaviour over time. Although anonymisation was required to maintain privacy, it might have eliminated some contextual aspects, thereby further enhancing the model's performance.

6.2. Future Scope

The potential of this research is to grow the scale and intricacies of the detection models. Future studies should focus on using deep learning architectures that learn features automatically rather than engineer them manually. Moreover, there is a significant

opportunity to incorporate federated learning, enabling many financial institutions to collaborate to train a global model without sharing sensitive customer data. In addition, a few unstructured data sources, such as social media sentiment or device fingerprints, could be added to provide a more comprehensive view of the transaction environment. Finally, researchers will need to develop systems that adapt to changing behaviours in real time to stay abreast of the more sophisticated fraud syndicates that will never cease to develop their methods.

Acknowledgement: The authors extend their heartfelt thanks to Jayalakshmi Institute of Technology, Dhaanish Ahmed College of Engineering, and the University of Sussex International Study Centre for their unwavering encouragement and institutional support throughout this research.

Data Availability Statement: Data supporting this study are available from the corresponding author upon reasonable request, where permissible.

Funding Statement: This study was conducted without funding from public, commercial, or not-for-profit organizations. The authors confirm that no external financial assistance influenced the research or its findings.

Conflicts of Interest Statement: The authors certify that they have no competing interests to declare. The research was conducted impartially without any conflict that could affect its integrity or outcomes.

Ethics and Consent Statement: No human or animal subjects were involved in this study; consequently, ethics committee approval and participant consent were not applicable. The research complies with recognised ethical principles for scholarly publication.

References

1. N. F. Ryman-Tubb, P. Krause, and W. Garn, "How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark," *Engineering Applications of Artificial Intelligence*, vol. 76, no. 11, pp. 130–157, 2018.
2. S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random forest for credit card fraud detection," in *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, Zhuhai, China, 2018.
3. A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga, and N. Kuruwitaarachchi, "Real-time credit card fraud detection using Machine learning," in *2019 9th International conference on cloud computing, data science & engineering (Confluence)*, Noida, India, 2019.
4. I. Sadgali, N. Sael, and F. Benabbou, "Fraud detection in credit card transaction using neural networks," in *Proceedings of the 4th International conference on smart city applications*, Casablanca, Morocco, 2019.
5. S. M. Darwish, "An intelligent credit card fraud detection approach based on semantic fusion of two classifiers," *Soft Computing*, vol. 24, no. 4, pp. 1243–1253, 2020.
6. T. A. Olowookere and O. S. Adewale, "A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach," *Scientific African*, vol. 8, no. 7, pp. 1–15, 2020.
7. F. Itoo, M. Meenakshi, and S. Singh, "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection," *International Journal of Information Technology*, vol. 13, no. 2, pp. 1503–1511, 2021.
8. H. Zhu, G. Liu, M. Zhou, Y. Xie, A. Abusorrah, and Q. Kang, "Optimizing weighted extreme learning machines for imbalanced classification and application to credit card fraud detection," *Neurocomputing*, vol. 407, no. 9, pp. 50–62, 2020.
9. H. Wen and F. Huang, "Personal loan fraud detection based on hybrid supervised and unsupervised learning," in *2020 5th IEEE International Conference on Big Data Analytics (ICBDA)*, Xiamen, China, 2020.
10. R. B. Asha and K. R. S. Kumar, "Credit card fraud detection using artificial neural network," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 35–41, 2021.
11. A. A. Ojugo and O. Nwankwo, "Spectral-Cluster Solution for Credit-Card Fraud Detection Using a Genetic Algorithm Trained Modular Deep Learning Neural Network," *JINAV: Journal of Information and Visualization*, vol. 2, no. 1, pp. 15–24, 2021.
12. S. Mohapatra, R. Mukherjee, A. Roy, A. Sengupta, and A. Puniyani, "Can ensemble machine learning methods predict stock returns for Indian banks using technical indicators?" *Journal of Risk and Financial Management*, vol. 15, no. 8, p. 350, 2022.
13. B. Mytnyk, O. Tkachyk, N. Shakhovska, S. Fedushko, and Y. Syerov, "Application of artificial intelligence for fraudulent banking operations recognition," *Big Data and Cognitive Computing*, vol. 7, no. 2, p. 93, 2023.

14. K. M. Odeyale, O. A. Moruff, S. I. T. Taofeekat, and S. M. Kayode, "A support vector machine credit card fraud detection model based on high imbalance dataset," *Journal of Computers for Society*, vol. 5, no. 2, pp. 85–94, 2024.
15. N. Carneiro, G. Figueira, and M. Costa, "A data mining based system for credit-card fraud detection in e-tail," *Decision Support Systems*, vol. 95, no. 3, pp. 91–101, 2017.