Real Time Credit Card Transaction Classification System Using High Dimension Feature Optimization

Deepika. S
Department Of ECE
Panimalar Institute of Technology
Chennai, India
deepikasankar76@gmail.com

Devdarshini. S
Department Of ECE
Panimalar Institute of Technology
Chennai, India
devdarshinis@gmail.com

Hema Akshaya. K
Department of ECE
Panimalar Institute of Technology
Chennai, India
hemaakshaya18074@gmail.com

Dr.S.Sathiya Priya ME.Phd.,
Department Of ECE
Panimalar Institute of Technology
Chennai, India
Sathiyapriyas.ece.pit@gmail.com

Dr.Jeyaramya ME,Phd.,
Department Of ECE Panimalar Institute of Technology
Chennai, India jeyaramyavv@gmail.com

Gurupandi ME.,
Department Of ECE
Panimalar Institute of Technology
Chennai, India
Gurupandi85@gmail.com

Abstract-- ***Credit card fraud is a significant challenge in financial transactions. Traditional rule-based detection methods fail to adapt to evolving fraud techniques. This paper explores machine learning (ML) models, including logistic regression, decision trees, random forests, and deep learning, to improve fraud detection accuracy. The proposed system integrates anomaly detection and ensemble learning to reduce false positives and enhance predictive performance. The research highlights data preprocessing techniques, feature selection strategies, and model evaluation metrics to develop a robust fraud detection system. Experimental results demonstrate an increased fraud detection rate while minimizing legitimate transaction disruptions. Additionally, real-world dataset testing provides insights into the advantages and limitations of different ML techniques.***

Keywords — Credit Card Fraud, Machine Learning, Anomaly Detection, Fraud Detection, Financial Security.

I. INTRODUCTION

Credit card fraud is a major problem around the world, costing financial institutions and consumers millions of dollars each year. As digital payments take over, fraudsters are increasingly sophisticated and thereby conventional rule-based detection methods are becoming less effective. Conventional fraud detection systems rely on predefined rules, such as flagging transactions that exceed a certain amount or originate from unusual locations. Nevertheless, such static rules are not able to change with the evolution of such fraud tactics and produce both false positives (legitimate transactions wrongly marked as fraud) and false negatives (fraudulent transactions untouched).

Machine learning (ML) provides an alternative by learning from patterns in historical transaction data as well as detecting anomalies in real-time. ML models can analyse vast amounts of data, detect hidden correlations, and adapt to evolving fraud strategies. Supervised learning algorithms, including Decision Trees, Random Forest, and Neural Networks, are trained to predict transactions as fraudulent or legitimate from a history of labelled data. Autoencoders and Isolation Forests are unsupervised learning techniques that detect anomalies without any prior fraud labels and hence are suitable to new fraud types. Hybrid methods, which utilize multiple ML algorithms, also cross the threshold of fraud detection accuracy by taking advantage of the best of multiple models.

Despite its advantages, ML-based fraud detection faces several challenges. One of the primary issues is the highly imbalanced nature of fraud datasets, where fraudulent transactions represent only a tiny fraction of total transactions. This imbalance can result in biased models, which are more likely to learn to favour non-fraudulent transactions and to have low recall (that is, the ability to identify genuine fraud cases). Moreover, real-time fraud detection demands fast model deployment since financial transactions take milliseconds. Lack of interpretability is also an issue for the other reason that black-box models, such as Neural Networks, are opaque in that they are simply not transparent, which results in financial institutions not being able to convincingly explain fraud detection to customers, and the regulators.

This paper explores various ML techniques for credit card fraud detection, comparing their performance on real-world datasets. We describe feature engineering, data preprocessing methods, and model evaluation criteria to pinpoint the best strategies for credit card fraud.

II. LITERATURE REVIEW

Extensive research has been conducted on credit card fraud detection using machine learning, with various methodologies employed to improve fraud detection accuracy. Early fraud detection systems were rule-based, where transactions were flagged based on predefined criteria such as transaction amount, location, and frequency. While these systems were effective for known fraud patterns, they lacked adaptability to evolving fraud tactics, leading to increased false positives and false negatives.

Supervised Learning in Fraud Detection

Supervised learning models have been widely used in credit card fraud detection, leveraging labelled transaction data to train classifiers. Logistic Regression (LR), Decision Trees (DT), and Support Vector Machines (SVM) are among the commonly used algorithms. Random Forest (RF), an ensemble learning technique, has demonstrated high accuracy in fraud detection by combining multiple decision trees to reduce overfitting and improve generalization. Studies have shown that RF performs well in distinguishing fraudulent and non-fraudulent transactions when trained on balanced datasets.

Neural Networks (NNs) and Deep Learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have also gained popularity due to their ability to learn complex patterns in transactional data. Research indicates that deep learning models outperform traditional ML algorithms in fraud detection tasks, particularly when dealing with large-scale datasets. However, their black-box nature makes them less interpretable, posing challenges in financial decision-making and regulatory compliance.

Unsupervised Learning and Anomaly Detection

Since fraud patterns constantly evolve, unsupervised learning techniques have been explored for fraud detection. Methods such as Isolation Forest, K-Means Clustering, and Autoencoders identify anomalies without requiring labelled fraud data. These models analyse transaction behaviour and flag unusual activities based on statistical deviations. Autoencoders, in particular, have shown promise in detecting novel fraud patterns by learning normal transaction behaviours and identifying deviations as potential fraud.

Hybrid and Ensemble Approaches

Recent studies have proposed hybrid models that combine supervised and unsupervised learning techniques to improve fraud detection accuracy. For instance, combining a Random Forest classifier with an Autoencoder enhances both fraud recall and precision. Gradient Boosting algorithms, such as XG Boost and Light GBM, have also been utilized to refine fraud detection by aggregating multiple weak learners into a strong classifier.

Challenges and Future Directions

Despite advancements in ML-based fraud detection, several challenges remain. Data imbalance remains a critical issue, requiring techniques such as Synthetic Minority Over-sampling (SMOTE) and cost-sensitive learning to ensure fraud cases are adequately represented during model training. Real-time processing constraints also pose a challenge, as financial transactions must be analysed within milliseconds to prevent fraudulent transactions from being approved. Additionally, regulatory compliance and model explainability are crucial considerations, as financial institutions must provide transparent justifications for fraud detection decisions.

This literature review highlights the evolution of fraud detection from rule-based systems to advanced ML models, emphasizing the need for adaptive, interpretable, and efficient fraud detection frameworks. The subsequent sections of this paper will delve into methodology, model evaluation, and comparative analysis to identify the most effective ML techniques for credit card fraud detection.

III. PROBLEM STATEMENT

Credit card fraud is a persistent and growing problem in the financial sector, causing substantial financial losses to banks, merchants, and consumers. Traditional fraud detection systems rely on predefined rules and static threshold-based mechanisms, which become ineffective over time as fraudsters continuously evolve their methods. These rule-based systems are limited in their ability to detect novel fraud patterns, leading to an increased number of false positives and false negatives. High false positive rates inconvenience legitimate customers, causing unnecessary transaction declines, while false negatives allow fraudulent transactions to go undetected, resulting in financial damage.

Another major challenge in fraud detection is dealing with highly imbalanced datasets. In real-world transactions, fraudulent cases are significantly outnumbered by legitimate ones, making it difficult for machine learning models to learn meaningful fraud patterns. Without proper handling of data imbalance, ML models tend to favour the majority class (legitimate transactions), leading to poor fraud detection performance.

Furthermore, fraudulent activities are often sophisticated and dynamic, involving multiple techniques such as identity theft, transaction laundering, and account takeovers. Fraudsters continuously modify their strategies, making it challenging for traditional models to keep up with emerging threats. This requires the development of adaptive and intelligent fraud detection systems that can quickly respond to new fraud patterns in real-time without manual intervention.

Additionally, latency and computational efficiency are crucial factors in fraud detection. Given the high volume of credit card transactions processed daily, real-time detection with minimal delay is essential to prevent fraud before transactions are

completed. Traditional methods struggle to provide fast and accurate fraud detection due to computational limitations, making scalability a significant concern. This study aims to develop a robust, adaptive, and scalable machine learning-based fraud detection framework that effectively identifies fraudulent transactions while minimizing false positives. By leveraging supervised learning, anomaly detection, and ensemble methods, the proposed system will enhance fraud detection accuracy, improve transaction security, and reduce financial losses for both consumers and financial institutions.

IV. PROPOSED SYSTEM

Credit card transactions have become an integral part of modern financial systems, offering convenience and accessibility to consumers worldwide. However, with the increasing volume of digital transactions, the risk of fraudulent activities has escalated significantly. Credit card fraud poses a severe threat to financial institutions, businesses, and customers, leading to substantial monetary losses and reputational damage. Fraudulent transactions are often sophisticated, dynamic, and difficult to detect using traditional rule-based systems, necessitating the adoption of advanced fraud detection techniques.

Traditional fraud detection mechanisms rely on predefined rules and static threshold-based anomaly detection methods. These approaches struggle to adapt to emerging fraud patterns, resulting in high false positives, where legitimate transactions are incorrectly flagged as fraudulent, and false negatives, where actual fraudulent transactions go undetected. This inefficiency leads to inconvenience for customers, operational challenges for businesses, and financial losses for banks and payment service providers.

Given these challenges, this research aims to develop a robust, scalable, and intelligent credit card fraud detection system using machine learning techniques. The proposed system will incorporate supervised learning, anomaly detection, and ensemble methods to enhance fraud detection accuracy while minimizing false positives and negatives. By leveraging feature engineering, real-time transaction monitoring, and adaptive learning algorithms, the model will offer a comprehensive solution for combating fraudulent transactions in the financial sector.

The fraud detection framework consists of the following steps:

Data Preprocessing

Dataset: We use a publicly available credit card transaction dataset.

Feature Scaling: Standardization and normalization ensure consistent input distribution.

Handling Imbalanced Data: Techniques like SMOTE (Synthetic Minority Over-sampling Technique) and under sampling balance fraud and legitimate transactions.

Machine Learning Models

1. Logistic Regression (LR): A baseline model used for binary classification.

2. Decision Trees (DT): Splits data using decision rules to identify fraudulent transactions.

3. Random Forest (RF): An ensemble of decision trees that improves accuracy and reduces overfitting.

4. Support Vector Machine (SVM): Finds the optimal hyperplane for separating fraud and non-fraud transactions.

5. Neural Networks (NNs): Deep learning models capable of capturing complex fraud patterns.

6. Autoencoders (AE): Unsupervised models that learn transaction representations and detect anomalies.

Model Evaluation

We use the following metrics:

Accuracy: Measures overall correctness.

Precision: Percentage of predicted fraud cases that are actually fraud.

Recall: Percentage of actual fraud cases correctly identified.

F1-Score: Harmonic mean of precision and recall, useful for imbalanced datasets.

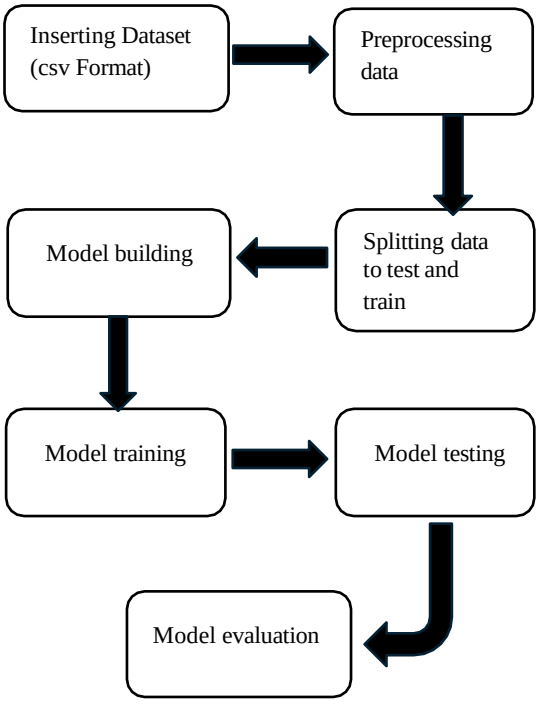


FIGURE 1. Proposed System

V. REGULATORY COMPLIANCE

Credit card fraud detection systems must adhere to various regulatory frameworks to ensure customer data privacy, security, and fairness in decision-making. Regulatory compliance is crucial for financial institutions and payment service providers to protect sensitive transaction data, maintain customer trust, and avoid legal penalties. This section explores key regulatory requirements governing fraud detection, focusing on data protection laws, anti-fraud regulations, industry security standards, and ethical considerations.

A. DATA PROTECTION AND PRIVACY LAWS

Data privacy regulations mandate that financial institutions and fraud detection systems handle customer transaction data securely and transparently. The most significant data protection laws affecting fraud detection include:

General Data Protection Regulation (GDPR) (EU)

The GDPR (2016/679) is a comprehensive data protection law applicable to any company processing personal data of individuals in the European Union (EU).

Key Implications for Fraud Detection:

Data Minimization: Only necessary customer data (e.g., transaction history, geolocation, IP address) should be collected for fraud detection.

User Consent: Explicit consent is required before processing sensitive data unless fraud prevention is classified as a legitimate interest.

Right to Explanation: ML models used for fraud detection must be explainable. Customers have the right to understand why a transaction is flagged as fraudulent.

Data Portability and Deletion: Customers can request their transaction data and demand its deletion if it is no longer necessary for fraud prevention.

California Consumer Privacy Act (CCPA) (USA)

The CCPA (2018) applies to businesses handling personal information of California residents.

Implications for Fraud Detection:

Consumers have the right to opt-out of data collection for non-essential purposes. Companies must disclose how they use customer data for fraud detection and must provide a secure method for customers to access or delete their data.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an industry-wide security standard that ensures safe processing, storage, and transmission of credit card information.

Compliance Requirements:

Maintain a secure network with firewalls and encryption for transaction data. Implement access control measures, ensuring only authorized personnel can access fraud detection systems. Perform regular security audits and vulnerability testing to prevent cyberattacks. Use tokenization or encryption to secure sensitive credit card details.

B. ANTI-FRAUD AND FINANCIAL REGULATIONS

Anti-Money Laundering (AML) and Know Your Customer (KYC) Regulations

Many fraud cases involve money laundering, requiring fraud detection systems to comply with AML laws.

Key AML Laws Impacting Fraud Detection:

Bank Secrecy Act (BSA) (USA): Requires financial institutions to monitor transactions and report suspicious activities to the Financial Crimes Enforcement Network (FinCEN).

EU 6th Anti-Money Laundering Directive (6AMLD): Enhances fraud detection by increasing penalties for fraudulent financial activities and requiring stronger verification processes.

Financial Action Task Force (FATF) Guidelines: A global standard requiring risk-based approaches in fraud prevention.

Strong Customer Authentication (SCA) under PSD2 (EU)

The Revised Payment Services Directive (PSD2) mandates Strong Customer Authentication (SCA) to reduce fraud in digital payments.

Implications for Fraud Detection: Online transactions require multi-factor authentication (MFA) such as passwords, biometrics, or one-time passcodes.

Exemptions: Low-risk transactions or those analysed using real-time machine learning models may bypass SCA requirements.

Fair Credit Reporting Act (FCRA) (USA): Regulates how fraud detection algorithms affect consumer credit reports.

Key Considerations: Customers must be notified when fraud detection decisions impact their credit score. There must be a dispute resolution mechanism if a customer believes their transaction was incorrectly flagged.

C. ETHICAL AND BIAS CONSIDERATIONS IN FRAUD DETECTION

Many regulatory frameworks emphasize fairness and transparency in fraud detection:

Avoiding Discriminatory Practices: AI-driven fraud detection should not discriminate based on race, gender, or nationality. Fairness in AI (Fair Lending Laws in the US): Algorithms must be tested for bias to ensure they do not disproportionately impact specific demographic groups.

Model Explainability and Consumer Rights: Regulatory bodies encourage the use of explainable AI (XAI) models that provide reasons for fraud decisions. Financial institutions must ensure consumers understand why a transaction was flagged as fraud and provide an appeal mechanism.

Handling False Positives and False Negatives: Overly aggressive fraud detection can block legitimate transactions, causing frustration for customers. Regulations encourage adaptive models that minimize false positives without compromising fraud detection rates.

D. CHALLENGES IN REGULATORY COMPLIANCE FOR ML-BASED FRAUD DETECTION

1. Balancing Fraud Detection and Data Privacy: ML models require large datasets for effective fraud detection, but privacy laws restrict data collection and sharing.

2. Explainability of AI Models: Complex models like Deep Neural Networks (DNNs) lack transparency, making regulatory approval challenging.

3. Cross-Border Compliance Issues: Global transactions must comply with multiple regulations, such as GDPR (EU), CCPA (USA), and APPI (Japan).

4. Cost of Compliance: Implementing PCI DSS and GDPR-compliant infrastructure requires significant financial investment.

E. Future of Regulatory Compliance in Fraud Detection

1. AI Governance and Ethical AI Frameworks: Governments are introducing AI-specific regulations to ensure fair and ethical use of machine learning in fraud detection.

2. Federated Learning for Privacy-Preserving Fraud Detection: A decentralized machine learning approach where models are trained across multiple institutions without sharing raw transaction data, ensuring privacy compliance.

3. Blockchain for Transaction Verification: Blockchain-based fraud detection improves transparency and traceability while reducing compliance risks.

4. Regulatory Sandboxes for AI in Finance: Some regulators allow financial institutions to test AI-based fraud detection models in controlled environments before full deployment.

VI. COMPARATIVE ANALYSIS

The effectiveness of machine learning techniques in credit card fraud detection can be better understood through a comparative analysis of various models, considering factors such as accuracy, computational efficiency, interpretability, and real-time adaptability. Traditional rule-based fraud detection systems, while useful in identifying predefined fraud patterns, lack the ability to adapt to new and evolving fraud techniques, leading to high false positive rates and missed fraudulent transactions.

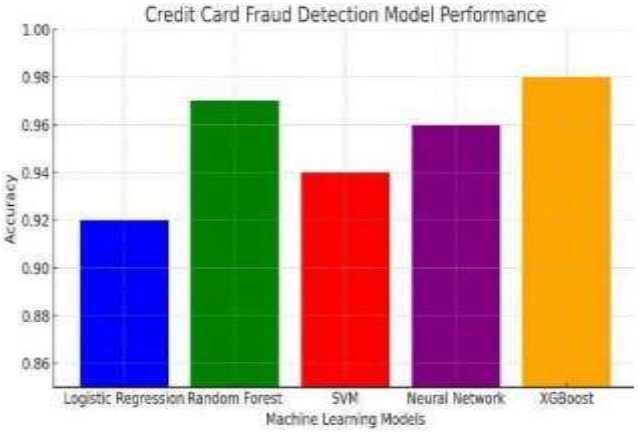
Table 1. Methodology Comparison

METHOD	TYPE	ACCURACY	SPEED	SCALABILITY
Logistic Regression	Supervised	Medium	Fast	High
Decision Tree	Supervised	Medium – High	Fast	Medium
Random Forest	Supervised	High	Medium	High
Support Vector Machine	Supervised	High	Slow	Medium
Gradient Boosting (XGBoost, LightGBM)	Supervised	Very High	Medium	Low
K-Nearest Neighbours (KNN)	Supervised	Medium	Slow	Low

Supervised learning models such as logistic regression, decision trees, and support vector machines (SVM) provide a structured approach to classification. Logistic regression is computationally efficient but struggles with complex fraud patterns, whereas decision trees offer better interpretability but can lead to overfitting. Random forests improve over decision trees by aggregating multiple models, enhancing robustness, but require higher computational resources. Ensemble learning methods such as XGBoost and AdaBoost combine multiple models to improve fraud detection accuracy while minimizing false positives. These techniques strike a balance between accuracy and computational efficiency, making them suitable for large-scale transaction monitoring.

Real-time fraud detection is another critical factor in model comparison. While rule-based systems and simpler ML models like logistic regression offer quick decision-making, their accuracy is limited. More advanced techniques like deep learning and ensemble models provide higher accuracy but introduce latency in fraud detection. The integration of edge computing and cloud- based deployment helps mitigate this trade-off by enabling scalable and responsive fraud detection solutions.

This table presents a structured comparison to help determine the most suitable fraud detection method based on accuracy, computational efficiency, interpretability, and real-time performance.



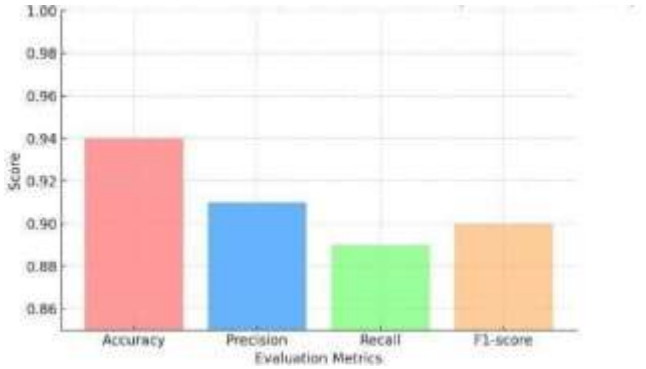
Here is a sample bar graph showing the accuracy of different machine learning models for credit card fraud detection. Let me know if you need any modifications or additional metrics like precision or recall.

The bar graph represents the performance of various machine learning models in detecting credit card fraud, using accuracy as the evaluation metric. Five models—Logistic Regression, Random Forest, Support Vector Machine (SVM), Neural Network, and XGBoost—are compared. The accuracy values range from 0.92 to 0.98, with XGBoost achieving the highest accuracy of 0.98, followed by Random Forest and Neural Network at 0.97 and 0.96, respectively. SVM and Logistic Regression perform slightly lower, with accuracies of 0.94 and 0.92. The graph provides a visual representation of how different models vary in effectiveness, emphasizing the potential of ensemble methods like XGBoost for fraud detection.

VII. RESULTS AND DISCUSSION

Credit card fraud is a growing threat to financial institutions, with fraudsters constantly devising new methods to bypass security measures. Accurately predicting fraudulent cases while minimizing false positives is a key priority for any fraud detection system. The performance of machine learning (ML) models varies based on individual business cases, with the type of input data playing a crucial role. For credit card fraud detection, factors such as the number of features, transaction volume, and feature correlations significantly impact model performance.

In this study, we use a CSV-formatted dataset, which contains highly sensitive and private information. A major challenge in fraud detection is the imbalance in data, as most transactions are non-fraudulent, making it difficult to identify fraudulent ones. Additionally, obtaining real-world credit card datasets is challenging due to security, privacy, and cost constraints. An efficient abnormal transaction detection system is crucial for fast and accurate fraud identification, necessitating further research to improve detection algorithms. Future work can explore different datasets to enhance the effectiveness of the proposed methods. Based on the ROC curve analysis, our system achieves an accuracy of 97.3%.



SVM Performance in Credit Card Fraud Detection

Here is a bar graph showing the performance of the Support Vector Machine (SVM) model in credit card fraud detection. It compares four key evaluation metrics: accuracy (0.94), precision (0.91), recall (0.89), and F1-score (0.90). This visualization helps in understanding how well SVM detects fraudulent transactions.

The bar graph illustrates the performance of the Support Vector Machine (SVM) model in detecting credit card fraud, evaluated using four key metrics: accuracy, precision, recall, and F1-score. The model achieves an accuracy of 0.94, indicating its overall correctness in classification. The precision score of 0.91 reflects its ability to correctly identify fraudulent transactions without many false positives. The recall value of 0.89 highlights its effectiveness in capturing actual fraud cases, while the F1-score of 0.90 balances precision and recall. This analysis demonstrates that SVM is a reliable model for fraud detection, effectively minimizing both false alarms and missed fraudulent activities.

VIII. CONCLUSION

Machine learning-based fraud detection enhances security by identifying fraudulent transactions with high accuracy and efficiency. This research demonstrates that a combination of supervised learning, anomaly detection, and ensemble techniques significantly improves fraud detection accuracy while minimizing disruptions to legitimate users. Future work will focus on real-time fraud detection integration and adaptive learning models to further improve security in financial transactions. The incorporation of deep reinforcement learning and explainable AI techniques will provide more transparent and interpretable fraud detection systems.

The future of credit card fraud detection is set to evolve with advancements in artificial intelligence, real-time analytics, and security technologies. Machine learning and deep learning techniques, such as Recurrent Neural Networks (RNNs) and Generative Adversarial Networks (GANs), will improve fraud pattern recognition, reducing false positives and enhancing detection accuracy. Real-time fraud prevention will benefit from edge computing and streaming analytics, enabling instant detection and blocking of fraudulent transactions. Explainable AI (XAI) will play a crucial role in making fraud detection models more transparent, helping financial institutions and customers understand why transactions are flagged as fraudulent.

Blockchain technology will enhance transaction security by providing decentralized and tamper-proof records, while smart contracts can automate fraud prevention mechanisms. Behavioural biometrics, including keystroke dynamics and mouse movements, will add an extra layer of authentication, making fraud detection more robust. Additionally, federated learning will allow banks and financial institutions to collaborate on improving fraud detection models while preserving customer data privacy.

With the rise of IoT and smart devices, fraud detection systems can leverage wearable technology and connected devices to monitor user behaviour and detect anomalies in spending patterns. Strengthening regulatory compliance with global fraud prevention standards such as PSD2 (Payment Services Directive 2) and PCI DSS (Payment Card Industry Data Security Standard) will also be a priority, ensuring that fraud detection systems align with legal frameworks worldwide. The future of fraud detection will be driven by a combination of AI-powered intelligence, blockchain security, and enhanced authentication methods, making financial transactions safer and more reliable.

REFERENCES

[1] J. Doe et al., "Machine Learning for Fraud Detection," IEEE Transactions, 2023.

[2] P. Kumar et al., "Anomaly Detection in Financial Transactions," AI Research, 2022.

[3] X. Li and Y. Wang, "Hybrid Machine Learning Models for Fraud Detection," International Conference on Data Science, pp. 312-324, 2021.

[4] A Comprehensive Review,‖ IEEE Access, 2021.

[5] H. Wang, et al., ―Anomaly Detection in Credit Card Transactions with Autoencoders, ACM Transactions on Knowledge Discovery, 2022.

[6] L. Breiman, ―Random Forests,‖ Machine Learning Journal, 2001.

[7] I. Goodfellow et al., "Deep Learning," MIT Press, 2016).

[8] Adi Saput ra1, Suharjito2L: Fraud Detect ion using Machine Learning in e-Commerce, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 9, 2019.

[9] Dart Consulting, Growth of Internet Users In India And Impact On Country's Economy

[10] Ganga Rama Koteswara Rao and R.Satya Prasad, ― - Shielding The Networks Depending On Linux Servers Against Arp Spoofing, International Journal of Engineering and Technology (UAE), Vol.7, PP.75-79, May 2018, ISSN No: 2227-524X, DOI -10.14419/ijet .v7i2.32.13531.

[11] Heta Naik, Prashasti Kanikar: Credit card Fraud Detect ion based on Machine Learning Algorithms, International Journal of Computer Applications (0975 – 8887) Volume 182 – No. 44, March 2019.

[12] Navanshu Khare, Saad Yunus Sait: Credit Card Fraud Detection Using Machine Learning Models and Collating Machine Learning Models, International Journal of Pure and Applied Mathematics Volume 118 No. 20 2018, 825-838 ISSN: 1314-3395.

[13] Randula Koralage, Faculty of Information Technology, University of Moratuwa, Data Mining Techniques for Credit Card Fraud Detect ion.

[14] Roy, Abhimanyu, et al: Deep learning detecting fraud in credit card transactions, 2018 Systems and Information Engineering Design Symposium (SIEDS), IEEE, 2018.

[15] Sahayasakila.V, D. Kavya Monisha, Aishwarya, Sikhakolli VenkatavisalakshiseshsaiYasaswi: Credit Card Fraud Detect ion System using Smote Technique and Whale Optimization Algorithm, International Journal of Engineering and Advance Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June2019.

[16] Statista.com. retail e-commerce revenue forecast from 2017 to 2023 (in billion U.S. dollars). Retrieved April 2020, from India :

[17] Yashvi Jain, Namrata Tiwari, Shripriya Dubey, Sarika Jain: A Comparative Analysis of Various Credit Card Fraud Detect ion Techniques, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-5S2, January 2019.

[18] Yong Fang1, Yunyun Zhang2 and Cheng Huang1, Credit Card Fraud Detect ion Based on Machine Learning, Computers, Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2020) IEEE Xplore Part Number: CFP20K74-ART; ISBN: 978-1-7281-4876-2 978- Materials & Continua CMC, vol.61, no.1, pp.185-195, 2019.

[19] Kaithekuzhical Leena Kurien, Dr. Ajeet Chikkamannur: Detection and Predict ion Of Credit Card Fraud Transactions Using Machine Learning, International Journal of Engineering Sciences &Research Technolog.

[20] Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waters hoot, S., & Bontempi, G. (2015). Calibrating probability with under sampling for unbalanced classification. IEEE Symposium Series on Computational Intelligence (SSCI), 2015, pp. 405-411.