*Eksplorium* *p*-ISSN 0854-1418
Volume 46 No. 2, June 2025: 637–649 *e*-ISSN 2503-426X

# Application of Artificial Intelligence in Fraud Detection in the Banking Sector

**Dr. J Saradha, Dr. M Suresh, Dr. V. Ramidha, Dr Datrika Venkata Madhusudan Rao, Dr. Shreevamshi Naveen, Dr. Mutyala Subramanyam**
Assistant Professor, Department of Management Studies,
SRM Institute of Science and Technology (Deemed to be University),
Tiruchirappalli, Tamil Nadu, India
Assistant Professor, Department of Management Studies,
SRM Institute of Science and Technology (Deemed to be University),
Tiruchirappalli, Tamil Nadu, India
Assistant Professor, Department of Management Studies,
SRM Institute of Science and Technology (Deemed to be University),
Tiruchirappalli, Tamil Nadu, India
Associate Professor, School of Management, CMR University, Bengaluru, Karnataka
Email: venkatamadhusudan.r@cmr.edu.in
Associate professor, Dayananda Sagar College of Engineering
Department of Management Studies, Shavige Malleshwara Hills, 91st Main Rd, 1st Stage, Kumaraswamy Layout, Bengaluru, 560078
Karnataka, Nshree118@gmail.com
Professor, School of Management,
CMR University (Lakeside Campus) Bengaluru; Karnataka.
drmutyala2013@gmail.com
Article Received: 10 May 2025, Revised: 14 June 2025, Accepted: 25 June 2025

**Abstract**

The rapid digitization of banking services has increased the susceptibility of financial systems to fraudulent activities. In response, Artificial Intelligence (AI) has emerged as a powerful tool in detecting and preventing fraud in the banking sector. This paper explores the various AI-driven techniques such as machine learning algorithms, neural networks, and natural language processing used to analyze vast volumes of transactional data in real-time. These technologies enable the identification of suspicious patterns, anomaly detection, and predictive risk assessment, significantly enhancing the speed and accuracy of fraud detection systems. Furthermore, AI models continuously learn from evolving fraud tactics, making them more adaptive and robust than traditional rule-based systems. Despite its advantages, the adoption of AI also presents challenges related to data privacy, algorithmic bias, and regulatory compliance. This study highlights the current applications, benefits, limitations, and prospects of AI in fraud detection, aiming to contribute to the development of more secure and intelligent banking ecosystems.

**Keywords:** Artificial Intelligence, Fraud Detection, Banking Sector, Machine Learning, Anomaly Detection, Financial Security, Predictive Analytics, Real-Time Monitoring.

## 1. Introduction

The digital transformation of the banking sector has revolutionized financial services, enhancing convenience and accessibility for customers. However, this digital shift has also led to a surge in fraudulent activities, including identity theft, phishing, account takeovers, and transaction fraud. According to a 2022 report by the Association of Certified Fraud Examiners (ACFE), financial institutions face some of the highest rates of fraud, incurring losses worth

billions of dollars annually. Traditional fraud detection methods, which rely heavily on predefined rules and manual reviews, have proven to be insufficient in combating increasingly sophisticated fraud schemes (West & Bhattacharya, 2016). Artificial Intelligence (AI) has emerged as a transformative technology capable of addressing these challenges through intelligent data analysis and predictive modeling. By leveraging machine learning, neural networks, and real-time data processing, AI systems can detect anomalous behavior and flag suspicious transactions more accurately and rapidly than human analysts (Ngai et al., 2011). These technologies enable banks to move from reactive fraud detection to proactive fraud prevention, significantly reducing both fraud losses and false positives. Moreover, the application of AI in fraud detection supports the scalability and adaptability of security systems, allowing them to learn from new fraud patterns and evolve accordingly. This research explores the implementation, effectiveness, and challenges of AI in fraud detection within the banking sector, aiming to provide insights into current practices and future innovations that could further strengthen financial security.

## 2. Evolution of Fraud Detection Techniques

Fraud detection in the banking sector has evolved significantly over the past few decades, transitioning from traditional manual systems to advanced, data-driven technologies. Initially, banks relied on **rule-based systems** and **manual audits** to detect suspicious activities. These systems were based on predefined rules and thresholds, such as flagging transactions exceeding a certain amount or involving high-risk countries. While useful in catching known fraud patterns, such approaches lacked adaptability and often failed to detect novel or sophisticated fraud schemes (Bolton & Hand, 2002). With the growth of online banking and digital transactions in the late 1990s and early 2000s, the volume and complexity of financial data increased exponentially. This prompted the integration of **statistical methods and data mining** techniques for fraud detection. These approaches involved analyzing historical transaction data to uncover hidden patterns and correlations indicative of fraudulent behavior (Phua et al., 2005). Despite offering improvements, these techniques were often static, limited in real-time capabilities, and prone to high false-positive rates.

The introduction of **machine learning (ML)** and **artificial intelligence (AI)** marked a paradigm shift in fraud detection. Unlike rule-based systems, AI models can learn from large datasets and identify complex, non-linear patterns. They continuously adapt to emerging fraud tactics without needing explicit programming. Techniques such as supervised learning, unsupervised anomaly detection, neural networks, and ensemble methods have proven effective in identifying subtle and previously unknown fraud activities in real-time (Kirkos et al., 2007). Today, AI-driven systems are integrated with **real-time transaction monitoring**, **behavioral analysis**, and **biometric verification**, providing banks with a robust and proactive approach to combating financial fraud. This evolution reflects a broader trend toward automation, adaptability, and predictive intelligence in financial security systems.

## 3. AI Technologies Used in Fraud Detection

The application of Artificial Intelligence (AI) in banking fraud detection encompasses a range of advanced technologies designed to process large datasets, identify anomalous patterns, and predict fraudulent activities in real time. These technologies outperform traditional systems by offering scalability, speed, and adaptability to evolving fraud tactics.

### 3.1 Machine Learning (ML)

Machine Learning is one of the most widely adopted AI technologies in fraud detection. ML models are trained on historical transaction data to classify transactions as fraudulent or legitimate. **Supervised learning algorithms** (e.g., decision trees, random forests, support vector machines) are used when labeled datasets are available, allowing the system to learn the characteristics of fraud patterns. **Unsupervised learning algorithms**, such as clustering and autoencoders, are employed to detect outliers or anomalies without prior labeling, making them suitable for discovering unknown fraud schemes (Bhattacharyya et al., 2011).

### 3.2 Deep Learning and Neural Networks

Deep learning models, particularly **Convolutional Neural Networks (CNNs)** and **Recurrent Neural Networks (RNNs)**, are increasingly used for their ability to process sequential data and extract complex features. RNNs, including **Long Short-Term Memory (LSTM)** networks, are particularly effective for analyzing time-series transaction data and identifying suspicious behavioral trends over time (Jurgovsky et al., 2018).

### 3.3 Natural Language Processing (NLP)

NLP is applied in the analysis of unstructured data such as customer emails, chat logs, and social media content. It helps detect phishing attempts, social engineering schemes, and fraudulent documentation by extracting relevant information and identifying inconsistencies or malicious intent in textual data (Chen et al., 2020).

### 3.4 Anomaly Detection Algorithms

Anomaly detection plays a central role in identifying deviations from established transaction behavior. AI systems use statistical and ML-based anomaly detection models to flag transactions that significantly deviate from a customer's normal activity pattern. Techniques like **Isolation Forests**, **k-means clustering**, and **Gaussian Mixture Models (GMMs)** are commonly used for this purpose (Ahmed et al., 2016).

### 3.5 Hybrid and Ensemble Methods

Hybrid models that combine multiple ML algorithms known as **ensemble methods** enhance detection accuracy and reduce false positives. Techniques like **bagging**, **boosting**, and

**stacking** are employed to merge the strengths of different models, leading to more robust and reliable fraud detection systems (Liu et al., 2020).

## 4. Real-Time Fraud Detection Using AI

The dynamic nature of financial fraud, characterized by its rapid execution and ever-evolving tactics, necessitates robust real-time detection mechanisms. Artificial Intelligence (AI) enables banks to monitor and analyze transactions as they occur, thereby identifying and mitigating fraudulent activities before they cause significant damage. Real-time fraud detection combines **streaming data analytics**, **machine learning**, and **behavioral modeling** to deliver instantaneous decision-making capabilities.

### 4.1 Transaction Monitoring

AI systems are designed to track large volumes of transactional data across multiple platforms (e.g., ATMs, mobile banking, online portals) in real time. **Machine learning algorithms** evaluate each transaction based on features like amount, location, device ID, and user behavior, comparing them against historical patterns to detect deviations. Real-time scoring engines assign risk levels to transactions and automatically trigger alerts or block suspicious activity (Ngai et al., 2011).

### 4.2 Behavioral Biometrics and User Profiling

AI enhances fraud detection by creating detailed profiles of user behavior, such as keystroke dynamics, mouse movement patterns, and mobile device orientation. These biometric signals are analyzed using **deep learning models** to differentiate between legitimate users and impostors in real time (Conti et al., 2021). By continuously learning and updating user behavior models, the system can detect even subtle changes that may indicate account takeover attempts.

### 4.3 Pattern Recognition and Outlier Analysis

Real-time fraud detection leverages **anomaly detection algorithms** to identify outliers—transactions that significantly deviate from normal behavior. For instance, if a customer usually makes small purchases within their locality but suddenly initiates a high-value transaction overseas, the system flags it for review. Models like **autoencoders** and **Isolation Forests** are commonly used for such tasks (Ghosh & Reilly, 1994; Ahmed et al., 2016).

### 4.4 Integration with AI-Powered Decision Engines

Modern fraud detection systems integrate AI models with decision engines that enforce fraud prevention policies instantly. These engines apply complex business rules, regulatory guidelines, and risk scores to determine the appropriate action approve, deny, or hold the transaction for manual review within milliseconds (Kumar & Ravi, 2016).

### 4.5 Examples in Practice

Many banks now use AI-powered platforms such as **SAS Fraud Management**, **FICO Falcon**, and **Feedzai**, which combine machine learning, graph analytics, and real-time processing to provide scalable fraud prevention solutions. These platforms support real-time feedback loops, allowing continuous model refinement and increased detection precision over time.

## 5. Case Studies and Applications

The adoption of Artificial Intelligence (AI) in fraud detection is no longer theoretical it has been actively implemented across global banking institutions, yielding significant improvements in fraud prevention. This section presents real-world case studies and applications that illustrate how banks and financial service providers use AI to combat fraud effectively.

### 5.1 HSBC – AI-Powered Transaction Monitoring

HSBC, one of the world's largest banking institutions, implemented an AI-powered fraud detection system developed in collaboration with **Quantexa**, a contextual decision intelligence platform. The solution uses **graph analytics** and **machine learning** to map relationships among customers, accounts, and transactions, enabling early detection of complex fraud rings and money laundering schemes. HSBC reported a significant increase in suspicious activity report (SAR) accuracy and reduction in false positives after implementing this system (HSBC Annual Report, 2021).

### 5.2 JPMorgan Chase – Deep Learning for Anomaly Detection

JPMorgan Chase utilizes **deep learning and neural networks** to analyze millions of transactions in real time. Their proprietary system, COiN (Contract Intelligence), originally developed for legal document review, has been extended to fraud detection and risk management. COiN helps identify anomalous transaction behaviors and automates decision-making processes, enabling faster and more accurate fraud detection (JPMorgan Chase, 2020).

### 5.3 HDFC Bank – AI Chatbot and Fraud Prevention

India's HDFC Bank uses an AI-based chatbot called **Eva**, developed by Senseforth.ai, which also integrates fraud detection capabilities. Eva interacts with users to resolve queries but also flags suspicious interactions and transactions in real-time. Behind the scenes, HDFC leverages AI and ML models for customer behavior analysis and credit card fraud detection, leading to a measurable decrease in fraud-related losses (HDFC Sustainability Report, 2022).

### 5.4 PayPal – Hybrid AI Systems for Fraud Detection

Although not a traditional bank, PayPal offers financial services and is a pioneer in using **hybrid AI systems** for fraud detection. It employs ensemble models combining logistic

regression, decision trees, and neural networks to monitor over **1 billion transactions** monthly. The system evaluates transactions in milliseconds and prevents thousands of fraud attempts daily, with continuously updated algorithms (Bhatla et al., 2003; PayPal Engineering Blog, 2021).

### 5.5 Feedzai – AI Fraud Detection as a Service

Feedzai is an enterprise AI company whose fraud detection platform is used by numerous banks, including **Banco do Brasil** and **Standard Chartered**. The platform uses **real-time data ingestion**, **anomaly scoring**, and **adaptive machine learning models** to block fraudulent activity before it completes. Banks using Feedzai report up to 95% reduction in false positives and significant cost savings (Feedzai Case Studies, 2021).

## 6. Benefits of AI in Fraud Detection

Artificial Intelligence (AI) has significantly transformed fraud detection in the banking sector, offering numerous advantages over traditional systems. AI technologies not only improve the **accuracy and speed** of detection but also enable proactive fraud prevention, dynamic risk assessment, and intelligent decision-making. The following are key benefits AI brings to fraud detection systems:

### 6.1 Enhanced Accuracy and Reduced False Positives

AI systems can analyze vast datasets and learn from historical patterns, enabling them to **distinguish between legitimate and fraudulent transactions** with high precision. Unlike rule-based systems, which often trigger false alarms, AI models continuously adapt to evolving fraud behaviors and improve over time. According to West and Bhattacharya (2016), machine learning algorithms reduce false positives by up to **30–50%** compared to traditional methods.

### 6.2 Real-Time Detection and Response

AI algorithms can process and evaluate transactions in milliseconds, enabling **real-time fraud detection**. This speed is crucial in preventing financial loss, especially in online and card-not-present transactions. Tools like neural networks and anomaly detection models help banks intervene before fraudulent transactions are completed (Jurgovsky et al., 2018).

### 6.3 Proactive and Predictive Capabilities

AI can go beyond detection by using **predictive analytics** to identify customers or accounts at high risk of fraud before any suspicious activity occurs. By learning behavioral patterns and identifying anomalies, AI systems can flag potential threats and recommend preventive actions. This predictive capability significantly enhances fraud risk management (Ngai et al., 2011).

### 6.4 Scalability and Efficiency

AI systems can **scale easily** to handle millions of transactions per second, making them ideal for large financial institutions with high transaction volumes. Additionally, automation of fraud detection processes reduces the need for manual reviews, lowering operational costs and improving resource efficiency (Kirkos et al., 2007).

### 6.5 Continuous Learning and Adaptability

AI models, particularly those based on **deep learning**, are capable of **self-learning**. They evolve with new data and fraud trends, improving their performance without requiring constant reprogramming. This adaptability is essential in combating the constantly changing nature of financial fraud (Sahin et al., 2013).

### 6.6 Improved Customer Experience

By accurately identifying genuine transactions and reducing the number of declined legitimate purchases, AI helps to **enhance customer trust** and satisfaction. Banks can ensure security without compromising the convenience of digital banking services.

## 7. Challenges and Limitations

While Artificial Intelligence (AI) offers transformative potential in fraud detection, its implementation in the banking sector is not without challenges. From technical complexities to ethical concerns, several barriers can hinder the full realization of AI's capabilities. Understanding these challenges is crucial for developing secure, fair, and reliable AI-based fraud detection systems.

### 7.1 Data Privacy and Security Concerns

AI systems require access to vast amounts of customer data to function effectively. This raises **data privacy** issues, especially with regulations like the **General Data Protection Regulation (GDPR)** in the EU and **India's Digital Personal Data Protection Act (2023)**. Improper handling of sensitive data can lead to legal consequences and erosion of customer trust (Zarsky, 2016).

### 7.2 Algorithmic Bias and Fairness

AI models can inadvertently learn and perpetuate **biases** present in historical data. For example, certain demographics may be disproportionately flagged as high risk, resulting in **unfair treatment** and reputational risks for banks. Ensuring fairness and transparency in AI decisions remains a major ethical and technical challenge (Barocas et al., 2019).

### 7.3 Lack of Explainability (Black-Box Models)

Many advanced AI models especially deep learning systems operate as **black boxes**, meaning their decision-making processes are not easily interpretable. This lack of transparency poses problems for regulatory compliance and reduces trust among stakeholders. **Explainable AI (XAI)** techniques are still evolving and not widely adopted in banking systems (Doshi-Velez & Kim, 2017).

### 7.4 High Implementation Costs and Technical Complexity

Deploying AI systems involves **significant investment** in infrastructure, skilled personnel, and data integration. Many small and mid-sized banks lack the resources to implement and maintain such systems. Additionally, the **integration of AI with legacy systems** can be complex and time-consuming (Patil & Patil, 2020).

### 7.5 Data Quality and Imbalanced Datasets

Effective AI models depend on **high-quality, labeled, and balanced datasets**. In fraud detection, fraudulent transactions are rare compared to legitimate ones, creating **class imbalance** that can reduce model accuracy. Poor data quality or noise can also mislead learning algorithms, resulting in ineffective models (Dal Pozzolo et al., 2015).

### 7.6 Evolving Fraud Techniques

Fraudsters continuously adapt to new detection mechanisms, developing **evasion strategies** that can bypass AI models. As fraud tactics evolve, AI systems must be regularly updated and retrained to remain effective. This constant evolution requires **ongoing monitoring and model maintenance** (Sahu & Gupta, 2021).

## 8. Regulatory and Compliance Considerations

The integration of Artificial Intelligence (AI) into fraud detection systems in the banking sector necessitates careful alignment with existing regulatory and compliance frameworks. As AI technologies analyze vast amounts of personal and financial data, regulatory bodies emphasize the need for **ethical usage**, **transparency**, **data protection**, and **accountability**. Ensuring AI-based systems comply with both national and international standards is critical for legal operation, customer trust, and risk mitigation.

### 8.1 Data Protection and Privacy Laws

AI systems process sensitive personal and transactional data, making compliance with data protection regulations essential. The **General Data Protection Regulation (GDPR)** in the European Union mandates transparency, data minimization, and individuals' rights over automated decision-making (Voigt & Von dem Bussche, 2017). In India, the **Digital Personal**

**Data Protection Act, 2023** enforces similar obligations, requiring financial institutions to ensure **consent-based processing**, **data localization**, and **purpose limitation**.

### 8.2 Regulatory Oversight by Central Banks

In many countries, central banks play a pivotal role in guiding the ethical deployment of AI in banking. The **Reserve Bank of India (RBI)**, for instance, has released guidelines on **digital lending**, **cybersecurity**, and **risk-based supervision** that indirectly govern AI-based fraud detection systems. Banks are expected to maintain **auditable models**, **robust governance**, and **periodic reviews** of AI applications to ensure compliance with supervisory expectations (RBI, 2022).

### 8.3 Need for Explainable AI (XAI)

Regulators increasingly demand that decisions made by AI systems, especially in high-stakes areas like fraud detection, be **explainable** and **auditable**. The **European Commission's AI Act** (proposed in 2021) introduces risk classifications for AI systems, with fraud detection likely categorized under "high-risk." Under such classifications, institutions must provide **transparent documentation**, **impact assessments**, and **human oversight mechanisms** (European Commission, 2021).

### 8.4 Anti-Money Laundering (AML) and KYC Compliance

AI is often integrated into **AML** and **Know Your Customer (KYC)** processes to detect unusual transaction patterns. Financial institutions must ensure that AI-powered AML systems align with the recommendations of global standards bodies such as the **Financial Action Task Force (FATF)**. Non-compliance may lead to hefty penalties, reputational damage, and cross-border legal complications (FATF, 2021).

### 8.5 Risk of Discrimination and Bias

Many regulations now emphasize **algorithmic fairness** and **non-discrimination** in automated systems. Financial institutions using AI for fraud detection must monitor for **unintended bias** against protected groups and implement governance frameworks to address fairness, accountability, and ethical concerns (Barocas et al., 2019).

## 9. Future Trends and Innovations

As financial fraud grows in sophistication, the future of fraud detection lies in smarter, more adaptive, and ethically governed AI technologies. Banks are increasingly investing in advanced AI tools that not only detect fraud but also anticipate it. Emerging innovations aim to enhance **accuracy**, **interpretability**, and **security** while ensuring **compliance** and **customer trust**.

### 9.1 Explainable AI (XAI)

One of the most anticipated trends is the development of **Explainable AI (XAI)**. Unlike traditional black-box models, XAI provides transparent and interpretable insights into AI decision-making. This is crucial for building trust with regulators and customers, especially in fraud detection, where automated decisions can have serious consequences. XAI is also being encouraged by regulatory frameworks such as the EU AI Act (Doshi-Velez & Kim, 2017; European Commission, 2021).

### 9.2 AI-Powered Behavioral Biometrics

The use of **behavioral biometrics** such as typing patterns, touch pressure, and navigation behavior is gaining traction. AI models analyze these subtle indicators to create unique user profiles, making it harder for fraudsters to mimic legitimate users. This technology is increasingly being deployed for continuous authentication across mobile and online banking platforms (Conti et al., 2021).

### 9.3 Integration with Blockchain for Fraud Prevention

The integration of **blockchain technology** with AI is being explored to enhance data integrity and transparency in financial transactions. Blockchain offers immutable records, while AI detects anomalies in those records, creating a powerful fraud prevention ecosystem. Smart contracts can also automate fraud checks and settlements (Casino et al., 2019).

### 9.4 Federated Learning and Privacy-Preserving AI

**Federated learning** allows AI models to be trained across decentralized data sources (e.g., multiple banks) without sharing raw data. This helps preserve privacy while benefiting from collaborative learning. It holds promise in enhancing fraud detection across institutions while complying with data protection regulations (Yang et al., 2019).

### 9.5 AI-Augmented Human Decision-Making

Rather than replacing humans, future fraud detection systems will increasingly adopt **AI-augmented approaches**, where AI flags potential fraud and human analysts make the final decision. This hybrid model ensures a balance between efficiency and judgment, especially in complex or high-stakes scenarios (Riggins & Wamba, 2015).

### 9.6 Continuous Learning and Adaptive Systems

Next-generation fraud detection systems will employ **continuous learning models** capable of updating themselves in real time based on new fraud tactics. These self-evolving systems will minimize the need for manual retraining and reduce model drift, making fraud detection systems more agile and proactive (Sarker, 2021).

## 10. Conclusion

The integration of Artificial Intelligence in fraud detection has revolutionized the banking sector's approach to financial security. By leveraging advanced techniques such as machine learning, deep learning, natural language processing, and behavioral analytics, banks can detect and prevent fraudulent activities with unprecedented speed, accuracy, and efficiency. AI not only enhances real-time monitoring and reduces false positives but also allows institutions to shift from reactive to proactive fraud prevention. Despite its transformative benefits, AI-based fraud detection is not without challenges. Issues related to data privacy, algorithmic bias, explainability, and regulatory compliance must be addressed to ensure responsible and ethical implementation. Moreover, the constant evolution of fraud tactics requires AI systems to be adaptive, scalable, and continuously updated. Looking ahead, innovations such as explainable AI, federated learning, blockchain integration, and AI-human hybrid systems are set to redefine the future of fraud prevention. With proper governance, investment, and strategic deployment, AI holds the potential to create a more secure, transparent, and resilient financial ecosystem.

## References

[1] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.

[2] Association of Certified Fraud Examiners (ACFE). (2022). Report to the Nations: Global Study on Occupational Fraud and Abuse.

[3] Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and Machine Learning. fairmlbook.org.

[4] Bhatla, T. P., Prabhu, V., & Dua, A. (2003). Understanding credit card frauds. Cards Business Review.

[5] Rodríguez González, V., Payá, Santos., C, A., y Peña Herrera. B. (2023). Estudio criminológico del ciberdelincuente y sus víctimas. Cuadernos de RES PUBLICA en Derecho y criminología, (1) 95-107. https://doi.org/10.46661/respublica.8072.

[6] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602-613.

[7] Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235-255.

[8] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Status, classification, and open issues. Telematics and Informatics, 36, 55–81.

[9] Chen, Y., Li, Y., & Xie, H. (2020). Detecting phishing websites using natural language processing and machine learning. Security and Communication Networks, 2020.

[10] Conti, M., Dragoni, N., & Lesyk, V. (2021). A survey of behavioral biometric systems for real-time fraud detection. ACM Computing Surveys (CSUR), 54(4), 1–36.

[11] Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waterschoot, S., & Bontempi, G. (2015). Learned lessons in credit card fraud detection from a practitioner perspective. Expert Systems with Applications, 41(10), 4915–4928.

[12] Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608.
[13] European Commission. (2021). Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act). https://eur-lex.europa.eu
[14] FATF. (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. https://www.fatf-gafi.org
[15] Feedzai. (2021). Customer Success Stories and Case Studies. https://feedzai.com
[16] Ghosh, S., & Reilly, D. L. (1994). Credit card fraud detection with a neural-network. Proceedings of the Twenty-Seventh Annual Hawaii International Conference on System Sciences, 3, 621–630.
[17] HDFC Bank. (2022). Sustainability and Business Responsibility Report. https://www.hdfcbank.com
[18] HSBC. (2021). Annual Report and Accounts. https://www.hsbc.com
[19] JPMorgan Chase. (2020). AI at JPMorgan: COiN and beyond. https://www.jpmorgan.com
[20] Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234-245.
[21] Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. Expert Systems with Applications, 32(4), 995-1003.
[22] Kumar, K., & Ravi, V. (2016). A survey of the applications of text mining in financial domain. Knowledge-Based Systems, 114, 128–147.
[23] Liu, Y., Wang, Y., & Zheng, X. (2020). A novel ensemble learning framework for financial fraud detection. Computers & Security, 92, 101745.
[24] Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559-569.
[25] Patil, V. V., & Patil, D. D. (2020). Application of AI in financial fraud detection: Challenges and prospects. International Journal of Engineering Research & Technology (IJERT), 9(07), 260–263.
[26] PayPal Engineering Blog. (2021). Scaling AI to fight fraud. https://medium.com/paypal-tech
[27] Phua, C., Lee, V., Smith, K., & Gayler, R. (2005). A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119.
[28] Reserve Bank of India (RBI). (2022). Master Directions on Digital Payment Security Controls. https://rbi.org.in
[29] Riggins, F. J., & Wamba, S. F. (2015). Research directions on the adoption, usage, and impact of the Internet of Things through the use of Big Data Analytics. Proceedings of the 48th Hawaii International Conference on System Sciences.
[30] Sahin, Y., & Duman, E. (2013). Detecting credit card fraud by decision trees and support vector machines. Proceedings of the International Multi Conference of Engineers and Computer Scientists.

[31] Sahu, T. K., & Gupta, A. (2021). A survey of fraud detection techniques in e-payment systems. Journal of Financial Crime, 28(4), 1041–1060.

[32] Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN Computer Science, 2(3), 160.

[33] Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.

[34] West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47-66.

[35] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19.

[36] Zarsky, T. Z. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision-making. Science, Technology, & Human Values, 41(1), 118–132.