**Journal of Information Systems Engineering and Management**
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Smart Fraud Detection and Prevention: Leveraging Generative AI for Enhanced Payment Security

Ashish Kumar
Independent Researcher, USA

**ARTICLE INFO**

Received: 12 July 2025

Revised: 22 Aug 2025

Accepted: 05 Sept 2025

**ABSTRACT**

The extended digitalization of financial transactions has posed exceptional problems to fraud detection and prevention systems, prompting the development from conventional rule-based structures to superior artificial intelligence systems. Smart fraud detection structures based on generative AI are a revolutionary step towards countering swiftly evolving and complicated fraud schemes that take advantage of weaknesses in virtual fee structures. These cognizant systems showcase better overall performance in managing high transaction volumes, detecting latent styles, and dynamically adjusting themselves to new danger vectors without the need for human intervention or significant reconfigurations. The combination of generative AI with standard machine learning techniques allows for more advanced anomaly detection, contextualization, and real-time response against threats, which excel far beyond traditional methods of detection. Modern implementations exhibit significant gains in detection accuracy, accompanied by the lowering of false positive rates, thus improving operational effectiveness and customer satisfaction. The hybrid human-AI collaboration mode takes advantage of computational capabilities and pattern recognition of artificial intelligence while maintaining critical human expertise for context-based decision-making and strategic control. Environmental, economic, and social implications are not limited to direct fraud avoidance but cover wider financial ecosystem stability, energy efficiency from optimized computational power, and a greater level of financial inclusion for vulnerable groups through secure digital payment access.

**Keywords:** Fraud Detection, Generative Artificial Intelligence, Payment Security, Machine Learning, Digital Payments

## 1. Introduction

### 1.1 Contextual Background

The worldwide finance region has experienced exceptional upheaval through the explosive upward push of electronic bills, cell banking, and online commerce platforms. The digitization procedure has notably transformed the purchasing and commercial enterprise charge habits, kick-starting significant economic growth and deepening economic inclusion possibilities. Present-day payment systems cope with billions of transactions each day via interconnected networks, making for clean commerce even as the supply sets delectable goals for superior cybercriminals.

Payment fraud improvement has reflected the technological boom directly, as cyber criminals use artificial intelligence, system mastering, and complex analytics to create more complicated assault strategies. Contemporary fraud tactics include synthetic identity establishment, advanced account takeover schemes, and payment manipulation methods implemented in real time, which test conventional security paradigms. The interconnectedness of global financial networks enhances successful attack effects, producing cascading effects that cut across institutional and geographical lines.

In addition to short-term monetary losses, deceptive practices erode consumer trust in electronic payment networks persistently, with widespread ripple effects across financial ecosystems. Reputation loss from successful fraud campaigns has a tremendous effect on client retention rates, marketplace capitalizations, and regulatory compliance ratings. These vast-ranging effects are fraud detection and prevention at the middle concerns for economic institutions, fee processors, and generation organizations working within electronic price structures.

### 1.2 Problem Statement

Traditional fraud detection methods have hitherto relied on static rule-based systems and simple machine learning models that show clear limitations in dealing with emerging fraud challenges [1]. Traditional methods show essential operational shortcomings that severely limit effectiveness within emerging threat environments.

Rule-based systems deliver explicit decision logic but are short on the necessary adaptability to combat new fraud methodologies and evolving patterns of attack. These systems function through pre-established conditions and thresholds that quickly fall out of date as fraudsters evolve advanced methods. Fixed system attributes lead to response capabilities in arrears, allowing sophisticated fraud schemes to run undetected over extended periods.

Simple machine learning deployments, though more accommodating than rule-based counterparts, often exhibit high false positive rates and shallow contextual awareness. The models consistently mark authentic transactions as suspicious, creating operational inefficiencies and customer frustration. They also fail to understand intricate behavioral patterns and multi-dimensional relationships among transactions inherent in sophisticated fraud attacks.

The time lag in evolving fraud velocities and adapting detection systems creates ongoing vulnerabilities that fraudsters methodically exploit. Legacy systems involve human-initiated updates, lengthy retraining cycles, and massive computational energy for danger variation, whereas fraudsters quickly trade the brand new attack vectors and evolve available schemes in real-time.

### 1.3 Purpose & Scope

This extensive survey discusses Smart Fraud Detection and Prevention system design and deployment based on Generative AI technologies to overcome the limitations of traditional techniques. The study discusses the capabilities of advanced AI systems in learning dynamically from past fraud data, adaptive threats in real-time, and intelligent alert generation with automated transaction control processes.

The scope covers in-depth human-AI interaction model examination in fraud detection scenarios, investigating artificial intelligence supplementation of human skills in the face of more complex threats. Positive and negative aspects of AI assistance in fraud avoidance are assessed, such as technical, operational, and ethical factors that determine system deployment performance [2].

### 1.4 Pertinent Statistics

Current industry studies yield strong proof for the need for an advanced fraud detection system and its value. Global payment card fraud losses neared billions in recent years, showcasing rising threat environments in worldwide markets [1]. Sophisticated AI-based detection systems exhibit vast performance gains over legacy methods, mitigating major conventional detection weaknesses while sustaining operational efficiency levels [2].

## 2. Current Human-AI Interaction Models

### 2.1 Hybrid Decision-Making Frameworks

Modern systems for detecting fraud make extensive use of hybrid models that bridge artificial intelligence techniques with human analytical capabilities. The models acknowledge that AI systems are best suited to process large volumes of transactions and detect statistical outliers, while human analysts bring the added value of contextual insight, instinctive pattern detection, and strategic reasoning abilities that augment automated systems.

In standard deployments, AI engines are the initial filtering mechanism, scanning transaction streams in real-time with machine learning and statistical models. Such engines alert potentially suspicious transactions based on trained patterns, risk ratings, and established thresholds. The alerted transactions are then escalated to human analysts to confirm alerts, analyze contextual conditions, and issue final approval or rejection decisions.

The segregation of duties accommodates the contrasting strengths of human and artificial intelligence. AI systems offer velocity, reliability, and the capacity to process intricate multi-dimensional patterns of data impossible to examine manually by human beings. Human analysts add domain knowledge, emotional intelligence, and wider contextual analysis skills that might not be included in transaction data [3].

### 2.2 Workflow Integration and Alert Management

Current fraud detection pipelines combine AI-crafted alerts with human exam processes using advanced case management platforms. Such systems provide analysts with detailed transaction profiles, risk ratings, and supporting material crafted by AI algorithms. Typically, systems rank alerts according to risk score, monetary potential, and available analyst, maximizing resource utilization and response times.

Sophisticated integration patterns include feedback mechanisms under which human decisions can teach and refine AI model performance with the passage of time. As analysts accept or reject identified risky transactions, such feedback is integrated into the training data for models to facilitate ongoing learning and adjustment. Repeated improvement enhances the suppression of false positives and the precision of risk assessment by machines.

The success of hybrid models relies heavily on human-AI interface design quality and transparency of AI-produced explanations. Models that supply interpretable justification for generating alerts and understandable actionable insights allow analysts to make better decisions and gain trust in recommendations made by AI.

### 2.3 Challenge in Existing Interaction Models

In spite of benefits, existing human-AI collaboration models are confronted with some key challenges that constrain effectiveness and scalability. Explainability is still a main concern, as sophisticated machine learning models tend to be "black boxes" that return risk scores without transparent explanations for decisions [4]. Transparency deficiencies can destroy analyst confidence and make it difficult to meet regulatory compliance obligations.

Workload management is another major challenge as the number of AI-generated alerts becomes so great that it exhausts human analysts, causing them to experience alert fatigue and suboptimal decision-making. Analysts, when confronted with high numbers of false positives, will develop decreased rigor in reviews or approval biases to cope with workload stress.

The difference in speed between AI processing and human checking creates bottlenecks that affect customer experience, especially for real-time payment cases where instantaneous decisions need to be made. Reconciling detailed human checking with customers' desire for quick transaction processing entails advanced queue management and decision prioritization practices.

| Framework Component | AI Capabilities and Functions | Human Capabilities and Functions |
|---|---|---|
| Primary Screening | Real-time transaction analysis using machine learning algorithms; pattern recognition across multi-dimensional data; automated flag generation based on risk scores and thresholds | Contextual understanding and intuitive pattern recognition; strategic decision-making; domain expertise application |
| Alert Processing | Comprehensive transaction profiling; risk assessment generation; alert prioritization based on financial impact and availability | Transaction validation; contextual factor investigation; final approval/rejection decisions; emotional intelligence application |
| Continuous Learning | Feedback incorporation into model training data; automated performance improvement; pattern adaptation without manual reconfiguration | Decision feedback provision; model performance evaluation; trust building through interface interaction |
| Workflow Integration | Case management system operation; evidence compilation; transparent reasoning provision for alerts | Clear actionable insight interpretation; informed decision-making; AI recommendation validation |
| System Limitations | Black box decision-making creates explainability issues, potential for overwhelming alert volumes, and processing speed advantages | Alert fatigue from high false positive volumes, decision quality degradation under workload pressure, and bottleneck creation in real-time scenarios |

Table 1: Human-AI Collaboration Framework in Contemporary Fraud Detection Systems [3, 4]

## 3. Advantages and Disadvantages of AI Collaboration

### 3.1 Improved Detection Accuracy and Flexibility

AI collaboration in fraud detection provides substantial gains in accuracy of detection through sophisticated pattern recognition features and ongoing learning mechanisms. Contemporary machine learning algorithms are able to discern intricate relationships and subtle patterns within transaction data that are impossible for rule-based systems or human analysts to identify by hand. These systems are particularly good at detecting multi-dimensional patterns involving spans of multiple transaction attributes, temporal relationships, and behavioral signals across large datasets.

AI systems' ability to adapt is a core benefit over other methods. Generative AI models are able to learn from fresh fraud scenarios and update their detection mechanisms in real-time without needing to have rules changed manually or undergo major system reconfiguration. This real-time learning ability allows for systems to remain one step ahead of changing fraud patterns and retain their potency against new attack vectors. Unsupervised and supervised learning methods exhibit special prowess in integrating various analytical methods to boost overall detection performance [5].

AI systems also exhibit better performance in detecting new fraud patterns and zero-day attacks not yet faced. With the help of unsupervised learning methods and anomaly detection methods, these systems are able to identify unusual transaction patterns that can signal new fraud tactics, facilitating proactive response and prevention.

### 3.2 Operational Efficiency and Cost Saving

The use of AI-based fraud detection systems provides significant operational efficiency gains and cost savings in various areas. Automated initial analysis and alert generation reduce the manual workload needed for transaction screening by orders of magnitude, enabling human analysts to work on high-value, sophisticated cases demanding human analysis and expertise.

Reduction of false positives is a significant advantage with direct implications for both operational cost and customer satisfaction. Legacy systems tend to produce significant false positive volumes, which have to be manually checked, and which use up analyst time and could suspend rightful machine-to-machine transactions. AI-based systems with sophisticated pattern recognition can also drive down false positive rates while keeping or enhancing genuine fraud detection rates. Deep learning methods have been shown to excel especially at hierarchical feature learning, providing more effective pattern recognition and fewer false positives [6].

The performance and scalability of AI systems allow for real-time detection of fraud within enormous volumes of transactions, which are impossible for human agents. That is a valuable potential in excessive-speed buying and selling environments, cell charge systems, and online trade websites, wherein brief decision-making is necessary to ensure the purchaser experience and competitive edge.

### 3.3 Challenges of Data Privacy and Regulatory Compliance

AI-based fraud detection structures have a chief problem in terms of ensuring information privacy protection and regulatory compliance duties. The systems need access to large amounts of personal and financial information to work properly and thereby pose issues regarding data security, protection of privacy, and abuse of sensitive data.

Regulatory regimes place severe demands on data collection, processing, and storage activities. Compliance with such regimes while ensuring the effectiveness of the system necessitates utmost care regarding data minimization tenets, purpose limitation, and user consent management. The international nature of numerous payment systems increases complexity, resulting from differences in regulatory requirements across countries.

### 3.4 Model Bias and Fairness Considerations

AI-based fraud detection systems can embed and even exaggerate existing biases in historical data and produce discriminatory results that disproportionately affect certain demographic categories or customer bases. The quality and representativeness of training data have important effects on model fairness and performance.

| Implementation Aspect | Benefits and Advantages | Challenges and Limitations |
|---|---|---|
| Detection Accuracy | Advanced pattern recognition across multi-dimensional data; real-time adaptation to new fraud schemes without manual updates; superior identification of emerging fraud patterns and zero-day attacks through unsupervised learning | Model complexity creates "black box" scenarios; potential for algorithmic bias affecting detection accuracy across demographic groups |
| Operational Efficiency | Automated preliminary analysis reducing manual workload; significant false positive | Resource-intensive implementation requirements; |

| | | |
|---|---|---|
| | reduction while maintaining detection rates; real-time processing capabilities for high-volume transactions | dependency on extensive computational infrastructure for optimal performance |
| Regulatory Compliance | Standardized processing approaches enabling consistent compliance protocols; automated documentation and audit trail generation | Strict data privacy protection requirements; complex multi-jurisdictional regulatory frameworks; extensive personal and financial data access needs |
| Data Management | Enhanced scalability for processing large transaction volumes; continuous learning from feedback mechanisms improves system performance | Data quality and representativeness concerns affecting model fairness; potential perpetuation of historical biases present in training datasets |

Table 2: Comparative Assessment of AI Implementation Advantages and Challenges in Fraud Prevention [5, 6]

## 4. Implementation Tools and Platforms

### 4.1 Real-Time Data Processing Infrastructure

The main point of successful AI-powered fraud detection systems is the strong real-time data processing infrastructure that can handle high volumes of transaction streams with low latency. Modern deployments need highly advanced streaming architectures to ensure optimal response time under heavy transaction volumes. Apache Kafka has become a vital piece of real-time data streaming technology that offers distributed and fault-tolerant message queuing functionality to provide efficient data transmission between transaction sources and fraud detection systems.

Apache Spark is complemented by Kafka to offer distributed computing functions for real-time data analysis and processing. Spark's streaming functionality also enables complex event processing, feature engineering, and model inference at scale that can handle workloads for sophisticated AI fraud detection models. The combination of Kafka and Spark can be a force to be reckoned with when examining a high volume of transactions and quickly moving through the end-to-end fraud risk assessment cycle.

Stream processing architectures have to be designed to handle variations in transaction volumes, seasonal peaks, and peak loading situations, while still effectively detecting fraud and maintaining system availability. Peak transaction rates for periods of high activity can be far in excess of typical processing demands, necessitating elastic scaling features and advanced resource management to maintain consistent performance under different operating scenarios.

### 4.2 Machine Learning and Model Development Frameworks

TensorFlow and PyTorch are the major frameworks used to develop and deploy machine learning models in fraud detection systems. TensorFlow's production-hardened ecosystem, consisting of TensorFlow Serving and TensorFlow Extended, offers end-to-end model life cycle management capability with support for deployment of models that perform large inference workloads with strict latency. Production deployments mainly use distributed training across multiple processing units for sophisticated fraud detection models.

PyTorch's dynamic computation graph and its easy-to-use development environment make it especially well-suited to research and experimenting with new fraud detection methods. The PyTorch environment facilitates both experimental development and production deployment needs, with model training cycles supporting datasets with detailed transaction histories.

Model development frameworks should accommodate a variety of algorithmic strategies, such as supervised learning for recognized fraud patterns, unsupervised learning for anomaly detection, and reinforcement learning for adaptive decision-making. Sophisticated ensemble strategies incorporating multiple algorithms show better performance, with scalable tree boosting systems yielding major improvements in predictive accuracy and computational efficiency [7].

### 4.3 Cloud-Based AI Platforms and Services

Cloud platforms offer scalable, managed services that minimize the infrastructure and complexity needs of deploying AI-based fraud detection systems. Cloud-based deployments reduce infrastructure setup time by orders of magnitude while offering automatic scaling features that accommodate transaction volume changes without human intervention. Platforms allow concurrent processing of many fraud detection models, which facilitates fast completion of risk assessment for individual transactions.

### 4.4 Emerging Generative AI Technologies

Generative AI models are a leap forward in fraud detection feature sets, with increased anomaly detection and explainability, which resolve many of the shortcomings of classical methods. Large language models can scan transaction descriptions, communication patterns, and contextual data to detect suspicious behavior that cannot be determined through numerical analysis. State-of-the-art multimodal features allow these systems to handle heterogeneous data types and offer holistic risk assessment with enhanced accuracy and reliability [8].

| Technology Category | Primary Tools and Platforms | Key Capabilities and Features |
|---|---|---|
| Real-Time Data Processing Infrastructure | Apache Kafka for distributed message queuing; Apache Spark for distributed computing and streaming analytics | Fault-tolerant data streaming capabilities; complex event processing and feature engineering; elastic scaling for varying transaction volumes during peak periods |
| Machine Learning Development Frameworks | TensorFlow with a production-ready ecosystem, including TensorFlow Serving and Extended, PyTorch with dynamic computation graphs and an intuitive development experience | Comprehensive model lifecycle management; distributed training across multiple processing units; support for supervised, unsupervised, and reinforcement learning approaches |
| Advanced AI and Cloud Integration | Cloud-based managed services with automatic scaling capabilities; Generative AI models, including large language models for enhanced detection | Rapid infrastructure deployment with reduced complexity; multimodal data processing for transaction descriptions and communication patterns; enhanced explainability features |

Table 3: Essential Tools and Platforms for Smart Fraud Detection System Development [7, 8]

## 5. Broader Implications

### 5.1 Environmental, Economic, and Social Effects

The deployment of AI-based anti-fraud systems creates substantial positive environmental effects through maximized computational resource use and minimized operational waste. Environmental impact assessments for such systems show substantial paper use reductions relative to conventional manual investigation procedures, with avoidance of travel requirements that previously emitted carbon worldwide in the financial sector. Conventional fraud investigation processes usually involve intensive manual research, physical documentation, and travel for verification, producing major environmental damages.

Sophisticated AI platforms optimize computational resources by means of smart workload allocation, scalable dynamic growth, and smart algorithm design that reduces unnecessary processing as opposed to static solutions. Contemporary cloud-based solutions harness renewable sources of energy and sophisticated cooling technologies, further reducing the environmental impact of fraud detection processes. Centralization of fraud detection functionality in efficient systems results in less total energy consumption than for distributed, but less efficient, legacy methods. Machine learning environments exhibit special effectiveness in resource allocation optimization and computational overhead minimization through smart model deployment and automatic scaling features [9].

Economic impacts reach far beyond the prevention of direct fraud loss to include wider financial system stability and expansion. Economic modeling illustrates how successful fraud detection mechanisms minimize systemic risk, decrease insurance prices, and enhance consumer confidence indicators within electronic payment systems. Such effects trickle down across the economy to facilitate higher transaction volumes, decreased security overhead expenditures, and higher rates of financial inclusion via secure digital payments in emerging markets.

The social impact of high-tech fraud detection is most important for vulnerable groups and emerging markets, where digital payments can unlock access to financial services and economic opportunity. Evidence suggests that reliable and efficient fraud detection systems lower barriers to digital financial inclusion and allow more people to engage in a digital economy. While that sounds like a good thing, it's also important to be cognizant of discriminatory barriers AI systems can create that disproportionately impact certain groups.

### 5.2 Long-term Perspective and Industry Disruption

The path of fraud detection technology is toward more advanced, dynamic systems that fuse several AI technologies with human knowledge to build robust defense systems against the dynamic threat. Next-generation systems will most probably incorporate real-time threat intelligence, behavioral biometrics, and sophisticated contextual analysis to deliver end-to-end fraud prevention with capabilities to automatically respond to new attack types. Sophisticated fraud detection systems exhibit outstanding efficiency in handling intricate patterns of transactions and detecting advanced attack strategies imperceptible to conventional systems [10].

Regulatory regimes are transitioning to meet the challenges and opportunities posed by AI-based fraud detection systems. New regulations center around algorithmic explainability, fairness criteria, and responsibility regimes ensuring responsible deployment while maintaining system efficacy.

### 5.3 Call to Action

Organizations in the digital payments value chain need to begin deploying AI-based adaptive fraud detection platforms that take advantage of automation mechanisms combined with human intelligence and oversight. The effective integration of intelligent fraud detection and prevention solutions requires heightened attention to platform architecture, data governance, and operational paradigms in order not to erode customer trust or run afoul of their legal obligations.

| Implication Category | Positive Impacts and Benefits | Implementation Considerations |
|---|---|---|
| Environmental Effects | Substantial reductions in paper consumption; elimination of travel requirements, reducing carbon emissions; optimized computational resource utilization through intelligent workload distribution and dynamic scaling | Need for renewable energy integration in cloud implementations; requirement for efficient algorithm design to minimize unnecessary processing |
| Economic Effects | Reduced systemic risk and lower insurance costs; improved consumer confidence in digital payment systems; increased transaction volumes and enhanced financial inclusion rates in developing markets | Careful attention to cost-benefit analysis; consideration of infrastructure investment requirements for optimal return on investment |
| Social Effects | Reduced barriers to digital financial inclusion for vulnerable populations; broader participation opportunities in digital economies; enhanced access to financial services in developing markets | Prevention of discriminatory barriers; ensuring AI systems do not unfairly impact specific demographic groups through bias mitigation |
| Industry Transformation | Integration of real-time threat intelligence and behavioral biometrics; sophisticated adaptive systems combining multiple AI technologies with human expertise | Proactive adoption requiring balanced automation with human oversight; attention to system design, data governance, and regulatory compliance requirements |

Table 4: Multi-Dimensional Impact Assessment of Smart Fraud Prevention Technologies [9, 10]

## Conclusion

Intelligent fraud detection and prevention based on generative artificial intelligence is a game-changer to offer protection to digital payment ecosystems against complex and dynamic threat vectors. Bringing together the advanced machine learning capabilities of generative AI technologies to provide unique types of adaptability, granularity, and contextual sensitivity that cannot match rule-bound systems. These smart systems exhibit a strong ability to learn dynamically from historical patterns of fraud in real-time while, at the same time, learning in real-time from new threat patterns as they emerge, thus constituting an anticipatory defense capability that remains ahead of fraudster creativity. Ultimately, effective artificial intelligence and human intelligence collaboration creates a powerful combination of computing, domain expertise, strategic foresight, and contextual reasoning. Future innovation will increasingly focus on stronger explainability, smarter bias detection, and cultivated and enhanced automated systems with human components or decision-making developed and deployed transparently and reliably using AI. Intelligent fraud prevention impacts well beyond direct financial harm to include economic conditions, environmentally sensitive resource optimization, and advancing social justice agendas around equitable service delivery in finance. Organizations that can harness these technologies will produce more secure, efficient, and accessible financial services, while achieving a competitive advantage in a bloody marketplace that evolves so quickly. As there is a transition to transparent and explainable AI systems capable of providing clear explanations of how decisions are reached, it will be vital to secure stakeholder trust and regulatory compliance in a rapidly changing digital economy.

## References

[1] Globe Newswire, "Payment Card Fraud Losses Approach $34 Billion," Fintech Futures, 2025. [Online]. Available: https://www.fintechfutures.com/press-releases/payment-card-fraud-losses-approach-34-billion

[2] Jarrod West and Maumita Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," Computer and Security, 2016. [Online]. Available: https://chengzhaoxi.xyz/download/pdf/paper/fintech/Intelligent-financial-fraud-detection_A-comprehensive-review.pdf

[3] Salvatore J. Stolfo, et al., "Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results," ResearchGate, 1998. [Online]. Available: https://www.researchgate.net/publication/2282588_Credit_Card_Fraud_Detection_Using_Meta-Learning_Issues_and_Initial_Results

[4] Shiguo Wang, "A Comprehensive Survey of Data Mining-Based Accounting-Fraud Detection Research," IEEE Xplore, 2010. [Online]. Available: https://ieeexplore.ieee.org/document/5522816

[5] Fabrizio Carcillo, et al., "Combining unsupervised and supervised learning in credit card fraud detection," Information Sciences, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0020025519304451

[6] Yann LeCun, et al., "Deep Learning," Nature, 2015. [Online]. Available: https://www.nature.com/articles/nature14539

[7] Tianqi Chen and Carlos Guestrin, "XGBoost: A Scalable Tree Boosting System," ACM Digital Library, 2016. [Online]. Available: https://dl.acm.org/doi/10.1145/2939672.2939785

[8] OpenAI, "GPT-4 Technical Report," arXiv, 2023. [Online]. Available: https://cdn.openai.com/papers/gpt-4.pdf

[9] Anjali, et al., "Transaction Fraud Detection using Amazon Fraud Detector and AWS Cloud Services," International Journal of Computer Applications, 2025. [Online]. Available: https://www.ijcaonline.org/archives/volume187/number11/transaction-fraud-detection-using-amazon-fraud-detector-and-aws-cloud-services/

[10]Server Consultancy, "AI in Fraud Detection: Protecting UK Accounting Firms and Their Clients," 2024. [Online]. Available: https://www.serverconsultancy.co.uk/ai-in-fraud-detection/