SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V12I14P103

Volume 12 Issue 4, 17-22, April 2025

Review Article

Intelligent AI Agents for Fraud and Abuse Detection: Leveraging Machine Learning, NLP, and Behavioural Analytics for Enhanced Security

Anirban Majumder

Applied Scientist, Amazon, Seattle, WA, USA.

Corresponding Author : anirbanmj16@gmail.com

Received: 16 February 2025 Revised: 23 March 2025 Accepted: 14 April 2025 Published: 29 April 2025

Abstract *- Fraud and abuse in financial transactions, healthcare claims, and digital interactions pose significant challenges to organizations worldwide. The conventional rule-based detection approaches are often limited in adapting to evolving fraudulent tactics. This paper explores the development of intelligent AI agents for fraud and abuse detection, leveraging Machine Learning (ML), Natural Language Processing (NLP), and Behavioural Analytics to enhance security and risk mitigation. To generate models, the AI solution incorporates supervised and unsupervised Machine learning models for finding deviations through anomaly detection, NLP approaches for text-based fraud identification and behavioural analytics to permit recognition of deviations in user activity. Leveraging these state-of-the-art approaches helps the system to enable real-time detection and prevention of fraudulent activities, enhancing accuracy and reducing false positives.*

This approach has effectively identified sophisticated instances of fraud across various industries , including financial services, healthcare, and e-commerce. Furthermore, AI-driven fraud detection significantly improves operational efficiency, lowers losses, and enhances cybersecurity protections.

Keywords *- Fraud detection, Artificial intelligence, Machine learning, Natural language processing, Behavioural analytics, Cybersecurity.*

1. Introduction

Fraud and abuse in digital transactions have become increasingly sophisticated, posing significant challenges to finance, healthcare, and e-commerce industries. Traditional rule-based fraud detection systems that store patterns with which to identify fraud will soon be unable to handle the fast-evolving techniques of criminals. However, now that more than ever before, lawbreakers use highly sophisticated methods, the use of AI-driven intelligent solutions can improve security and financial safety to mitigate such risks. Fraud detection frameworks have integrated technologies like Machine Learning (ML), Natural Language Processing (NLP) and Behavioral Analytics for a more dynamic approach to detecting such malicious acts [1].

Machine learning algorithms effectively identify fraud by scanning millions of transaction records, identifying patterns, and reporting. Irregularities in real-time. Deep learning, decision trees, and unsupervised learning are methods that identify if someone is exhibiting abnormal behavior and are models capable of discriminating between normal and abnormal behaviors. Reinforcement learning, on the other hand, allows AI agents to build on past successes and failures. As a result, they can identify new fraudulent patterns emerging in society and avoid adverse reports [2]. Additionally, NLP plays a crucial role in detecting fraud and scams in textual messages. Channels include emails, chat conversations, and customer reviews. Thanks to advanced algorithms, NLP models can detect suspicious messages, phishing attempts, and fraudulent claims by analyzing linguistic patterns, sentiment, and overall intent. Overall, NLP assists fraud detection across the insurance industry.

By observing user interactions and transaction behavior with behavioral analytics, an AI-based system for fraud prevention becomes stronger. Behavioral biometrics like keystroke dynamics, mouse movement patterns and voice recognition serve as a means for AI agents to detect anomalies that might signal that unauthorized access or account takeover attempts are being made. This way an AI-based fraud detection system begins to provide the same level of security as in one-to-one dealings with another person. Combining these methods, AI-based fraud detection systems offer live security and proactive response measures that enhance security, reduce loss, and protect trust in the digital ecosystem [3].

The core research gap is that traditional anti-fraud mechanisms have limited responsiveness and understanding of the entire situation and cannot detect new, complex frauds in a timely manner. With fraudsters increasingly moving to automation, synthetic identities and deepfake technology, there is a pressing need for intelligent, scalable and real-time fraud detection frameworks. In response to this real problem, this paper discusses how we can use Artificial Intelligence (particularly Machine Learning, Natural Language Processing, and Behavioral Analysis) to make fraud detection systems adaptive and dynamic.

NLP provides an important layer, and by analyzing the effect, expressed or implied attitudes as good patterns that can be picked up on, functions to uncover deceptions in written text communications, be it phishing emails" or false claims, for example. At the same time, behavioral analytics strengthen fraud detection by observing the behavioral patterns of individual users, such as keystroke dynamics, device fingerprints and login patterns. It provides a biometric approach to anomaly detection.

When AI capabilities are brought to bear, modern fraud detection systems become contextually aware and self-learning, and they provide real-time defences that overcome the limitations of older approaches while enhancing security in the digital economy.

2. Literature Review

Artificial intelligence (AI) has been progressively used in fraud detection over the past 10 years. This transition will likely continue as standard rule-based systems are proving more and less effective against adaptive and sophisticated fraud, let alone actively looking for it. Anomalies in financial transactions can now be modelled from a semi-supervised perspective using statistical and machine learning algorithms, thanks to Papasavva, A.(2024) pioneering forays into the field. Contemporary researchers explore supervised and unsupervised models, including decision trees, support vector machines, and deep neural networks, in various ways for more precise fraud checking (M. K. H. (2024). These methods can help scalable fraud detection systems learn complex transaction patterns and adapt to new attack vectors.

In particular, intelligent fraud detection has become increasingly dependent on machine learning (ML). To capture the temporal and spatial patterns of transaction data, researchers have used deep learning models such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs) (Olutimehin, A. T. (2025). Despite being only one of the many examples, reinforcement learning has shown promise in continuously improving detection accuracy based on live feedback. As NLP can manage text-based fraud like phishing, fake reviews, and identity theft, it is pivotal to fraud detection. In such fields as insurance and health care, NLP has been picking up anomalies within the documentation of claims and patient records, including structured and unstructured data. Both intelligent AI systems and AI-based behavior models thus provide comprehensive anti-fraud protection that simultaneously accesses a wide array of detection vectors, offering context-sensitive, robust resistance against fraud and exploitation of computer networks.

3. How Machine Learning, NLP & Behavioral Analytics Help AI Agents Detect Fraud and Abuse Across Industries

Fraud and abuse are a perennial challenge across all industries, resulting in financial losses, security risks, and reputational harm. That makes it necessary to develop AI-driven solutions that traditional fraud detection methods often cannot keep up with since the attack methods for fraudsters are constantly evolving. Utilizing Machine Learning (ML), Natural Language Processing (NLP), and Behavioral Analytics, the combination of AI attitude agents, after inquiry big data, notice different preferences and detect fraud in real time [4]. These help businesses boost security, minimize financial risk, and build trust in digital transactions.

Here are the areas in how AI-driven fraud detection works within different industries:

3.1. Financial Services & Banking

Financial fraud detection is necessary for the financial sector to prevent unauthorized payments, identity theft, security breaches, and money laundering activities [5].

3.1.1. Machine Learning

AI models study transaction trends and highlight irregularities like surprising cash withdrawals, rapid transfers of funds, and mirror transactions. Techniques including Random Forests, Neural Networks, and Isolation Forests have provided real-time fraud detection [6].

3.1.2. NLP

Text-based communication can reveal fraudulent intent in emails, loan applications, or customer interactions, so analyzing them is a typical application of NLP [7].

3.1.3. Behavioral Analytics

AI analyzes the login pattern of users on online banks (e.g., How fast a user types, How frequently a user logs in, and which device is used). If it detects a deviation (e.g., it is your first time logging on from Madame's London base), the fraud alerts start alerting [5].

3.2. E-Commerce & Retail

Online retailers face fraud related to fake reviews, payment fraud, and account takeovers.

3.2.1. Machine Learning

AI models detect fraudulent purchases by analyzing user behavior, and comparing it to known fraud patterns. Supervised learning is used to classify risky transactions based on previously known fraud cases [8].

3.2.2. NLP

Analyzes tone, sentiment, and structure of user-generated reviews and complaints to detect fake reviews, promotional abuse, and fraudulent seller activity [7].

3.2.3. Behavioural Analytics

Tracking clicks, time spent on particular pages, and unusual checkout activity identify auto bot orders or reseller abuse [4].

3.3. Healthcare & Insurance

Fraudulent claims and identity theft cost billions each year to the healthcare industry [9].

3.3.1. Machine Learning

Using all structured and unstructured claim data within the Patient records, AI identifies outliers such as duplicate claims, exaggerated injuries and unneeded procedures and tests [9].

3.3.2. NLP

Extract and validate factual data from medical reports, prescriptions and insurance claims, checking for falsified documents or inconsistencies

3.3.3. Behavioral Analytics

Monitoring trends such as patient-doctor interactions, prescription fulfilment, and claim submissions to identify fraudulent activities such as prescription fraud and doctor shopping [9].

3.3.4. Cybersecurity & Identity Verification

Phishing, account takeovers, and identity theft are just a few examples of fraudsters often manipulating weaknesses in cybersecurity systems [10].

3.3.5. Machine Learning

AI models detect unauthorized access attempts based on IP tracking, login frequency, and behavioural anomalies. Models based on deep learning can classify types of attacks and predict threats before an imminent security breach [10].

3.3.6. NLP

Scans emails, messages, and URLs to discover phishing indicators and catch suspicious keywords or links to a malicious website.

3.3.7. Behavioral Analytics

Keeping track of typing patterns, mouse movements, and voice recognition helps identify fraudulent login attempts. So, suppose an attacker is trying to access the system using stolen credentials but doing something the said organization or agent does not generally do. In that case, the system can mark suspicious activity and block access [7].

3.4. Telecommunications

Subscription fraud, fake SIM activation, and spam calls/SMS scams are some fraud issues telecom companies face [11].

3.4.1. Machine Learning

To detect abnormal calling patterns and identify fraud like mass robocalls and SIM swap fraud.

3.4.2. NLP

Spam SMS, robocalls, and scam emails are filtered by analyzing the text within the content and the nature of the scam keywords used.

3.4.3. Behavioral Analytics

Tracks customer calling habits, device switching, and abnormal data usage to identify if an account has been tampered with.

3.5. Government & Public Services

Governments face fraud issues such as tax fraud, benefit fraud, and identity theft [8].

3.5.1. Machine Learning

AI models further analyze tax records, employment history, and benefit claims to identify discrepancies and patterns of fraud. v

3.5.2. NLP

Identify fraudulent claims for social assistance, reports of tax evasion, and misinformation campaigns on the internet.

3.5.3. Behavioral Analytics

Monitors activities conducted on Government portals to flag abnormal access patterns or attempts to alter public records.

4. AI Agents in Fraud and Abuse Detection

AI agents are innovative systems capable of independently finding, analyzing, and reacting to fraud across sectors. Integration of Machine Learning (ML), Natural Language Processing (NLP), and Behavioral Analytics in these agents enables organizations to enhance their fraud detection and prevention capabilities.

Here are some notable applications for Intelligent AI Agents:

4.1. IBM Watson Fraud Detection

Industry: Banking, Financial Services, Insurance (BFSI)

Use of AI agents: It uses AI-powered anomaly detection to spot fraudulent transactions in real time. Applies NLP to analyze emails, chat messages, and documents for fraud indicators. Integrates behavioral analytics to monitor user login and transaction behavior [12].

4.2. Google AI Fraud Detection System

Industry: E-Commerce, Digital Payments

Use of AI agents: Uses ML models to detect abnormal payment patterns on platforms like Google Pay. Employs

NLP to identify phishing attempts and fake reviews. Monitors user behavior (e.g., sudden location changes, multiple failed transactions) to detect fraud [13].

4.3. Darktrace AI Cybersecurity Agent

Industry: Cybersecurity, Identity Protection

Use of AI agents: It uses machine learning to detect advanced cyber threats and insider fraud. Applies behavioral analytics to track user activity and spot unusual login behaviours. It uses NLP for phishing email detection and fraud pattern recognition [14].

4.4. PayPal AI Fraud Detection System

Industry: Online Payments, Digital Wallets

Use of AI agents: It uses deep learning algorithms to detect fraudulent transactions. Applies NLP to analyze customer complaints and transaction descriptions for scam detection. Monitors purchase behavior and IP address usage for fraud prevention [15].

4.5. FICO Falcon Fraud Manager

Industry: Credit Cards, Banking

Use of AI agents: Uses ML-based predictive analytics to detect credit card fraud. Employs real-time behavioural tracking to monitor spending patterns. It uses NLP for transaction text analysis to detect suspicious descriptions [16].

4.6. SAS Fraud Management

Industry: Healthcare, Insurance

Use of AI agents: Uses AI models to detect fraudulent medical claims.
NLP analyzes medical reports, prescriptions, and claim descriptions to spot inconsistencies. Tracks healthcare provider behavior to detect overbilling and identity theft [17].

5. Case Studies

5.1. Case Study 1: Global Bank's AI-Driven Check Fraud Detection, Industry: Banking and Financial Services

One of the most prominent global banks was hit with high stake losses and operational neglect due to check fraud. The bank collaborated with Cognizant to develop an AI and machine learning-based solution to enhance the speed and accuracy of check verification processes.

The AI system was trained on large historical transaction record datasets, allowing it to recognize patterns in the data that suggest fraudulent checks. With this system added to its current infrastructure, the bank could automatically tag and highlight suspicious transactions for further human review.

The company prevented over $20 million loss in fraud by significantly reducing check fraud activity across the service. The bank also saw reduced operational expenditures and less time to validate the checks.

5.2. Case Study 2: Krungthai Card PCL's AI-Enhanced Fraud Management, Industry: Credit Card Services

Credit card issuer Krungthai Card PCL (KTC) is one of Thailand's largest credit card providers and needed a way to prevent fraud on the accounts of its 3.3 million customers without incurring excessive operating costs. To augment its fraud detection, KTC turned to ACI Worldwide's AI-driven payments intelligence solution. Implemented an Intelligent AI agent to analyze transaction data in real-time and was able to identify and flag abnormal transactions with the potential of being classified as fraudulent.

This proactive approach allowed KTC to respond swiftly to threats and reduce false positives. Adopting the AI solution enabled KTC to effectively combat fraud, minimize associated costs, and deliver incremental revenue, enhancing customer trust and satisfaction.

5.3. Case Study 3: Esure's Integration of AI for Fraud Detection, Industry: Insurance

Esure Group is a large insurance company looking to solve the ongoing problem of claim fraud, which costs them money and effort. Ensure engaged DataSentics to help them with their digital transformation by employing cutting-edge machine learning techniques for fraud detection.

The project used a new fraud detection model using digital behaviour data developed on the Databricks platform. This model used advanced streamlining machine learning algorithms to analyze trends to prevent fraudulent claims quickly. Implementing the AI-driven fraud detection model decreased false positive rates and enabled earlier detection of fraudulent activities. It made it more effective and less expensive for Esure to detect fraud.

6. Future Scope

As fraud tactics become increasingly sophisticated, the future of AI-powered fraud detection will depend on higher Perform Machine Learning (ML), Natural Language Processing (NLP), and Behavioral Analytics methods. Innovation will be a key driver in positively impacting the development of fraud prevention systems in different industry sectors, particularly with technologies such as explainable AI (XAI), blockchain, federated learning, deep reinforcement learning, etc.

6.1. Explainable AI (XAI) for Transparency in Fraud Detection

The "black box" nature of machine learning models, and the difficulty this presents to financial institutions and regulators in understanding how AI reaches conclusions is one of the most serious pitfalls with AI-based fraud detection. Explainable AI (XAI): Explainable AI will enhance fraud detection by making AI models more interpretable and trustworthy. It will enable compliance teams to audit fraud decisions more efficiently, decreasing false positives while ensuring fairness in fraud detection systems.

6.2. Federated Learning for Cross-Industry Fraud Prevention

Since traditional fraud detection needs centralized data processing, companies have difficulty sharing fraud intelligence because of data privacy laws (e.g., GDPR, CCPA). By comparison, federated learning can allow AI models to be trained on data across multiple organizations without sharing raw data, enabling collaborative fraud pattern detection by financial institutions, healthcare providers, and e-commerce companies.

6.2.1. Blockchain for Enhanced Security & Fraud Prevention

Blockchain technology and fraud detection using AI, along with big data, can revolutionize fraud detection in the financial sector by creating a decentralized, decentralized, tamper-proof ledger for all transactions. In banking, for example, blockchain could help combat identity fraud by using cryptographic methods to record customer credentials as a unique code where only the code is stored. In supply chain management, AI-based intelligent contracts can identify counterfeit products or payment fraud before transactions.

6.2.2. Real-Time Deep Reinforcement Learning for Adaptive Fraud Detection

Fraud methods are dynamic, which means AI systems need real-time learning and adaptation. The AI agents can learn to change the processing method for differentiating fraud by using Deep Reinforcement Learning (DRL) to feed it real-world data. Traditional rule-based systems are static, but fraud detection can use DRL to automatically tune fraud detection thresholds, forecast emerging fraud types, and minimize lost revenue.

6.2.3. AI-Powered Behavioral Biometrics for Identity Verification:

In future fraud prevention, organizations will depend more on AI-supported behavioural biometrics like keystroke dynamics, voice and gait analysis, etc. Instead of traditional passwords, or OTPs, which are highly hackable, these technologies will replace authentication methods through user behaviour analysis on digital platforms. Behavioural biometrics will be one of the layers in MFA, mainly focused on identity theft, SIM swap fraud, and account takeover.

7. Challenges and Considerations in AI-Driven Fraud and Abuse Detection

7.1. Data Privacy and Compliance Issues

AI-powered fraud detection systems are based on transactions, personal data, and behaviour patterns. On the other hand, regulations such as GDPR, CCPA, and HIPAA have strict guidelines that restrict how data can be collected, shared, and processed. Organizations must follow regulatory frameworks whilst being able to detect fraud, so it is a balancing act. Moreover, issues like user consent, ethical AI practices, and data model bias must also be addressed to achieve fairness in fraud detection.

7.2. Evolving Fraud Tactics and AI Adversarial Attacks

Fraudsters continuously adapt and evolve their strategies, using advanced techniques such as deepfake fraud, synthetic identity fraud, and AI-generated phishing attacks. Such fierce threats remain ineffective using traditional rule-based fraud detection systems. Moreover, adversarial approaches can also be used against AI, with fraudsters creating scenarios that exploit weaknesses in the machine learning models that make up your fraud detection mechanisms by providing misleading information to bypass them. Organizations must fortify their AI security tools to counteract these emerging threats and constantly update their fraud detection models.

7.3. Balancing False Positives and User Experience

A commonly made business case in AI-powered fraud detection is that they can reduce the number of false positives, where everyday transactions or activities are flagged as fraudulent events. Many false positives lead to customer dissatisfaction, transaction hindrances, and damage to reputation. On the one hand, fraud detection systems that are too lenient might let fraudulent behaviour go undetected. They must, therefore, hone their AI algorithms to strike a balance between security and user experience, utilizing aspects such as real-time behavioural analytics, adaptive authentication, and AI explainability to improve fraud detection intelligently while minimizing disruption to genuine users.

8. Conclusion

Fraud and abuse detection powered by AI has emerged as a critical tool for enterprises to combat financial crimes. AI agents have scored higher in identifying theft and cyber fraud more effectively than traditional processes. With the help of Machine Learning (ML), Natural Language Processing (NLP), and Behavioral Analytics, AI agents can examine massive datasets, spot dispersed fraudulent activity in time and provide a higher level of protection. Emerging technologies like explainable AI, federated learning and blockchain will integrate with advancements in fraud prevention, enabling even tighter preventative control and more accurate and privacy-preserving solutions.

However, the road ahead has hurdles, including data privacy concerns, fast-changing fraud techniques, and the balancing act of false positives. If managed well, AI-led fraud detection can remain both practical and ethical. To combat the evolving threat of cybercriminals, organizations need continuous monitoring, regulatory compliance, and adaptive fraud detection. With the development of AI, businesses will need to work toward creating transparent fraud detection systems that are secure and easy for customers to use, making it a safer digital environment for consumers and businesses.

References

[1] Antonis Papasavva et al., "Application of AI-Based Models for Online Fraud Detection and Analysis," *arXiv*, pp. 1-41, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Md Kamrul Hasan Chy, "Proactive Fraud Defense: Machine Learning's Evolving Role in Protecting Against Online Fraud," *World Journal of Advanced Research and Reviews*, vol. 23, no. 3, pp. 1580-1589, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Ruinan Zhang, Fanglan Zheng, Wei Min, "Sequential Behavioral Data Processing using Deep Learning and the Markov Transition Field in Online Fraud Detection," *arXiv*, pp. 1-5, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[4] Chandra Shekhar Pareek, "From Detection to Prevention: The Evolution of Fraud Testing Frameworks in Insurance through AI," *Journal of Artificial Intelligence, Machine Learning & Data Science*, vol. 1, no. 2, pp. 1-8, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Albert Y.S. Lam, "Artificial Intelligence Applications in Financial Technology," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 20, no. 1, pp. 1-5, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] Abdulalem Ali et al., "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Applied Sciences*, vol. 12, no. 19, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Petros Boulieris et al., "Fraud Detection with Natural Language Processing," *Machine Learning*, vol. 113, pp. 5087-5108, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ramiz Salama, Diletta Cacciagrano. and Fadi Al-Turjman, "Connecting AI and Blockchain to Improve Security of Financial Services," *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*, vol. 232, pp. 67-77, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Eman Nabrawi, and Abdullah Alanazi, "Fraud Detection in Healthcare Insurance Claims Using Machine Learning," *Risks*, vol. 11, no. 9, pp. 1-11, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Mayra Macas, Chunming Wu, and Walter Fuertes "A Survey on Deep Learning for Cybersecurity: Progress, Challenges, and Opportunities, Computer Networks, vol. 212, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Alejandro G. Martín et al., "An Approach to Detect User Behaviour Anomalies within Identity Federations," *Computers & Security*, vol. 108, pp. 1-18, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] IBM, IBM Safer Payments – Real-time Payment Fraud Detection. [Online]. Available: https://www.ibm.com/products/safer-payments

[13] Google Cloud, Financial Fraud Detection with AI, 2023. [Online]. Available: https://cloud.google.com/solutions/financial-fraud-detection

[14] Darktrace, Enterprise Immune System – Cyber AI. [Online]. Available: https://www.darktrace.com/en/products/enterprise-immune-system

[15] PayPal, How We Fight Fraud with AI. [Online]. Available: https://newsroom.paypal-corp.com

[16] FICO, Falcon Fraud Manager, 2025. [Online]. Available: https://www.fico.com/en/products/fico-falcon-fraud-manager

[17] SAS, Fraud Detection and Prevention with SAS AI. [Online]. Available: https://www.sas.com/en_us/solutions/fraud-detection.html

[18] Halima Oluwabunmi Bello, Developing Predictive Financial Fraud Models Using AI-Driven Analytics within Cybercrime-Resilient Security Ecosystems, vol. 6, no. 1, pp. 5055-5069, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Oluwatobi Timothy Soyombo et al., "Reviewing the Role of AI in Fraud Detection and Prevention in Financial Services," *International Journal of Science and Research Archive*, vol. 11, no. 1, pp. 2101-2110, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nitin Liladhar Rane, Saurabh P. Choudhary, and Jayesh Rane, "Blockchain and Artificial Intelligence (AI) Integration for Revolutionizing Security and Transparency in Finance," *SSRN*, pp. 1-21, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Abayomi Titilola Olutimehin, "The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cybersecurity for Cryptocurrency Platforms," *SSRN*, pp. 1-23, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[22] Halima Oluwabunmi Bello, "Integrating Behavioral Biometrics and Machine Learning to Combat Evolving Cybercrime Tactics In Financial Systems," *International Journal of Computer Applications Technology and Research*, vol. 14, no. 2, pp. 121-133, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[23] Balagopal Ramdurai, "Large Language Models (LLMs), Retrieval-Augmented Generation (RAG) Systems, and Convolutional Neural Networks (CNNs) in Application Systems," *International Journal of Marketing and Technology*, vol. 15, no. 1, pp. 1-14, 2025. [Google Scholar] [Publisher Link]

[24] Osama Alkadi et al., "A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9463-9472, 2021. [CrossRef] [Google Scholar] [Publisher Link]