JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(2), JUNE, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

The Role of Artificial Intelligence in Cybersecurity for Financial Fraud Detection and Prevention

[1]Gbenga Akinyemi, [2]Muyideen Omuya Momoh, [3]Hayatu Idris Bulama, [4]Mohammed Habib Abdullahi
1University of Hertfordshire, Hertfordshire Business School, United Kingdom
2&4Department of Mechatronic Engineering, Air Force Institute of Technology Kaduna, Nigeria,
3Department of Electrical and Electronics Engineering, Air Force Institute of Technology Kaduna, Nigeria

ABSTRACT
Financial fraud, particularly computer-environment-reliant fraud has been an ongoing global concern. Sources, both anecdotal and research, have consistently inundated the print media with concerning reports of cyber fraud various kinds running into billions of dollars yearly. From the forgoing, it is evident that traditional systems of fraud mitigation are fast losing its grips on the menace fraudulent activities. Traditional fraud mitigation parameters are rule based. They are targeted against meeting certain rule challenge. More so, criminals appear to keep changing their pattern of crimes to fool the system and stay undetected. Rule-based traditional approaches are not effective against the current state of dynamism and persistence in fraudulent financial cybercrimes. AI and machine learning approaches have proven to be more resilient in tackling the today's threat of cybercrimes as they evolve. The reason being that AI is equally an evolving mechanism which collects data from both historic and learning activities, while building a continuous model capable of acting proactively to arrest threats before they occur. Hence, this is poised to demonstrate the importance of AI in fraud mitigation, given the current patterns of crimes marked by sophistication and persistence. This study analyzes how artificial intelligence contributes to strengthening cybersecurity, with a focus on detecting and preventing financial fraud. It reviews different AI techniques—including both supervised and unsupervised machine learning approaches—that examine transaction behaviors and identify anomalies indicative of fraudulent activity. The research underscores AI's capacity for real-time detection and automated response, which enhances the ability of financial institutions to address increasingly complex cyber threats. Incorporating AI into cybersecurity strategies offers a promising avenue for creating more secure financial environments and fostering greater customer confidence in digital banking.

ARTICLE INFO
Article History
Received: November, 2024
Received in revised form: February, 2025
Accepted: May, 2025
Published online: June, 2025

KEYWORDS
Artificial Intelligence, Financial Fraud, Cyber Security, Machine Learning, Piracy

INTRODUCTION

Financial fraud is the illegal act by which a person or company takes advantage of that illegal act that benefits a person, causing the other party a loss. It is an act of dishonesty, an attempted deception that causes damage and is carried out with the intention of obtaining an illicit profit (Hashim *et al*., 2020). That is, an act of deception orchestrated to attract illicit benefit. Financial fraud has grown not only because of the great development that the financial area has taken over the years but also because of the transfer of various physical operations to cyberspace, which has caused vulnerabilities in companies and has allowed criminals to find loopholes (Aslan *et al*., 2023). The financial sector

Corresponding author: Gbenga Akinyemi
✉ oluwagbenga.akinyemi@gmail.com
University of Hertfordshire, Hertfordshire Business School, United Kingdom.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(2), JUNE, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

is now an important target for hackers and fraudsters, both inside and outside the organizations and thus disrupt economic stability and cause damage by losing sensitive data from both companies and clients. Cybercrime is the act by which computers are used to carry out illegal actions (Chinedu *et al*., 2020). Cybercrime can include, among others, banking fraud, cyberespionage, identity theft, online sexual exploitation, sending and distributing malware and even piracy.

Cybercrime can be characterized by the following factors: these are the main perpetrator, the victim; there are usually high losses on a global scale; the cybercriminals are usually professionals in IT; most cybercrime occurs from a distance and is caused by the low risks that the perpetrators perceive, including the fact that they are often not punished (Franjić 2020; Daniel *et al*., 2021). Cybersecurity is how organizations protect themselves against malicious attempts to access systems and sensitive information, and cybersecurity focuses on preventing those unauthorized attacks. Cybersecurity specifically in financial institutions focuses on protecting sensitive data and financial transactions carried out between companies and customers. Cybersecurity has control frameworks that put forth a defensive structure which banks must comply with to preserve their customers' security.

Cybersecurity is a fundamental pillar for the proper functioning of a state; a financial institution must educate its customers and citizens about the importance of being conscious of various forms of cyberthreats, fraudulent and scam patterns employed by criminals. Following this, cybersecurity policies formulation are paramount. The lack of an adequate cybersecurity policy may trigger events that affect the reputation of the bank and trust in it, as well as adversely affect the economy of nations (Nwankwo et al., 2022; Akinyemi 2025).

Categories of Financial Fraud

Financial fraud can be classified into several categories as discussed shown in Figure 1 and also discussed in the subsequent subsection.

Credit Card Fraud

Credit card fraud refers to the theft and improper usage of a person's credit card for financial gain. This may occur both in physical stores where an unauthorized person uses a credit card without the owner's knowledge, and in online stores where an unauthorized person uses a credit card to make online purchases. Merchants who face such frauds are greatly affected because of the chargeback rules of credit card companies, as a result, card companies lose current and future revenue (Dara & Gundemoni 2006).

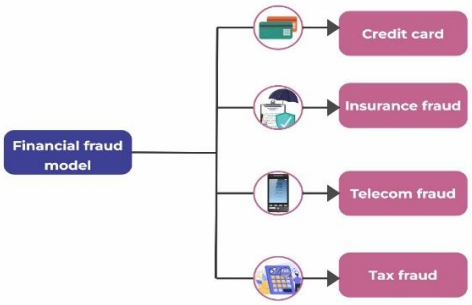

Figure 1: Financial fraud model

Insurance Fraud

Insurance fraud consists of lodgment by a person or organization of false claims or exaggerated claims to insurance companies for compensation that is unduly qualified. There are numerous fraudulent activities that insurance companies face and struggle to deal with. Because of the complicated nature of the insurance industry, investigators, lawyers and businesses also have been affected as a result of growing insurance fraud (Sonal 2022).

Telecom Fraud

Telecom fraud involves making use of telecommunications services and resources illegally and at no cost or at an unqualified low cost. Such fraudulent activities mainly include bypass fraud and reuse fraud. The growth of telecom frauds can be attributed to the increase in number of Internet users. The spread of technology has become both a facilitator and a shield of new types of telecom fraud, which makes the detection of these telecom scams increasingly difficult (Ayamga 2018).

Corresponding author: Gbenga Akinyemi
oluwagbenga.akinyemi@gmail.com
University of Hertfordshire, Hertfordshire Business School, United Kingdom.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(2), JUNE, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Tax Fraud

Tax fraud refers to individuals or entities intentionally misrepresenting financial information to tax authorities to avoid paying the proper taxes. Falsifying information, claiming unwarranted deductions or tax credits, or not paying taxes at all can be considered tax fraud. Despite the effects of the more serious types of tax fraud, they can go undetected for very long periods, since the problems of tax fraud often rely on the assurance that dishonest taxpayers will seize the chance to not pay their tax obligation (Abiddin & Akinyemi 2024).

Evolution of AI Technologies

Artificial Intelligence (AI) is an area of computer science that emulates intelligent behavior in computerized devices (Gams *et al*., 2019; Zhang & Lu 2021; Haldorai 2023). AI possesses the capability to learn from experience, adjust to changing inputs, analyze a demonstrated behavior of other agents, comprehend the implications of an existent situation, predict the effect of possible future actions and execute the right solution of all actions. In its endeavor to offer a solution to human problems, AI employs an interdisciplinary approach that chips in from mathematics, philosophy, psychology, neuropsychology, linguistics, computer engineering, and computer science.

AI is more extensive than mere problem-solving capabilities as it attempts to fill the gap between the behavior of man and machines. The futuristic vision of AI research aims at constructing machines that can execute all the problems humans can achieve (Baduge *et al*., 2022). Machine Learning (ML) is one of the key areas of AI and focuses on system behavior that simulates humans. This enables a computer to categorize, predict and cluster the solution approach without programming (Adeyeye & Akanbi 2024). AI has the capacity to automate specified tasks, which require expert human. This paper examines the role of Artificial Intelligence technology in Cyber Security for Financial Fraud Detection and Prevention.

AI Applications in Cybersecurity

Advancements in AI technology have augmented a wide range of cybersecurity tasks, leading to a surge of applications focused on threat detection and response, behavioral analysis, and automated incident response (Patil 2016). AI can augment many of the traditional techniques used for cybersecurity but at greater scale and speed. Cybersecurity professionals often face information overload, including security analysts who need to sift through massive potential security breaches to find real threats. More so, humans also struggle with speed of detection and response, especially in the face of evolving attacks that are difficult to detect. To address the limitations of human analysts, AI can monitor large datasets in real time. When combined with predictive modeling capabilities, it can efficiently analyze logs, alerts, and audit trails to identify patterns indicative of risks and threats—even within infrastructures with rapidly evolving perimeters. With its ability to swiftly detect and respond to cyber-attacks, AI has become an indispensable tool in modern cybersecurity operations.

Threat Detection and Response

Threat detection and response is the foundation of most security operations centers (SOCs). SOCs are responsible for detecting and responding to security incidents quickly and efficiently. They are typically reliant on a mixture of both human analysts and underlying technology to aid the detection and response processes. However, the rise of malicious automation—used by threat actors to create noise or amplify attacks—has significantly increased the difficulty of distinguishing genuine threats from false alarms. This results in an overwhelming number of alerts and further strains the human elements within SOCs (Chamkar et al., 2024). To tackle this, Security Information and Event Management (SIEM) vendors are evolving their platforms by integrating centralized data ingestion, aggregation, and correlation.

These platforms increasingly leverage machine learning-driven analytics to reduce the volume of irrelevant alerts and highlight high-risk

Corresponding author: Gbenga Akinyemi
✉ *oluwagbenga.akinyemi@gmail.com*
University of Hertfordshire, Hertfordshire Business School, United Kingdom.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(2), JUNE, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

incidents. As a result, AI enhances the accuracy and response time of SOCs, helping organizations stay ahead of emerging threats.

Behavioral Analysis

Behavioral analysis is another critical area where AI has made significant strides (Sheta, 2021; Samayamantri *et al*., 2024). Initially rooted in pattern-matching and heuristic-based techniques, behavioral analysis has evolved into a more sophisticated AI-driven discipline. AI-facilitated behavioral analysis is now widely recognized as a gold standard, especially in domains such as financial fraud detection and cybersecurity in eCommerce and retail.

Moreso, in banking sector, AI behavioral analysis is instrumental in detecting identity theft and false declines. By learning and continuously adapting to patterns of normal user behavior, AI can automatically differentiate between legitimate and fraudulent activities. These algorithms assess various parameters, including exposure risk, behavioral anomalies, and evolving usage trends, to adjust their thresholds dynamically. AI systems also support business-specific strategies, such as monitoring blacklist transactions linked to known criminal entities or adjusting model sensitivities based on fraud trends.

Machine Learning Techniques for Fraud Detection

Artificial Intelligence and Machine Learning techniques play a fundamental role in detecting financial fraud because they allow the implementation of pattern recognition methods to analyze massive amounts of transactions and identify anomalies with accuracy. Upon noticing an anomaly, fraud prevention mechanisms can block further operations and alert the users. Numerous methods have been proposed to this end in the last decade. The two main families of fraud detection techniques consist of supervised and unsupervised learning models. Due to the unbalanced nature of the fraud detection problem, where most transactions are not fraudulent and only a tiny fraction are anomalies, the supervised learning methods are usually implemented alongside anomaly detection methods for feature extraction, clustering, pre-processing, and imputation. In this section, the two main machine learning approach for financial fraud detection are presented.

Supervised Learning Approaches

Supervised learning approaches aim to create labeled data, which is a non-trivial problem in fraud detection (Alshantti 2024). Then, models based on logistic regression, Bayesian networks, decision trees, support two, Random Forest, and K-nearest-neighbors can be used to create the real fraudulent transactions class. These algorithms have been mixed to improve the estimation of the optimization threshold. The labeling of data can be performed in several ways. The first approach adopts a fully supervised setup, where a global fraud label is assigned based on the transaction's final destination—typically the associated bank account. However, the bank account is not always the only access point, and transactions are often conducted through various proxies or login addresses without any fraudulent intent.

The second approach introduces the concept of a Guest User—a user who exhibits behavioral attributes similar to those of a previously labeled fraudulent account, but in one or more non-fraudulent transactions that may have been overlooked during the bank's observation period. This methodology relies on similarity functions defined at the behavioral level. In this context, non-target users may carry out certain actions on behalf of Trusted Users—users who have not been flagged with any fraud labels.

Unsupervised Learning Techniques

Unsupervised learning techniques can be utilized to cluster or categorize the data without prior labeling of the samples. More precisely, they can be applied in the cases of fraud detection where no previous data of fraudulent activities are available for training a model. On the other hand, most of the unsupervised detection techniques are clustering-based approaches and have controversial detection results (Alshantti 2024). The popular among these clustering techniques are K-means, clustering with validity index,

Corresponding author: Gbenga Akinyemi
oluwagbenga.akinyemi@gmail.com
University of Hertfordshire, Hertfordshire Business School, United Kingdom.

Gaussian mixture model, fuzzy clustering, Fuzzy C-Means clustering, and fuzzy wavelet clustering. Other methods proposed in the field for unsupervised fraud detection are the nearest neighbour distance, Hidden Markov model, co-clustering, Independent Component Analysis, Bayesian network, selective naive Bayes classifier, k nearest neighbours, Gaussian process model, convex hull, the minimum description length principle, Principal Component Analysis, spectral component analysis, clustering subspace pattern, neuro-fuzzy approach, and more.

The incredible amount of transactions present in the financial sector makes it extremely hard to use supervised learning methods because all transactions should be labeled. The unlabeled data allows observing transactions as they are being executed. The unsupervised detection techniques are considered less efficient than supervised techniques but provide useful suggestions for the clever application of the tools. Sophisticated models can implement them to get better classification results. The prediction capabilities of the mentioned methods will not surpass the supervised scheme, but they can be remarkably applicable in problems where getting labeled samples is not possible or when fraudulent actions are very scarce compared to legitimate ones.

CONCLUSION

Artificial intelligence plays a crucial role in advancing cybersecurity measures within the financial industry. Utilizing sophisticated AI methods such as behavioral pattern analysis and machine learning models allows institutions to better identify and counteract fraudulent actions. Although challenges exist, particularly concerning data labeling and imbalanced datasets, AI solutions provide scalable and adaptive tools necessary for protecting vital financial information. As cyber threats continue to become more advanced, ongoing innovation and research into AI-driven security solutions are essential to preserve the integrity, safety, and trust in financial systems globally.

REFERENCES

Abiddin, N. Z., & Akinyemi, G. (2024). The Intersection Between E-Tax Administration, Sustainable Public Procurement and Sustainable Public Performance: A Review Conceptual Framework. *Journal of Lifestyle and SDGs Review*, *4*(2), e02328-e02328.

Akinyemi, G. (2025). Unlocking Financial Security with Blockchain: Opportunities and Challenges. *ATBU Journal of Science, Technology and Education*, *13*(2), 1-9.

Adeyeye, O. J., & Akanbi, I. (2024). Artificial intelligence for systems engineering complexity: a review on the use of AI and machine learning algorithms. *Computer Science & IT Research Journal*, *5*(4), 787-808.

Alshantti, A. A. S. (2024). On the Applications of Machine Learning for Alleviating Challenges in the Financial Crime Domain.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

Ayamga, D. (2018). Telecommunication fraud prevention policies and implementation challenge.

Baduge, S. K., Thilakarathna, S., Perera, J. S., Arashpour, M., Sharafi, P., Teodosio, B., ... & Mendis, P. (2022). Artificial intelligence and smart vision for building and construction 4.0: Machine and deep learning methods and applications. *Automation in Construction*, *141*, 104440.

Chamkar, A. S., Maleh, Y., & Gherabi, N. (2024). Security operation center. *The Art of Cyber Defense: From Risk Assessment to Threat Intelligence*, 271.

Chinedu, P. U., Nwankwo, W., Aliu, D., Shaba, S. M., & Momoh, M. O. (2020). Cloud security concerns: assessing the fears of service adoption. *Archive of Science and Technology*, *1*(2), 164-174.

Corresponding author: Gbenga Akinyemi
✉ *oluwagbenga.akinyemi@gmail.com*
University of Hertfordshire, Hertfordshire Business School, United Kingdom.

Daniel, A., Shaba, S. M., Momoh, M. O., Chinedu, P. U., & Nwankwo, W. (2021). A computer security system for cloud computing based on encryption technique. *Computer Engineering and Applications*, *10*(1), 41-53.

Dara, J., & Gundemoni, L. (2006). Credit Card Security and E-Payment: Enquiry into credit card fraud in E-Payment.

Franjić, S. (2020). Cybercrime is very dangerous form of criminal behavior and cybersecurity. *Emerging Science Journal*, *4*(18), 18-26.

Gams, M., Gu, I. Y. H., Härmä, A., Muñoz, A., & Tam, V. (2019). Artificial intelligence and ambient intelligence. *Journal of Ambient Intelligence and Smart Environments*, *11*(1), 71-86.

Haldorai, A. (2023). A review on artificial intelligence in internet of things and cyber physical systems. *Journal of Computing and Natural Science*, *3*(1), 012-023.

Hashim, H. A., Salleh, Z., Shuhaimi, I., & Ismail, N. A. N. (2020). The risk of financial fraud: a management perspective. *Journal of Financial Crime*, *27*(4), 1143-1159.

Nwankwo, W., Chinedu, P. U., Daniel, A., Shaba, S. M., Muyideen, M. O., Nwankwo, C. P., ... & Uwadia, F. (2022, November). Educational FinTech: Promoting Stakeholder Confidence Through Automatic Incidence Resolution. In *The International Symposium on Computer Science, Digital Economy and Intelligent Systems* (pp. 947-963). Cham: Springer Nature Switzerland.

Patil, P. (2016). Artificial intelligence in cybersecurity. *International journal of research in computer applications and robotics*, *4*(5), 1-5.

Samayamantri, L. S., Singhal, S., Krishnamurthy, O., & Regin, R. (2024). AI-Driven Multimodal Approaches to Human Behavior Analysis. In *Advancing Intelligent Networks Through Distributed Optimization* (pp. 485-506). IGI Global.

Sheta, S. V. (2021). Artificial Intelligence Applications in Behavioral Analysis for Advancing User Experience Design. *Available at SSRN 5034079*.

Sonal, S. (2022). Insurance Fraud Prevention Laws, a Need of Time: A Critical Analysis. *Indian JL & Legal Rsch.*, *4*, 1.

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. *Journal of Industrial Information Integration*, *23*, 100224.

Corresponding author: Gbenga Akinyemi
✉ *oluwagbenga.akinyemi@gmail.com*
University of Hertfordshire, Hertfordshire Business School, United Kingdom.