World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Detecting insider threats in banking using AI-driven anomaly detection with a data science approach to cybersecurity

Akintayo Micheal Ajayi [1], Abraham Okandeji Omokanye [2], Olawale Olowu [3], Ademilola Olowofela Adeleye [4], Olayinka Mary Omole [5,*] and Ifeoluwa Uchechuwkuw Wada [6]

[1] *College of Engineering Technology, Grand Canyon University, Phoenix, Arizona, USA.*
[2] *Department of Engineering and Computer Science, University of East London.*
[3] *Interswitch Group, Lagos, Nigeria.*
[4] *Joltz Security Nigeria Limited, Lagos, Nigeria.*
[5] *IT Project Manager independent Research consultant, Toronto, Canada.*
[6] *Department of Information Technology services, Washburn University, Topeka, KS USA.*

World Journal of Advanced Research and Reviews, 2024, 24(02), 123–132

Publication history: Received on 27 September 2024; revised on 04 November 2024; accepted on 06 November 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.2.3182

Abstract

The banking sector faces an increasingly critical challenge in detecting and preventing insider threats, which account for significant financial losses and data breaches annually. This comprehensive review explores how artificial intelligence-driven anomaly detection, integrated with advanced data science approaches and cybersecurity frameworks, is transforming insider threat detection in banking institutions. By synthesizing current research in behavioral analytics, machine learning methodologies, and employee activity monitoring, the study examines how AI-driven technologies are revolutionizing traditional approaches to insider threat detection and risk management. The review critically analyzes emerging AI-driven methodologies, particularly focusing on unsupervised learning techniques, behavioral pattern analysis, and real-time employee activity monitoring systems. Through an extensive examination of behavioral analytics frameworks, privileged access monitoring, and user entity behavior analytics (UEBA), the research illuminates both the potential and challenges of AI-powered insider threat detection. The investigation reveals significant advancements in behavioral anomaly detection, predictive modeling of employee activities and network behavior analysis while simultaneously addressing critical privacy considerations and regulatory complexities specific to employee monitoring.

Keywords: Insider Threat Detection; Behavioral Analytics; Employee Monitoring; Anomaly Detection; User Entity Behavior Analytics (UEBA); Privileged Access Management

1. Introduction

The global banking ecosystem is experiencing unprecedented challenges in financial crime prevention, characterized by increasingly complex and technologically sophisticated criminal strategies. Traditional detection methods have become increasingly inadequate in addressing the rapidly evolving landscape of financial malfeasance, necessitating a fundamental reimagining of prevention and detection mechanisms.

The current technological landscape presents both remarkable opportunities and significant challenges for financial institutions [1]. Emerging artificial intelligence and advanced technological paradigms offer unprecedented capabilities in detecting, predicting, and preventing financial crimes. Machine learning algorithms, deep learning networks, and

* Corresponding author: Olayinka Mary Omole

sophisticated data analytics have demonstrated remarkable potential in identifying intricate patterns and anomalies that would remain invisible to traditional investigative approaches [2].

The banking sector reported over $70 billion in losses due to insider threats in 2023, with privileged users accounting for 60% of incidents [3]. Traditional detection methods have proven inadequate against sophisticated insider threats, who leverage their authorized access and institutional knowledge to circumvent security measures. The complexity of modern banking systems, combined with employees' extensive access privileges, creates an environment where malicious insider activities can remain undetected for extended periods. [4]

This comprehensive review aims to provide a holistic examination of the current state of financial crime prevention in banking, with a specific focus on the transformative potential of artificial intelligence and advanced technologies. By critically analyzing existing methodologies, technological innovations, and implementation challenges, the research seeks to accomplish several key objectives. First, to evaluate the effectiveness of current financial crime detection strategies and their inherent limitations. Second, to explore the diverse applications of AI and machine learning in identifying and preventing financial criminal activities. Third, to assess the integration of cybersecurity frameworks and data science approaches in creating more robust prevention mechanisms.

The scope of the review encompasses multiple interconnected domains, including supervised and unsupervised learning techniques, threat intelligence systems, big data analytics, predictive modeling, and regulatory compliance considerations. By synthesizing insights from diverse technological and academic perspectives, the research aims to provide a comprehensive understanding of how advanced technologies are fundamentally reshaping financial crime prevention strategies in the banking sector.

2. State of Financial Crime Prevention in Banking

In the context of insider threats, traditional detection methods in banking have historically relied on periodic access reviews, basic user activity logging, and manual supervision processes [5]. These conventional approaches have proven particularly inadequate in identifying sophisticated insider activities, where perpetrators often operate within their authorized access levels and understand internal control mechanisms. The complexity of insider threat detection is further compounded by the need to monitor legitimate activities while identifying potentially malicious behavior patterns.

The limitations of traditional detection mechanisms become particularly pronounced in an era of unprecedented financial complexity [6]. Manual review processes are inherently time-consuming, resource-intensive, and prone to human error. Financial institutions have historically grappled with high false-positive rates, where legitimate transactions are incorrectly flagged as suspicious, leading to unnecessary customer friction and operational inefficiencies [7]. Moreover, these systems typically exhibited minimal adaptability, failing to incorporate real-time learning and dynamic risk assessment capabilities.

The limitations of traditional detection mechanisms become especially pronounced when dealing with insider threats. Manual review processes struggle to differentiate between legitimate work activities and malicious insider actions, leading to both false positives and dangerous oversight [8]. Employee monitoring systems based on static rules fail to adapt to evolving job roles and responsibilities, creating significant blind spots in detecting insider misconduct. The challenge of establishing reliable baseline behavior patterns while respecting employee privacy adds another layer of complexity to detection efforts [9].

Current challenges in financial crime detection are multifaceted and increasingly complex. The globalization of financial systems, proliferation of digital transaction channels, and rapid technological innovations have created an intricate landscape of potential vulnerabilities [10]. Cybercriminals continuously evolve their strategies, leveraging advanced technologies and sophisticated network connections to circumvent traditional detection mechanisms [11]. The emergence of cryptocurrency, cross-border digital transactions, and complex financial instruments has further complicated the detection landscape.

The regulatory framework surrounding financial crime prevention has become progressively more stringent and comprehensive. Regulatory bodies worldwide have implemented increasingly sophisticated compliance requirements, mandating robust risk management protocols and advanced detection capabilities [12]. Frameworks such as the Bank Secrecy Act (BSA), Anti-Money Laundering (AML) regulations, and Know Your Customer (KYC) guidelines have established comprehensive standards for financial institutions.

Recent regulatory updates have specifically addressed insider threat detection, including the Insider Threat Program requirements under NIST SP 800-53 and updated guidelines from financial regulatory bodies [13]. These new requirements mandate sophisticated insider threat detection capabilities, continuous monitoring of employee activities, robust audit trails, and proactive threat detection mechanisms. Financial institutions must now demonstrate comprehensive programs for identifying and mitigating insider threats while maintaining compliance with employee privacy regulations.

3. AI and Machine Learning Applications

3.1. Supervised Learning Approaches

Supervised learning represents a critical methodology in financial crime detection, leveraging historical transaction data to train algorithms capable of recognizing complex fraudulent patterns [14]. These approaches utilize labeled datasets where known instances of financial crimes are used to teach machine learning models intricate detection mechanisms. By analyzing extensive historical data, supervised learning algorithms develop increasingly sophisticated pattern recognition capabilities that can identify potential criminal activities with remarkable precision [15].

The core strength of supervised learning lies in its ability to classify transactions based on predefined characteristics of known fraudulent behaviors. Neural networks and decision tree algorithms can process vast quantities of transactional data, identifying subtle correlations and anomalies that would remain imperceptible to human investigators [16]. Financial institutions can effectively map historical fraud patterns, creating predictive models that continuously evolve and adapt to emerging criminal methodologies.

In the context of insider threat detection, supervised learning models leverage historical cases of confirmed insider misconduct [17]. These models analyze patterns in employee system access, transaction approvals, data access timing, and system privilege usage. The algorithms can identify subtle deviations from department-specific work patterns and flag potential insider activities for investigation.

3.2. Unsupervised Anomaly Detection

Unsupervised anomaly detection techniques offer a complementary approach to supervised methodologies, focusing on identifying statistically significant deviations from established behavioral norms [18]. Unlike traditional supervised approaches, these techniques do not rely on predefined labeling, instead employing sophisticated clustering algorithms and statistical distribution analysis to detect unusual transaction patterns.

These methodologies excel in identifying previously unknown patterns of insider threat behavior by establishing baseline behavioral models for different employee roles. The analysis encompasses system access patterns, data transfer activities, temporal usage patterns, and combinations of seemingly normal activities that may indicate suspicious behavior [19]. Advanced clustering algorithms group similar employee behaviors, revealing hidden patterns that might indicate potential insider threats.

While unsupervised anomaly detection excels at identifying unknown patterns without predefined labels, deep learning technologies extend these capabilities by processing complex, multi-dimensional data through sophisticated neural networks [20]. This complementary approach combines the flexibility of unsupervised learning with the advanced pattern recognition capabilities of deep learning architectures.

3.3. Deep Learning in Fraud Detection

Deep learning technologies have revolutionized fraud detection capabilities through advanced neural network architectures. These sophisticated algorithms process multi-dimensional data sources, incorporating contextual information beyond traditional transactional parameters [21]. Convolutional and recurrent neural networks enable comprehensive analysis of complex, interconnected financial behaviors, providing unprecedented insights into potential criminal activities.

By leveraging multiple layers of computational analysis, deep learning models can identify intricate relationships and patterns that traditional statistical methods might overlook [22]. These technologies can integrate diverse data sources, including transaction histories, user behaviors, geographic information, and temporal patterns to create holistic fraud detection mechanisms.

3.4. Real-time Transaction Monitoring Systems

Real-time transaction monitoring systems represent the pinnacle of AI-driven financial crime prevention [23]. These advanced platforms leverage machine learning algorithms to continuously analyze transactions, providing instantaneous risk assessments and potential intervention mechanisms. By integrating multiple data sources and employing sophisticated predictive modeling, these systems can identify potential criminal activities with remarkable precision and minimal latency.

The key advantage of real-time monitoring lies in its ability to provide immediate risk assessment, enabling financial institutions to intervene potentially fraudulent activities at the moment of occurrence [24]. Advanced algorithmic approaches can generate dynamic risk scores, allowing for instantaneous decision-making and prevention of financial crimes.

4. Cybersecurity Integration

4.1. Threat Intelligence Systems

Threat intelligence systems have become fundamental components of comprehensive financial crime prevention strategies [25]. These advanced platforms aggregate and analyze data from multiple sources, providing holistic insights into emerging cyber threats and potential vulnerabilities. By continuously monitoring global threat landscapes, financial institutions can develop proactive defensive strategies.

The complexity of modern cyber threats requires sophisticated intelligence gathering mechanisms that can predict and preempt potential security breaches [26]. Advanced threat intelligence platforms utilize machine learning and big data analytics to create comprehensive threat assessment frameworks.

4.2. Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) technologies offer comprehensive monitoring and analysis capabilities, integrating security event data from diverse technological ecosystems [27]. These sophisticated platforms enable real-time threat detection, comprehensive logging, and advanced forensic analysis. SIEM technologies provide financial institutions with unprecedented visibility into potential security vulnerabilities and suspicious activities [28].

By centralizing log management and providing comprehensive security event correlation, SIEM platforms can identify complex attack patterns that might go unnoticed through traditional monitoring approaches [29]. The integration of machine learning algorithms further enhances these platforms' predictive capabilities.

4.3. Identity and Access Management

Identity and access management represents a critical layer of cybersecurity integration in financial crime prevention. Advanced biometric authentication, multi-factor verification, and behavioral analysis technologies have transformed traditional access control mechanisms [30]. These sophisticated approaches go beyond traditional password-based systems, incorporating contextual and behavioral insights to verify user identities. Recent research has demonstrated that beyond simple password methods, multi-factor authentication (MFA) has become crucial in strengthening access controls in financial systems. MFA significantly reduces unauthorized access risks even when login credentials are compromised by requiring additional verification factors such as biometrics or one-time passwords, making it an essential component of modern financial security frameworks [31].

Behavioral analytics framework, including typing patterns, mouse movements, and device interaction characteristics, provide additional layers of authentication that significantly reduce the risk of unauthorized access [32]. Machine learning algorithms continuously learn and adapt to individual user behaviors, creating dynamic and responsive security frameworks.

Modern identity management frameworks incorporate sophisticated privileged access monitoring capabilities that track and analyze high-risk user activities [33]. User and Entity Behavior Analytics (UEBA) enhances these systems by establishing baseline behavioral patterns for different user roles and detecting anomalous activities [34]. The monitoring framework conducts continuous employee activity monitoring across systems, creating comprehensive behavioral analytics profiles that help identify potential insider threats while maintaining necessary access controls.

4.4. Blockchain-based Solutions

Blockchain-based solutions have emerged as innovative approaches to enhancing financial security and transparency. Distributed ledger technologies offer unprecedented capabilities in creating immutable, transparent transaction records [35]. By decentralizing transaction verification and creating comprehensive audit trails, blockchain technologies introduce fundamental innovations in financial crime prevention methodologies.

The inherent characteristics of blockchain immutability, transparency, and decentralized verification—provide robust mechanisms for preventing financial fraud. Smart contracts and cryptographic protocols can automate compliance processes, reducing human error and creating tamper-proof transaction records [36]. While cybersecurity integration provides the foundation for secure operations, the data science framework builds upon these security measures to extract actionable insights. This synergy between security infrastructure and analytical capabilities creates a comprehensive approach to financial crime prevention.

5. Data Science and Analytics Framework

5.1. Big Data Analytics in Crime Detection

Big data analytics has emerged as a transformative approach in financial crime detection, enabling financial institutions to process and analyze massive volumes of complex, multi-dimensional data [37]. Traditional analytical methods are fundamentally insufficient in handling the enormous scale and complexity of modern financial transactions. By leveraging advanced computational technologies, big data analytics can simultaneously process structured and unstructured data sources, identifying intricate patterns and potential criminal activities that would remain undetectable through conventional analysis [38].

The integration of distributed computing frameworks and advanced machine learning algorithms allows for real-time processing of vast datasets [39]. These technologies can correlate information from diverse sources, including transaction histories, social media interactions, geolocation data, and external economic indicators, creating comprehensive risk assessment models with unprecedented depth and accuracy.

5.2. Predictive Modeling Approaches

Predictive modeling represents a sophisticated approach to anticipating potential financial criminal activities before they materialize [40]. These advanced analytical techniques utilize historical data to develop probabilistic models that can forecast potential risks and suspicious behaviors. Machine learning algorithms, particularly ensemble methods and advanced neural networks, enable the creation of dynamic predictive models that continuously learn and adapt to emerging financial crime patterns [41].

The core strength of predictive modeling lies in its ability to move beyond reactive detection, transitioning towards proactive prevention [42]. By identifying subtle precursor indicators and statistical anomalies, these models can generate early warning systems that alert financial institutions to potential risks with remarkable precision.

5.3. Network Analysis for Pattern Detection

Network analysis provides a sophisticated methodology for understanding complex interconnections within financial transaction ecosystems [43]. By mapping relationships between entities, transactions, and behavioral patterns, these advanced analytical techniques can reveal hidden networks of potentially fraudulent activities. Graph theory and advanced computational algorithms enable the visualization and analysis of intricate relationships that might indicate organized financial criminal operations [44].

Machine learning enhanced network analysis, can identify sophisticated patterns of collusion, money laundering, and complex fraud schemes that would remain invisible through traditional investigative approaches [45]. These techniques can detect subtle anomalies in transaction networks, revealing potential criminal infrastructures with unprecedented granularity.

5.4. Comprehensive Privacy Framework and Behavioral Analytics

Comprehensive privacy frameworks and behavioral analytics in financial crime prevention require a delicate balance between technical implementation and behavioral monitoring [46]. Financial institutions employ advanced cryptographic techniques such as homomorphic encryption and differential privacy to enable thorough data analysis

while ensuring strict confidentiality and regulatory compliance. Through these sophisticated methods, organizations can effectively analyze comprehensive datasets without compromising individual privacy rights.

The behavioral analytics framework operates within this privacy conscious environment by implementing federated learning and secure multi-party computation, alongside advanced anonymization and secure storage protocols [47]. This technical foundation supports the continuous monitoring of employee activities, establishing baseline work patterns, tracking system access behaviors, and analyzing communication trends to create comprehensive behavioral models. Organizations maintain this security infrastructure through clear governance policies on data collection and retention, implementing defined access controls, conducting regular privacy impact assessments, and managing employee rights and consent. The framework integrates seamlessly with regulatory requirements through documented compliance measures, regular audits, and established incident response procedures, ensuring that behavioral analytics fulfills its security objectives while maintaining robust privacy protections and creating a balanced framework that safeguards both organizational assets and individual privacy rights in the modern financial environment.

6. Challenges and Limitations

The implementation of advanced technological solutions in financial crime prevention confronts numerous significant challenges. Technical obstacles remain substantial, with complex integration requirements and the inherent complexity of developing sophisticated machine learning models capable of adapting to rapidly evolving criminal methodologies [48]. Financial institutions must invest considerable resources in technological infrastructure, talent acquisition, and continuous model refinement.

Implementation barriers extend beyond technological constraints, encompassing organizational culture, resistance to technological transformation, and significant financial investments required for comprehensive system overhauls [49]. Many traditional financial institutions struggle with legacy technological ecosystems that are fundamentally incompatible with advanced analytical approaches.

Privacy and ethical considerations represent critical challenges in developing advanced financial crime prevention technologies. The extensive data collection and analysis required raise significant concerns regarding individual privacy, potential algorithmic bias, and the potential for unintended discriminatory outcomes [50]. Balancing effective crime prevention with robust ethical frameworks demands sophisticated governance mechanisms and transparent algorithmic design.

Regulatory compliance introduces additional layers of complexity, with financial institutions required to navigate intricate and often evolving legal frameworks. The rapid pace of technological innovation frequently outstrips regulatory adaptation, creating potential legal uncertainties and implementation challenges for advanced crime prevention technologies.

7. Future Directions and Opportunities

The future of financial crime prevention is intrinsically linked to continuous technological innovation and interdisciplinary collaboration. Emerging technologies such as quantum computing, advanced artificial intelligence, and sophisticated distributed ledger systems present unprecedented opportunities for transforming financial security frameworks [51]. These technologies promise to deliver increasingly sophisticated, adaptive, and proactive crime prevention mechanisms.

Significant research gaps persist in understanding the full potential of advanced technologies in financial crime prevention. Interdisciplinary research combining computer science, forensic accounting, behavioral psychology, and legal frameworks will be crucial in developing comprehensive, ethically robust prevention strategies [52]. Academic and industrial collaborations can accelerate the development of more sophisticated analytical approaches.

Integration opportunities span multiple domains, including enhanced international regulatory cooperation, development of global standards for technological implementation, and creation of collaborative platforms for threat intelligence sharing. The future of financial crime prevention will likely rely on unprecedented levels of technological collaboration and information exchange across institutional and national boundaries [53].

Policy recommendations must focus on creating flexible, technology neutral regulatory frameworks that can adapt to rapid technological changes. Governments and regulatory bodies must develop sophisticated approaches that

encourage technological innovation while maintaining robust protective mechanisms for financial systems and individual rights.

8. Conclusion and Recommendation

The landscape of financial crime prevention has undergone a fundamental transformation, driven by the convergence of artificial intelligence, advanced data analytics, and sophisticated cybersecurity technologies. This comprehensive review illuminates the profound potential of emerging technologies to revolutionize how financial institutions detect, prevent, and mitigate financial criminal activities. The integration of machine learning, deep learning, and real-time monitoring systems represents a paradigm shift from reactive detection to proactive prevention, offering unprecedented capabilities in identifying complex and evolving financial crime patterns.

The research underscores the critical importance of a holistic approach to financial crime prevention. Traditional methodologies have been demonstrably insufficient in addressing the increasingly sophisticated strategies employed by financial criminals. Advanced technologies provide a multidimensional framework for understanding and counteracting potential threats, leveraging complex data analysis, network pattern recognition, and predictive modeling to create more robust protective mechanisms.

Critically, the future of financial crime prevention is not solely technological but fundamentally interdisciplinary. The successful implementation of advanced prevention strategies requires a delicate balance between technological innovation, ethical considerations, regulatory compliance, and human expertise. As financial systems become increasingly complex and interconnected, the need for adaptive, intelligent, and comprehensive crime prevention approaches becomes increasingly paramount.

Recommendations

The first critical recommendation is the development of comprehensive, integrated technological ecosystems within financial institutions. Organizations must invest in holistic technological transformation, moving beyond siloed approaches to create unified, adaptive crime prevention frameworks. This requires significant investment in advanced machine learning infrastructure, continuous talent development, and a culture of technological innovation and adaptability.

Collaborative approaches represent a second fundamental recommendation. Financial institutions, regulatory bodies, and technological innovators must develop unprecedented levels of information sharing and collaborative threat intelligence. The creation of global platforms for real-time threat analysis, standardized data exchange protocols, and collaborative research initiatives can significantly enhance the collective capacity to detect and prevent financial criminal activities.

The final recommendation focuses on developing robust ethical and regulatory frameworks that can accommodate rapid technological innovation. Policymakers and regulatory bodies must create flexible, technology-neutral guidelines that encourage technological advancement while maintaining stringent protective mechanisms. This requires a proactive approach to policy development, with continuous dialogue between technological innovators, financial institutions, legal experts, and regulatory bodies to ensure that prevention technologies remain both cutting-edge and ethically responsible.

The implementation of these recommendations requires a holistic approach that recognizes the interconnected nature of technological solutions and human factors. Building upon the technological and collaborative frameworks discussed above, the final recommendation addresses the critical human element through behavioral analytics integration.

The fourth critical recommendation focuses on implementing comprehensive behavioral analytics programs that integrate with the previously discussed technological and collaborative frameworks. Organizations must develop sophisticated monitoring approaches that balance security requirements with privacy considerations, creating a unified approach to insider threat detection and prevention. This integration requires that organizations must ensure the behavioral analytics programs align seamlessly with AI and machine learning capabilities discussed in earlier recommendations. These programs should fully integrate with the collaborative frameworks established above to maximize effectiveness. The implementation must strictly adhere to the proposed regulatory and ethical guidelines to maintain compliance. Furthermore, the behavioral analytics system needs to maintain clear connections to the technological ecosystem recommendations to ensure cohesive operations. This balanced approach creates a comprehensive security framework that addresses both technical and human aspects of financial crime prevention

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Kidwell DS, Blackwell DW, Whidbee DA. Financial institutions, markets, and money. John Wiley & Sons; 2016 Oct 31.

[2] Balcıoğlu YS. Revolutionizing Risk Management AI and ML Innovations in Financial Stability and Fraud Detection. InNavigating the Future of Finance in the Age of AI 2024 (pp. 109-138). IGI Global.

[3] George AS, Baskar T, Srikaanth PB. Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal. 2024 Feb 25;2(1):51-75.

[4] Al-Mhiqani, M.N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K.H., Ali, N.S. and Yunos, Z., 2020. A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. *Applied Sciences*, *10*(15), p.5208.

[5] Cappelli DM, Moore AP, Trzeciak RF. The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley; 2012 Jan 20.

[6] Allioui H, Mourdi Y. Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. Sensors. 2023 Sep 22;23(19):8015.

[7] Banik S, Dandyala SS. Automated vs. Manual Testing: Balancing Efficiency and Effectiveness in Quality Assurance. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 2019 Dec 15;10(1):100-19.

[8] Cappelli DM, Moore AP, Trzeciak RF. The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley; 2012 Jan 20.

[9] Anti E, Vartiainen T. Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review. Association for Information Systems.

[10] Halawi L, Bacon R. Exploring the Nexus of Cybercrime, Money Laundering, Ethics and Deterrence in the Age of Smart Machines.

[11] Obi OC, Akagha OV, Dawodu SO, Anyanwu AC, Onwusinkwue S, Ahmad IA. Comprehensive review on cybersecurity: modern threats and advanced defense strategies. Computer Science & IT Research Journal. 2024 Feb 2;5(2):293-310.

[12] Sharman JC. The money laundry: Regulating criminal finance in the global economy. Cornell University Press; 2011 Oct 15.

[13] Boakye-Gyan K. An Approach to a Comprehensive Framework for Insider Threat. Capitol Technology University; 2021.

[14] Bello OA, Folorunso A, Ejiofor OE, Budale FZ, Adebayo K, Babatunde OA. Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions. International Journal of Management Technology. 2023;10(1):85-108.

[15] Kute DV, Pradhan B, Shukla N, Alamri A. Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review. IEEE access. 2021 Jun 4;9:82300-17.

[16] Chen Z, Van Khoa LD, Teoh EN, Nazir A, Karuppiah EK, Lam KS. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. Knowledge and Information Systems. 2018 Nov;57:245-85.

[17] Manoharan P. *Supervised Learning for Insider Threat Detection* (Doctoral dissertation, Victoria University).

[18] Goldstein M, Uchida S. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PloS one. 2016 Apr 19;11(4):e0152173.

[19] Manoharan P. *Supervised Learning for Insider Threat Detection* (Doctoral dissertation, Victoria University).

[20] Parimala VK, editor. Anomaly Detection: Recent Advances, AI and ML Perspectives and Applications.

[21] Shehadeh M. Exploring Cutting-Edge Algorithms in Islamic Banking: Machine Learning and Deep Learning for Enhanced Decision-Making and Risk Management.

[22] Ikemefuna CD, Okusi O, Iwuh AC, Yusuf S. ADAPTIVE FRAUD DETECTION SYSTEMS: USING ML TO IDENTIFY AND RESPOND TO EVOLVING FINANCIAL THREATS.

[23] Xu J, Yang T, Zhuang S, Li H, Lu W. AI-based financial transaction monitoring and fraud prevention with behaviour prediction.

[24] Adeyemo K, Obafemi FJ. A Survey on the Role of Technological Innovation in Nigerian Deposit Money Bank Fraud Prevention. South Asian Journal of Social Studies and Economics. 2024 Feb 12;21(3):133-50.

[25] Singh VB, Singh P, Guha SK, Shah AI, Samdani A, Nomani MZ, Tiwari M. The Future of Financial Crime Prevention and Cybersecurity with Distributed Systems and Computing Approaches. Meta Heuristic Algorithms for Advanced Distributed Systems. 2024 Apr 2:321-40.

[26] Kasowaki L, Alp K. Threat Intelligence: Understanding and Mitigating Cyber Risks. EasyChair; 2024 Jan 6.

[27] Gnatyuk S, Berdibayev R, Aleksander M, Sydorenko V, Zhyharevych O, Polozhentsev A. Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure. InData-Centric Business and Applications: Advancements in Information and Knowledge Management, Volume 1 2024 Aug 8 (pp. 247-269). Cham: Springer Nature Switzerland.

[28] Malik AW, Bhatti DS, Park TJ, Ishtiaq HU, Ryou JC, Kim KI. Cloud digital forensics: Beyond tools, techniques, and challenges. Sensors. 2024 Jan 10;24(2):433.

[29] Sania NS, Gigras Y, Mahajan S. Gatividhi Guard: The Activity Guardian—Revolutionizing Security Information and Event Management (SIEM) Technology. Journal of Operating Systems Development & Trends. 2024;11(1):29-44p.

[30] Oyeniyi LD, Ugochukwu CE, Mhlongo NZ. Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices. Computer Science & IT Research Journal. 2024 Apr 17;5(4):903-25.

[31] Olaiya OP, Adesoga TO, Ojo A, Olagunju OD, Ajayi OO, Adebayo YO. Cybersecurity strategies in fintech: safeguarding financial data and assets. GSC Advanced Research and Reviews. 2024;20(1):050-6.

[32] Oduri S. Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era. International Journal of Innovative Research in Science Engineering and Technology. 2024;13:13632-40.

[33] Oduri S. Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era. International Journal of Innovative Research in Science Engineering and Technology. 2024;13:13632-40.

[34] Mohanty RK, Kumar AP, Padmaja R, Prashanthi V. Deep Learning for Analyzing User and Entity Behaviors: Techniques and Applications. InConsumer and Organizational Behavior in the Age of AI 2024 (pp. 219-250). IGI Global.

[35] Udeh EO, Amajuoyi P, Adeusi KB, Scott AO. Blockchain-driven communication in banking: Enhancing transparency and trust with distributed ledger technology. Finance & Accounting Research Journal. 2024 Jun 6;6(6):851-67.

[36] Kumar B, Malaviya MP, Dhodhiawala Z, Hafeez SA, Murala DK. Financial Fraud Detection and Prevention Using Blockchain and Integration of Hyperledger. IUP Journal of Computer Sciences. 2024 Oct 1;18(4).

[37] Sabharwal R. An Innovative Big Data Analytics Method for Detecting Data Abnormalities in Business Organisations.

[38] Ogbu AD, Iwe KA, Ozowe W, Ikevuje AH. Geostatistical concepts for regional pore pressure mapping and prediction. Global Journal of Engineering and Technology Advances. 2024;20(01):105-17.

[39] Althati C, Tomar M, Shanmugam L. Enhancing Data Integration and Management: The Role of AI and Machine Learning in Modern Data Platforms. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023. 2024 Feb 22;2(1):220-32.

[40] Asghar J, Abbas G. AI and Predictive Analytics: A New Era of Fraud Detection and AML in Financial Services.

[41] Adeniran IA, Efunniyi CP, Osundare OS, Abhulimen AO. Enhancing security and risk management with predictive analytics: A proactive approach. International Journal of Management & Entrepreneurship Research. 2024;6(8).

[42] Adeniran IA, Efunniyi CP, Osundare OS, Abhulimen AO. Enhancing security and risk management with predictive analytics: A proactive approach. International Journal of Management & Entrepreneurship Research. 2024;6(8).

[43] Challoumis C. THE FUTURE OF MONEY-EXPLORING AI'S ROLE IN FINANCE AND PAYMENTS. InXVI International Scientific Conference 2024 Oct (pp. 158-189).

[44] Chatterjee P, Das D, Rawat DB. Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements. Future Generation Computer Systems. 2024 Apr 30.

[45] Alshantti AA. On the Applications of Machine Learning for Alleviating Challenges in the Financial Crime Domain.

[46] Shoetan PO, Oyewole AT, Okoye CC, Ofodile OC. Reviewing the role of big data analytics in financial fraud detection. Finance & Accounting Research Journal. 2024 Mar 17;6(3):384-94.

[47] Amo-Filva D, Fonseca D, García-Peñalvo FJ, Forment MA, Guerrero MJ, Godoy G. Exploring the landscape of learning analytics privacy in fog and edge computing: A systematic literature review. Computers in Human Behavior. 2024 May 15:108303.

[48] Phd CK, CNA DO, Osasona AV. An Assessment of Forensic Accountants in Detection and Prevention of Financial Crimes in Business Organizations. Zien Journal of Social Sciences and Humanities. 2024 Apr 12;31:1-1.

[49] Ahmadirad Z. The Beneficial Role of Silicon Valley's Technological Innovations and Venture Capital in Strengthening Global Financial Markets. International journal of Modern Achievement in Science, Engineering and Technology. 2024 Aug 30;1(3):9-17.

[50] Halawi L, Bacon R. Exploring the Nexus of Cybercrime, Money Laundering, Ethics and Deterrence in the Age of Smart Machines.

[51] Aivaz KA, Florea IO, Munteanu I. Economic Fraud and Associated Risks: An Integrated Bibliometric Analysis Approach. Risks. 2024 Apr 30;12(5):74.

[52] Halawi L, Bacon R. Exploring the Nexus of Cybercrime, Money Laundering, Ethics and Deterrence in the Age of Smart Machines.

[53] Radanliev P. Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology. 2024 Feb 7:1-51.