International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

AI-powered financial crime prevention with cybersecurity, IT, and data science in modern banking

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

[1] *Department of Engineering and Computing, School of Architecture, Computing, and Engineering, University of East London, London, United Kingdom.*
[2] *College of Engineering Technology, Grand Canyon University, Phoenix, Arizona, USA.*
[3] *Interswitch Group, Lagos, Nigeria.*
[4] *Joltz Security Nigeria Limited, Lagos, Nigeria.*
[5] *Department of Computer Science, Montclair State University, New Jersey, USA.*
[6] *Independent Research Consultant (Foylan Incorporated), IT Project Manager, Toronto, Canada.*

International Journal of Science and Research Archive, 2024, 13(02), 570–579

Publication history: Received on 25 September 2024; revised on 05 November 2024; accepted on 07 November 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.13.2.2143

Abstract

Financial crime in modern banking has evolved significantly with the digital transformation of financial services, presenting unprecedented challenges to traditional prevention methods. This comprehensive review examines the integration of artificial intelligence (AI), cybersecurity frameworks, and data science methodologies in combating financial crime within the banking sector. We analyze the current state of AI-powered solutions, including machine learning models, real-time detection systems, and advanced analytics frameworks that have transformed financial crime prevention. The review synthesizes findings from recent studies and industry implementations, highlighting the synergistic relationship between AI technologies and cybersecurity measures in creating robust defense mechanisms. Our analysis reveals that while AI-powered solutions demonstrate superior detection rates and reduced false positives compared to traditional methods, significant challenges remain in areas of data privacy, regulatory compliance, and system integration. The paper concludes by identifying critical research gaps and proposing future directions for enhancing the effectiveness of AI-based financial crime prevention systems. This review provides valuable insights for researchers, banking professionals, and policymakers working at the intersection of AI, cybersecurity, and financial crime prevention.

Keywords: Artificial Intelligence; Financial Crime Prevention; Machine Learning; Cybersecurity; Banking Security; Data Analytics

1. Introduction

The proliferation of digital banking services and financial technology has fundamentally transformed the landscape of financial crime, creating new vulnerabilities while simultaneously offering unprecedented opportunities for detection and prevention. Financial institutions face increasingly sophisticated criminal activities that exploit the complexity and interconnectedness of modern banking systems[1]. This evolution of financial crime has necessitated a corresponding advancement in prevention methodologies, leading to the emergence of AI-powered solutions integrated with robust cybersecurity frameworks and sophisticated data science approaches.

* Corresponding author: Ernest C Chianumba

Our review methodology encompasses systematic analysis of peer-reviewed literature, industry reports, regulatory frameworks, and empirical studies from the past five years, with particular emphasis on implementations in major financial institutions. We evaluate the evolution and effectiveness of various artificial intelligence approaches, including machine learning algorithms and real-time monitoring systems, while examining their integration with cybersecurity frameworks and data analytics platforms. This analysis provides insights into both theoretical advances and practical implementations of AI-powered financial crime prevention systems, with special attention to regulatory compliance and operational effectiveness.

The traditional approaches to financial crime prevention, primarily based on rule-based systems and manual oversight[2], have proven inadequate in addressing the scale and complexity of modern financial crimes. The global financial sector reports annual losses exceeding $2.1 trillion due to various forms of financial crime[3], highlighting the urgent need for more effective prevention mechanisms. The integration of AI technologies presents a promising solution, offering capabilities that extend far beyond conventional detection methods in both scope and effectiveness.

This review article examines the current state of AI-powered financial crime prevention, analyzing the convergence of artificial intelligence, cybersecurity, and data science in creating comprehensive defense mechanisms. We explore how these technologies work synergistically to enhance the security of banking systems while addressing the challenges of implementation, regulation, and privacy concerns. The review synthesizes findings from recent academic research, industry reports, and practical implementations to provide a comprehensive understanding of current capabilities and limitations.

2. State of Financial Crime Prevention in Banking

2.1. Evolution of Financial Crime Landscape

The digital transformation of banking services has catalyzed a dramatic evolution in financial crime, necessitating a fundamental reassessment of prevention strategies[4]. The interconnected nature of modern financial systems has created new vulnerabilities that criminals increasingly exploit through sophisticated methods. The complexity of these attacks has increased exponentially, with criminals utilizing advanced technologies to orchestrate multi-channel fraud campaigns that traditional detection systems struggle to identify.

Recent studies have shown a significant increase in sophisticated financial attack methodologies, with particular growth in cyber-enabled fraud techniques [5].These attacks increasingly leverage artificial intelligence and machine learning technologies, enabling criminals to adapt their strategies rapidly in response to conventional detection methods [6]. The emergence of real-time payment systems and digital banking platforms has created new attack vectors, with criminals exploiting the speed and complexity of modern financial transactions to conceal their activities [7].

2.2. Traditional Detection Methods and Their Limitations

Contemporary banking systems have historically relied on rule-based detection methods and manual oversight processes for identifying suspicious activities [8]. These traditional approaches operate through predetermined rules and thresholds, analyzing transaction patterns against static criteria to flag potential incidents of financial crime. However, the effectiveness of these conventional methods has diminished significantly in the face of evolving criminal sophistication.

Traditional rule-based systems typically achieve detection rates of only 35% for sophisticated fraud attempts, with false-positive rates often exceeding 95% [9]. This high rate of false positives creates substantial operational burden, requiring significant manual review resources while potentially overlooking genuine criminal activities.

2.3. Regulatory Framework Evolution

The regulatory landscape governing financial crime prevention has undergone significant transformation in response to emerging threats and technological capabilities. International frameworks such as the EU's 6AMLD (Sixth Anti-Money Laundering Directive) and the FATF's updated recommendations have imposed increasingly stringent requirements on financial institutions [10]. These regulations mandate enhanced customer due diligence procedures, real-time transaction monitoring capabilities, and sophisticated risk assessment methodologies.

The implementation of these regulatory requirements has driven substantial changes in banking operations and technology infrastructure. Financial institutions must now maintain comprehensive audit trails of their detection and

prevention activities, demonstrating the effectiveness of their systems to regulatory authorities. This regulatory burden has become a significant driver for the adoption of more sophisticated prevention technologies.

2.4. Emerging Threat Patterns

Contemporary financial crimes exhibit increasing complexity, leveraging advanced technologies and exploiting vulnerabilities in digital banking systems [11]. Synthetic identity fraud has emerged as a particularly challenging threat, growing by 248% since 2020 [12]. These sophisticated schemes combine legitimate and fabricated personal information to create convincing false identities that can withstand traditional verification methods.

Authorized push payment (APP) scams have similarly evolved, increasing by 71% annually [13]. Criminals exploit social engineering techniques and real-time payment systems to manipulate legitimate customers into authorizing fraudulent transactions. The sophistication of these attacks often renders traditional fraud detection systems ineffective, as the transactions are initiated through legitimate customer accounts and authentication methods.

Money laundering schemes have become more sophisticated, utilizing cryptocurrency mixers, cross-border transactions, and layered transaction patterns that traditional monitoring systems struggle to detect [14]. The integration of legitimate business operations with criminal enterprises has created complex networks that require advanced analytics capabilities to identify and investigate effectively.

2.5. Impact on Banking Operations

The evolving threat landscape has fundamentally transformed banking operations across multiple dimensions of financial services delivery. Financial institutions have experienced significant operational restructuring to accommodate enhanced security measures, with an average increase of 34% in operational costs directly attributed to financial crime prevention measures [15]. The integration of advanced security protocols has necessitated substantial modifications to existing banking processes, particularly in areas of customer onboarding, transaction processing, and international fund transfers.

Operational efficiency has been significantly impacted by the need for enhanced due diligence procedures [16]. Banks report an average increase of 42% in customer onboarding time due to sophisticated verification requirements [17]. Furthermore, the complexity of modern financial crimes has led to structural changes within banking organizations, with institutions establishing specialized units dedicated to financial crime prevention.

Customer experience and service delivery have been substantially affected by enhanced security requirements [18]. Banks must now balance robust security measures with customer satisfaction, leading to the development of new service models that incorporate advanced authentication methods while maintaining accessibility and convenience. This operational evolution has catalyzed significant investments in technology infrastructure, with global banks allocating an average of 15% of their technology budgets specifically to financial crime prevention systems.

2.6. Cross-Border Banking Challenges

The international nature of modern banking services presents unique challenges for financial crime prevention. Cross-border transactions introduce additional complexities in monitoring and compliance, requiring coordination between multiple jurisdictional frameworks and regulatory requirements[19]. International banks must navigate varying regulatory standards while maintaining consistent security measures across their global operations.

The complexity of international financial crime prevention is further compounded by differences in technological infrastructure and data sharing capabilities between jurisdictions. Banks must implement sophisticated systems capable of operating effectively across multiple regulatory environments while maintaining compliance with local data protection and privacy requirements.

3. AI and Machine Learning Applications in Financial Crime Prevention

3.1. Advanced Detection Architectures

Modern AI systems employ sophisticated architectures that combine multiple machine learning techniques to create comprehensive detection frameworks. Deep learning models, particularly Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, have demonstrated remarkable success in identifying complex fraud patterns. These advanced architectures analyze temporal transaction patterns, customer behavior sequences, and

contextual information simultaneously, achieving detection rates exceeding 97% accuracy for specific types of financial fraud [20].

The implementation of deep neural networks has revolutionized the approach to pattern recognition in financial transactions. These systems process millions of data points simultaneously, identifying subtle correlations that traditional rule-based systems often miss. Recent studies indicate that deep learning architectures reduce false positive rates by 83% while maintaining high sensitivity to genuine fraudulent activities [21].

3.2. Ensemble Learning Approaches

The integration of multiple AI models through ensemble learning techniques has emerged as a particularly effective approach to financial crime detection. These systems combine various machine learning algorithms, including gradient boosting machines, random forests, and neural networks, to create robust detection frameworks. The implementation of ensemble approaches has demonstrated significant improvements in reducing false-positive rates when compared to single-model implementations, making them a valuable tool in enhancing the accuracy of financial crime detection systems [22].

Contemporary ensemble systems implement sophisticated voting mechanisms that weight individual model outputs based on their historical accuracy in specific fraud scenarios [23]. This adaptive approach enables the system to optimize its detection capabilities across different types of financial crime, demonstrating substantial improvements in detection accuracy when compared to traditional methods.

3.3. Real-time Processing Systems

Modern AI systems have overcome the latency limitations of traditional batch processing approaches through innovative architectures and processing methodologies [24]. These systems analyze transactions in real-time, typically processing decisions within milliseconds while maintaining high accuracy rates. The implementation of parallel processing frameworks enables simultaneous analysis of multiple transaction characteristics, including historical patterns, behavioral biometrics, and network relationships.

Advanced streaming analytics capabilities enable these systems to process millions of transactions per second, identifying potential fraud attempts before transactions are completed. This real-time capability has reduced financial losses from fraudulent activities by an average of 76% in implementing institutions [25].

3.4. Natural Language Processing Applications

The integration of advanced Natural Language Processing (NLP) models has significantly enhanced the capability to detect financial crimes through unstructured data analysis. These systems analyze customer communications, social media interactions, and documentation to identify potential indicators of fraudulent activity. Modern NLP implementations achieve accuracy rates exceeding 89% in identifying suspicious patterns in textual data [26].

3.5. Adaptive Learning Systems

Contemporary AI solutions employ sophisticated adaptive learning mechanisms that enable continuous system improvement through operational experience. These systems automatically adjust their detection parameters based on confirmed fraud cases and false positive outcomes, reducing the need for manual tuning while improving detection accuracy over time. Research indicates that adaptive systems improve their detection rates by approximately 2.5% monthly during their first year of operation [27].

3.6. Model Interpretability and Compliance

The development of explainable AI frameworks has become crucial for regulatory compliance and operational transparency. Modern systems implement various techniques for model interpretation, including SHAP (SHapley Additive exPlanations) values and LIME (Local Interpretable Model-agnostic Explanations), enabling detailed analysis of decision-making processes [28]. These frameworks provide necessary transparency for regulatory compliance while maintaining high detection accuracy.

4. Cybersecurity Integration

4.1. Threat Intelligence Systems

The foundation of modern cybersecurity integration lies in sophisticated threat intelligence systems that provide real-time awareness of emerging threats and attack patterns [29]. These systems aggregate data from multiple sources, including dark web monitoring, behavioral analytics, and global threat feeds, enabling financial institutions to proactively identify and respond to potential threats. Advanced AI algorithms process this intelligence data, creating dynamic risk profiles that adapt to evolving threat landscapes.

Recent advancements in threat intelligence systems have incorporated machine learning models capable of processing unstructured data from diverse sources, including social media, dark web forums, and cryptocurrency transaction networks [30]. These enhanced systems demonstrate significant improvements in early threat detection compared to traditional methods, with the ability to identify emerging attack patterns well before they materialize into actual threats. Financial institutions implementing these advanced threat intelligence frameworks have reported substantial reductions in successful cyber-attacks targeting their systems.

4.2. Security Information and Event Management (SIEM)

Modern SIEM platforms incorporate advanced AI capabilities, enabling the correlation of security events across multiple systems and networks. These implementations process large volumes of security events in real-time, utilizing machine learning algorithms to efficiently identify potential security incidents with high accuracy. The integration with financial crime prevention systems creates a unified defense framework that addresses both cybersecurity and financial crime risks simultaneously [31].

The evolution of SIEM platforms has led to the development of predictive security analytics capabilities that leverage historical data patterns to forecast potential security incidents [32]. These systems employ deep learning models trained on vast datasets of previous security events, achieving an accuracy in predicting emerging security threats.

4.3. Identity and Access Management

IAM systems have evolved to incorporate biometric authentication, behavioral analytics, and zero-trust architectures. Advanced AI algorithms analyze user behavior patterns, detecting anomalies that might indicate compromised credentials or unauthorized access attempts [33]. The implementation of adaptive authentication frameworks has significantly enhanced security and reduced unauthorized access incidents across financial institutions that have deployed these solutions.

Contemporary IAM frameworks have expanded to include continuous authentication mechanisms that monitor user behavior throughout active sessions, rather than relying solely on initial authentication [34]. These systems analyze numerous behavioral parameters in real-time, including keystroke patterns, mouse movements, and transaction behavior, creating unique behavioral profiles for each user. This comprehensive monitoring approach has proven effective in preventing account takeover incidents while maintaining user satisfaction through non-intrusive monitoring methods.

4.4. Blockchain-based Solutions

Blockchain technology has emerged as a powerful tool in enhancing the security and transparency of financial transactions [35]. These systems create immutable transaction records that facilitate audit trails and enhance the ability to detect and prevent fraudulent activities. The integration of smart contracts within blockchain frameworks has revolutionized automated compliance monitoring and enforcement. These self-executing contracts incorporate regulatory requirements and institutional policies, automatically flagging transactions that deviate from established parameters. The implementation of smart contract based compliance systems has demonstrated substantial improvements in both processing efficiency and accuracy of suspicious activity detection [36].

5. Data Science and Analytics Framework

5.1. Big Data Analytics in Crime Detection

Advanced analytics platforms process structured and unstructured data from multiple sources, including transaction records, customer interactions, and external data feeds [37]. These systems employ distributed computing architectures

capable of processing petabytes of data in real-time, enabling the identification of complex fraud patterns that would be impossible to detect through traditional methods.

The implementation of advanced streaming analytics capabilities has transformed the ability to process and analyze financial transactions in real-time [38]. Modern systems utilize parallel processing frameworks that can analyze millions of transactions simultaneously across multiple dimensions, including historical patterns, network relationships, and behavioral indicators. This enhanced processing capability has substantially improved the speed and accuracy of fraudulent transaction detection, enabling near instantaneous analysis while maintaining high accuracy rates [39].

5.2. Predictive Modeling Approaches

Contemporary predictive models incorporate sophisticated machine learning algorithms that forecast potential criminal activities based on historical patterns and emerging trends [40]. These systems utilize attention mechanisms and transformer architectures to analyze temporal sequences of transactions, demonstrating significant capabilities in identifying previously unknown fraud patterns. The implementation of transfer learning techniques has substantially improved the efficiency of training new fraud detection models, enabling faster adaptation to emerging threats.

Recent advances in deep learning architectures have enabled the development of more sophisticated predictive models that can identify complex fraud patterns across multiple channels simultaneously [41]. These systems utilize attention mechanisms and transformer architectures to analyze temporal sequences of transactions, demonstrating significant capabilities in identifying previously unknown fraud patterns. The implementation of transfer learning techniques has substantially improved the efficiency of training new fraud detection models, enabling faster adaptation to emerging threats.[42]

5.3. Network Analysis for Pattern Detection

Network analysis methodologies have proven particularly effective in detecting organized financial crime operations. Advanced graph analytics algorithms process millions of connections simultaneously, identifying subtle patterns that indicate coordinated criminal activities [43].

The evolution of graph neural networks has enhanced the ability to analyze complex financial relationships and identify suspicious patterns of activity [44]. These systems process temporal graph structures that represent evolving relationships between entities, transactions, and behaviors, demonstrating significantly improved detection capabilities compared to traditional rule based systems for complex money laundering schemes [45]. The integration of dynamic graph analysis capabilities enables real time monitoring of transaction networks, identifying potential criminal activities as they emerge.

5.4. Data Privacy and Protection Methods

Modern systems employ advanced encryption techniques, data anonymization, and privacy-preserving machine learning approaches to maintain security while enabling effective analysis. Federated learning techniques allow financial institutions to collaborate in fraud detection while maintaining data privacy, improving overall system effectiveness [46].

The development of homomorphic encryption capabilities has enabled financial institutions to perform complex analytics on encrypted data without compromising sensitive information [47]. These systems demonstrate significantly improved computation efficiency compared to previous privacy preserving methods while maintaining complete data confidentiality. The implementation of differential privacy techniques ensures that individual transaction details remain protected while allowing accurate aggregate analysis for fraud detection purposes..

5.4.1. Challenges and Limitations

The implementation of AI-powered financial crime prevention systems faces several significant challenges. Technical challenges include the complexity of integrating diverse data sources, maintaining system performance at scale, and ensuring real-time processing capabilities. Financial institutions struggle with legacy system integration reporting significant technical barriers to full AI implementation [48]. The rapid evolution of criminal techniques requires continuous system updates and refinement, creating substantial operational overhead.

Implementation barriers extend beyond technical considerations to include organizational and operational challenges. Financial institutions face significant resource constraints in terms of skilled personnel, with a global shortage of

professionals who possess both financial crime expertise and AI implementation experience [49]. The cost of implementation remains prohibitive for smaller institutions, creating potential vulnerabilities in the global financial system.

Privacy and ethical considerations present ongoing challenges in the deployment of AI-powered solutions. The need to balance effective crime detection with customer privacy rights creates complex operational requirements. Regulatory compliance issues continue to evolve, with varying requirements across jurisdictions creating challenges for international financial institutions. The need for model transparency and explainability often conflicts with the complexity of advanced AI algorithms, requiring careful balance between detection effectiveness and regulatory compliance [50].

5.4.2. Future Directions and Opportunities

Emerging technologies present significant opportunities for enhancing financial crime prevention capabilities. Quantum computing applications show promise in processing complex encryption algorithms and detecting sophisticated fraud patterns [51]. Advanced natural language processing models demonstrate potential for improving the analysis of unstructured data in financial crime detection. The integration of edge computing architectures offers possibilities for enhanced real-time processing capabilities while maintaining data privacy [52].

Significant research gaps exist in areas of model interpretability, cross-border cooperation frameworks, and privacy-preserving analytics. Future research should focus on developing more sophisticated approaches to balancing detection effectiveness with privacy protection. The development of standardized evaluation frameworks for AI-powered financial crime prevention systems represents a critical area for future investigation.

Integration opportunities exist in the convergence of various technological approaches. The combination of blockchain technology with AI-powered analytics offers potential for creating more robust and transparent financial systems [53]. Enhanced collaboration between financial institutions, technology providers, and regulatory bodies could lead to more effective global financial crime prevention frameworks.

6. Conclusion

The landscape of financial crime prevention has undergone a fundamental transformation through the integration of artificial intelligence, cybersecurity frameworks, and advanced data science methodologies. This comprehensive review has demonstrated that the synergistic relationship between these technologies has created unprecedented capabilities for detecting and preventing financial crime, while simultaneously raising important considerations about privacy, regulation, and implementation challenges.

The evidence presented throughout this review indicates that AI-powered solutions consistently demonstrate superior detection rates and reduced false positives compared to traditional methods, marking a significant advancement in the field of financial crime prevention. However, the continued evolution of criminal sophistication necessitates ongoing advancement in prevention technologies and methodologies, highlighting the dynamic nature of this critical domain.

Recommendations

Financial institutions should prioritize investment in developing more sophisticated AI models that provide transparent decision-making processes while maintaining high detection accuracy. This involves not only technical advancement but also careful consideration of ethical implications and privacy concerns. The implementation of these systems must be accompanied by robust governance frameworks that ensure responsible use of AI technologies while maintaining stakeholder trust.

The establishment of standardized frameworks for system evaluation and implementation represents a critical step in advancing the field. Financial institutions, technology providers, and regulatory bodies should collaborate to develop common standards for measuring system effectiveness, sharing threat intelligence, and establishing best practices for AI implementation. This standardization would facilitate more effective cross-border cooperation and system integration.

Success in future financial crime prevention depends on fostering greater collaboration between stakeholders and maintaining continuous investment in technological innovation. Financial institutions must balance the need for

effective crime prevention with privacy protection and regulatory compliance, while working closely with regulators to ensure that these systems remain both effective and compliant with evolving regulatory requirements.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Menon S, Guan Siew T. Key challenges in tackling economic and cybercrimes: Creating a multilateral platform for international co-operation. Journal of Money Laundering Control. 2012 Jul 6;15(3):243-56.

[2] Agorbia-Atta C, Atalor I. Enhancing anti-money laundering capabilities: The Strategic Use of AI and Cloud Technologies in Financial Crime Prevention. World Journal of Advanced Research and Reviews. 2024;23(2):2035-47.

[3] NJOROGE EW. *Effect of Cyber Crime Related Costs On Development of Financial Innovation Products and Services* (Doctoral dissertation, JKUAT-COHRED).

[4] Challoumis C. HOW ARTIFICIAL INTELLIGENCE IS RESHAPING FINANCIAL TRANSACTIONS AND INVESTMENTS. BBC. 2024 Oct;3:293.

[5] Gavėnaitė-Sirvydienė J. Development of cyber security assessment tool for financial institutions

[6] Donald A, Iqbal J. Implementing Cyber Defense Strategies: Evolutionary Algorithms, Cyber Forensics, and AI-Driven Solutions for Enhanced Security.

[7] Omolara AE, Jantan A, Abiodun OI, Singh MM, Anbar M, Kemi DV. State-of-the-art in big data application techniques to financial crime: a survey. International Journal of Computer Science and Network Security. 2018 Jul 30;18(7):6-16.

[8] Hassan M, Aziz LA, Andriansyah Y. The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics. 2023 Aug 5;6(1):110-32.

[9] Maruatona O. *Internet banking fraud detection using prudent analysis* (Doctoral dissertation, University of Ballarat).

[10] Ozioko AC. EVOLUTION OF ANTI-MONEY LAUNDERING LAWS: A COMPARATIVE STUDY. Multi-Disciplinary Research and Development Journals Int'l. 2024 Sep 25;6(1):1-27

[11] Babu Nuthalapati S. AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking. Educational Administration: Theory and Practice. 2023;29(1):357-68.

[12] Yu J, Yu Y, Wang X, Lin Y, Yang M, Qiao Y, Wang FY. The Shadow of Fraud: The Emerging Danger of AI-powered Social Engineering and its Possible Cure. arXiv preprint arXiv:2407.15912. 2024 Jul 22.

[13] Montague DA. Essentials of online payment security and fraud prevention. John Wiley & Sons; 2010 Nov 5.

[14] Anika IE. *New technology for old crimes? the role of cryptocurrencies in circumventing the global anti-money laundering regime and facilitating transnational crime* (Doctoral dissertation, University of British Columbia).

[15] Gomber P, Kauffman RJ, Parker C, Weber BW. On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. Journal of management information systems. 2018 Jan 2;35(1):220-65.

[16] LUFT LE. Exploratory analysis: Can blockchain technology improve M&A due diligence processes efficiency.

[17] Shastri R, Khandelwal U. Impact of Digital On-Boarding Quality on Customer Satisfaction: The Moderating Role of Perceived Risk. Journal of Relationship Marketing. 2024 Jun 28:1-32.

[18] Li F, Lu H, Hou M, Cui K, Darbandi M. Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. Technology in Society. 2021 Feb 1;64:101487.

[19] Zhang Y. Developing cross-border blockchain financial transactions under the belt and road initiative. The Chinese Journal of Comparative Law. 2020 Jun 1;8(1):143-76.

[20] 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.

[21] Alarfaj FK, Malik I, Khan HU, Almusallam N, Ramzan M, Ahmed M. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access. 2022 Apr 12;10:39700-15.

[22] Alsumaini AY. *Two-Stage Ensemble Learning for NIDS Multiclass Classification* (Master's thesis, Hamad Bin Khalifa University (Qatar)).]

[23] Chhabra R, Goswami S, Ranjan RK. A voting ensemble machine learning based credit card fraud detection using highly imbalance data. Multimedia Tools and Applications. 2024 May;83(18):54729-53.]

[24] Tadi V. Revolutionizing Data Integration: The Impact of AI and Real-Time Technologies on Modern Data Engineering Efficiency and Effectiveness.]

[25] Vyas B. Java in Action: AI for Fraud Detection and Prevention. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2023 Nov:58-69.

[26] Qatawneh AM. The role of artificial intelligence in auditing and fraud detection in accounting information systems: moderating role of natural language processing. International Journal of Organizational Analysis. 2024 Jul 25.

[27] Banala S. The Future of IT Operations: Harnessing Cloud Automation for Enhanced Efficiency and The Role of Generative AI Operational Excellence. International Journal of Machine Learning and Artificial Intelligence. 2024 Jul 4;5(5):1-5.

[28] Muhammad AJ. Evaluation of Explainable AI Techniques for Interpreting Machine Learning Models.

[29] Sarker IH. AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability. Springer Nature; 2024.

[30] Alturkistani H, Chuprat S. Artificial Intelligence and Large Language Models in Advancing Cyber Threat Intelligence: A Systematic Literature Review. Available at SSRN 4903071.]

[31] Familoni BT, Shoetan PO. Cybersecurity in the financial sector: a comparative analysis of the USA and Nigeria. Computer Science & IT Research Journal. 2024 Apr 17;5(4):850-77.

[32] Shelke P, Hämäläinen T. Analysing Multidimensional Strategies for Cyber Threat Detection in Security Monitoring. InProceedings of the European Conference on Cyber Warfare and Security 2024 (Vol. 23, No. 1). Academic Conferences International Ltd.

[33] Alzaabi FR, Mehmood A. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access. 2024 Feb 26;12:30907-27.

[34] Gudala L, Reddy AK, Sadhu AK, Venkataramanan S. Leveraging Biometric Authentication and Blockchain Technology for Enhanced Security in Identity and Access Management Systems. Journal of Artificial Intelligence Research. 2022 Sep 21;2(2):21-50.].

[35] Odeyemi O, Okoye CC, Ofodile OC, Adeoye OB, Addy WA, Ajayi-Nifise AO. Integrating AI with blockchain for enhanced financial services security. Finance & Accounting Research Journal. 2024 Mar 15;6(3):271-87.

[36] Zheng Z, Xie S, Dai HN, Chen W, Chen X, Weng J, Imran M. An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems. 2020 Apr 1;105:475-91.

[37] Heger DO. Big data analytics—'Where to go from here'. International Journal of Developments in Big Data and Analytics. 2014;1(1):42-58.

[38] [Javaid HA. The Future of Financial Services: Integrating AI for Smarter, More Efficient Operations. MZ Journal of Artificial Intelligence. 2024 Aug 11;1(2).]

[39] Shoetan PO, Familoni BT. Transforming fintech fraud detection with advanced artificial intelligence algorithms. Finance & Accounting Research Journal. 2024 Apr 17;6(4):602-25.

[40] Safat W, Asghar S, Gillani SA. Empirical analysis for crime prediction and forecasting using machine learning and deep learning techniques. IEEE access. 2021 May 6;9:70080-94.

[41] Sharma R, Mehta K, Sharma P. Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention. InRisks and Challenges of AI-Driven Finance: Bias, Ethics, and Security 2024 (pp. 90-120). IGI Global.

[42] Lebichot B, Le Borgne YA, He-Guelton L, Oblé F, Bontempi G. Deep-learning domain adaptation techniques for credit cards fraud detection. InRecent Advances in Big Data and Deep Learning: Proceedings of the INNS Big Data and Deep Learning Conference INNSBDDL2019, held at Sestri Levante, Genova, Italy 16-18 April 2019 2020 (pp. 78-88). Springer International Publishing.

[43] Needham M, Hodler AE. A comprehensive guide to graph algorithms in neo4j. Neo4j. com. 2018.

[44] Ma X, Wu J, Xue S, Yang J, Zhou C, Sheng QZ, Xiong H, Akoglu L. A comprehensive survey on graph anomaly detection with deep learning. IEEE Transactions on Knowledge and Data Engineering. 2021 Oct 8;35(12):12012-38

[45] Lute S. *What If we Cannot See the Full Picture? Anti-Money Laundering in Transaction Monitoring* (Doctoral dissertation, Vrije Universiteit Amsterdam).

[46] Lakhan A, Mohammed MA, Nedoma J, Martinek R, Tiwari P, Vidyarthi A, Alkhayyat A, Wang W. Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. IEEE journal of biomedical and health informatics. 2022 Apr 8;27(2):664-72.

[47] Haryaman A, Amrita ND, Redjeki F. SECURE AND INCLUSIVE UTILIZATION OF SHARED DATA POTENTIAL WITH MULTI-KEY HOMOMORPHIC ENCRYPTION IN BANKING INDUSTRY. Journal of Economics, Accounting, Business, Management, Engineering and Society. 2024 Aug 3;1(9):1-3.

[48] Rane N, Choudhary SP, Rane J. Acceptance of artificial intelligence technologies in business management, finance, and e-commerce: factors, challenges, and strategies. Studies in Economics and Business Relations. 2024 Sep 7;5(2):23-44.

[49] Kayode-Ajala O. Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. Applied Research in Artificial Intelligence and Cloud Computing. 2023 Aug 4;6(8):1-21.

[50] Vegesna VV. Privacy-Preserving Techniques in AI-Powered Cyber Security: Challenges and Opportunities. International Journal of Machine Learning for Sustainable Development. 2023 Dec 5;5(4):1-8.

[51] Belghachi M. A Comprehensive Survey on Quantum Machine Learning Algorithms for Fraud Detection in Financial Sectors. Available at SSRN 4792054. 2024 Apr 11.

[52] Nain G, Pattanaik KK, Sharma GK. Towards edge computing in intelligent manufacturing: Past, present and future. Journal of Manufacturing Systems. 2022 Jan 1;62:588-611.

[53] Jhansi MV. MEDIATING EFFECT OF ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN TECHNOLOGY IN FINANCE: OPPORTUNITIES AND CHALLENGES