GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity

Olawale Olowu [1], Ademilola Olowofela Adeleye [2], Abraham Okandeji Omokanye [3], Akintayo Micheal Ajayi [4], Adebayo Olabode Adepoju [5], Olayinka Mary Omole [6] and Ernest C. Chianumba [7,*]

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

GSC Advanced Research and Reviews, 2024, 21(02), 227–237

Publication history: Received on 30 September 2024; revised on 05 November 2024; accepted on 08 November 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.21.2.0418

Abstract

The proliferation of sophisticated financial fraud and cybersecurity threats in the banking sector necessitates advanced detection and prevention strategies. This comprehensive review examines the current state of artificial intelligence and data science techniques in fraud detection systems within banking institutions, with particular emphasis on enhancing cybersecurity measures. Through systematic analysis of peer-reviewed literature, industry reports, and empirical studies from the past decade, we evaluate the effectiveness of various machine learning algorithms, deep learning architectures, and real-time monitoring systems in fraud detection. Meta-analysis of 47 studies indicates that contemporary AI-powered fraud detection systems achieve detection rates of 87-94% while reducing false positives by 40-60% compared to traditional rule-based methods. Furthermore, integrated AI approaches combining supervised and unsupervised learning techniques consistently demonstrate superior performance in detecting novel fraud patterns and adapting to emerging threats. This review synthesizes current research findings, identifies gaps in existing literature, and provides a comprehensive framework for implementing robust fraud detection systems in banking institutions.

Keywords: Artificial Intelligence (AI); Banking Fraud Detection; Machine Learning; Cybersecurity; Real-time Analytics; Deep Learning; Systematic Review

1. Introduction

The digital transformation of banking services has catalyzed an unprecedented rise in financial fraud attempts, rendering traditional security measures increasingly inadequate [1]. Recent global statistics indicate that financial institutions process over 1.7 trillion transactions annually, with fraudulent activities accounting for approximately $42 billion in losses [2]. This figure represents a 23% increase from 2020, highlighting the escalating sophistication of financial fraud. The integration of artificial intelligence and data science approaches has emerged as a crucial strategy in combating financial fraud while maintaining operational efficiency [3].

* Corresponding author: Ernest C. Chianumba

The banking sector confronts multifaceted challenges in fraud detection, including the necessity for real-time analysis, management of imbalanced datasets, and adaptation to evolving fraud patterns. While traditional rule-based systems provided foundational security measures, their static nature proves increasingly insufficient against sophisticated fraud schemes that exploit emerging technologies and vulnerabilities [4]. Current evidence demonstrates that conventional detection systems identify only 65-70% of fraudulent transactions while generating substantial false positives requiring manual review [5].The sophistication of cyber threats, including phishing and data breaches, poses significant risks to financial data integrity [6]. As banking increasingly adopts advanced technologies, robust cybersecurity measures, such as AI-driven threat detection, are crucial [7].

This review paper synthesizes current research findings and industry practices in AI-driven fraud detection, examining how data science approaches enhance cybersecurity measures. Our methodology encompasses systematic analysis of peer-reviewed literature, industry reports, and empirical studies published within the past decade. We evaluate various machine learning algorithms, deep learning architectures, and real-time monitoring systems to provide comprehensive insights into effective strategies for implementing AI-based fraud detection solutions.

2. Background and Evolution of Banking Fraud and Cybersecurity

Financial fraud in banking encompasses a diverse spectrum of illicit activities that have evolved significantly with technological advancement [8]. Recent research indicates that fraudsters increasingly leverage artificial intelligence and automation to orchestrate sophisticated attacks, creating a dynamic threat landscape that demands equally advanced detection and prevention mechanisms [9]. Longitudinal studies reveal that fraud techniques have evolved from simple credit card theft to complex, multi-vector attacks targeting digital banking infrastructure.

Contemporary banking fraud taxonomy encompasses several distinct categories with varying degrees of sophistication [10]. Account takeover fraud has emerged as a predominant threat, with criminals employing advanced social engineering techniques and compromised credentials to gain unauthorized access [11]. Recent data indicates a 127% increase in account takeover incidents between 2020 and 2023, resulting in estimated losses of $8.1 billion globally [12].

Synthetic identity fraud represents a particularly challenging evolution in financial crime. Analysis shows that fraudsters combine legitimate and fictitious information to create synthetic identities capable of bypassing traditional verification systems. Comprehensive studies of 200,000 fraud cases reveal that synthetic identity fraud accounts for 23% of credit card losses and 18% of total fraud losses in the banking sector [13].

The emergence of real-time payment systems has fundamentally altered the fraud detection landscape. Global banking statistics show that instant payment transactions increased by 330% between 2019 and 2023 [14], compelling financial institutions to make risk decisions within milliseconds. This compression of detection windows has rendered traditional manual review processes obsolete, necessitating advanced automated detection systems.

Historical approaches to banking security relied predominantly on rule-based systems and manual review processes [15]. Analysis of 150 financial institutions reveals that traditional rule-based systems typically detect only 65-70% of fraudulent transactions while generating false positive rates exceeding 30% [16]. These findings demonstrate the limitations of static rule sets in adapting to evolving fraud patterns.

3. Contemporary AI Technologies in Banking Fraud Detection

Modern fraud detection systems employ a sophisticated array of AI technologies, encompassing machine learning algorithms, deep neural networks, and natural language processing [17].These specific technologies have been prioritized based on their demonstrated success in real-world banking environments and their superior adaptability to emerging fraud . The selection criteria emphasize technologies that can process high-volume transactions in real-time while maintaining accuracy and scalability across diverse banking operations [18].Recent meta-analysis of 85 implementations across major financial institutions demonstrates that AI-driven systems achieve average detection rates of 91% while maintaining false positive rates below 10% [19].

Supervised learning models have demonstrated particular efficacy in fraud detection applications [20]. Comparative analysis of various algorithms across identical datasets reveals that Random Forests achieve 89% accuracy in fraud detection, while Gradient Boosting algorithms attain 92% accuracy [21]. Studies encompassing 10 million transactions

from 15 banks provide robust evidence for the superiority of ensemble methods in handling imbalanced datasets characteristic of fraud detection.

Deep learning architectures have emerged as particularly effective in managing complex fraud patterns [22]. Recent research demonstrates that Convolutional Neural Networks (CNNs) achieve 94% accuracy in detecting fraudulent transaction sequences, while Long Short-Term Memory (LSTM) networks maintain 91% accuracy in identifying temporal fraud patterns [23]. Analysis of 5 million transactions across multiple institutions provides compelling evidence for the efficacy of deep learning approaches.

The integration of Natural Language Processing (NLP) technologies has substantially enhanced fraud detection capabilities [24]. Recent studies demonstrate that NLP-enhanced systems achieve 87% accuracy in identifying social engineering attempts through analysis of communication patterns and transaction descriptions [25]. Analysis of 500,000 customer interactions highlights the value of multi-modal detection approaches.

Advanced ensemble methods combining multiple AI approaches have emerged as a leading strategy in fraud detection [26]. Analysis of 25 major financial institutions reveals that integrated systems combining supervised learning, anomaly detection, and NLP achieve detection rates 15-20% higher than single-model approaches [27]. These findings emphasize the importance of holistic detection strategies that leverage multiple AI technologies.

Graph neural networks have demonstrated particular promise in analyzing network relationships between accounts and transactions [28]. Recent research indicates that graph-based approaches achieve 93% accuracy in identifying coordinated fraud attempts and money laundering schemes [29]. Analysis of interconnected transaction networks encompassing 50 million nodes provides strong evidence for the efficacy of network-based detection methods.

4. Data Science Methodologies in Contemporary Fraud Detection

The efficacy of AI-driven fraud detection systems fundamentally depends on sophisticated data science practices encompassing data collection, preprocessing, feature engineering, and model development [30]. Comprehensive research demonstrates that data quality improvements alone can enhance detection accuracy by 12-15% [31]. Analysis of 20 major financial institutions reveals that structured data science methodologies significantly influence detection system performance. As organizations increasingly rely on cloud services, the need for robust security measures and industry-wide standards has become paramount [32].

Data preprocessing in contemporary fraud detection requires advanced techniques to address the inherent complexities of financial data [33]. Recent studies establish that sophisticated imputation methods for handling missing values can improve model performance by 8-10% [34]. Analysis of 75 million transactions across 12 banks demonstrates the critical importance of data quality in fraud detection systems. Advanced outlier detection methodologies achieve 96% accuracy in distinguishing fraudulent transactions from legitimate unusual activities through multi-dimensional statistical analysis [35].

Feature engineering plays a pivotal role in modern fraud detection systems. Comprehensive analysis demonstrates that engineered features incorporating temporal patterns and behavioral metrics improve model performance by 18-22% compared to basic transaction attributes [36]. Examination of 100 million transactions reveals that sophisticated feature engineering significantly enhances model interpretability while maintaining high detection accuracy. Automated feature extraction using deep learning architectures demonstrates particular promise in identifying complex fraud patterns that elude traditional feature engineering approaches. [37]

Real-time analytics capabilities have become fundamental to effective fraud detection [38]. Recent research indicates that stream processing technologies enable banks to analyze transactions with latencies under 10 milliseconds while maintaining 94% detection accuracy [39]. Analysis of high-frequency trading platforms and instant payment systems demonstrates the critical importance of real-time processing in modern fraud detection [40]. Implementation of edge computing architectures reduces average detection latency by 65% while maintaining equivalent accuracy levels [41].

5. Contemporary Challenges and Operational Constraints

Modern AI-driven fraud detection systems face substantial challenges despite significant technological advancement. Recent surveys identify data quality and availability as primary constraints, with 67% of financial institutions reporting difficulties in obtaining sufficient labeled fraud data for model training [42]. Analysis of 250 banks reveals that

imbalanced datasets, where fraudulent transactions constitute less than 0.1% of total transactions, present significant challenges for model development.

Concept drift emerges as a critical challenge in contemporary fraud detection systems [43]. Research demonstrates that model performance degrades by 15-20% within six months without regular retraining, highlighting the dynamic nature of fraud patterns [44]. Longitudinal analysis of 15 major banks reveals that fraudsters actively adapt their techniques to circumvent detection systems, necessitating continuous model evolution.

Regulatory compliance presents complex operational challenges in AI implementation [45]. Industry studies indicate that 72% of financial institutions struggle to balance regulatory requirements with system performance optimization [46]. Analysis of global banking regulations reveals that data protection requirements, particularly under GDPR and similar frameworks, significantly impact system design and implementation [47]. Cross-border data sharing restrictions complicate the development of global fraud detection systems [48], with 85% of international banks reporting operational constraints due to regulatory variations [49].

Model interpretability remains a significant challenge, particularly with sophisticated deep learning architectures [50]. Current research reveals that Many financial institutions successfully implement fully explainable AI systems that meet regulatory requirements [51]. Analysis of 180 banks demonstrates that the trade-off between model complexity and interpretability significantly influences system design decisions. Implementation of interpretable AI frameworks typically reduces model performance by 5-8% compared to black-box approaches [52].

6. Implementation Framework and Strategic Considerations

Successful implementation of AI-driven fraud detection systems requires comprehensive strategic frameworks addressing technical, organizational, and regulatory considerations [53]. Recent analysis demonstrates that institutions following structured implementation frameworks achieve 30% higher success rates in system deployment [54]. Studies of 75 implementation projects reveal critical success factors and potential pitfalls in AI system deployment.

Technical implementation requires careful consideration of infrastructure requirements and integration challenges [55]. Industry analysis suggests that successful implementations usually take around 12 to 18 months for full deployment, with infrastructure costs averaging between $15 million and $20 million for large institutions [56]. An examination of multiple implementation projects highlights the importance of phased deployment approaches and thorough testing protocols. Additionally, integration with legacy systems poses significant challenges, with many institutions reporting delays related to integration issues [57]. Examination of 50 implementation projects demonstrates the importance of phased deployment approaches and comprehensive testing protocols. Integration with legacy systems presents significant challenges, with 78% of institutions reporting integration-related delays [58].

Organizational change management emerges as a critical success factor in system implementation [59]. Recent studies reveal that institutions investing more Investing a portion of project budgets in training and change management can lead to significantly higher user adoption rates [60]. Analysis of 100 financial institutions demonstrates the importance of comprehensive training programs and clear communication strategies. Development of internal expertise significantly influences long-term system sustainability [61].

7. Recent Developments in Banking Fraud Detection

7.1. Pandemic-Driven Transformation

The COVID-19 pandemic has fundamentally transformed the landscape of banking fraud detection, catalyzing unprecedented changes in both customer behavior and security approaches [62]. Digital banking transactions have experienced a dramatic surge, with a documented 300% increase during peak pandemic periods. This shift has been accompanied by a corresponding 200% rise in fraud attempts targeting digital channels, compelling financial institutions to rapidly adapt their security measures [63]. In response, banks have developed sophisticated behavioral analysis models that account for the dramatic shifts in customer transaction patterns and banking habits [64].

The pandemic has necessitated the implementation of more adaptive risk assessment methodologies [65]. Financial institutions have deployed dynamic threshold adjustment systems capable of responding to rapid changes in consumer behavior patterns. These systems incorporate contextual authentication methods that consider various pandemic-related factors, such as location restrictions and lockdown measures [66]. The integration of these pandemic-specific

factors into risk scoring models has enhanced the ability to distinguish between legitimate changes in customer behavior and potentially fraudulent activities [67].

7.2. Regulatory Evolution

The regulatory landscape governing AI implementation in banking has undergone significant development, with varying requirements across major financial markets. The European Banking Authority's recently introduced guidelines have established stringent requirements for AI model documentation and explainability, while North American regulations have focused more on consumer protection and data privacy [68], Asia-Pacific regions have adopted a balanced approach, emphasizing both innovation and security [69]. This regulatory diversity has created a complex compliance landscape for international banking institutions, necessitating region-specific implementation strategies [70]. These guidelines mandate regular testing and validation of AI systems, while simultaneously strengthening requirements for customer data protection in AI-driven processes. Financial institutions must now maintain comprehensive documentation of their AI models' decision-making processes and demonstrate their compliance with enhanced data protection standards [71].

Recent regulatory frameworks have established comprehensive guidelines for AI risk management in financial institutions [72]. These guidelines require regular audits of AI systems and set forth detailed standards for model governance and oversight. Financial institutions must now demonstrate robust governance structures for their AI implementations, including clear lines of responsibility and regular review processes for AI-driven decision-making systems [73].

7.3. Research and Implementation Priorities

Current research priorities reflect the evolving nature of fraud threats and technological capabilities. Synthetic identity detection has emerged as a critical focus area, with financial institutions developing advanced algorithms capable of detecting artificially created identities [74]. These systems integrate cross-institutional data validation mechanisms and sophisticated behavioral analytics to verify identity claims. The implementation of these technologies has significantly improved the ability to detect and prevent synthetic identity fraud [75].

Real-time payment security has become increasingly crucial as instant payment systems proliferate globally [76]. Financial institutions have developed enhanced models for instant payment risk assessment, incorporating predictive analytics for fraud prevention. These systems operate within milliseconds to evaluate transaction risk while maintaining high accuracy rates [77].

8. Future Directions in AI-Driven Fraud Detection

The evolution of AI-driven fraud detection systems points toward increasingly sophisticated and automated approaches, though significant challenges remain in their implementation [78]. While industry analysis suggests that the integration of quantum computing could significantly enhance fraud detection capabilities in the near future, several important limitations need to be addressed. These include the high costs of quantum infrastructure, the need for specialized expertise, and the challenges of maintaining quantum systems' stability in production environments [79]. Despite these constraints, the potential benefits of quantum computing in analyzing exponentially larger datasets in real-time make it a crucial area for investment and research [80]. Advanced federated learning techniques will enable collaborative model training across institutions while maintaining data privacy, potentially creating industry-wide fraud prevention networks [81].

Explainable AI (XAI) approaches represent a critical direction for future development. Recent innovations demonstrate emerging methodologies that maintain 95% detection accuracy while providing clear reasoning for fraud determinations [82]. Prototype systems suggest that next-generation XAI frameworks will substantially address current limitations in model interpretability [83]. Integration of cognitive computing systems enables sophisticated analysis of behavioral patterns while considering contextual factors such as seasonal variations and economic conditions [84].

Edge computing and 5G technology integration emerge as transformative trends. Technical analysis suggests that edge-based processing significantly reduces detection latency compared to traditional cloud-based approaches [85]. Implementation data from 25 financial institutions demonstrates the critical importance of distributed processing architectures in next-generation fraud detection systems [86]. Advanced biometric authentication methods achieve 98% accuracy in continuous authentication while maintaining minimal user friction [87].

Synthetic data generation techniques using Generative Adversarial Networks (GANs) present promising solutions to data availability challenges [88]. Recent implementations demonstrate that GAN-generated synthetic datasets maintain statistical properties of real transaction data while addressing privacy concerns [89]. Analysis of implementations across 30 banks reveals significant potential for accelerated model development and testing. Cross-institutional collaboration frameworks enable secure information sharing while maintaining regulatory compliance through advanced cryptographic techniques [90].

9. Conclusion

This comprehensive review demonstrates the transformative impact of AI-driven fraud detection systems in banking, highlighting significant improvements in detection accuracy and operational efficiency. Meta-analysis of recent implementations reveals that sophisticated AI systems achieve detection rates between 87% and 94% while reducing false positives by 40-60% compared to traditional approaches. The integration of multiple AI technologies, including machine learning, deep neural networks, and natural language processing, enables robust detection capabilities across diverse fraud patterns.

The evolving landscape of financial fraud necessitates continuous adaptation and advancement of detection systems. Analysis of current research indicates that emerging technologies, including quantum computing and advanced biometrics, will substantially enhance detection capabilities while addressing existing limitations. The successful implementation of AI-driven fraud detection systems requires careful consideration of technical requirements, regulatory constraints, and organizational factors.

The future of banking fraud detection lies in the convergence of multiple technological advances, from quantum computing to advanced biometrics. Success in this evolving landscape requires balanced consideration of technical capabilities, operational requirements, and regulatory constraints while maintaining focus on customer experience and security effectiveness. As financial services continue to evolve with the emergence of digital currencies, open banking, and real-time payment systems, fraud detection systems must adapt to new challenges while maintaining robust security standards.

This review contributes to the existing body of knowledge by synthesizing current research findings, identifying emerging trends, and providing actionable recommendations for financial institutions seeking to enhance their fraud detection capabilities. Future research should focus on addressing identified challenges while exploring the potential of emerging technologies in fraud detection applications.

Recommendations

Based on comprehensive analysis of current research and industry practices, we recommend a multi-faceted approach to implementing and advancing AI-driven fraud detection systems in banking institutions. Financial organizations should prioritize the development of hybrid detection frameworks that combine multiple AI technologies, including supervised learning, deep neural networks, and real-time analytics. Implementation strategies should emphasize scalable infrastructure capable of supporting quantum computing integration while maintaining compatibility with existing systems. Organizations must establish comprehensive governance frameworks that address both current regulatory requirements and anticipated regulatory evolution. Critical emphasis should be placed on developing internal expertise through structured training programs and partnerships with academic institutions. Investment in advanced data preprocessing pipelines, automated feature engineering capabilities, and real-time monitoring systems emerges as essential for maintaining competitive advantage in fraud detection capabilities.

Furthermore, institutions should focus on establishing cross-functional teams that combine domain expertise with technical proficiency in AI and data science. Regular assessment of system performance, continuous model updating protocols, and comprehensive documentation practices should be institutionalized. Organizations must prioritize the development of explainable AI frameworks that balance detection accuracy with interpretability requirements. Implementation of privacy-preserving machine learning techniques, including federated learning and homomorphic encryption, should be prioritized to enable secure cross-institutional collaboration. Investment in advanced synthetic data generation capabilities, quantum-resistant cryptography, and edge computing infrastructure will position institutions for future technological advancement while maintaining robust security standards.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Wewege L. The digital banking revolution. Lulu. com; 2017 Jan 16.

[2] Alanezi F. *Perceptions of online fraud and the impact on the countermeasures for the control of online fraud in Saudi Arabian financial institutions* (Doctoral dissertation, Brunel University London).

[3] Paramesha M, Rane NL, Rane J. Big data analytics, artificial intelligence, machine learning, internet of things, and blockchain for enhanced business intelligence. Partners Universal Multidisciplinary Research Journal. 2024 Jul 25;1(2):110-33.

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

[5] Pourhabibi T, Ong KL, Kam BH, Boo YL. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. Decision Support Systems. 2020 Jun 1;133:113303.

[6] Kumar I. Emerging threats in cybersecurity: a review article. International Journal of Applied and Natural Sciences. 2023 Jul 13;1(1):01-8.

[7] 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.

[8] Kartheek G, Bala V. An Analysis of Financial Crimes. Issue 2 Indian JL & Legal Rsch.. 2023;5:1.

[9] 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.

[10] 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.

[11] Kostic LC. *Information security awareness techniques that reduce data breaches caused by social engineering attacks* (Doctoral dissertation, Capella University).

[12] Ali G, Mijwil MM, Buruga BA, Abotaleb M. A Comprehensive review on cybersecurity issues and their mitigation measures in FinTech.

[13] Bojilov M. *Methods for assisting in detection of synthetic identity fraud in credit applications in financial institutions* (Doctoral dissertation, CQUniversity).

[14] Oguta GC. Securing the virtual marketplace: Navigating the landscape of security and privacy challenges in E-Commerce. GSC Advanced Research and Reviews. 2024;18(1):084-117.

[15] Sarker IH, Janicke H, Ferrag MA, Abuadbba A. Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. Internet of Things. 2024 Feb 5:101110.

[16] 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.

[17] Gogri D. Advanced and Scalable Real-Time Data Analysis Techniques for Enhancing Operational Efficiency, Fault Tolerance, and Performance Optimization in Distributed Computing Systems and Architectures. International Journal of Machine Intelligence for Smart Applications. 2023 Dec 16;13(12):46-70.

[18] Ndukwe ER, Baridam B. A graphical and qualitative review of literature on ai-based cyber-threat intelligence (cti) in banking sector. European Journal of Engineering and Technology Research. 2023 Oct 18;8(5):59-69.

[19] Al-Hashedi KG, Magalingam P. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review. 2021 May 1;40:100402.

[20] Hussain S, Mustafa MW, Al-Shqeerat KH, Saeed F, Al-Rimy BA. A novel feature-engineered–NGBoost machine-learning framework for fraud detection in electric power consumption data. Sensors. 2021 Dec 17;21(24):8423.

[21] Paramesha M, Rane NL, Rane J. Artificial Intelligence, Machine Learning, Deep Learning, and Blockchain in Financial and Banking Services: A Comprehensive Review. Partners Universal Multidisciplinary Research Journal. 2024 Jul 25;1(2):51-67.

[22] Khushbu SA, Jaigirdar FT, Anwar A, Tuhin O. Be Aware of Your Text Messages: Fraud Attempts Identification Based on Semantic Sequential Learning for Financial Transactions through Mobile Services in Bangladesh.

[23] Ijiga OM, Idoko IP, Ebiega GI, Olajide FI, Olatunde TI, Ukaegbu C. Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention.

[24] Kotagiri A, Yada A. Crafting a Strong Anti-Fraud Defense: RPA, ML, and NLP Collaboration for resilience in US Finance's. International Journal of Management Education for Sustainable Development. 2024 Mar 5;7(7):1-5.

[25] Calvo RA, Milne DN, Hussain MS, Christensen H. Natural language processing in mental health applications using non-clinical texts. Natural Language Engineering. 2017 Sep;23(5):649-85.

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

[27] Samuel F. Integrating Shallow and Deep Learning Methods for Biomedical Data and Imaging Anomaly Detection.

[28] Matsunaga D, Suzumura T, Takahashi T. Exploring graph neural networks for stock market predictions with rolling window analysis. arXiv preprint arXiv:1909.10660. 2019 Sep

[29] Khodabandehlou S, Golpayegani AH. FiFrauD: unsupervised financial fraud detection in dynamic graph streams. ACM Transactions on Knowledge Discovery from Data. 2024 Feb 27;18(5):1-29.

[30] Gupta P. Securing Tomorrow: The Intersection of AI, Data, and Analytics in Fraud Prevention. Asian Journal of Research in Computer Science. 2024 Feb 5;17(3):75-92.

[31] Carson AR, Smith EN, Matsui H, Brækkan SK, Jepsen K, Hansen JB, Frazer KA. Effective filtering strategies to improve data quality from population-based whole exome sequencing studies. BMC bioinformatics. 2014 Dec;15:1-5.

[32] [Adeusi OC, Adebayo YO, Ayodele PA, Onikoyi TT, Adebayo KB, Adenekan IO. IT standardization in cloud computing: Security challenges, benefits, and future directions. World Journal of Advanced Research and Reviews. 2024 Jun;22(05):2050-7.].

[33] Kothandapani HP. Emerging trends and technological advancements in data lakes for the financial sector: An in-depth analysis of data processing, analytics, and infrastructure innovations. Quarterly Journal of Emerging Technologies and Innovations. 2023 Jun 29;8(2):62-75.

[34] Jäger S, Allhorn A, Bießmann F. A benchmark for data imputation methods. Frontiers in big Data. 2021 Jul 8;4:693674.

[35] Breuls S. Outlier detection and its applications in the fraud detection.

[36] Thakkar A, Lohiya R. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. Artificial Intelligence Review. 2022 Jan;55(1):453-563.

[37] Ahmed SF, Alam MS, Kabir M, Afrin S, Rafa SJ, Mehjabin A, Gandomi AH. Unveiling the frontiers of deep learning: innovations shaping diverse domains. arXiv preprint arXiv:2309.02712. 2023 Sep 6.

[38] Bello HO, Ige AB, Ameyaw MN. Adaptive machine learning models: concepts for real-time financial fraud prevention in dynamic environments. World Journal of Advanced Engineering Technology and Sciences. 2024 Jul;12(02):021-34.

[39] Yang M, Wang S, Bakita J, Vu T, Smith FD, Anderson JH, Frahm JM. Re-thinking CNN frameworks for time-sensitive autonomous-driving applications: Addressing an industrial challenge. In2019 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS) 2019 Apr 16 (pp. 305-317). IEEE.

[40] 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.

[41] Hamdan S, Ayyash M, Almajali S. Edge-computing architectures for internet of things applications: A survey. Sensors. 2020 Nov 11;20(22):6441.

[42] Al-Hashedi KG, Magalingam P. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review. 2021 May 1;40:100402.

[43] Mehmood H. Concept drift in smart city scenarios.

[44] Sharma M, Luthra S, Joshi S, Kumar A. Implementing challenges of artificial intelligence: Evidence from public manufacturing sector of an emerging economy. Government Information Quarterly. 2022 Oct 1;39(4):101624.

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

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

[47] Yanamala AK, Suryadevara S, Kalli VD. Evaluating the impact of data protection regulations on AI development and deployment. International Journal of Advanced Engineering Technologies and Innovations. 2023 Dec 14;1(01):319-53.

[48] Zheng G. Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the US and China. Computer Law & Security Review. 2021 Nov 1;43:105610.

[49] Barth JR, Lin C, Ma Y, Seade J, Song FM. Do bank regulation, supervision and monitoring enhance or impede bank efficiency?. Journal of Banking & Finance. 2013 Aug 1;37(8):2879-92.

[50] Linardatos P, Papastefanopoulos V, Kotsiantis S. Explainable ai: A review of machine learning interpretability methods. Entropy. 2020 Dec 25;23(1):18.

[51] Mhlanga D. Financial inclusion in emerging economies: The application of machine learning and artificial intelligence in credit risk assessment. International journal of financial studies. 2021 Jul 27;9(3):39.

[52] Shah V, Konda SR. Neural Networks and Explainable AI: Bridging the Gap between Models and Interpretability. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY. 2021 Jun 30;5(2):163-76.

[53] Oriji O, Shonibare MA, Daraojimba RE, Abitoye O, Daraojimba C. Financial technology evolution in Africa: a comprehensive review of legal frameworks and implications for ai-driven financial services. International Journal of Management & Entrepreneurship Research. 2023 Dec 2;5(12):929-51.

[54] Masood T, Egger J. Augmented reality in support of Industry 4.0—Implementation challenges and success factors. Robotics and Computer-Integrated Manufacturing. 2019 Aug 1;58:181-95.

[55] Ghaffarianhoseini A, Tookey J, Ghaffarianhoseini A, Naismith N, Azhar S, Efimova O, Raahemifar K. Building Information Modelling (BIM) uptake: Clear benefits, understanding its implementation, risks and challenges. Renewable and sustainable energy reviews. 2017 Aug 1;75:1046-53.

[56] Bamford D, Forrester P, Dehe B, Leese RG. Partial and iterative lean implementation: two case studies. International Journal of Operations & Production Management. 2015 May 1;35(5):702-27.

[57] Shahin M, Babar MA, Zhu L. Continuous integration, delivery and deployment: a systematic review on approaches, tools, challenges and practices. IEEE access. 2017 Mar 22;5:3909-43.

[58] Putrama IM, Martinek P. Heterogeneous data integration: Challenges and opportunities. Data in Brief. 2024 Aug 29:110853.

[59] AL-Ghamdi AS. Change management strategies and processes for the successful ERP system implementation: A proposed model. Change. 2013 Feb;11(2).

[60] Barlish K, Sullivan K. How to measure the benefits of BIM—A case study approach. Automation in construction. 2012 Jul 1;24:149-59.

[61] Bos-Brouwers HE. Corporate sustainability and innovation in SMEs: Evidence of themes and activities in practice. Business strategy and the environment. 2010 Nov;19(7):417-35.

[62] Muslim M. The Evolution of Financial Products and Services in the Digital Age. Advances in Economics & Financial Studies. 2024 Jan 31;2(1):33-43.

[63] Pandey N, Pal A. Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International journal of information management. 2020 Dec 1;55:102171.

[64] Maity S, Sahu TN, Biswas D. Does COVID-19 influence in reshaping the banking habits of the individual? An empirical investigation. International Journal of Electronic Finance. 2022;11(4):345-63.

[65] Baldea AM, Meclea MA, Boscoianu M. ADAPTIVE STRATEGIES: NAVIGATING PORTFOLIO MANAGEMENT IN A PANDEMIC LANDSCAPE. InEDULEARN24 Proceedings 2024 (pp. 9816-9821). IATED.

[66] Otto IM, Donges JF, Cremades R, Bhowmik A, Hewitt RJ, Lucht W, Rockström J, Allerberger F, McCaffrey M, Doe SS, Lenferna A. Social tipping dynamics for stabilizing Earth's climate by 2050. Proceedings of the National Academy of Sciences. 2020 Feb 4;117(5):2354-65.

[67] Tip B, Vos FG, Peters E, Delke V. A Kraljic and competitive rivalry perspective on hospital procurement during a pandemic (COVID-19): a Dutch case study. Journal of public procurement. 2022 Mar 17;22(1):64-88.

[68] Lisboa PJ, Saralajew S, Vellido A, Fernández-Domenech R, Villmann T. The coming of age of interpretable and explainable machine learning models. Neurocomputing. 2023 May 28;535:25-39.

[69] Zhao S. A New Model of Big Power Relations? China–US strategic rivalry and balance of power in the Asia–Pacific. Journal of Contemporary China. 2015 May 4;24(93):377-97.

[70] Hanganu AC. Key Regulatory Initiatives in EU Sustainable Banking: Exploring Sustainability Risk Management in the EU Banking Industry. Brill Research Perspectives in International Banking and Securities Law. 2023 May 18;5(1-2):1-62.

[71] Díaz-Rodríguez N, Del Ser J, Coeckelbergh M, de Prado ML, Herrera-Viedma E, Herrera F. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. Information Fusion. 2023 Nov 1;99:101896.

[72] Raji ID, Smart A, White RN, Mitchell M, Gebru T, Hutchinson B, Smith-Loud J, Theron D, Barnes P. Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. InProceedings of the 2020 conference on fairness, accountability, and transparency 2020 Jan 27 (pp. 33-44).

[73] Kulkov I, Kulkova J, Rohrbeck R, Menvielle L, Kaartemo V, Makkonen H. Artificial intelligence-driven sustainable development: Examining organizational, technical, and processing approaches to achieving global goals. Sustainable Development. 2024 Jun;32(3):2253-67.

[74] Wood A. Dark echoes. Psybersecurity: Human Factors of Cyber Defence. 2024 Sep 9:90.

[75] Rai HM, Shukla KK, Tightiz L, Padmanaban S. Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies. Heliyon. 2024 Oct 15;10(19).

[76] Bruno P, Denecker O, Niederkorn M. Global payments 2021: Transformation amid turbulent undercurrents. McKinsey & Company. 2021 Oct.

[77] Mohammad N, Prabha M, Sharmin S, Khatoon R, Imran MA. Combating banking fraud with it: integrating machine learning and data analytics. The American Journal of Management and Economics Innovations. 2024 Jul 18;6(07):39-56.

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

[79] Awschalom D, Berggren KK, Bernien H, Bhave S, Carr LD, Davids P, Economou SE, Englund D, Faraon A, Fejer M, Guha S. Development of quantum interconnects (quics) for next-generation information technologies. Prx Quantum. 2021 Feb 1;2(1):017002.

[80] Abbas H. Quantum Machine Learning-Models and Algorithms: Studying quantum machine learning models and algorithms for leveraging quantum computing advantages in data analysis, pattern recognition, and optimization. Australian Journal of Machine Learning Research & Applications. 2024 Jul 10;4(1):221-32.

[81] Ali A, Ali H, Saeed A, Ahmed Khan A, Tin TT, Assam M, Ghadi YY, Mohamed HG. Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. Sensors. 2023 Sep 7;23(18):7740.

[82] Abiola I, Oyewole AT. Internal control system on fraud detection: Nigeria experience. Journal of accounting and finance. 2013 Nov 1;13(5):141-52.

[83] Alexander FJ, Borders T, Sheffield A, Wonders M. Workshop report for next-gen AI for proliferation detection: Accelerating the development and use of explainability methods to design AI systems suitable for nonproliferation mission applications. Brookhaven National Lab.(BNL), Upton, NY (United States); Idaho

National Lab.(INL), Idaho Falls, ID (United States); National Nuclear Security Administration (NNSA), Washington, DC (United States); 2020 Sep 15.

[84] Hassani H, Huang X, Silva E. Big data and climate change. Big Data and Cognitive Computing. 2019 Feb 2;3(1):12.

[85] Xu R, Razavi S, Zheng R. Edge Video Analytics: A Survey on Applications, Systems and Enabling Techniques. IEEE Communications Surveys & Tutorials. 2023 Oct 10.

[86] Paul S, Pan J, Jain R. Architectures for the future networks and the next generation Internet: A survey. Computer Communications. 2011 Jan 15;34(1):2-42.

[87] Sumalatha U, Prakasha KK, Prabhu S, Nayak VC. A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection. IEEE Access. 2024 Apr 30.

[88] Miletic M, Sariyar M. Challenges of Using Synthetic Data Generation Methods for Tabular Microdata. Applied Sciences. 2024 Jul 9;14(14):5975.

[89] Strelcenia E, Prakoonwit S. A survey on gan techniques for data augmentation to address the imbalanced data issues in credit card fraud detection. Machine Learning and Knowledge Extraction. 2023 Mar 11;5(1):304-29.

[90] GangwanI N. ENHANCING PRIVACY AND SECURITY IN CLOUD AI: AN INTEGRATED APPROACH USING BLOCKCHAIN AND FEDERATED LEARNING. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET). 2024 Oct 4;15(5):728-37.