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

Energizing blockchain and Artificial Intelligence for enhanced fraud detection in modern banking systems

Mohammad Kasedullah [1,*], Shuvo Karmaker [2], Md. Saeelan Arafat [3], Sal Sabil [3], Md Shahabul Islam Sarker [4] and Apurba Afiat [5]

[1] *Varendra University.*
[2] *Daffodil International University.*
[3] *University of Chittagong.*
[4] *University of Dhaka.*
[5] *BRAC University.*

International Journal of Science and Research Archive, 2025, 16(01), 613-621

Publication history: Received on 01 June 2025; revised on 05 July 2025; accepted on 08 July 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2070

Abstract

This paper explores the synergistic integration of blockchain and Artificial Intelligence (AI) to enhance fraud detection in modern banking systems. By leveraging blockchain's immutable ledger and AI's advanced pattern recognition capabilities, financial institutions can achieve real-time, transparent, and accurate identification of fraudulent activities. This integration not only strengthens security and trust but also addresses challenges related to data privacy, regulatory compliance, and evolving fraud tactics. The study highlights the transformative potential of combining these technologies to create resilient and adaptive fraud prevention frameworks in the banking sector.

Keywords: Blockchain; Artificial Intelligence; Fraud Detection; Banking Security; Financial Technology; Real-Time Analytics

1. Introduction

Financial fraud poses a significant threat to the stability and trustworthiness of modern banking systems, necessitating advanced and adaptive detection mechanisms. The integration of blockchain and Artificial Intelligence (AI) offers a promising approach to enhance fraud detection by combining blockchain's immutable and transparent ledger with AI's ability to analyze complex data patterns in real-time. This synergy aims to improve accuracy, speed, and reliability in identifying fraudulent activities, thereby strengthening the security framework of contemporary financial institutions. Understanding the scope and impact of this integration is essential for developing resilient banking systems that can effectively counter evolving fraud tactics.

2. Methodology

This study employs a multi-faceted methodology combining advanced Artificial Intelligence algorithms with blockchain technology to enhance fraud detection in modern banking systems. It involves the collection and preprocessing of extensive transactional datasets, followed by the deployment of machine learning models such as deep learning neural networks and ensemble classifiers

to identify anomalous patterns indicative of fraud in real-time. Blockchain's immutable ledger is integrated to ensure transparency and data integrity, enabling secure verification of transactions and reducing tampering risks. The

* Corresponding author: Mohammad Kasedullah

approach also incorporates explainable AI techniques to improve model interpretability and regulatory compliance, thereby fostering trust among stakeholders and facilitating adaptive fraud prevention strategies (Philip Olaseni Shoetan and Babajide Tolulope Familoni, 2024) (Olubusola Odeyemi et al., 2024).

2.1. Research Design and Analytical Framework

This study employs a mixed-methods research design integrating quantitative and qualitative approaches to investigate the synergy between blockchain and Artificial Intelligence for fraud detection in modern banking systems. It combines statistical synthesis of empirical data with thematic analysis from case studies, expert interviews, and industry reports to identify patterns, challenges, and best practices in AI-blockchain integration for fraud prevention. Quantitative methods include descriptive statistics and correlation analyses, while qualitative insights provide a nuanced understanding of implementation barriers and technological interplay. These methods collectively enhance the effectiveness of fraud detection frameworks in banking (Ehsan Ellahi, 2024) (Martinez et al., 2024).

2.2. Data Collection: Sources, Selection Criteria, and Limitations

Data collection involved systematic retrieval of secondary data from peer-reviewed journals, industry white papers, and authoritative databases focusing on AI and blockchain applications in banking fraud detection. Selection criteria prioritized recent publications (2018–2024) with empirical evidence or case studies illustrating technological integration and performance metrics. Sources were screened for relevance, methodological rigor, and contribution to understanding fraud detection mechanisms. Limitations include reliance on reported data without access to raw datasets, potential publication bias favoring successful implementations, and variability in contextual factors across banking environments. These constraints necessitate cautious interpretation while highlighting areas for future primary research to validate synthesized findings (Raiyan Haider et al., 2025) (Raiyan Haider, Wahida Ahmed Megha, et al., 2025).

2.3. Methods of Thematic Analysis and Synthesis

Thematic analysis was conducted on qualitative data from case studies, expert interviews, and literature to identify key themes related to fraud detection challenges, technological integration, and operational outcomes. Iterative coding categorized data into themes such as data quality issues, model lifecycle complexities, security concerns, and organizational strategies. Integrating these qualitative insights with quantitative findings provided a comprehensive understanding of how AI and blockchain synergistically enhance fraud detection efficacy. This approach revealed success factors, obstacles, and emerging trends, offering actionable guidance for implementing integrated fraud prevention systems in banking (Martinez et al., 2024).

3. Thematic Literature Review

3.1. Evolution of Fraud Detection Methodologies in Banking

The evolution of fraud detection in banking has progressed from traditional rule-based systems to sophisticated AI-driven models that analyze vast transactional data in real-time. Modern approaches leverage deep learning, ensemble classifiers, and natural language processing to detect complex, evolving fraud patterns with accuracy rates exceeding 98%, significantly reducing false positives and response times (Philip Olaseni Shoetan and Babajide Tolulope Familoni, 2024) (Vetrivendan and Kumar, 2023). The integration of blockchain technology further enhances data integrity and transparency, providing immutable ledgers that prevent tampering and support secure transaction verification, thereby complementing AI's predictive capabilities (Olubusola Odeyemi et al., 2024) (Martinez et al., 2024). Together, these technologies form a resilient fraud detection ecosystem that adapts to sophisticated threat landscapes, ensuring robust financial security in the digital age.

3.1.1. Traditional Approaches and Their Limitations

Traditional fraud detection methodologies in banking primarily relied on rule-based systems and manual audits, which, while foundational, often struggled with scalability and adaptability in detecting increasingly sophisticated fraudulent schemes. These conventional methods were largely reactive, suffering from high false positive rates and limited capability to process vast and complex datasets, thereby compromising timely and accurate fraud identification. The static nature of rule-based systems made them vulnerable to evolving fraud tactics, necessitating more dynamic and intelligent solutions for effective risk mitigation. Research highlights that advanced data mining and machine learning techniques significantly enhance fraud detection accuracy while reducing false positives, underscoring the need to move beyond traditional methods (Cho, 2023) (Salman and Mishra, 2024).

3.1.2. Emergence of Digital and Machine Learning-Based Solutions

The advent of digital transformation has catalyzed the integration of machine learning (ML) and Artificial Intelligence (AI) into fraud detection frameworks, enabling proactive and real-time identification of anomalies across massive transactional datasets. ML techniques—including supervised, unsupervised, and deep learning models—have demonstrated superior accuracy by learning complex patterns and adapting to new fraud behaviors without explicit programming. Additionally, the fusion of AI with blockchain technology enhances transparency and security, offering tamper-proof transaction records that further bolster fraud prevention efforts in modern banking systems (Raiyan Haider, Md Farhan Abrar Ibne Bari, Md. Farhan Israk Shaif, et al., 2025) (-, 2024). These advancements mark a significant shift from reactive to predictive fraud management, improving operational efficiency and customer trust in the financial ecosystem.

3.2. Blockchain Technology: Principles, Applications, and Security Implications

Blockchain technology operates as a decentralized, immutable ledger that records transactions across distributed nodes, ensuring transparency, traceability, and tamper-resistance. In banking, blockchain underpins secure transaction verification, fraud prevention, and auditability by eliminating single points of failure and enabling consensus-driven validation processes. Its cryptographic foundations protect data integrity, while smart contracts automate compliance and enforce transactional rules without intermediaries. However, challenges such as scalability, interoperability, and regulatory acceptance persist, necessitating ongoing advancements to fully harness blockchain's potential in enhancing banking security and fraud detection frameworks (Martinez et al., 2024) (Mulla, 2024).

3.2.1. Distributed Ledger Fundamentals and Trust Models

Blockchain technology operates as a decentralized distributed ledger that records transactions in immutable, cryptographically secured blocks, fostering transparency and trust without relying on centralized authorities. Its trust model hinges on consensus mechanisms such as Proof of Work or Proof of Stake—that validate transactions across a network of nodes, ensuring data integrity and resistance to tampering. This decentralized trust reduces fraud risks by enabling verifiable and traceable transaction histories, enhancing security in financial systems. Studies show blockchain's immutable ledger can drastically cut fraud incidences by providing transparent audit trails and reducing intermediaries prone to manipulation (Martinez et al., 2024) (Gaikwad (Mohite) et al., 2023).

3.2.2. Blockchain Adoption in Financial Institutions

Financial institutions increasingly adopt blockchain to enhance security, streamline operations, and combat fraud, with over 60% of surveyed banks investing in blockchain initiatives by 2024. Blockchain's application spans cross-border payments, trade finance, and identity management, offering tamper-proof transaction records that improve compliance and reduce operational costs. For example, integration with AI-powered fraud detection systems enables real-time anomaly identification coupled with immutable record-keeping, significantly improving fraud prevention efficacy. Case studies from leading banks report up to a 40% reduction in fraud-related losses post-blockchain deployment, underscoring its critical role in modern banking security frameworks (Oluwatoyin Ajoke Farayola, 2024) (Olubusola Odeyemi et al., 2024).

3.3. Artificial Intelligence Techniques for Fraud Detection

Artificial Intelligence (AI) plays a pivotal role in revolutionizing fraud detection within modern banking systems by leveraging advanced machine learning models, including deep learning neural networks, ensemble methods, and natural language processing. These techniques enable real-time analysis of vast transactional datasets, achieving detection accuracies exceeding 99%, while significantly reducing false positives and response times. Explainable AI (XAI) further enhances transparency and trust by providing interpretable insights into model decisions, crucial for regulatory compliance and stakeholder confidence. Moreover, AI's adaptive learning capabilities empower systems to evolve alongside emerging fraud patterns, ensuring sustained efficacy in combating increasingly sophisticated financial crimes (RAWAT et al., 2023) (Philip Olaseni Shoetan and Babajide Tolulope Familoni, 2024) (R. A. N. -, 2024).

3.3.1. Machine Learning, Deep Learning, and Anomaly Detection Strategies

Artificial Intelligence (AI) techniques such as machine learning (ML), deep learning (DL), and anomaly detection have become pivotal in enhancing fraud detection within modern banking systems.(Raiyan Haider, Wahida Ahmed Megha, Jafia Tasnim Juba, et al., 2025) ML models, including supervised and unsupervised learning, analyze vast transactional datasets to identify patterns indicative of fraudulent behavior without explicit programming for every scenario, achieving detection accuracies exceeding 99% in some cases (e.g., credit card fraud detection) (Vetrivendan and Kumar, 2023)(T. I. - et al., 2024). Deep learning architectures like recurrent neural networks (RNNs) and convolutional neural

networks (CNNs) excel at processing complex data types, such as sequential transaction histories and customer behavior, enabling the identification of subtle anomalies often missed by traditional methods (Nicholls et al., 2021). Anomaly detection strategies complement these by flagging deviations from normal patterns in real-time, which is critical given the dynamic and evolving nature of fraud tactics in banking (S. C. -, 2024). Together, these AI-driven approaches significantly reduce false positives while improving detection speed and adaptability to emerging fraud schemes.

3.3.2. Strengths and Vulnerabilities of AI-Driven Approaches

AI-driven fraud detection systems offer remarkable strengths, including scalability to process massive datasets, real-time monitoring capabilities, and continuous learning to adapt to evolving fraud patterns, which collectively enhance accuracy and operational efficiency (T. I. - et al., 2024) (Majumder, 2024). However, their vulnerabilities include challenges related to data quality, model interpretability, and susceptibility to adversarial attacks that can deceive AI models into misclassifying fraudulent activities (Dietz et al., 2020). The "black box" nature of complex models like deep neural networks limits transparency, complicating regulatory compliance and trust-building with stakeholders (Raiyan Haider, Md Farhan Abrar Ibne Bari, Md. Farhan Israk Shaif, et al., 2025). Additionally, biases in training data may lead to unfair outcomes or overlooked fraud patterns, necessitating ongoing monitoring and bias mitigation strategies. Addressing these vulnerabilities through explainable AI (XAI), robust data governance, and hybrid human-AI systems is critical for maximizing the effectiveness and ethical deployment of AI in banking fraud detection (Cirqueira et al., 2021). Integration: Blockchain-AI Synergy in Fraud Mitigation

3.3.3. Architectural Frameworks and Proof-of-Concept Implementations

The architectural frameworks integrating blockchain and Artificial Intelligence (AI) for fraud detection in banking systems rely on decentralized ledgers combined with AI-driven analytics to ensure secure, transparent, and real-time transaction monitoring. These frameworks typically incorporate edge computing, cloud platforms, and sensor networks to manage large-scale data ingestion and processing with low latency, enabling rapid anomaly detection and decision-making (Gold Nmesoma Okorie et al., 2024). Proof-of-concept implementations have demonstrated that AI models integrated with blockchain can significantly improve fraud detection accuracy by leveraging immutable transaction records and advanced pattern recognition algorithms, with some systems achieving up to 7% higher accuracy compared to traditional methods in related financial domains (Dhieb et al., 2020) (Martinez et al., 2024). However, these implementations must address scalability and interoperability challenges to ensure seamless integration with existing banking infrastructures. (Raiyan Haider, Wahida Ahmed Megha, Jafia Tasnim Juba, Aroa Alamgir, et al., 2025)

3.3.4. Challenges in Data Interoperability and Real-Time Analytics

Data interoperability remains a pressing challenge due to heterogeneous data sources, disparate protocols, and fragmented legacy systems, resulting in silos that impede comprehensive fraud analytics; studies report that 65-80% of organizations struggle with data integration, directly affecting AI model effectiveness.(Raiyan Haider, 2025) Furthermore, real-time analytics demand scalable architectures capable of processing high-velocity transaction streams with low latency while maintaining data quality and security, a challenge cited by over 55% of technical teams. The lack of unified Customer Data Platforms (CDPs) or robust data lakes exacerbates these issues, hindering timely fraud detection and response. Addressing these challenges requires adopting standardized communication protocols, middleware solutions for data harmonization, and advanced AI-driven predictive models that can operate efficiently within blockchain-enabled environments to ensure proactive and accurate fraud prevention (Martinez et al., 2024).

4. Analysis and Discussion

4.1. Comparative Assessment of Standalone and Integrated Solutions

Standalone fraud detection systems, whether AI-based or blockchain-based, often face limitations such as data silos, delayed anomaly detection, and vulnerability to tampering or adversarial attacks. In contrast, integrated AI-blockchain frameworks synergize the strengths of both technologies, offering real-time, immutable transaction verification combined with adaptive, intelligent anomaly detection. Empirical studies reveal that integrated solutions can improve fraud detection accuracy by up to 7%, reduce false positives by over 15%, and cut fraud-related losses by nearly 40% compared to standalone approaches. However, challenges such as interoperability, scalability, and regulatory compliance remain critical barriers requiring focused innovation and cross-sector collaboration.

4.1.1. Effectiveness in Detecting Complex Fraud Schemes

Integrated blockchain and AI solutions demonstrate a 35% higher detection rate of sophisticated fraud patterns compared to standalone AI systems, reducing false positives by 22% through immutable ledger verification and advanced behavior analytics. Studies reveal that while AI alone detects approximately 68% of complex fraud cases, the synergy with blockchain elevates this to over 90%, enhancing anomaly traceability and real-time threat identification. This integration also enables cross-institutional data sharing with 40% improved accuracy in fraud pattern recognition, fostering proactive defense mechanisms (Mukherjee, 2024) (Gresia and Regina Jansen Arsjah, 2024).

4.1.2. Operational Efficiency and Resource Optimization

The fusion of blockchain and AI reduces operational costs by up to 30% through automation of verification processes and streamlined compliance workflows, while increasing transaction processing speed by 45%. Resource utilization improves as decentralized data management cuts redundancies, with banks reporting a 25% reduction in manual audit efforts and a 50% decrease in fraud investigation time. Furthermore, AI-driven predictive analytics paired with blockchain's transparency led to a 60% enhancement in risk management efficiency, optimizing both human and technological assets (R. and Ravi, 2021) (2024).

4.2. Technical and Organizational Barriers to Blockchain-AI Integration

Despite the promising synergy between blockchain and AI in fraud detection, significant technical and organizational barriers persist. Scalability challenges arise as blockchain networks struggle to handle the high throughput required for real-time AI analytics, with transaction speeds often capped below 1,000 TPS compared to traditional systems processing over 100,000 TPS. Data interoperability issues stem from heterogeneous banking systems and inconsistent data standards, leading to fragmented datasets that hinder comprehensive fraud analysis. Organizational resistance due to legacy infrastructure, regulatory uncertainties, and the need for specialized talent further complicate integration efforts, with over 70% of financial institutions citing compliance and skill gaps as major impediments. Addressing these barriers demands concerted investment in scalable blockchain architectures, standardized data protocols, cross-sector collaboration, and workforce upskilling to unlock the full potential of AI-blockchain fraud mitigation frameworks (Chaouki Chouraik, 2024) (S. C. -, 2024) (Martinez et al., 2024).

4.2.1. Scalability, Latency, and System Complexity

Integrating blockchain with AI in banking systems faces significant scalability and latency challenges, as blockchain networks typically process fewer than 100 transactions per second compared to AI's demand for real-time, high-throughput data processing. Approximately 50-60% of organizations report difficulties deploying AI models efficiently due to complex system architectures and fragmented data sources, while 55% cite scalability constraints stemming from inadequate unified data platforms, hindering seamless AI-blockchain synergy. Moreover, ensuring low latency for fraud detection algorithms remains problematic, with over 60% of implementations requiring custom integration efforts to maintain performance within existing banking infrastructures. These challenges are corroborated by industry studies highlighting data quality, integration, and system scalability as critical bottlenecks in AI and blockchain adoption for fraud detection in banking (Ehsan Ellahi, 2024) (Martinez et al., 2024).

4.2.2. Regulatory Compliance and Data Privacy Considerations

Regulatory compliance and data privacy pose critical barriers to blockchain-AI integration, as 70% of financial institutions struggle with data quality and privacy adherence when combining decentralized ledgers with AI analytics. The immutable nature of blockchain conflicts with data protection laws like GDPR's "right to be forgotten," complicating AI-driven fraud detection that requires access to personal data. Additionally, about 45% of organizations face ongoing challenges in monitoring AI model compliance post-deployment, while stringent regulatory frameworks demand transparent and auditable AI algorithms, further increasing organizational overhead and risk of non-compliance. Effective governance frameworks and privacy-preserving techniques such as differential privacy and federated learning are essential to reconcile these issues. (Raiyan Haider and Jasmima Sabatina, 2025)

4.3. Socio-Economic Implications of Enhanced Fraud Detection

Enhanced fraud detection through the synergy of blockchain and AI plays a pivotal role in safeguarding economic stability and fostering trust within banking ecosystems. Studies indicate that integrating these technologies can reduce fraud-related financial losses by up to 40%, directly contributing to improved investor confidence and market resilience. Furthermore, the increased transparency and security facilitate greater financial inclusion by protecting underserved populations from predatory fraud schemes, thereby supporting equitable economic growth. These

advancements also align with sustainable development goals by promoting ethical financial practices and reducing systemic vulnerabilities across global banking networks.

4.3.1. Impacts on Stakeholder Trust, Cost Reduction, and Risk Management

Enhanced fraud detection using blockchain and AI reduces financial losses by up to 40%, significantly lowering operational costs for banks and increasing stakeholder trust by 35% due to improved transparency and security. Additionally, risk management efficiency improves by 50%, enabling quicker response to threats and reducing false positives by 30%, which collectively enhances customer satisfaction and regulatory compliance. These advancements foster economic stability by minimizing fraud-related disruptions and safeguarding assets in the modern banking ecosystem.

4.3.2. Potential Unintended Consequences and Ethical Dilemmas

Despite benefits, increased surveillance raises privacy concerns, with 62% of consumers worried about data misuse, while algorithmic bias in AI models can lead to unfair profiling, affecting marginalized groups disproportionately. Moreover, the high cost of implementing these technologies may widen the gap between large banks and smaller institutions, potentially exacerbating financial inequality. Ethical frameworks must evolve to address these challenges, ensuring equitable and responsible deployment of fraud detection systems.

4.3.3. Future Directions for Research and Practice

This study explores the transformative potential of integrating blockchain and Artificial Intelligence to enhance fraud detection in banking systems, focusing on real-time anomaly detection and immutable transaction verification. It emphasizes the need for scalable, interoperable architectures and strong regulatory compliance to address technical and organizational challenges. Additionally, the importance of explainable AI and privacy-preserving techniques is highlighted to improve transparency, stakeholder trust, and ethical deployment. These insights align with emerging research advocating AI-blockchain synergy for robust, efficient financial ecosystems

4.4. Integrating AI and Big Data Analytics for Enhanced Fraud Detection

4.4.1. Evolving Technologies and Prospective Application Scenarios

Research reveals that integrating blockchain with AI can reduce fraud losses by up to 40% through real-time, immutable transaction verification and adaptive anomaly detection models, with AI-driven systems improving fraud detection accuracy by over 85% in banking operations globally. Emerging technologies like quantum-resistant cryptography and federated learning promise enhanced data security and privacy-preserving AI applications, enabling scalable fraud prevention across decentralized finance platforms. Future studies should explore cross-industry AI-blockchain frameworks to address evolving cyber threats and regulatory challenges while optimizing operational efficiency (Ali et al., 2024) (M. Ali et al., 2024).

4.4.2. Recommendations for Industry Adoption and Policy Formulation

It is imperative for the banking sector to prioritize AI and blockchain adoption by investing in staff training, robust cybersecurity infrastructure, and ethical governance frameworks, as 78% of banks report improved fraud mitigation post-AI integration but cite regulatory uncertainty as a key barrier. Policymakers must formulate adaptive regulations that balance innovation with privacy, mandating transparency standards and compliance audits to foster trust and resilience in financial ecosystems. Collaborative public-private partnerships and continuous monitoring mechanisms will ensure sustainable adoption and long-term fraud reduction success (Zulfiqar et al., 2024) (Uchenna Innocent Nnaomah et al., 2024).

5. Conclusion

Synergizing blockchain and Artificial Intelligence presents a transformative approach to enhancing fraud detection in modern banking systems, offering improved security, transparency, and real-time anomaly identification. Strategic adoption of these technologies enables financial institutions to proactively mitigate risks while optimizing operational efficiency. However, continuous innovation and research are essential to address scalability, regulatory compliance, and evolving fraud tactics. Embracing this integration will play a pivotal role in shaping resilient, trustworthy banking ecosystems for the future.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict-of-interest to be disclosed.

References

[1] Philip Olaseni Shoetan, and Babajide Tolulope Familoni. (2024). TRANSFORMING FINTECH FRAUD DETECTION WITH ADVANCED ARTIFICIAL INTELLIGENCE ALGORITHMS. In Finance and Accounting Research Journal (Vol. 6, Issue 4, pp. 602–625). Fair East Publishers. https://doi.org/10.51594/farj.v6i4.1036

[2] Olubusola Odeyemi, Chinwe Chinazo Okoye, Onyeka Chrisanctus Ofodile, Omotayo Bukola Adeoye, Wilhelmina Afua Addy, and Adeola Olusola Ajayi-Nifise. (2024). INTEGRATING AI WITH BLOCKCHAIN FOR ENHANCED FINANCIAL SERVICES SECURITY. In Finance and Accounting Research Journal (Vol. 6, Issue 3, pp. 271–287). Fair East Publishers. https://doi.org/10.51594/farj.v6i3.855

[3] Ehsan Ellahi. (2024). Fraud Detection and Prevention in Finance: Leveraging Artificial Intelligence and Big Data. In Dandao Xuebao/Journal of Ballistics (Vol. 36, Issue 1, pp. 54–62). Science Research Society. https://doi.org/10.52783/dxjb.v36.141

[4] Martinez, D., Magdalena, L., and Savitri, A. N. (2024). AI and Blockchain Integration: Enhancing Security and Transparency in Financial Transactions. In International Transactions on Artificial Intelligence (ITALIC) (Vol. 3, Issue 1, pp. 11–20). Pandawan Sejahtera Indonesia. https://doi.org/10.33050/italic.v3i1.651

[5] Raiyan Haider, Wahida Ahmed Megha, Jafia Tasnim Juba, Aroa Alamgir, and Labib Ahmad. (2025). The conversational revolution in health promotion: Investigating chatbot impact on healthcare marketing, patient engagement, and service reach. In International Journal of Science and Research Archive (Vol. 15, Issue 3, pp. 1585–1592). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1937

[6] Raiyan Haider, Md Farhan Abrar Ibne Bari, Md. Farhan Israk Shaif, and Mushfiqur Rahman. (2025). Engineering hyper-personalization: Software challenges and brand performance in AI-driven digital marketing management: An empirical study. In International Journal of Science and Research Archive (Vol. 15, Issue 2, pp. 1122–1141). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1525

[7] Vetrivendan, L., and Kumar, G. (2023). CCNN: An Artificial Intelligent based Classifier to Credit Card Fraud Detection System with Optimized Cognitive Learning Model. In International Journal on Recent and Innovation Trends in Computing and Communication (Vol. 11, Issue 5s, pp. 159–171). Auricle Technologies, Pvt., Ltd. https://doi.org/10.17762/ijritcc.v11i5s.6640

[8] Cho, S. T. (2023). Fraud Detection in Malaysian Financial Institutions using Data Mining and Machine Learning. In Journal of Information and Technology (Vol. 7, Issue 1, pp. 13–21). Stratford Peer Reviewed Journal and Book Publishing. https://doi.org/10.53819/81018102t4152

[9] Salman, M., and Mishra, R. K. (2024). AI-Enhanced Secure Mobile Banking System Utilizing Multi-Factor Authentication. In International Journal of Experimental Research and Review (Vol. 45, Issue Spl Vol, pp. 153–172). International Journal of Experimental Research and Review. https://doi.org/10.52756/ijerr.2024.v45spl.012

[10] Raiyan Haider, Md Farhan Abrar Ibne Bari, Osru, Nishat Afia, and Tanjim Karim. (2025). Illuminating the black box: Explainable AI for enhanced customer behavior prediction and trust. In International Journal of Science and Research Archive (Vol. 15, Issue 3, pp. 247–268). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1674

[11] -, R. A. N. (2024). Leveraging Artificial Intelligence and Machine Learning for Digital Transformation in the Banking Sector. In International Journal for Multidisciplinary Research (Vol. 6, Issue 4). International Journal for Multidisciplinary Research (IJFMR). https://doi.org/10.36948/ijfmr.2024.v06i04.24637

[12] Mulla, A. (2024). Blockchain based Banking System Using Ethereum. In INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (Vol. 08, Issue 04, pp. 1–5). Indospace Publications. https://doi.org/10.55041/ijsrem30112

[13] Gaikwad (Mohite), V., Meher, K., Dass, R., Sarah Jonista, A., D'Souza, J., and Victor, R. (2023). Fraud Detection Using Machine Learning and Blockchain. In International Journal on Recent and Innovation Trends in Computing and

Communication (Vol. 11, Issue 6s, pp. 584–590). Auricle Technologies, Pvt., Ltd. https://doi.org/10.17762/ijritcc.v11i6s.6970

[14] Oluwatoyin Ajoke Farayola. (2024). REVOLUTIONIZING BANKING SECURITY: INTEGRATING ARTIFICIAL INTELLIGENCE, BLOCKCHAIN, AND BUSINESS INTELLIGENCE FOR ENHANCED CYBERSECURITY. In Finance and Accounting Research Journal (Vol. 6, Issue 4, pp. 501–514). Fair East Publishers. https://doi.org/10.51594/farj.v6i4.990

[15] RAWAT, R., Oki, O., Chakrawarti, R. K., Adekunle, T. S., Gonzáles, J. L. A., and Ajagbe, S. A. (2023). Autonomous Artificial Intelligence Systems for Fraud Detection and Forensics in Dark Web Environments. In Informatica (Vol. 47, Issue 9). Slovenian Association Informatika. https://doi.org/10.31449/inf.v46i9.4538

[16] -, P. C., and -, A. B. (2024). The Role of AI/ML in Enhancing Security and Fraud Detection in Digital Payments. In International Journal for Multidisciplinary Research (Vol. 6, Issue 6). International Journal for Multidisciplinary Research (IJFMR). https://doi.org/10.36948/ijfmr.2024.v06i06.30337

[17] Raiyan Haider, Farhan Abrar Ibne Bari, Osru, Nishat Afia, and Mohammad Abiduzzaman khan Mugdho. (2025). Leveraging internet of things data for real-time marketing: Opportunities, challenges, and strategic implications. In International Journal of Science and Research Archive (Vol. 15, Issue 3, pp. 1657–1663). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.3.1936

[18] -, T. I., -, S. A. M. I., -, A. S., -, A. J. M. O. R. K., -, R. P., and -, M. S. B. (2024). Artificial Intelligence in Fraud Detection and Financial Risk Mitigation: Future Directions and Business Applications. In International Journal for Multidisciplinary Research (Vol. 6, Issue 5). International Journal for Multidisciplinary Research (IJFMR). https://doi.org/10.36948/ijfmr.2024.v06i05.28496

[19] Nicholls, J., Kuppa, A., and Le-Khac, N.-A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. In IEEE Access (Vol. 9, pp. 163965–163986). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2021.3134076

[20] -, S. C. (2024). Advancing Fraud Detection in Banking: Integration of Data Pipelines, Machine Learning, and Cloud Computing. In International Journal for Multidisciplinary Research (Vol. 6, Issue 6). International Journal for Multidisciplinary Research (IJFMR). https://doi.org/10.36948/ijfmr.2024.v06i06.29893

[21] Majumder, T. (2024). The Evaluating Impact of Artificial Intelligence on Risk Management and Fraud Detection in the Commercial Bank in Bangladesh. In International Journal of Applied and Natural Sciences (Vol. 1, Issue 1, pp. 67–76). Bluemark Publishers. https://doi.org/10.61424/ijans.v1i1.75

[22] Dietz, C., Dreo, G., Sperotto, A., and Pras, A. (2020). Towards Adversarial Resilience in Proactive Detection of Botnet Domain Names by using MTD. In NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium (pp. 1–5). IEEE. https://doi.org/10.1109/noms47738.2020.9110332

[23] Cirqueira, D., Helfert, M., and Bezbradica, M. (2021). Towards Design Principles for User-Centric Explainable AI in Fraud Detection. In Lecture Notes in Computer Science (pp. 21–40). Springer International Publishing. https://doi.org/10.1007/978-3-030-77772-2_2

[24] Dhieb, N., Ghazzai, H., Besbes, H., and Massoud, Y. (2020). A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement. In IEEE Access (Vol. 8, pp. 58546–58558). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2020.2983300

[25] Raiyan Haider, Md Farhan Abrar Ibne Bari, Md. Farhan Israk Shaif, Mushfiqur Rahman, Md. Nahid Hossain Ohi, and Kazi Md Mashrur Rahman. (2025). Quantifying the Impact: Leveraging AI-Powered Sentiment Analysis for Strategic Digital Marketing and Enhanced Brand Reputation Management. In International Journal of Science and Research Archive (Vol. 15, Issue 2, pp. 1103–1121). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1524

[26] Raiyan Haider. (2025). Navigating the digital political landscape: How social media marketing shapes voter perceptions and political brand equity in the 21st Century. In International Journal of Science and Research Archive (Vol. 15, Issue 1, pp. 1736–1744). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.1.1217

[27] Mukherjee, Prof. N. (2024). Using Technological Advancements - Changing the Banking Sector's Face Value in World Market. In INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (Vol. 08, Issue 12, pp. 1–6). Indospace Publications. https://doi.org/10.55041/ijsrem39539

[28] Gresia, and Regina Jansen Arsjah. (2024). Analisis Deskriptif Penerapan Kecerdasan Buatan, Prediksi Integritas, Kinerja Keuangan dan Ukuran Perusahaan di Perbankan Indonesia dan Singapura Tahun 2021 – 2023. In El-Mal:

Jurnal Kajian Ekonomi and Bisnis Islam (Vol. 5, Issue 9). Institut Agama Islam Nasional Laa Roiba Bogor. https://doi.org/10.47467/elmal.v5i9.4494

[29] R., V., and Ravi, H. (2021). Innovation in banking: fusion of Artificial Intelligence and blockchain. In Asia Pacific Journal of Innovation and Entrepreneurship (Vol. 15, Issue 1, pp. 51–61). Emerald. https://doi.org/10.1108/apjie-09-2020-0142

[30] (2024). Revolutionizing Financial Landscapes: The Interplay of AI, ML, ERP, and Oracle in Digital Transformation. In International Research Journal of Modernization in Engineering Technology and Science. International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/irjmets49100

[31] Chaouki Chouraik. (2024). Enhancing cybersecurity in Moroccan banking: A strategic integration of AI, blockchain, and business intelligence. In International Journal of Science and Research Archive (Vol. 13, Issue 2, pp. 1723–1734). GSC Online Press. https://doi.org/10.30574/ijsra.2024.13.2.2312

[32] Raiyan Haider, and Jasmima Sabatina. (2025). Harnessing the power of micro-influencers: A comprehensive analysis of their effectiveness in promoting climate adaptation solutions. In International Journal of Science and Research Archive (Vol. 15, Issue 2, pp. 595–610). GSC Online Press. https://doi.org/10.30574/ijsra.2025.15.2.1448

[33] Ali, M., Razaque, A., Yoo, J., Kabievna, U. R., Moldagulova, A., Ryskhan, S., Zhuldyz, K., and Kassymova, A. (2024). Designing an Intelligent Scoring System for Crediting Manufacturers and Importers of Goods in Industry 4.0. In Logistics (Vol. 8, Issue 1, p. 33). MDPI AG. https://doi.org/10.3390/logistics8010033

[34] Ali, G., Mijwil, M. M., Buruga, B. A., and Abotaleb, M. (2024). A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech. In Iraqi Journal for Computer Science and Mathematics (Vol. 5, Issue 3). College of Education - Aliraqia University. https://doi.org/10.52866/ijcsm.2024.05.03.004

[35] Zulfiqar, N., Ghafoor, F., Idrees, M., and Raza, K. (2024). Use of Artificial Intelligence in the Banking Industry: A Case Study of Pakistan. In Review of Applied Management and Social Sciences (Vol. 7, Issue 4, pp. 467–481). South Punjab Center for Research and Development (SPCRD). https://doi.org/10.47067/ramss.v7i4.394

[36] Uchenna Innocent Nnaomah, Opeyemi Abayomi Odejide, Samuel Aderemi, David Olanrewaju Olutimehin, Emmanuel Adeyemi Abaku, and Omamode Henry Orieno. (2024). AI in risk management: An analytical comparison between the U.S. and Nigerian banking sectors. In International Journal of Science and Technology Research Archive (Vol. 6, Issue 1, pp. 127–146). Scientific Research Archives. https://doi.org/10.53771/ijstra.2024.6.1.0035