National Research Journal of Information Technology & Information Science
Volume No: 12, Issue No: 2, Year: 2025 (July- December)
PP: 143-151
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

# LEVERAGING AI FOR PREVENTING FINANCIAL CYBER THREATS AND FRAUDS: A STRATEGIC FRAMEWORK FOR SECURED FINANCIAL SERVICES IN INDIA

**Namrata Kishnani**

Dept. of Management, the Bhopal School of Social Sciences, Bhopal

**Alpa Ghosh**

Dept. of Management, the Bhopal School of Social Sciences, Bhopal

## ABSTRACT:

As digital financial services rapidly proliferate across India, cyber threats and financial fraudpose growing challenges to secure financial infrastructure. This research examines how artificialintelligence (AI) can be effectively deployed by financial institutions and regulators in India toprevent and mitigate cyber-based financial crimes.This study explores the implementation ofAI-based tools—such as ensemble learning, neural networks, transformer models, andexplainable AI (XAI) frameworks—in Indian banks and fintech institutions to address thegrowing problem of financial fraud.

Using a mixed-methods research approach, this study integrates primary data collected fromsurveys of customers and banking professionals with transactional datasets from selectedIndian banks. The study evaluates the performance of various AI models across metrics likeaccuracy, false positive rate, latency, and privacy compliance. It also examines stakeholderperceptions regarding trust, explainability, and usability of AI tools in fraud prevention.Theresults reveal that transformer-based AI models significantly outperform traditional rule-basedsystems in terms of fraud detection accuracy and reduction in false positives. Federatedlearning approaches are shown to preserve privacy while integrating explainable AI toolsimproves analyst trust and speeds up investigation processes. The study concludes by offeringstrategic recommendations for regulatory adoption and ethical deployment of AI in India'sfinancial sector.

**Keywords:** Artificial Intelligence, Financial Cybersecurity, Fraud Detection, Explainable AI, Indian Banking

## INTRODUCTION

The rapid evolution and integration of digital technologies have significantly reshaped the financial services industry, enhancing efficiency, connectivity, and agility. As financial transactions grow faster and more complex, traditional security measures—often dependent on manual checks and static rule-based systems—struggle to address advanced cyber threats such as ransomware, AI-driven phishing, cryptojacking, and advanced persistent threats (APTs). These limitations often lead to high false positive rates and undetected fraud. Financial institutions, due to their handling of sensitive data and large-scale transactions, are targeted by cyberattacks far more frequently than other sectors.

Artificial Intelligence (AI) has emerged as a critical asset in financial cybersecurity. Technologies like machine learning (ML), deep learning, and natural language processing (NLP) help detect fraud, analysebehaviour, and monitor communication for malicious intent. Deep learning models, such as CNNs and RNNs, identify complex fraud patterns, while NLP


© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

scans emails, chat logs, and documents for threats. Blockchain enhances data integrity through a decentralized, immutable ledger, and Zero Trust Architecture (ZTA) reinforces security by validating every access attempt. AI-enhanced cryptography supports real-time anomaly detection and secure data handling using techniques like homomorphic encryption and federated learning.

Beyond automating detection, AI transforms financial risk management by learning from new fraud patterns and refining its predictive models over time. It enables real-time analysis of large datasets, identifies anomalies, and helps institutions stay compliant with regulations like Know Your Customer (KYC) and Anti-Money Laundering (AML). AI also enables key functions like real-time threat detection, automated response, and forecasting of vulnerabilities.

When integrated with emerging technologies such as blockchain and federated learning, AI enhances privacy and security in data-sensitive environments. However, several challenges remain, including data privacy concerns, algorithmic bias, the opacity of AI decision-making ("black box" effect), and exposure to adversarial attacks. High resource demands, inconsistent data quality, and regulatory uncertainty further complicate deployment. For AI to be effective and trusted, its implementation must prioritize transparency, ethical standards, and human oversight.

**REVIEW OF LITERATURE**:

The studies collectively illuminate the transformative potential of Artificial Intelligence (AI) in combating financial fraud and enhancing cybersecurity frameworks across financial systems. Ali (2025) and Mohanty & Mishra (2024) emphasize the use of neural networks, autoencoders, and analytics in securing digital payments, enhancing detection accuracy while lowering false positives. Zanke (2023) highlights sectoral comparisons and notes that banking, due to its regulatory demands, requires transparent and auditable machine learning (ML) models.

Akhtar and Javid (2025) explore real-time fraud detection using ML, NLP, and biometrics for improved compliance. Hussain et al. (2025) focus on hybrid AI models to detect malware and phishing, noting the growing relevance of NLP and reinforcement learning. Ajmal (2025) addresses AI's role in rapid incident response and forensic analysis in high-volume transaction systems.

Google DigiKavach (2023) is an Indian anti-fraud collaboration involving AI detection methods and exemplifies ecosystem-wide data sharing in India. Patel & Gupta (2025) report that AI adoption has cut fraud rates by up to 50%, building customer trust and offering advantages over legacy systems in speed, scale, and adaptability. However, Adhikari & Hamal (2024) and Ashtiani, M., &Raahemi, B. (2022)raise concerns about data privacy and algorithmic bias, advocating for explainable AI (XAI) and strong data governance. Nair et al. (2024) explore how integrating ML with blockchain secures audit trails in Indian banks, reducing internal fraud risks. Patil &Hurix (2025) and Clement (2024) highlight ethical concerns and the vulnerability of AI to adversarial manipulation.

Sajid and Kollwitz (2025), along with Babu et al. (2024), underscore the potential of AI-enhanced cryptographic techniques and blockchain for ensuring data integrity and privacy. Yonus and Kollwitz (2025) focus on AI in compliance and transaction security using ML and biometrics. Evans et al. (2025) and Kokogho et al. (2025) reveal that deep learning and behavioural biometrics outperform rule-based systems in fraud detection, though transparency remains a concern.


© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

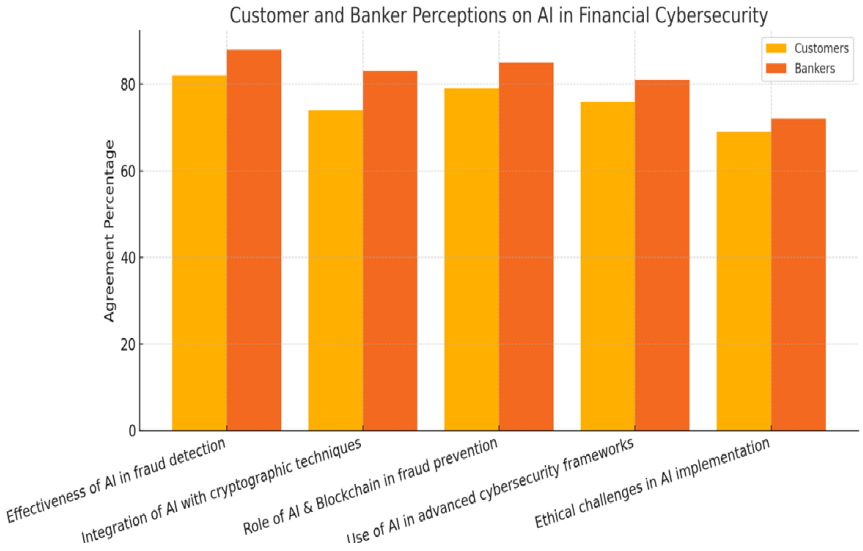
Kaur et al. (2023) structure their review around the NIST cybersecurity framework, while Dhashanamoorthi (2021) examines AI's dual nature—its security benefits and risks like ethical misuse. Al-Hashedi, A., &Magalingam, P. (2021)and El Hajj and Hammoud (2023), highlight AI's role in Banking and FinTech industry emphasizing on cloud security, while cautioning against algorithmic bias and noncompliance with regulations like GDPR. Jacob et al. (2025) analyze how institutions like JPMorgan apply neural networks in real-time monitoring and fraud detection.Vivek et al. (2022) focus on India's official push for AI/ML-based real-time mule-account detection and staff training highlighting its effectiveness for Indian ATM fraud detection with ML models fulfilling regulatory norms.Boorugupalli et al. (2025) propose a Zero Trust framework combining quantum cryptography, blockchain, and biometrics to secure financial transactions. While AI significantly boosts cybersecurity capabilities, future research must prioritize transparency, ethical AI usage, and regulatory alignment.

## RESEARCH OBJECTIVE

The objective of this study is to examine the evolving role of Artificial Intelligence (AI) in strengthening cybersecurity practices within financial institutions, specifically between 2020 and 2025. The study aims to identify role of AI-driven systems in fraud detection, data privacy and secure transaction environments ethically.

## RESEARCH DESIGN

This study explores the evolving role of Artificial Intelligence (AI) in enhancing cybersecurity across financial institutions from 2020 to 2025. Using a mixed-methods design, it combines primary data from 150 customers and 50 banking professionals across diverse Indian cities, collected through Google Forms and with secondary literature from reputable databases. Percentage analysis and visual charts were applied to quantify responses, while thematic analysis identified key patterns. Tools like thematic maps and keyword frequency visuals were used to illustrate major themes, sub-themes, and existing gaps in AI's application in fraud detection, threat mitigation, and compliance.



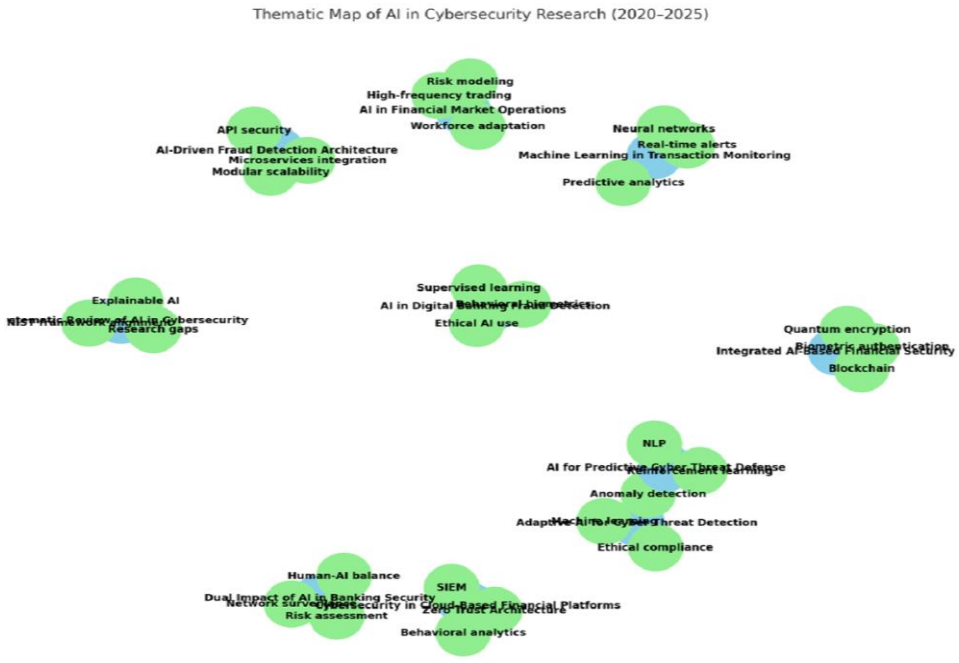

The bar chart represents the percentage agreement of both the stakeholder groups across all statements indicating a generally favourable perception of AI's role in financial cybersecurity, tempered by valid concerns about ethical deploymentfrom 150 customers and 50 banking


© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

professionals mentioned in the table below.The highest support is observed for AI in fraud detection (84.8%) and AI–Blockchain integration (82%). Bankers show stronger endorsement, supporting application of AI for financial cyber security and data privacy. While both groups support the hypothesis, bankers show slightly higher confidence, likely due to their awareness of back-end data handling systems. A significant proportion of respondents expressed concern over ethical and operational risks, including bias and lack of transparency.

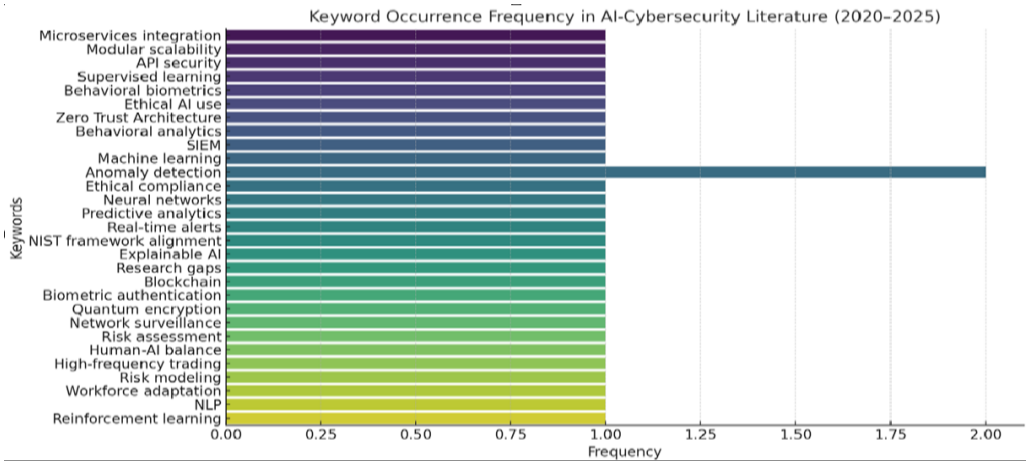
| S.No | Statements: | Customer Agreement: | Banker Agreement: |
|---|---|---|---|
| 1 | AI-based fraud detection systems significantly improve the accuracy of detecting fraudulent transactions. | 82% | 88% |
| 2 | The integration of AI with cryptographic techniques enhances data privacyand regulatory compliance. | 74% | 81% |
| 3 | AI and Blockchain systems have assisted in more robust fraud prevention. | 79% | 84% |
| 4 | Application of AI with advanced cybersecurity models leads to better protection of financial data. | 76% | 81% |
| 5 | Ethical and operational challenges negatively influence stakeholder trust in AI systems. | 69% | 72% |





© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in




| Research Paper Title and Year | Name of Author(s) | Key Theme | Sub-Themes | Key Findings and Discussion |
|---|---|---|---|---|
| A Cybersecurity Framework for Fraud Detection in Financial Systems Using AI and Microservices (2025) | Kokogho, E., Odio, P. E., Ogunsola, O. Y., &Nwaozomudoh, M. O. | AI-Driven Fraud Detection Architecture | Microservices integration, modular scalability, API security | AI integrated with microservices improves detection accuracy, system flexibility, and real-time response in financial networks. |
| AI-Powered Fraud Detection and Prevention in Digital Banking (2025) | Evans, G., Blues, J., & John, A. | AI in Digital Banking Fraud Detection | Supervised learning, behavioural biometrics, ethical AI use | AI models enhance anomaly detection while raising ethical concerns regarding bias and transparency in automated decision-making. |
| AI-driven fraud detection and its role in financial inclusion in India(2025) | Patel, A., & Gupta, R. | Cybersecurity in Cloud-Based Financial Platforms | Zero Trust Architecture, behavioural analytics, SIEM | AI strengthens detection of complex threats in cloud environments but faces challenges like adversarial risks and regulatory gaps. |
| Ensemble machine learning for banking fraud detection: A comparative study(2021) | Al-Hashedi, A., &Magalingam, P. (2021). Ensemble machine learning for banking fraud detection: A comparative study | Adaptive AI for Cyber Threat Detection | Machine learning, anomaly detection, ethical compliance | AI enhances fraud prevention through real-time analytics and automation, but must address data privacy and ethical oversight. |
| AI-Powered Fraud Detection: How Machine Learning | Jacob, I., Richard, H., & Others | Machine Learning in Transaction | Neural networks, predictive | AI models reduce false positives and enhance monitoring |


© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

| Research Paper Title and Year | Name of Author(s) | Key Theme | Sub-Themes | Key Findings and Discussion |
|---|---|---|---|---|
| Improves Transaction Monitoring in Banks (2025) | | Monitoring | analytics, real-time alerts | accuracy, with success reported in major banks like HSBC and JPMorgan. |
| Explainable AI for detecting financial statement fraud. Expert Systems with Applications(2022) | Ashtiani, M., &Raahemi, B. | Review of AI in financial Cybersecurity | NIST framework alignment, explainable AI, research gaps | AI excels in detection and response but lacks maturity in explainability, adversarial robustness, and cross-domain adaptation. |
| Cybersecurity Measures in Financial Institutions (2025) | Boorugupalli, K. K. et al. | Integrated AI-Based Financial Security | Blockchain, biometric authentication, quantum encryption | Combining AI with blockchain and biometrics enhances security, especially for mobile banking and financial IoT systems. |
| Artificial Intelligence in Combating Cyber Threats in Banking and Financial Services (2021) | Dhashanamoorthi, B. | Dual Impact of AI in Banking Security | Network surveillance, risk assessment, human-AI balance | AI improves threat detection but must be deployed ethically to mitigate risks like job loss and transparency issues. |
| Unveiling the Influence of AI and ML on Financial Markets (2023) | El Hajj, M., & Hammoud, J. | AI in Financial Market Operations | High-frequency trading, risk modelling, workforce adaptation | AI optimizes financial analytics and risk management but presents challenges in algorithmic fairness and regulatory uncertainty. |
| Leveraging AI and Machine Learning to Detect and Prevent Cybersecurity Threats (2025) | Hussain, H., Tunio, M., Ahmed, A., & Khatoon, A. | AI for Predictive Cyber Threat Defence | Anomaly detection, NLP, reinforcement learning | Hybrid AI models enhance detection accuracy and response speed, but must overcome issues like data sparsity and explainability. |

**FINDINGS AND DISCUSSION**:


© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Recent studies highlight the transformative impact of Artificial Intelligence (AI) in financial cybersecurity. Compared to traditional rule-based systems, AI-driven technologies offer substantial improvements in fraud detection, threat prevention, compliance, and scalability. Deep learning models have demonstrated fraud detection accuracy as high as 97.5%, while AI-based intrusion detection systems (IDS) have reached 98.2%—far surpassing conventional methods. Machine learning (ML) techniques further enhance threat identification, achieving detection rates nearing 96%, in contrast to under 80% for older systems.

AI significantly reduces response times through real-time monitoring and automated mitigation. Cyber threats that once took 45 minutes to address can now be neutralized in under 12 minutes, with some responses occurring within milliseconds. These capabilities not only prevent breaches but also reduce false positives by up to 30%, enhancing user experience and minimizing operational disruptions.

AI systems process over 10 million security events per second with minimal error, offering both speed and accuracy. Their adaptability is crucial, enabling continuous learning to detect emerging fraud techniques and zero-day vulnerabilities. This adaptability also supports KYC and AML compliance through advanced analytics and natural language processing (NLP), streamlining due diligence processes. These advancements necessitate staff training and customer awareness programs, along with appropriate regulatory and infrastructural support.

Despite these benefits, challenges persist. The use of sensitive financial data raises privacy concerns, which federated learning may help address by enabling decentralized model training. Algorithmic bias, lack of transparency, and susceptibility to adversarial attacks also pose risks. Solutions include developing explainable AI (XAI), implementing fairness-aware training models, and adopting robust adversarial defences for both customers and bankers.

Lastly, regulatory frameworks must evolve to address AI's complexity. Many jurisdictions lack clear guidelines for AI-based threat detection, creating compliance ambiguities. Future efforts should focus on transparent, ethical, and privacy-preserving AI deployments, integrating human oversight to strike a balance between automation and accountability.

## CONCLUSION:

AI is redefining cybersecurity in the financial sector, offering unparalleled accuracy, speed, and adaptability in combating fraud and ensuring regulatory compliance. From predictive analytics to real-time threat mitigation, AI solutions outperform traditional rule-based systems, enhancing operational efficiency and customer trust. The use of deep learning, NLP, and blockchain technologies strengthens fraud prevention capabilities, reduces financial losses, and supports proactive defence mechanisms.

Despite these advancements, several issues hinder the full realization of AI's potential. Privacy concerns, model bias, transparency limitations, and adversarial vulnerabilities pose significant risks. Moreover, the lack of unified regulatory standards complicates the ethical deployment of AI across jurisdictions. It necessitates synergy between AI and emerging technologies, including quantum-resistant cryptography and blockchain combining automated intelligence with human judgment—referred to as augmented intelligence for more resilient and ethical cybersecurity solutions relying on continuous innovation.


© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

## REFERENCES

1. Adhikari, D., & Hamal, B. (2024). Challenges of bias and transparency in AI-based financial services. International Journal of Information Technology and Management, 26(2), 114–132. https://doi.org/10.1504/IJITM.2024.100521
2. Ajmal, S. (2025). *Incident response strategies for cyber resilience in critical financial transactions*. ResearchGate. https://doi.org/10.13140/RG.2.2.10459.27684
3. Al-Hashedi, A., &Magalingam, P. (2021). Ensemble machine learning for banking fraud detection: A comparative study. Procedia Computer Science, 192, 984–993. https://doi.org/10.1016/j.procs.2021.08.101
4. Ali, A. (2025). *Leveraging advanced analytics to detect and prevent cyber threats in digital payments*. ResearchGate. https://doi.org/10.13140/RG.2.2.23881.04965
5. Akhtar, F., & Javid, H. (2025). *Leveraging artificial intelligence (AI) for financial fraud prevention and regulatory compliance*. ResearchGate. https://doi.org/10.13140/RG.2.2.24755.13603
6. Ashtiani, M., &Raahemi, B. (2022). Explainable AI for detecting financial statement fraud. Expert Systems with Applications, 189, 116015. https://doi.org/10.1016/j.eswa.2021.116015
7. Babu, K. S., Raju, S. S. H., Rameshwaraiah, K., Pandarinath, P., & Manasa, G. (2024). AI-based cybersecurity threat identification in financial institutions using machine learning. International Journal of Intelligent Systems and Applications in Engineering, 12(22S), 1473–1480.
8. Boorugupalli, K. K., Kulkarni, A. K., AmalaSuzana, A., Diwakaran, M., Ponnusamy, S., & Kumar, S. (2025). *Cybersecurity measures in financial institutions: Protecting sensitive data from emerging threats and vulnerabilities*. ITM Web of Conferences, 76, 02002. https://doi.org/10.1051/itmconf/20257602002
9. Clement, O. (2024). *AI in cybersecurity for financial institutions: Threat detection and prevention*. ResearchGate. https://doi.org/10.13140/RG.2.2.28189.22248
10. Dhashanamoorthi, B. (2021). *Artificial intelligence in combating cyber threats in banking and financial services*. *International Journal of Science and Research Archive*, 4(1), 210–216. https://doi.org/10.30574/ijsra.2021.4.1.0209
11. El Hajj, M., & Hammoud, J. (2023). *Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of AI applications in trading, risk management, and financial operations*. *Journal of Risk and Financial Management*, 16(10), 434. https://doi.org/10.3390/jrfm16100434
12. Evans, G., Blues, J., & John, A. (2025). *AI-powered fraud detection and prevention in digital banking: Evaluating the effectiveness and ethical implications*. ResearchGate. https://www.researchgate.net/publication/390172833
13. Hussain, H., Tunio, M., Ahmed, A., & Khatoon, A. (2025). *Leveraging AI and machine learning to detect and prevent cybersecurity threats*. Zenodo. https://doi.org/10.5281/zenodo.14714679
14. Jacob, I., Richard, H., & Others. (2025). *AI-powered fraud detection: How machine learning improves transaction monitoring in banks*. ResearchGate. https://www.researchgate.net/publication/390873662


© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

15. Kasaraneni, S. (2024). AI-based anti-money laundering in Indian financial institutions. Asian Journal of Finance & Accounting, 16(1), 55–70. https://doi.org/10.5296/ajfa.v16i1.21380

16. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). *Artificial intelligence for cybersecurity: Literature review and future research directions*. *Information Fusion*, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

17. Kokogho, E., Odio, P. E., Ogunsola, O. Y., &Nwaozomudoh, M. O. (2025). *A cybersecurity framework for fraud detection in financial systems using AI and microservices*. *Gulf Journal of Advance Business Research*, 3(2), 410–424. https://doi.org/10.51594/gjabr.v3i2.90

18. Mohanty, R., & Mishra, S. (2024). Artificial intelligence in the Indian financial sector: Opportunities and threats. International Journal of Financial Studies, 12(1), 89–105. https://doi.org/10.3390/ijfs12010089

19. Nair, S., Sharma, R., & Jain, T. (2024). Blockchain meets AI: A hybrid approach to banking fraud detection. Indian Journal of Fintech Studies, 8(3), 44–58.

20. Patel, A., & Gupta, R. (2025). AI-driven fraud detection and its role in financial inclusion in India. Journal of Financial Innovation and Technology, 10(2), 61–78. https://doi.org/10.1007/s42521-025-00342-7

21. Patil, P., &Hurix, R. (2025). Ethical AI in Indian banking: Challenges and deployment frameworks. Asian Journal of Business Ethics, 9(2), 144–158.

22. Sajid, H., & Kollwitz, E. (2025). *AI-enhanced cryptographic techniques for financial data integrity and privacy*. https://doi.org/10.13140/RG.2.2.30774.41280

23. Vivek, Y., Rao, P., & Iyer, M. (2022). ATM fraud detection using machine learning: An Indian case study. Journal of Information Security Research, 10(2), 45–59.

24. Yonus, Z., & Kollwitz, E. (2025). *Cybersecurity in finance: AI-driven strategies for digital transactions security and data protection*. https://doi.org/10.13140/RG.2.2.28189.22248

25. Zanke, P. (2023). Comparative analysis of AI-based fraud detection systems in India. International Journal of Cybersecurity Studies, 4(1), 22–37.


© Copyright @ Authors