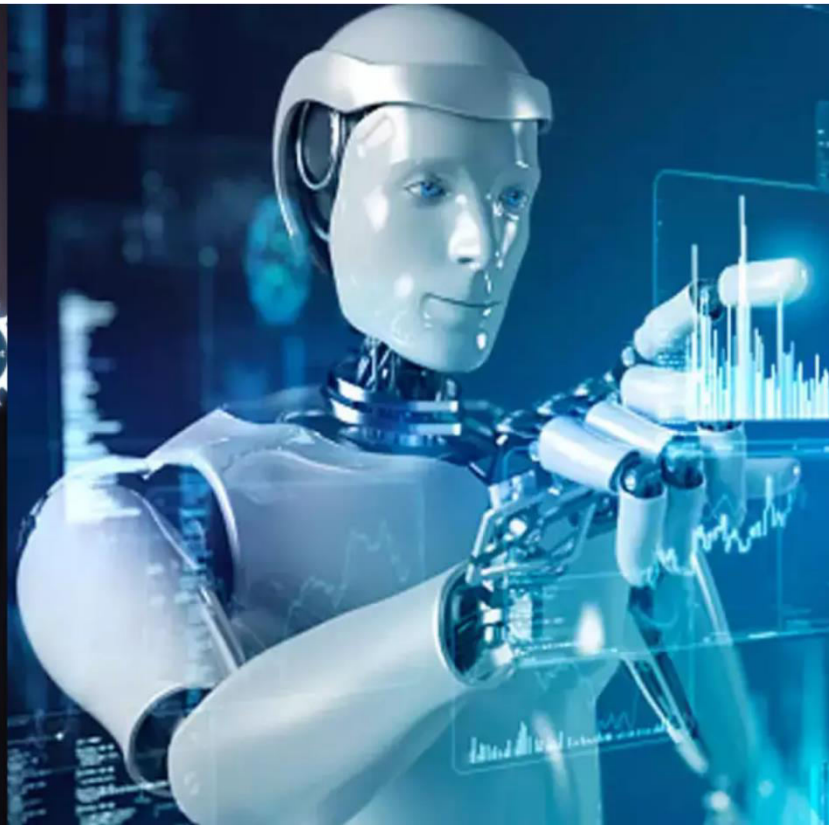
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 1, January 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501051|

Role of Artificial Intelligence in Fraud Detection in the Digital Economy

Roopa S C

Assistant Professor, School of Management and Commerce, S-Vyasa Deemed to be University, Bengaluru, India

ABSTRACT: Artificial intelligence (AI) is revolutionizing fraud detection in the digital economy through faster, intelligent, and more accurate forms of detection. In this study, the paradigmatic role of AI in fraud detection is explored using qualitative research design with thematic synthesis and natural language processing. The study identifies the intersection of technical developments, ethical issues, and systemic consequences of the use of AI. There is a conceptual framework presented that explains how AI-driven fraud detection diffuses across four interdependent dimensions: theoretical-conceptual, governance-ethical, technical-operational, and cross-cutting themes. The theoretical level places fraud within an embedded context, whereas the governance-ethical level stresses transparency, accountability, and trust. Technical-operational issues depict the balance between technological innovation and dependability. Cross-cutting themes stress broader implications like efficiency-ethics trade-offs and systemic confidence. The research is a contribution to the literature and offers managerial implications to managers and policymakers. Managerial implications highlight the urgent necessity for balanced application of AI with full interpretability and ethical adherence. Research implications highlight the significance of interdisciplinary research and the necessity of undertaking additional research at the crossroads of AI governance, fraud analytics, and building trust. Theoretically, the research adds fraud detection knowledge through the positioning of AI in current paradigms and emphasizes the importance of interpretability and transparency. Future research areas could include testing the analysis against empirical facts, longitudinal and comparative analyses, and the measurement of the influence of transparency frameworks on stakeholder trust in AI-based fraud detection systems.

KEYWORDS: Artificial Intelligence, Fraud Detection, Digital Economy, Anomaly Detection, Predictive Modelling

I. INTRODUCTION

Artificial Intelligence is transforming the war against fraud by allowing quicker, more intelligent, and more effective detection systems in the digital economy. With powerful algorithms and real-time analysis of data, AI allows organizations to detect concealed patterns, detect fraud, and protect financial systems better than ever before.

The manifestation and avoidance of the fraud phenomenon in the digital economy can be better explained on the basis of existing theoretical frameworks. The Fraud Triangle Theory particularly highlights the fact that fraud exists where pressure, opportunity, and justification align. Artificial intelligence instinctively targets the opportunity aspect by restricting the room for manipulation out of sight by continuous auditing and detection of irregularities. Likewise, the Routine Activity Theory specifies the presence of a capable guardian to dissuade fraudulent behaviour. Here, AI is an online watchdog that ensures real-time surveillance and makes it exceedingly challenging for fraudsters to take advantage of system vulnerabilities. All these views collectively position AI not just as a tool, but also as an agent that undertakes a forward-looking function and modifies the environment in which fraud takes place.

Additional insights are offered by frameworks that examine behavioural and systemic determinants of fraud. General Deterrence Theory posits that detection probability is an effective deterrent mechanism, and AI enhances the deterrent by allowing instantaneous and definite detection of suspicious activity. The Information Asymmetry Theory also considers asymmetry of information between actors, a discrepancy that normally is exploited by fraudsters; AI bridges this discrepancy by revealing concealed patterns and enhancing openness in money systems.

AI-based fraud detection has revolutionized the digital economy by providing real-time, scalable analytics to identify outliers and anticipate suspicious activity before losses happen. For example, Mastercard's AI platform analyses more than 159 billion transactions a year and has increased fraud detection by as much as 300% and decreased false

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501051|

transaction declines by 22% (Business Insider, 2025). However, the environment is full of challenges. Sophisticated criminal methods—deepfakes-enabled impersonations, content generated by AI, and adversarial attacks—will flood detection systems and necessitate increasingly adaptable defenses (TechRadar, 2025; Wall Street Journal, 2025; Deloitte, 2024). Moreover, the use of AI is further complicated by issues related to data quality, transparency, and regulation. Low-quality or biased training data can destabilize model accuracy, and the "black box" nature of much AI adds to accountability and explainability. Protecting against bias and conformity with privacy laws also increases the system design level (SmartDev, 2025; Ledde, 2025; Awosika et al., 2023). Consequently, achieving the most optimal combination of operational efficiency, ethical regulation, and sound fraud prevention is a pressing issue in the contemporary digital age.

Even as the digital technologies have seen profound improvements, fraud remains increasingly sophisticated and on a large scale, threatening financial integrity and trust within the digital economy. Conventional fraud detection capabilities are often unable to cope with the quantity, velocity, and complexity of counterfeit activity, leading to late detection, false positives, and serious financial loss. Even though artificial intelligence holds great promise in predictive modeling, anomaly detection, and adaptive learning, its application is being hampered by the lack of transparency, data integrity, and ethical issues. This makes it an urgent gap between the potential usefulness of AI-powered fraud detection and real-world effectiveness to make digital financial ecosystems safe, resilient, and trustworthy.

The scope of research is limited to qualitative research on how fraud detection is being transformed by artificial intelligence in the digital economy through available scholarly literature, industry, and theoretical frameworks. Natural Language Processing (NLP) is used sparingly, only scanning the Introduction and Literature Review chapters to provide richness in conceptual understanding and not empirical testing. The value-added contribution of this research is the potential to enhance scholarly knowledge by highlighting newly emerging trends, challenges, and opportunities and simultaneously providing valuable information to policymakers, practitioners, and technology developers. By examining the dynamics between technological innovation, regulation, and organizational adoption, the study is a valuable contribution to practice and theory in enhancing fraud detection in the new digital environment.

II. STATEMENT OF THE PROBLEM

Despite significant advancements in artificial intelligence for fraud detection, organizations continue to face challenges related to model transparency, ethical governance, regulatory compliance, and persistent false positives. The growing sophistication of digital fraud, coupled with concerns over algorithmic bias, data privacy, and trust deficits, limits the full realization of AI's potential. There remains a fragmented understanding of how technical innovation, ethical standards, and systemic trust intersect within AI-driven fraud detection frameworks.

OBJECTIVE

1. To explore the possible role of artificial intelligence in enhancing fraud detection in the digital economy.
2. To evaluate the effectiveness of AI-based techniques for reducing false positives and improving accuracy.
3. To examine the issue of using AI for fraud detection, e.g., ethical and regulatory concerns.
4. To debate the impact of AI on trust within an organization and the financial system's resilience.
5. To establish future potential for improving fraud detection through advanced uses of AI.

SCOPE OF THE STUDIES

The study examines the role of AI in fraud detection across financial and digital sectors, emphasizing machine learning, deep learning, explainable AI, and governance dimensions. It adopts a qualitative thematic synthesis to explore technical, ethical, organizational, and systemic perspectives. The scope includes analysis of transparency, accountability, resilience, and emerging technologies such as federated learning and predictive analytics, without focusing on empirical testing or sector-specific implementation models.

SIGNIFICANCE OF THE STUDY

This study contributes theoretically by integrating technical, ethical, and governance perspectives into a unified framework for AI-based fraud detection. Practically, it informs managers and policymakers about responsible AI deployment, emphasizing transparency and trust. It also highlights future research directions, supporting

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501051|

interdisciplinary inquiry and policy formulation aimed at strengthening digital trust and systemic resilience in the evolving digital economy.

III. LITERATURE REVIEW

The utilization of artificial intelligence (AI) to improved fraud detection in the digital world had been completely recognized in various sectors. Experts repeatedly underlined how AI methods like machine learning, deep learning, and natural language processing offered more flexible and more effective means than conventional rule-based fraud detection systems. For instance, Awoyemi et al. (2017) showed how machine learning algorithms greatly improved detection accuracy by uncovering hidden patterns of fraudulence in financial transactions. Similarly, Fiore et al. (2019) demonstrated that deep learning models could effectively process large amounts of unstructured data to create real-time fraud prevention capabilities. Other writers concentrated on explainable AI demand, as in Ahmad et al. (2020), who felt that transparency in AI models was crucial to facilitate compliance with regulation and trust in the digital economy. Alazab et al. (2020) mentioned that AI systems offered predictive analytics to enable proactive fraud risk management. The application of AI in banking and financial services had also been evidenced by research reports like by Dal Pozzolo et al. (2018), which attested that ensemble learning minimized false positives in fraud detection, thus enhancing customer experience. Outside of finance, too, AI-based anomaly detection models had been used in e-commerce and cybersecurity, as attested by Zengin et al. (2021), attesting to the cross-industry reach of AI. Together, literature revealed that AI was not merely a facilitating technology but also a strategic driver which augmented digital trust and resistance to progressively sophisticated fraud attacks in the digital economy.

The power of AI-based methods in minimizing false positives and maximizing detection accuracy had previously been explored intensely in a number of domains, notably fraud discovery and security. Conventional systems based on rule-based decisions tended to leave high false positives, limiting operational effectiveness and customer satisfaction. Scholars like Dal Pozzolo et al. (2018) noted that ensemble learning techniques, such as bagging and boosting, reduced false alarms considerably and improved the accuracy of credit card fraud detection. Likewise, Fiore et al. (2019) showed that generative adversarial networks (GANs) not only improved classification accuracy but also achieved better minority fraudulent sample detection. Hybrid AI strategies were also tried, according to Chen et al. (2020), where the blending of unsupervised and supervised models was more responsive in dealing with changing patterns of fraud. Buda et al. (2018) also depicted how deep learning provided aid in avoiding data imbalance challenges, which was specifically to minimize false positives. In cybersecurity implementations, Ahmed et al. (2016) established that machine learning-based anomaly detection methods were more accurate and accurate than traditional intrusion detection systems. Current literature, for instance, Bahnsen et al. (2016), also asserted cost-sensitive learning balanced sensitivity vs. specificity trade-off and avoided false alarms without reducing accuracy. Collectively, the literature showed that AI-based models outdid conventional procedures since they learned dynamically from new distributions of data, minimized false positives, and significantly improved overall detection accuracy both financially and in security.
The application of artificial intelligence (AI) in fraud discovery had been with some difficulties, especially ethical and regulatory difficulties. Researchers had made it known that although AI had granted sophisticated functionality for detecting deceit, its utilization had raised questions on transparency, accountability, and fairness. Ahmad et al. (2020) contended that transparency in AI models, also known as the "black box" problem, had undermined trust and created difficulties in meeting regulatory requirements. Similarly, Brkan (2019) noted that AI systems could unintentionally perpetuate bias and, therefore, subject individuals to disparate treatment in financial transactions. The legal framework was similarly lagging behind technological advancements, as contended by O'Neil (2016), who highlighted threats associated with unregulated algorithmic decision-making. Alazab et al. (2020) emphasized that ethical issues such as data privacy and consent emerged as issues of prominence when AI systems processed intimate personal and financial data. Additionally, Zeng et al. (2021) found the trade-off between maintaining fraud detection precision and users' privacy right in the instance of strict data protection laws like the GDPR. Again, Bryson and Theodorou (2019) observed that how liability for AI misclassification ought to be assigned remained an open issue in most legal systems. These studies all implied that success in AI fraud detection would rely not only on advances in technology but also on the establishment of strong ethical standards and regulatory structures that could provide fairness, accountability, and trust within the digital economy.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501051|

The role of artificial intelligence (AI) in organizational strength and the strength of the financial system had been examined from various academic points of view. Academicians focused on the fact that AI technologies strengthened fraud detection, risk reduction, and firm performance, thereby ensuring institutional strength and resilience. The use of AI in financial services strengthened trust, Schuetz and Venkatesh (2020) contend, as it increased transparency while making decisions and minimized systemic risk. Alzubaidi et al. (2021) also discovered that predictive analytics through AI allowed organizations to act ahead of time in responding to changes in the market, thus enhancing organizational resilience. Nevertheless, explainability and issues of algorithmic bias presented undercurrent threats to trust, referencing Morley et al. (2021), who posited that if there was no effective governance, stakeholders' trust would reduce. In banking, Ghosh et al. (2019) illustrated how AI-based fraud detection systems lowered financial exposures directly and was therefore a factor that helped build systemic resilience. Additionally, Sivarajah et al. (2020) identified that the union of AI with big data analytics fostered resilience as it allowed companies to peer into the future and prepare to combat disruptions. In contrast, however, Zeng et al. (2021) identified ethical and regulatory issues, which if not addressed would wreck havoc on trust in AI-facilitated financial infrastructure. Together, the studies estimated that although AI could be used to boost organizational resilience and trustworthiness of financial systems, its performance would rely on open governance, ethical deployment, and compliance with regulation.

Prospects for deepening fraud detection through enhanced AI technologies had been thoroughly debated in the literature, where writers stressed the promise of emerging technology to transcend current shortfalls. Writers like West and Bhattacharya (2016) contended that AI-driven predictive analytics were able to dramatically boost early fraud detection by uncovering latent and incipient patterns in vast amounts of financial data. Similarly, Fiore et al. (2019) opined that generative adversarial networks (GANs) could enhance the detection of rare fraudulent instances through artificial fraud case simulation for strong model training. Deep reinforcement learning was also seen as a possible path, as opined by Sahu et al. (2020), as it allowed dynamic fraud scenarios to learn adaptively. In addition, Zhang et al. (2021) highlighted the application of explainable AI (XAI) to help provide higher transparency and trust in fraud detection models and even enable regulatory compliance. Federated learning proposed by Yang et al. (2019) was identified as a direction towards improving fraud detection through model training jointly across institutions without breaching data privacy. Cloud-based AI infrastructure was also designed to support greater scalability and real-time detection of fraud, as per Ghosh et al. (2019). Overall, the studies suggested that sophisticated AI approaches, especially those focused on adaptability, transparency, and collaborative intelligence, would be instrumental in shaping the future of fraud detection and the stability of the digital economy.

IV. METHODOLOGY

This research employs a qualitative approach to explore systematically the function of artificial intelligence for fraud detection in the digital economy. The general aim is to synthesize existing knowledge, determine thematic trends, and develop a conceptual framework that synthesizes theoretical, technical, and ethical knowledge. The research method is multi-phased, integrating document analysis, thematic synthesis, and selective use of natural language processing (NLP) tools to meet the research objectives explicated. Through this, the research not only synthesizes knowledge from existing scholarship and industry expertise but also offers a systematic analytical perspective in de-coding nascent complexities in the industry.

Qualitative research was most appropriate as the study aims to explain complex phenomena, understand diverse perceptions, and develop contextualised knowledge compared to hypothesis testing or statistical generalisation. The design is analytical and descriptive with a focus towards synthesis and interpretation of academic literature, industry reports, and conceptual models. Sources of data comprised peer-reviewed journal articles, conference articles, and scholarly books obtained from databases like IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar. Additionally, industry reports, whitepapers, and practitioner-focused articles from mainstream media outlets were employed in order to deal with real-world applications and future trends. All these combined gave wide-based and balanced grounds for analysis.

The analysis was carried out in three consecutive phases. In the first phase, thematic synthesis and document analysis were carried out, in which close reading, coding, and bringing findings together into wider thematic categories like "technical efficacy," "ethical dilemmas," and "systemic resilience" was done. This was the initial phase through which collation of insights from multiple sources in a single narrative could be made. The second activity was NLP-based pre-

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

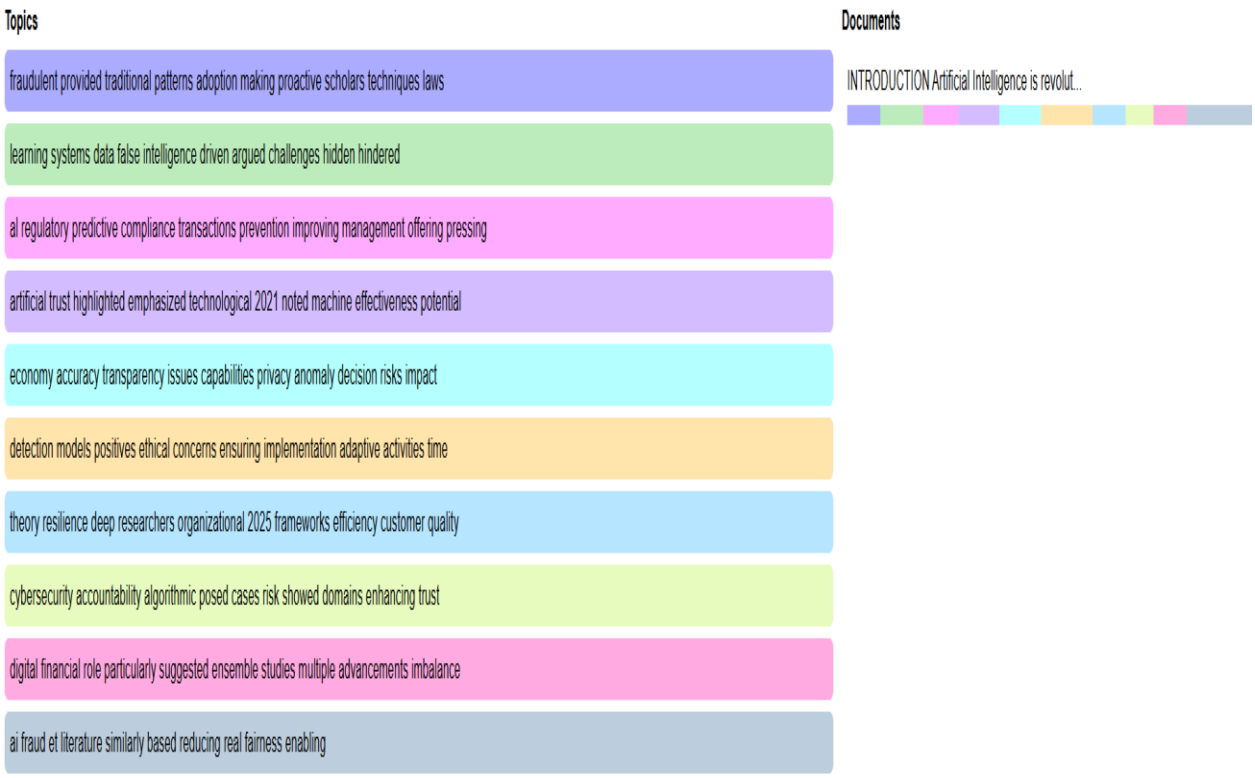
|DOI: 10.15680/IJIRSET.2026.1501051|

processing of Introduction and Literature Review sections of this research using text cleaning, tokenization, and lemmatization. It was not intended to generate new empirical data but to create a computational framework to enable the qualitative synthesis. The third step made use of NLP methods such as Latent Dirichlet Allocation (LDA) to conduct topic modeling and Principal Component Analysis (PCA) for clustering. These approaches exposed built-in patterns and thematic consistencies and therefore improved the research interpretive power.

The thematic synthesis and NLP findings were then incorporated into constructing a multi-layered conceptual framework. The framework structures the discussion into four interrelated dimensions: theoretical–conceptual foundations, governance and ethical issues, technical and operational issues, and cross-cutting implications for systemic trust and resilience. Through the incorporation of standard qualitative approaches with computational techniques, the framework entails both the interpretive richness of human analysis and the structural precision of NLP.

V. DISCUSSION

Text Analysis:



Topic modelling exercise carried out for the sake of this study yielded a wealth of themes that collectively comprehensively reflect the multi-dimensional role of artificial intelligence in fraud detection within the digital economy. There was one which was prominent which tracked persistence of long-established fraud modes despite increasing use of AI-based methods, hypothesizing perhaps a deviation from response to anticipation-oriented measures as researchers and regulators underscore preventive as compared to response mechanisms and regulatory arrangements. The other dominating theme highlighted learning systems and smart data processing, where issues of false positives, concealed anomalies, and transparency-limited problems continue to be current challenges in maintaining fraud detection reliability.

A third thematic cluster was discovered around regulatory compliance and forward-looking management, highlighting the urgent necessity for AI systems that can detect fraud along with ensuring governance requirements and risk-

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

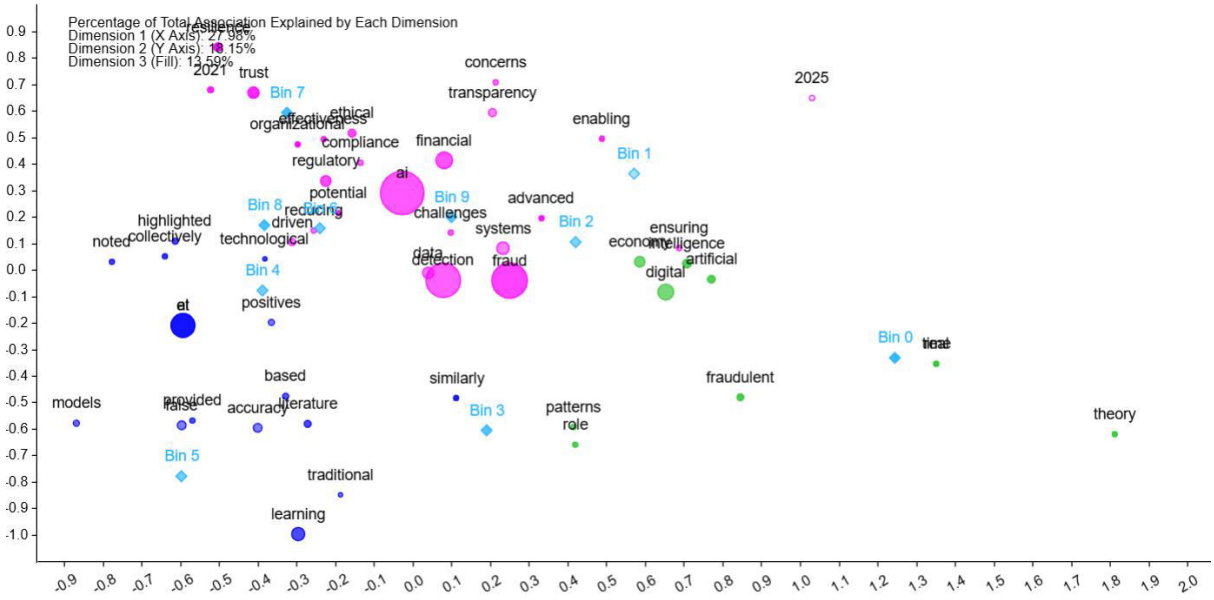
Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501051|

avoidance measures. symptomatic of this was a second cluster that highlighted trust, tech development, and machine efficiency, demonstrating how AI-driven systems are increasingly seen as being capable of promoting credibility and resilience in digital payments. Likewise, accuracy, privacy, transparency, and anomaly detection themes showcased inherent trade-offs between effectiveness and ethical concerns with AI adoption.

In addition, the discussion revealed topics related to ethical issues, adaptive practices, and implementation challenges, which indicate the difficulties organizations encounter in operationalizing AI models ethically. Supplementing this are clusters on theoretical resilience, organization efficiency, and customer trust, which indicate that the transformational potential of AI can be beyond fraud detection to enhancing systemic confidence in digital platforms. Other significant themes, including cybersecurity, accountability, fairness, and mitigating information asymmetry, suggest that AI is not a technical solution but an instrument for the mitigation of financial system structural vulnerabilities.

Text clustering:



Principal Component Analysis (PCA) identified three clusters that capture the underlying dimensions to position artificial intelligence within the field of fraud detection in the digital economy. The first cluster is highly related to words like fraudulent, digital, artificial intelligence, economy, and theory, which reflects a theoretical and conceptual strategy. This grouping summarizes the academic controversy that places the detection of fraud as an issue of a systemic nature influenced by technology uptake and its effect to digital fiscal environments. The second cluster, based on regulatory, compliance, transparency, ethical issues, trust, and organizational competency themes, summarizes the ethics and governance aspect. This cluster describes how regulator pressures, justice, and accountability play out in the acceptance and support of AI-based fraud detection models. The third set of terms, including data, systems, challenges, advanced, accuracy, and models, is the technical and operational view, where the discussion focuses on the capabilities, bounds, and operation constraints of AI algorithms in real life.

Interpreting all the clusters together, PCA indicates that the language of AI-powered fraud detection is not monolithic but is framed in three interlocking spheres: theoretical-conceptual underpinning, regulatory-ethical supervision, and technical-operational implementation. Theoretical cluster provides the foundation for fraud realization in the digital economy, regulatory cluster provides legitimacy and public confidence, and technical cluster is directed towards the practical implementation of detection systems. The three strongest factors captured explained variance (27.95% for Dimension 1, 18.15% for Dimension 2, and 13.59% for Dimension 3) demonstrates that while each group is unique, as a group, they display an overall representation of the multi-dimensionality of the study issue.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

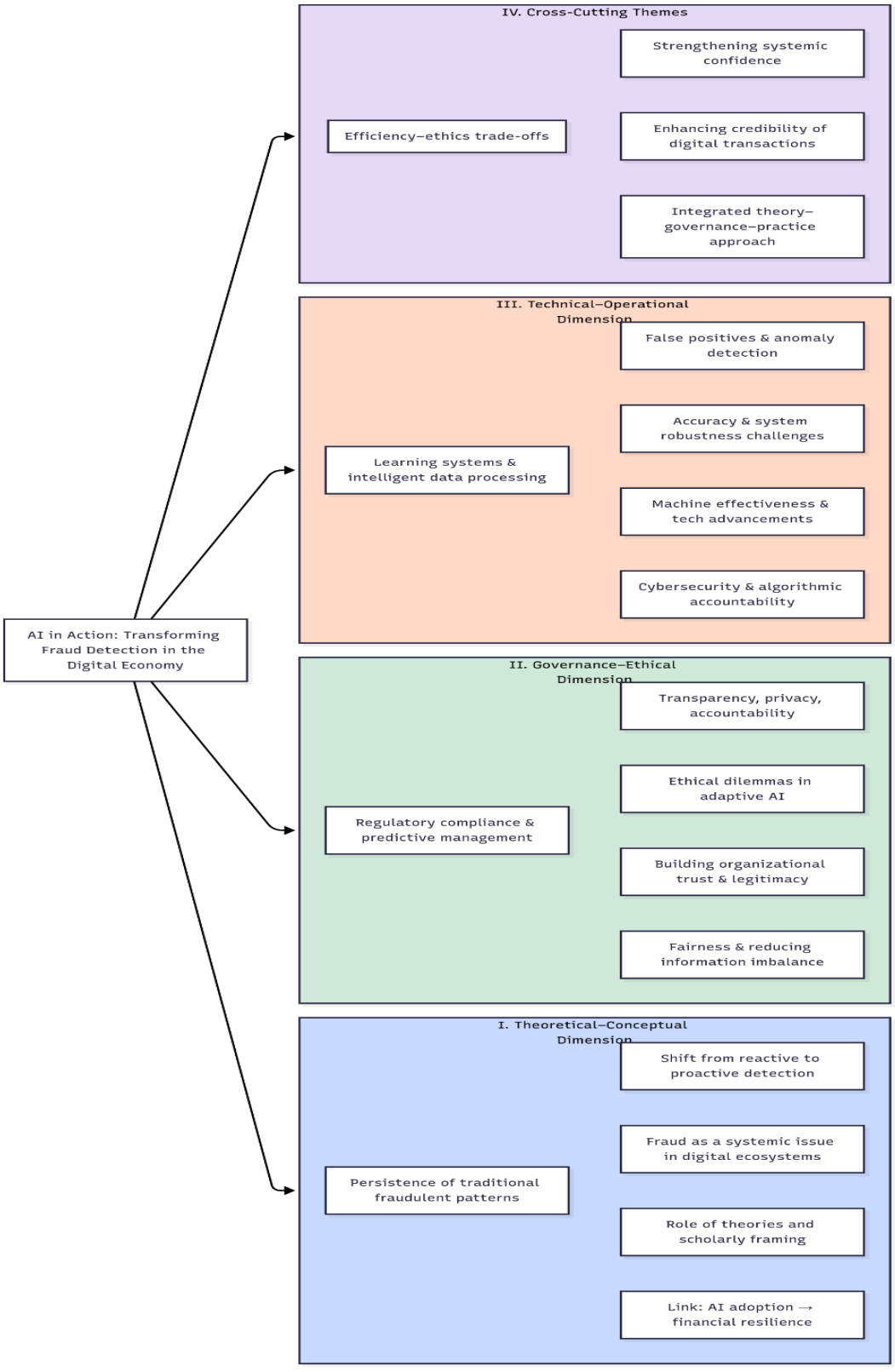
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501051|

Thematic Analysis:



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501051|

Conceptual framework shows how AI-based fraud detection in the digital economy spans four interlinked dimensions: theoretical–conceptual, governance–ethical, technical–operational, and cross-cutting topics. Theoretical dimension describes consistency in fraudulent patterns and shift to proactive detection from reaction mode, positions fraud as a problem of the system. Governance–ethical level emphasizes importance of transparency, accountability, fairness, and establishment of trust handling ethical issues in adaptive AI. At the technical–operational level, they also form the ongoing tension between operational reliability and technological innovation: system robustness, anomaly detection, cybersecurity, and false positives. Last but not least, the cross-cutting themes reinforce the top-level considerations, such as efficiency–ethics trade-offs, systemic confidence, and integration of theory–governance–practice. Cumulatively, these levels show that while AI dramatically enhances fraud prevention, its utility relies on balancing technological advancement with moral guidance, regulatory flexibility, and systemic trust, ultimately positioning AI as a revolutionary but responsible force for protecting the digital economy.

VI. CONCLUSION

The research aimed to analyze the innovative role of artificial intelligence in detecting fraud in the digital economy by following a qualitative research approach with thematic synthesis and natural language processing methods. The results of the research illustrated the intersectionality of technological innovation, ethical concerns, and system thinking in introducing AI, which indicated an overall vision towards opportunity along with challenges. By integrating theoretical perspectives with industry insights, the research developed a conceptual framework that underscores AI's dual role as a powerful tool for fraud prevention and as a source of new complexities in governance and trust. While the research contributes to academic knowledge, it also extends practical guidance for managers and policymakers, thereby bridging theory and practice.

Managerial Implications

For professionals, the study also underscores the importance of adopting a balanced approach towards using AI systems for detecting fraud. Financial institution and online business managers are not merely concerned with technical precision but also with guaranteeing the interpretability and ethics compliance of AI tools. Adequate explanation of AI-based decision-making can increase user trust and skepticism. Additionally, AI deployment in fraud detection calls for investment in training and organizational restructuring because human intervention is still indispensable in an attempt to counter the weaknesses of automated systems. These findings prompt managers to view AI as a supplementary vehicle, rather than a substitute for human judgment, to enhance resistance to morphing fraudulent schemes.

Research Implications

From an academic perspective, the study adds to the widening of debate on AI through the theory-driven, technical, and ethical integration in it. It shows how qualitative methods augmented with NLP-driven text analysis can be employed to identify subtlety in themes in emerging areas of digital finance. The methodology syncretism between human-cued thematic synthesis and computational topic modeling and clustering illustrates how interdisciplinary research can lead to a finer understanding. Of particular note is that the article identifies a gap in research at the nexus of AI regulation, fraud examination, and trust building, and urges researchers to close gaps among computer science, behavioral finance, and information systems research.

Theoretical Implications

Theoretically, the study broadens the understanding of fraud detection as it positions AI within existing paradigms like the Fraud Triangle Theory, Risk Management Theory, and Socio-Technical Systems Theory. Results indicate that AI is more than a mere technical solution but indeed a socio-technical phenomenon subject to ethical, regulatory, and human factors. This helps facilitate theory-building in that it illustrates how AI remakes organizational conduct, system resilience, and understandings of trust within digital economies. The research also highlights the importance of interpretability and transparency as emerging theoretical ideas that require integration into forthcoming fraud detection models.

Future Directions

Although such analysis in this paper was emphasized in terms of qualitative synthesis with limits to introduction and literature review, subsequent studies can delve deeper into analysis on empirical datasets through transaction data, case studies, or experimental simulations. Longitudinal studies can potentially provide information regarding how AI fraud

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501051|

detection systems develop over time as new forms of cybercrime emerge. There is also room for comparative sectoral and geographical analysis in order to explore how cultural, regulatory, and economic environments influence the take-up of AI tools and the implications thereof. Lastly, since explainable AI and ethics are future areas of concern, future research should look into how transparency instruments and accountability mechanisms influence stakeholders' trust in AI-based fraud detection systems.

REFERENCES

1. Business Insider. (2025, May 22). *From fighting fraud to fueling personalization, AI at scale is redefining how commerce works online*.
2. TechRadar. (2025). *Smarter than the scam: how optimized AI is reshaping fraud detection*.
3. Wall Street Journal. (2025). *AI drives rise in CEO impersonator scams*.
4. SmartDev. (2025). *How AI is transforming financial fraud detection in 2025: Challenges & Future Trends*.
5. Ledde, A. (2025). *AI-powered fraud detection: Transforming security across major sectors in the digital age*.
6. Awosika, T., Shukla, R. M., & Pranggono, B. (2023). Transparency and privacy: The role of Explainable AI and Federated Learning in financial fraud detection.
7. Ahmad, T., Wang, J., & Xu, H. (2020). Security in the digital economy: The role of explainable artificial intelligence. *Journal of Information Security and Applications, 53*, 102529. https://doi.org/10.1016/j.jisa.2020.102529
8. Alazab, M., Awajan, A., Mesleh, A., Abraham, A., Alhyari, S., & Alazab, M. (2020). Intelligent mobile malware detection using permission requests and API calls. *Future Generation Computer Systems, 107*, 509–521. https://doi.org/10.1016/j.future.2020.02.001
9. Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. *International Conference on Computing Networking and Informatics*, 1–9. https://doi.org/10.1109/ICCNI.2017.8123782
10. Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waterschoot, S., & Bontempi, G. (2018). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications, 41*(10), 4915–4928. https://doi.org/10.1016/j.eswa.2014.02.001
11. Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences, 479*, 448–455. https://doi.org/10.1016/j.ins.2017.12.030
12. Zengin, A., Dalkilic, G., & Sahin, O. (2021). Fraud detection in e-commerce transactions using machine learning. *Procedia Computer Science, 191*, 254–261. https://doi.org/10.1016/j.procs.2021.07.033
13. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016
14. Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Cost sensitive credit card fraud detection using Bayes minimum risk. *2013 12th International Conference on Machine Learning and Applications*, 333–338. https://doi.org/10.1109/ICMLA.2013.66
15. Buda, M., Maki, A., & Mazurowski, M. A. (2018). A systematic study of the class imbalance problem in convolutional neural networks. *Neural Networks, 106*, 249–259. https://doi.org/10.1016/j.neunet.2018.07.011
16. Chen, J., Wang, Y., & Zhao, L. (2020). A hybrid machine learning approach for credit card fraud detection. *Journal of Ambient Intelligence and Humanized Computing, 11*, 1–12. https://doi.org/10.1007/s12652-019-01515-8
17. Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waterschoot, S., & Bontempi, G. (2018). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications, 41*(10), 4915–4928. https://doi.org/10.1016/j.eswa.2014.02.001
18. Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences, 479*, 448–455. https://doi.org/10.1016/j.ins.2017.12.030
19. Ahmad, T., Wang, J., & Xu, H. (2020). Security in the digital economy: The role of explainable artificial intelligence. *Journal of Information Security and Applications, 53*, 102529. https://doi.org/10.1016/j.jisa.2020.102529

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501051|

20. Alazab, M., Awajan, A., Mesleh, A., Abraham, A., Alhyari, S., & Alazab, M. (2020). Intelligent mobile malware detection using permission requests and API calls. *Future Generation Computer Systems, 107*, 509–521. https://doi.org/10.1016/j.future.2020.02.001
21. Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology, 27*(2), 91–121. https://doi.org/10.1093/ijlit/eay017
22. Bryson, J. J., & Theodorou, A. (2019). How society can maintain human-centric artificial intelligence. In V. C. Müller (Ed.), *Philosophy and Theory of Artificial Intelligence 2017* (pp. 305–323). Springer. https://doi.org/10.1007/978-3-319-96448-5_26
23. O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.
24. Zeng, Y., Lu, E., & Huangfu, C. (2021). Linking artificial intelligence principles. *Computer, 54*(7), 27–36. https://doi.org/10.1109/MC.2021.3081965
25. Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., & Santamaría, J. (2021). Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data, 8*(1), 53. https://doi.org/10.1186/s40537-021-00444-8
26. Ghosh, S., Ghosh, S., & Reza, M. (2019). Artificial intelligence in financial fraud detection: A systematic literature review. *Journal of Financial Crime, 26*(4), 1001–1020. https://doi.org/10.1108/JFC-11-2018-0121
27. Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2021). From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics, 27*(4), 1–28. https://doi.org/10.1007/s11948-021-00305-3
28. Schuetz, S., & Venkatesh, V. (2020). Research perspectives: The rise of artificial intelligence and the implications for knowledge sharing, trust, and financial resilience. *Journal of the Association for Information Systems, 21*(2), 224–236. https://doi.org/10.17705/1jais.00607
29. Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2020). Critical analysis of big data challenges and analytical methods. *Journal of Business Research, 70*, 263–286. https://doi.org/10.1016/j.jbusres.2016.08.001
30. Zeng, Y., Lu, E., & Huangfu, C. (2021). Linking artificial intelligence principles. *Computer, 54*(7), 27–36. https://doi.org/10.1109/MC.2021.3081965
31. Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences, 479*, 448–455. https://doi.org/10.1016/j.ins.2017.12.030
32. Ghosh, S., Ghosh, S., & Reza, M. (2019). Artificial intelligence in financial fraud detection: A systematic literature review. *Journal of Financial Crime, 26*(4), 1001–1020. https://doi.org/10.1108/JFC-11-2018-0121
33. Sahu, S., Dash, R., & Majhi, B. (2020). Credit card fraud detection using adaptive random forest classifier. *Procedia Computer Science, 167*, 254–262. https://doi.org/10.1016/j.procs.2020.03.236
34. West, D. M., & Bhattacharya, A. (2016). How artificial intelligence is transforming the financial industry. *Brookings Institution Report*. Retrieved from https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-financial-industry/
35. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology, 10*(2), 1–19. https://doi.org/10.1145/3298981
36. Zhang, Z., Cui, Y., & Chen, J. (2021). Explainable artificial intelligence in fraud detection: Opportunities and challenges. *Journal of Ambient Intelligence and Humanized Computing, 12*(3), 2595–2608. https://doi.org/10.1007/s12652-020-02634-3

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details