International Journal of Social Sciences and Management Review

Volume: 08, Issue: 05 September - October 2025

ISSN 2582-0176

ADVANCING ANOMALY AND FRAUD DETECTION IN BIG DATA WITH ARTIFICIAL INTELLIGENCE

MOHAMMED KASHIF,
Jamia Millia Islamia University, New Delhi, India

ABDUL RAHMAN JIBRAN SYED,
Lewis University, IL, USA

MUBASHIR ALI AHMED
University of the People, CA, USA

https://doi.org/10.37602/IJSSMR.2025.8526

ABSTRACT

The digital transformation across industries has generated unprecedented volumes of Big Data, creating opportunities for innovation while increasing vulnerability to anomalies and fraud. Traditional detection methods lack the scalability and accuracy required for such complex, high-dimensional data streams. This paper explores the role of AI—leveraging machine learning, deep learning, reinforcement learning, and hybrid approaches—in overcoming these limitations. Case studies from finance, healthcare, cybersecurity, e-commerce, and telecommunications demonstrate the effectiveness of AI models, including autoencoders, isolation forests, and neural networks, in detecting sophisticated fraud patterns. Challenges such as data imbalance, real-time processing, interpretability, and ethical concerns like privacy and bias are also addressed. The paper highlights future directions in explainable AI, federated learning, and edge-based systems to support transparent, scalable, and privacy-aware anomaly detection in Big Data environments.

Keywords: artificial intelligence (AI), fraud detection, anomaly detection, big data analytics, machine learning, deep learning, real-time monitoring, data privacy, explainable AI (XAI), imbalanced data, cybersecurity, financial fraud, federated learning, edge AI, and pattern recognition.

1.0 INTRODUCTION

Data from various sources, including social media, financial transactions, IoT sensors, e-commerce websites, and cloud infrastructure, has led to a Big Data boom in today's hyperconnected digital world [1]. Even though this vast amount of data encourages new services and forward-thinking, it also creates an environment that is conducive to criminals taking advantage of weaknesses through fraud, cyberattacks, and other strange activities [2]. In a variety of fields, including as computer security, finance, insurance, telephone, and medicine, their recognition is highly appreciated. However, the velocity, volume, and variety of data are too much for the systems that are in place now, which mostly rely on statistical modelling, human verification, and pre-coded rules.

The detection of anomalies and fraud trends has been revolutionized by artificial intelligence (AI) technologies based on machine learning (ML), deep learning (DL), and reinforcement

Volume: 08, Issue: 05 September - October 2025

ISSN 2582-0176

learning (RL) [3]. With minimal to no human involvement, artificial intelligence (AI) products have the potential to identify underlying patterns, learn from past experiences, and adjust to novel behaviours. This is especially helpful for Big Data applications that need to be accurate, scalable, and fast. Artificial intelligence (AI) has proven to be more accurate and adaptable than conventional techniques in a variety of applications, such as identifying insider threats on corporate networks and questionable credit card activities [4].

Detecting fraud is made more difficult by shifting fraud patterns, noisy real-world data, and highly skewed data (where real transactions often outnumber fraudulent ones). False positives can be expensive in sectors like banking, finance, and healthcare where business operations are crucial. Because of this, there is a pressing demand for AI systems that can function in real time in a Big Data context and are robust and explicable [5].

Giving a thorough overview of the application of artificial intelligence (AI) to the detection of anomalies and fraud in large datasets is the aim of this study [6]. The present state of artificial intelligence is examined in this study, including hybrid frameworks, supervised and unsupervised learning, ensemble techniques, and neural network architecture. It illustrates the advantages and drawbacks of current systems with real-world case studies and actual deployment scenarios from a range of businesses.

Additionally, the research discusses significant issues including model interpretability, data privacy, and ethics. With a focus on cutting-edge technologies like explainable AI (XAI), federated learning, and AI at the edge, it outlines a future research approach [7]. By developing data systems that can fend off attacks brought on by new anomalies, our research helps to make data systems safer, smarter, and more accountable.

2.0 BACKGROUND AND LITERATURE REVIEW

After decades of research in data mining, statistics, and security, artificial intelligence (AI) has long been used to identify abnormalities and fraud [8]. However, a number of new challenges that traditional approaches are unable to handle have surfaced as Big Data technology has advanced. The shortcomings of current methods, developments in fraud detection technology, and how more sophisticated AI frameworks are revolutionizing this important topic are all covered in this part [9]

A. Traditional Approaches for Anomaly and Fraud Detection

Anomalies were previously found by statistical methods such time series analysis, logistic regression, and linear regression [10]. Rule-based systems are also frequently used in financial and network systems, producing alarms according to predetermined criteria. Low-volume applications can benefit from their utilization, but they have trouble adjusting to shifting patterns and perform poorly in Big Data scenarios that involve high-dimensional, unstructured, or streaming data.

B. Evolution of Machine Learning Methods

Because machine learning allows models to learn from historical data and generalize to new patterns, it has sparked a paradigm shift. Support Vector Machines (SVM), Random Forests,

Volume: 08, Issue: 05 September - October 2025

ISSN 2582-0176

and Decision Trees are examples of supervised learning algorithms that have been popular in well-formatted fraud detection applications [11]. Meanwhile, unsupervised learning methods such as k-means clustering, Isolation Forests, and DBSCAN have also become effective for finding anomalies without labelled training data. These techniques showed improved detection rates and adaptability.

C. Emergence of Deep Learning and Combined Models

Deep learning has brought greater sophistication, with models able to learn complex features from raw data. Autoencoders are used heavily for anomaly detection in data compression and reconstruction, flagging significant anomalies as abnormal. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks have been helpful in handling sequential transactional data [12]. Hybrid methods integrating supervised and unsupervised learning or mixed AI approaches have emerged to improve robustness and performance.

D. Gaps in Existing Work

While such developments have occurred, many challenges still exist. The majority of AI models are "black boxes" and thus render their decisions difficult to interpret [13]. In addition, little research has been conducted on integrating explainability, privacy protection, and real-time adaptability in AI-based fraud detection systems. The scalability of deep learning techniques in resource-constrained environments is also an open problem [14].

Table 1: Comparative Overview of AI Methods for Fraud Detection

Technique	Type	Strengths	Limitations
Logistic Regression	Statistical	Simple, interpretable	Limited to linear relationships
Decision Trees	Supervised ML	Easy to interpret, fast	Prone to overfitting
Isolation Forest	Unsupervised ML	Efficient for anomaly detection	Poor performance on clustered anomalies
Autoencoders	Deep Learning	Captures complex patterns	Lack interpretability
RNN/LSTM	Deep Learning	Good for sequential/temporal data	Computationally expensive
Hybrid ML + DL Models	Hybrid	Increased accuracy and robustness	High complexity, integration challenges

3. Anomaly and Fraud Detection Techniques using AI

Artificial Intelligence has transformed the paradigm of fraud detection and anomaly detection in Big Data by enabling systems to find sophisticated, dynamic patterns with minimal intervention by humans [15]. This section classifies AI techniques into supervised, unsupervised, deep learning, and reinforcement learning techniques, each offering particular strengths in managing various fraud scenarios.

A. Supervised Machine Learning Techniques

Supervised learning employs labelled data to train models to differentiate between normal and anomalous or fraudulent patterns [16].

a. Common methods are:

1) **Decision Trees and Random Forests:** Precise and interpretable models appropriate for transactional fraud detection.
2) **Support Vector Machines (SVM):** Appropriate for binary classification and are known to project high-dimensional data into a lower-dimensional feature space [17].
3) **Logistic Regression:** It is extensively used in banks because it is easy to interpret and simple.

Nevertheless, supervised models rely heavily on high-quality labelled data, which in fraud detection are severely limited by fraud's rarity and varying nature.

B. Unsupervised Machine Learning Techniques

Unsupervised learning is most suited where there is no labelled data. These methods identify abnormal deviations from normal behaviour [18].

1) **K-Means Clustering:** Clusters comparable data points and marks outliers as possible anomalies.
2) **Isolation Forest:** Isolates anomalies based on the fact that anomalies are rare and distinctive.
3) **DBSCAN:** Finds dense clusters and marks low-density points as outliers [19].

These techniques are good for zero-day fraud detection but can be bad in accuracy in noisy or high-dimensional data landscapes.

C. Deep Learning Techniques

Deep learning facilitates the representation of non-linear, high-level abstractions in big data [20]:

1) **Autoencoders:** Trained to recreate input data; big reconstruction error means there is an anomaly [21].
2) **Convolutional Neural Networks (CNNs):** Used for spatial patterns of fraud, i.e., image-based identity verification fraud.
3) **RNNs and LSTMs:** Ideal for sequential data such as credit card transaction history and network traces.

While deep learning models are extremely accurate, they are "black-box" in nature, hence difficult to interpret [22].

D. Reinforcement Learning and Hybrid Models

Reinforcement Learning (RL) is a newer paradigm in which agents learn to find optimal detection strategies by interacting with an environment [23]:

1) RL agents learn to actively update fraud detection thresholds over time.
2) Hybrid models blend several approaches (e.g., decision trees and CNNs) to take advantage of each's strengths.

These are research-oriented in nature but hold promising promise in real-time adaptive systems for anomaly detection.

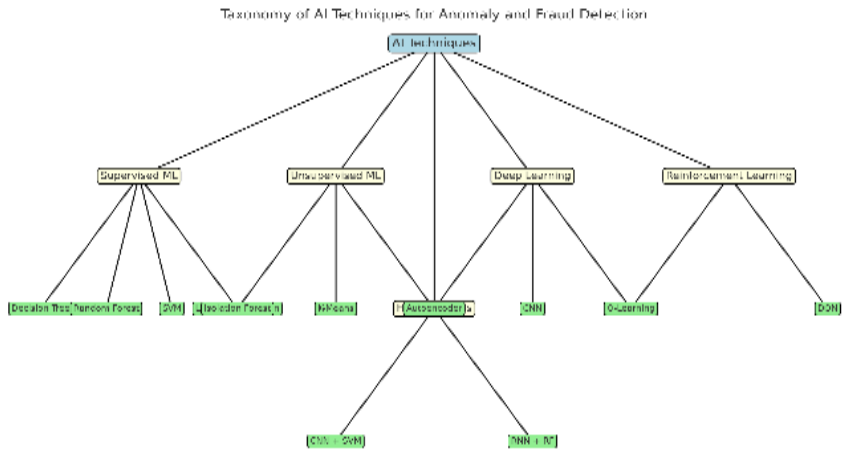


Figure 1: AI Techniques for Fraud and Anomaly Detection

4.0 APPLICATIONS AND CASE STUDIES

AI-powered anomaly and fraud detection systems are increasingly being applied in an increasingly broad range of industries, from the finance and healthcare sectors and e-commerce and cybersecurity [24]. These applications help to demonstrate the practical value of machine learning and deep learning algorithms in real-world applications of detecting concealed patterns, reducing false positives, and maintaining pace with changing patterns of threats [25].

A. Banking and Financial Services

Fraud detection in the financial sector prevents unauthorized transactions, identity theft, and account takeovers [26]. AI models examine transaction patterns, user location, frequency, and amount to determine suspicious transactions in real-time.

B. Case Study:

Visa and Mastercard employ AI-powered transaction monitoring systems driven by neural networks and decision trees to detect high-risk transactions in milliseconds [27]. Models are continuously updated through customer behaviour analysis and outlier scores, thus making them extremely effective in reducing levels of chargeback fraud.

C. E-commerce and Retail

Online retailer sites are vulnerable to various forms of fraud, including the establishment of false accounts, return fraud, and abuse of promotions. Algorithmic models utilizing deep

Volume: 08, Issue: 05 September - October 2025

ISSN 2582-0176

learning, like isolation forests and unsupervised clustering, detect outliers in customer account, payment, and delivery behaviour [28].

D. Case Study

Deep learning tools such as RNNs are used by Amazon to analyse clickstreams and purchase history to identify spurious purchasers and questionable vendors [29]. Feedback loops are utilized by the system to adjust models because fraud methods evolve.

E. Healthcare and Insurance

Medical fraud involves billing for services not received, payment for services twice, or up coded procedures [30]. AI is applied to analyse electronic health records (EHRs) and insurance claims for inconsistencies.

F. Case Study:

UnitedHealth Group employed ML classifiers to review claims data and EHRs and detected nearly $1 billion of fraudulent claims annually [31]. Decision trees and logistic regression models are applied, augmented with rule-based filters.

G. Cybersecurity and Network Monitoring

Intrusion Detection Systems (IDS) based on AI monitor network activity for malicious access patterns, data extraction, or denial-of-service attacks [32]. Real-time anomaly detection models execute algorithms on large-scale streaming big data.

H. Case Study:

DARPA Cyber Grand Challenge demonstrated AI agents, developed through reinforcement learning, to automatically detect and patch software system vulnerabilities in real-time [33].

Table 2: AI Applications in Domain-Specific Fraud Detection

Domain	AI Techniques Used	Application	Impact
Finance	SVM, RNNs, Autoencoders	Credit card fraud, identity theft	Real-time alerts, fewer false positives
E-commerce	Isolation Forest, Clustering	Fake reviews, account abuse	Reduced customer complaints
Healthcare	Decision Trees, Logistic Regression	Billing and claims fraud	Cost savings, faster claim validation
Cybersecurity	Reinforcement Learning, LSTM	Intrusion detection, malware spotting	Faster breach response, adaptive defence

5.0 LIMITATIONS AND CHALLENGES

Volume: 08, Issue: 05 September - October 2025

ISSN 2582-0176

Although AI has made considerable progress in anomaly and fraud detection in Big Data, its deployment is not without several significant challenges. These constraints cut across technical, operational, ethical, and practical domains. Understanding these challenges is important to come up with more secure, stable, and scalable AI-based solutions [34].

A. Data Imbalance and Quality Issues

Problems with anomaly and fraud detection are characterized by highly skewed datasets where the number of legitimate transactions is many times greater than the number of fraudulent transactions [35]. AI systems are prone to miss detections (false negatives) as a result of the skew, which tends to favour the majority class.

Additionally, model precision may be harmed by noisy, missing, or incomplete data—all of which are prevalent in real-world contexts. The process of labelling fraud data is quite laborious and prone to mistakes, which hinders the creation of practical supervised models [36].

B. Model Interpretability and Transparency

The majority of artificial intelligence (AI) systems, especially deep learning algorithms, are opaque and don't disclose anything about their decision-making process [37]. In high-risk sectors like finance and healthcare, where people need explanations for fraud detection results, transparency may be difficult.

Additionally, regulators demand that AI systems be explicable, especially when automated decisions have an impact on a customer's financial or legal status [38].

C. Real-time Processing and Scalability

Real-time decision-making across several data sources is necessary for anomaly detection in big data. The majority of AI models—especially deep learning models—cannot satisfy real-time latency requirements and are computationally costly [39].

Scalability is another challenge because AI systems need to handle massive volumes of dynamic data from numerous sources with high accuracy and few false positives.

D. Adversarial Attacks and Model Robustness

By taking advantage of model flaws and subtly changing data to make it invisible, attackers can change AI models [40]. In industries like banking and cybersecurity, where skilled scammers are always improving their tactics, the issue is particularly troublesome.

The model must be retrained frequently and incorporate adversarial defence techniques in order to achieve the necessary level of strength.

E. Ethical and Privacy Considerations

AI technologies often make it possible to access private and sensitive financial data. Important factors include public trust, privacy protection, and legal compliance (such as GDPR and

Volume: 08, Issue: 05 September - October 2025

ISSN 2582-0176

HIPAA) [41]. Moreover, biased algorithms may have discriminatory effects that disproportionately impact marginalized groups.

Bar figure Description: Severity of AI Challenges Across Domains

Domain	Data Imbalance	Interpretability	Real-time Needs	Security Risks	Privacy Risks
Finance	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Healthcare	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
E-commerce	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Cybersecurity	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Legend: = On a scale of 1 to 10, relative severity.

This bar graph illustrates the priorities and challenges faced by various sectors.

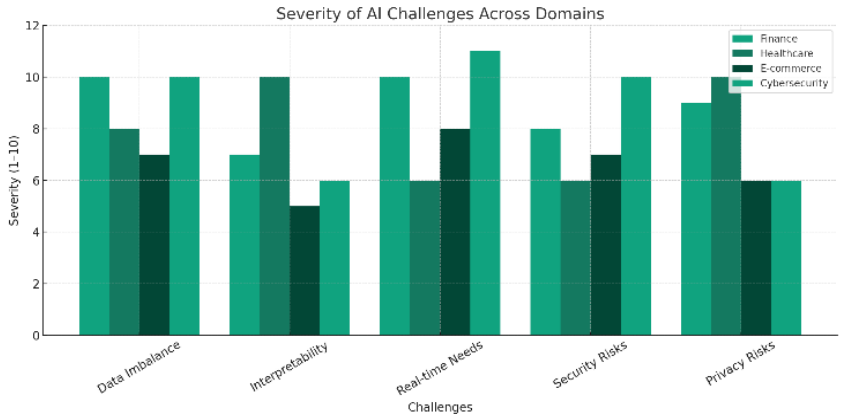


Figure 2: Severity of AI Challenges Across Domains

6.0 ETHICAL, LEGAL, AND PRIVACY CONCERNS

Although AI solutions for Big Data fraud and anomaly detection have a lot of promise, they also present significant privacy, legal, and ethical issues [42]. Fairness, accountability, and compliance must be guaranteed since more systems significantly affect healthcare access, financial decisions, and cyber security.

A. Ethical Concerns: Bias and Discrimination

The biases of society may be unintentionally reinforced by machine learning algorithms based on biased or historical data [43]. For instance, based on patterns seen in prior fraud cases, a fraud-detection system may routinely identify people of particular geographic regions or economic groups.

1) It has been alleged that credit-scoring algorithms utilize gender or race as proxy to discriminatorily deny loans.

2) **Ethical Risk:** Inadvertent bias will cause businesses to lose confidence and suffer reputational and social harm.

Mitigation strategies include bias auditing, diverse training data sets, and the implementation of explainable AI (XAI) to give open decision-making [44].

B. Legal Challenges: Compliance and Accountability

AI-driven fraud detection must adhere to a variety of regional and international laws, such as:

1) **GDPR (EU):** Gives the right to individuals to understand and contest automated decisions [45].
2) **HIPAA (US):** Maintains confidentiality and integrity of health information [46].
3) **RBI Guidelines (India):** Makes financial decisioning systems explainable [47].

But when AI models are black boxes that cannot be explained, it's difficult to blame anyone. Legal frameworks are lagging behind such technologies, and ambiguity is left for regulators as well as practitioners.

C. Privacy Risks: Data Security and Consent

Big Data ecosystems are based on the centralization of individuals' sensitive information on more than a single system and network [48]. Such data is continuously analysed for patterns by AI software developers, which leads to issues with informed consent, spying, and exploitation.

1) **Important Concern:** Local data protection laws may be broken by cross-border data transfers and cloud-based anti-fraud software [49].
2) **New solution:** Training models without a central party accessing raw data is made possible by federated learning and privacy-preserving techniques (such as differential privacy).

Line Diagram Explanation: Growing Concerns About Privacy, Ethics, and the Law (2020–2030)

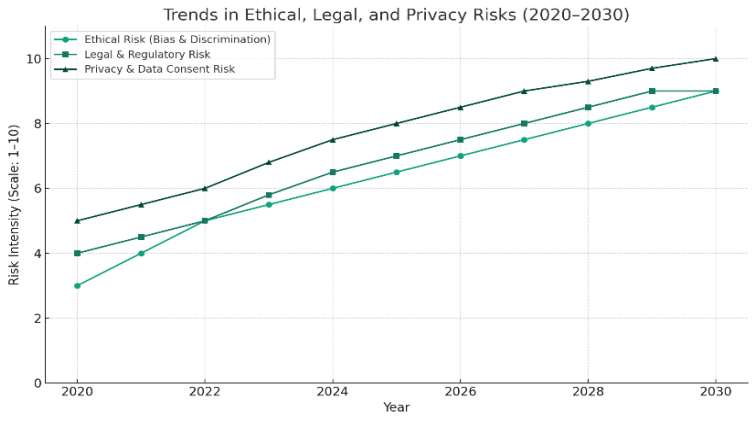


Figure 3: Trends in Ethical, Legal, and Privacy Risks (2020-2030)

Volume: 08, Issue: 05 September - October 2025

ISSN 2582-0176

All lines are rising, indicating a growing need for standards that need privacy-conscious designs, synchronized global legal frameworks, and ethical AI control.

7.0 FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

The future of AI in anomaly and fraud detection necessitates model, infrastructure, and policy innovation due to the increasing sophistication of Big Data settings and the increasing skill of fraudsters. The key areas of innovation that will influence the next ten years of AI-based fraud prevention are highlighted in this section [50].

A. Explainable and Interpretable AI (XAI)

Creating understandable and explainable AI models is one of the biggest challenges [51]. Authorities and businesses seek justifications for AI choices that impact the financial or legal standing of customers.

1) Additionally, research on model-agnostic explanation tools, interpretable deep models, and simple-to-use visualization dashboards in the future cannot be avoided.
2) Interoperability with the likes of GDPR would be a necessary requirement in order to stay ahead of the right to explanation.

B. Federated and Privacy-Preserving Learning

As privacy laws and challenges with cross-border data sharing become more common, federated learning will become more and more popular [52]. In these networks, decentralized training on edge devices is allowed without sending private information to central servers.

1) In federated situations, optimizations will concentrate on enhancing model accuracy, efficiency, and resilience to data poisoning assaults.
2) Security can be enhanced by synergistic techniques like differential privacy and homomorphic encryption.

C. Edge and Real-Time AI for Streaming Fraud Detection

AI models must be deployed at the edge, where the data is generated, in order to discover anomalies in real-time streaming Big Data [53].

1) Stream processing libraries, small deep learning models, and edge AI processors will all be included into next-generation systems.
2) For applications that need low latency, such as mobile banking, the Internet of Things, and smart cities, this is essential.

D. Adaptive and Continual Learning Systems

Fraud tactics quickly grow outdated. Static models quickly become outdated. New-generation AI systems need to facilitate adaptive learning, where models improve step by step without having to be retrained from scratch [54].

Volume: 08, Issue: 05 September - October 2025

ISSN 2582-0176

1) Thank you. Online learning, lifelong learning, and unsupervised drift detection will be investigated.
2) The systems will feed themselves and decrease reliance on retraining by hand.

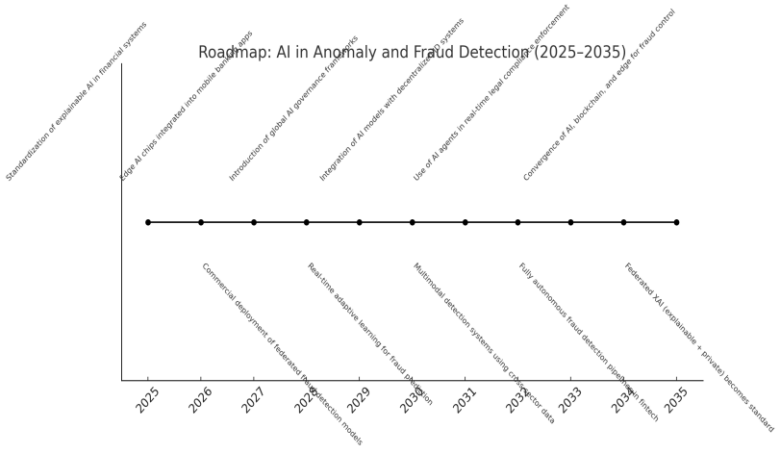
E. Cross-Domain and Multimodal Detection Paradigms

IoT, social media, and cloud environments are becoming integrated, and fraud is now not a solo phenomenon in a single realm [55].

1) The future paradigms will integrate text, voice, image, and transactional data to reveal complex fraud networks.
2) Graph-based and multimodal neural networks will take the lead.

Table 3: AI for Anomaly and Fraud Detection (2025–2035) Roadmap

Year	Milestone
2025	Standardization of explainable AI in financial systems
2026	Commercial deployment of federated fraud detection models
2027	Edge AI chips integrated into mobile banking apps
2028	Real-time adaptive learning for fraud prediction
2029	Introduction of global AI governance frameworks
2030	Multimodal detection systems using cross-sector data
2031	Integration of AI models with decentralized ID systems
2032	Fully autonomous fraud detection pipelines in fintech
2033	Use of AI agents in real-time legal compliance enforcement
2034	Federated XAI (explainable + private) becomes standard
2035	Convergence of AI, blockchain, and edge for fraud control



Volume: 08, Issue: 05 September - October 2025

ISSN 2582-0176

Figure 4: AI for Anomaly and Fraud Detection (2025–2035) Roadmap

8.0 CONCLUSION

The integration of Artificial Intelligence into anomaly and fraud detection has redefined how organizations navigate the challenges posed by the ever-growing volume, velocity, and complexity of Big Data. Following AI's development from conventional rule-based systems to complex, adaptive learning frameworks that can identify complex and new fraudulent patterns in industries like finance, healthcare, cybersecurity, and e-commerce, this study examined the scope and depth of AI's influence.

A thorough analysis of deep learning, reinforcement learning, supervised, unsupervised, and hybrid approaches shows that artificial intelligence (AI) improves the scalability, accuracy, and speed of fraud detection. Case study-based real-world applications demonstrate how they can lower financial loss, protect networks, and boost operational effectiveness. There are limitations and obligations associated with this transformative potential.

Concerns of class imbalance, data quality, real-time reaction needs, and model interpretability remain paramount. Since powerful deep learning algorithms are "black boxes," transparency and legal compliance are diminished. Additionally, using AI to make high-risk decisions has inevitable ethical, legal, and privacy repercussions. Global legal inconsistencies, explainability issues, algorithmic prejudice, and data theft all threaten the legitimacy and equity of AI systems.

It will take a comprehensive approach that combines technological innovation and robust governance to enable the safe and ethical deployment of AI to fraud detection in the future. The method presented here aims to replace existing reactive systems with AI systems that are transparent, self-governing, and protect privacy. The creation of interpretable AI models, the application of edge AI for real-time processing, federated learning for safe, decentralized training, and multimodal systems for merging data from various sources to better comprehend aberrant behaviour in context are the most important imminent developments.

Politicians, legal professionals, and AI researchers must also work together to create ethical standards and legal frameworks that safeguard both persons and businesses. Cross-border data governance, ethical AI development standards, and open auditing techniques are necessary to identify AI fraud.

In conclusion, despite the unknown and complex nature of the future, artificial intelligence (AI) can play a significant role in combating the sophisticated nature of fraud and anomalies in Big Data systems. By emphasizing creativity and ethical commitment, AI-based fraud detection could develop into not just clever and effective but also secure, equitable, and trustworthy, guaranteeing long-term worth and societal advantage.

REFERENCES

[1] Khadri, W., Reddy, J. K., Mohammed, A., & Kiruthiga, T. (2024, July). The Smart Banking Automation for High Rated Financial Transactions using Deep Learning. In

2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC) (pp. 686-692). IEEE.

[2] Aasimuddin, M., & Mohammed, S. AI-Generated Deepfakes for Cyber Fraud and Detection.

[3] Mohammed, A. K., & Ansari, M. A. (2024). The Impact and Limitations of AI in Power BI: A Review. International Journal of Multidisciplinary Research and Publications (IJMRAP),. Pp. 23-27, 2024., 7(7), 24–27.

[4] Kumar, P. (2024). Artificial intelligence and service flexibility in healthcare: Exploring the nexus. Asia Pacific Journal of Health Management, 19(2), 147-155.

[5] Li, L., & Zhang, J. (2021). Research and analysis of an enterprise E-commerce marketing system under the big data environment. Journal of Organizational and End User Computing (JOEUC), 33(6), 1-19.

[6] Chittoju, S. S. R., Kolla, S., Ahmed, M. A., & Mohammed, A. R. Synergistic Integration of Blockchain and Artificial Intelligence for Robust IoT and Critical Infrastructure Security.

[7] Bárcena, J. L. C., Daole, M., Ducange, P., Marcelloni, F., Renda, A., Ruffini, F., & Schiavo, A. (2022, January). Fed-XAI: Federated Learning of Explainable Artificial Intelligence Models. In XAI. it@ AI* IA (pp. 104-117).

[8] Bhargava, N., Bhargava, R., Rathore, P. S., & Agrawal, R. (Eds.). (2021). Artificial Intelligence and Data Mining Approaches in Security Frameworks. John Wiley & Sons.

[9] Irshad, A. (2024). Role of AI in Business Framework Revolution in Developed Countries. International Journal of Business & Computational Science, 1(1).

[10] Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. European Journal of Computer Science and Information Technology, 11(6), 84-102.

[11] Chittoju, S. R., & Ansari, S. F. (2024). Blockchain's Evolution in Financial Services: Enhancing Security, Transparency, and Operational Efficiency. International Journal of Advanced Research in Computer and Communication Engineering, 13(12), 1-5

[12] Ghojogh, B., & Ghodsi, A. (2023). Recurrent neural networks and long short-term memory networks: Tutorial and survey. arXiv preprint arXiv:2304.11461.

[13] Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., ... & Hussain, A. (2024). Interpreting black-box models: a review on explainable artificial intelligence. Cognitive Computation, 16(1), 45-74.

[14] Mighan, S. N., & Kahani, M. (2021). A novel scalable intrusion detection system based on deep learning. International Journal of Information Security, 20(3), 387-403.

[15] Himeur, Y., Elnour, M., Fadli, F., Meskin, N., Petri, I., Rezgui, Y., ... & Amira, A. (2023). AI-big data analytics for building automation and management systems: a survey, actual challenges and future perspectives. Artificial intelligence review, 56(6), 4929-5021.

[16] Khadri, S. W., Mohammed, I. K., Rasheed, H., & Gunda, S. K. R. (2025). Adaptive Trade Exception Handling in Financial Institutions: A Reinforcement Learning Approach with Dynamic Policy Optimization. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 19-23.

[17] Navia-Vázquez, A., Gutierrez-Gonzalez, D., Parrado-Hernández, E., & Navarro-Abellan, J. J. (2024). Distributed support vector machines. IEEE Transactions on Neural Networks, 17(4), 1091-1097.

[18] Syed, W. K., Mohammed, A., Reddy, J. K., & Dhanasekaran, S. (2024, July). Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures. In 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC) (pp. 1331-1336). IEEE.

[19] Fuchs, M., & Höpken, W. (2022). Clustering: hierarchical, k-means, DBSCAN. In Applied Data Science in Tourism: Interdisciplinary Approaches, Methodologies, and Applications (pp. 129-149). Cham: Springer International Publishing.

[20] Balammagary, S., Mohammed, N., Mohammed, S., & Begum, A. (2025). AI-Driven Behavioural Insights for Ozempic Drug Users. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 10-13.

[21] Bank, D., Koenigstein, N., & Giryes, R. (2023). Autoencoders. Machine learning for data science handbook: data mining and knowledge discovery handbook, 353-374.

[22] Zargar, S. (2021). Introduction to sequence learning models: RNN, LSTM, GRU. Department of Mechanical and Aerospace Engineering, North Carolina State University, 37988518.

[23] Abdulsamad, H., & Peters, J. (2023). Model-based reinforcement learning via stochastic hybrid models. IEEE Open Journal of Control Systems, 2, 155-170.

[24] Mohammed, A., Sultana, G., Aasimuddin, F. M., & Mohammed, S. (2025). Leveraging Natural Language Processing for Trade Exception Classification and Resolution in Capital Markets: A Comprehensive Study. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 14-18.

[25] Fan, D. P., Ji, G. P., Cheng, M. M., & Shao, L. (2021). Concealed object detection. IEEE transactions on pattern analysis and machine intelligence, 44(10), 6024-6042.

[26] Janamolla, K., Sultana, G. S., Aasimuddin, F. M., Mohammed, A. F., & Pasha, F. S. A. P. (2025). Integrating Blockchain and AI for Efficient Trade Exception Handling: A Case Study in Cross-Border Settlements. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 24-30.

[27] Mohammed, S., Vali, M. Q., & Mohammed, A. R. Securing Healthcare IT Systems: Addressing Cybersecurity Threats in a Critical Industry.

[28] Ntumba, C., Aguayo, S., & Maina, K. (2023). Revolutionizing retail: a mini review of e-commerce evolution. Journal of Digital Marketing and Communication, 3(2), 100-110.

[29] Alroobaea, R. (2022). Sentiment analysis on amazon product reviews using the recurrent neural network (rnn). International Journal of Advanced Computer Science and Applications, 13(4).

[30] Mohammed, S., Mohammed, N., & Sultana, W. (2024). A review of AI-powered diagnosis of rare diseases. International Journal of Current Science Research and Review, 7(09).

[31] Garry, E. M., Weckstein, A. R., Quinto, K., Lasky, T., Chakravarty, A., Leonard, S., ... & Gatto, N. M. (2021). Use of an EHR to inform an administrative data algorithm to categorize inpatient COVID-19 severity. medRxiv, 2021-10.

[32] Mohammed, N. U., Mohammed, Z. A., Gunda, S. K. R., Mohammed, A., & Khaja, M. U. Networking with AI: Optimizing Network Planning, Management, and Security through the medium of Artificial Intelligence.

[33] Dubber, T., & Lazar, S. (2025). Military AI Cyber Agents (MAICAs) Constitute a Global Threat to Critical Infrastructure. arXiv preprint arXiv:2506.12094.

[34] Gadicha, A. B., Maniyar, M. M., Gadicha, V. B., & Burange, M. S. (2025). Cloud-Based AI Security Solution. In Deep Learning Innovations for Securing Critical Infrastructures (pp. 181-206). IGI Global Scientific Publishing.

[35] Mohammed, Z., Mohammed, N. U. M., Mohammed, A., Gunda, S. K. R., & Ansari, M. A. A. (2025). AI-Powered Energy Efficient and Sustainable Cloud Networking. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 31-36.

[36] Igual, L., & Seguí, S. (2024). Supervised learning. In Introduction to Data Science: A Python Approach to Concepts, Techniques and Applications (pp. 67-97). Cham: Springer International Publishing.

[37] Delcaillau, D., Ly, A., Papp, A., & Vermet, F. (2022). Model transparency and interpretability: Survey and application to the insurance industry. European Actuarial Journal, 12(2), 443-484.

[38] Lepekh, S. (2022). Consumers of financial services: features of the legal status in the conditions of financial inclusion. Amazonia Investiga, 11(53), 308-319.

[39] Mohammed, A. K., Ansari, S. F., Ahmed, M. I., & Mohammed, Z. A. Boosting Decision-Making with LLM-Powered Prompts in PowerBI.

[40] Mohammed, A., Mohammed, N. U., Gunda, S. K. R., & Mohammed, Z. Fundamental Principles of Network Security.

[41] Aldboush, H. H., & Ferdous, M. (2023). Building trust in fintech: an analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. International Journal of Financial Studies, 11(3), 90.

[42] Ahmed, M. I., Mohammed, A. R., Ganta, S. K., Kolla, S. K., & Kashif, M. K. (2025). AI-Driven Green Construction: Optimizing Energy Efficiency, Waste Management and Security for Sustainable Buildings. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 37-41.

[43] Levey, S., & Cheng, L. R. L. (2022). The impact of bias and discrimination. Communication Disorders Quarterly, 43(4), 215-223.

[44] Wang, F., Harindintwali, J. D., Wei, K., Shan, Y., Mi, Z., Costello, M. J., ... & Tiedje, J. M. (2023). Climate change: Strategies for mitigation and adaptation. The Innovation Geoscience, 1(1), 100015-1.

[45] Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. Journal of Information Technology, 38(1), 16-44.

[46] Mandl, K. D., & Perakslis, E. D. (2021). HIPAA and the leak of “deidentified” EHR data. N Engl J Med, 384(23), 2171-2173.

[47] Rishi, D. (2023). RBI Guidelines on Mobile Banking Transactions in India (2008): A Comprehensive Analysis. Issue 2 Indian JL & Legal Rsch., 5, 1.

[48] Altamimi, H., Liu, Q., & Jimenez, B. (2023). Not too much, not too little: Centralization, decentralization, and organizational change. Journal of Public Administration Research and Theory, 33(1), 170-185.

[49] Adebowale, A. M., & Akinnagbe, O. B. (2023). Cross-platform financial data unification to strengthen compliance, fraud detection and risk controls. World J Adv Res Rev, 20(3), 2326-2343.

[50] Soyombo, O. T. (2024). Reviewing the role of AI in fraud detection and prevention in financial services. International Journal of Science and Research Archive, 11(1), 2101-2110.

Volume: 08, Issue: 05 September - October 2025

ISSN 2582-0176

[51] Dwivedi, R., Dave, D., Naik, H., Singhal, S., Omer, R., Patel, P., ... & Ranjan, R. (2023). Explainable AI (XAI): Core ideas, techniques, and solutions. ACM computing surveys, 55(9), 1-33.

[52] Yin, X., Zhu, Y., & Hu, J. (2021). A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. ACM Computing Surveys (CSUR), 54(6), 1-36.

[53] Immadisetty, A. (2025). Real-time fraud detection using streaming data in financial transactions. Journal of Recent Trends in Computer Science and Engineering (JRTCSE), 13(1), 66-76.

[54] Zhao, Y., Saxena, D., & Cao, J. (2023). AdaptCL: Adaptive continual learning for tackling heterogeneity in sequential datasets. IEEE transactions on neural networks and learning systems.

[55] Planamente, M. (2023). Multi-Modal Learning for Cross-Domain Analysis of Egocentric Action and Object Recognition.

