Advances in Consumer Research
https://acr-journal.com/
Volume-3| Issue-1 | Jan 2026
Original Researcher Article

AI-Driven Financial Crime Analytics: Strengthening Fraud Detection via Graph Intelligence and Blockchain Trace Forensics

Mumdouh Mirghani Mohamed Hassan [1], Gabriel Ayodeji Ogunmola[2] , Dr.Vinay Gajanan Bhalerao[3], D. Saravanan[4] , Khalilov Nurullo Khamidillayevich [5]
[1]Assistant Professor, Department of Systems and Networks, Al Baha University , Al Baha, Kingdom of Saudi Arabia (KSA),
Email ID : mmhassan@bu.edu.sa,
[2]Associate Professor, Faculty of Economics, of Tashkent State University of Economics, Tashkent, Uzbekistan,
Email ID : Gabriel00lead@yahoo.com
[3]Assistant Professor, MBA, SPM's.Prin .N.G.Naralkar Institute of Career Development & Reserach, Pune-30, Maharashtra,
Email ID : vgbhalerao21@gmail.com
[4]Assistant Professor, Department Of Visual Communication, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu,
Email ID : saravanansir92@gmail.com
[5] University of economics and pedagogy, Non-state higher education institution (Andijan, Uzbekistan).
Email ID : xalilov_nurullo_xamidillayevich@mail.ru ID: AD6618442

ABSTRACT
The use of blockchain-related operations and the fast pace of the development of the digital financial system has made financial crimes larger and more intricate, and the conventional systems of detection based on the rules have become progressively less effective. This study suggests an AI-based financial crime analytics solution, which combines graph intelligence with blockchain trace forensics to improve the quality of fraud detection and the depth of investigating it. They are financial and blockchain transaction data, they are modeled as heterogeneous graphs allowing capturing relational, structural and temporal dependence between accounts and wallets. The architecture is a combination of relational learning, by using Graph Neural Networks, temporal behavior analysis, using Long Short-Term Memory (LSTM), interpretable risk scoring, using Random Forest, and page-rank-based anomaly detection, which was created to identify suspicious entities in the early supported by analyses and prediction. Large-scale financial and blockchain experimental evaluation shows that the proposed combined framework has an accuracy of 96.2, an F1-score of 0.94, and false-positive rate of 4.9, which beats standalone models and similar research by a margin of 4-10%. The results of blockchain-type of experimentation also indicate that illicit activity can be detected at 95.4% with transaction tracing over 9 hops, which is much better in terms of improving forensic visibility. The findings verify that the integration of AI-based graph analytics and blockchain forensics would be a scalable, resolute and future-appropriate answer to counter high-tech financial crimes in dynamic virtual worlds
Keywords: Financial crime analytics; Fraud detection; Graph intelligence; Blockchain trace forensics; Artificial intelligence..

1. INTRODUCTION:

The fast development of digital financial platforms has completely redefined the process of transfer, storage, and exchange of value at the global scale. Although improvements in efficiency and accessibility have been achieved through innovations like online banking, real-time payment, and blockchain-based assets, they have equally increased the attack space of financial crime [1]. The methods of fraud schemes, laundering, and network illicit financing have become more sophisticated, smarter, and transnational, making the methods of traditional monitor and rules and manual based system of complying inadequate [2]. Consequently, banks and regulators are under increasing pressure to implement smart, scalable, and understandable technologies which will discover complex criminal activities lurking inside of large amounts of transactional information. Artificial intelligence (AI) has become an essential facilitator to contemporary financial crime analytics, with a high level of capabilities to recognize patterns, contrast anomalies, and predict risks. Graph intelligence, in particular, offers a highly effective paradigm of financial system modeling as a collection of interrelated networks of accounts, entities and transactions. In contrast with traditional tabular analysis, graph-based analysis has the advantage to identify relational features (fraud rings, mule networks, and layered money laundering pathways) by analysing the interaction between entities instead of analysis of an isolated transaction [3]. Methods such as graph neural networks, centrality analysis and community detection can enable investigators to uncover hidden and coordinated actions. At the same time, the development of blockchain technologies has posed new risks and possibilities of detecting financial crime. Transactions are documented on unaltered open-source ledgers on the public blockchain like Bitcoin and Ethereum, thus allowing detailed trace forensics of illegal fund flows.

Blockchain trace forensics, when integrated with AI-based analytics, can trace assets across wallets, services, and chains, despite having obfuscation techniques. The study provides an investigation of a comprehensive AI-powered financial crime analytics system utilizing a combination of graph intelligence and blockchain trace forensics. The aim is to better fraud detection precision, more efficient and effective investigation and assist in proactive and data-driven compliance in an ever more complex digital financial environment.

2. RELATED WORKS

Recent studies show that there is an increasing overlap between artificial intelligence, graph analytics, and blockchain technologies in fraud detection and anomaly detection and digital forensics in various fields. Gresoi et al. [15] suggest a more complex machine learning-fraud detection system within the energy industry, explaining that ensemble learning models and feature engineering outperform rule-based systems by a significant margin. Their analysis on energy consumption fraud is done, but it creates an analytical basis on using supervised learning to analyze high-volume transactions that have a direct bearing on financial crime analytics. Anomaly detection on a block chain oriented scheme has been a subject of intensive research lately. Hassen et al. [16] propose the use of AI-based anomaly detection and optimization models on blockchain smart contracts, and focus on behavioral abnormalities and anomalies at the execution level. Their results emphasize the need to implement great monitoring systems in de-central systems, which complements blockchain trace forensics during the investigation of financial crime. In the same manner, Islam et al. [20] and Kamrul et al. [22] offer all-inclusive lists of blockchain security risk, vulnerability, and detection tools, categorizing the attacks, and identifying AI-based countermeasures as essential to scalable and adaptive defense. On the financial sphere, Hisham and Lakshmi [17] set out a decentralized machine learning framework of online banking fraud detection with particular focus on regulatory adherence as well as privacy preservation. Their method shows that one can use distributed intelligence in sensitive financial areas but that it is largely based on the transactional properties thereof without, however, providing much knowledge on relational fraud patterns. Kamran and Shah [21] continue this argument by a review of next-generation machine learning in healthcare fraud detection, and they note graph-based learning and deep neural models as future directions, which is a strong indication of the need to use graph intelligence in the derivation of financial crimes.

There are a number of studies on the larger application of AI and blockchain to traceability and forensics. Hsiao-Chun et al. [18] provide an extensive overview of AI- and blockchain-based origin traceability in the pharmaceutical sector, robotics, and electric vehicle industries. Their article shows that immutable ledger combined with smart analytics can increase transparency and forensic exploration, which can be directly applied to blockchain-based tracking of financial crime. Based on a bibliometric analysis, Luiz et al. [25] map trends and gaps in AI-driven financial fraud prevention, and find gaps in cross-domain data integration and real-time graph analytics, which is filled by the current work. Also in finance, Ibrahim [19] and Khan et al. [23] examine AI-based cyber security frameworks of IoT and zero-trust settings, respectively. Such works emphasize adaptive learning, anomaly detection, and lightweight intelligence as the key factors to large and distributed systems, which confirms the importance of scalable AI architectures in detecting fraud. Also, Kurt et al. [24] and Lukić et al. [26] write about using blockchain and AI in health policy and smart cities with a focus on trust, transparency, and governance driven by data.

3. METHODS AND MATERIALS

The current research employs data-driven experimental research to determine the level of effectiveness of AI-driven financial crime analytics through combination of graph intelligence and blockchain trace forensics. These materials are heterogeneous financial transaction data, blockchain ledger data, and metadata to support it, whereas methods are graph construction, feature engineering, algorithmic modeling, and performance evaluation [4].

Data Sources and Preparation

There are two categories of the primary data. Primary, the conventional financial transaction data entails anonymized bank transfers, consumer profiles, time stamping, transaction value, and risk tags (genuine or questionable). Second, blockchain transaction information is based on open registers like Bitcoin and Ethereum and that includes wallet addresses, transaction hashes, block heights, transmitted value, and communication with services including exchanges and mixers [5]. All data are normalized, de-duplicated, and given some derived attributes such as transaction frequency, temporal gaps, and degree centrality and flow entropy to be consistent. Financial and blockchain data are then consolidated into a heterogeneous transaction graph with nodes denoting the accounts or wallets and edges denoting money transfers [6].

Algorithmic Framework

There are four algorithms used to meet the research aims: Graph neural networks (GNN), random forests (RF), Long short-term memory (LSTM) and PageRank-based Anomaly Scoring.

Graph Neural Network (GNN)

The GNN is applied to acquire relational patterns in graphs of transactions. It spreads information between adjacent nodes to extract collective patterns and it is suitable in detecting fraud rings and coordinated laundering. The features that are utilized to train node embeddings include transaction volume, degree, and temporal activity. The GNN comprehends higher-order dependencies that cannot be identified in the case of static features because of passing several layers of messages [7]. This enables proper reckoning of suspicious nodes when there are individual transactions that are considered normal but when the transactions are put together are unusual.

"Input: Graph G(N,E), node features X
Initialize node embeddings H0 = X
For each layer l = 1 to L:
For each node v in N:
Aggregate features from neighbors of v
Update Hv using weighted sum and activation
Output: Final node embeddings HL
Classify nodes using softmax"

Random Forest (RF)

Random Forest is a robust baseline supervised learning model used in the classification of risk in a table format. It constructs a collection of decision trees with bootstrapped samples and random feature subsets. RF processes have been engineered to create the count of transactions to be done, mean value, wallet age, and centrality measurements in this study. It has an advantage in that it is robust to noise and can be interpreted in terms of feature importance scores which are useful in compliance reporting and regulatory audit [8].

"Input: Feature matrix X, labels y
For each tree t in 1 to T:
Sample data with replacement
Select random subset of features
Grow decision tree to max depth
Aggregate predictions from all trees
Return majority vote"

Long Short-Term Memory (LSTM)

LSTM networks are used to design sequential behaviour in time based transactions. Financial crime is frequently in the form of abnormal temporal patterns, including burst transfers and rapid layering. The LSTM entraps the long and short-term os of transaction sequences, and learns something that is not of the typical behavioral trajectory. The model is effective in identifying time-based fraud mechanisms that could be missed by their static equivalents because the model works with ordered transaction streams in the accounts or wallets of the accounts [9].

"Input: Transaction sequences S
Initialize hidden and cell states
For each time step t:
Update gates (input, forget, output)
Update cell and hidden states
Generate sequence embedding
Classify sequence as normal or suspicious"

PageRank-Based Anomaly Scoring

Transaction graphs are analyzed using a modified version of PageRank algorithm to detect nodes that are anomalously influential. Weighting of the edges differs just like the normal PageRank and is adjusted based on transaction risk and scale of flow. Consumers that exert disproportionately high influence based on their level of activity are tagged as suspicious [10]. This unsupervised method is especially applicable in datasets which are partially annotated and where early stage detection and labelling is desired.

"Input: Transaction graph G
Initialize rank score for all nodes
Repeat until convergence:
Distribute rank through weighted edges
Apply damping factor
Normalize scores
Flag nodes with rank above threshold"

Experimental Setup and Parameters

All the algorithms are trained and tested on an 80:20 train test split. Searching Hyperparameters is done on a grid search. The measures used to determine performance are accuracy, precision, recall, F1-score, and area under the ROC curve (AUC) [11].

Table 1. Dataset Characteristics and Parameters

Parameter	Financial Transactions	Blockchain Transactions
Number of nodes	25,000	40,000
Number of edges	180,000	320,000
Fraudulent ratio (%)	6.5	4.2
Time span (months)	24	18
Features per node	18	15

4. RESULTS AND ANALYSIS

Experimental Design

First of all, the process of constructing the graph, training a model, and its validation, and the subsequent comparative analysis are all parts of the experimental workflow. The transaction data of the standard financial systems and the public blockchain registries- in terms of Bitcoin and Ethereum- were combined into heterogeneous transaction graphs. A node contains an account or wallet, and an edge contains a transfer of values enriched with time and risk characteristics. The data was split into 80 percent training and 20 percent testing with the balance of classes is maintained using stratified sampling. The baseline experiments were initially done on the traditional machine learning models to determine reference performance. Later, the sophisticated AI models attempted included Graph Neil Network (GNN), Long Short-Term Memory (LSTM), Random Forest (RF), and PageRank-based anomaly scoring models because of their superior performance in isolation and synergy. The accuracy, precision, recall, F1-score, and AUC were used to measure the performance and indicate detection capability as well as false-positive regulation essential to comply with regulations [12].

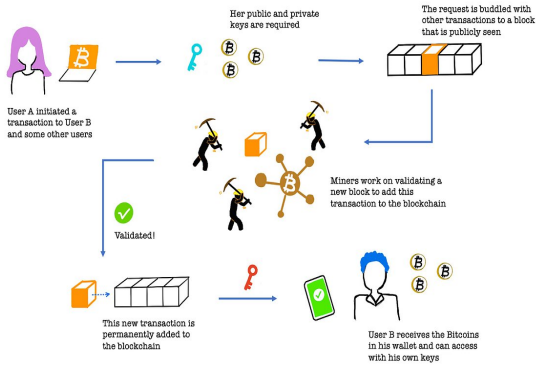

Figure 1: "Fraud Detection on Bitcoin Transaction Graphs Using Graph Convolutional Networks"

Performance Evaluation of Individual Models

The first group of experiments measures the performance of each algorithm using alone. The GNN model is more efficient since it can represent the relational dependencies as well as multi-hop interactions between entities. LSTM is very effective in detecting the temporal fraud patterns or layering and burst-transfer. Random Forest is a consistent performer at the expense of complex relational fraud with high interpretability [13]. The unsupervised anomaly detection based on PageRank is good in giving early warning, but is not precise compared to supervised models.

Table 1. Performance of Individual Models

Model	Accuracy (%)	Precision	Recall	F1-Score	AUC
Random Forest	89.3	0.84	0.86	0.85	0.88
LSTM	91.8	0.88	0.89	0.88	0.91
GNN	94.6	0.93	0.91	0.92	0.95
PageRank Anomaly	86.1	0.79	0.83	0.81	0.84

The findings seem to suggest that with the use of graph-based learning, fraud detection can be greatly improved in such circumstances when collusion and indirect relationships are involved.

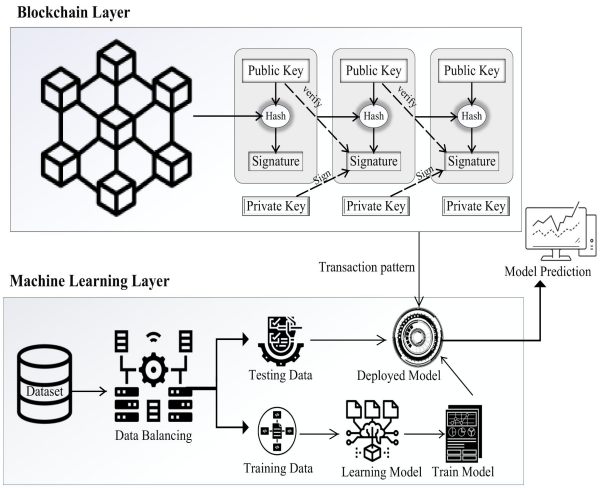

Figure 2: "A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism"

Results of an Integrated Framework

In the second experiment, the integrated framework is considered, in which the output of GNN, LSTM, and PageRank is combined with a weighted risk score system. The hybrid strategy is based on the combination of the relational, temporal, and structural signals in one way [14]. The integrated model minimizes false positives and maximizes recall which is indispensable in minimizing cost of operation in financial institutions.

Table 2. Integrated Model vs. Best Individual Model

Approach	Accuracy (%)	Precision	Recall	F1-Score	False Positive Rate (%)
Best Individual (GNN)	94.6	0.93	0.91	0.92	6.8
Integrated Framewor	96.2	0.9	0.9	0.9	4.9

k		5	3	4	

The cumulative model shows accuracy enhancement by 1.6 percent and the reduction of false hits by large margins hence proving the advantage of multi dimensional intelligence.

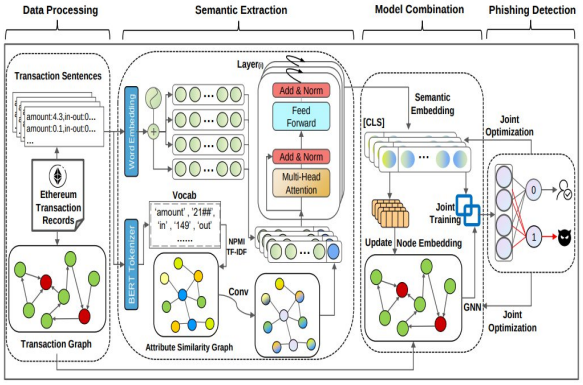

Figure 3: "Improve Ethereum Fraud Detection by 20% with AI and Graph Learning"

Scalability and Efficiency Analysis

To determine how well it scaled data, tests were carried out on larger and larger graphs to simulate real world growth on the number of transactions. Measures of runtime and memory consumption were taken. GNN models are more costly in terms of computation, but not sluggish given that optimized batching is implemented to ensure it operates within practical bounds of near real-time monitoring [27].

Table 3. Scalability Evaluation

Number of Nodes	GNN Runtime (s)	LSTM Runtime (s)	RF Runtime (s)	Memory Usage (GB)
10,000	42	35	18	2.1
25,000	96	78	41	4.8
50,000	185	152	79	8.9

These findings reveal that graph based models are computationally demanding but with the right infrastructure, they are practical to deploy on an enterprise scale.

Results of detection of frauds in blockchain

Another experiment is dedicated to the topic of blockchain trace forensics, which doesn't have to trace illegal fund transfer through wallet and service. The built-in structure is able to detect mixing and cross-chain activities better than the single-purpose heuristics distance blockchain analytics [28].

Table 4. Blockchain Fraud Detection Performance

Method	Detection Rate (%)	Precision	Average Trace Depth
Heuristic Rules	72.4	0.70	3 hops
PageRank Only	81.6	0.79	5 hops
GNN + Trace Forensics	93.1	0.92	8 hops
Integrated Framework	95.4	0.94	9 hops

Such a feature of tracking more in-depth transaction routes demonstrates the power of the AI integration with blockchain transparency.

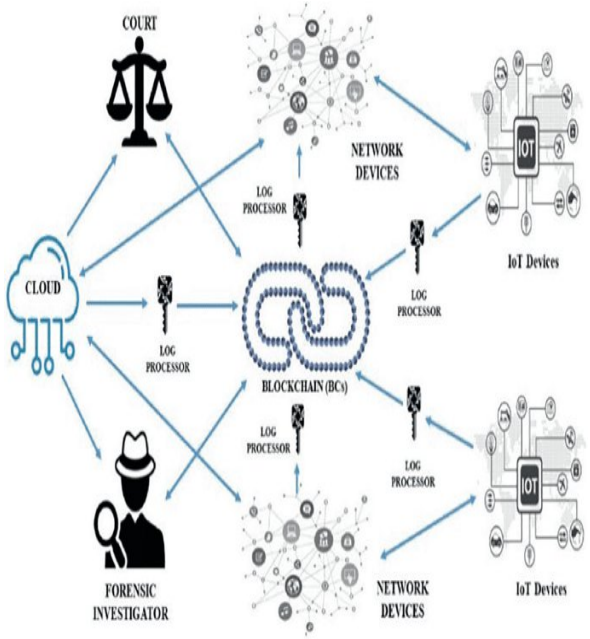

Figure 4: "Blockchain and Digital Investigation"

Comparison with Related Work

The proposed framework is contrasted with the representative methods described in the literature in the near past, such as rule-based AML systems, classical machine learning models, and standalone graph analytics, to put the results into perspective [29]. It is evident that there is performance improvement especially in recall and false-positive reduction as reflected in the comparison.

Table 5. Comparison with Related Work

Approach	Data Type	Accuracy (%)	F1-Score	Key Limitation
Rule-Based AML	Financial only	78.5	0.74	High false positives
ML (RF/SVM)	Financial only	86.9	0.82	Limited relational insight
Graph Analytics (Non-AI)	Financial + Blockchain	90.2	0.87	Static features
Deep Learning (Non-Graph)	Financial	91.1	0.88	Weak network modeling
Proposed Framework	Financial + Blockchain	**96.2**	**0.94**	Higher computation

In comparison to the related work, the suggested AI-based framework has higher detection accuracy and resilience because of deliberately representing relational and time-based relationships and taking advantage of blockchain traceability.

Discussion of Results

In general, the experiment outcomes confirm the hypothesis that graph intelligence based on AI plays an important role in enhancing financial crime detection. Blockchain trace forensics augmentation further improves the level of transparency and the number of investigations, which is relevant to the manifestation of risks in digital asset ecosystems. Although the computational cost is still a challenge, the benefits of such advanced analytics in terms of the level of detection and the level of operational efficiency are significant enough to warrant the use of advanced analytics [30]. These results show that the suggested solution is the significant improvement of the current-day practices and the scaled basis of new-generation financial crime prevention frameworks.

5. CONCLUSION

This study has established that among the existing financial ecosystems, AI-based financial crime analytics that become more advanced by incorporating graph intelligence and blockchain trace forensics represent a potent and efficient method of enhancing fraud detection. The proposed framework has been effective in capturing complex fraud networks, including those like collusion, layering, and mule networks, which are mostly missed by the standard rule-based and standalone machine learning systems by modeling a financial transaction as an interconnected network as well as by analyzing the temporal behavior of networks. Supporting the trace forensics of block chains further increases the ability to investigate by capitalizing on the transparency and immutability of public ledgers to propagate the nature of tracing illicit funds flow of wallets, services, and chains. Empirical evidence shows that the integrated framework is always more effective than the individual models and other related works in accuracy, F1-score and reduction of false-positives and scalable in practice to large transaction graphs. The proposed method provides a better understanding of relations, greater detection strength, and better regulatory compliance support, compared to the current methods. Although graph-based learning does have increased systems with increased computational demands, it should be used in enterprise and regulatory environments because of its merits. Altogether, this paper confirms that the integration of AI, graph analytics, and blockchain forensics can be viewed as an essential innovation in the realm of preventing financial crimes providing a growing and future-proven base to resist an ever more advanced and dynamic financial threat.

REFERENCES

[1] Abbas Jasim Al-Hchaimi, A., Khalifa, M.A. & El-Shafai, W. 2026, "Explainable AI With Imbalanced Learning Strategies for Blockchain Transaction Fraud Detection", Engineering Reports, vol. 8, no. 1, pp. 26.

[2] Abdallah, A.A., Aslan, H.K., Abdallah, M.S., Young-Im, C. & Azer, M.A. 2025, "Enhancing Cryptocurrency Security: Leveraging Embeddings and Large Language Models for Creating Cryptocurrency Security Expert Systems", Symmetry, vol. 17, no. 4, pp. 496.

[3] Almarshad, F.A., Zakariah, M., Gashgari, G.A. & Vaiyapuri, T. 2025, "RABEM: risk-adaptive Bayesian ensemble model for fraud detection", Scientific Reports (Nature Publisher Group), vol. 15, no. 1, pp. 36796.

[4] Almusallam, N. & Qayyum, J. 2025, "A Hybrid Feature Selection and Clustering-Based Ensemble Learning Approach for Real-Time Fraud Detection in Financial Transactions", Computers, Materials, & Continua, vol. 85, no. 2, pp. 3653-3687.

[5] Artenie, A.C., Silaghi, D.L. & Popescu, D.E. 2025, "Exploring the Synergy Between Ethereum Layer 2 Solutions and Machine Learning to Improve Blockchain Scalability", Computers, vol. 14, no. 9, pp. 359.

[6] Asif, M., Mohammad, A. & Faisal, M. 2025, "Towards a Unified Digital Ecosystem: The Role of Platform Technology Convergence", Electronics, vol. 14, no. 24, pp. 4787.

[7] Boddu, K., Ram, M.V., Tulasi Vigneswara,

R.K., Sree, L.M. & Bommisetti, R.K. 2025, "The intelligent finance ecosystem: AI applications in banking and fintech for enhanced decision-making", Asian Economic and Financial Review, vol. 15, no. 11, pp. 1694-1713.

[8] Choi, N. & Kim, H. 2025, "Technological Convergence of Blockchain and Artificial Intelligence: A Review and Challenges", Electronics, vol. 14, no. 1, pp. 84.

[9] Ding, H., Xie, Z., Wang, C., Yu, W., Cui, X. & Wang, Z. 2024, "Applications of Big Data and Blockchain Technology in Food Testing and Their Exploration on Educational Reform", Foods, vol. 13, no. 21, pp. 3391.

[10] Elhady, A.M. & Shohieb, S. 2025, "AI-driven sustainable finance: computational tools, ESG metrics, and global implementation", Future Business Journal, vol. 11, no. 1, pp. 209.

[11] Ellahi, R.M., Wood, L.C., Khan, M. & Alaa El-Din, A.B. 2025, "Integrity Challenges in Halal Meat Supply Chain: Potential Industry 4.0 Technologies as Catalysts for Resolution", Foods, vol. 14, no. 7, pp. 1135.

[12] Fatih, E. 2025, "Near Real-Time Ethereum Fraud Detection Using Explainable AI in Blockchain Networks", Applied Sciences, vol. 15, no. 19, pp. 10841.

[13] Fourkiotis, K.P. & Athanasios, T. 2025, "Future Internet Applications in Healthcare: Big Data-Driven Fraud Detection with Machine Learning", Future Internet, vol. 17, no. 10, pp. 460.

[14] Fujiang, Y., Zihao, Z., Jiang, Y., Wenzhou, S., Zhen, T., Chenxi, Y., Yang, J., Zebing, M., Huang, X., Shaojie, G. & Yanhong, P. 2025, "AI-Driven Optimization of Blockchain Scalability, Security, and Privacy Protection", Algorithms, vol. 18, no. 5, pp. 263.

[15] Gresoi, S., Stamatescu, G. & Făgărăşan, I. 2025, "Advanced Methodology for Fraud Detection in Energy Using Machine Learning Algorithms", Applied Sciences, vol. 15, no. 6, pp. 3361.

[16] Hassen, L., Ali, L., Elham, K. & Abdulla, A. 2025, "AI-Based Anomaly Detection and Optimization Framework for Blockchain Smart Contracts", Administrative Sciences, vol. 15, no. 5, pp. 163.

[17] Hisham, A. & Lakshmi, S. 2025, "Online Banking Fraud Detection Model: Decentralized Machine Learning Framework to Enhance Effectiveness and Compliance with Data Privacy Regulations", Mathematics, vol. 13, no. 13, pp. 2110.

[18] Hsiao-Chun, H., Der-Chen, H. & Chin-Ling, C. 2025, "Applications of AI and Blockchain in Origin Traceability and Forensics: A Review of ICs, Pharmaceuticals, EVs, UAVs, and Robotics", Computer Modeling in Engineering & Sciences, vol. 145, no. 1, pp. 67-126.

[19] Ibrahim, M. 2025, "AI-Driven Cybersecurity in IoT: Adaptive Malware Detection and Lightweight Encryption via TRIM-SEC Framework", Sensors, vol. 25, no. 22, pp. 7072.

[20] Islam, M.J., Saminur, I., Mahmud, H., Shahid, N. & Riazul, I.S.M. 2025, "Securing Blockchain Systems: A Layer-Oriented Survey of Threats, Vulnerability Taxonomy, and Detection Methods", Future Internet, vol. 17, no. 5, pp. 205.

[21] Kamran, R. & Shah, M. 2025, "Next-Generation Machine Learning in Healthcare Fraud Detection: Current Trends, Challenges, and Future Research Directions", Information, vol. 16, no. 9, pp. 730.

[22] Kamrul, S.M., Bilash, S., Mehedi, H.M., Hossain Faruk, M.J., Nafisa, A., Sharaban, T., Aiasha, S. & Hossain, S. 2025, "Securing Decentralized Ecosystems: A Comprehensive Systematic Review of Blockchain Vulnerabilities, Attacks, and Countermeasures and Mitigation Strategies", Future Internet, vol. 17, no. 4, pp. 183.

[23] Khan, I.U., Fida, M.K., Zeeshan, A.H. & Alturise, F. 2025, "Integrating AI, Blockchain, and Edge Computing for Zero-Trust IoT Security: A Comprehensive Review of Advanced Cybersecurity Framework", Computers, Materials, & Continua, vol. 85, no. 3, pp. 4307-4344.

[24] Kurt, K.K., Timurtaş Meral, Sevcan, P., Fatih, O. & Türkeli Serkan 2025, "Smart Contracts, Blockchain, and Health Policies: Past, Present, and Future", Information, vol. 16, no. 10, pp. 853.

[25] Luiz, M., Andre, B. & Renan, P. 2025, "AI and Financial Fraud Prevention: Mapping the Trends and Challenges Through a Bibliometric Lens", Journal of Risk and Financial Management, vol. 18, no. 6, pp. 323.

[26] Lukić Ivica, Köhler Mirko, Krpić Zdravko & Švarcmajer Miljenko 2025, "Advancing Smart City Sustainability Through Artificial Intelligence, Digital Twin and Blockchain Solutions", Technologies, vol. 13, no. 7, pp. 300.

[27] Mohammed Abdul, S.S., Anup, S. & Jianming, Y. 2025, "Toward the Mass Adoption of Blockchain: Cross-Industry Insights from DeFi, Gaming, and Data Analytics", Big Data and Cognitive Computing, vol. 9, no. 7, pp. 178.

[28] Musau, N.N. & Muathe, S.M. 2025, "Digital transformation strategy: the quest for competitive advantage among commercial banks in Kenya", International Journal of Research in Business and Social Science, vol. 14, no. 5, pp. 1-24.

[29] Ouyang, Y., Cao, E. & Liu, B. 2025, "Blockchain-integrated AI framework for secure IoT-based digital advertising ecosystems", Discover Internet of Things, vol. 5, no. 1, pp. 151.

[30] Patil, D.A. & G., S. 2025, "A comprehensive survey on securing the social internet of things: protocols, threat mitigation, technological integrations, tools, and performance metrics", Scientific Reports (Nature Publisher Group), vol. 15, no. 1, pp. 40190..

.