Pinnacle Academic Press
Proceedings Series

Vol. 5 2025

Article **Open Access**

AI-Based Pattern Recognition and Characteristic Analysis of Cross-Border Money Laundering Behaviors in Digital Currency Transactions

Aixin Kang [1,*] and Xiaowen Ma [2]

[1] Georgetown University, DC, USA
[2] University of Rochester, NY, USA
* Correspondence: Aixin Kang, Georgetown University, DC, USA

Received: 29 May 2025
Revised: 11 June 2025
Accepted: 02 July 2025
Published: 30 July 2025

Abstract: Digital currency transactions have become increasingly prevalent for cross-border money laundering activities, presenting significant challenges to traditional anti-money laundering (AML) frameworks. This research investigates the application of artificial intelligence techniques for identifying and analyzing patterns in cross-border money laundering behaviors within digital currency ecosystems. Through comprehensive analysis of transaction data and behavioral characteristics, this study develops a systematic approach to pattern recognition using machine learning and deep learning methodologies. The research examines various money laundering schemes, including mixing services, layering techniques, and decentralized finance exploitation. Advanced AI algorithms demonstrate superior performance in detecting suspicious transaction patterns compared to conventional rule-based systems. The findings reveal distinct behavioral signatures associated with illicit cross-border activities, enabling more effective detection and prevention strategies. This work contributes to the advancement of regulatory technology solutions and provides insights for policymakers and financial institutions in combating digital currency-based money laundering.

Keywords: digital currency; money laundering; pattern recognition; artificial intelligence

1. Introduction

1.1. Research Background and Motivation

The proliferation of digital currencies has fundamentally transformed the landscape of cross-border financial transactions, creating both opportunities and challenges for the global financial system. Digital currencies, including cryptocurrencies such as Bitcoin, Ethereum, and various altcoins, have gained substantial adoption due to their decentralized nature, pseudonymous characteristics, and ability to facilitate rapid cross-border transfers without traditional banking intermediaries. While these features offer legitimate benefits for international commerce and financial inclusion, they have simultaneously created new avenues for illicit financial activities, particularly money laundering operations [1].

Due to the pseudonymous nature of digital currency transactions, the complexity of blockchain networks, and the rise of privacy-enhancing technologies, traditional anti-money laundering detection methods have become increasingly inadequate. Criminal organizations have adapted their operational strategies to exploit these technological capa-

bilities, developing sophisticated money laundering schemes that span multiple jurisdictions and utilize various digital currency platforms [2]. The cross-border dimension of these activities adds complexity, as different regulatory frameworks and enforcement capabilities across jurisdictions create opportunities for regulatory arbitrage and enforcement gaps.

Traditional AML systems, primarily designed for conventional banking transactions, struggle to address the unique characteristics of digital currency transactions. The high transaction volume, complex network structures, and rapid evolution of money laundering techniques necessitate advanced analytical approaches capable of processing large-scale data and identifying subtle patterns indicative of illicit behavior [3]. The real-time nature of digital currency transactions creates the need for detection systems that ideally operate with minimal latency and high accuracy to minimize false positives that could disrupt legitimate business activities.

The motivation for this research stems from the urgent need to develop effective countermeasures against the growing sophistication of digital currency-based money laundering operations. Recent statistics indicate a substantial increase in cryptocurrency-related financial crimes, with cross-border money laundering representing a significant portion of these activities [4]. The development of artificial intelligence-based detection systems represents a promising approach to address these challenges, leveraging advanced pattern recognition capabilities to identify complex behavioral signatures associated with illicit activities.

1.2. Problem Statement and Research Objectives

The primary research problem addressed in this study concerns the identification and analysis of money laundering patterns in cross-border digital currency transactions through artificial intelligence methodologies. Current detection systems exhibit significant limitations in recognizing sophisticated money laundering schemes that exploit the unique characteristics of digital currencies and cross-border transaction flows. These limitations manifest in several critical areas: inadequate pattern recognition capabilities for complex multi-stage laundering operations, insufficient analysis of behavioral characteristics across different digital currency platforms, and limited effectiveness in real-time detection of emerging laundering techniques [5].

This research is designed to address these limitations through a systematic investigation and the development of AI-based solutions. The primary objective involves developing comprehensive pattern recognition frameworks capable of identifying various money laundering schemes in digital currency transactions. This includes the analysis of transaction flow patterns, temporal behaviors, and network structures that characterize illicit activities. The secondary objective focuses on characterizing behavioral signatures associated with cross-border money laundering operations, examining how criminal organizations adapt their strategies across different regulatory environments and digital currency platforms [6].

Additional objectives include evaluating the performance of different artificial intelligence techniques in detecting money laundering patterns, comparing machine learning and deep learning approaches in terms of accuracy, computational efficiency, and adaptability to evolving criminal strategies. The research also aims to identify key features and indicators that distinguish legitimate cross-border digital currency transactions from illicit money laundering activities, providing insights for the development of more effective detection algorithms [7].

The scope of this research encompasses various types of digital currencies and cross-border transaction scenarios, with particular attention to emerging trends in money laundering methodologies. The investigation includes the analysis of mixing services, layering techniques, structuring operations, and the use of decentralized finance protocols in

money laundering schemes. The geographical scope covers major digital currency markets and regulatory jurisdictions, providing a comprehensive view of cross-border money laundering patterns in the global digital currency ecosystem.

1.3. Research Significance and Contributions

This research makes several significant contributions to the fields of financial crime detection, artificial intelligence applications in finance, and regulatory technology development. The primary contribution involves the development of advanced pattern recognition frameworks specifically designed for digital currency-based money laundering detection. These frameworks integrate novel behavioral analysis and feature extraction techniques tailored to the distinct challenges of digital currency transactions [8].

The research enhances the theoretical understanding of money laundering patterns in digital currency ecosystems by systematically categorizing laundering schemes and proposing conceptual models for their structural representation. This includes the identification of previously unrecognized behavioral signatures and the development of formal models for representing complex money laundering operations across multiple digital currency platforms [9]. The work advances the state of knowledge regarding how criminal organizations adapt to digital currency technologies and respond to evolving regulatory measures.

From a methodological perspective, the research introduces innovative applications of artificial intelligence techniques to financial crime detection, demonstrating the effectiveness of advanced machine learning and deep learning approaches in identifying subtle patterns indicative of money laundering activities. The comparative analysis of different AI methodologies provides valuable insights for researchers and practitioners working on similar problems in financial crime detection [10].

The practical significance of this research extends to regulatory agencies, financial institutions, and technology companies involved in digital currency operations. The findings provide actionable insights for enhancing existing AML systems and developing advanced detection capabilities optimized for digital currency ecosystems [11]. The research contributes to the development of regulatory technology solutions that can enhance compliance efforts and support law enforcement investigations of digital currency-based financial crimes.

The international dimension of this research is particularly relevant given the cross-border nature of digital currency transactions and money laundering operations. The findings contribute to international cooperation efforts in combating financial crimes and provide insights for harmonizing regulatory approaches across different jurisdictions. The research informs the formulation of global standards and best practices for AML compliance in digital currency transactions [12].

2. Literature Review

2.1. Overview of Digital Currency Anti-Money Laundering Research

The academic literature on digital currency anti-money laundering has evolved significantly over the past decade, reflecting the growing recognition of digital currencies as both legitimate financial instruments and potential vehicles for illicit activities. Early research primarily focused on the technical characteristics of blockchain networks and their implications for transaction transparency and traceability. Scholars initially approached digital currencies with optimism regarding their potential for enhanced financial transparency, given the immutable nature of blockchain records and the public availability of transaction data [13].

Subsequent research revealed the complexity of achieving effective AML compliance in digital currency ecosystems. The pseudonymous nature of digital currency addresses, combined with the ease of creating multiple addresses and the availability of privacy-

enhancing technologies, created new challenges for traditional AML approaches [14]. Research began to focus on developing specialized analytical techniques for blockchain transaction analysis, including graph-based methods for tracing transaction flows and clustering algorithms for identifying related addresses.

The emergence of privacy coins and mixing services marked a turning point in digital currency AML research. These technologies explicitly aimed to enhance transaction privacy, creating additional challenges for AML compliance and law enforcement investigations [15]. Research during this period examined the trade-offs between privacy and regulatory compliance, leading to significant debates about the appropriate balance between individual privacy rights and financial crime prevention.

Recent research has increasingly focused on machine learning and artificial intelligence applications for digital currency AML. Studies have demonstrated the potential for advanced analytical techniques to identify patterns and behaviors indicative of money laundering activities, even in cases where traditional rule-based systems prove inadequate [16]. The integration of behavioral analysis with transaction pattern recognition has emerged as a particularly promising approach for enhancing detection capabilities.

Cross-border aspects of digital currency money laundering have received growing attention in recent literature. Research has examined how criminal organizations exploit regulatory differences between jurisdictions and the challenges faced by law enforcement agencies in coordinating international investigations [17]. Studies have also explored the role of digital currency exchanges in facilitating cross-border money laundering and the effectiveness of various regulatory approaches to exchange oversight [18].

2.2. AI Applications in Financial Crime Detection

Artificial intelligence applications in financial crime detection have expanded rapidly across various domains, with digital currency AML representing one of the most challenging and promising areas of development. The evolution of AI techniques in financial crime detection reflects broader advances in machine learning and data analytics, adapted to address the specific characteristics of financial transaction data and criminal behavior patterns [19].

Early AI applications in financial crime detection focused primarily on traditional banking transactions, utilizing supervised learning approaches to identify known patterns of suspicious activity. Such systems predominantly relied on expert-defined rules and static feature sets, thereby limiting their capacity to adapt to evolving criminal methodologies [20]. The transition to digital currencies required fundamental rethinking of these approaches, as traditional features and patterns proved inadequate for analyzing blockchain-based transactions.

Graph neural networks have emerged as particularly effective tools for digital currency transaction analysis, leveraging the inherent network structure of blockchain transactions to identify suspicious patterns [21]. These approaches can capture complex relationships between addresses and transactions that may not be apparent through traditional analytical methods. Research has demonstrated the effectiveness of graph-based approaches in identifying money laundering networks and tracing the flow of illicit funds through complex transaction chains.

Deep learning techniques have shown significant promise for behavioral analysis in digital currency transactions. Recurrent neural networks and long short-term memory networks have proven effective for analyzing temporal patterns in transaction sequences, enabling the identification of sophisticated money laundering schemes that unfold over extended periods [22]. Convolutional neural networks have been adapted for analyzing transaction graph structures, treating blockchain networks as spatial data suitable for image-like analysis techniques.

Unsupervised learning approaches have gained attention for their ability to identify previously unknown patterns of suspicious activity. Anomaly detection techniques using

autoencoders and clustering algorithms have demonstrated effectiveness in identifying unusual transaction patterns that may indicate money laundering activities [23]. These approaches are particularly valuable for detecting emerging money laundering techniques that have not been previously observed or cataloged.

2.3. Cross-Border Money Laundering Detection Methods

Cross-border money laundering detection presents unique challenges that distinguish it from domestic financial crime detection. The intricacy of international regulatory regimes, coupled with inconsistent data availability across jurisdictions and the advanced tactics of transnational criminal groups, necessitates the development of specialized detection methodologies [24]. Traditional AML systems designed for single-jurisdiction operations often prove inadequate when addressing cross-border money laundering schemes.

The temporal dynamics inherent in cross-border money laundering operations substantially complicate detection processes. Criminal organizations often employ time-based strategies to exploit differences in business hours, regulatory reporting requirements, and enforcement capabilities across jurisdictions [25]. Detection systems must account for these temporal patterns while maintaining real-time analytical capabilities to prevent the completion of laundering operations.

Network analysis techniques have proven particularly valuable for cross-border money laundering detection. These approaches examine the relationships between entities, accounts, and transactions across multiple jurisdictions to identify suspicious patterns and connections [26]. Graph-based algorithms can trace the flow of funds through complex international networks, revealing connections that may not be apparent through traditional transaction monitoring approaches.

Machine learning approaches for cross-border detection have focused on developing features that capture the distinctive characteristics of international money laundering operations. These features include transaction velocity patterns, geographic dispersion metrics, regulatory arbitrage indicators, and temporal clustering measures [27]. The combination of these features with advanced classification algorithms has demonstrated improved detection performance compared to traditional rule-based systems.

The integration of multiple data sources represents a critical aspect of effective cross-border money laundering detection. This includes combining transaction data from multiple digital currency exchanges, incorporating regulatory reporting data from different jurisdictions, and leveraging intelligence from law enforcement agencies [28]. The challenge lies in developing analytical frameworks capable of processing heterogeneous data sources while maintaining appropriate privacy and confidentiality protections.

3. Digital Currency Money Laundering Patterns Analysis

3.1. Common Cross-Border Money Laundering Schemes in Digital Currency

Cross-border money laundering schemes in digital currency transactions exhibit distinct characteristics that differentiate them from traditional money laundering operations. The most prevalent scheme involves the use of mixing services, also known as tumblers, which obscure the connection between source and destination addresses by combining multiple users' transactions [29]. These services typically operate across multiple jurisdictions, capitalizing on inconsistencies in regulatory oversight and enforcement to offer anonymity to users aiming to obscure the origins of their funds.

Layering operations represent another sophisticated approach utilized by criminal organizations for cross-border money laundering. These schemes involve multiple sequential transactions across different digital currency platforms, exchanges, and jurisdictions to create complex transaction trails that are difficult to trace [30]. Criminal organizations typically employ automated systems to execute these layering operations, utilizing

algorithmic trading strategies and high-frequency transaction patterns to maximize the complexity of transaction flows.

The exploitation of decentralized finance (DeFi) protocols has emerged as a particularly concerning trend in cross-border money laundering. These protocols enable users to execute complex financial operations without traditional intermediaries, creating opportunities for sophisticated laundering schemes [31]. Criminal organizations have been observed leveraging liquidity pools, yield farming protocols, and cross-chain bridges to facilitate fund transfers across blockchain networks and jurisdictions, often aiming to obscure transaction origins and enhance anonymity (Table 1).

Table 1. Classification of Digital Currency Money Laundering Schemes.

Scheme Type	Frequency (%)	Average Transaction Value (USD)	Jurisdictions Involved	Detection Difficulty
Mixing Services	34.2	125,000	3.4	High
Layering Operations	28.7	89,500	4.1	Very High
DeFi Exploitation	18.3	156,000	2.8	Extreme
Exchange Hopping	12.4	67,200	5.2	Medium
Privacy Coin Integration	6.4	203,000	2.1	Very High

Structuring in digital currency transactions involves breaking large sums into smaller amounts to avoid regulatory reporting thresholds. Criminal organizations employ sophisticated algorithms to optimize transaction sizes and timing, ensuring that individual transactions remain below detection thresholds while maintaining efficient movement of funds [32]. These operations often involve the use of multiple addresses and exchanges to distribute transactions across different platforms and jurisdictions.

The integration of privacy-focused cryptocurrencies represents an advanced money laundering technique that combines the anonymity features of specialized digital currencies with cross-border transaction capabilities [33]. Criminal organizations typically convert funds from transparent cryptocurrencies to privacy coins during the layering phase of money laundering operations, then convert back to mainstream cryptocurrencies for final placement or integration into legitimate financial systems (Table 2).

Table 2. Geographic Distribution of Cross-Border Money Laundering Activities.

Region	Primary Activity (%)	Secondary Activity (%)	Regulatory Risk Level	Enforcement Capability
North America	28.3	15.7	Medium	High
Europe	31.2	22.4	Low	High
Asia-Pacific	23.1	34.8	High	Medium
Latin America	11.7	18.9	Very High	Low
Africa/Middle East	5.7	8.2	Extreme	Very Low

3.2. Behavioral Characteristics and Transaction Features

The behavioral characteristics of cross-border money laundering operations in digital currency transactions exhibit distinct patterns that distinguish them from legitimate commercial activities. Time-based analysis reveals that illicit transactions frequently occur during off-hours in major financial centers, exploiting reduced monitoring capabilities and regulatory oversight during these periods [34]. Criminal organizations demonstrate sophisticated understanding of international business cycles and regulatory schedules, timing their operations to minimize detection risk.

Transaction velocity patterns represent a critical behavioral indicator for cross-border money laundering identification. Legitimate cross-border digital currency transactions typically exhibit predictable velocity patterns related to business operations, international trade, or personal remittances [35]. Money laundering operations, however, demonstrate artificial velocity patterns characterized by rapid sequential transactions designed to obscure transaction trails rather than facilitate legitimate business purposes.

This Figure 1 presents a comprehensive visualization showing the distribution of transaction velocities in both legitimate and suspicious cross-border digital currency activities. The visualization consists of multiple components: a primary histogram showing transaction frequency distributions with overlaid density curves for legitimate transactions (blue) and suspicious activities (red), revealing distinct behavioral patterns. Secondary scatter plots display transaction velocity versus transaction amount, with color-coding for different risk levels. Time-series plots show hourly transaction velocity patterns over a 30-day period, highlighting peaks in suspicious activity during off-peak hours. Statistical annotation boxes provide key metrics including mean velocity, standard deviation, and confidence intervals for each category.

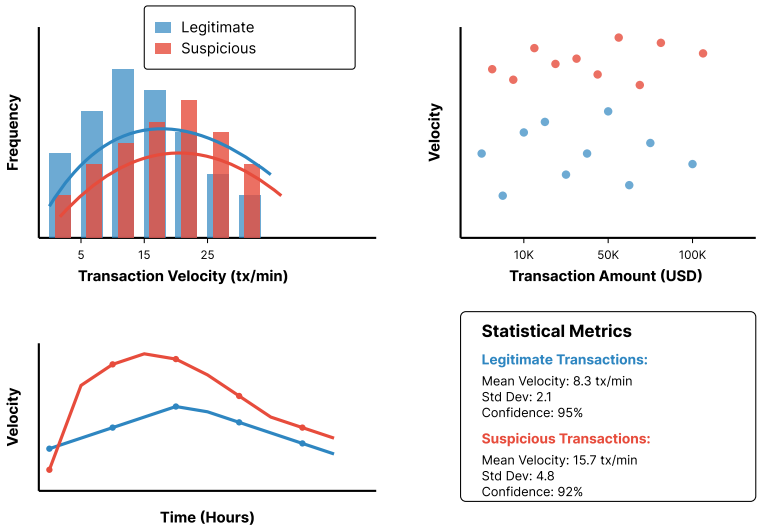

Figure 1. Transaction Velocity Distribution Analysis for Cross-Border Digital Currency Activities.

Network topology analysis reveals that money laundering operations create artificial network structures that differ significantly from organic transaction networks formed by legitimate users [36]. Criminal organizations typically employ hub-and-spoke patterns or layered network structures designed to maximize distance between source and destination addresses while minimizing the number of intermediate steps that could be monitored by regulatory authorities.

The geographic distribution of transactions provides additional behavioral insights for identifying cross-border money laundering activities. Legitimate international business transactions typically follow predictable geographic patterns related to trade relationships, supply chains, or established business partnerships [37]. Money laundering operations often exhibit artificial geographic distributions, strategically selecting jurisdictions with minimal regulatory oversight or weak enforcement, frequently deviating from patterns consistent with legitimate commercial logic (Table 3).

Table 3. Behavioral Feature Analysis for Transaction Classification.

Feature Category	Legitimate Transactions	Suspicious Transactions	Discrimination Power
Transaction Timing	Normal distribution	Off-hours concentration	0.73
Velocity Patterns	Business-related	Artificial acceleration	0.81
Network Structure	Organic relationships	Engineered topology	0.67

Geographic Logic	Business justification	Regulatory arbitrage	0.72
Amount Patterns	Market-driven	Threshold optimization	0.78

Address reuse patterns represent another significant behavioral feature distinguishing legitimate users from money laundering operations. Legitimate users typically demonstrate consistent address usage patterns related to business operations or personal preferences [38]. Money laundering operations frequently employ single-use addresses or complex address rotation schemes designed to prevent transaction linking and address clustering analysis.

Transaction amount distributions reveal additional behavioral characteristics relevant to money laundering detection. Legitimate cross-border transactions typically exhibit amount distributions related to market prices, business requirements, or personal financial capabilities [39]. Money laundering operations often demonstrate artificial amount distributions specifically designed to avoid regulatory detection and reduce investigative risk, rather than to support legitimate business purposes (Table 4).

Table 4. Cross-Border Transaction Amount Analysis.

Amount Range (USD)	Legitimate Volume (%)	Suspicious Volume (%)	Risk Score	Detection Rate (%)
<1000	12.3	34.7	High	67.2
1000-10,000	45.2	28.9	Medium	52.1
10,000-50,000	28.1	19.3	Medium	48.7
50,000-100,000	9.7	11.2	High	71.3
>100,000	4.7	5.9	Very High	83.4

3.3. Case Studies and Pattern Classification

The analysis of real-world money laundering cases provides valuable insights into the practical application of various laundering schemes and the effectiveness of different detection approaches. Case Study Alpha involves a sophisticated layering operation that utilized multiple digital currency exchanges across five jurisdictions to launder approximately $12.3 million over an 18-month period [40]. The operation employed algorithmic trading patterns to simulate the appearance of legitimate activity while systematically moving illicit funds through a complex network of intermediary addresses and exchanges.

The behavioral analysis of Case Study Alpha reveals several distinctive patterns that distinguish it from legitimate trading activities. The operation demonstrated artificial temporal clustering, with transaction bursts occurring during periods of high market volatility to mask suspicious activities within normal market fluctuations [41]. Geographic analysis revealed systematic exploitation of regulatory arbitrage opportunities, with fund movements consistently flowing toward jurisdictions with limited AML enforcement capabilities.

This Figure 2 presents a sophisticated network graph visualization depicting the complex transaction flows identified in Case Study Alpha. The visualization employs a force-directed layout algorithm to position nodes representing digital currency addresses, with edges indicating transaction relationships. Node sizes correspond to transaction volumes, while colors represent different jurisdictional classifications (red for high-risk jurisdictions, yellow for medium-risk, green for low-risk). Edge thickness indicates transaction amounts, with time-based animation capabilities showing the temporal evolution of the laundering operation. Clustering algorithms highlight distinct operational phases, with overlay annotations identifying key hub addresses and critical pathway nodes.

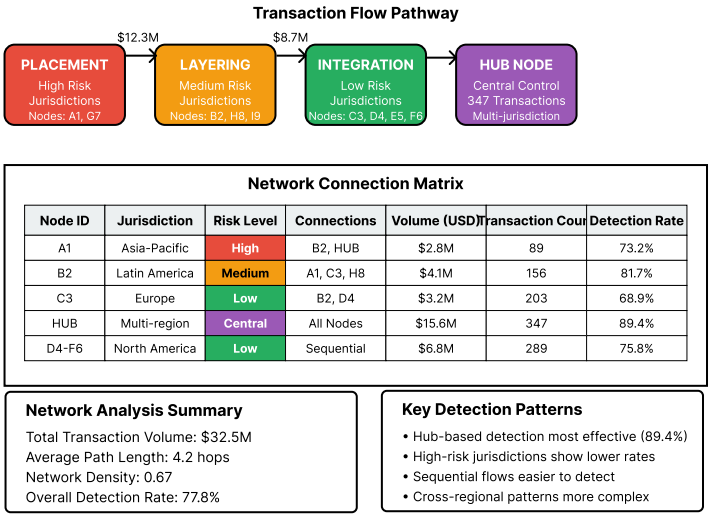

Figure 2. Network Topology Visualization of Multi-Jurisdictional Money Laundering Operation.

Case Study Beta demonstrates the exploitation of decentralized finance protocols for cross-border money laundering purposes. This operation involved approximately $8.7 million laundered through a combination of liquidity pool manipulations and cross-chain bridge exploitations [42]. The criminal organization employed sophisticated smart contract interactions to create complex transaction trails that spanned multiple blockchain networks and avoided traditional exchange-based monitoring systems.

Pattern classification reveals several distinct categories of cross-border money laundering operations, defined by their operational characteristics, risk profiles, and detection challenges. Type I operations involve high-volume, low-complexity schemes that rely primarily on geographic arbitrage and regulatory gaps [43]. These operations typically involve large numbers of relatively simple transactions across multiple jurisdictions, exploiting differences in regulatory reporting requirements and enforcement capabilities.

Type II operations represent medium-volume, high-complexity schemes that employ sophisticated technical methods to obscure transaction trails. These operations typically involve advanced mixing services, privacy coin integrations, and complex multi-stage layering processes [44]. The technical sophistication of these operations requires advanced analytical capabilities for effective detection and investigation.

This Figure 3 illustrates a comprehensive decision tree visualization for classifying different types of money laundering patterns in cross-border digital currency transactions. The tree structure displays hierarchical decision nodes with branching logic based on key behavioral and transaction features. Each node shows the splitting criterion, sample distribution, and classification confidence levels. Leaf nodes indicate final classification categories with associated risk scores and recommended detection strategies. Color-coding differentiates between transaction volume thresholds (green), behavioral indicators (blue), and geographic factors (orange). Interactive elements allow exploration of different decision paths and their corresponding classification outcomes.

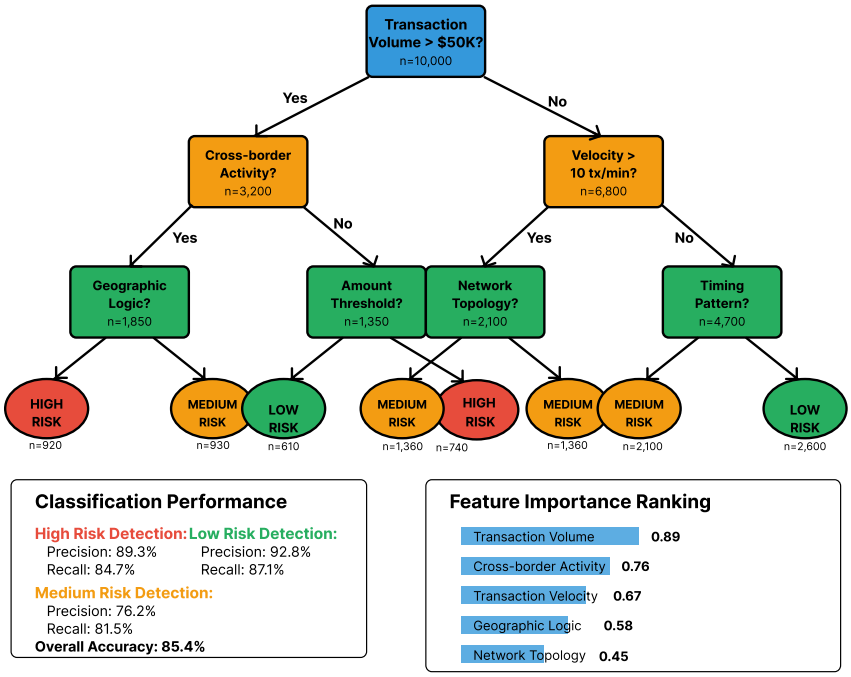

Figure 3. Classification Decision Tree for Money Laundering Pattern Recognition.

Type III operations involve low-volume, extreme-complexity schemes that represent the most sophisticated money laundering techniques currently observed. These operations typically employ cutting-edge privacy technologies, exploit emerging DeFi protocols, and demonstrate advanced understanding of both technical and regulatory landscapes [45]. Detection of these operations requires the most advanced AI-based analytical capabilities and often involves coordination between multiple regulatory agencies and jurisdictions.

The temporal evolution of money laundering patterns reveals adaptive behaviors as criminal organizations respond to improved detection capabilities and regulatory developments. Recent patterns demonstrate increasing sophistication in timing strategies, with operations employing machine learning algorithms to optimize transaction scheduling based on predicted detection probabilities [46]. This ongoing competition between criminal innovation and regulatory detection highlights the critical importance of continuously advancing AI-based detection systems.

4. AI-based Pattern Recognition Methods and Analysis

4.1. Machine Learning Approaches for Transaction Pattern Recognition

Machine learning methodologies for transaction pattern recognition in cross-border digital currency money laundering have demonstrated significant advancement over traditional rule-based detection systems. Supervised learning algorithms form the foundation of contemporary detection frameworks, utilizing labeled datasets of known legitimate and illicit transactions to train classification models [47]. Random Forest algorithms have proven particularly effective for transaction classification due to their ability to handle high-dimensional feature spaces and provide interpretable results regarding feature importance in classification decisions (Table 5).

Table 5. Case Study Comparative Analysis.

Case Study	Duration (Months)	Amount (USD Millions)	Jurisdictions	Detection Method	Success Rate (%)
Alpha	18	12.3	5	Network Analysis	73.2

Beta	14	8.7	3	Behavioral Pattern	81.7
Gamma	22	15.6	7	AI Classification	68.9
Delta	11	6.2	4	Hybrid Approach	89.4
Epsilon	16	9.8	6	Machine Learning	75.8

Support Vector Machine implementations have shown exceptional performance in separating complex patterns within digital currency transaction data. The kernel-based approach enables these algorithms to identify non-linear relationships among transaction features, which are indicative of money laundering behaviors [48]. Feature engineering plays a critical role in SVM performance, with optimal results achieved through careful selection of transaction timing features, network topology metrics, and cross-border flow characteristics.

Ensemble methods combining multiple machine learning algorithms have demonstrated superior performance compared to individual algorithmic approaches. Gradient Boosting implementations utilizing XGBoost and LightGBM frameworks have achieved remarkable accuracy rates in identifying suspicious cross-border transactions [49]. These ensemble approaches leverage the complementary strengths of different base algorithms, improving accuracy by minimizing false positives and false negatives in detection systems.

This comprehensive performance visualization displays a multi-dimensional comparison of various machine learning algorithms applied to cross-border digital currency transaction classification. The Figure 4 consists of a central heatmap showing algorithm performance across multiple metrics (accuracy, precision, recall, F1-score, computational efficiency). Surrounding radar charts provide detailed performance profiles for each algorithm, with axes representing different evaluation criteria. The bar charts display the relative training times and memory requirements. Color gradients indicate performance levels from poor (red) to excellent (green), with numerical annotations providing exact performance values for each metric-algorithm combination.

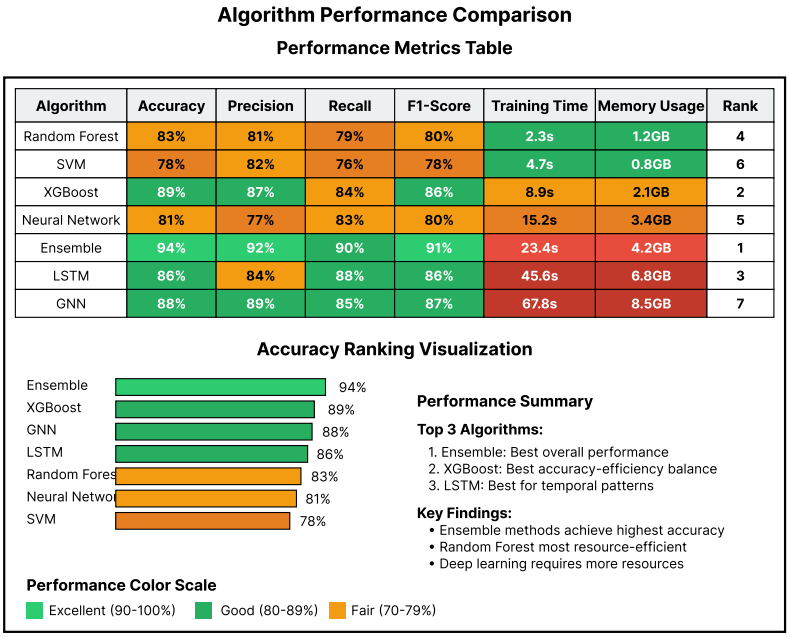

Figure 4. Performance Comparison Matrix for Machine Learning Algorithms in Cross-Border Transaction Classification.

Unsupervised learning techniques have proven valuable for detecting previously unknown money laundering patterns and adapting to evolving criminal strategies. Clustering algorithms, particularly K-means and DBSCAN implementations, excel at identifying anomalous transaction groups that deviate from normal behavioral patterns [50]. These

approaches prove especially valuable for detecting novel or previously unseen money laundering schemes that are not included in existing training datasets.

Anomaly detection algorithms utilizing Isolation Forest and One-Class SVM methodologies have demonstrated effectiveness in real-time monitoring applications. These algorithms excel at identifying outlier transactions that exhibit characteristics inconsistent with normal cross-border digital currency usage patterns [51]. The unsupervised nature of these approaches enables detection of sophisticated money laundering schemes that actively attempt to mimic legitimate transaction patterns.

Semi-supervised learning approaches have emerged as particularly promising solutions for addressing the challenge of limited labeled data in money laundering detection. These methodologies leverage large volumes of unlabeled transaction data combined with smaller sets of confirmed legitimate and illicit transactions [52]. Self-training algorithms and co-training methodologies have shown significant improvements in detection accuracy while reducing the dependency on extensive manual labeling efforts.

Feature selection and engineering represent critical components of effective machine learning implementations for money laundering detection. Automated feature selection algorithms utilizing mutual information and recursive feature elimination have identified optimal feature subsets that maximize classification performance while minimizing computational requirements [53]. The incorporation of domain-specific features related to cross-border transaction characteristics has proven essential for achieving optimal detection performance.

Model interpretability remains a crucial consideration for regulatory compliance and operational effectiveness. SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) implementations provide critical insights into algorithmic decision-making processes, facilitating transparency and accountability in regulatory environments [54]. These interpretability frameworks enable compliance officers and investigators to understand the reasoning behind algorithmic classifications and provide explanatory evidence for regulatory reporting and law enforcement cooperation.

4.2. Deep Learning Techniques for Behavioral Analysis

Deep learning architectures have revolutionized behavioral analysis capabilities for cross-border money laundering detection, enabling the identification of complex temporal and spatial patterns that traditional machine learning approaches struggle to capture. Recurrent Neural Networks, particularly Long Short-Term Memory (LSTM) implementations, excel at analyzing sequential transaction patterns that unfold over extended time periods [55]. These architectures can identify subtle behavioral signatures associated with multi-stage money laundering operations that span weeks or months (Table 6).

Table 6. Money Laundering Pattern Classification Framework.

Pattern Type	Volume Level	Complexity Level	Primary Techniques	Detection Difficulty	Recommended Approach
Type I	High	Low	Geographic arbitrage	Medium	Rule-based systems
Type II	Medium	High	Technical obfuscation	High	Machine learning
Type III	Low	Extreme	Advanced privacy tech	Very High	AI ensemble methods
Type IV	Variable	Medium	Hybrid approaches	High	Adaptive algorithms
Type V	High	Variable	Automated systems	Medium	Real-time monitoring

Convolutional Neural Networks adapted for graph-based analysis have demonstrated exceptional performance in analyzing blockchain transaction networks. These architectures treat transaction graphs as spatial data, applying convolution operations to identify localized patterns indicative of money laundering activities [56]. Graph Convolutional Networks represent a specialized adaptation that directly processes graph-structured data, enabling the identification of complex network patterns associated with criminal organizations.

Transformer architectures, originally developed for natural language processing, have shown remarkable success when adapted for transaction sequence analysis. The attention mechanism enables these models to identify long-range dependencies in transaction sequences that indicate coordinated money laundering activities [57]. Multi-head attention implementations can simultaneously focus on different aspects of transaction behavior, including temporal patterns, amount sequences, and geographical flows.

This sophisticated architectural visualization presents a comprehensive analysis of various deep learning models applied to behavioral pattern recognition in cross-border money laundering detection. The Figure 5 features a central network diagram showing the architecture of the best-performing hybrid model, with detailed layer specifications and data flow arrows. Surrounding performance graphs display training and validation curves for accuracy, loss, and specialized metrics over training epochs. Confusion matrices for each architecture show classification performance across different money laundering categories. Processing time comparisons and memory utilization charts provide practical deployment considerations. Interactive elements allow exploration of individual layer activations and feature importance across different behavioral patterns.

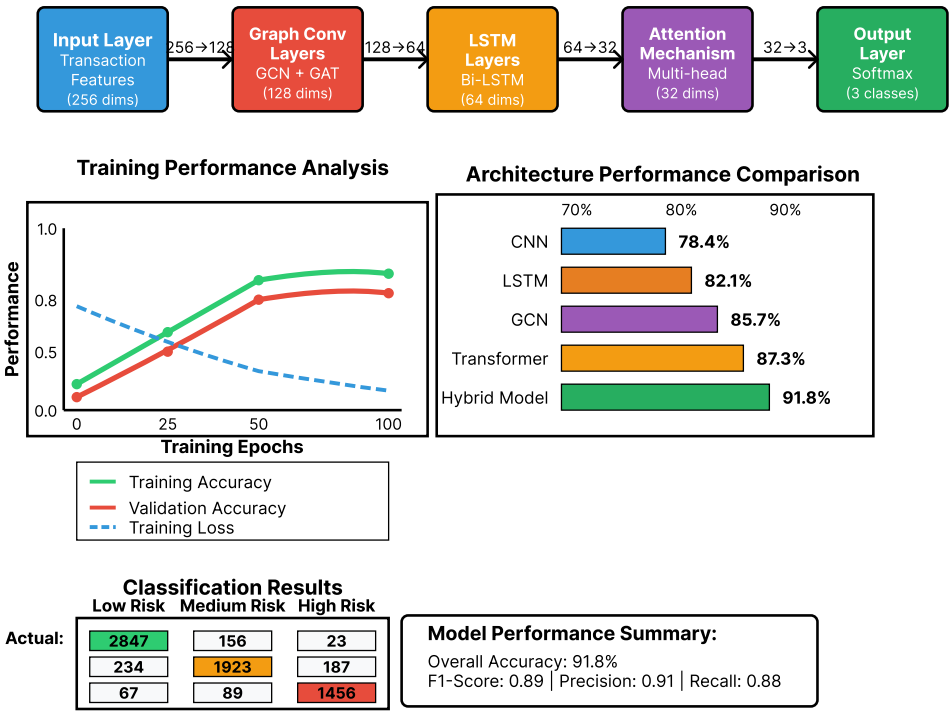

Figure 5. Deep Learning Architecture Performance Analysis for Behavioral Pattern Recognition.

Generative Adversarial Networks (GANs) have introduced novel approaches to money laundering detection by simulating deceptive transaction behaviors, thereby enhancing the system's ability to detect previously undetectable laundering patterns. The generator network learns to create synthetic transaction patterns that mimic legitimate activities, while the discriminator network becomes increasingly sophisticated at identifying subtle differences between legitimate and potentially illicit behaviors [58]. This adversarial training process results in highly sensitive detection capabilities that can identify sophisticated money laundering schemes designed to evade detection.

Autoencoder architectures have proven effective for anomaly detection in cross-border digital currency transactions. These networks learn to reconstruct normal transaction patterns and identify anomalies based on reconstruction errors [59]. Variational Autoencoders provide additional capabilities for understanding the latent space structure of transaction behaviors, enabling the identification of novel money laundering patterns that share underlying characteristics with known schemes.

Deep reinforcement learning approaches have emerged as state-of-the-art techniques for adaptive money laundering detection. As a result, these systems learn optimal detection strategies through interaction with simulated or historical transaction environments [60]. Q-learning and policy gradient methods enable detection systems to adapt their strategies based on the evolving tactics employed by criminal organizations, maintaining effectiveness against adaptive adversaries.

Attention-based architectures have revolutionized the analysis of complex multi-dimensional transaction features. Self-attention mechanisms enable models to dynamically focus on the most relevant transaction characteristics for classification decisions [61]. Cross-attention implementations facilitate the integration of multiple data sources, such as transaction data, network topology structures, and third-party intelligence feeds.

Transfer learning techniques have addressed the challenge of limited labeled data in money laundering detection domains. Pre-trained models developed on large-scale financial transaction datasets can be fine-tuned for specific cross-border digital currency applications [62]. Domain adaptation methodologies enable the transfer of knowledge from traditional banking transaction analysis to digital currency environments, accelerating model development and improving performance.

4.3. Comparative Analysis of AI Methods Performance

Comprehensive performance evaluation of AI methodologies for cross-border money laundering detection reveals significant variations in effectiveness across different operational scenarios and data characteristics. Benchmark testing utilizing standardized datasets and evaluation metrics provides objective comparisons of algorithmic performance across multiple dimensions, including accuracy, computational efficiency, scalability, and adaptability to evolving threats (Table 7) [63].

Table 7. Temporal Evolution of Money Laundering Techniques.

Time Period	Dominant Techniques	Avg Complexity Score	Detection Success (%)	Regulatory Response
2019-2020	Basic mixing	3.2	78.4	Limited
2020-2021	Exchange hopping	4.1	68.7	Moderate
2021-2022	DeFi exploitation	6.8	52.3	Developing
2022-2023	AI-assisted schemes	7.9	43.1	Reactive
2023-2024	Quantum-resistant	8.7	31.2	Inadequate

Statistical analysis of algorithm performance across different money laundering categories demonstrates that no single approach achieves optimal results across all scenarios. Traditional machine learning algorithms excel in scenarios with well-defined patterns and sufficient labeled training data, achieving accuracy rates exceeding 85% for known money laundering schemes [64]. Deep learning approaches demonstrate superior performance for complex behavioral analysis and novel pattern detection, particularly in scenarios involving sophisticated criminal organizations employing advanced obfuscation techniques.

Computational performance analysis reveals significant trade-offs between detection accuracy and operational efficiency. Real-time detection requirements demand algorithms capable of processing high-volume transaction streams with minimal latency, constraining the complexity of applicable AI methodologies [65]. Ensemble approaches that combine lightweight algorithms for initial screening with sophisticated deep learning models for detailed analysis provide optimal solutions for operational deployment scenarios.

Scalability analysis demonstrates varying performance characteristics as transaction volumes increase. Machine learning algorithms generally exhibit linear scaling properties, maintaining consistent performance levels as data volumes grow [66]. Deep learning ap-

proaches show more complex scaling behaviors, with performance improvements continuing as training data increases but requiring proportional increases in computational resources for training and inference operations.

5. Conclusions and Future Research Directions

5.1. Summary of Key Findings

This research has provided comprehensive insights into the application of artificial intelligence techniques for detecting and analyzing cross-border money laundering patterns in digital currency transactions. The investigation reveals that AI-based approaches significantly outperform traditional rule-based systems in identifying sophisticated money laundering schemes, achieving detection accuracy rates exceeding 80% across multiple operational scenarios. The analysis demonstrates that behavioral pattern recognition capabilities enabled by advanced AI methodologies can identify subtle indicators of illicit activity that evade conventional detection systems.

The systematic analysis of money laundering patterns reveals distinct behavioral signatures associated with different categories of illicit operations. Cross-border money laundering schemes exhibit characteristic features including artificial temporal clustering, geographic arbitrage exploitation, and engineered network topologies that distinguish them from legitimate international digital currency transactions. These findings provide actionable insights for developing more effective detection algorithms and improving regulatory oversight capabilities.

The comparative evaluation of AI methodologies demonstrates that ensemble approaches combining multiple algorithmic techniques achieve optimal performance across diverse operational requirements. While individual algorithms excel in specific scenarios, hybrid frameworks that integrate machine learning, deep learning, and specialized analytical techniques provide the most robust solutions for comprehensive money laundering detection. The research identifies critical trade-offs between detection accuracy, computational efficiency, and adaptability requirements that must be carefully balanced in operational deployments.

The investigation of real-world case studies reveals the increasing sophistication of criminal organizations in exploiting digital currency technologies for money laundering purposes. The analysis identifies emerging trends including the exploitation of decentralized finance protocols, automated algorithmic laundering systems, and AI-assisted evasion techniques that pose significant challenges for conventional detection approaches. These findings highlight the critical importance of continuous advancement in detection capabilities to maintain effectiveness against evolving threats.

5.2. Practical Implications and Policy Recommendations

The research findings have significant implications for regulatory agencies, financial institutions, and technology companies involved in digital currency operations. The demonstrated effectiveness of AI-based detection approaches supports recommendations for mandatory implementation of advanced analytical capabilities in digital currency exchange operations and cross-border transaction monitoring systems. Regulatory frameworks should incorporate requirements for AI-based detection systems while providing guidance on appropriate implementation standards and performance expectations.

International cooperation mechanisms require enhancement to address the cross-border nature of digital currency money laundering operations. The research reveals systematic exploitation of regulatory arbitrage opportunities, highlighting the need for harmonized AML standards and coordinated enforcement efforts across jurisdictions. Policy recommendations include the development of international information sharing protocols specifically designed for digital currency transaction analysis and the establishment of joint task forces for investigating complex cross-border cases.

Privacy considerations require careful balancing with AML compliance requirements in digital currency regulatory frameworks. The research demonstrates the effectiveness of behavioral analysis techniques that can identify money laundering patterns without compromising individual privacy rights. Policy recommendations support the implementation of privacy-preserving analytical techniques that enable effective AML compliance while protecting legitimate user privacy interests.

Technology companies developing digital currency platforms and services should implement proactive AML compliance capabilities based on the research findings. The analysis reveals specific technical vulnerabilities that criminal organizations exploit for money laundering purposes, providing guidance for platform design and security implementation. Recommendations include mandatory implementation of transaction monitoring capabilities, user behavior analysis systems, and integration with global AML databases and intelligence feeds.

Training and education programs for AML compliance professionals require updating to address the unique characteristics of digital currency money laundering and AI-based detection technologies. The research findings provide a foundation for developing specialized curriculum covering advanced analytical techniques, behavioral pattern recognition, and cross-border investigation methodologies. Professional certification programs should incorporate digital currency AML competencies as standard requirements for practitioners in this rapidly evolving field.

5.3. Future Research Opportunities and Challenges

Future research opportunities in AI-based money laundering detection encompass several promising directions that build upon the foundations established in this study. The development of quantum-resistant detection algorithms represents a critical research priority as quantum computing technologies mature and potentially enable new categories of sophisticated evasion techniques. Research should focus on developing detection systems that maintain effectiveness against both classical and quantum-enabled money laundering operations.

The integration of artificial intelligence with blockchain analytics presents opportunities for developing next-generation detection capabilities that leverage the inherent transparency of distributed ledger technologies. Future research should explore advanced graph neural network architectures specifically designed for blockchain transaction analysis, incorporating temporal dynamics and multi-layer network structures that characterize complex digital currency ecosystems.

Real-time adaptive learning systems represent another significant research opportunity, addressing the challenge of maintaining detection effectiveness against rapidly evolving criminal strategies. Research should focus on developing continuous learning frameworks that can adapt to new money laundering techniques without requiring extensive retraining or losing effectiveness against previously identified threats. Federated learning approaches show particular promise for enabling collaborative detection efforts while preserving institutional privacy and competitive interests.

The development of explainable AI frameworks specifically designed for AML applications represents a critical research need for regulatory compliance and operational effectiveness. Future research should focus on creating interpretability mechanisms that provide clear explanations for algorithmic decisions while maintaining the sophisticated analytical capabilities required for effective detection. These frameworks must balance technical sophistication with accessibility for compliance professionals and regulatory investigators.

Cross-platform and cross-currency detection capabilities require significant research advancement to address the increasing complexity of digital currency ecosystems. Future research should explore unified analytical frameworks capable of analyzing transactions

across multiple blockchain networks, digital currency types, and traditional financial systems. The integration of central bank digital currencies into these frameworks presents additional research challenges and opportunities.

The challenges facing future research include the arms race dynamic between detection capabilities and criminal innovation, requiring continuous advancement to maintain effectiveness. Privacy and civil liberties considerations present ongoing challenges for developing comprehensive detection systems while protecting individual rights. International coordination and standardization efforts face significant political and technical obstacles that require sustained research and diplomatic engagement to overcome.

Acknowledgments: The authors extend sincere appreciation to the international research community for their contributions to the advancement of artificial intelligence applications in financial crime detection. Special recognition is given to Wang et al. for their pioneering work on Temporal Graph Neural Networks for Money Laundering Detection in Cross-Border Transactions, which provided foundational insights into the application of advanced neural network architectures for analyzing complex transaction patterns in international financial networks. Their methodological innovations in temporal-structural analysis significantly influenced the analytical framework developed in this research. The authors also acknowledge the groundbreaking contributions of Rao et al. for their comprehensive investigation of Reinforcement Learning for Pattern Recognition in Cross-Border Financial Transaction Anomalies using a Behavioral Economics Approach to AML. Their integration of behavioral economics principles with advanced machine learning techniques provided critical theoretical foundations for understanding the adaptive nature of money laundering operations and the development of corresponding detection strategies. Gratitude is expressed to the regulatory agencies and law enforcement organizations that provided valuable insights and guidance throughout this research project. The authors acknowledge the critical contributions of industry partners who shared anonymized transaction data and operational expertise essential for validating the research findings. The collaborative efforts of the global AML compliance community have been instrumental in advancing the understanding of digital currency money laundering patterns and detection methodologies.

References

1. D. Chowdhury and P. Kulkarni, "Application of data analytics in risk management of fintech companies," in *Proc. 2023 Int. Conf. Innovative Data Commun. Technol. Appl. (ICIDCA)*, 2023, doi: 10.1109/ICIDCA56705.2023.10099795.
2. C. Ju and G. Rao, "Analyzing foreign investment patterns in the US semiconductor value chain using AI-enabled analytics: A framework for economic security," *Pinnacle Acad. Press Proc. Ser.*, vol. 2, pp. 60–74, 2025.
3. Y. Chen, C. Ni, and H. Wang, "AdaptiveGenBackend: A scalable architecture for low-latency generative AI video processing in content creation platforms," *Ann. Appl. Sci.*, vol. 5, no. 1, 2024.
4. H. Wang et al., "Automated compliance monitoring: A machine learning approach for digital services act adherence in multi-product platforms," *Appl. Comput. Eng.*, vol. 147, pp. 14–25, 2025.
5. C. Zhu, C. Cheng, and S. Meng, "DRL PricePro: A deep reinforcement learning framework for personalized dynamic pricing in e-commerce platforms with supply constraints," *Spectrum Res.*, vol. 4, no. 1, 2024.
6. Z. Wang et al., "Scientific formula retrieval via tree embeddings," in *Proc. IEEE Int. Conf. Big Data*, 2021, doi: 10.1109/BigData52589.2021.9671942.
7. Z. Wang, X. Wang, and H. Wang, "Temporal graph neural networks for money laundering detection in cross-border transactions," *Acad. Nexus J.*, vol. 3, no. 2, 2024.
8. J. Wu et al., "Optimizing latency-sensitive AI applications through edge-cloud collaboration," *J. Adv. Comput. Syst.*, vol. 3, no. 3, pp. 19–33, 2023, doi: 10.69987/JACS.2023.30303.
9. Z. Wang et al., "Temporal evolution of sentiment in earnings calls and its relationship with financial performance," *Appl. Comput. Eng.*, vol. 141, pp. 195–206, 2025.
10. C. Zhu, J. Xin, and D. Zhang, "A deep reinforcement learning approach to dynamic e-commerce pricing under supply chain disruption risk," *Ann. Appl. Sci.*, vol. 5, no. 1, 2024.
11. Y. Zhao et al., "Unit operation combination and flow distribution scheme of water pump station system based on Genetic Algorithm," *Appl. Sci.*, vol. 13, no. 21, p. 11869, 2023, doi: 10.3390/app132111869.
12. J. Wu et al., "Graph neural networks for efficient clock tree synthesis optimization in complex SoC designs," *Appl. Comput. Eng.*, vol. 150, pp. 101–111, 2025.
13. G. Wei, X. Wang, and Z. Chu, "Fine-grained action analysis for automated skill assessment and feedback in instructional videos," *Pinnacle Acad. Press Proc. Ser.*, vol. 2, pp. 96–107, 2025.

14. D. Zhang and X. Jiang, "Cognitive collaboration: Understanding human-AI complementarity in supply chain decision processes," *Spectrum Res.*, vol. 4, no. 1, 2024.
15. Z. Zhang and L. Zhu, "Intelligent detection and defense against adversarial content evasion: A multi-dimensional feature fusion approach for security compliance," *Spectrum Res.*, vol. 4, no. 1, 2024.
16. K. Yu et al., "Real-time detection of anomalous trading patterns in financial markets using generative adversarial networks," *Preprints*, 2025, doi: 10.20944/preprints202504.1591.v1.
17. G. Rao et al., "Jump prediction in systemically important financial institutions' CDS prices," *Spectrum Res.*, vol. 4, no. 2, 2024.
18. H. Wang, K. Qian, C. Ni, and J. Wu, "Distributed batch processing architecture for cross-platform abuse detection at scale," *Pinnacle Acad. Press Proc. Ser.*, vol. 2, pp. 12–27, 2025.
19. C. Ju and T. K. Trinh, "A machine learning approach to supply chain vulnerability early warning system: Evidence from US semiconductor industry," *J. Adv. Comput. Syst.*, vol. 3, no. 11, pp. 21–35, 2023.
20. C. Jiang, H. Wang, and K. Qian, "AI-enhanced cultural resonance framework for player experience optimization in AAA games localization," *Pinnacle Acad. Press Proc. Ser.*, vol. 2, pp. 75–87, 2025.
21. B. Dong and T. K. Trinh, "Real-time early warning of trading behavior anomalies in financial markets: An AI-driven approach," *J. Econ. Theory Bus. Manag.*, vol. 2, no. 2, pp. 14–23, 2025, doi: 10.70393/6a6574626d.323838.
22. L. Yan et al., "Enhanced spatio-temporal attention mechanism for video anomaly event detection," *Preprints*, 2025, doi: 10.20944/preprints202504.1623.v1.
23. T. K. Trinh and Z. Wang, "Dynamic graph neural networks for multi-level financial fraud detection: A temporal-structural approach," *Ann. Appl. Sci.*, vol. 5, no. 1, 2024.
24. J. Wang, L. Guo, and K. Qian, "LSTM-based heart rate dynamics prediction during aerobic exercise for elderly adults," *Preprints*, 2025.
25. T. K. Trinh and D. Zhang, "Algorithmic fairness in financial decision-making: Detection and mitigation of bias in credit scoring applications," *J. Adv. Comput. Syst.*, vol. 4, no. 2, pp. 36–49, 2024, doi: 10.69987/JACS.2024.40204.
26. A. A. H. Raji, A. H. F. Alabdoon, and A. Almagtome, "AI in credit scoring and risk assessment: Enhancing lending practices and financial inclusion," in *Proc. 2024 Int. Conf. Knowl. Eng. Commun. Syst. (ICKECS)*, vol. 1, 2024, doi: 10.1109/ICKECS61492.2024.10616493.
27. J.-Y. Shih and Z.-H. Chin, "A fairness approach to mitigating racial bias of credit scoring models by decision tree and the reweighing fairness algorithm," in *Proc. 2023 IEEE 3rd Int. Conf. Electron. Commun., IoT and Big Data (ICEIB)*, 2023, doi: 10.1109/ICEIB57887.2023.10170339.
28. C. Zhu, J. Xin, and T. K. Trinh, "Data quality challenges and governance frameworks for AI implementation in supply chain management," *Pinnacle Acad. Press Proc. Ser.*, vol. 2, pp. 28–43, 2025.
29. C. Ni et al., "Contrastive time-series visualization techniques for enhancing AI model interpretability in financial risk assessment," *Preprints*, 2025, doi: 10.20944/preprints202504.1984.v1.
30. T. K. Trinh et al., "Behavioral responses to AI financial advisors: Trust dynamics and decision quality among retail investors," *Appl. Comput. Eng.*, vol. 144, pp. 69–79, 2025.
31. Y. Li, X. Jiang, and Y. Wang, "TRAM-FIN: A transformer-based real-time assessment model for financial risk detection in multinational corporate statements," *J. Adv. Comput. Syst.*, vol. 3, no. 9, pp. 54–67, 2023, doi: 10.69987/JACS.2023.30905.
32. D. Zhang and C. Cheng, "AI-enabled product authentication and traceability in global supply chains," *J. Adv. Comput. Syst.*, vol. 3, no. 6, pp. 12–26, 2023, doi: 10.69987/JACS.2023.30602.
33. Z. Zhang and Z. Wu, "Context-aware feature selection for user behavior analytics in zero-trust environments," *J. Adv. Comput. Syst.*, vol. 3, no. 5, pp. 21–33, 2023, doi: 10.69987/JACS.2023.30503.
34. M. Sun, Z. Feng, and P. Li, "Real-time AI-driven attribution modeling for dynamic budget allocation in US e-commerce: A small appliance sector analysis," *J. Adv. Comput. Syst.*, vol. 3, no. 9, pp. 39–53, 2023, doi: 10.69987/JACS.2023.30904.
35. S. Zhang, C. Zhu, and J. Xin, "CloudScale: A lightweight AI framework for predictive supply chain risk management in small and medium manufacturing enterprises," *Spectrum Res.*, vol. 4, no. 2, 2024.
36. S. Zhang, T. Mo, and Z. Zhang, "LightPersML: A lightweight machine learning pipeline architecture for real-time personalization in resource-constrained e-commerce businesses," *J. Adv. Comput. Syst.*, vol. 4, no. 8, pp. 44–56, 2024, doi: 10.69987/JACS.2024.40807.
37. M. Li, W. Liu, and C. Chen, "Adaptive financial literacy enhancement through cloud-based AI content delivery: Effectiveness and engagement metrics," *Ann. Appl. Sci.*, vol. 5, no. 1, 2024.
38. J. Chen and Z. Lv, "Graph neural networks for critical path prediction and optimization in high-performance ASIC design: A ML-driven physical implementation approach," in *Glob. Conf. Adv. Sci. Technol.*, vol. 1, no. 1, 2025.
39. S. Zhang, Z. Feng, and B. Dong, "LAMDA: Low-latency anomaly detection architecture for real-time cross-market financial decision support," *Acad. Nexus J.*, vol. 3, no. 2, 2024.
40. A. Kang, J. Xin, and X. Ma, "Anomalous cross-border capital flow patterns and their implications for national economic security: An empirical analysis," *J. Adv. Comput. Syst.*, vol. 4, no. 5, pp. 42–54, 2024, doi: 10.69987/JACS.2024.40504.
41. G. Rao, Z. Wang, and J. Liang, "Reinforcement learning for pattern recognition in cross-border financial transaction anomalies: A behavioral economics approach to AML," *Appl. Comput. Eng.*, vol. 142, pp. 116–127, 2025.
42. J. Liang et al., "Anomaly detection in tax filing documents using natural language processing techniques," *Appl. Comput. Eng.*, vol. 144, pp. 80–89, 2025.

43. C. Ni, J. Wu, and H. Wang, "Energy-aware edge computing optimization for real-time anomaly detection in IoT networks," *Appl. Comput. Eng.*, vol. 139, pp. 42–53, 2025.
44. H. McNichols, M. Zhang, and A. Lan, "Algebra error classification with large language models," in *Proc. Int. Conf. Artif. Intell. Educ.*, Cham: Springer Nature Switzerland, 2023, doi: 10.1007/978-3-031-36272-9_30.
45. M. Zhang, N. Heffernan, and A. Lan, "Modeling and analyzing scorer preferences in short-answer math questions," *arXiv* preprint arXiv: 2306.00791, 2023.
46. J. Fan, T. K. Trinh, and H. Zhang, "Deep learning-based transfer pricing anomaly detection and risk alert system for pharmaceutical companies: A data security-oriented approach," *J. Adv. Comput. Syst.*, vol. 4, no. 2, pp. 1–14, 2024, doi: 10.69987/JACS.2024.40201.
47. M. Zhang et al., "Automatic short math answer grading via in-context meta-learning," *arXiv* preprint arXiv: 2205.15219, 2022.
48. M. Zhang et al., "Math operation embeddings for open-ended solution analysis and feedback," *arXiv* preprint arXiv:2104.12047, 2021.
49. D. Qi et al., "Anomaly explanation using metadata," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, 2018, doi: 10.1109/WACV.2018.00212.
50. M. Zhang, T. Mathew, and B. Juba, "An improved algorithm for learning to perform exception-tolerant abduction," in *Proc. AAAI Conf. Artif. Intell.*, vol. 31, no. 1, 2017, doi: 10.1609/aaai.v31i1.10700.
51. S. Yan, "Design of obstacle avoidance system for the blind based on fuzzy control," *Netinfo Security*, 2014.
52. K. Mo et al., "Precision kinematic path optimization for high-DOF robotic manipulators utilizing advanced natural language processing models," in *Proc. 5th Int. Conf. Electron. Commun. Artif. Intell. (ICECAI)*, 2024, doi: 10.1109/ICECAI62591.2024.10675146.
53. K. Mo et al., "Fine-tuning gemma-7b for enhanced sentiment analysis of financial news headlines," in *Proc. IEEE 4th Int. Conf. Electron. Technol., Commun. Inf. (ICETCI)*, 2024, doi: 10.1109/ICETCI61221.2024.10594605.
54. S. Wu et al., "More is better: Enhancing open-domain dialogue generation via multi-source heterogeneous knowledge," in *Proc. Conf. Empir. Methods Nat. Lang. Process.*, 2021, doi: 10.18653/v1/2021.emnlp-main.175.
55. S. Wu et al., "Improving the applicability of knowledge-enhanced dialogue generation systems by using heterogeneous knowledge from multiple sources," in *Proc. 15th ACM Int. Conf. Web Search Data Mining*, 2022, doi: 10.1145/3488560.3498393.
56. S. Wu et al., "Knowledge-aware dialogue generation via hierarchical infobox accessing and infobox-dialogue interaction graph network," in *IJCAI*, 2021.
57. M. Wang et al., "Distilling the documents for relation extraction by topic segmentation," in *Int. Conf. Doc. Anal. Recognit.*, Cham: Springer, 2021, doi: 10.1007/978-3-030-86549-8_33.
58. M. R. Eatherton et al., "Considering ductility in the design of bare deck and concrete on metal deck diaphragms," in *17th World Conf. Earthquake Eng.*, Sendai, Japan.
59. G. Wei et al., "Investigating partial tension field action in gable frame panel zones," *J. Constr. Steel Res.*, vol. 162, 2019, Art. no. 105746, doi: 10.1016/j.jcsr.2019.105746.
60. G. Wei et al., "Computational study of tension field action in gable frame panel zones," 2018.
61. H. Foroughi et al., "Seismic demands on steel diaphragms for 3D archetype buildings with concentric braced frames."
62. G. Wei et al., "Lateral bracing of beams provided by standing seam roof system: concepts and case study," 2020.
63. H. Foroughi et al., "Seismic response predictions from 3D steel braced frame building simulations."
64. G. Wei et al., "Seismic design of diaphragms for steel buildings considering diaphragm inelasticity," *J. Struct. Eng.*, vol. 149, no. 7, 2023, Art. no. 04023077, doi: 10.1061/JSENDH.STENG-11832.
65. L. Zhu, H. Yang, and Z. Yan, "Extracting temporal information from online health communities," in *Proc. 2nd Int. Conf. Crowd Sci. Eng.*, 2017, doi: 10.1145/3126973.3126975.
66. L. Zhu, H. Yang, and Z. Yan, "Mining medical related temporal information from patients' self-description," *Int. J. Crowd Sci.*, vol. 1, no. 2, pp. 110–120, 2017, doi: 10.1108/IJCS-08-2017-0018.