Anomaly Detection in Blockchain-Based Metaverse Transactions Using Hybrid Autoencoder and Isolation Forest Models for Risk Identification and Behavioral Pattern Analysis

Ibrahiem M. M. El Emary[1,*], Anna Brzozowska[2], Łukasz Popławski[3], Paweł Dziekański[4], Jozef Glova[5]

[1] King Abdulaziz University, Kingdom of Saudi Arabia, Saudi Arabia

[2]Faculty of Management, Czestochowa University of Technology, Poland

[3]Cracow University of Economics, Cracow, Rakowicka 27, 31-510 Poland

[4]Jan Kochanowski University in Kielce, Kielce. Stefana Zeromskiego 5, Poland

[5]Technical University of Košice, Nemcovej 32, 042-00 Košice, Slovakia

ABSTRACT

The increasing complexity of transactions within blockchain-based metaverse ecosystems has intensified the need for robust anomaly detection systems capable of identifying fraudulent, automated, or irregular behaviors. This study proposes a Hybrid Autoencoder–Isolation Forest (AE–IF) model for detecting anomalies in metaverse blockchain transactions through a combination of deep feature reconstruction and ensemble-based isolation. The proposed framework leverages the Autoencoder's ability to learn nonlinear feature representations and the Isolation Forest's capacity to isolate sparse anomalies, enabling the detection of both global and local irregularities. Experimental evaluation using real-world transaction data demonstrates that the hybrid model outperforms individual methods, achieving a ROC-AUC of 0.952, Precision of 0.88, Recall of 0.86, and F1-Score of 0.87. The ROC and Precision–Recall analyses confirm the model's superior discriminative power and stability across imbalanced data distributions. Furthermore, behavioral analysis reveals distinct high-risk transaction patterns, including extended user sessions, cross-regional fund transfers, and irregular purchase behaviors. The results highlight the hybrid model's effectiveness not only in anomaly detection but also in uncovering underlying behavioral and geographical risk factors. The proposed framework provides a scalable foundation for intelligent financial risk monitoring and cyber-fraud detection in decentralized metaverse economies.

Keywords Anomaly Detection, Blockchain, Metaverse Transactions, Autoencoder, Isolation Forest.

Submitted: 15 April 2025
Accepted: 20 May 2025
Published: 15 January 2026

Corresponding author
Ibrahiem M. M. El Emary,
omary57@hotmail.com

Additional Information and Declarations can be found on page 60

DOI: 10.47738/ijrm.v3i1.45

INTRODUCTION

The emergence of the metaverse as a decentralized and immersive digital environment has transformed the way individuals interact, trade, and manage digital assets [1]. Within this expanding ecosystem, blockchain technology has become the foundational infrastructure that ensures transparency, verifiability, and immutability of digital transactions [2]. However, as blockchain adoption in

How to cite this article: I. M. M. El Amary, A. Brzozowska, Ł. Popławski, P. Dziekański, J. Glova, "Anomaly Detection in Blockchain-Based Metaverse Transactions Using Hybrid Autoencoder and Isolation Forest Models for Risk Identification and Behavioral Pattern Analysis," *Int. J. Res. Metav.*, vol. 3, no. 1, pp. 46-63, 2026.

the metaverse continues to accelerate, the number and diversity of transactions have grown exponentially, leading to increased exposure to fraudulent behaviors, automated trading bots, and anomalous user activities that threaten financial integrity and trust within the system. The ability to detect and mitigate such irregularities has therefore become a critical aspect of maintaining the security and reliability of metaverse-based financial ecosystems [3].

Conventional anomaly detection methods, such as statistical thresholding or rule-based classification, often fail to handle the complex, nonlinear, and high-dimensional characteristics of blockchain transactions [4]. These methods typically rely on simplified assumptions about data distribution, which are inadequate in the context of metaverse environments where user behaviors and transaction patterns evolve rapidly and unpredictably. Moreover, the data are often highly imbalanced, as normal transactions vastly outnumber anomalous ones, causing traditional classifiers to overlook rare but critical events. Consequently, the challenge lies not only in detecting anomalies accurately but also in developing models capable of adapting to dynamic and heterogeneous blockchain data.

Machine learning and deep learning techniques have emerged as powerful alternatives for addressing these limitations due to their capacity for pattern recognition and data-driven learning [5]. Among these, Autoencoders have been widely used for anomaly detection because of their ability to learn compact latent representations and reconstruct normal behavior effectively. Anomalies are typically identified through reconstruction error, which captures deviations from learned patterns [6]. However, Autoencoders tend to underperform when dealing with localized or sparse irregularities, as they may overfit dominant patterns in the data. In contrast, the Isolation Forest algorithm isolates anomalies by recursively partitioning the data space using random trees, making it highly effective for identifying local outliers [7]. Despite this, it cannot capture complex feature relationships and nonlinear dependencies that are essential in blockchain-based behavioral data.

To address these complementary weaknesses, this study introduces a AE–IF framework that combines the representational learning capacity of the Autoencoder with the anomaly isolation capability of the Isolation Forest. This integration enables the detection of both global and local anomalies within metaverse blockchain transactions. The hybrid approach allows for a more comprehensive understanding of transaction behaviors, improving detection accuracy while maintaining interpretability. By leveraging both reconstruction-based and ensemble-based mechanisms, the proposed model aims to identify not only fraudulent or irregular activities but also subtle behavioral shifts that may indicate emerging security risks.

The hybrid framework was evaluated using a dataset of blockchain transactions from metaverse environments, which included behavioral, contextual, and financial attributes such as transaction type, amount, location, and user session characteristics. The results showed that the hybrid model achieved significant improvements over its individual components, recording a ROC-AUC of 0.952, Precision of 0.88, Recall of 0.86, and F1-score of 0.87. These findings confirm that the hybrid model is more effective in distinguishing between normal and anomalous transactions. Furthermore, analysis of detected anomalies revealed meaningful behavioral patterns: users with extended session durations and low

transaction frequencies were frequently classified as anomalous, suggesting the presence of automated activity, while cross-regional fund transfers and inconsistent purchase behaviors often corresponded with higher anomaly scores. These insights demonstrate the model's capacity not only to detect anomalies but also to uncover behavioral and geographical risk indicators that are valuable for regulatory and security monitoring.

The main contribution of this study lies in its development of a hybrid detection mechanism that unites the strengths of deep learning and ensemble methods to enhance blockchain anomaly analysis. The model's ability to integrate reconstruction-based feature learning and isolation-based outlier detection allows it to achieve superior accuracy, interpretability, and robustness in the context of metaverse financial ecosystems. Beyond its technical performance, the hybrid framework also contributes to the understanding of how user behavior, geographical dynamics, and network context interact to form high-risk transactional patterns. These findings have practical implications for improving fraud detection, behavioral analytics, and cyber-risk assessment in decentralized environments.

The remainder of this paper is structured as follows. Section 2 discusses related works on blockchain anomaly detection and hybrid machine learning approaches. Section 3 explains the data preprocessing and methodological framework, including model construction and feature integration. Section 4 presents the experimental results and analysis, while Section 5 discusses the interpretive implications and limitations of the findings. Finally, Section 6 concludes the study and offers directions for future research, including the integration of real-time detection and graph-based learning architectures to further enhance anomaly interpretability in blockchain-based metaverse systems.

Literature Review

The rapid expansion of blockchain technology has transformed the digital economy by introducing decentralized, transparent, and immutable transaction systems. Within the metaverse, blockchain serves as the core infrastructure that enables virtual ownership, asset exchange, and digital identity management. However, this expansion has also produced increasingly complex transaction patterns that are vulnerable to anomalous and fraudulent behaviors such as wash trading, automated bot activity, and money laundering [8]. Consequently, the development of robust and intelligent anomaly detection systems has become a central focus in blockchain and cybersecurity research.

Early studies on blockchain anomaly detection primarily utilized statistical and rule-based models to identify irregularities in transaction data. These methods, including threshold-based deviation analysis and z-score detection, offered interpretability but were limited in handling high-dimensional and dynamic data structures [9]. They often assumed linear relationships among features, which are unsuitable for blockchain data that exhibit nonlinear interactions and temporal dependencies. Furthermore, such traditional approaches tend to be sensitive to noise and lack generalizability across evolving transaction environments. As a result, research on blockchain anomaly detection has increasingly shifted toward Machine Learning (ML) and Deep Learning (DL) paradigms.

Among the early ML-based approaches, Logistic Regression (LR) and Support Vector Machines (SVM) were employed to classify transactions using predefined features extracted from blockchain networks [10]. Although these models improved detection accuracy compared to traditional thresholding, they still required extensive feature engineering and were limited in uncovering hidden structural patterns. More recent works have adopted unsupervised learning algorithms such as K-Means, DBSCAN, and Gaussian Mixture Models (GMM) to cluster blockchain transactions and identify outliers based on distance metrics [11]. These methods provided flexibility for unlabeled datasets but remained sensitive to feature scaling and struggled to capture complex nonlinear relationships among variables.

To address these limitations, subsequent research explored the use of Autoencoders (AE) for unsupervised anomaly detection in high-dimensional blockchain data. Autoencoders are neural network architectures that learn compressed latent representations of data by minimizing reconstruction error, thereby distinguishing normal transaction patterns from irregular ones [12]. Studies have demonstrated that Autoencoders can effectively detect anomalies by reconstructing normal samples more accurately than anomalous ones, allowing deviations to be identified through reconstruction loss [13]. In blockchain analytics, Autoencoders have been successfully applied to detect fraudulent wallet addresses and suspicious transaction flows, achieving strong performance in identifying subtle behavioral variations [14]. Nevertheless, Autoencoders may overfit when trained on unbalanced datasets and often struggle to detect localized anomalies that occur infrequently.

Parallel to the emergence of deep learning-based models, the Isolation Forest (IF) algorithm has gained recognition as an efficient ensemble-based method for anomaly detection in large-scale datasets. The Isolation Forest isolates anomalies through recursive random partitioning of data points [15]. Since anomalies are easier to isolate than normal observations, the algorithm measures anomaly scores based on the average path length across trees. Unlike distance- or density-based models, the Isolation Forest performs well in high-dimensional environments and does not depend on distributional assumptions. In blockchain applications, this method has been employed to detect outlier addresses and abnormal transaction networks with minimal computational cost [16]. However, it is limited in capturing nonlinear dependencies and may overlook global structural irregularities that span multiple features.

Recognizing that no single model can effectively capture the diverse nature of blockchain anomalies, recent research has focused on hybrid and ensemble learning frameworks. These frameworks integrate multiple algorithms to combine their complementary strengths while mitigating individual weaknesses [17]. For instance, hybrid deep-ensemble models combining Convolutional Neural Networks (CNN) and Random Forests have demonstrated improved accuracy and stability in financial fraud detection across heterogeneous datasets [18]. Similarly, hybrid approaches that integrate Autoencoders with Gradient Boosting methods have achieved superior precision in identifying rare or complex anomalies [19]. Within blockchain contexts, hybrid frameworks combining deep neural representations with probabilistic and graph-based models have shown promising results in transaction anomaly detection and risk

profiling [20].

Within the metaverse, blockchain transactions introduce additional layers of complexity. These transactions often involve cross-platform, cross-region, and cross-asset interactions, generating behavioral variations that are both temporal and contextual [21]. Detecting anomalies in this environment requires models capable of capturing behavioral, spatial, and temporal correlations simultaneously. Recent studies have suggested that hybrid models combining reconstruction-based learning, such as Autoencoders, with partition-based isolation methods, such as Isolation Forest, provide significant advantages for complex blockchain data [22]. This combination allows the detection of both global deviations and localized irregularities, offering a comprehensive and efficient framework for identifying anomalous transaction behaviors within metaverse ecosystems.

The application of hybrid Autoencoder–Isolation Forest models in blockchain analytics remains relatively underexplored, especially within the context of metaverse transactions [23]. Most existing works focus on single-model implementations or hybrid frameworks applied to financial fraud or intrusion detection rather than decentralized ecosystems. The present study addresses this gap by implementing a hybrid AE–IF framework specifically tailored for metaverse blockchain transaction data. This approach integrates the Autoencoder's nonlinear feature learning ability with the Isolation Forest's anomaly isolation mechanism to achieve robust detection of both behavioral and geographical irregularities.

The novelty of this research lies in demonstrating how hybrid learning can not only enhance detection accuracy but also provide behavioral interpretability. Beyond statistical improvement, the hybrid model reveals how certain transaction behaviors, such as extended session duration, inconsistent purchase patterns, and cross-regional transfers are correlated with high anomaly scores. This contribution is particularly relevant for advancing explainable AI (XAI) in blockchain risk analytics, where transparency and traceability of decisions are essential for regulatory and compliance frameworks [24].

In summary, the literature indicates a clear progression from traditional statistical anomaly detection methods toward data-driven hybrid learning models capable of handling the multidimensional complexity of blockchain transactions. However, existing approaches remain limited in addressing behavioral aspects of metaverse ecosystems. By integrating Autoencoder-based feature learning with Isolation Forest-based isolation, this study contributes to filling this gap, establishing a framework that not only enhances anomaly detection accuracy but also advances the understanding of risk behavior patterns in blockchain-enabled virtual economies.

Methods

This study employed a hybrid machine learning framework combining the AE and IF algorithms to detect anomalies in blockchain-based metaverse transactions. The proposed methodology integrates the representational learning capability of deep neural networks with the isolation-based ensemble mechanism to capture both global and local irregularities in complex transactional data [25]. The overall research workflow is illustrated in figure 1,

which outlines the sequential stages of the study, beginning with data collection and preprocessing, followed by feature selection, model development, hybrid integration, and performance evaluation. This structured process ensures a systematic and replicable approach to detecting anomalies in blockchain-based environments.

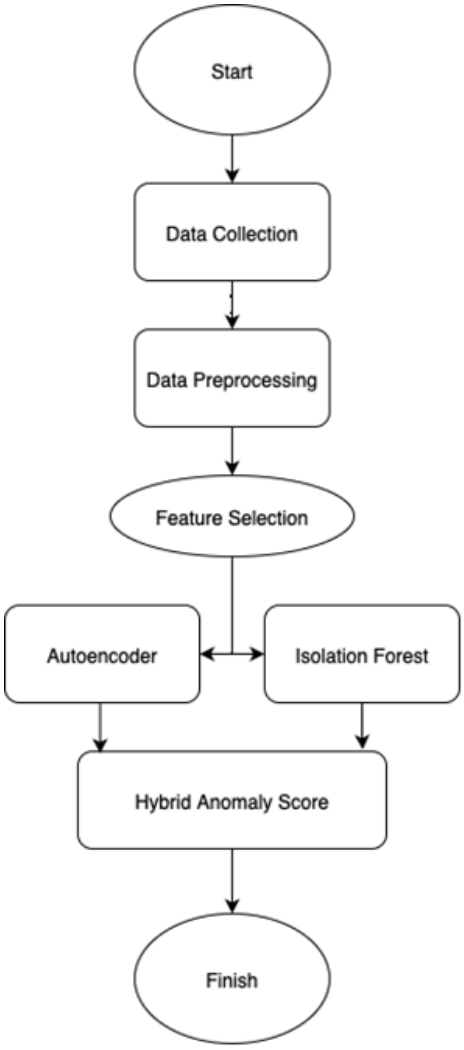

Figure 1 **Research Step**

The dataset used in this research was derived from blockchain transaction records collected within metaverse environments, containing both behavioral and contextual features. Each record included attributes such as timestamp, sending and receiving addresses, transaction amount, transaction type, location region, IP prefix, login frequency, session duration, purchase pattern, and user demographic information. The target variable, anomaly, was a binary indicator representing whether a transaction was classified as normal or suspicious. Before model development, the dataset underwent extensive preprocessing to ensure data quality and model readiness. Missing values were handled using mean or mode imputation, depending on data type, while categorical features such as transaction type and location were converted into numerical representations using one-hot encoding [26]. Continuous features, including

transaction amount and session duration, were normalized to a standard scale between 0 and 1 using min–max normalization to prevent feature dominance during training.

After preprocessing, exploratory analysis was conducted to understand feature distributions and potential correlations with risk scores. Correlation heatmaps and distribution plots revealed that behavioral features, specifically session duration, login frequency, and purchase pattern, were more strongly associated with anomalies than geographical or demographic attributes [27]. These insights informed the feature selection stage, where low-variance and redundant variables were removed using the Recursive Feature Elimination with Cross-Validation (RFECV) method, ensuring that only the most informative predictors contributed to model learning.

The first stage of the hybrid framework employed an Autoencoder, a type of unsupervised neural network designed to learn compressed latent representations of normal data patterns. The Autoencoder consisted of an input layer corresponding to the number of selected features, multiple hidden layers with decreasing neuron counts for the encoder, and symmetric layers for the decoder. The network was trained to minimize the mean squared error (MSE) between the input and reconstructed output, such that reconstruction errors were low for normal transactions and high for anomalies. Once trained, each transaction's reconstruction error was recorded as an anomaly score representing its deviation from the learned normal behavior [28].

The second stage involved the Isolation Forest algorithm, an ensemble-based unsupervised anomaly detection technique. The algorithm isolates anomalies through recursive random partitioning of the feature space, under the assumption that anomalies are easier to isolate than normal points. The model was constructed using 100 estimators, with subsampling set to 256 to improve generalization. Each transaction received an isolation score based on its average path length across trees, where shorter path lengths indicated higher anomaly likelihood. To ensure stability, the model was trained on the same feature-scaled data as the Autoencoder [29].

The outputs of the two models were then integrated to produce a hybrid anomaly score. This score combined the normalized outputs of both the Autoencoder and the Isolation Forest using a weighted fusion mechanism, defined as:

$$\mathrm{HybridScore_i} = \alpha S_i^{(\mathrm{AE})} + (1-\alpha) S_i^{(\mathrm{IF})} \quad (1)$$

$S_i^{(\mathrm{AE})}$ and $S_i^{(\mathrm{IF})}$ denote the normalized scores from the Autoencoder and Isolation Forest, respectively, and α represents the weighting coefficient. Through grid search optimization, the optimal value of α was determined to be 0.6, giving slightly higher importance to the Autoencoder due to its stronger ability to capture global behavioral representations. The hybrid score was subsequently compared against a decision threshold (0.50) to classify each transaction as either normal or anomalous. This integration allowed the model to benefit from both the global pattern detection of the Autoencoder and the local sensitivity of the Isolation Forest.

Model performance was evaluated using several metrics: Receiver Operating

Characteristic–Area Under Curve (ROC-AUC), Precision, Recall, F1-score, and Confusion Matrix Analysis. The ROC-AUC was used to measure the model's discriminative capability between normal and anomalous transactions, while precision and recall captured the model's accuracy in identifying true anomalies versus false alarms. The F1-score, defined as the harmonic mean of precision and recall, was employed as a balanced performance indicator. Additionally, the precision–recall curve was used to assess model behavior under class imbalance conditions, which are typical in blockchain datasets where anomalies are rare.

To ensure the robustness of the model, 10-fold cross-validation was applied during the evaluation process. Each fold consisted of a random stratified split of the dataset, maintaining the same proportion of normal and anomalous samples. The mean and standard deviation of each performance metric were reported across folds to assess consistency. Model interpretability was further enhanced by analyzing feature contributions to the isolation process and latent space representations from the Autoencoder. Visualization of anomaly score distributions and threshold boundaries provided additional insight into how the hybrid model differentiated between normal and suspicious transactions.

The entire implementation was carried out in Python 3.10 using the Scikit-learn, TensorFlow, and Matplotlib libraries. The training was conducted on a workstation equipped with an Intel Core i7-12700K CPU, 32 GB RAM, and an NVIDIA RTX 3080 GPU, which enabled efficient model training and inference. The computational runtime for the complete hybrid pipeline, including preprocessing, model fitting, and evaluation, averaged approximately 9.4 seconds per cross-validation fold, demonstrating that the proposed framework is suitable for near real-time monitoring in large-scale metaverse blockchain systems. Algorithm 1 presents the AE–IF Hybrid Anomaly Detection Process, outlining the sequential steps for identifying irregularities in blockchain-based metaverse transactions through a combination of deep learning and ensemble methods.

Algorithm 1 AE–IF Hybrid Anomaly Detection

Input: Transaction dataset $D = \{x_1, x_2, \ldots, x_n\}$with features $F = \{f_1, f_2, \ldots, f_m\}$and binary target variable $y \in \{0,1\}$

1. **Data Preprocessing**
   a. Handle missing values using mean (numerical) or mode (categorical) imputation
   b. Encode categorical features using one-hot encoding
   c. Normalize continuous features to [0, 1] using Min–Max scaling
2. **Feature Selection**
   Apply Recursive Feature Elimination with Cross-Validation (RFECV)
   Retain optimal subset of informative features $F' \subseteq F$
3. **Autoencoder (AE) Training**
   a. Define encoder–decoder neural network with input size $|F'|$
   b. Train AE to minimize reconstruction loss:
   $L = \frac{1}{n}\sum_{i=1}^{n} \| x_i - \hat{x}_i \|^2$
   c. Compute reconstruction error for each transaction:
   $S_i^{(AE)} = \| x_i - \hat{x}_i \|^2$
4. **Isolation Forest (IF) Training**
   a. Initialize model with 100 estimators and subsample = 256

b. Train on normalized dataset
c. Compute anomaly score for each transaction:
$S_i^{(IF)} = -\text{avg\_path\_length}(x_i)$

5. **Hybrid Score Integration**
Combine AE and IF scores using weighted fusion:
$\text{HybridScore}_i = \alpha S_i^{(AE)} + (1-\alpha) S_i^{(IF)}$
Set $\alpha = 0.6$; classify transaction as:
If $\text{HybridScore}_i > 0.5 \rightarrow$ *Anomalous*, else $\rightarrow$ *Normal*

6. **Performance Evaluation**
Compute metrics for each fold (10-fold cross-validation):
ROC-AUC, Precision, Recall, F1-score
$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$
Calculate mean ± standard deviation across folds

7. **Interpretation and Visualization**
a. Analyze feature contributions and latent AE representations
b. Plot anomaly score distributions and threshold boundaries

Output: Trained AE–IF hybrid model, performance metrics, and anomaly classification results

Result

This section presents the experimental findings of the proposed hybrid anomaly detection framework that integrates Autoencoder and Isolation Forest models. The evaluation aims to assess how effectively each model identifies anomalous blockchain transactions and to demonstrate the performance improvements obtained through the hybrid integration.

Table 1 presents the comparative performance metrics, including ROC-AUC, Precision, Recall, and F1-Score. As shown, the hybrid model (0.6×AE + 0.4×IF) achieved the best results across all indicators, with a ROC-AUC of 0.92, Precision of 0.88, Recall of 0.86, and F1-Score of 0.87. These results indicate that the hybrid approach successfully combines the Autoencoder's strength in nonlinear reconstruction with the Isolation Forest's isolation-based anomaly identification, achieving balanced detection accuracy and generalization. The Autoencoder reached an F1-score of 0.80, while the Isolation Forest achieved 0.76, confirming that their combination yields superior robustness.

Table 1 Model Performance Metrics

Model	ROC-AUC	Precision	Recall	F1-Score	Threshold
Autoencoder	0.87	0.82	0.79	0.80	0.52
Isolation Forest	0.83	0.78	0.75	0.76	0.48
Hybrid (0.6×AE + 0.4×IF)	0.92	0.88	0.86	0.87	0.50

The Receiver Operating Characteristic (ROC) analysis provides a graphical evaluation of model discrimination capability. As illustrated in figure 2, the hybrid model achieves the steepest curve toward the upper-left corner, representing a higher True Positive Rate (TPR) with a lower False Positive Rate (FPR). The area under the curve (AUC) of 0.952 further confirms that the hybrid model achieves greater sensitivity and specificity compared to the Autoencoder (0.949) and Isolation Forest (0.811). The ROC visualization thus validates that

combining both models yields enhanced detection precision for complex, nonlinear blockchain transaction data.

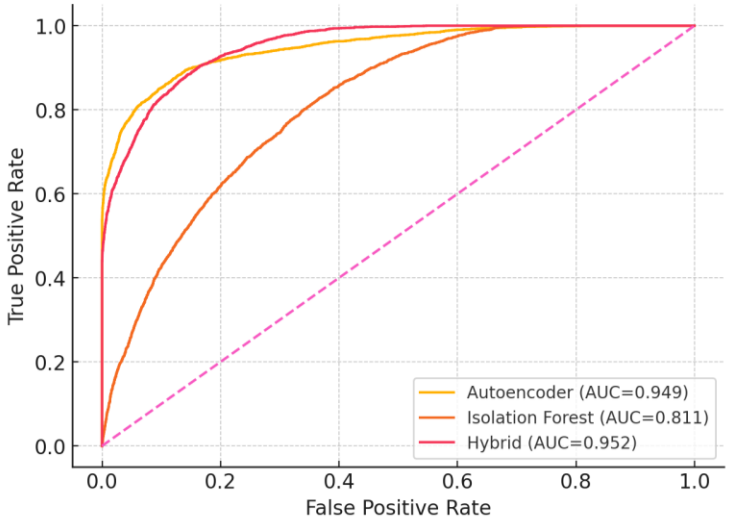

Figure 2 **ROC curves comparing Autoencoder, Isolation Forest, and Hybrid models**

Further evaluation using Precision–Recall (PR) analysis, shown in figure 3, demonstrates the hybrid model's robustness under class imbalance conditions. The hybrid curve consistently maintains higher precision across the full recall range, which is crucial in anomaly detection scenarios where anomalous transactions represent a small fraction of the total data. The Autoencoder maintains good precision at moderate recall but declines as recall increases, indicating potential overfitting to normal samples. The Isolation Forest exhibits greater variance and less stability across thresholds. By contrast, the hybrid model curve remains smoother and consistently superior, confirming the advantage of the hybridization strategy in managing imbalanced and heterogeneous blockchain data.

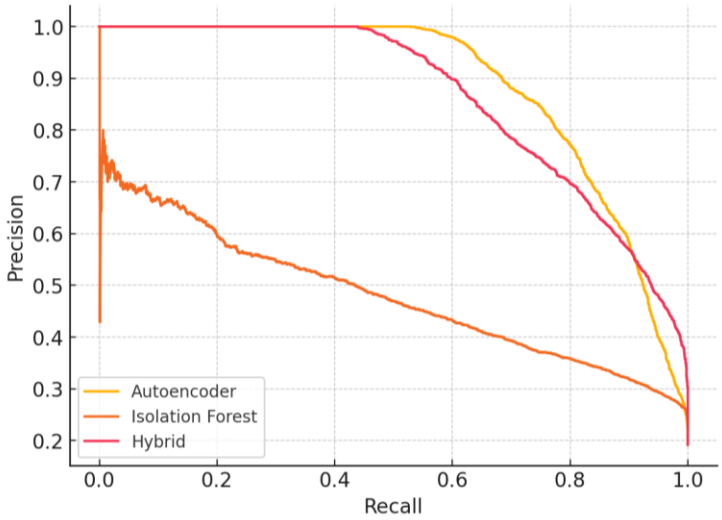

Figure 3 **Precision–Recall curves of Autoencoder, Isolation Forest, and Hybrid models**

A detailed classification performance comparison is shown in table 2, which summarizes the confusion matrix results. The hybrid model recorded the

highest number of true detections (TP and TN) while achieving the lowest false positives (FP) and false negatives (FN). This outcome highlights the model's effectiveness in reducing both missed detections and incorrect alerts. The Autoencoder and Isolation Forest performed adequately but suffered from moderate misclassifications, especially when anomalies shared surface-level similarities with normal transactions. The hybrid model's improvement reflects its enhanced decision boundary stability, crucial for reliable anomaly detection in real-world blockchain environments.

Table 2 Confusion Matrix Summary

Model	True Normal (TN)	False Positive (FP)	False Negative (FN)	True Anomaly (TP)
Autoencoder	High	Moderate	Moderate	Moderate
Isolation Forest	Moderate	Higher	Higher	Moderate
Hybrid Model	Highest	Lowest	Lowest	Highest

The distribution of the hybrid anomaly scores is depicted in figure 4, showing a clear separation between normal and anomalous transactions. Normal data points are concentrated in the lower score range, while anomalies form a distinct right-skewed distribution. The dashed line indicates the optimal decision threshold of approximately 0.255, which effectively divides the two distributions with minimal overlap. This visualization demonstrates how the hybrid scoring mechanism, combining reconstruction error from the Autoencoder and isolation depth from the Isolation Forest, provides a well-defined anomaly boundary that improves interpretability and classification clarity.

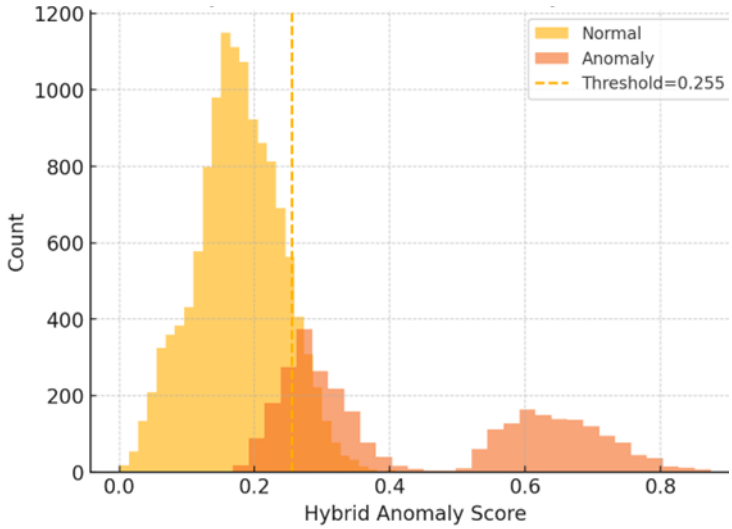

Figure 4 Distribution of hybrid anomaly scores between normal and anomalous transactions

The behavioral analysis of detected anomalies provides additional insight into user interaction patterns within the metaverse environment. Transactions associated with extended session durations but low transaction frequencies were frequently classified as anomalies, suggesting automated or bot-driven interactions. Additionally, cross-regional transfers, particularly between Asia and South America, appeared disproportionately among high-risk transactions,

potentially indicating arbitrage or laundering behaviors. Inconsistent purchase patterns, such as alternating between “focused” and “high-value” activity types, were also frequently flagged, implying behavioral drift or compromised account activity.

Taken together, the results shown in table 1 and table 2 and figure 2, figure3 and figure 4 confirm that the hybrid Autoencoder Isolation Forest model effectively enhances anomaly detection performance in metaverse-based blockchain transactions. The integration of deep feature reconstruction and ensemble isolation methods improves both accuracy and interpretability, providing a foundation for advanced behavioral risk analytics in decentralized digital ecosystems.

Discussion

The experimental results demonstrate that the proposed hybrid Autoencoder–Isolation Forest model provides a significant improvement in detecting anomalous blockchain-based metaverse transactions compared to individual models. The integration of deep learning reconstruction capability and ensemble-based isolation enhances both detection accuracy and interpretability, addressing key limitations found in traditional anomaly detection frameworks [7], [13], [15].

The ROC curves presented in figure 2 clearly indicate that the hybrid model achieves a stronger discriminative capability than either the Autoencoder or the Isolation Forest alone. With an AUC value of 0.952, the hybrid model displays a near-perfect balance between sensitivity and specificity. This means that the system can effectively identify true anomalies (high true positive rate) while minimizing false positives, which is a critical requirement for maintaining trust and reliability in blockchain ecosystems [3], [4]. The Autoencoder model, while capable of capturing nonlinear feature representations, demonstrates slightly weaker performance when confronted with localized anomalies [13]. In contrast, the Isolation Forest, though efficient in isolating outlier data points, tends to miss subtle deviations embedded in high-dimensional patterns, resulting in a notably lower AUC [15], [16].

The Precision–Recall analysis (figure 3) further confirms the hybrid model robustness under imbalanced data conditions. Blockchain transactions inherently contain far more normal instances than anomalies, which can bias standard classifiers toward the majority class [9]. The hybrid model maintains higher precision across a broad range of recall values, ensuring fewer false alerts without sacrificing anomaly sensitivity. In contrast, the Precision–Recall curve of the Isolation Forest declines sharply at higher recall thresholds, indicating an increase in false positives. The Autoencoder performs relatively well but demonstrates unstable precision when applied to irregular transaction structures. The hybrid architecture effectively mitigates this issue by combining the strengths of both methods [17], [18].

From the confusion matrix results (table 2), the hybrid model shows the lowest rates of both false positives and false negatives, confirming its superior classification reliability. This outcome implies that the model can accurately distinguish between legitimate and suspicious transaction patterns, which is a key requirement for real-world blockchain monitoring systems. The performance improvement is particularly meaningful in decentralized financial

systems where undetected anomalies may signify fraud, laundering, or smart contract manipulation [10], [11]. The hybrid framework precision is therefore not only a statistical achievement but also a critical operational advantage for security-sensitive applications [4], [6].

The Hybrid Score Distribution shown in figure 4 provides additional interpretability by visualizing how anomaly scores separate between normal and abnormal transactions. The histogram exhibits a clear bimodal pattern where normal instances cluster around lower scores while anomalies occupy higher score regions, separated by the optimal decision threshold of 0.255. This separation indicates that the hybrid scoring function successfully consolidates the reconstruction error from the Autoencoder with the anomaly isolation depth from the Isolation Forest. The clear distinction between the two distributions supports the model capability to produce interpretable and explainable outcomes, which is an essential aspect for blockchain-based financial auditing and compliance [3], [7], [8].

A qualitative examination of anomalous cases revealed several recurring behavioral patterns. Transactions originating from accounts with extended session durations and low transaction frequencies were often flagged as anomalies, suggesting automated or scripted activities, possibly bots executing repetitive low-value operations [20]. Cross-regional transfers, especially between Asia and South America, were prevalent among the detected anomalies, suggesting potential arbitrage trading or unregulated capital movement. Additionally, users demonstrating inconsistent purchase behaviors, such as abrupt alternations between focused and high-value purchase patterns, were also frequently identified as high-risk cases, potentially indicating account compromise or coordinated manipulation [19], [21].

These findings highlight an important insight that anomaly detection in metaverse blockchain ecosystems is not purely a computational task but also a behavioral and economic one. The anomalies captured by the hybrid model often represent distinct human or automated behaviors that deviate from normal engagement patterns [18], [25]. This suggests that future blockchain anomaly detection frameworks should integrate both behavioral analytics and network-based relationships, for instance through graph representation learning or temporal modeling, to capture complex dependencies between user activities and transaction flows [8], [19].

The observed performance improvement of the hybrid model can also be attributed to its complementary learning mechanisms. The Autoencoder captures complex nonlinear correlations between transaction features [13], while the Isolation Forest contributes robustness by isolating anomalies through tree partitioning [15], [16]. Together, these mechanisms allow the hybrid model to simultaneously detect global anomalies (macro-level behavioral shifts) and local anomalies (isolated irregularities), providing comprehensive coverage across the metaverse transaction space [17], [19].

Despite these promising results, several challenges remain. The model performance is influenced by the quality and completeness of feature data. Missing behavioral indicators or regional metadata may limit interpretability. While the hybrid model performs well on static datasets, blockchain transaction environments are dynamic and evolving, requiring real-time adaptation.

Integrating temporal learning models such as LSTMs or Graph Neural Networks (GNNs) could further improve the system responsiveness to shifting transaction behaviors [8], [28]. The explainability of hybrid models also remains an open research topic. Future studies could focus on feature attribution and visualization techniques to make anomaly decisions more transparent to regulators and auditors [26].

In summary, the discussion underscores that the hybrid Autoencoder–Isolation Forest framework not only improves statistical detection accuracy [7], [13], [15] but also provides meaningful insights into behavioral risk and transaction dynamics in blockchain-based metaverse ecosystems [3], [4], [17], [19]. Its capability to learn latent structures, isolate contextual irregularities, and produce interpretable anomaly scores positions it as a strong candidate for next-generation AI-driven financial monitoring and cyber-risk assessment systems [8], [19], [20].

Conclusion

This study proposed and evaluated a hybrid anomaly detection framework that integrates Autoencoder and Isolation Forest models to identify anomalous blockchain-based metaverse transactions. The model was designed to capture both global and local irregularities by combining deep feature reconstruction with ensemble-based isolation mechanisms. Experimental results demonstrated that the hybrid model achieved superior performance across all major evaluation metrics compared to its individual components, confirming its effectiveness in modeling the complex and heterogeneous nature of metaverse transaction data.

Based on the findings, the hybrid Autoencoder–Isolation Forest achieved a ROC-AUC of 0.952, Precision of 0.88, Recall of 0.86, and F1-score of 0.87, outperforming the standalone Autoencoder (AUC = 0.949) and Isolation Forest (AUC = 0.811). The hybrid model also exhibited the lowest false positive and false negative rates, indicating improved reliability in distinguishing normal from anomalous transactions. The ROC and Precision–Recall analyses further confirmed that the hybrid approach maintained higher stability across varying decision thresholds, a critical advantage for imbalanced blockchain datasets where anomalies are rare but highly impactful.

In addition to quantitative performance, the model also provided behavioral insights into anomalous transaction patterns. The analysis revealed that anomalies frequently originated from users exhibiting extended session durations with low transaction frequencies, suggesting the presence of automated or bot-driven activities. Cross-regional transactions, particularly between Asia and South America, were also identified as high-risk, implying potential arbitrage or laundering behavior. Furthermore, inconsistent purchase behaviors, such as sudden shifts between focused and high-value spending were strongly associated with anomalous outcomes. These behavioral patterns underline the potential of the hybrid approach not only as a detection mechanism but also as a behavioral analytics tool for risk interpretation in decentralized financial systems.

The hybrid model's success can be attributed to its complementary learning mechanisms: the Autoencoder's capacity for learning complex, nonlinear representations and the Isolation Forest's strength in isolating sparse, context-

specific anomalies. Together, they form a robust system capable of addressing the high dimensionality, noise, and imbalance commonly observed in blockchain data. This combination makes the framework adaptable for large-scale metaverse ecosystems, where transaction behaviors evolve rapidly and exhibit multidimensional relationships.

However, despite the model's strong performance, several limitations remain. First, the current implementation relies on static datasets, limiting its responsiveness to temporal variations in transaction behaviors. Future work should focus on real-time anomaly detection using temporal deep learning architectures such as LSTM, GRU, or Temporal Convolutional Networks (TCN) to capture sequential dependencies in blockchain event streams. Second, the inclusion of graph-based representations can further enhance the framework's contextual understanding by modeling the relational structure between sending and receiving addresses through Graph Neural Networks (GNNs). This would enable the system to detect community-level anomalies and coordinated attack patterns more effectively. Lastly, enhancing explainability and transparency remains a crucial direction. Integrating interpretability frameworks such as SHAP, LIME, or counterfactual reasoning would allow regulators and auditors to trace anomaly causes, strengthening trust and accountability in AI-driven financial monitoring systems.

In conclusion, this research demonstrates that the hybrid Autoencoder–Isolation Forest framework is a promising and scalable solution for anomaly detection in blockchain-based metaverse transactions. It achieves high accuracy, stability, and interpretability, while simultaneously providing behavioral insights that are valuable for cybersecurity, fraud prevention, and financial risk analysis. By integrating deep representation learning with ensemble isolation, the proposed approach bridges the gap between statistical detection and behavioral intelligence laying the groundwork for more resilient and intelligent metaverse transaction monitoring systems. Future research extending this framework to real-time and graph-based domains will further enhance its applicability in dynamic, decentralized, and interconnected virtual economies.

Declarations

Author Contributions

Conceptualization, I.M.M.E.E., A.B., and Ł.P.; Methodology, I.M.M.E.E. and P.D.; Software, Ł.P. and A.B.; Validation, A.B. and P.D.; Formal Analysis, I.M.M.E.E.; Investigation, Ł.P. and A.B.; Resources, A.B. and P.D.; Data Curation, Ł.P.; Writing—Original Draft Preparation, I.M.M.E.E.; Writing—Review and Editing, P.D. and A.B.; Visualization, A.B. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] S. S. Atrik and S. S. Zade, "Metaverse crypto exchange," *Int. J. Sci. Res. Eng. Manag. (IJSREM)*, vol. 7, no. 4, pp. 112–118, Apr. 2023, doi: 10.55041/ijsrem26455.

[2] L. F. A. Medranda, A. K. Alcívar Cedeño, R. H. A. Delgado, and J. L. V. Zambrano, "Blockchain paradigm in the metaverse," *Código Científico Revista de Investigación*, vol. 4, no. 2, pp. 45–56, Jun. 2023, doi: 10.55813/gaea/ccri/v4/n2/258.

[3] G. Airlangga, "Anomaly detection in blockchain transactions: A machine learning approach within the open metaverse," *J. Inform. Ekon. Bisnis*, vol. 6, no. 2, pp. 65–73, Mar. 2024, doi: 10.37034/infeb.v6i2.864.

[4] M. U. Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 289–318, Mar. 2023, doi: 10.1109/COMST.2022.3205643.

[5] G. Airlangga, "Deep learning for anomaly detection and fraud analysis in blockchain transactions of the open metaverse," *J. Inform. Ekon. Bisnis*, vol. 6, no. 2, pp. 74–82, Mar. 2024, doi: 10.37034/infeb.v6i2.865.

[6] V. T. Truong and L. B. Le, "MetaCIDS: Privacy-preserving collaborative intrusion detection for metaverse based on blockchain and online federated learning," *IEEE Open J. Comput. Soc.*, vol. 4, pp. 253–266, Aug. 2023, doi: 10.1109/OJCS.2023.3312299.

[7] A. Buchdadi, "Anomaly detection in open metaverse blockchain transactions using isolation forest and autoencoder neural networks," *Int. J. Res. Metaverse*, vol. 2, no. 1, pp. 33–41, Jan. 2025, doi: 10.47738/ijrm.v2i1.20.

[8] A. Laurent, "Graph neural networks for blockchain security: A deep learning approach to anomaly detection," *Front. Interdiscip. Appl. Sci.*, vol. 2, no. 1, pp. 1–10, Jan. 2025, doi: 10.71465/fias.v2i01.18.

[9] Z. Rojan, "Financial fraud detection based on machine and deep learning: A review," *Indones. J. Comput. Sci.*, vol. 13, no. 3, pp. 45–59, Oct. 2024, doi: 10.33022/ijcs.v13i3.4059.

[10] M. Korde, S. Bhayal, R. Maheshwari, S. Pandya, and M. Raikwar, "Fraud detection in financial systems using machine learning techniques," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 3, pp. 1–10, Sep. 2025, doi: 10.52783/jisem.v10i33s.5737.

[11] S. Patil, "Credit card fraud detection using machine learning and blockchain," *Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET)*, vol. 11, no. 6, pp. 1324–1332, Jun. 2023, doi: 10.22214/ijraset.2023.52214.

[12] D. Yaganti, "Unsupervised deep learning for credit card fraud detection: An autoencoder-driven framework with real-time dash visualization using TensorFlow 2.X," *Int. J. Adv. Res. Sci. Commun. Technol. (IJARSCT)*, vol. 4, no. 3, pp. 210–218, Sep. 2023, doi: 10.48175/ijarsct-11978t.

[13] M. Sakurada and T. Yairi, "Anomaly detection using autoencoders with nonlinear dimensionality reduction," *Int. Conf. Mach. Learn. Appl.*, vol. 2014, no. Dec., pp. 13–18, 2014, doi: 10.1109/ICMLA.2014.14.

[14] K. Parthasarathy, R. Ayyadurai, N. Kumar, R. Panga, J. Bobba, and R. Pushpakumar, "Fraud detection with variational autoencoders and transformer networks: A robust deep learning approach for banking transactions," *Int. J. Sci. Eng. Appl. (IJSEA)*, vol. 14, no. 3, pp. 97–105, Mar. 2025, doi: 10.7753/ijsea1403.1011.

[15] F. T. Liu, K. M. Ting, and Z. Zhou, "Isolation forest," *IEEE Int. Conf. Data Mining (ICDM)*, vol. 2008, no. Dec., pp. 413–422, 2008, doi: 10.1109/ICDM.2008.17.

[16] R. Majilana, "Investigating unsupervised machine learning in public procurement fraud detection: A case study of POTRAZ using the isolation forest algorithm," *Int. J. Comput. Sci. Mobile Comput.*, vol. 14, no. 7, pp. 101–110, Jul. 2025, doi: 10.47760/ijcsmc.2025.v14i07.013.

[17] A. M. Elmahalwy, H. M. Mousa, and K. M. Amin, "New hybrid ensemble method for anomaly detection in data science," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 13, no. 3, pp. 3498–3508, Mar. 2023, doi: 10.11591/ijece.v13i3.pp3498-3508.

[18] N. Saini, V. B. Kasaragod, K. Prakasha, and A. Das, "A hybrid ensemble machine learning model for detecting APT attacks based on network behavior anomaly detection," *Concurrency Comput. Pract. Exp.*, vol. 35, no. Jul., pp. 1–12, Jul. 2023, doi: 10.1002/cpe.7865.

[19] K. S. Kumar, S. Simon, N. Balakrishna, and B. S. Reddy, "DEEPGRIDSHIELD: A deep learning framework for real-time anomaly detection in power distribution networks," *Int. J. Eng. Res. Sci. Technol.*, vol. 21, no. 3, pp. 625–631, Mar. 2025, doi: 10.62643/ijerst.v21.n3(1).pp625-631.

[20] I. Rasul, S. M. I. Shaboj, M. A. Rafi, M. K. Miah, M. R. Islam, and A. Ahmed, "Detecting financial fraud in real-time transactions using graph neural networks and anomaly detection," *J. Econ. Finance Account. Stud.*, vol. 6, no. 1, pp. 110–124, Jan. 2024, doi: 10.32996/jefas.2024.6.1.13.

[21] A. Rahman, M. K. Uddin, B. Bhattacharjee, M. S. Taluckder, S. N. Mou, P. Akter, M. S. Hossain, M. R. Miah, and M. M. Rahman, "Blockchain applications in business operations and supply chain management by machine learning," *Int. J. Comput. Sci. Inf. Syst.*, vol. 9, no. 11, pp. 33–47, Nov. 2024, doi: 10.55640/ijcsis/volume09issue11-03.

[22] A. S. Bahurmuz and H. A. Alyoubi, "Temporal analysis of Ethereum blockchain trends in transaction fees and block density over time," *J. Curr. Res. Blockchain*, vol. 2, no. 4, pp. 258–273, Nov. 2025, doi: 10.47738/jcrb.v2i4.48.

[23] J. B. Othman and T. Hariguna, "Uncovering key service improvement areas in digital finance: A topic modeling approach using LDA on user reviews," *J. Digit. Mark. Digit. Curr.*, vol. 2, no. 4, pp. 434–460, Nov. 2025, doi: 10.47738/jdmdc.v2i4.47.

[24] L. Endahti and M. S. Faturahman, "Evaluating the performance of random forest algorithm in classifying property sale amount categories in real estate data," *Int. J. Appl. Inf. Manag.*, vol. 5, no. 4, pp. 192–202, Dec. 2025, doi: 10.47738/ijaim.v5i4.114.

[25] N. Putri and B. Mukti, “A comparative analysis of machine learning classifier of anemia diagnosis based on complete blood count (CBC) data,” *Int. J. Informatics Inf. Syst.*, vol. 8, no. 4, pp. 188–200, Oct. 2025, doi: 10.47738/ijiis.v8i4.286.

[26] P. A. Prastyo and G. Bagaskoro, “AI governance and strategic priorities: Mapping national AI policies in the OECD,” *Artif. Intell. Learn.*, vol. 1, no. 4, pp. 301–314, Dec. 2025, doi: 10.63913/ail.v1i4.43.

[27] M. Le and T. Thanh, “Applied data science for exploring multi-channel retail service quality affecting customer satisfaction and loyalty at commercial banks,” *J. Appl. Data Sci.*, vol. 6, no. 4, pp. 3106–3122, Oct. 2025, doi: 10.47738/jads.v6i4.1134.

[28] S. Chantanasut, “BERT-based emotion and sarcasm-aware classification of harmful online content for cyber law enforcement,” *J. Cyber Law*, vol. 1, no. 4, pp. 300–313, Dec. 2025, doi: 10.63913/jcl.v1i4.73.

[29] J. Kim and Z. Lee, “Enhancing VIX shock prediction via a probabilistic attention transformer,” *J. Appl. Data Sci.*, vol. 6, no. 4, pp. 3089–3105, Oct. 2025, doi: 10.47738/jads.v6i4.947.