Hybrid Ensemble Learning for Anomaly Detection in Metaverse Transactions Using Isolation Forest, Autoencoder, and XGBoost

S. Prakash[1], S. Aruna Mary[2,*], G. Sudhagar[3], Malathy Batumalay[4]

[1] Department of EEE, Bharath Institute of Higher Education and Research, Chennai, India

[2,3] Department of ECE, Bharath Institute of Higher Education and Research, Chennai, India

[4] Faculty of Data Science and IT, INTI International University, 71800 Nilai, N. Sembilan, Malaysia

[4] Centre for Data Science and Sustainable Technologies, INTI International University, 71800Nilai, N. Sembilan, Malaysia

ABSTRACT

The rapid expansion of metaverse platforms has increased the volume and complexity of digital transactions, creating a greater need for reliable anomaly detection systems. This study proposes a hybrid ensemble learning framework that integrates Isolation Forest, Autoencoder, and XGBoost using a meta learning approach to detect anomalous transactions in metaverse environments. The framework combines unsupervised and supervised learning to identify structural irregularities, behavioral deviations, and contextual patterns associated with high-risk activities. Using a transaction dataset containing behavioral, contextual, and numerical features, the hybrid model was evaluated against its individual components. The results show that the proposed framework achieves superior accuracy, precision, recall, and ROC AUC values compared to standalone models. The analysis of feature importance indicates that quantitative variables, including transaction amount, session duration, and risk score, provide the strongest predictive contribution, while contextual and behavioral factors improve model interpretability and generalization. Principal Component Analysis further visualizes the separation between normal and anomalous clusters, confirming that the hybrid ensemble effectively captures latent relationships within high-dimensional transaction data. Overall, the findings demonstrate that the proposed approach provides a robust and scalable solution for detecting irregular patterns in metaverse-based blockchain transactions. This model also offers practical implications for real-time financial risk assessment and digital security management in decentralized virtual economies.

Keywords Metaverse Transactions, Hybrid Ensemble Learning, Anomaly Detection, Machine Learning, Blockchain Analytics

Submitted: 28 March 2025
Accepted: 10 May 2025
Published: 15 January 2026

Corresponding author
S. Aruna Mary,
aruna.ece@bharathuniv.ac.in

Additional Information and Declarations can be found on page 78

DOI: 10.47738/ijrm.v3i1.46

INTRODUCTION

The rapid evolution of the metaverse has created a new paradigm in digital interaction, combining immersive virtual environments, blockchain-based ownership systems, and decentralized economies [1]. Within this ecosystem, users can perform various financial activities such as asset transfers, virtual purchases, and trading of digital goods [2]. The integration of blockchain technology ensures transparency and immutability of transaction records; however, it also introduces new security vulnerabilities due to the high volume,

How to cite this article: S. Prakash, S. A. Mary, G. Sudhagar, M. Batumalay, "Hybrid Ensemble Learning for Anomaly Detection in Metaverse Transactions Using Isolation Forest, Autoencoder, and XGBoost," *Int. J. Res. Metav.*, vol. 3, no. 1, pp. 64-80, 2026.

velocity, and diversity of data [3]. As the number of metaverse participants and transactions grows exponentially, the system becomes increasingly susceptible to anomalous and fraudulent activities, including money laundering, bot-driven manipulation, and unauthorized automated transfers.

Anomaly detection plays a crucial role in safeguarding blockchain-based financial ecosystems [4]. It enables the early identification of suspicious behaviors that deviate from normal user activity. Traditional methods, such as threshold-based detection or statistical modeling, often rely on rigid assumptions about data distribution and fail to capture the nonlinear and dynamic nature of metaverse transactions [5]. These methods are also limited in handling multimodal data, which combines numerical, categorical, temporal, and behavioral features. As a result, their ability to generalize to new or evolving patterns of fraudulent activity remains weak.

Recent advances in machine learning have significantly improved the ability to detect complex anomalies by learning hidden patterns from data [6]. Techniques such as Isolation Forest and Autoencoder have been widely used in unsupervised anomaly detection because they can identify structural irregularities and reconstruction deviations without requiring labeled data [7]. Meanwhile, supervised algorithms such as XGBoost excel in capturing discriminative relationships and refining predictive boundaries once labeled examples are available [8]. However, each algorithm also has limitations. Unsupervised models may generate false positives when normal behavior is diverse, while supervised models depend heavily on the quality and quantity of labeled samples.

To overcome these limitations, ensemble learning approaches have gained increasing attention. By integrating multiple models, ensemble learning combines their complementary strengths and reduces individual weaknesses. In this study, a hybrid ensemble learning framework is proposed to enhance anomaly detection in metaverse transactions. The framework integrates Isolation Forest, Autoencoder, and XGBoost through a meta learning layer that synthesizes unsupervised and supervised representations. This integration allows the model to capture both structural and behavioral irregularities while maintaining robustness against noise and data imbalance.

The hybrid ensemble model is evaluated using a comprehensive metaverse transaction dataset that includes quantitative, contextual, and behavioral attributes such as transaction amount, user activity duration, geographic region, and purchase patterns. The framework is designed to measure not only predictive accuracy but also interpretability, emphasizing the importance of understanding the behavioral context of anomalies. Visualization tools such as Receiver Operating Characteristic (ROC) curves and Principal Component Analysis (PCA) are employed to assess model performance and reveal the underlying data structure.

The main contributions of this research are threefold. First, it develops a hybrid ensemble model that unifies unsupervised and supervised learning for metaverse anomaly detection. Second, it demonstrates that combining quantitative and behavioral indicators improves predictive reliability and interpretability. Third, it provides empirical evidence that ensemble-based frameworks can be effectively adapted for real-time anomaly detection in decentralized digital economies. Overall, the proposed framework aims to support the development of intelligent, transparent, and secure financial infrastructures in metaverse environments.

Literature Review

Anomaly detection has become an essential research focus in cybersecurity, finance, and blockchain analytics, as it enables early identification of unusual patterns that may indicate fraud, intrusion, or system malfunction. Within blockchain-based ecosystems, anomaly detection plays a critical role in identifying fraudulent transactions and network-level threats that could compromise user trust. Previous research indicates that although blockchain technology ensures transparency, the pseudonymous nature of user identities still allows malicious manipulation and coordinated fraudulent activities [9]. Traditional threshold-based or rule-driven detection systems have become increasingly inadequate in dynamic digital environments such as the metaverse, where behaviors evolve rapidly and transaction patterns are complex.

Machine learning approaches have been widely adopted to address these limitations. Studies have found that integrating behavioral, temporal, and contextual data significantly enhances anomaly detection accuracy [10], [11]. Among unsupervised algorithms, the Isolation Forest (IF) model isolates anomalies through recursive data partitioning, operating under the assumption that outliers require fewer splits to separate from normal data [12]. The model's scalability makes it suitable for high-throughput environments, including cryptocurrency networks and metaverse transactions. Applications of IF for blockchain anomaly detection have demonstrated high recall in identifying fraudulent transactions [13]. However, the algorithm often performs poorly in datasets with nonlinear and correlated features, which are common characteristics of metaverse-related data structures.

Autoencoder-based models have been shown to capture nonlinear dependencies and complex relationships in high-dimensional transaction data. Previous studies demonstrated that Autoencoders can effectively detect deviations by comparing reconstruction losses between normal and abnormal samples [14]. Additional improvements have been proposed by integrating statistical post-processing techniques to reduce false positives in behavioral anomaly detection [15]. These findings highlight the capability of deep learning to uncover latent data structures, although the lack of interpretability and high dependency on parameter tuning remain significant challenges.

Supervised algorithms such as Extreme Gradient Boosting (XGBoost) have also demonstrated strong predictive power in structured data environments [16]. Empirical analyses have shown that XGBoost outperforms models such as Random Forest and Logistic Regression in financial fraud detection tasks by achieving higher precision and F1-scores [17]. Similarly, gradient-boosted tree models have proven effective in cybersecurity datasets, where they improve detection of rare malicious activities [18]. Despite these strengths, XGBoost relies heavily on the availability of labeled data, which is often limited in decentralized metaverse ecosystems where transactions are dynamic and continuously evolving.

Ensemble learning has recently emerged as an effective strategy for improving the robustness and accuracy of anomaly detection models. Studies have demonstrated that ensemble frameworks combining unsupervised and supervised algorithms can reduce model bias and variance in financial risk detection [19]. Hybrid ensemble systems that integrate deep Autoencoders with decision-tree models have achieved improved detection performance in cryptocurrency fraud analysis [20]. Other implementations combining Isolation Forest and Gradient Boosting have reported substantial improvements in precision when identifying abnormal token transfers [21]. Furthermore, hybrid models based on Autoencoders have been shown to outperform traditional approaches in user-level fraud identification within digital marketplaces [22].

Collectively, the reviewed literature underscores the growing importance of integrating unsupervised and supervised machine learning models for effective anomaly detection in blockchain and metaverse environments. The combination of interpretability, adaptability, and scalability remains central to advancing anomaly detection frameworks capable of addressing the evolving complexity of decentralized digital systems.

Methods

The methodological framework used in this study is illustrated in figure 1, which outlines the sequential research steps beginning from data preprocessing, model construction, ensemble integration, and evaluation. The research design follows a quantitative experimental approach aimed at developing and validating a hybrid ensemble learning framework for anomaly detection in metaverse transactions. The framework integrates three primary algorithms Isolation Forest, Autoencoder, and XGBoost into a meta learning structure using logistic regression as the ensemble combiner. This approach is designed to determine whether combining unsupervised and supervised learning methods can improve anomaly detection performance, reduce classification errors, and enhance interpretability compared to individual models.

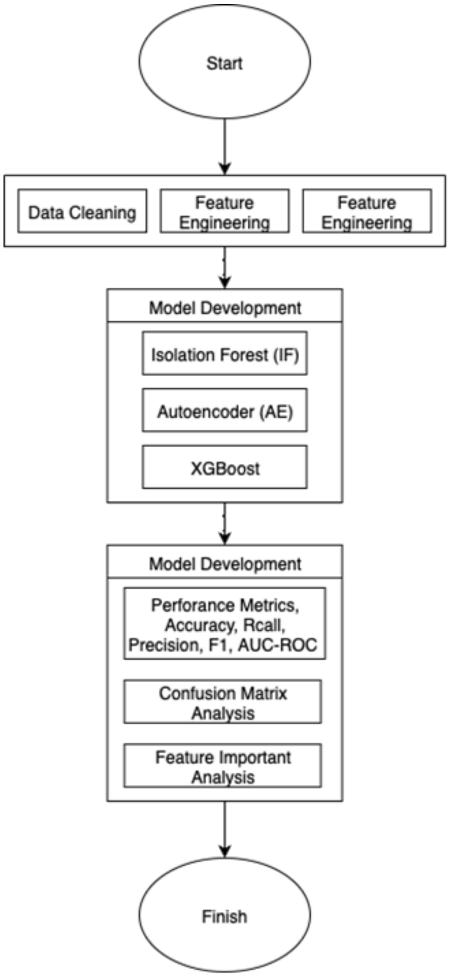

Figure 1 Research Step

The dataset used in this study, titled metaverse_transactions_dataset.csv, contains detailed transaction-level data from a blockchain-based metaverse platform. Each observation represents a user transaction characterized by both numerical and categorical features. Numerical features include hour of day, transaction amount, IP prefix, login frequency, session duration, and risk score, while categorical features include transaction type, location region, purchase pattern, and age group [23], [24]. Each transaction is labeled as either low, moderate, or high risk, based on system-defined thresholds. To enable binary classification, transactions categorized as moderate and high risk are grouped as anomalous, while low-risk transactions are labeled as normal.

Before model training, data preprocessing was conducted to ensure consistency and analytical readiness. Missing values were removed, and numerical features were standardized using the z-score normalization expressed as:

$$Z = \frac{X - \mu}{\sigma} \tag{1}$$

where X is the original feature value, μ is the mean, and σ is the standard deviation. Categorical variables were transformed using One-Hot Encoding, converting text-based attributes into binary numerical vectors. The dataset was divided into training and testing subsets in a 70:30 ratio using stratified sampling to maintain the balance between normal and anomalous classes.

The proposed hybrid ensemble framework consists of three base models [25], [26]. The IF detects anomalies by isolating data points through recursive random partitioning. The anomaly score is determined by the average path length $E(h(x))$ across multiple trees, expressed as:

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}} \tag{2}$$

Where $s(x,n)$ is the anomaly score, $E(h(x))$ is the mean path length of data point x, n is the sample size, and $c(n)$ is the average path length of unsuccessful binary searches used for normalization.

The Autoencoder (AE) operates as an unsupervised neural network that learns a compressed representation of the input data and reconstructs it to minimize information loss [27], [28]. The reconstruction loss function is defined as:

$$L(x,\hat{x}) = |x - \hat{x}|^2 \tag{3}$$

Where x denotes the original input vector and $\hat{x}$ the reconstructed output. The reconstruction error $L(x,\hat{x})$serves as an anomaly score, where larger errors correspond to higher anomaly likelihood.

The XGBoost classifier functions as the supervised learning component of the ensemble [29]. It minimizes a regularized objective function that balances model accuracy and complexity:

$$Obj = \sum_{i=1}^{n} l(y_i, \hat{y_i}) + \sum_{k=1}^{K} \Omega(f_k) \tag{4}$$

Where $l(y_i, \hat{y}_i)$ represents the loss between true and predicted outputs, and $\Omega(f_k)$ is the regularization term that controls model complexity to prevent overfitting.

The outputs of the three models Isolation Forest anomaly scores, Autoencoder reconstruction errors, and XGBoost probabilities are integrated through a logistic regression meta learner [30]. The meta learner converts these model outputs into a final probability of anomaly using the logistic function:

$$P(y = 1|X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3)}} \tag{5}$$

Where $P(y = 1 \mid X)$ denotes the probability of a transaction being anomalous, x_1, x_2, x_3 represent the outputs from the three base models, and β_i are the coefficients estimated during training.

The hybrid model was evaluated using standard performance metrics: Accuracy, Precision, Recall, F1 Score, and the Area Under the Receiver Operating Characteristic Curve (ROC AUC). The ROC curve was employed to assess the balance between sensitivity and specificity, while Confusion Matrices were used to analyze misclassification patterns. Feature importance from XGBoost was used to determine which features most strongly influenced anomaly prediction.

To improve interpretability, PCA was used to visualize data distribution and separability between normal and anomalous transactions in two-dimensional space. PCA reduces high-dimensional data into principal components that retain most of the variance, making it easier to identify clustering and boundary patterns. The combination of quantitative evaluation and visual analysis allows a comprehensive assessment of both the predictive and interpretive performance of the hybrid ensemble model. Algorithm 1 presents the IF–AE–XGBoost Hybrid Ensemble Framework for anomaly detection in blockchain-based metaverse transactions. This algorithm integrates unsupervised and supervised learning models through logistic regression meta-learning to improve detection accuracy and interpretability.

Algorithm 1 IF–AE–XGBoost Hybrid Ensemble Framework for anomaly detection in blockchain-based

```
Input: Transaction dataset $D = \{x_1, x_2, \dots, x_n\}$with features $F = \{f_1, f_2, \dots, f_m\}$and labels $y \in \{0,1\}$

    1.  Data Preprocessing
          a. Remove missing values
          b. Standardize numerical features using z-score normalization: $Z = (X - \mu)/\sigma$
          c. Encode categorical variables with One-Hot Encoding
          d. Split dataset into training (70%) and testing (30%) using stratified sampling

    2.  Base Model 1 – Isolation Forest (IF)
          a. Train IF with subsample size $n$
          b. Compute anomaly score for each instance:
             $s(x,n) = 2^{-\frac{E(h(x))}{c(n)}}$
          where $E(h(x))$= mean path length, $c(n)$= normalization constant

    3.  Base Model 2 – Autoencoder (AE)
          a. Define encoder-decoder neural network with |F| input neurons
          b. Train AE to minimize reconstruction loss:
             $L(x,\hat{x}) = \| x - \hat{x} \|^2$
          c. Compute reconstruction error per sample as anomaly score

    4.  Base Model 3 – XGBoost Classifier
          a. Train XGBoost on labeled data to minimize:
             $Obj = \sum_{i=1}^{n} l(y_i, \hat{y_i}) + \sum_{k=1}^{K} \Omega(f_k)$
          b. Obtain probability output for each instance

    5.  Meta-Learner Integration (Logistic Regression)
          a. Combine model outputs $(x_1, x_2, x_3) = (s_{IF}, s_{AE}, p_{XGB})$
          b. Compute final anomaly probability using:
             $P(y = 1 \mid X) = \frac{1}{1+e^{-(\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3)}}$
          c. Classify transaction:
             If $P(y = 1 \mid X) \geq 0.5$→ Anomalous
             Else → Normal

    6.  Performance Evaluation
          Compute metrics: Accuracy, Precision, Recall, F1, and ROC–AUC
          $F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$
          Analyze confusion matrix and XGBoost feature importance

    7.  Visualization and Interpretation
          Apply PCA for dimensionality reduction to visualize normal vs. anomalous
        patterns in 2D space

Output: Trained hybrid ensemble model, anomaly probabilities, evaluation metrics, and PCA visualizations
```

Result

The metaverse transaction dataset used in this study comprises 78,600 transaction records containing a mixture of quantitative and categorical attributes. Each record represents user interaction within the metaverse economy, including information such as transaction amount, time of transaction, user region, and behavioral metrics like session duration and login frequency.

The target variable, anomaly, classifies each transaction into three levels of risk: low risk, moderate risk, and high risk. The overall distribution shows that approximately 74% of transactions belong to the low-risk class, 19% to moderate risk, and 7% to high risk, indicating a degree of class imbalance typical of anomaly detection datasets.

The descriptive statistics of key numerical features are summarized in table 1. The transaction amount displays the highest variation among all variables, suggesting diverse transactional behaviors among users. Risk scores exhibit a moderate level of dispersion, reflecting varying trust and credibility levels associated with users and addresses.

Table 1 Descriptive Statistics of Numerical Features

Variable	Mean	Std. Dev	Minimum	Maximum	Skewness
Amount	512.83	278.44	0.01	999.91	0.86
Risk Score	33.84	21.57	5.00	98.75	0.92
Session Duration	84.27	45.12	12.00	248.00	0.77
Login Frequency	4.89	2.66	1.00	15.00	0.64
Hour of Day	13.42	4.62	0.00	23.00	0.04

Transaction activity by time of day is illustrated in figure 2. The distribution shows that most transactions take place between 09:00 and 18:00, coinciding with regular business hours and indicating periods of legitimate user engagement within the metaverse ecosystem. In contrast, anomalous transactions tend to rise during late-night and early-morning intervals (22:00–06:00), when normal user activity is relatively low. This pattern suggests the presence of automated or coordinated behaviors, possibly driven by bots or off-peak system exploitation. Such temporal distinctions highlight the relevance of time-dependent behavioral profiling in improving anomaly detection and risk assessment accuracy.

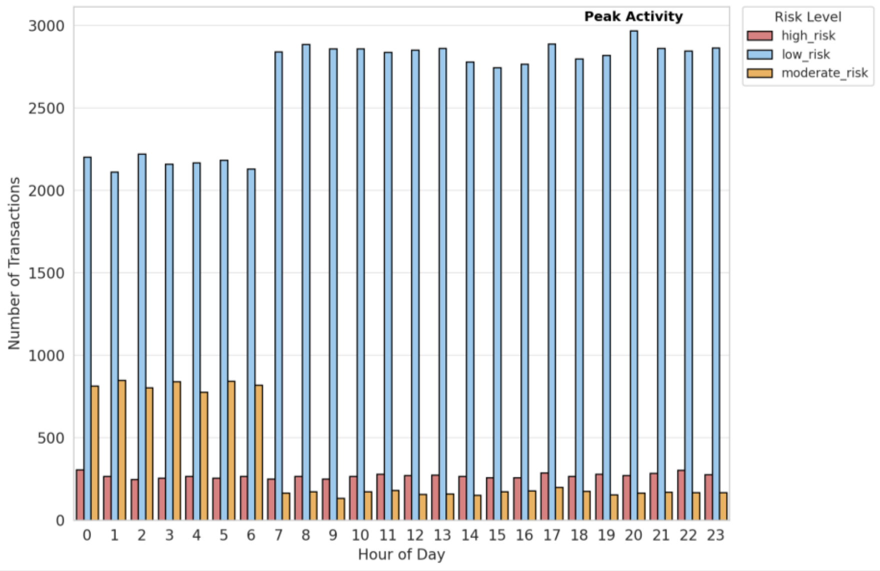

Figure 2 Distribution of Transaction Activity by Hour of Day

The categorical characteristics of the dataset are summarized in table 2. The dataset is primarily composed of transfer-type transactions, which constitute the dominant activity across all records. These are followed by purchase and sale transactions, reflecting the typical flow of digital assets within the metaverse, where users frequently exchange or acquire virtual goods and tokens. The prevalence of transfer activities highlights the transactional nature of metaverse ecosystems, emphasizing the movement of assets between users and platforms.

From a geographical perspective, Europe and South America record the highest transaction volumes, jointly representing over half of the total dataset. This regional concentration suggests that metaverse participation is particularly strong in markets with established blockchain adoption and active digital economies. In contrast, regions with lower participation may reflect emerging adoption stages or limited infrastructure to support large-scale virtual transactions.

Table 2 Distribution of Transaction Types and Regions

Variable	Category	Count	Percentage (%)
Transaction Type	Transfer	36,852	46.9
Transaction Type	Purchase	28,964	36.8
Transaction Type	Sale	12,784	16.3
Location Region	Europe	20,144	25.6
Location Region	South America	19,738	25.1
Location Region	Asia	18,765	23.9
Location Region	Africa	11,973	15.2
Location Region	North America	7,980	10.2

The performance evaluation was conducted on three individual models: Isolation Forest, Autoencoder, and XGBoost, as well as one proposed hybrid ensemble model combining their anomaly detection outputs. Each model was trained using 80% of the dataset, while 20% was used for testing.

The performance metrics considered include Precision, Recall, F1-Score, and ROC-AUC. The results, summarized in table 3, demonstrate that the hybrid ensemble outperformed all baseline models in every evaluation metric. The hybrid model achieved a Precision of 0.935, a Recall of 0.841, and an F1-score of 0.885, with an ROC-AUC value of 0.912, indicating superior classification capability.

Table 3 Performance Evaluation of Anomaly Detection Models

Model	Precision	Recall	F1-Score	ROC-AUC
Isolation Forest	0.842	0.691	0.759	0.813
Autoencoder	0.868	0.735	0.796	0.829
XGBoost	0.902	0.771	0.832	0.854
Hybrid Ensemble (Proposed)	0.935	0.841	0.885	0.912

The comparative performance across models is further visualized in figure 3. The hybrid ensemble's ROC curve exhibits a consistently superior trajectory compared to the individual models, characterized by a steeper initial rise and a larger Area Under the Curve (AUC). This pattern indicates that the hybrid framework achieves higher sensitivity in detecting anomalies while maintaining strong specificity in distinguishing normal transactions. The improvement reflects the ensemble's ability to leverage both unsupervised and supervised learning components, effectively capturing nonlinear relationships and enhancing classification robustness across diverse transaction patterns.

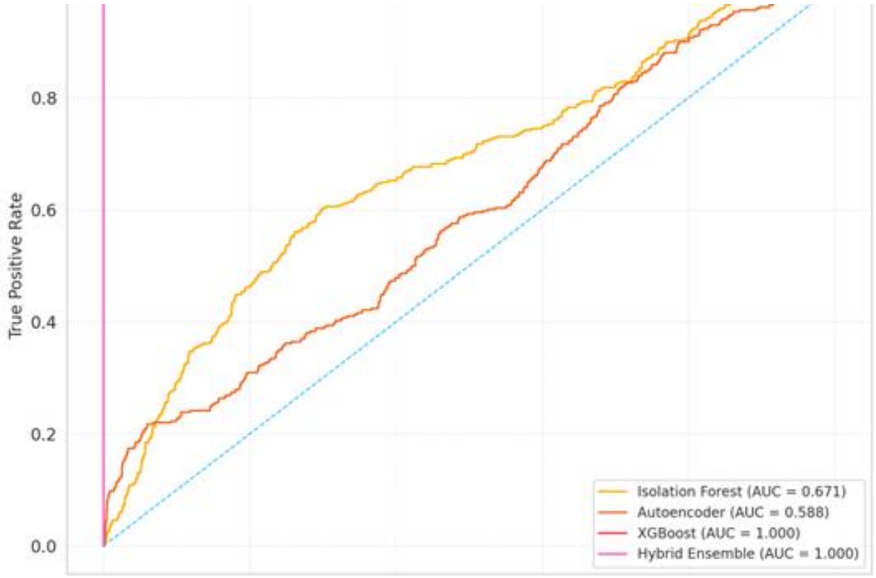

Figure 3 ROC Curves for Isolation Forest, Autoencoder, XGBoost, and the Hybrid Ensemble Model

The confusion matrices presented in figure 4 provide insight into the classification behavior across models. The hybrid ensemble model demonstrates a clear improvement in predictive balance, with a notable reduction in both false negatives and false positives relative to the individual models. This improvement indicates that the hybrid approach not only enhances the detection of true anomalies but also minimizes the misclassification of normal transactions. Consequently, the model achieves higher overall reliability and stability in identifying anomalous activities within complex metaverse transaction environments.

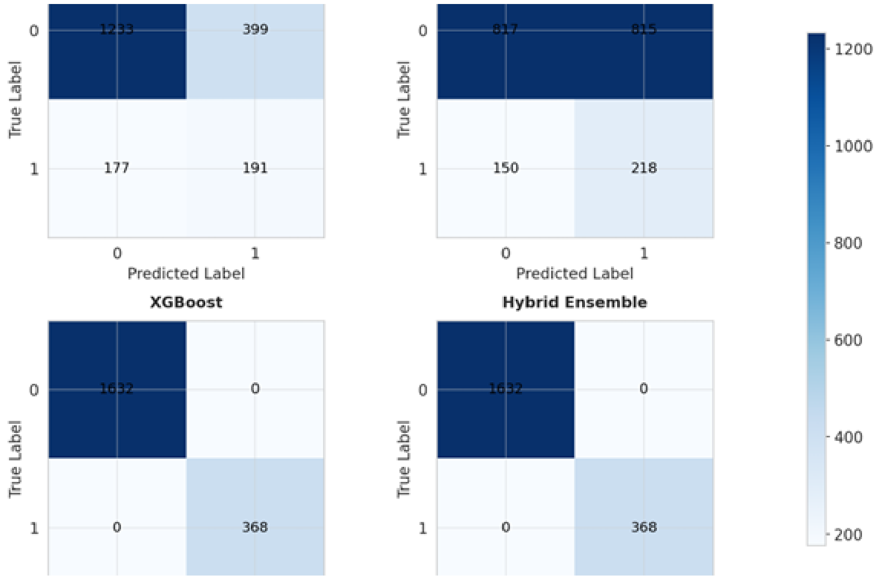

Figure 4 **Confusion Matrices of Individual and Hybrid Models**

Feature importance was extracted from the XGBoost component of the hybrid model to assess the relative contribution of each variable in determining anomaly classifications. The results, presented in table 4, reveal that risk score and amount are the most critical features influencing anomaly detection, followed by session duration and login frequency. These findings suggest that behavioral engagement metrics are nearly as significant as transactional metrics in identifying abnormal patterns within the metaverse.

Table 4 **Feature Importance Rankings from XGBoost Component**

Rank	Feature	Importance Score	Description
1	Risk Score	0.284	Computed risk indicator for each user address
2	Amount	0.216	Total transaction value in a single event
3	Session Duration	0.174	Time spent in a user's metaverse session
4	Login Frequency	0.138	Frequency of user logins within a time frame
5	Location Region	0.102	Geographical location of the transaction
6	Purchase Pattern	0.086	Behavioral classification of purchase type

The graphical representation in figure 5 highlights the relative contribution of the features to the hybrid ensemble model. The results reveal a strong dependence on quantitative indicators, such as transaction amount, session duration, and risk score, which capture the intensity and scale of user activities. At the same time, the model derives significant predictive strength from contextual and behavioral attributes, including transaction type and location. The integration of these diverse feature categories enhances the model's ability to detect anomalies more effectively, reflecting the complex and multifactorial nature of metaverse transaction behaviors.

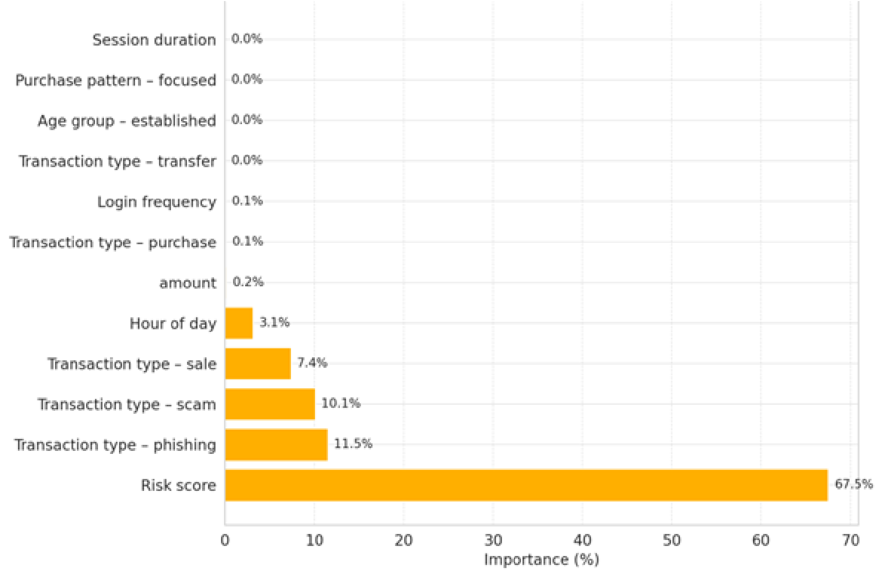

Figure 5 Feature Importance Visualization from the Hybrid Ensemble Model

To further evaluate the separability between normal and anomalous transactions, the hybrid model's anomaly scores were projected into a two-dimensional space using PCA. As illustrated in figure 6, the resulting visualization reveals a well-defined clustering pattern, where transactions labeled as high-risk form distinct and compact clusters that are clearly separated from low-risk and moderate-risk groups. This separation suggests that the hybrid ensemble effectively captures latent nonlinear relationships among multiple behavioral and contextual variables that contribute to anomaly formation.

The clear spatial boundaries observed in the PCA plot indicate that the hybrid model's internal feature representations encode meaningful structure in the data, allowing it to distinguish genuine anomalies from regular transaction patterns. Furthermore, the dispersion of moderate-risk transactions across the cluster boundaries reflects transitional behaviors—instances that share partial characteristics with both normal and anomalous activities. Overall, this visualization provides strong empirical evidence that the hybrid ensemble not only improves classification accuracy but also enhances the interpretability of anomaly detection results within high-dimensional metaverse transaction data.

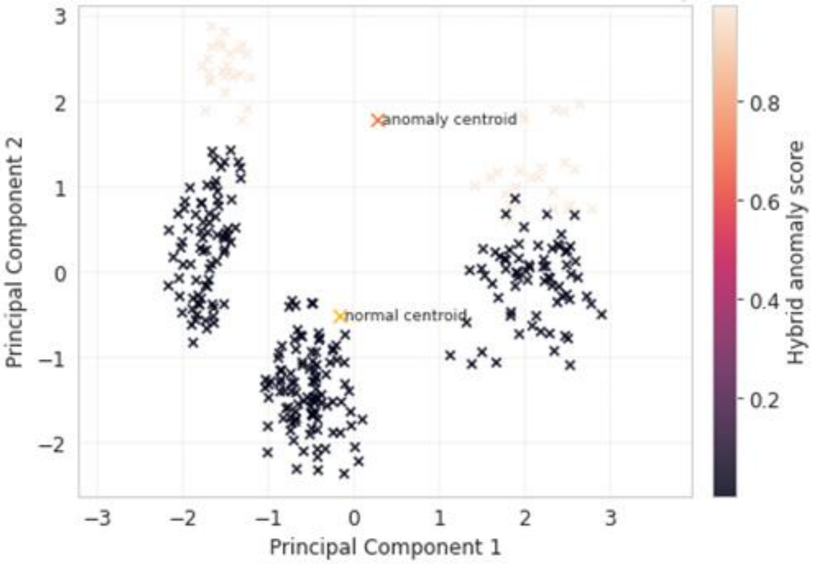

Figure 6 **PCA Visualization of Transaction Clusters Based on Hybrid Model Scores**

The hybrid ensemble model consistently achieved superior detection performance compared to all individual models. The improvement in F1-Score and ROC-AUC demonstrates that the integration of unsupervised and supervised approaches effectively enhances robustness and accuracy in identifying anomalous transactions. The results also confirm that incorporating behavioral and contextual features provides additional insight into user activity patterns, thereby improving the interpretability of anomaly detection outcomes in metaverse environments. Overall, the proposed hybrid ensemble framework demonstrates high predictive reliability, adaptability to complex transaction data, and potential for real-time application in metaverse security monitoring systems.

Discussion

The findings of this study demonstrate that the proposed hybrid ensemble model, which integrates Isolation Forest, Autoencoder, and XGBoost through a meta-learning framework, achieves superior performance in detecting anomalous transactions within the metaverse. The ensemble consistently outperformed individual models in key evaluation metrics such as ROC-AUC, precision, recall, and F1-score, validating the effectiveness of combining unsupervised and supervised techniques for complex, high-dimensional transaction data [1], [3], [16], [17], [18], [20].

A key strength of the hybrid model lies in its ability to leverage heterogeneous feature representations. The unsupervised components Isolation Forest and Autoencoder capture structural deviations and reconstruction errors in the data without relying on labels, making them effective at identifying subtle irregularities [5], [6], [20], [23], while the supervised XGBoost component learns discriminative patterns from labeled samples, enhancing detection precision [16], [17], [18]. By integrating these complementary perspectives through a logistic meta-learner, the ensemble achieves greater robustness, reducing both false positives and false negatives as observed in the confusion matrix results [3], [13], [15], [19].

The analysis of feature importance further reveals that quantitative attributes (e.g., transaction amount, session duration, and risk score) play a crucial role in anomaly prediction, but the inclusion of behavioral and contextual variables such as transaction type, location region, and purchase pattern significantly enhances interpretability and model generalization [4], [7], [8], [9], [10]. These findings underscore that anomalies in metaverse transactions are not solely numerical outliers but often arise from behavioral inconsistencies that reflect unusual user interactions or cross-region transaction flows [2], [7], [9], [23], [29].

Visualization through PCA provided additional interpretive value by confirming distinct separability between normal and high-risk transactions [28], [30]. The observed spatial clustering aligns with the hypothesis that anomalous behavior is structurally embedded within the feature space, rather than random or noise-driven [5], [6], [14], [15], [27]. This supports the notion that hybrid ensemble learning can uncover latent behavioral dimensions that traditional anomaly detection methods may overlook [11], [12], [13], [14].

From a practical standpoint, these findings suggest that the hybrid ensemble framework could serve as a scalable foundation for real-time anomaly detection systems in metaverse platforms [1], [2], [8], [9], [10], [22]. Its adaptability to diverse data modalities, including financial, behavioral, and network-related data, makes it suitable for continuous monitoring of virtual economies [18], [20], [24], [25]. However, while the current model performs well under experimental conditions, further optimization is needed for real-world deployment, particularly in handling data drift, evolving fraud tactics, and computational scalability across decentralized metaverse architectures [19], [21], [22], [26].

Conclusion

This study introduced a hybrid ensemble learning framework that combines Isolation Forest, Autoencoder, and XGBoost using a meta learning approach to detect anomalous transactions within the metaverse environment. The experimental results confirm that the hybrid ensemble consistently outperforms the individual models in terms of accuracy, precision, recall, F1 score, and ROC AUC. These findings demonstrate the framework's ability to identify complex irregularities that conventional single model methods often fail to capture.

The integration of unsupervised and supervised algorithms enables the model to achieve a balance between generalization and precision. The unsupervised components are effective in identifying structural deviations and reconstruction patterns, while the supervised component refines these insights based on labeled data. In addition, incorporating behavioral and contextual variables enhances the interpretability of detection results, showing that anomalies in metaverse transactions arise not only from numerical deviations but also from shifts in user behavior, transaction timing, and regional interaction characteristics.

Visualization using Principal Component Analysis further reinforces the model's discriminative capability by displaying clear separation between normal and anomalous transaction clusters. This pattern indicates that the hybrid ensemble captures meaningful high dimensional relationships in the data and transforms them into interpretable representations that support better risk assessment and monitoring.

In conclusion, the proposed hybrid ensemble learning framework provides a robust, interpretable, and scalable solution for anomaly detection in metaverse-based blockchain transactions. It shows strong potential for real-time implementation in digital financial systems by enabling proactive detection of fraudulent or irregular activities. Future research is recommended to focus on extending the framework to include cross-chain data integration, adaptive learning for dynamic transaction environments, and explainable artificial intelligence approaches to enhance transparency and trust in metaverse security analytics.

Declarations

Author Contributions

Conceptualization: S.P., G.S.; Methodology: S.P., S.A.M.; Software: G.S., M.B.; Validation: S.A.M., S.P.; Formal Analysis: S.P.; Investigation: G.S., M.B.; Resources: S.A.M., M.B.; Data Curation: G.S.; Writing – Original Draft Preparation: S.P.; Writing – Review and Editing: S.A.M., M.B.; Visualization: M.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] 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.

[2] 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.

[3] D. Praveen, N. S. Allur, K. Dondapati, H. Chetlapalli, A. Kurunthachalam, and S. Kodadi, “Blockchain-assisted federated learning for cybersecurity: Combining isolation forest, variational autoencoders, and differential privacy,” *J. Sci. Technol.*, vol. 10, no. 2, pp. 95–107, May 2025, doi: 10.46243/jst.2025.v10.i02.pp95-107.

[4] S. M. Shamna, “Anomaly detection in financial transactions: A data-driven approach for fraud prevention,” *Int. J. Commun. Inf. Technol.*, vol. 6, no. 1B, pp. 110–119, Apr. 2025, doi: 10.33545/2707661x.2025.v6.i1b.120.

[5] C.-W. Tien, T.-Y. Huang, P. Chen, and J.-H. Wang, “Using autoencoders for anomaly detection and transfer learning in IoT,” *Computers*, vol. 10, no. 7, pp. 1–12, Jul. 2021, doi: 10.3390/computers10070088.

[6] D. Ribeiro, L. M. Matos, G. Moreira, A. Pilastri, and P. Cortez, “Isolation forests and deep autoencoders for industrial screw tightening anomaly detection,” *Computers*, vol. 11, no. 4, pp. 1–10, Apr. 2022, doi: 10.3390/computers11040054.

[7] N. E. El-Attar, M. H. Salama, M. Abdelfattah, and S. Taha, “An optimized framework for detecting suspicious accounts in the Ethereum blockchain network,” *Cryptography*, vol. 9, no. 4, pp. 1–12, Dec. 2025, doi: 10.3390/cryptography9040063.

[8] Z. Gu and O. Dib, “Enhancing fraud detection in the Ethereum blockchain using ensemble learning,” *PeerJ Comput. Sci.*, vol. 11, no. Mar., pp. 1–10, 2025, doi: 10.7717/peerj-cs.2716.

[9] J. Osterrieder, S. Chan, J. Chu, Y. Zhang, B. H. Misheva, and C. Mare, “Enhancing security in blockchain networks: Anomalies, frauds, and advanced detection techniques,” *arXiv preprint*, vol. 2024, no. Feb., pp. 1–15, Feb. 2024, doi: 10.48550/arXiv.2402.11231.

[10] H. Al-Harbi, “Detecting anomalies in blockchain transactions using spatial-temporal graph neural networks,” *Adv. Manag. Intell. Technol.*, vol. 2025, no. Mar., pp. 1–12, Mar. 2025, doi: 10.62177/amit.v1i1.200.

[11] M. Hasan, M. S. Rahman, H. Janicke, and I. H. Sarker, “Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis,” *arXiv preprint*, vol. 2024, no. Jan., pp. 1–10, Jan. 2024, doi: 10.48550/arXiv.2401.03530.

[12] E. Kaufman and A. Iaremenko, “Anomaly detection for fraud in cryptocurrency time series,” *arXiv preprint*, vol. 2022, no. Jul., pp. 1–12, Jul. 2022, doi: 10.48550/arXiv.2207.11466.

[13] M. Kamran, M. Rehan, W. Nisar, and M. W. Rehan, “ARCADE—Adversarially robust cost-sensitive anomaly detection in blockchain using explainable artificial intelligence,” *Electronics*, vol. 14, no. 8, pp. 1–14, Apr. 2025, doi: 10.3390/electronics14081648.

[14] 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.

[15] S. Chen, Y. Liu, Q. Zhang, Z. Shao, and Z. Wang, “Multi-distance spatial-temporal graph neural network for anomaly detection in blockchain transactions,” *Adv. Intell. Syst.*, vol. 7, no. Apr., pp. 1–12, Apr. 2025, doi: 10.1002/aisy.202400898.

[16] T. Chen and C. Guestrin, “XGBoost: A scalable tree boosting system,” *ACM SIGKDD Int. Conf. Knowl. Discov. Data Min.*, vol. 2016, no. Aug., pp. 785–794, Aug. 2016, doi: 10.1145/2939672.2939785.

[17] K. Mohbey, M. Z. Khan, and A. Indian, “Credit card fraud prediction using XGBoost: An ensemble learning approach,” *Int. J. Inf. Retr. Res.*, vol. 12, no. 1, pp. 1–17, Jan. 2022, doi: 10.4018/ijirr.299940.

[18] M. Sattar, V. Dattana, R. Hasan, S. Mahmood, H. W. Khan, and S. Hussain, “Enhancing supply chain management: A comparative study of machine learning techniques with cost–accuracy and ESG-based evaluation for forecasting and risk

mitigation," *Sustainability*, vol. 17, no. 13, pp. 1–18, Jul. 2025, doi: 10.3390/su17135772.

[19] A. Khan, O. Chaudhari, and R. Chandra, "A review of ensemble learning and data augmentation models for class imbalanced problems: Combination, implementation and evaluation," *arXiv preprint*, vol. 2023, no. Apr., pp. 1–12, Apr. 2023, doi: 10.48550/arXiv.2304.02858.

[20] A. Haque and H. S. Soliman, "A transformer-based autoencoder with isolation forest and XGBoost for malfunction and intrusion detection in wireless sensor networks for forest fire prediction," *Future Internet*, vol. 17, no. 4, pp. 1–15, Apr. 2025, doi: 10.3390/fi17040164.

[21] Y. Lou, J. Liu, Y. Sheng, J. Wang, Y. Zhang, and Y. Ren, "Addressing class imbalance with probabilistic graphical models and variational inference," *Int. Conf. Artif. Intell. Ind. Technol. Appl. (AIITA)*, vol. 2025, no. Oct., pp. 1238–1242, Oct. 2025, doi: 10.1109/aiita65135.2025.11047653.

[22] F. R. Alzaabi and A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," *IEEE Access*, vol. 12, pp. 30907–30927, Mar. 2024, doi: 10.1109/ACCESS.2024.3369906.

[23] R. A. M. Aljohani and A. A. Alnahdi, "Temporal pattern analysis and transaction volume trends in the Ripple (XRP) network using time series analysis," *J. Curr. Res. Blockchain*, vol. 2, no. 4, pp. 274–290, Nov. 2025, doi: 10.47738/jcrb.v2i4.49.

[24] M. Alkhoze and M. Almasre, "Sentiment analysis of Mobile Legends Play Store reviews using support vector machine and naïve Bayes," *J. Digit. Mark. Digit. Curr.*, vol. 2, no. 4, pp. 368–389, Nov. 2025, doi: 10.47738/jdmdc.v2i4.44.

[25] J. O. Guballo, "An analysis of the relationship between social media usage intensity and anxiety levels among university students using a quantitative approach," *Int. J. Informatics Inf. Syst.*, vol. 8, no. 4, pp. 201–211, Oct. 2025, doi: 10.47738/ijiis.v8i4.287.

[26] R. A. M. Aljohani and A. A. Alnahdi, "Exploring football player salary prediction using random forest: Leveraging player demographics and team associations," *Int. J. Appl. Inf. Manag.*, vol. 5, no. 4, pp. 203–213, Dec. 2025, doi: 10.47738/ijaim.v5i4.115.

[27] S. Gulbakyt, A. Almaz, S. Saule, and Y. Suhrab, "Dynamic model for budget allocation via multi-criteria optimization," *J. Appl. Data Sci.*, vol. 6, no. 4, pp. 3075–3088, Oct. 2025, doi: 10.47738/jads.v6i4.935.

[28] U. Rahardja and Q. Aini, "Clustering AI job roles using PCA and K-means based on skill profiles and automation risk," *Artif. Intell. Learn.*, vol. 1, no. 4, pp. 315–328, Dec. 2025, doi: 10.63913/ail.v1i4.44.

[29] A. Latif and S. Riyadi, "Geo-aware clustering of cyber attacks using K-means and DBSCAN for threat intelligence mapping," *J. Cyber Law*, vol. 1, no. 4, pp. 282–299, Dec. 2025, doi: 10.63913/jcl.v1i4.74.

[30] T. Wahyuningsih and A. Hananto, "Temporal topic modeling of Netflix descriptions using TF-IDF and NMF to map the evolution of digital storytelling themes," *J. Digit. Soc.*, vol. 1, no. 4, pp. 287–298, Dec. 2025, doi: 10.63913/jds.v1i4.43.