Journal of Applied Science, Engineering, Technology, and Education *ISSN: 2685-0591 (online)*
Vol. 8 No. 2 (2026)
https://doi.org/10.35877/454RI.asci4873

Explainable Anomaly Detection Framework for Digital Crowdsourcing Platforms Using Optimized Isolation Forest and Local Outlier Factor

Mohd. Norhisham Razali[a], Norizuandi Ibrahim[b], Sokkhey PHAUK[c], Rozita Hanapi[a], & Norlelawati Ismawi[a]

[a]*Faculty of Business and Management, Universiti Teknologi MARA, Cawangan Sarawak, Malaysia*
[b]*Faculty of Computer Science and Mathematics, Universiti Teknologi MARA, Cawangan Sarawak, Malaysia*
[c]*Department of Applied Mathematics and Statistics, Institute of Technology of Cambodia (ITC), Russian Confederation Boulevard, Phnom Penh, Cambodia*

Abstract

Digital crowdsourcing platforms rely on freelancer profiles to support trust, reputation, and hiring decisions. However, anomalous profiles exhibiting unusual combinations of pricing, reputation, verification status, and engagement characteristics may reduce platform reliability and decision quality. Existing anomaly detection studies primarily emphasize detection performance while providing limited attention to hyperparameter optimization and model interpretability. This study proposes an explainable anomaly detection framework for identifying anomalous freelancer profiles using Isolation Forest (IF) and Local Outlier Factor (LOF). Hyperparameter optimization techniques, including Grid Search, Randomized Search, Genetic Algorithm, and Bayesian Optimization, were applied to improve model robustness and stability. Model performance was assessed using Accuracy, Precision, Recall, F1-score, ROC-AUC, and Matthews Correlation Coefficient (MCC). The results show that hyperparameter optimization improved the overall classification accuracy of several models. Among the evaluated models, the Genetic Algorithm produced the highest F1-score for LOF, while the optimized Isolation Forest models achieved higher accuracy but lower recall than the default configuration. To improve transparency, SHAP-based explainability was integrated to identify feature-level contributions influencing anomaly predictions, enabling platform administrators to interpret detected anomalies and support decision-making. The proposed framework demonstrates that combining explainable AI with systematic hyperparameter optimization provides a more transparent and comprehensive approach for anomaly detection in digital crowdsourcing platforms.

Keywords: Anomaly Detection, Hyperparameter Optimization, Explainable AI, Trustworthy AI, Crowdsourcing Platforms.

Received: 15 September 2020 Revised: 29 November 2021 Accepted: 2 December 2021

1. Introduction

Digital crowdsourcing platforms have transformed the global labor market by enabling organizations to access a distributed workforce while offering freelancers flexible employment opportunities. Platforms such as online freelancing marketplaces support large-scale interactions through digital profiles that represent skills, reputation, pricing, and engagement history. These profiles are central to trust-building and informed hiring decisions. However, the rapid expansion of these platforms has introduced significant challenges to maintaining ecosystem integrity. Anomalous freelancer profiles—such as those exhibiting unrealistic pricing, manipulated reputation signals, inconsistent verification status, or unusual behavioral patterns—can distort marketplace dynamics and reduce user trust. Such anomalies may result from fraud, profile manipulation, or atypical user behavior, making their detection essential for platform governance.

* Corresponding author.
E-mail address: hishamrazali@uitm.edu.my

Anomaly detection techniques have been widely adopted to address these issues, particularly unsupervised machine learning methods such as Isolation Forest (IF) and Local Outlier Factor (LOF), which are suitable for environments lacking labeled data. However, their performance is highly dependent on hyperparameter tuning. Poor configuration may lead to unstable results, high false-positive rates, or missed anomalies, limiting their practical reliability. In addition, most existing approaches lack interpretability. Many anomaly detection models function as black-box systems, producing anomaly scores without explaining the underlying reasons. In governance contexts, this lack of transparency reduces trust and limits the usability of model outputs for decision-making. Therefore, integrating explainable artificial intelligence (XAI) is essential to improve accountability and interpretability. Furthermore, prior studies often focus primarily on detection accuracy, while neglecting robustness, stability across parameter settings, and agreement between models.

To address these limitations, this study proposes a trustworthy and explainable anomaly detection framework for freelancer profile analysis in digital crowdsourcing platforms. The framework integrates Isolation Forest and Local Outlier Factor with systematic hyperparameter optimization using Grid Search, Randomized Search, Genetic Algorithms, and Bayesian Optimization. This enhances robustness and reduces sensitivity to parameter selection. An additional explainability layer using SHAP is incorporated to interpret anomaly scores and identify feature-level contributions driving anomalous classifications. This transforms model outputs into interpretable insights that support human-in-the-loop validation and governance decision-making.

The contributions of this study are as follows:

- A systematic hyperparameter optimization strategy to improve stability and reliability of Isolation Forest and Local Outlier Factor in unsupervised anomaly detection.
- Integration of SHAP-based explainability to provide feature-level interpretation of anomalous freelancer profiles
- Evaluation using multiple criteria, including clustering separability, anomaly consistency, and cross-model agreement, to ensure more reliable unsupervised assessment.

In summary, this research integrates robust anomaly detection with explainable AI to support trustworthy decision-making in digital crowdsourcing platforms, enabling effective identification of anomalous freelancer behavior while maintaining transparency and interpretability.

2. Related Works

Anomaly detection plays a critical role in identifying irregular behavior and potential fraud in online platforms and digital marketplaces. Various approaches have been proposed to detect anomalous patterns, including feature-based, content-based, graph-based, and unsupervised learning techniques (Zhang et al., 2015). These approaches have been widely applied in contexts such as online social networks and e-commerce platforms to identify suspicious activities including spam, phishing, and fraudulent behavior (Sakthivanitha et al., 2025; Zhang et al., 2015). Beyond social platforms, anomaly detection techniques have also been applied in financial systems, particularly in cryptocurrency markets, where unusual trading patterns and fraudulent transactions are prevalent. In such contexts, unsupervised machine learning algorithms such as Local Outlier Factor (LOF) and Isolation Forest have demonstrated effectiveness in detecting abnormal behavior in high-dimensional and unlabeled datasets (Witayanont & Viyanon, 2025; Yahia et al., 2024). These approaches are particularly valuable in real-world scenarios where labeled anomaly data are scarce or unavailable.

2.1. Isolation Forest and Local Outlier Factor in Unsupervised Anomaly Detection

Among unsupervised anomaly detection techniques, Isolation Forest (IF) and Local Outlier Factor (LOF) are widely used due to their effectiveness in detecting abnormal observations in complex datasets. Isolation Forest is favored for its computational efficiency and scalability, making it suitable for large-scale anomaly detection tasks (Agyemang, 2024; Carletti et al., 2023) . The algorithm isolates anomalies by recursively partitioning the dataset through random decision trees, allowing anomalous observations to be separated with fewer splits. Despite its efficiency, Isolation Forest presents challenges in interpretability due to the stochastic nature of its tree construction and may struggle to effectively detect local outliers in dense regions of data (Carletti et al., 2023; Chaabouni & Boujelben, 2025).

In contrast, Local Outlier Factor is a density-based method that evaluates the relative density of data points compared to their neighbors. This approach enables LOF to effectively detect local anomalies that deviate from surrounding data distributions (Yahia et al., 2024). Comparative studies suggest that LOF can outperform Isolation Forest in terms of

precision and recall when identifying complex anomaly structures (Agyemang, 2024; Darrab et al., 2024). However, LOF may face scalability challenges when applied to very large datasets due to its reliance on nearest-neighbor computations (Chaabouni & Boujelben, 2025). Given their complementary strengths, combining insights from both algorithms can provide a more comprehensive understanding of anomalous patterns.

2.2. Hyperparameter Optimization for Robust Anomaly Detection

Although Isolation Forest and LOF have demonstrated strong anomaly detection capabilities, their performance is highly sensitive to hyperparameter configurations (Younis, 2026). Improper parameter settings can lead to unstable detection results, increased false positives, or missed anomalies. To address this issue, researchers have explored various hyperparameter optimization techniques to enhance model robustness and stability. Methods such as adaptive particle swarm optimization (APSO) and Bayesian optimization have been employed to fine-tune model parameters and improve predictive performance (Li et al., 2023; Wang et al., 2026). For example, APSO has been applied to optimize parameters in LSSVM models, resulting in improved localization accuracy (Wang et al., 2026). Similarly, Bayesian optimization has been used to enhance deep learning models such as 1D-CNN for structural anomaly detection tasks (Li et al., 2023). Despite these advances, relatively limited research has systematically examined the impact of hyperparameter optimization strategies on traditional unsupervised anomaly detection models such as Isolation Forest and LOF. Consequently, further investigation is needed to establish robust tuning strategies that ensure stable and reliable anomaly detection outcomes.

2.3. Explainable AI in Unsupervised Anomaly Detection

In recent years, Explainable Artificial Intelligence (XAI) has emerged as a key research direction aimed at improving the transparency and interpretability of machine learning models. This is particularly important for anomaly detection systems, where users must understand why a particular observation has been flagged as anomalous.

Techniques such as SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) have been adapted to interpret anomaly detection models by quantifying the contribution of individual features to anomaly scores (Khalid et al., 2025; Kiefer & Pesch, 2021). For example, SHAP enables analysts to identify which variables most strongly influence the classification of a profile as anomalous, providing valuable insights into model behavior (Kim et al., 2021).

These explanation techniques are increasingly applied in high-stakes domains such as cybersecurity, where transparency and trust in AI-driven decisions are essential (Muça & Ahmad, 2026) . Studies have shown that combining machine learning models with explainability techniques can significantly enhance interpretability while maintaining strong predictive performance (Hermosilla et al., 2025; Mohale & Obagbuwa, 2025)

Additionally, methods such as ClAMP and EXPLAIN-IT have been proposed to improve interpretability in clustering-based anomaly detection by generating human-readable explanations and meaningful clusters (Bobek et al., 2022; Morichetta et al., 2019). However, the integration of XAI techniques within unsupervised anomaly detection frameworks remains relatively limited, highlighting the need for further research to improve transparency and user trust (Mohanty et al., 2025)

2.4. Anomaly Detection Challenges in Digital Crowdsourcing Platforms

Digital crowdsourcing and freelancing platforms introduce unique anomaly detection challenges that differ from those observed in traditional domains. In such platforms, anomalies may manifest as fraudulent freelancer profiles, manipulated reputation metrics, unrealistic pricing structures, or unusual combinations of skills, verification status, and engagement patterns.

However, much of the existing anomaly detection literature focuses on generic fraud detection or cybersecurity contexts, with limited attention given to the distinctive characteristics of crowdsourcing ecosystems (Dehkordi et al., 2025; Lunawat et al., 2024). The dynamic and rapidly evolving nature of user interactions in these platforms further complicates anomaly detection, as behavioral patterns and marketplace conditions can change quickly (Dehkordi et al., 2025; Vajpayee & Hossain, 2024). Consequently, anomaly detection models designed for static or homogeneous datasets may struggle to adapt to the complex behavioral signals present in crowdsourcing environments.

In a nutshell, while prior studies have explored anomaly detection algorithms, hyperparameter optimization, and explainable AI techniques individually, limited research has integrated these elements into a unified framework for detecting anomalies in digital crowdsourcing platforms. In particular, few studies systematically evaluate the robustness of unsupervised anomaly detection models through hyperparameter optimization while simultaneously providing interpretable explanations for detected anomalies.

Therefore, this study proposes a trustworthy and explainable anomaly detection framework for freelancer profiles in digital crowdsourcing platforms. By combining Isolation Forest and Local Outlier Factor models with systematic hyperparameter optimization and an explainable interpretation layer, the proposed approach aims to enhance detection robustness, interpretability, and decision support for platform governance.

3. Explainable Anomaly Detection Framework

This study proposes an integrated Explainable Anomaly Detection Framework to improve the trustworthiness, robustness, and interpretability of freelancer profile analysis in digital crowdsourcing platforms. The framework combines unsupervised anomaly detection, systematic hyperparameter optimization, quantitative performance evaluation, and Explainable Artificial Intelligence (XAI) to generate reliable and interpretable anomaly detection results suitable for platform governance. As illustrated in Figure 1, the framework comprises four interconnected stages: (1) data collection and feature representation, (2) optimized anomaly detection, (3) quantitative performance evaluation, and (4) explainable anomaly interpretation for governance-oriented decision support. Unlike conventional anomaly detection approaches that primarily emphasize predictive performance, the proposed framework integrates model optimization, comprehensive evaluation, and explainability into a unified decision-support pipeline.

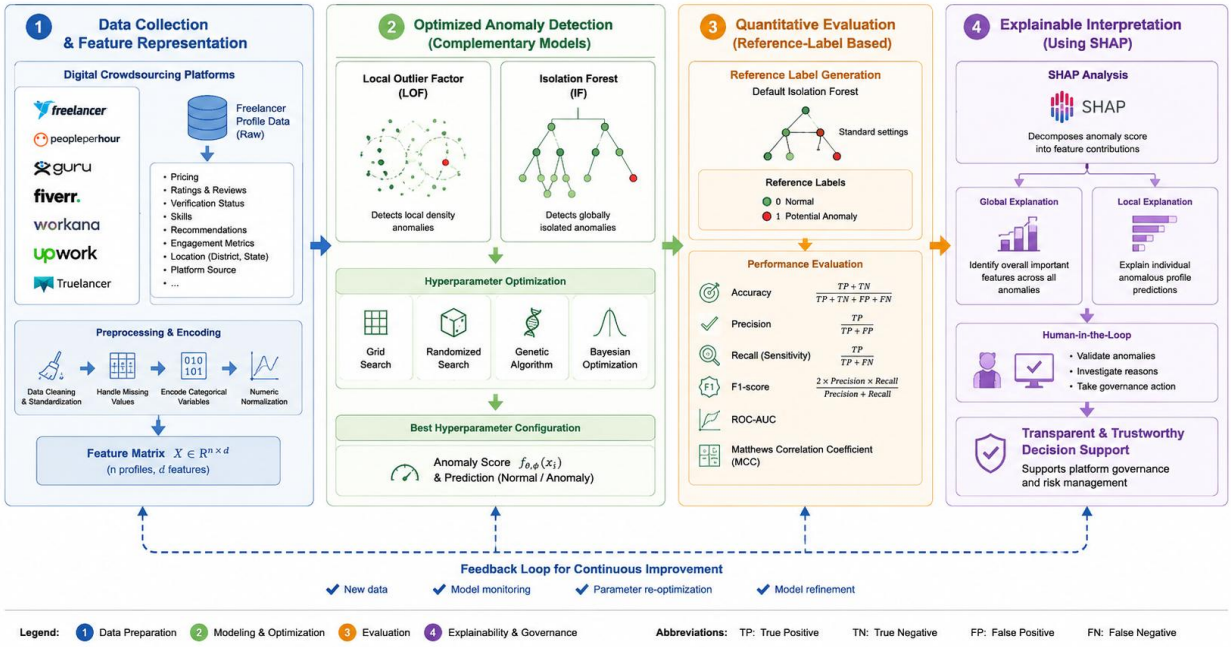


Fig. 1. Research Framework

In the first stage, freelancer profile data are collected from multiple digital crowdsourcing platforms and transformed into structured numerical feature representations. The collected profiles contain heterogeneous attributes describing economic, reputational, behavioural, and platform-related characteristics, including pricing, ratings, reviews, verification status, recommendations, engagement metrics, location, skills, and platform source. A preprocessing pipeline performs data cleaning, standardization, categorical encoding, and numerical normalization to construct a feature matrix suitable for machine learning analysis. This unified representation enables consistent processing across all anomaly detection models.

The second stage performs anomaly detection using two complementary unsupervised learning algorithms: Isolation Forest (IF) and Local Outlier Factor (LOF). Isolation Forest identifies globally isolated observations through recursive

random partitioning, whereas Local Outlier Factor detects anomalies based on local density deviations among neighbouring freelancer profiles. To improve robustness and reduce sensitivity to manual parameter selection, systematic hyperparameter optimization is incorporated within the framework. Isolation Forest is optimized using Grid Search and Randomized Search, while Local Outlier Factor is optimized using Grid Search, Randomized Search, Genetic Algorithm, and Bayesian Optimization. The optimized models generate anomaly scores and binary anomaly predictions for subsequent evaluation.

The third stage provides a quantitative assessment of anomaly detection performance. A reference-label dataset is generated using the default Isolation Forest model with standard hyperparameter settings. These reference labels provide a consistent baseline for evaluating all optimized anomaly detection models. Performance is assessed using multiple complementary evaluation metrics, including Accuracy, Precision, Recall, F1-score, Receiver Operating Characteristic–Area Under the Curve (ROC-AUC), and Matthews Correlation Coefficient (MCC). Employing multiple evaluation metrics provides a balanced assessment of classification effectiveness and enables objective comparison among different optimization strategies.

The final stage enhances model transparency through SHAP (Shapley Additive Explanations). SHAP decomposes anomaly predictions into feature-level contributions, allowing both global and local interpretation of detected anomalies. Global explanations identify the overall importance of features influencing anomaly detection, whereas local explanations reveal why an individual freelancer profile is classified as anomalous. These explanations support human-in-the-loop validation, enabling platform administrators to verify anomaly predictions, investigate contributing factors, and make informed governance decisions with greater confidence.

Overall, the proposed Explainable Anomaly Detection Framework operationalizes trustworthy AI by integrating optimized anomaly detection, comprehensive quantitative evaluation, and explainable machine learning within a single analytical workflow. Rather than functioning solely as a predictive anomaly detection model, the framework serves as a governance-oriented decision support system that enhances transparency, robustness, accountability, and evidence-based decision-making in digital crowdsourcing platforms.

4. Experimental Setup

The dataset was collected from several digital crowdsourcing platforms, including Freelancer, PeoplePerHour, Guru, Fiverr, Workana, Upwork, and Truelancer. It is represented as $D = \{r_1, r_2, \dots, r_n\}$, where (n) is the number of freelancer profiles. Each profile contains multiple attributes, including location (district and state), pricing, verification status, skills, ratings, recommendations, review counts, and platform source. These attributes include both categorical and numerical data, forming a heterogeneous dataset used for analysis.

A preprocessing function was applied to clean and standardize the raw data by removing non-numeric symbols, normalizing text formatting, and converting Boolean values into binary form {0,1}. The resulting cleaned dataset is represented as (D'). Since anomaly detection models require numerical input $x_i \in R^d$, categorical attributes were converted into numerical values using label encoding in Python. Each unique category was mapped to a distinct integer value through an encoding function ϕ_j, ensuring that different categories received different numerical representations. This transformation enabled categorical data to be processed effectively by the anomaly detection models. After preprocessing and encoding, each freelancer profile was represented as a numerical feature vector $x_i \in R^d$. The full dataset was then organized into a feature matrix $X = [x_1, x_2, \dots, x_n]^T \in R^{n \times d}$, where (n) represents the number of freelancer profiles and (d) represents the total number of attributes. This matrix served as the input for the anomaly detection models. Numeric attributes such as pricing, ratings, recommendations, and transaction-related values were retained in their original form to preserve their natural distributions and avoid distortion during preprocessing.

A rule-based reference dataset was constructed using domain-informed heuristic rules reflecting economically and behaviorally implausible freelancer profiles. The rules were designed independently of the anomaly detection algorithms to avoid circular evaluation and were based on combinations of inconsistent verification status, unrealistic pricing, reputation indicators, and engagement characteristics. Each freelancer profile was assigned a binary reference label (0 = normal, 1 = potential anomaly).

5. Methodology

This study proposes a robust and explainable anomaly detection framework for identifying anomalous freelancer profiles in digital crowdsourcing platforms. The framework integrates two complementary unsupervised anomaly

detection models—Isolation Forest (IF) and Local Outlier Factor (LOF)—with systematic hyperparameter optimization, quantitative performance evaluation, and Explainable Artificial Intelligence (XAI). Let the preprocessed dataset be represented as $X = \{x_1, x_2, \dots, x_n\}$, where each freelancer profile $x_i \in \mathbb{R}^d$. The anomaly detection model learns a scoring function f_θ that assigns an anomaly score to each freelancer profile according to a given hyperparameter configuration ϕ. A profile is classified as anomalous when its anomaly score exceeds a threshold T, determined by the contamination parameter. The framework also incorporates human-in-the-loop interpretability to ensure anomaly detection results remain transparent and suitable for platform governance.

Isolation Forest detects anomalies by recursively partitioning the feature space using randomly selected features and split points. Profiles requiring fewer partitions to become isolated receive higher anomaly scores. The model employs several hyperparameters, including the number of trees, sample size, feature subset size, contamination rate, and bootstrap strategy. Owing to its tree-based architecture, Isolation Forest is computationally efficient and well suited for high-dimensional datasets.

Local Outlier Factor (LOF) detects anomalies by comparing the local density of a profile with that of its neighbouring observations. Profiles exhibiting substantially lower local density than their neighbours are assigned higher anomaly scores. The LOF model is controlled by several hyperparameters, including the number of neighbours, search algorithm, and contamination rate, making it effective for identifying local behavioural anomalies within heterogeneous freelancer data.

Hyperparameter optimization was performed to identify the most suitable parameter configuration for each anomaly detection model. For Isolation Forest, Grid Search and Randomized Search were employed, whereas Local Outlier Factor was optimized using Grid Search, Randomized Search, Genetic Algorithm (GA), and Bayesian Optimization. The Genetic Algorithm iteratively evolves candidate solutions through selection, crossover, and mutation, while Bayesian Optimization searches the parameter space using a probabilistic surrogate model and acquisition function. These optimization techniques aim to improve model robustness and reduce sensitivity to manual parameter selection.

A reference-label dataset was generated using a default Isolation Forest model with standard hyperparameter settings. The generated binary labels served as a consistent reference for evaluating all default and optimized anomaly detection models. Model performance was assessed by comparing the predicted anomaly labels against the reference labels using Accuracy, Precision, Recall, F1-score, Receiver Operating Characteristic–Area Under the Curve (ROC-AUC), and Matthews Correlation Coefficient (MCC). Employing multiple complementary evaluation metrics provides a more comprehensive assessment of anomaly detection performance than relying solely on a single metric.

To improve interpretability, SHAP (Shapley Additive Explanations) was applied to explain anomaly detection decisions. SHAP decomposes anomaly scores into feature-level contributions, enabling identification of the attributes most responsible for anomalous classifications. Global explanations were obtained by aggregating SHAP values across all detected anomalies, whereas local explanations were generated for individual freelancer profiles. This explainability layer enhances transparency and supports human validation and governance-oriented decision-making.

In addition to quantitative evaluation, anomaly score distributions together with contour and scatter plot visualizations were used to illustrate the separation between normal and anomalous freelancer profiles. These visual analyses complement the quantitative performance measures by providing intuitive insights into the behavioural patterns captured by the anomaly detection models.

6. Experimental Results

6.1 Hyperparameter Optimization

This experiment aimed to optimize the Isolation Forest (IF) model for anomaly detection in the crowdsourcing dataset using two hyperparameter tuning approaches: GridSearchCV and RandomizedSearchCV. The optimal configurations obtained from both methods are summarized in Table 1.

Table 1. Optimization Configurations (Isolation Forest)

Method	Trees	Samples	Contam.	Features	Boot
Grid Search	50	256	0.05	0.5	Yes
Random Search	150	512	0.15	1.0	No

The results show clear differences between the two optimization methods. GridSearchCV selected a smaller model (50 trees), while RandomizedSearchCV chose a larger one (150 trees), which may improve stability and robustness in detecting diverse anomalies. For data sampling, GridSearchCV used smaller subsets (256 samples per tree), whereas RandomizedSearchCV used larger subsets (512), allowing better coverage of data patterns. The contamination rate also differed, with GridSearchCV using a conservative 5% anomaly assumption, while RandomizedSearchCV used 15%, leading to more aggressive anomaly detection. In terms of features, GridSearchCV used only 50% of features per tree to reduce overfitting, while RandomizedSearchCV used all features for full information usage. Finally, GridSearchCV applied bootstrap sampling for stability, whereas RandomizedSearchCV did not, increasing tree diversity. Overall, GridSearchCV is more conservative and stable, while RandomizedSearchCV is more aggressive and flexible in detecting anomalies.

To optimize the Local Outlier Factor (LOF) model, four hyperparameter tuning strategies were evaluated using Grid Search, Random Search, Genetic Algorithm and Bayesian Optimization. Each approach explored different combinations of n_neighbors, algorithm type, and contamination levels. The Silhouette Score was used as the primary metric to evaluate clustering quality and the separation between normal and anomalous observations.

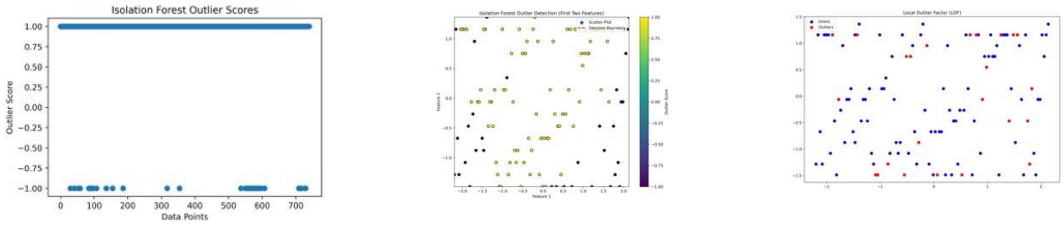
Table 2. Optimization Configuration (Local Outlier Factor)

Method	n_neighbors	Algorithm	Contamination	Silhouette
Grid Search	5	auto	0.01	0.3219
Random Search	15	ball_tree	0.05	0.2546
Genetic Algorithm	34	ball_tree	0.118	0.2315
Bayesian Optimization	50	auto	0.01	0.5564

Bayesian Optimization achieved the best performance with the highest Silhouette Score (0.5564), indicating the clearest separation between normal and anomalous data. This shows it was most effective in tuning the LOF model. Grid Search gave stable but moderate results (0.3219), though it is limited by its fixed search space. Random Search performed worse (0.2546) due to its less consistent sampling of parameters. The Genetic Algorithm had the lowest score (0.2315), suggesting it needs further tuning or more iterations to improve performance. Overall, Bayesian Optimization is the most effective method in this experiment, while Grid Search is a solid baseline and the other methods require refinement.

6.2 Outlier Detection using Optimized Isolation Forest based on RandomizedSearchCV

This experiment evaluated the optimized Isolation Forest (IF) model for detecting anomalous freelancer profiles using RandomizedSearchCV for hyperparameter tuning. The model successfully separated normal profiles (inliers) from anomalous profiles (outliers), with most profiles classified as normal and only a small portion flagged as anomalies. The visualizations show a clear separation between normal and anomalous observations. Most freelancer profiles had low anomaly scores, while anomalies appeared with much higher scores, indicating unusual patterns in attributes such as pricing, reviews, or engagement. The scatter plot also showed that anomalies were grouped in specific regions, suggesting meaningful detection rather than random classification.

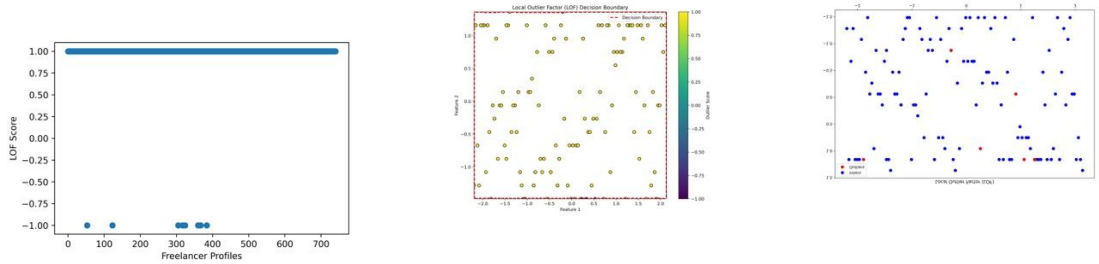


(a) Outlier Score (b) Decision (c)Final Scattered Plot

Fig. 2. Outlier Detection Visualization using Isolation Forest

Comparisons between optimization methods showed that Grid Search produced more conservative results with fewer detected anomalies, while Randomized Search identified more anomalies due to its higher contamination setting. Although this increases sensitivity, it may also lead to more false positives. Overall, the optimized Isolation Forest model showed strong performance in detecting irregular freelancer profiles while maintaining good separation between normal and anomalous data.

6.3 Outlier Detection using optimized Local Outlier Factor based on Bayesian Optimization



(a) Outlier Score (b) Decision (c)Final Scattered Plot

Fig. 3. Outlier Detection Visualization using Local Outlier Factor (LOF)

To complement the Isolation Forest analysis, the Local Outlier Factor (LOF) model was applied using Bayesian Optimization for hyperparameter tuning. Unlike Isolation Forest, LOF detects anomalies by comparing the local density of each profile with its neighboring profiles. The LOF score distribution showed that most freelancer profiles had scores close to the normal threshold, indicating consistent behavior across the dataset. Very few strong anomalies were detected, suggesting that most profiles share similar characteristics in pricing, reputation, and engagement. The scatter plot and decision boundary visualizations also confirmed that most data points were classified as normal, with only limited evidence of local density deviations. This suggests that the dataset is relatively stable and well-clustered. Overall, the optimized LOF model indicates that most freelancer profiles fall within expected behavioral patterns. While Isolation Forest is better at detecting global anomalies, LOF provides additional insight into local behavioral differences, making both methods complementary for anomaly detection.

6.4 Quantitative Performance Evaluation

Table 3. Performance of all models (Accuracy, Precision, Recall, F1, ROC-AUC, MCC)

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC	MCC	TP	TN	FP	FN
IF_Default	0.7139	0.0946	0.0461	0.0619	0.4662	-0.0912	7	522	67	145
IF_GS	0.7584	0.1351	0.0329	0.0529	0.4893	-0.0397	5	557	32	147
IF_RS	0.7584	0.1351	0.0329	0.0529	0.4893	-0.0397	5	557	32	147
LOF_Default	0.7328	0.1892	0.0921	0.1239	0.4951	-0.0131	14	529	60	138
LOF_GS	0.7841	0	0	0	0.4932	-0.0531	0	581	8	152
LOF_RS	0.7692	0.2432	0.0592	0.0952	0.5058	0.0216	9	561	28	143
LOF_GA	0.7166	0.1705	0.0987	0.125	0.4874	-0.0315	15	516	73	137
LOF_BO	0.7841	0	0	0	0.4932	-0.0531	0	581	8	152

Table 3 compares the performance of the default and optimized Isolation Forest (IF) and Local Outlier Factor (LOF) models using six evaluation metrics. Although several optimized models achieved higher classification accuracy than their default counterparts, improvements in accuracy were not consistently accompanied by better anomaly detection capability. This is evident from the relatively low Precision, Recall, F1-score, ROC-AUC, and MCC values across most models.

The default Isolation Forest achieved an accuracy of 71.39%, while both the Grid Search (IF_GS) and Random Search (IF_RS) configurations increased the accuracy to 75.84%, representing an improvement of approximately 6.23%. However, despite the higher accuracy, both optimized models exhibited lower Recall (3.29%) and lower F1-score (0.0529) compared with the default model (Recall = 4.61%, F1-score = 0.0619). The optimized models detected only 5 true anomalies, whereas the default model detected 7 true anomalies. This indicates that the optimization process improved the classification of normal freelancer profiles (higher TN and lower FP) but reduced the model's ability to identify anomalous profiles.

Furthermore, the ROC-AUC values remained below 0.50, while the negative MCC values indicate that the optimized Isolation Forest models did not achieve meaningful discrimination between normal and anomalous instances.

Among the LOF variants, the default model achieved an accuracy of 73.28% with an F1-score of 0.1239. Grid Search and Bayesian Optimization produced the highest accuracy (78.41%), yet both models failed to detect a single anomaly (TP = 0, Recall = 0, F1-score = 0). These models classified nearly all freelancer profiles as normal, resulting in a high number of True Negatives (581) but missing every anomalous instance (152 False Negatives). Consequently, although

overall accuracy increased, these optimized models were ineffective for anomaly detection.Random Search achieved a moderate balance with an accuracy of 76.92%, identifying 9 anomalies and obtaining an F1-score of 0.0952.

Interestingly, the Genetic Algorithm produced the highest F1-score (0.1250) among all LOF models. Although its overall accuracy (71.66%) was lower than the other optimized variants, it successfully detected 15 anomalies, the highest number of True Positives among all evaluated models. This demonstrates that the Genetic Algorithm optimization improved the model's sensitivity towards anomalous freelancer profiles, which is more desirable in anomaly detection tasks.

6.5 Effect of Hyperparameter Optimization

Table 4. Accuracy Improvement of Optimized Models over Default Models

Algorithm	Default Model	Best Optimized Model	Default Accuracy	Optimized Accuracy	Improvement (%)
Isolation Forest	IF Default	IF Grid Search	0.7139	0.7584	+6.23%
Local Outlier Factor	LOF Default	LOF Grid Search	0.7328	0.7841	+7.00%

Table 4 presents the comparison between the default and the best-performing optimized configurations for Isolation Forest and Local Outlier Factor based on overall classification accuracy. The optimized Isolation Forest model obtained using Grid Search increased the classification accuracy from 71.39% to 75.84%, representing an improvement of 6.23% over the default configuration. Similarly, the optimized Local Outlier Factor model obtained using Grid Search achieved an accuracy of 78.41%, improving from 73.28% for the default model, corresponding to an improvement of 7.00%.

These results indicate that hyperparameter optimization enhanced the overall classification capability of both anomaly detection algorithms. By selecting more suitable parameter combinations, the optimized models were able to classify a larger proportion of freelancer profiles correctly than the default parameter settings.

However, the improvement observed in classification accuracy should be interpreted cautiously. As shown in Table 5, the higher accuracy achieved by the optimized models did not consistently correspond to improved anomaly detection performance. For example, although the optimized LOF model achieved the highest classification accuracy, it failed to identify any anomalous freelancer profiles, resulting in zero Recall and F1-score. This indicates that the model primarily improved the classification of normal instances while sacrificing its ability to detect anomalies.

Therefore, while hyperparameter optimization contributed to higher overall classification accuracy, the experimental findings demonstrate that accuracy alone is insufficient for evaluating anomaly detection models. Additional performance metrics such as Precision, Recall, F1-score, ROC-AUC, and MCC are essential to provide a more comprehensive assessment of anomaly detection effectiveness, particularly when dealing with imbalanced datasets.

6.6 Explainable AI (XAI) Results

To improve the interpretability of the anomaly detection models, SHAP (Shapley Additive Explanations) was applied to both the optimized Isolation Forest (IF) and Local Outlier Factor (LOF) models. The objective was to identify which freelancer profile attributes contributed most strongly to the anomaly detection decisions and to provide transparent insights into model behavior.

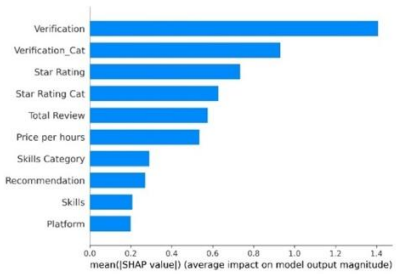


Fig. 1. Feature Importance using SHAP for Isolation Forest

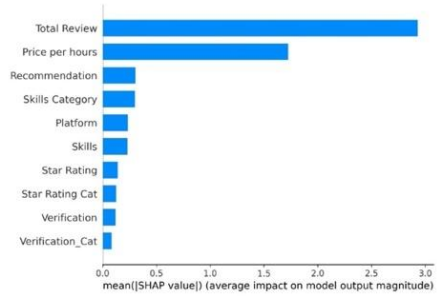


Fig. 2. Feature Importance using SHAP for Local Outlier Factor

As shown in Figure 4, the SHAP analysis shows that verification status is the most important factor in detecting anomalous freelancer profiles. Profiles with missing or unusual verification patterns were more likely to be flagged as anomalies, highlighting the importance of verification in distinguishing suspicious accounts. Reputation-related features, such as star ratings and total reviews, also had strong influence. Unusual combinations, such as very high ratings with few reviews, contributed to higher anomaly scores. In comparison, features like hourly price, skills, and platform participation had lower impact on anomaly detection. These findings suggest that verification and reputation consistency are key indicators for maintaining trust and identifying suspicious freelancer profiles.

As shown in Figure 5, the SHAP analysis for the LOF model shows that total reviews and price per hour are the most important features in detecting anomalies. Profiles with unusual combinations, such as very high review counts with very low prices, were more likely to be flagged as anomalous. Other features, including recommendations, skill category, platform participation, and skill diversity, had moderate influence. In contrast, ratings and verification status had lower impact in the LOF model. These findings suggest that LOF mainly detects anomalies based on unusual numerical patterns and local data density differences. Overall, the results show that Isolation Forest and LOF capture different types of anomalies. Isolation Forest focuses more on verification and reputation issues, while LOF emphasizes pricing and review irregularities, making both models complementary in anomaly detection.

7. Conclusions

This study proposed an explainable anomaly detection framework for identifying anomalous freelancer profiles in digital crowdsourcing platforms. The framework integrates complementary unsupervised anomaly detection models, systematic hyperparameter optimization, quantitative performance evaluation, and Explainable Artificial Intelligence (XAI) to improve the robustness, transparency, and interpretability of anomaly detection for platform governance.

The experimental results demonstrate that hyperparameter optimization influences the performance of anomaly detection models, although the improvements vary depending on the optimization strategy and evaluation metric. For Isolation Forest, the optimized models achieved higher overall classification accuracy than the default configuration but exhibited lower recall and F1-score, indicating that higher accuracy does not necessarily correspond to better anomaly detection capability. For Local Outlier Factor, the Genetic Algorithm achieved the highest F1-score among the optimized models, while Grid Search and Bayesian Optimization produced the highest classification accuracy by adopting more conservative anomaly predictions. These findings highlight the importance of evaluating anomaly detection models using multiple complementary performance metrics rather than relying on a single measure.

The study also demonstrates the complementary characteristics of Isolation Forest and Local Outlier Factor. Isolation Forest is more effective at identifying globally isolated observations, whereas Local Outlier Factor captures anomalies based on local density variations. Combining both approaches provides a broader perspective on anomalous freelancer behaviour across digital crowdsourcing platforms.

To enhance transparency, SHAP-based explainability was incorporated to interpret anomaly predictions at the feature level. The explainability analysis revealed that verification status, reputation indicators, pricing, and engagement-related attributes contribute differently across the two anomaly detection models, providing meaningful insights into the characteristics of anomalous freelancer profiles. These explanations support human-in-the-loop validation and improve confidence in AI-assisted governance decisions.

Overall, the proposed framework demonstrates that integrating hyperparameter optimization, comprehensive quantitative evaluation, and explainable AI provides a more trustworthy and interpretable approach to anomaly detection in digital crowdsourcing platforms. Future work may explore additional anomaly detection algorithms, larger cross-platform datasets, and semi-supervised or weakly supervised learning approaches to further improve anomaly detection performance and practical applicability.

Acknowledgements: The authors gratefully acknowledge Universiti Teknologi MARA (UiTM) for its continuous support through the provision of research facilities, infrastructure, and an academic environment that facilitated the completion of this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

Contribution: Razali: Drafting manuscript, concept and design. Norizuandi Ibrahim: critical revision of manuscript, material support. PHAUK: Interpretation, supervision. Hanapi: Data acquisition, data analysis. Ismawi: statistical analysis

References

Agyemang, E. F. (2024). Anomaly detection using unsupervised machine learning algorithms: A simulation study. *Scientific African*, *26*. https://doi.org/10.1016/j.sciaf.2024.e02386

Bobek, S., Kuk, M., Szelazek, M., & Nalepa, G. J. (2022). Enhancing Cluster Analysis With Explainable AI and Multidimensional Cluster Prototypes. *IEEE Access*, *10*, 101556 – 101574. https://doi.org/10.1109/ACCESS.2022.3208957

Carletti, M., Terzi, M., & Susto, G. A. (2023). Interpretable Anomaly Detection with DIFFI: Depth-based feature importance of Isolation Forest. *Engineering Applications of Artificial Intelligence*, *119*. https://doi.org/10.1016/j.engappai.2022.105730

Chaabouni, A., & Boujelben, M. A. (2025). Outlier Ensemble Based on Isolation Forest: The CBOEA Approach. *Foundations of Computing and Decision Sciences*, *50*(1), 27 – 55. https://doi.org/10.2478/fcds-2025-0002

Darrab, S., Allipilli, H., Ghani, S., Changaramkulath, H., Koneru, S., Broneske, D., & Saake, G. (2024). Anomaly Detection Algorithms: Comparative Analysis and Explainability Perspectives. *Communications in Computer and Information Science*, *1943 CCIS*, 90 – 104. https://doi.org/10.1007/978-981-99-8696-5_7

Dehkordi, S. B., Nasri, S., & Dami, S. (2025). Advances in network security and new anomaly detection techniques. *Majlesi Journal of Electrical Engineering*, *19*(2). https://doi.org/10.57647/j.mjee.2025.1902.26

Hermosilla, P., Berríos, S., & Allende-Cid, H. (2025). Explainable AI for Forensic Analysis: A Comparative Study of SHAP and LIME in Intrusion Detection Models. *Applied Sciences (Switzerland)*, *15*(13). https://doi.org/10.3390/app15137329

Khalid, Z., Iqbal, F., & Saqib, M. (2025). Bridging knowledge gaps in digital forensics using unsupervised explainable AI. *Forensic Science International: Digital Investigation*, *53*. https://doi.org/10.1016/j.fsidi.2025.301924

Kiefer, S., & Pesch, G. (2021). Unsupervised Anomaly Detection for Financial Auditing with Model-Agnostic Explanations. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12873 LNAI*, 291 – 308. https://doi.org/10.1007/978-3-030-87626-5_22

Kim, D., Antariksa, G., Handayani, M. P., Lee, S., & Lee, J. (2021). Explainable anomaly detection framework for maritime main engine sensor data. *Sensors*, *21*(15). https://doi.org/10.3390/s21155200

Li, X., Guo, H., Xu, L., & Xing, Z. (2023). Bayesian-Based Hyperparameter Optimization of 1D-CNN for Structural Anomaly Detection. *Sensors*, *23*(11). https://doi.org/10.3390/s23115058

Lunawat, S., Rao, J., & Patil, P. (2024). A Comprehensive Survey on Anomaly Detection in Social Media Networks: Challenges, Methods, and Future Directions. *4th International Conference on Sustainable Expert Systems, ICSES 2024 - Proceedings*, 363 – 370. https://doi.org/10.1109/ICSES63445.2024.10763303

Mohale, V. Z., & Obagbuwa, I. C. (2025). Evaluating machine learning-based intrusion detection systems with explainable AI: enhancing transparency and interpretability. *Frontiers in Computer Science*, *7*. https://doi.org/10.3389/fcomp.2025.1520741

Mohanty, M., Rath, P. S., Mohapatra, A. G., Mohanty, A., & Senapati, S. K. (2025). AI-enhanced data processing for modeling applications. *Advances in Computers*. https://doi.org/10.1016/bs.adcom.2025.09.004

Morichetta, A., Casas, P., & Mellia, M. (2019). Explain-IT: Towards explainable AI for unsupervised network traffic analysis. *Big-DAMA 2019 - Proceedings of the 3rd ACM CoNEXT Workshop on Big DAta, Machine Learning*

and Artificial Intelligence for Data Communication Networks, Part of CoNEXT 2019, 22 – 28. https://doi.org/10.1145/3359992.3366639

Muça, F., & Ahmad, W. (2026). Explainable AI for Malware Classification: Bridging the Gap Between Accuracy and Transparency. *Communications in Computer and Information Science*, *2669 CCIS*, 79 – 99. https://doi.org/10.1007/978-3-032-07373-0_6

Sakthivanitha, M., Priscila, S. S., & Praveen, B. M. (2025). E-commerce Security: An Overview of AI Driven Threat / Anomaly Detection. *International Journal of Engineering Trends and Technology*, *73*(6), 157 – 172. https://doi.org/10.14445/22315381/IJETT-V73I6P114

Vajpayee, P., & Hossain, G. (2024). Reduction of Cyber Value at Risk (CVaR) Through AI Enabled Anomaly Detection. *Conference Proceedings - IEEE SOUTHEASTCON*, 623 – 629. https://doi.org/10.1109/SoutheastCon52093.2024.10500040

Wang, S., Zhang, L., & Huang, X. (2026). Indoor WiFi Localization via Robust Fingerprint Reconstruction and Multi-Mechanism Adaptive PSO-LSSVM Optimization. *Applied Sciences (Switzerland)*, *16*(2). https://doi.org/10.3390/app16020753

Witayanont, Y., & Viyanon, W. (2025). Anomaly Detection in Bitcoin Network: Using Distance-based and Tree-based Unsupervised Learning Methods. *Proceedings of the 6th ACM International Symposium on Blockchain and Secure Critical Infrastructure, BSCI 2024*. https://doi.org/10.1145/3659463.3660022

Yahia, A., Mouhssine, Y., Elalaoui, A., & Ouatik Elalaoui, S. (2024). Leveraging Machine Learning for Anomaly Detection Methods in Cryptocurrency: A Data-Driven Study. *10th Edition of the International Conference on Optimization and Applications, ICOA 2024 - Proceedings*. https://doi.org/10.1109/ICOA62581.2024.10754457

Younis, S. B. (2026). An Immersive Digital Twin Framework for Intelligent Spatially Grounded Anomaly Detection in Smart Homes. *International Journal of Intelligent Engineering and Systems*, *19*(2), 1016 – 1030. https://doi.org/10.22266/ijies2026.0228.61

Zhang, Y.-Q., Lv, S.-Q., & Fan, D. (2015). Anomaly detection in online social networks. *Jisuanji Xuebao/Chinese Journal of Computers*, *38*(10), 2011 – 2027. https://doi.org/10.11897/SP.J.1016.2015.02011