IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁑ Peer-reviewed & Refereed journal ⁑ Vol. 13, Issue 9, September 2026

DOI: 10.17148/IARJSET.2026.13903

SecureCrowd: Fraud Detection and Trust Analysis in Crowdfunding

Atigadda Rama Devi[1], Panyashree K Murthy[2], P Dimple[3], Sonu C K[4], Dr. Ranjeet Kumar[5]

Dept of CSE, Don Bosco Institute of Technology Bengaluru, India[1-4]

Associate Professor, Dept. of CSE, Don Bosco Institute of Technology, Bangalore, India[5]

Abstract: Crowdfunding has emerged as an accessible means of raising financial assistance for medical needs, education, disaster response, social welfare, and community initiatives. Despite its benefits, the open and decentralized nature of online fundraising can expose donors to fraudulent campaigns, inaccurate information, inadequate verification, and uncertainty regarding campaign credibility. This paper presents SecureCrowd, a web-based crowdfunding platform designed to support fraud identification and trust-oriented campaign verification through machine learning and administrative assessment. The proposed system enables campaign creators to submit fundraising requests together with relevant supporting documents, while administrators evaluate campaigns using machine-learning predictions and documentary evidence before approval. Logistic Regression, Decision Tree, and Random Forest classifiers are employed, and their individual predictions are combined through majority voting to obtain the final classification. Campaign characteristics such as fundraising category, intended purpose, required amount, beneficiary information, urgency, previous campaign activity, description-related attributes, contact information, and supporting-document details are considered during the analysis. SecureCrowd is developed using Python and Django, with SQLite for data storage and HTML, CSS, JavaScript, Scikit-learn, and Pandas for application and data-processing functions. The platform provides role-based access, campaign management, document handling, donation tracking, verification workflows, and fundraising-progress visualization. Functional testing indicates successful operation of the major authentication, campaign, verification, donation, database, and dashboard functions. The proposed platform demonstrates the potential of combining machine-learning-based analysis with human administrative verification to promote greater transparency and confidence in online crowdfunding.

Index Terms: crowdfunding, fraud detection, trust analysis, machine learning, campaign verification, Django, donation management

I. INTRODUCTION

Crowdfunding enables individuals and organizations to obtain financial assistance from a large number of contributors through online fundraising campaigns. Such platforms can support a wide range of purposes, including medical assistance, educational requirements, disaster relief, social welfare programs, NGO activities, and other community-oriented initiatives. However, the accessibility and openness of online fundraising also introduce challenges related to fraudulent campaigns and misleading fundraising requests.

For donors, determining whether a campaign is legitimate can be difficult when only limited information is available. Factors such as the campaign description, requested funding amount, beneficiary details, urgency of the request, previous fundraising activity, and supporting documents may not provide sufficient assurance when evaluated manually. Consequently, fraudulent campaigns can undermine donor confidence and reduce transparency on crowdfunding platforms. The project report identifies fraudulent fundraising activities, misleading requests, limited donor trust, and insufficient verification as significant concerns in conventional crowdfunding systems.

SecureCrowd is proposed to address these challenges by integrating campaign management, machine-learning-assisted fraud analysis, and structured administrative verification within a single platform. In the proposed workflow, a campaign creator enters the required campaign information and uploads supporting documents. The machine-learning component then evaluates relevant campaign attributes using multiple classification techniques. The resulting prediction is provided to an administrator along with the available campaign evidence. The administrator can subsequently review the information and approve or reject the campaign. Only campaigns that successfully pass the verification process are made accessible to donors.

The primary contribution of SecureCrowd is its integration of fraud analysis into a complete crowdfunding management workflow rather than treating fraud classification as an in-dependent task. The system employs Logistic

DOI: 10.17148/IARJSET.2026.13903

Regression, Decision Tree, and Random Forest classifiers and combines their predictions using majority voting. In addition to fraud analysis, the platform maintains user, campaign, and donation information, supports document verification, provides role-specific dashboards, and enables monitoring of fundraising progress. Through this combination of automated analysis and human review, SecureCrowd aims to provide a more structured approach to campaign verification and donor trust.

II. PROBLEM STATEMENT AND OBJECTIVES

The system is designed to reduce the risk associated with suspicious fundraising campaigns while retaining administrative control over campaign approval. The main objectives are:

- develop a secure web-based crowdfunding platform;
- identify suspicious campaigns using machine-learning classifiers;
- support campaign verification using prediction results and uploaded documents;
- improve trust and transparency between creators and donors;
- provide trust and risk information during campaign evaluation;
- manage donations and fundraising progress; and
- provide separate dashboards for creators, administrators, and donors.

III. RELATED WORK

Existing research has investigated several approaches for improving the security and reliability of online crowdfunding platforms. Previous studies have examined machine-learning techniques for identifying fraudulent fundraising campaigns, artificial-intelligence-assisted campaign verification, risk pre-diction, suspicious-activity classification, ensemble learning, secure crowdfunding architectures, and methods for improving transparency. These studies indicate that computational analysis can provide an additional layer of support when evaluating the reliability of online fundraising activities.

Machine-learning-based approaches are particularly useful because campaign information can contain multiple attributes that may contribute to identifying suspicious behavior. Classification algorithms can analyze these characteristics and provide an indication of whether a campaign requires further attention. Ensemble-based approaches can further combine the decisions of multiple models, reducing dependence on the behavior of a single classifier.

Although these approaches provide useful foundations for fraud analysis, SecureCrowd focuses on integrating prediction into the broader operational process of a crowdfunding platform. Instead of limiting the system to independent fraud classification, the proposed platform connects campaign sub-mission, supporting-document management, machine-learning analysis, administrator verification, campaign approval or rejection, donor access, and donation tracking. The machine-learning output is therefore treated as a decision-support mechanism rather than a final determination of campaign authenticity.

SecureCrowd combines Logistic Regression, Decision Tree, and Random Forest classifiers and applies majority voting to generate the final prediction. This prediction is subsequently considered by the administrator together with campaign in-formation and supporting evidence. The integrated approach is intended to combine automated analytical assistance with human verification, providing a structured mechanism for managing campaign reliability and donor access.

IV. PROPOSED SYSTEM

SecureCrowd supports three primary user categories: campaign creators, administrators, and donors. The workflow is:

1) user registration and authentication;
2) campaign creation and supporting-document upload;
3) campaign feature processing;
4) Logistic Regression, Decision Tree, and Random Forest prediction;
5) majority-voting final classification;
6) administrator review of prediction and campaign evidence;
7) campaign approval or rejection;
8) donor access to approved campaigns; and
9) donation and fundraising-progress tracking.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2026

DOI: 10.17148/IARJSET.2026.13903

V. MACHINE LEARNING BASED FRAUD DETECTION

The machine-learning component evaluates campaign-related information. The project uses Logistic Regression, Decision Tree, and Random Forest.

A. *Logistic Regression*

For an input vector **x**, Logistic Regression can represent the probability of a positive class as

$$P(y = 1|\mathbf{x}) = \frac{1}{1 + e^{-(\beta_0 + \beta^T x)}} \quad (1)$$

It provides a straightforward classification baseline.

B. *Decision Tree*

A Decision Tree recursively divides campaign records using selected attributes and thresholds. Its decision structure can provide an interpretable sequence of rules for classification.

C. *Random Forest*

Random Forest combines multiple decision trees and aggregates their predictions. It provides an ensemble perspective and is used as one of the independent classifiers in SecureCrowd.

D. *Majority Voting*

Let the predictions of the three classifiers be p_1, p_2, and p_3.The final prediction is

$$\hat{y} = \mathrm{mode}(p_1, p_2, p_3). \quad (2)$$

Thus, the class receiving the majority of model decisions becomes the final result.

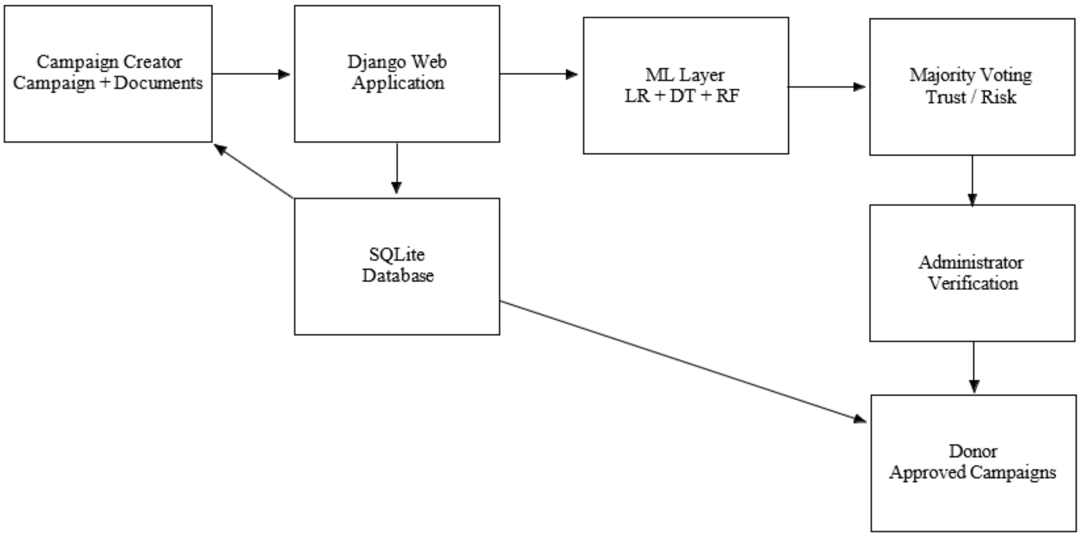

Fig. 1. High-level Secure Crowd architecture and verification workflow.

VI. TRUST AND RISK ANALYSIS

SecureCrowd uses the machine-learning result as a trust-oriented decision-support signal. The project describes campaign outcomes using categories such as Reliable, Medium Risk, and Suspicious. A trust score represents the reliability information generated during campaign verification.

The trust result is not treated as an absolute guarantee of authenticity. The administrator remains responsible for reviewing the campaign and its supporting documents before approval. This human-in-the-loop approach combines automated analysis with evidence-based administrative review.

DOI: 10.17148/IARJSET.2026.13903

VII. SYSTEM MODULES

A. *Campaign Management*

Creators can register, log in, create campaigns, provide beneficiary information, specify required funds, describe the purpose and fund-usage plan, select urgency, and upload supporting documents.

B. *Campaign Verification and Fraud Detection*

The system analyzes campaign information using the three classifiers and combines their results through majority voting. Administrators can review prediction results and campaign evidence and then approve or reject campaigns.

C. *Document Verification*

Supporting documents can be uploaded, stored, viewed, and downloaded for verification.

D. *Donation and Fund Management*

Donors can view approved campaigns, inspect details, en-ter donation amounts, and use the project's demonstration payment workflow. The collected amount is updated after successful donation activity.

TABLE I
MAJOR SECURECROWD DATABASE STRUCTURES

Table	Purpose
User	Authentication, identity, and access information.
UserProfile	Role information and additional profile data.
Campaign	Campaign, beneficiary, funding, document, status, and verification information.
Donation	Donor, campaign, amount, and donation timestamp information.

E. *Dashboard and Visualization*

Creator dashboards support campaign creation and monitoring. Administrator dashboards support verification, fraud analysis, and donation monitoring. Donor dashboards provide ap-proved campaign viewing, donation support, and fundraising-progress tracking.

VIII. DATABASE DESIGN

SecureCrowd uses SQLite as its central database. The report identifies four main structures: User, UserProfile, Campaign, and Donation.

The Campaign table contains attributes such as title, cate-gory, purpose, description, fund-usage plan, required amount, collected amount, duration, beneficiary information, contact information, document information, urgency, previous campaign counts, expected beneficiaries, declaration, status, and creation time. The Donation table records the donor, campaign, amount, and donation time.

IX. IMPLEMENTATION

The platform is implemented using Python and Django. HTML, CSS, and JavaScript provide the web interface. SQLite provides persistent storage, while Scikit-learn and Pandas support machine-learning and data-processing tasks.

TABLE II
REPRESENTATIVE FUNCTIONAL TEST RESULTS

ID	Test	Result
TC08	Donor dashboard	Pass
TC09	Donation management	Pass
TC10	Fund tracking	Pass
TC11	Dashboard monitoring	Pass
TC12	Logout/session termination	Pass

DOI: 10.17148/IARJSET.2026.13903

The implementation is modular. Campaign management, fraud detection, donation handling, dashboard visualization, document verification, and database management operate as connected components. Django also provides authentication, session handling, URL routing, forms, and database integration.

X. SECURITY AND ACCESS CONTROL

SecureCrowd uses authenticated access, session management, role-based dashboard navigation, administrative verification, and controlled document handling. The User and UserProfile structures distinguish users and their roles. Only approved campaigns are exposed to donors, creating a verification gate between campaign submission and public fundraising.

The current project uses a demonstration payment mechanism. Therefore, the implementation should be considered an academic prototype rather than a production financial transaction system.

XI. TESTING AND RESULTS

Functional testing covered authentication, campaign management, fraud detection, donation management, fund tracking, dashboard operation, document handling, and database interaction.

The project report states that users could register and log in, creators could create campaigns, documents could be uploaded and viewed, administrators could approve or reject campaigns, donors could view approved campaigns, donation amounts could be updated, and dashboard and database operations worked correctly.

The machine-learning module generated campaign verification results using Logistic Regression, Decision Tree, and Random Forest, with majority voting used for the final pre-diction.

The available report does not provide numerical model accuracy, precision, recall, F1-score, dataset size, or train/test split values. These values should be added from the actual experiments before claiming quantitative ML performance in an IEEE submission.

XII. DISCUSSION

SecureCrowd demonstrates how machine-learning-based analysis can be incorporated into a complete crowdfunding management and verification process. Rather than using the prediction output as an independent decision, the system treats it as supporting information for administrative evaluation.

Campaign documents and other available evidence can be examined by the administrator before a campaign is approved, while the approval mechanism restricts donor access to campaigns that have completed the defined verification process.

The use of three different classification techniques provides multiple analytical perspectives. Logistic Regression offers a relatively straightforward classification approach, Decision Tree provides an interpretable decision structure, and Random Forest introduces an ensemble-based classification method. Their predictions are combined through majority voting, al-lowing the final classification to reflect the decision shared by most of the participating models.

The proposed platform also contributes to operational transparency by maintaining campaign and donation information and presenting relevant details through role-based dashboards. Campaign creators can monitor their fundraising activities, administrators can review campaigns and verification information, and donors can access approved campaigns and monitor fundraising progress. Document management further supports the verification process by allowing relevant supporting information to be submitted and reviewed.

The current implementation should, however, be interpreted as an academic prototype. The available project report does not provide numerical measurements for model accuracy, precision, recall, F1-score, dataset size, or training and testing splits. Therefore, the present discussion focuses primarily on the successful implementation and functional operation of the platform rather than making quantitative claims about predictive performance. A more comprehensive evaluation using a documented dataset and standard machine-learning metrics would be required to establish the effectiveness of the individual models and the majority-voting approach.

XIII. LIMITATIONS

The current prototype does not include real banking trans-actions, live payment-gateway integration, blockchain-based transaction verification, mobile deployment, real-time notifications, AI chatbot support, or multilingual support. The donation mechanism is intended for academic demonstration. Detailed quantitative ML evaluation is also

DOI: 10.17148/IARJSET.2026.13903

not documented in the project report. Therefore, the current paper emphasizes functional validation rather than claiming a specific predictive accuracy.

XIV. FUTURE ENHANCEMENT

The project report identifies several future directions: real payment gateway integration, mobile application support, AI chatbot assistance, email and SMS notifications, blockchain-based transaction tracking, advanced fraud analytics, cloud database integration, and real-time campaign monitoring.

Future work can additionally evaluate the models on a documented dataset using precision, recall, F1-score, ROC-AUC, and confusion matrices. Trust scores can also be calibrated and accompanied by explanations so administrators can understand the factors influencing a prediction.

XV. CONCLUSION

SecureCrowd presents an integrated framework for im-proving fraud detection and trust-oriented verification in on-line crowdfunding. The proposed platform brings together campaign creation, machine-learning-assisted fraud analysis, supporting-document verification, administrative approval, do-nation management, and fundraising monitoring within a Django-based web application.

The system employs Logistic Regression, Decision Tree, and Random Forest classifiers to analyze campaign-related information, while majority voting is used to combine their predictions. Attributes including funding requirements, beneficiary information, campaign urgency, previous campaign activity, description characteristics, and supporting information contribute to the analysis. The resulting prediction serves as a decision-support signal for administrators, who retain responsibility for reviewing campaign evidence and determining whether a campaign should be approved.

Functional testing of the implemented prototype indicates successful operation of the major authentication, campaign management, document handling, verification, donation, fund-tracking, dashboard, and database workflows. The system therefore demonstrates the feasibility of combining automated classification with structured human verification to support greater transparency in crowdfunding.

The current implementation remains an academic prototype and does not claim a specific level of machine-learning ac-curacy because detailed quantitative evaluation is not documented in the available project report. Future evaluation using a properly documented dataset and metrics such as precision, recall, F1-score, ROC-AUC, and confusion matrices would provide a stronger assessment of the proposed models. Overall, SecureCrowd provides a foundation for developing more reliable and transparent crowdfunding platforms through the combined use of machine learning and administrative verification.

REFERENCES

[1]. A. Sharma and R. Gupta, “Machine Learning Based Fraud Detection in Crowdfunding Platforms,” *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 15, no. 2, pp. 210–218, 2024.

[2]. P. Verma and S. Kulkarni, “Crowdfunding Campaign Verification Using Artificial Intelligence Techniques,” *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, vol. 10, no. 1, pp. 95–102, 2024.

[3]. M. Reddy and K. Prakash, “Fraudulent Campaign Detection in Online Fundraising Platforms Using Machine Learning,” *Journal of Information Technology and Digital World*, vol. 6, no. 3, pp. 145–153, 2025.

[4]. S. Ahmed and T. Joseph, “Online Donation Fraud Analysis Using Clas-sification Algorithms,” *International Research Journal of Engineering and Technology (IRJET)*, vol. 11, no. 4, pp. 532–538, 2024.

[5]. R. Kumar and D. Singh, “AI-Based Risk Prediction for Crowdfunding Campaigns,” *International Journal of Computer Applications*, vol. 186, no. 12, pp. 20–27, 2025.

[6]. V. Patel and A. Nair, “Machine Learning Approaches for Detecting Sus-picious Crowdfunding Activities,” *International Journal of Engineering Research & Technology (IJERT)*, vol. 13, no. 5, pp. 311–318, 2024.

[7]. K. Rao and P. Mehta, “Secure Crowdfunding Platform with Fraud Detection and Donation Tracking,” *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 12, no. 1, pp. 410–417, 2025.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2026

DOI: 10.17148/IARJSET.2026.13903

[8]. T. Narayan and S. Bhat, "Crowdfunding Transparency Improvement Using Artificial Intelligence," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 13, no. 2,pp. 1220–1228, 2025.

[9]. L. Fernandes and J. Roy, "Detection of Fraudulent Fundraising Cam-paigns Using Ensemble Learning Models," *International Journal of Research Publication and Reviews (IJRPR)*, vol. 6, no. 3, pp. 950–958, 2025.

[10]. D. Wilson and H. George, "Web-Based Crowdfunding Verification System Using Machine Learning," *International Journal of Innovative Science and Research Technology (IJISRT)*, vol. 10, no. 6, pp. 184–191, 2025.