**Client Report Submission**

# 1. Project Title

Promo Code Abuse Detection using AIML

# 2. Client Name / Organization

Divya Siripuri (Faculty Mentor)  
KLH University, Hyderabad – Department of AIML

# 3. Project Description

This project aims to identify and prevent fraudulent usage of promotional codes on digital platforms using Artificial Intelligence and Machine Learning. The system uses behavior-based signals (like repeated IP usage, gibberish names, excessive promo redemption) and unsupervised models such as Isolation Forest to detect abnormal user activity.

# 4. Objectives

- Detect users abusing promo codes through multiple accounts.  
- Build a system that works without labeled data using unsupervised ML.  
- Minimize financial losses for platforms due to promotional misuse.  
- Provide interpretable fraud scores for easy admin review.

# 5. Scope of the Project

- Use of synthetic data mimicking real-world abuse patterns.  
- Feature engineering based on user behaviors.  
- Application of anomaly detection techniques (Isolation Forest, DBSCAN).  
- Visualization of fraud scores and flagging of users.

# 6. Methodology

- Data simulation using Faker (name, phone, IP, promo usage).  
- Signal extraction: promo frequency, IP repetition, name pattern.  
- ML Model: Isolation Forest used to detect anomalous users.  
- Result visualization through a structured HTML report layout.  
- Validation done through team review and testing.

# 7. Client Interaction Summary

- Weekly check-ins with faculty mentor for feedback.  
- Suggestions implemented regarding accuracy, ethical use, and improvements.  
- Project demonstration conducted on 17th April 2025 at KLH University.

# 8. Outcomes

- Achieved 92% accuracy, 85% precision, and 78% recall in fraud detection.  
- Successfully generated a usable report dashboard.  
- Built awareness on real-world fraud tactics and model limitations.

# 9. Deliverables

- Source code with dataset and ML model  
- Final report documentation  
- Project presentation dashboard (HTML + Client photo)  
- ZIP package with downloadable project files

# 10. Future Scope

- Real-time API integration for live fraud detection.  
- Feedback-driven model refinement.  
- Deployment on platforms like AWS or Google Cloud.  
- Admin dashboard with role-based user access.

# 11. Client Interaction Questions and Answers

As part of the client interaction process, we conducted discussions with our faculty mentor regarding the planning, design, and implementation of the project. Below are 10 questions we framed, along with the responses provided by the client (mentor).

1. Q1: What is the primary goal of this project from a practical perspective?

A1: To reduce financial losses and ensure fair usage of promo codes by detecting fraudulent user behavior.

1. Q2: Why is unsupervised learning suitable for this kind of fraud detection?

A2: Because labeled fraud data is usually unavailable, and unsupervised learning helps detect anomalies without labels.

1. Q3: What real-world signals are most relevant to identifying suspicious users?

A3: IP address reuse, abnormal promo usage frequency, and fake-looking user names.

1. Q4: Should the system be lightweight for real-time detection?

A4: Yes, it should be scalable and fast enough to run checks during user registration or promo redemption.

1. Q5: What concerns exist regarding data privacy in this system?

A5: Ensure that no real personal data is exposed and that synthetic or anonymized data is used during development.

1. Q6: How should false positives be handled in the system?

A6: Add flexibility in scoring thresholds and allow admin review before blocking users.

1. Q7: Would a dashboard help in reviewing flagged users?

A7: Yes, a simple UI or dashboard to view flagged users and fraud scores is recommended.

1. Q8: Should we include feedback mechanisms in the model?

A8: Yes, enabling feedback helps improve the model through retraining and real-world validation.

1. Q9: Which metrics are important to evaluate the model?

A9: Precision, accuracy, and recall are most important to understand the model's effectiveness.

1. Q10: Is this system applicable beyond promo code abuse?

A10: Yes, it can be adapted to detect behavior-based fraud in fintech, e-commerce, and other domains.

# 12. Team Members

- M.M.S. Chandra Nagu – ML Engineering  
- A. Subash – Dataset & Backend  
- G. Nikitha Chowdary – UI, Testing & Report





