# Automated Fake Review Detection for E-Commerce

# 1. Project Title

## Enhancing Open-Source for Automated Fake Review Detection in E-Commerce

# 2. Aim of the Project

The objective is to develop an open-source system that detects fake e-commerce reviews in platforms with an emphasis on system enhancement. The proposed system will track fraudulent reviews in real-time by enhancing its capabilities in Natural Language Processing (NLP) as well as sentiment analysis capabilities metadata evaluations and reviewer behaviour assessment (Maysam Jalal Abd and Mohsin Hasan Hussein, 2024).

## Research Gap:

Existing methods for detecting false reviews depend on static data collections and hardcoded linguistic indicators which fail to identify new kinds of fraud activities. This project closes the present gap by developing improved open-source frameworks that perform adaptive real-time fake review detection (Editor, 2024).

Additionally, current open-source tools like SpaCy and Scikit-Learn struggle with real-time adaptability in detecting deceptive patterns such as bot-generated reviews, paid promotional reviews, and mass manipulation strategies (e.g., coordinated review bombing). This project aims to bridge this gap by enhancing open-sourceframeworks to handle real-time, adaptive fake review detection with improved NLP, metadata tracking, and reviewer behaviour analysis.

# 3. Research Questions (RQ) /Hypothesis

Primary Research Question:

The optimization of an open-source AI-based platform which detects fake reviews in e-commerce platforms requires an assessment of how to enhance both system accuracy rates and platform adaptability.

Sub-questions:

1. What modifications can NLP technologies implement to boost the capability of detecting irregularities in fake review language?

2. What changes should be implemented to existing open-source ML models for optimizing their precision and recall functions in the identification of fraudulent reviews?

3. Which techniques will result in maximum efficiency for( timestamps, and verification) when detecting fraud?

4. How does analysing reviewer behaviour contribute to improved accuracy in detecting fraudulent content, and what specific patterns are most indicative of fake reviews?.

# 4. Objectives

1. Evaluate existing open-source fake review detection models (such as SpaCy, Scikit-Learn, and NetworkX) to identify their limitations and improvement areas.
2. Research and development work will produce improved NLP-based technology that detects deceptive reviews through linguistic pattern examination combined with sentiment analysis functions.
3. The process of algorithm “Anomaly-Aware Fraud Scoring System” implementation should include model modification and optimization to enhance fraud detection capabilities.(Sun et al., 2024).
4. The system should include an anomaly detection system that will improve fraud detection capability.
5. The organization should build a real-time fraud detection dashboard through visualization solutions including Streamlet.

# 5. Short Description of Idea

The Automated Fake Review Detection for E-Commerce project works to improve open-source models which detect misleading reviews thus guaranteeing authenticity in digital marketplaces. Present fake review detection systems use fixed datasets along with predefined rules which fail to catch the latest fraud strategies. The project implements continuous learning methods to enhance real-time adaptability while it improves the techniques of NLP sentiment analysis and machine learning methodologies.

This platform unites three essential improvements which involve linguistic analysis reviewer tracking and metadata-based detection methods. The system examines text patterns user sentiment scores and anomalous reviewer activity through the combination of SpaCy, Scikit-Learn and NetworkX with TensorFlow. The model will continuously learn new ways of detecting fraud by using adaptive algorithms and adapt itself to emerging fraudulent tactics to establish an advanced protection network for e-commerce platforms(Baishya et al., 2021).

# 6. Open-Source Tools Used

**Existing Projects: Algorithms Used & Their Drawbacks**

Most present-day fake review detection systems use either static rule-based models or machine learning classifiers which demonstrate limited flexibility for advanced fraud approaches.

**Existing Algorithms & Their Drawbacks**

1. **TF-IDF + Logistic Regression/SVM**
   * ✅ *Used for text-based classification (fake vs. real reviews).*
   * ❌ *The system fails to detect advanced fake reviews across different natural language variations particularly those generated bytechnology.*
2. **Random Forest & XGBoost**
   * ✅ *This model demonstrates success at identifying fraudulent patterns found in reviewer metadata.*
   * ❌ *Struggles with real-time adaptability and dynamic fraud techniques.*
3. **LSTM-Based Detection**
   * ✅ *Effective for sequence-based pattern recognition.*
   * ❌ *The system requires high computational power while remaining susceptible to fitting patterns that may change during an evolution of fraud patterns.*

# **Unique Algorithm We Are Using & Why It’s Better**

#### **Anomaly-Aware Fraud Scoring System (Proposed Adaptive Model)**

#### Real-time anomaly detection together with adaptive machine learning and graph-based fraud analysis form a new approach in the system.

#### **How It’s Better Than Existing Models?**

The continuous learning ability allows it to adapt in real-time for detection of new fraud patterns while static ML models cannot achieve this.

Multiple fraud detection layers exist through an integrated system which combines NLP (BERT) and Metadata Tracking (XGBoost) and Reviewer Graph Analysis (NetworkX).

Anomaly-Based Scoring generates precise fraud probability evaluations by analysing reviewer actions with linguistic patterns together with metadata information.

#### **Performance Improvement Over Existing Models**

The system provides higher precision through automatic threshold control which decreases misidentification cases.

The system enables the processing of big e-commerce information at real-time speeds to improve scalability.

The adaptive combination of models predominantly surpasses conventional fraud prevention approaches because it continuously adapts to fresh deceptive methods making online stores more reliable and secure.

## Enhancement Scope:

The performance of sentiment models trained for previous tasks needs improvement to achieve effective fraud pattern detection in context.

The ML frameworks require enhanced optimisation of their anomaly detection algorithm.

The team should use visualization tools through Streamlit to create an operational dashboard that alerts about current frauds in real time.

# 7. Research Methodology

## 7.1 Data Collection

The review process includes text data evaluation derived from open-source e-commerce databases.

• User Behaviour Data: Includes reviewer frequency, IP addresses, and geolocation.

The dataset contains timestamps from ratings, purchase records, and rating patterns as metadata elements.

## 7.2 NLP-Based Text Analysis

The analysis group performs Linguistic Feature Extraction by seeking repeated phrases and assessing unnatural text elements.

• Stylometry Analysis: Detecting inconsistencies in reviewer writing style.

• TF-IDF & BERT Embeddings: Enhancing feature representation.

## 7.3 Reviewer Behaviour & Network Analysis

Review clustering through graph networks allows the detection of fraudulent reviewer operations.

The system uses IP and Geolocation Analysis methods to detect patterns when users use multiple IP addresses for posting reviews (Ijraset.com, 2023).

## 7.4 Machine Learning Model Development

The development process includes Supervised Learning through the use of labelled fake review datasets.

Unsupervised Learning methods discover fraudulent patterns which have not yet been identified.

The evaluation measures for the models include precision, recall, and F1-score, along with ROC-AUC.

## 7.5 Real-Time Metadata Analysis

The system detects temporal irregularities in review posting timestamps.

The system confirms the authenticity of reviewers through a process which cross-validates their purchase records.

# 8. Expected Contributions

• Enhancement of Open-SourceModels for improved fake review detection.

An Adaptive Learning Framework needs development to fight new emerging fraud methods.

• Scalability for Large-Scale E-Commerce platforms with real-time fraud detection.

• Improved Trust & Transparency in online product reviews (Paul and Nikolaev, 2021).

# 9. Conclusion

The research project enhances open-sourcetechnology through the development of an accurate and flexible fake review identification solution. This research implements advanced NLP, sentiment analysis with metadata evaluation and reviewer behaviour tracking to address the current difference between static models and real-time fraud detection requirements.

# References

Baishya, D., Deka, J.J., Dey, G. and Singh, P.K. (2021). SAFER: Sentiment Analysis-Based FakE Review Detection in E-Commerce Using Deep Learning. *SN Computer Science*, 2(6). doi:https://doi.org/10.1007/s42979-021-00918-9.

Editor (2024). *Fake Reviews and How to Detect Them With the Help of AI*. [online] AltexSoft. Available at: <https://www.altexsoft.com/blog/fake-review-detection/>.

Ijraset.com. (2023). *A Brief Study on the Fake Review Detection methods on Ecommerce Websites using Machine Learning, Artificial Intelligence, and Data Science*. [online] Available at: https://www.ijraset.com/research-paper/fake-review-detection-methods-on-ecommerce-websites [Accessed 27 Feb. 2025].

Maysam Jalal Abd and Mohsin Hasan Hussein (2024). Fake reviews detection in e-commerce using machine learning techniques: A comparative survey. *BIO Web of Conferences*, 97, pp.00099–00099. doi:https://doi.org/10.1051/bioconf/20249700099.

Paul, H. and Nikolaev, A. (2021). Fake review detection on online E-commerce platforms: a systematic literature review. *Data Mining and Knowledge Discovery*, 35. doi:https://doi.org/10.1007/s10618-021-00772-6.

Sun, P., Bi, W., Zhang, Y., Wang, Q., Kou, F., Lu, T. and Chen, J. (2024). Fake Review Detection Model Based on Comment Content and Review Behavior. *Electronics*, [online] 13(21), p.4322. doi:https://doi.org/10.3390/electronics13214322.

# Appendix

* Do you require data information and code which needs challenging access?

All necessary information along with tools exist publicly and they are easy to access.

* The proposal implements a study along with development work.

The project requires adaptive fraud detection model development through machine learning with additional graph analysis capabilities.

* The project duration can be considered achievable through defined evaluation steps and model training stages and data collection phases.

The project timeline proves to be realistic due to defined checkpoints for data collection phases and model training sections and performance assessments.

* The project represents an appropriate form of work.

The approach uses novel strategies to address a major problem in fake review identification through an operational solution.

* What will you learns?

Techniques in NLP, anomaly detection and graph-based fraud analysis for real-world fraud detection.

* What is your contributions?

A combined fraud detection platform increases the ability to accurately discover false review content and adapt for future improvements.

* The artifact will have this capability.

The system will perform real-time fake review detection through the integration of anomaly detection and fraud scoring layered security systems.

* Your solution addresses the following question.

Engineering an adaptive system for fake review detection leads to both higher detection accuracy along with detecting a larger volume of fake online reviews.

# Project Timeline (600 Hours)

| **Phase** | **Tasks** | **Time Allocation** |
| --- | --- | --- |
| **Week 1-2 (80 hours)** | I will perform research on fraud detection methods while collecting data sets and establishing the problem statement. | 80 hours |
| **Week 3-4 (80 hours)** | The operations include data preprocess followed by review text and metadata and reviewer network cleaning and structuring. | 80 hours |
| **Week 5-6 (80 hours)** | The system implements BERT + TF-IDF to detect anomalies in text. | 80 hours |
| **Week 7-8 (80 hours)** | Develop XGBoost-based metadata anomaly detection. | 80 hours |
| **Week 9-10 (80 hours)** | The project adopts NetworkX to establish a graph model which analyzes reviewer behavioral patterns. | 80 hours |
| **Week 11 (40 hours)** | Strategies for combining models need to be executed alongside normalization procedures for developing a single fraud scoring framework. | 40 hours |
| **Week 12 (40 hours)** | Evaluate how the models perform as well as perform scale tests and adjust detection thresholds | 40 hours |
| **Week 13 (40 hours)** | The team should perform evaluations and compare results to current systems before analyzing detection precision rates of fraud. | 40 hours |
| **Week 14 (40 hours)** | The project includes steps for documenting the methodology together with findings which leads to the creation of the final report. | 40 hours |
| **Week 15 (40 hours)** | The project delivers the final version after review for potential errors followed by improvements and completion of submission. | 40 hours |