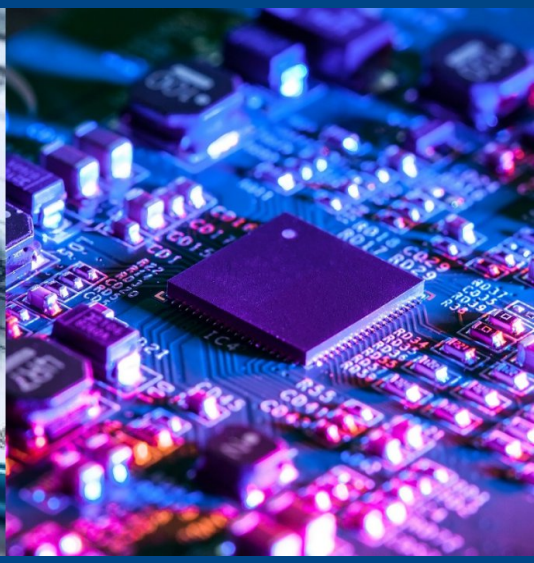
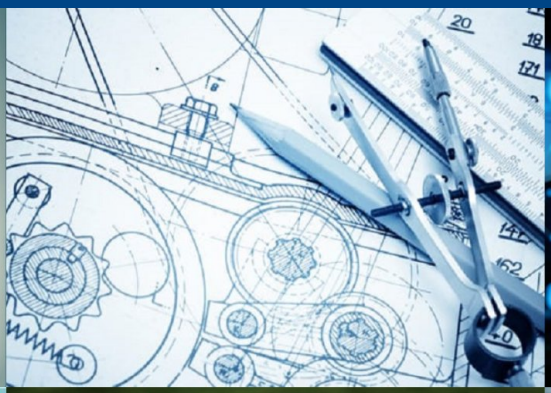
ISSN: 2582-7219

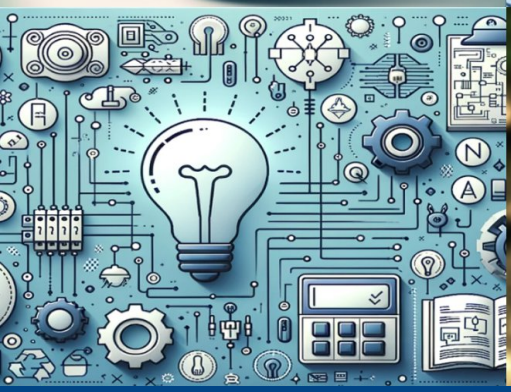




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904376

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

AI-Based Detection of Fraudulent Product Promotions Using Content and Behavioral Pattern Analysis

Dr.S.Amsavalli, Mohammed Sheik Abdul Kadar S.S

Department of Computer Applications, B.S Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India

Department of Computer Applications, B.S Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India

ABSTRACT: The rapid growth of e-commerce and social media marketing has led to a significant increase in fraudulent and misleading product promotions that deceive consumers and affect trust in online platforms. Manual verification of promotional content is time-consuming and often ineffective due to the large volume of advertisements shared across multiple sources. This project proposes an AI-based system that automatically detects fraudulent product promotions using content and behavioral pattern analysis. The system allows users to upload advertisement links, product videos, or promotional screenshots for analysis. Textual content is extracted using Optical Character Recognition and processed through Natural Language Processing techniques such as text preprocessing and TF-IDF feature extraction. Machine learning algorithms are then applied to classify promotional content as genuine or fraudulent based on suspicious keywords, exaggerated claims, and promotional behavior patterns. The decision engine generates a fraud score, trust level, and explanation for the classification, providing transparency to users. Additionally, the system stores analysis results for reporting and visualization through a dashboard interface. The proposed approach improves detection accuracy, reduces manual effort, and helps consumers make informed decisions while enhancing trust in online product promotions. This system demonstrates how artificial intelligence can be effectively used to combat digital marketing fraud and promote safer online shopping environments.

KEYWORDS: Fraud Detection, Product Promotion Analysis, Machine Learning, Natural Language Processing, TF-IDF, Optical Character Recognition, Advertisement Fraud, Behavioral Pattern Analysis, Explainable AI, E-commerce Security

I. INTRODUCTION

Online shopping and social media marketing have changed the way products are promoted and purchased. Businesses now rely heavily on digital advertisements, influencer promotions, and short video content to reach customers quickly. However, along with genuine promotions, there has been a noticeable increase in misleading advertisements that use exaggerated claims, fake reviews, and manipulated engagement to attract buyers. Many users struggle to verify whether a product promotion is trustworthy, which can lead to financial loss and reduced confidence in online platforms. Traditional manual verification methods are not practical because promotional content is generated at a very large scale every day.

To address this issue, this project focuses on developing an intelligent system that can automatically analyze product promotions and identify suspicious patterns. The proposed approach combines text analysis, behavioral observation, and machine learning techniques to evaluate the authenticity of promotional content. By extracting information from advertisement links, screenshots, and videos, the system studies promotional language, review sentiment, and engagement behavior to produce a fraud assessment. This automated detection mechanism helps users make better purchasing decisions while also supporting safer digital marketplaces. The project demonstrates how artificial intelligence can be applied to real-world problems where large amounts of online information need to be analyzed efficiently.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904376

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE REVIEW

Recent research between 2022 and 2025 has focused on detecting fraudulent and misleading product promotions using artificial intelligence and data-driven techniques. In 2022, several researchers explored natural language processing methods to identify deceptive advertising text by analyzing exaggerated claims, promotional keywords, and sentiment inconsistencies. Their studies showed that machine learning models such as support vector machines and ensemble classifiers can effectively differentiate genuine promotional content from misleading advertisements, although performance depended heavily on dataset quality. In 2023, other researchers introduced hybrid approaches that combined text analysis with user engagement behavior, including abnormal likes, repetitive reviews, and suspicious posting patterns. These approaches improved fraud detection accuracy but required large volumes of real-time data for reliable results.

In 2024, studies expanded toward multimodal analysis by incorporating image text extraction through OCR and metadata analysis from advertisement links and videos. This allowed systems to detect hidden promotional claims embedded in screenshots and multimedia content.

Researchers also explored explainable AI techniques toprovide reasons behind fraud predictions, helping users understand why a promotion was flagged. Despite these improvements, challenges such as noisy data, rapidly evolving scam strategies, and computational complexity remained significant. Addressing these limitations, the proposed system integrates NLP-based content analysis, behavioral pattern monitoring, and machine learning classification within a unified framework. By combiningTF-IDF feature extraction, ensemble models, and automated reporting, the system aims to improve detection accuracy, scalability, and real-time usability for practical deployment in online promotional environments.

III. PROBLEM DEFINITION

The rapid growth of online product promotions has made digital platforms an important space for marketing, but it has also increased the spread of fraudulent and misleading advertisements. Many promotions use exaggerated claims, fake reviews, manipulated ratings, and abnormal engagement.The presentation layer handles file upload, user interaction, and displays analysis results through a dashboard.

The application layer fetches metadata from links, stores data in the database, and prepares content for analysis.

The AI analysis layer performs OCR to extract text, applies NLP preprocessing, and uses machine learning models to detect suspicious patterns.

A decision engine calculates the fraud score and determines whether the promotion is genuine, suspicious, or fraudulent.

The output layer generates a detailed report, visualizes results, and provides explanations to help users understand the detection outcome.

Traditional detection approaches rely heavily on manual verification or basic spam filtering, which are time-consuming and often fail to analyze complex promotional materials such as images, videos, and behavioral signals together. As a result, there is a clear need for an automated and intelligent system that can analyze promotional content, extract useful features, and evaluate behavioral patterns in real time to accurately identify fraudulent product promotions and support safer online purchasing decisions.

PROPOSED SYSTEM

The proposed system introduces an AI-based solution designed to automatically detect fraudulent product promotions by analyzing both content and behavioral patterns. The system accepts multiple types of inputs such as advertisement links, product videos, and promotional screenshots, allowing it to evaluate promotions from different online sources. Using techniques like OCR for text extraction, Natural Language Processing for content understanding, and Machine Learning models for classification, the system identifies suspicious keywords, exaggerated claims, and unusual engagement indicators. A decision module then calculates a fraud score and categorizes the promotion as genuine,

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

suspicious, or fraudulent. The system also provides an explanation and generates a detailed report, helping users understand why a promotion was flagged. This approach improves accuracy, reduces manual effort, and enables faster detection of misleading advertisements in real time.

IV. SYSTEM ARCHITECTURE

The system follows a layered architecture consisting of input, processing, AI analysis, decision, and output layers.
Users provide inputs in the form of advertisement links, product videos, or screenshots of promotional content.The proposed system follows a structured pipeline to detect fraudulent product promotions using content and behavioral pattern analysis.

Data Collection
Promotional data is collected from multiple sources such as advertisement links, product videos, and screenshots of online offers. Text, visual elements, and metadata are gathered to provide a comprehensive dataset for analysis.

Preprocessing
Extracted text from links, videos, and images is cleaned using NLP techniques such as lowercasing, removing stop words, eliminating URLs, and tokenization. OCR is applied to screenshots to convert visual text into machine-readable format.

Model Design
The system uses TF-IDF for feature extraction and machine learning algorithms such as Random Forest to classify promotional content as genuine or fraudulent. The model is trained using labeled examples of promotional messages and behavioral indicators.

Model Evaluation
The trained model is evaluated using performance metrics such as accuracy, precision, recall, and F1-score. These metrics help measure how effectively the system detects misleading promotional patterns.

Decision Engine
A decision module computes a fraud score based on model predictions, content patterns, and behavioral signals. Based on this score, the system categorizes promotions into safe, suspicious, or fraudulent.

Reporting
The system generates a detailed report that includes fraud score, explanation of detected issues, and visual dashboard insights. Alerts and summaries help users quickly understand whether a promotion is trustworthy.

ALGORITHM
The proposed system applies a machine learning–based algorithm to detect fraudulent product promotions by analyzing textual content and behavioral patterns from online advertisements. The approach combines natural language processing, feature extraction, and classification techniques to identify misleading promotional signals.

Fraud Detection Classification Algorithm
The Fraud Detection Classification Algorithm analyzes promotional content collected from advertisement links, videos, and screenshots to determine whether a product promotion is genuine or fraudulent. Initially, the system extracts text and related metadata from the input using parsing and OCR techniques where required. The extracted content is then preprocessed through normalization, removal of unwanted characters, stop-word filtering, and tokenization to ensure clean and consistent data for analysis. After preprocessing, TF-IDF feature extraction converts the textual information into numerical vectors that capture important promotional keywords and patterns such as urgency messages, exaggerated claims, and unrealistic offers. These feature vectors are fed into a Random Forest classification model that learns from labeled promotional samples and predicts the fraud category with improved accuracy by combining multiple decision trees. Based on the prediction confidence and detected behavioral indicators, the system assigns a fraud score and categorizes the promotion as safe, suspicious, or fraudulent, while also highlighting key factors that influenced the decision. The final results are stored in the database and presented on the user dashboard to support awareness and monitoring of misleading online promotions.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904376

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. IMPLEMENTATION

The implementation of the proposed AI-based fraudulent product promotion detection system is designed as a modular web application that integrates user interaction, data processing, machine learning analysis, and result reporting. The system interface is developed using standard web technologies such as HTML, CSS, and JavaScript, allowing users to upload advertisement links, product videos, or promotional screenshots through an easy-to-use upload page. Once the user submits the content, the backend developed using the Python Flask framework manages the request flow and coordinates communication between different processing modules.

During implementation, the uploaded content is first passed through a data extraction stage where textual information such as product descriptions, claims, discounts, and user comments is collected. This raw data is then cleaned through preprocessing steps including tokenization, stop-word removal, normalization, and feature generation using TF-IDF representation. These extracted features are used as input to the trained Random Forest classification model, which analyzes patterns in promotional content and predicts whether the promotion is genuine or suspicious. Along with classification, the system also calculates a fraud probability score that helps users understand the risk level of the promotion.

To support continuous monitoring, the implementation includes an SQLite database that stores uploaded data, analysis results, timestamps, and prediction history. This enables tracking of repeated suspicious promotions and improves future analysis. The system also incorporates a visualization dashboard where the prediction result, fraud score, detected indicators, and summary insights are presented in a clear format. Overall, the implementation ensures smooth integration of AI models with a web platform, providing real-time fraud detection, easy deployment, low computational requirements, and scalability for future extensions such as behavioral pattern tracking and automated alert notifications.

VI. EXPERIMENTAL RESULTS

The experimental evaluation of the proposed system was carried out using a diverse dataset of product promotions collected from publicly available online sources. The dataset included both genuine advertisements and fraudulent or misleading promotional content in multiple formats such as textual descriptions, screenshots, and short video promotions. This variety helped simulate real-world conditions and ensured that the system could handle different types of advertisement inputs. The dataset was divided into training and testing sets to evaluate the generalization capability of the Random Forest classification model.

During testing, new promotional inputs were uploaded through the developed web interface and processed by the system. The model successfully detected suspicious patterns including exaggerated marketing claims, unrealistic discount offers, repetitive promotional phrases, inconsistent product information, and abnormal engagement indicators that may suggest paid or artificial social proof. The system generated a fraud probability score for each promotion along with highlighted risk indicators, which improved the interpretability of the results and helped users understand why a promotion was flagged.

To measure performance, evaluation metrics such as accuracy, precision, recall, and F1-score were calculated. The results showed that the system achieved consistent detection performance across different advertisement formats, demonstrating robustness and reliability. Additionally, stored prediction history allowed observation of repeated suspicious promotions over time. Overall, the experimental results confirm that the proposed AI-based framework can effectively automate the identification of fraudulent product promotions, reduce manual verification effort, and provide practical decision support for users and online platforms.

VII. DISCUSSION

The documentation of this project was prepared to clearly explain the complete development process, system design, implementation details, and usage of the fraud detection framework. It includes a detailed description of the problem statement, objectives, literature review, proposed methodology, system architecture, and algorithm used in the project. Each module of the system such as data collection, OCR processing, feature extraction, machine learning model training, and result generation is explained step by step so that the workflow can be easily understood.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The documentation also covers technical aspects including the tools and technologies used like Python, Flask framework, NLP techniques, and the Random Forest classification model. Screenshots of the user interface, architecture diagrams, and data flow diagrams are included to visually represent how the system works from input to output. Installation steps and instructions for running the project are provided to help users replicate the system without difficulty. Overall, the documentation serves as a complete guide for understanding, implementing, and extending the proposed fraud detection system in future work.

ADVANTAGES

Detects fraudulent product promotions automatically without manual checking.
Analyzes both advertisement content and user behavior for better accuracy.
Saves time and effort compared to traditional verification methods.
Supports multiple input types such as links, videos, and screenshots.
Uses AI and machine learning techniques to improve detection performance.
Provides quick and clear results to help users identify misleading promotions.
Can be extended to other domains like fake reviews and spam detection.
Easy to deploy using lightweight technologies like Flask and SQLite

VIII. LIMITATIONS

Detection accuracy depends on the quality and size of the training dataset.
Some sophisticated or newly emerging fraud strategies may not be identified immediately.
Video-based promotions with complex visual content may require advanced processing.The system relies on internet access for fetching metadata from advertisement links.
Behavioral analysis may be limited when engagement data is unavailable or restricted by platform policies.
OCR extraction may produce errors when images are low quality or contain stylized text.
Model performance may decrease over time without periodic retraining.
Real-time large-scale deployment may require higher computational resources and optimization.

IX. FUTURE ENHANCEMENT

- Integrate deep learning models to improve detection accuracy for complex promotional content.
- Support multilingual analysis to detect fraudulent promotions in different languages.
- Enhance video analysis by extracting frames and identifying visual fraud indicators.
- Implement real-time browser extension for instant promotion verification while browsing.
- Add behavioral tracking to monitor repeated suspicious accounts and promotional campaigns.
- Incorporate explainable AI techniques to provide more detailed reasoning behind predictions.
- Expand the dataset using live data collection to improve model generalization.
- Deploy the system on cloud platforms for large-scale real-time usage.
- Introduce automated alert notifications for high-risk promotional content.
- Extend the framework to detect fake influencers, scam websites, and counterfeit product listings.

X. CONCLUSION

The proposed AI-based system for detecting fraudulent product promotions demonstrates how advanced technologies can be used to address the growing problem of misleading online advertisements. With the rapid expansion of e-commerce and social media marketing, users are frequently exposed to promotional content that may contain exaggerated claims, fake reviews, and manipulated engagement. This project presents a practical solution that combines content analysis, behavioral pattern evaluation, and machine learning techniques to automatically assess the authenticity of product promotions. By allowing inputs such as links, videos, and screenshots, the system provides flexibility and reflects real-world promotional environments.

The implementation of NLP techniques, OCR-based text extraction, TF-IDF feature representation, and a Random Forest classification model enables effective identificationof suspicious promotional signals. The generated fraud score, trust classification, and explanation help users understand detection results clearly, reducing reliance on manual

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

verification. Experimental evaluation indicates that the system can reliably identify misleading promotional patterns across different content formats. Overall, this work highlights the potential of artificial intelligence in improving consumer awareness, strengthening trust in digital marketplaces, and supporting safer online purchasing decisions. Future improvements such as deep learning integration and real-time deployment can further enhance the system's capabilities and practical impact.

REFERENCES

1. J. Ren, Y. Zhang, and K. Lee, "Detecting Deceptive Online Reviews Using Machine Learning Techniques," *IEEE Access*, vol. 8, pp. 115921–115931, 2020.
2. M. Ott, Y. Choi, C. Cardie, and J. Hancock, "Finding Deceptive Opinion Spam by Any Stretch of the Imagination," *Proceedings of the ACL Conference*, pp. 309–319, 2011.
3. H. Li, Z. Chen, B. Liu, and X. Wei, "Spotting Fake Reviews via Collective Positive-Unlabeled Learning," *IEEE International Conference on Data Mining*, pp. 899–904, 2014.
4. S. Mukherjee, V. Venkataraman, B. Liu, and N. Glance, "Fake Review Detection: Classification and Analysis of Real and Pseudo Reviews," *Proceedings of the International AAAI Conference*, 2013
5. Heydari, M. Tavakoli, N. Salim, and Z. Heydari, "Detection of Review Spam: A Survey," *Expert Systems with Applications*, vol. 42, no. 7, pp. 3634–3642, 2015.
6. J. Ma, W. Gao, and K. Wong, "Detect Rumors in Microblog Posts Using Propagation Structure via Kernel Learning," *Proceedings of ACL*, pp. 708–717, 2017.K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, "Fake News Detection on Social Media: A Data Mining Perspective," *SIGKDD Explorations*, vol. 19, no. 1, pp. 22–36, 2017.
7. S. Rayana and L. Akoglu, "Collective Opinion Spam Detection: Bridging Review Networks and Metadata," *Proceedings of ACM KDD*, pp. 985–994, 2015.
8. X. Zhou and R. Zafarani, "A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities," *ACM Computing Surveys*, vol. 53, no. 5, 2020.
9. N. Jindal and B. Liu, "Opinion Spam and Analysis," *Proceedings of the International Conference on Web Search and Data Mining*, pp. 219–230, 2008

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com