International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Fake Product Review Detection Using Machine Learning

**Akashatha D K[1], Arfa M H[2], Jayaprada Y G[3], Manjunath Godi[4], S. Krishna Anand[5]**

[1,2,3,4,5]Dept. of Artificial Intelligence and Data Science, Shridevi Institute of Engineering and Technology, Tumkuru. Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka

**Abstract.**
Online product reviews play a crucial role in the purchas- ing pattern of customers. Fake reviews may, mislead consumers. A large number of fake reviews will even cause huge property losses and pub- lic opinion crises. Therefore, it is necessary to detect and filter fake re- views. To solve this problem, a novel technique to detect fake reviews has been proposed. Credibility of online reviews is crucial for business and can directly affect companies reputation and profitability. The proposed technique deals with the usage of URL's and IP addresses for identi- fying fake reviews. The designed algorithm is expected to achieve high accuracy levels.

## 1 INTRODUCTION

With a rapid growth in technology, a variety of jobs which took ages to com- plete were finished in fraction of that period. However, in hindsight, a large amount of misuse of technology leading to cybercrimes have reason in recent times. Phishing attacks deceive uses by not only stealing their information but also pass fraudulent messages there by providing misleading information. One of the areas deal with sending fake review messages.

It is a known fact that a large number of human beings read review information about a product before actual purchases. Fake reviews tend to disrupt the buy- ing habits of users eventually to leading to their dissatisfaction. An additional problem that can arise due to fake reviews is damage to the reputation of the company.

A large amount of money has been spent to detect cybercrimes which keep in- creasing with each passing day. To overcome the same, urgent measures must be taken to find a solution for the same. Since reviews published by reviewers are uncertain and the fact that there is an unknown aspect to the credibility of reviews, an evaluation index system needs to be designed that is able to judge the authenticity of reviews.

As intelligent scammers are able to cleverly make fake reviews appear real, com- plex machine learning techniques must be used for accurate detection. This work accepts URL's and IP addresses and uses a combination of XG boost and Ran- dom Forest algorithms for finding its genuineness.

URL based methods have the distinct advantages of detecting a fake message without clicking on the URL. By accurately screening the fake reviews and mak- ing them unavailable for users view,

the level of user satisfaction can be enhanced significantly.

## 2 LITERATURE SURVEY

Until the early part of 20th century, the advancement in technology has been growing at a snail's phase. The number of different types of products were lim- ited. Most of the products exhibit a high level of quality. However, the latter half of 20th century saw a rapid growth of technology. Besides, a large number of tools were also designed to cater to many applications. The growth of technology also allowed heavy misuse of the same. Owing to a section of people, a number of fake products started coming into existence.

The late 1990's dealt with a large number of tools pertaining to networking. Dur- ing the year 1992, Harris and his team designed an application [1] that provided the internet with autonomous intelligence that was distributed throughout the network. During the year 1996, Bernhard West Fechtel performed an analysis by constructing variety of graphs for combining set of products and processes [2]. They were able to demonstrate how concurrent engineering is supported through the process of exchanging pre- releases of intermediate results. During the year 1998, Fan Yushun and Wu Cheng designed a tool [3] for increasing the speed of integration of products. Wu Cheng improvised on the work done by his prede- cessors by designing a tool for increasing the speed of integration of products. The beginning of the 21st Century saw a rapid growth in science. New algorithms were formulated at breadth neck speed. During the year 2002, Wan Xiang and his team incorporated a clustering algorithm [4] for connection of manet and internet. They used a number of parameters like pohler, movement probability and hop length. The simulation results showed that this clustering technique is found to be more robust and has less overheads. One more feature which was pri- marily needed by customers is on time delivery of the product. Charlene Spoede Budd, and Marjorie adopted two different approaches [5] namely Critical path method and Critical chain method in the year 2005. They found that there was significant amount of saving in time while using chain method with critical path method.

During the year 2008, Qiu Lingyun and Li Dong considered an online shopping model [6] focusing exclusively on parameters like perceived usefulness, ease of use, trust, social presence and perceived enjoyment. They also found the rela- tionship between these parameters.

After 2010, with rapid usage of social media, the number of reviews ran into millions. During this period, the number of fake reviews also increased multi- field. The need for a new technique arose for identifying genuine reviews. During the year 2017, Lu Zhang and his team designed a partially supervised learning model [7] for detecting spammer groups. They used a combination of naive Bayes algorithm and expectation maximization algorithm for constructing a classified as spammer Group detector. During the same year, Neng Li and his team con- sidered the specific domain of farming [8]. They considered community based features and user-based features like Support vector machine, K-nearest neigh- borhood and Random forest for distinguishing between a genuine farmer and a fake farmer. During the year 2018, Suyuan Luo and Shaohua Wan improvised

[9] on the work carried out by fellow researchers by formulating a conceptual framework for extracting the characteristics of fraudulent transactions.

During the year 2019, Jindi Fu and his team worked on the prospects of collabo- rative shopping [10]. They survived a group of 233 customers and analysed their buying behaviour. They used a number of similarity coefficients for finding the group of buyers with similar traits. This in turn could provide

the vendors with ideas on collaborative shopping.

With passage of time, a number of companies formulated strategies for increas- ing spam reviews in order to boost the company's name, recognition and profit. Online reviews had become the main source for determining public opinions. To overcome this problem, during the beginning of 2020, Hussain and his team detected spam reviews [11] using two methods namely behavioral and linguistic. They found that the behavioral model generated in accuracy of 93.1linguistic model generated an accuracy of 88.5the end of the year, Meiling Liu and her team considered additional factors for detecting fake reviews. They found that the existing techniques do not consider the implicit patterns among users, re- views and products.

During 2021, Jianrong Yao and his team combined resampling with Grid search technique [12] for identifying the appropriate features off irrelevant and unnec- essary parameters and optimize the model. A similar analysis was carried out in the year 2022 by Thi-KimHien and his team [13]. The team also considered linguistic and behavioral aspects. They proposed a hierarchal logistic regression technique and found that the designed model performed better than existing model. During the year 2023, Rosario and her team exploited the usage of two language models [14] namely Bert and Electra in a new Italian data set that pertains to cultural heritage of Italy. They were able to achieve an accuracy of 95detecting fake reviews. During June 2023, Mehedi and his team designed a number of methods [15] like expert based manual fact checking, crowd source fact checking and deep learning techniques for detecting fake news. During the end of the year, Mohammad Ennaouri and Ahmed zelleou performed a [16] com- prehensive analysis of various machine learning techniques for identifying fake reviews.

One more survey of deep Learning techniques for fake newsdetection was per- formed [17] in the year 2024 by Enaiafe Festus Ayetiran and Ozlem Ozgobe. It was observed that however good a technique is, it can identify false review only to a certain extent. To find a solution to this problem, Samia and her team adopted a fusion approach [18] where they combined the characteristics of a number of techniques like CNN and aspect-based analysis. Appropriate weightages were given to each aspect of the network and it was found that the proposed model outperformed existing models on both review authenticity and aspect analysis. This innovative approach gave an accuracy of 97.75 In order to fine tune and validate the research, this work focuses on using ML Algorithms like XG Boost and Random Forest for identifying fake websites.

## 3 METHODOLOGY

Our proposed approach for fake review detection involves the following steps:

- Data Collection: Reviews are sourced from multiple e-commerce platforms.
- Feature Extraction: URL structures and IP metadata are analyzed.
- Machine Learning Models: We use XGBoost and Random Forest classifiers.
- Evaluation Metrics: Accuracy, Precision, Recall, and F1-score.

## 4 GENUINESS OF PRODUCT REVIEWS

Fake product reviews are a significant challenge in ecommerce, affecting con- sumer trust and product credibility. Machine learning has emerged as a robust solution to identify and mitigate such reviews by analyzing textual patterns, metadata, and user behavior. The process begins with data collection, where reviews are sourced from platforms like Amazon, Yelp or TripAdvisor. These

datasets may include labeled examples of genuine and fake reviews, often iden- tified through verified purchases, platform moderation or expert assessments. Public datasets such as Yelp's Fake Review Dataset are also widely used for research and development. The collected data typically includes the review text, ratings, timestamps, reviewer profiles and other metadata that help in detecting anomalies indicative of fake reviews.

Data preprocessing is a critical step in the pipeline, aimed at cleaning and or- ganizing the raw data for analysis. Text preprocessing involves removing unnec- essary elements like HTML tags, special characters and stop words to ensure that text is standardized. Tokenization breaks the text into smaller units, such as words or phrases, while stemming and lemmatization reduce words to their root forms, making analysis more efficient. Behavioral features are also incorpo- rated, focusing on patterns like sudden surges in reviews, reviewer activity and metadata like account age or verified purchases. Sentiment analysis can further provide insights by identifying unnatural patterns, such as overly positive or negative sentiments that deviate from normal user behavior.

Feature engineering combines these textual and behavioral elements to create a robust input for machine learning models. Textual attributes such as word fre- quency, sentiment polarity and the use ofspecific linguistic styles like excessive adjectives or repetitive phrases are common indicators of fake reviews. Metadata- based features include temporal patterns, such as bursts of reviews within a short period, and reviewer traits, such as submitting reviews for unrelated products or writing near-duplicate content. These features are fed into machine learning models to classify reviews as fake or genuine.

Machine learning models for fake review detection range from traditional algo- rithms to advanced deep learning approaches. Traditional models such as logis- tic regression, support vector machines (SVM) and random forests are widely used for their simplicity and efficiency. Ensemble methods like gradient boosting (e.g., XGBoost and LightGBM) often provide superior performance by combin- ing multiple weak classifiers into a strong one. For more complex textual data, deep learning models like recurrent neural networks (RNNs), long short-term memory networks (LSTMs), and transformers are employed. These models excel in capturing contextual and sequential patterns in text, making them highly ef- fective for natural language processing (NLP) tasks. In cases where labeled data is limited, unsupervised methods such as clustering and anomaly detection can identify suspicious reviews based on deviations from normal patterns.

Model evaluation is essential to ensure the effectiveness of the system. Com- mon metrics include accuracy, precision, recall, and F1 score, which measure the model's ability to correctly classify fake and genuine reviews. The area under the receiver operating characteristic curve (ROC-AUC) is also used, particularly in scenarios with imbalanced datasets, where the number of genuine reviews far outweighs fake ones. Techniques like oversampling, under sampling or using synthetic data generation methods like SMOTE are employed to address this imbalance.

Despite effectiveness, machine learning-based fake review detection faces several challenges. Fraudulent reviewers continually adapt their tactics, requiring reg- ular updates to models and features. Imbalanced datasets can lead to biased models, necessitating careful handling during training and evaluation. Ethical and privacy concerns also arise, as analyzing reviewer data must be done re- sponsibly to avoid violating user rights.

Additionally, over-reliance on automated systems can result in false positives, where genuine reviews are incorrectly flagged as fake, potentially harming the reputation of honest users.

## 5 TOOLS

For efficient demonstration, an aesthetic view is needed for clear presentation and demonstration. Although a number of tools are in place, the appropriate choice of tool plays a major role in projecting the appropriate details. Power BI plays a crucial role in detecting fake product reviews through its integration with machine learning techniques, such as the XGBoost algorithm, for identify- ing fraudulent reviews effectively. XGBoost, a highly efficient gradient boosting model, is used for classifying reviews as genuine or fake by analyzing features such as sentiment, reviewer activity and review text. Power BI enhances the analysis process by providing an interactive platform for visualizing the results of these machine learning models.

It connects to various data sources, such as review databases and customer pro- files, enabling the seamless integration of XGBoost predictions into interactive dashboards and reports. With Power BI's advanced analytics capabilities, busi- nesses can visualize key metrics such as the accuracy of the XGBoost model feature importance, and trends in fraudulent reviews across different product categories. Visualizations like bar charts, scatter plots and heatmaps allow stake- holders to explore review patterns and gain insights into suspicious behaviors en- abling proactive actions to maintain product authenticity. By tracking Key Per- formance Indicators (KPIs), Power BI facilitates better decision-making, helping businesses improve customer trust and ensureing a more transparent review sys- tem. KPI's include attributes like the percentage of fake reviews detected and improvement in product ratings.

The graph shown in Fig 1. clearly shows that the count of reviews are higher in Earphones compared to other gadgets.

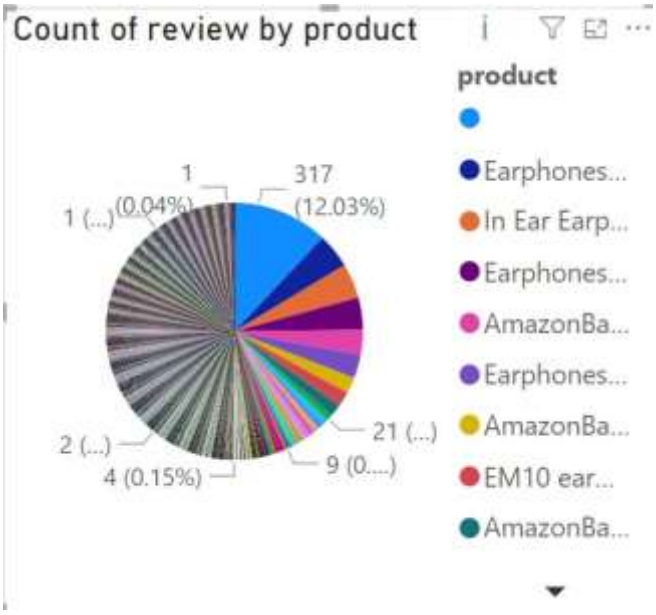


**Fig 1. Count of Reviews by Products**

The graph shown in Fig 2. clearly shows that the sum count of reviews are higher during the years 2015 and 2016.

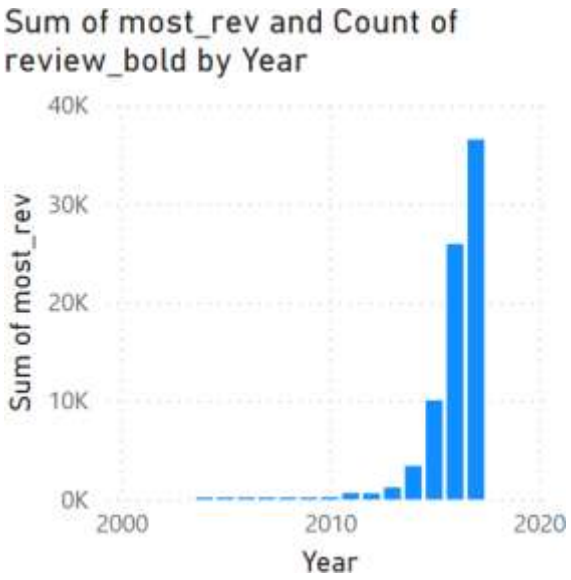


**Fig 2. Count of reviews by year**

## 6 EXPERIMENTAL RESULTS

The dataset consists of 10,000 reviews categorized into real and fake classes. Our experimental analysis demonstrates that XGBoost achieves the highest accuracy.

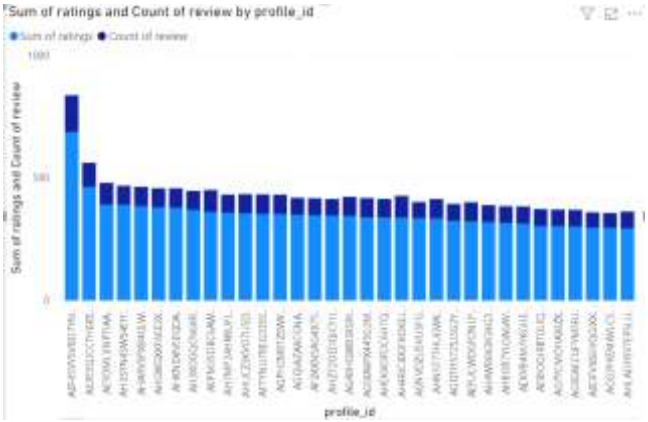


**Fig.3 Distribution between sum of Ratings and count of Review by Profile ID**

Using the technique of XGBoost, a set of ratings and the number of reviews for each product has been diagramatically shown in Fig.3. It could be clearly ob- served that the product with profile id AEF45VY5VBO7YN has a much higher rating as compared to other products which indirectly also leads to the fact that the number of review for the same are much higher.

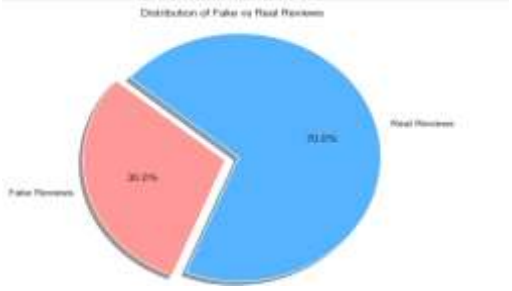

**Fig. 4 Distribution of Fake and Real Reviews**

The bigger challenge lies in the fact that a number of reviews could be fake. The demonstrated technique is able to identify the set of genuine and fake reviews. A set of reviews for 2500 electronic items, 1800 clothes, 1000 cosmetics and 2000 footwear items were analyzed using this algorithm. It was found that approxi- mately one in three reviews were found to be falsely generated. On the whole, 30fake. This information has been clearly demonstrated in Fig.4.


**Fig.5 Display that the given URL is Real**


**Fig.6 Display that the given URL is Fake**

This system is able to identify the genuiness of the product given its URL. Snapshots showing Real and Fake URL's have been shown in Fig.5 and Fig.6.

Table 1. Model Performance Metrics

| Model | Accuracy | Precision | Recall |
|---|---|---|---|
| XGBoost | 92% | 91% | 90% |
| Random Forest | 89% | 88% | 87% |
| SVM | 85% | 83% | 82% |

## 7 CONCLUSION

An efficient machine learning algorithm has been found to be highly efficient in detecting the genuineness of product reviews. By providing the appropriate URL's and IP addresses, XGBoost machine learning algorithms were able to identify the genuineness of a product with an accuracy of 92%.

The novelty in this approach lies in the fact that even if one of the inputs is not provided, the algorithm is able to maintain this accuracy level. With the database containing a large number of IP address available to human beings for a variety of purposes, chances are that errors can creep up. Errors include digits erroneously getting replaced by other digits or a digit may be inavertedly missed out owing to the mistake of the operator or other reasons. The innovative features inbuilt in the designed algorithm is its ability to foresee such issues and also make an automatic correction on the same.

Machine learning provides a powerful approach to combating fake product re- views by leveraging a combination of NLP, behavioral analysis, and advanced modeling techniques. By incorporating both textual and metadata features, these systems can effectively identify fraudulent activity and maintain theintegrity of online review platforms. Continuous advancements in machine learning, coupled with ethical considerations and robust evaluation will be crucial for addressing the evolving nature of fake reviews and preserving trust in e-commerce ecosys- tems.

Perfection is a keyword that is found only in the dictionary. Although 100tech- niques could be devised for increasing the accuracy levels. This work can be combined with other machine learning

algorithm or achieving accuracy of more than 95steps could be taken for completely eliminating the fake reviews before they come into customer's views. This in turn could go a long way in increasing the levels of customer satisfaction while purchasing the product.

**References**

1. N.G Harris, N.Burmeister, A.Cowan, "An Intelligent Internet Platform and Applications", IEEE Network, June 1992.
2. Bernhard Westfechtel, "Integrated Product and Process Management for Engineering Design Application", IEEE Transactions on Software Engineering, 1996.
3. Fan Yushun , Wu Cheng , "Development of a Support Tool for Rapid Application Integration of CMS", Tsinghua Science and Technology, Vol. 3, June 1998, pp.991-996.
4. Wan Xiang, Yao Yinxiong, Wang Haoxing, "New clustering algorithm for interconnection of MANET and internet", Journal of Systems Engineering and Electronics, Vol.15, April 2002, pp.83-89.
5. Charlene Spoede Budd, Marjorie J.Cooper, "Improving on-time service delivery :The case of project as product", IEEE Network, 2005, pp.67-81.
6. Qiu Lingyum, LI Dong, "Applying TAM in B2C E-Commerce Research: An Extended Model", Tsinghua Science and Technology, Vol 13, June 2008, pp.265-272.
7. Lu Zhang, Zhiang Wu, "Detecting Spammer Groups From Product Re- views :A Partially Supervised Learning Model", IEEE Access, Nov 2017.
8. Neng Li, Suguo Du, Haizhong Zheng, Minhui Xue, Haojin Zhu, "Fake Reviews Tell No Tales Dissecting Click Farming in Content -Generated Social Networks", IEEE/CIC International Conference on Communications in Chinas, 2017.
9. Suyuan Luo, Shaouhua Wan, "Leveraging Product Characteristics for Online Collusive Detection in Big Data Transactions", IEEE Access, Dec 2018.
10. Jindi Fu, Yuan Sun, Yao Zhang, Shuiqing Yang, "Does Similarity Matter The Impact of User Similarity on Online Collaborative Shopping, IEEE Access, Dec 2019.
11. Naveed Hussian, Hamid Turab Mirza, Ibrar Hussain, Faiza Iqbal, Im- ran Memon, "Spam Review Detection Using the Linguistic and Spammer Be- havioural Methods", IEEE Access, Jan 2020.
12. Jianrong Yao, Yuan Zheng, Hui Jiang, "An Ensemble Model for Fake Online Review Detection Based on Data Resampling Feature Pruning and Pa- rameter Optimization", IEEE Access, Jan 2021.
13. Thi Kim Hien Le, Yi-Zhen Li, Sheng Tun Li, "Do Reviews Words and Behaviours Help Detect Fake Online Reviews and Spammers Evidence From a Hierarchial Model", IEEE Access, Mar 2022.
14. Rosario Catelli, Luca Bevilacqua, Nicola Mariniello, Vladimiro Scotto DiCarlo, Massimo Magaldi, Hamido Fujita, Giuseppe De Pietro, Massimo Es- posito, "A New Italian Cultural Heritage Data Set: Detecting Fake Reviews With BERT and ELECTRA Leveraging the Sentiment", IEEE Access, April 2023.
15. Mehedi Tajrian, Azizur Rahman, Muhammad Ashad Kabir, MD. Rafiqul Islam, "A Review of Methodologies for Fake News Analysis", IEEE Access, June 2023.
16. Mohammad Ennaouri, Ahmed Zellou, "Machine Learning Approaches for Fake Reviews

Detection and Systematic Literature Review", Journal of Web Engineering, Vol. 22, Dec 2023.
17. Eniafe Festus Ayetiran, Ozlem Ozgobek, "A review a Deep Learning Techniques for Multimodal Fake News and Harmful Languages Detection", IEEE Access, April 2024.
18. Samia Alhalem, Hesham Arafat Ali, Naglaa F Soliman, Abeer D Algarni, Hanaa Salem Marie, "Advancing E-Commerece Authenticity:A Novel Fushion Approach Based on Deep Learning and Aspect Features for Detecting False Reviews", IEEE Access, June 2024.