



# Survey of Fake Review Detection and Classification on Amazon Dataset

<sup>1</sup>Kajal Bisen, <sup>2</sup>Prof Hitesh Gupta, <sup>3</sup>Dr. Vivek Richhariya

<sup>1</sup>MTech Scholar, Department of Computer Science & Engineering, Lakshmi Narain College of Technology, Bhopal, India

<sup>2</sup>Assistant Professor, Department of Computer Science & Engineering, Lakshmi Narain College of Technology, Bhopal, India

<sup>3</sup>Professor & HOD, Department of Computer Science & Engineering, Lakshmi Narain College of Technology, Bhopal, India

*Abstract*— The ubiquity of online reviews has transformed the decision-making process for consumers, with platforms like Amazon hosting millions of product reviews. However, the prevalence of fake reviews poses significant challenges to maintaining the integrity and reliability of this user-generated content. This survey paper provides a comprehensive review of the state-of-the-art techniques for detecting and classifying fake reviews on the Amazon dataset. We examine various approaches, including text-based analysis, sentiment analysis, and behavioral analysis, along with machine learning and deep learning methods. By analyzing the strengths and limitations of these techniques, we aim to provide a clear understanding of the current landscape and identify future directions for research in this critical area. This survey highlights the importance of developing robust detection mechanisms to ensure the trustworthiness of online reviews and supports the ongoing efforts to combat fraudulent activities in e-commerce.

*Keywords*— *Fake Review, Classification, Amazon, Dataset.*

## I. INTRODUCTION

The advent of e-commerce has fundamentally changed the way consumers interact with products and services, with platforms like Amazon playing a pivotal role in this transformation. These platforms not only facilitate the purchase of a wide array of goods but also provide a space for users to share their experiences through reviews. These user-generated reviews are crucial as they significantly influence potential buyers' decisions and offer valuable feedback to sellers. However, the integrity of these reviews has been increasingly compromised by the presence of fake reviews, which are intentionally misleading and designed to manipulate consumer perception.

Fake reviews can take various forms, including overly positive reviews intended to boost the reputation of a product and overly negative reviews aimed at damaging the reputation of competitors. The motives behind these fake reviews are

diverse, ranging from attempts to increase sales to efforts to sabotage rival products. This phenomenon poses a serious challenge not only for consumers, who rely on honest feedback to make informed decisions, but also for e-commerce platforms striving to maintain credibility and trustworthiness. Consequently, detecting and mitigating fake reviews has become a critical area of research and development.

The Amazon dataset, with its extensive and diverse collection of reviews, offers a rich resource for studying fake review detection. Researchers have leveraged this dataset to develop and test various methodologies aimed at identifying fraudulent activities. These methodologies typically fall into three broad categories: text-based analysis, sentiment analysis, and behavioral analysis. Each approach focuses on different aspects of the review data, providing unique insights into the characteristics of fake reviews and contributing to the development of more effective detection models.

Text-based analysis involves examining the linguistic features of reviews to detect anomalies that may indicate deceit. Techniques such as Term Frequency-Inverse Document Frequency (TF-IDF), n-grams, and word embeddings are employed to extract features that can distinguish between genuine and fake reviews. Sentiment analysis, on the other hand, focuses on the emotional tone of reviews. By assessing the sentiment expressed in the text, researchers can identify patterns that deviate from normal user behavior, such as overly enthusiastic praise or unwarranted criticism, which are often hallmarks of fake reviews.

Behavioral analysis examines the patterns and activities of reviewers to detect suspicious behavior. Factors such as the frequency of reviews, the diversity of products reviewed, and the timing of reviews can provide significant clues about the authenticity of a reviewer. For instance, a reviewer who posts a high number of reviews in a short period or reviews a wide range of unrelated products may be engaging in fraudulent activity. By integrating these various analytical approaches,



researchers aim to develop comprehensive models that can accurately detect and classify fake reviews, thereby enhancing the reliability of online review systems and contributing to a more trustworthy e-commerce environment.

## II. LITERATURE REVIEW

S. C, et al.,[1] Fake reviews are a growing concern for e-commerce websites and other online platforms. To tackle this issue, researchers have developed an advanced convolutional neural network system that can detect and classify fake reviews. This system has been specifically designed to analyze the Amazon review dataset, and by integrating various text pre-processing methods and an innovative attention mechanism, it has significantly improved its classification accuracy.

J. Jeong, et al.,[2] Inexperienced consumers may have high uncertainty about experience goods that require technical knowledge and skills to operate effectively; therefore, experienced consumers' prior reviews can be useful for inexperienced consumers. However, one-sided review systems (e.g., Amazon) only provide the opportunity for consumers to write a review as a buyer and contain no feedback from the seller's side, so the information displayed about individual buyers is limited. Overall, this approach developed in this work is applicable, scalable, and interpretable for distinguishing important drivers of consumer reviews for different goods in a specific industry and can be used by industry to design customer-oriented marketing strategies.

B. Lebichot et al.,[3] Credit card fraud jeopardizes the trust of customers in e-commerce transactions. This led in recent years to major advances in the design of automatic Fraud Detection Systems (FDS) able to detect fraudulent transactions with short reaction time and high precision. Nevertheless, the heterogeneous nature of the fraud behavior makes it difficult to tailor existing systems to different contexts (e.g. new payment systems, different countries and/or population segments). Given the high cost (research, prototype development, and implementation in production) of designing data-driven FDSs, it is crucial for transactional companies to define procedures able to adapt existing pipelines to new challenges. From an AI/machine learning perspective, this is known as the problem of transfer learning.

X. Chen et al.,[4] This work studies the automated control method for regulating air conditioner (AC) loads in incentive-based residential demand response (DR). The critical challenge is that the customer responses to load adjustment are uncertain and unknown in practice. In this work, we formulate the AC control problem in a DR event as a multi-period stochastic optimization that integrates the indoor thermal dynamics and customer opt-out status transition. Specifically, machine learning techniques including Gaussian process and logistic regression are employed to learn the unknown thermal dynamics model and customer opt-out behavior model, respectively.

S. Wu et al.,[5] In the telco industry, attracting new customers is no longer a good strategy since the cost of retaining existing customers is much lower. Churn management becomes instrumental in the telco industry. As there is limited study combining churn prediction and customer segmentation, this work aims to propose an integrated customer analytics framework for churn management. There are six components in the framework, including data pre-processing, exploratory data analysis (EDA), churn prediction, factor analysis, customer segmentation, and customer behaviour analytics. This framework integrates churn prediction and customer segmentation process to provide telco operators with a complete churn analysis to better manage customer churn. Three datasets are used in the experiments with six machine learning classifiers. First, the churn status of the customers is predicted using multiple machine learning classifiers. Synthetic Minority Oversampling Technique (SMOTE) is applied to the training set to deal with the problems with imbalanced datasets.

K. Ali et al.,[6] presented TagSee, a multi-person tracking system based on monostatic RFID imaging. TagSee is based on the insight that when customers are browsing the items on a shelf, they stand between the tags deployed along the boundaries of the shelf and the reader, which changes the multi-paths that the RFID signals travel along, and both the RSS and phase values of the RFID signals that the reader receives change. Based on these variations observed by the reader, TagSee constructs a coarse grained image of the customers.



## International Journal of Recent Development in Engineering and Technology

Website: [www.ijrdet.com](http://www.ijrdet.com) (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)

E. Umuhoza et al.,[7] Given the fierce competition that has come up because of evolving FinTech and e-payment industries in the global market, the credit card industry has become extremely competitive. To survive, financial institutions need to offer their credit card customers with more innovative financial services that provide a personalized customer experience beyond their banking needs. While we are witnessing this high competition that aims to provide better services to credit card holders, Africa risks remaining behind once again: in 2017, the World Bank reported that only 4.47% of Africans aged 15 and above hold a credit card. In this work, we define and describe the steps that can be taken to build a behavioral-based segmentation model that differentiates African credit cardholders based on their purchases data.

L. Fan et al.,[8] Load forecasting can enhance the reliability and efficiency of operations in a home energy management system (HEMS). The rise of big data with machine learning in recent years makes it a potential solution. This work proposes two new energy load forecasting methods, enhancing the traditional sequence to sequence long short-term memory (S2S-LSTM) model. Method 1 integrates S2S-LSTM with human behavior patterns recognition, implemented and compared by 3 types of algorithms: density based spatial clustering of applications with noise (DBSCAN), K-means and Pearson correlation coefficient (PCC). Among them, PCC is proven to be better than the others and suitable for a large number of residential customers.

Y. Yuan et al.,[9] Advanced metering infrastructure (AMI) enables utilities to obtain granular energy consumption data, which offers a unique opportunity to design customer segmentation strategies based on their impact on various operational metrics in distribution grids. However, performing utility-scale segmentation for unobservable customers with only monthly billing information, remains a challenging problem. To address this challenge, we propose a new metric, the coincident monthly peak contribution (CMPC), that quantifies the contribution of individual customers to system peak demand. Furthermore, a novel multi-state machine learning-based segmentation method is developed that estimates CMPC for customers without smart meters (SMs): first, a clustering technique is used to build a databank

containing typical daily load patterns in different seasons using the SM data of observable customers.

F. Zheng et al.,[10] Mobile networks and smart phones have become ubiquitous in our daily life. Large amount of customer related telecom data from various sources are generated every day, from which diversified behavior patterns can be revealed, including some anomalous behaviors that are vicious. It becomes increasingly important to achieve both efficient and effective customer behavior analysis based on the telecom big data. In this work, the Multi-faceted Telecom Customer Behavior Analysis (MTCBA) framework for anomalous telecom customer behavior detection and clustering analysis is proposed. In this framework, further design the hierarchical Locality Sensitive Hashing-Local Outlier Factor (hierarchical LSH-LOF) scheme for suspicious customer detection, and the Autoencoders with Factorization Machines (FM-AE) structure for dimension reduction to achieve more efficient clustering.

### III. FAKE REVIEW DETECTION TECHNIQUES

The detection of fake reviews encompasses a variety of techniques that can be broadly categorized into text-based analysis, sentiment analysis, and behavioral analysis. Each of these approaches leverages different aspects of the review data to identify fraudulent activities.

1. **Text-Based Analysis:** Text-based analysis focuses on the linguistic characteristics of reviews. Techniques such as Term Frequency-Inverse Document Frequency (TF-IDF), n-grams, and word embeddings are commonly used to extract features from the review text. These features are then used to train machine learning models to distinguish between genuine and fake reviews. Recent advancements in natural language processing (NLP) have introduced sophisticated models like transformers, which can capture deeper contextual nuances in the text, thereby enhancing detection accuracy.
2. **Sentiment Analysis:** Sentiment analysis examines the emotional tone of reviews. Fake reviews often exhibit exaggerated sentiments, either overly positive



## **International Journal of Recent Development in Engineering and Technology**

**Website: [www.ijrdet.com](http://www.ijrdet.com) (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)**

or excessively negative. By analyzing sentiment scores and patterns, researchers can identify reviews that deviate from the norm. Techniques such as sentiment polarity analysis and emotion detection have been employed to uncover inconsistencies that may indicate fraudulent intent.

3. **Behavioral Analysis:** Behavioral analysis investigates the patterns and behaviors of reviewers. Features such as review frequency, review length, reviewer history, and temporal patterns can provide valuable insights into the likelihood of a review being fake. For instance, reviewers who post numerous reviews within a short period, or who review a wide range of unrelated products, may exhibit suspicious behavior indicative of fake reviews.

### **IV. MACHINE LEARNING AND DEEP LEARNING APPROACHES**

Machine learning and deep learning techniques form the backbone of modern fake review detection systems. Traditional machine learning algorithms such as logistic regression, support vector machines (SVM), and random forests have been widely used in this domain. These algorithms can be trained on labeled datasets to classify reviews based on the extracted features.

Deep learning approaches, particularly those involving neural networks, have shown great promise in recent years. Recurrent neural networks (RNNs) and convolutional neural networks (CNNs) can capture sequential and spatial patterns in the text, respectively. The advent of transformer models, such as BERT and GPT, has further revolutionized the field by enabling the analysis of long-range dependencies and context within reviews. These models can be fine-tuned on specific datasets to achieve high accuracy in fake review detection.

### **Comparative Analysis and Evaluation**

Evaluating the performance of fake review detection models involves various metrics such as accuracy, precision, recall, and F1-score. It is crucial to conduct a comparative analysis of different techniques to understand their strengths and limitations. Ensemble methods, which combine multiple

classifiers, have been found to enhance detection performance by leveraging the complementary strengths of individual models.

### **V. CHALLENGES AND FUTURE DIRECTIONS**

Despite significant advancements, fake review detection faces several challenges. The ever-evolving tactics of fraudsters necessitate continuous adaptation and improvement of detection models. Additionally, the imbalanced nature of datasets, with a smaller proportion of fake reviews compared to genuine ones, poses a challenge for model training. Future research should focus on developing more robust models that can generalize well across different product categories and adapt to emerging fraudulent patterns.

Moreover, the integration of explainable AI techniques can enhance the transparency and interpretability of detection models, making them more trustworthy for end-users and platform administrators. Collaborative efforts between researchers, industry practitioners, and regulatory bodies are essential to develop comprehensive solutions that can effectively combat fake reviews and maintain the integrity of online review systems.

### **VI. PROPOSED STRATEGY**

- Load the Amazon Review Dataset from the Kaggle

In this step, the customer review dataset will be downloaded from kaggle source. It is a large dataset providing company. Then load this dataset into the python environment.

- Visualizing the Dataset

Now open the dataset files and view the various data in term of features like product name, quantity, review, purchasing time, number of visit, add to cart etc.

- Pre-process the Dataset



## International Journal of Recent Development in Engineering and Technology

Website: [www.ijrdet.com](http://www.ijrdet.com) (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)

Now the data preprocess step applied, here data is finalized for processing. Missing data is either removed or replaced with a constant one or zero in this step.

- Splitting the Dataset into training and testing

In this step, the final preprocessed dataset is divided into the training and the testing dataset. In the machine learning, firstly the machine is trained through the given dataset then it comes in the tested period for the remaining dataset.

- Classification Using Machine Learning Algorithm

Now apply the machine learning technique to find the performance parameters. The existing work applied several techniques and found Naïve Bayes is a better method than others. In the proposed method, we apply the logistic regression method and optimize the better results than other approaches. According to the researchers, the logistic regression method is good for optimization to enhance the accuracy.

- Performance Metrics (Accuracy, Precision, Recall, F1 - Score)

Now the performance parameters are calculated in terms of precision, recall, f-1 measure, accuracy etc by using the following formulas-

True Positive (TP): predicted true and event are positive.

True Negative (TN): Predicted true and event are negative.

False Positive (FP): predicted false and event are positive.

False Negative (FN): Predicted false and event are negative.

### VII. CONCLUSION

The detection and classification of fake reviews on e-commerce platforms like Amazon are paramount to maintaining the integrity and trustworthiness of user-generated content. Through the combined efforts of text-based analysis, sentiment analysis, and behavioral analysis, researchers have developed sophisticated methodologies that significantly enhance the identification of fraudulent reviews. This survey highlights the critical advancements and ongoing challenges in

this field, emphasizing the need for continuous innovation to stay ahead of evolving fraudulent tactics. By improving detection mechanisms, we can ensure a more reliable and trustworthy online shopping experience, ultimately benefiting consumers, businesses, and the broader e-commerce ecosystem.

### REFERENCES

1. S. C. R. S and U. K, "Fake Review Detection and Classification Using Improved Convolutional Neural Network on Amazon Dataset," 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2023, pp. 398-403, doi: 10.1109/ICPCSN58827.2023.00071.
2. J. Jeong, "Identifying Customer Preferences From User-Generated Content on Amazon.Com by Leveraging Machine Learning," in IEEE Access, vol. 9, pp. 147357-147396, 2021, doi: 10.1109/ACCESS.2021.3123301.
3. B. Lebichot, T. Verhelst, Y. -A. Le Borgne, L. He-Guelton, F. Oblé and G. Bontempi, "Transfer Learning Strategies for Credit Card Fraud Detection," in IEEE Access, vol. 9, pp. 114754-114766, 2021, doi: 10.1109/ACCESS.2021.3104472.
4. X. Chen, Y. Li, J. Shimada and N. Li, "Online Learning and Distributed Control for Residential Demand Response," in IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 4843-4853, Nov. 2021, doi: 10.1109/TSG.2021.3090039.
5. S. Wu, W. -C. Yau, T. -S. Ong and S. -C. Chong, "Integrated Churn Prediction and Customer Segmentation Framework for Telco Business," in IEEE Access, vol. 9, pp. 62118-62136, 2021, doi: 10.1109/ACCESS.2021.3073776.
6. K. Ali and A. X. Liu, "Monitoring Browsing Behavior of Customers in Retail Stores via RFID Imaging," in IEEE Transactions on Mobile Computing, doi: 10.1109/TMC.2020.3019652.
7. E. Umuhoza, D. Ntirushwamaboko, J. Awuah and B. Birir, "Using Unsupervised Machine Learning Techniques for Behavioral-based Credit Card Users Segmentation in Africa," in SAIEE Africa Research Journal, vol. 111, no. 3, pp. 95-101, Sept. 2020, doi: 10.23919/SAIEE.2020.9142602.



**International Journal of Recent Development in Engineering and Technology**

**Website: [www.ijrdet.com](http://www.ijrdet.com) (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)**

8. A. Sonkar, S. K. Sahu, A. Nayak, D. Sahu, P. Verma and R. Tiwari, "An Efficient Privacy-Preserving Machine Learning for Blockchain Network," *2024 4th International Conference on Intelligent Technologies (CONIT)*, Bangalore, India, 2024, pp. 1-6, doi: 10.1109/CONIT61985.2024.10627061.
9. Y. Yuan, K. Dehghanpour, F. Bu and Z. Wang, "A Data-Driven Customer Segmentation Strategy Based on Contribution to System Peak Demand," in *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 4026-4035, Sept. 2020, doi: 10.1109/TPWRS.2020.2979943.
10. F. Zheng and Q. Liu, "Anomalous Telecom Customer Behavior Detection and Clustering Analysis Based on ISP's Operating Data," in *IEEE Access*, vol. 8, pp. 42734-42748, 2020, doi: 10.1109/ACCESS.2020.2976898.