A hybrid approach to behavioral spam review detection on e-commerce platforms using apriori and CNN

Ganesh Wayal, Vijay Bhandari
Department of Computer Science and Engineering, Madhyanchal Professional University, Bhopal, India

Article Info

Article history:

Received Nov 12, 2024
Revised Apr 8, 2025
Accepted Jul 2, 2025

Keywords:

Behavioral analysis
Convolutional neural networks
E-commerce websites
Mitigation strategies
Reviewer reputation modeling
Sentiment analysis
Spam detection

ABSTRACT

Spam reviews significantly undermine the credibility of online review systems on e-commerce websites. This paper presents a hybrid methodology that combines the Apriori algorithm and convolutional neural networks (CNN) to efficiently identify and mitigate spam reviews. By examining user behavior, including activity patterns, reviewer reputation, temporal dynamics, and sentiment consistency, we propose a comprehensive model for understanding user interactions and engagement. To extract important information and build precise spam detection models, we use data mining and machine learning approaches. Furthermore, contextual and domain-specific analyses are conducted to improve detection strategies. The study highlights the significance of hybrid techniques in preserving the integrity of e-commerce platforms through successful industry implementations and presents evaluation metrics, problems, and future research objectives.

Corresponding Author:

Ganesh Wayal
Department of Computer Science and Engineering, Madhyanchal Professional University
Bhopal, India
Email: ganeshw2006@gmail.com

1. INTRODUCTION

In the digital era, e-commerce websites have revolutionized shopping by offering convenience, variety, and access to a global marketplace. A crucial aspect influencing consumer decision-making on these platforms is online reviews. Potential clients can make well-informed purchasing selections with the help of online reviews, which offer insightful commentary from past customers. However, the authenticity and trustworthiness of these reviews have been significantly compromised by the presence of review spam [1], [2].

Review spam refers to the deliberate manipulation of reviews for promotional, malicious, or deceptive purposes. It encompasses a wide range of deceptive tactics, including fake reviews, opinion spam, and Sybil attacks [3]. Fake reviews are comments written by people or organizations with the intention of harming rival businesses or promoting their own goods. Submissions of false reviews that distort the reviewer's actual opinions are known as opinion spam. Sybil attacks involve the creation of multiple fake identities to deceive readers and manipulate the overall rating of a product or service [4]. A serious threat to the trustworthiness and dependability of e-commerce platforms is the proliferation of review spam. Consumers rely on reviews to make informed decisions, and when these reviews are tainted by spam, the trustworthiness of the entire system is compromised [5]–[7].

This study addresses the gaps in existing research on spam review detection. While previous studies have individually analyzed either behavioral patterns or textual features, they have not adequately explored integrating both aspects comprehensively. Specifically, earlier approaches have overlooked the combined effect of user behavior analysis (e.g., posting frequency, reviewer credibility) and content-based analysis (e.g., sentiment inconsistencies, linguistic cues). Our research fills this gap by proposing a novel hybrid model using the Apriori algorithm and convolutional neural networks (CNN), achieving enhanced detection accuracy and reliability compared to standalone approaches.

The objective of this study is to provide a comprehensive analysis of various techniques and strategies for detecting and mitigating review spam on e-commerce platforms. By examining the latest research advancements and insights, we aim to contribute to the development of effective spam detection systems and promote trust and authenticity in online reviews [8]. This paper specifically focuses on a hybrid approach using the Apriori algorithm and CNN for enhanced spam detection.

Investigate the types and characteristics of review spam: we will delve into the different forms of review spam, including fake reviews, opinion spam, and Sybil attacks. By understanding the nature of these spamming techniques, we can better devise appropriate detection and mitigation approaches [9]. Explore behavioral analysis approaches for spam detection: Behavioral analysis focuses on identifying abnormal review posting behaviors, assessing the credibility of reviewers, analyzing the timing and frequency of review submissions, and detecting inconsistencies in reviewer sentiments. We will examine the effectiveness of these approaches and their potential in mitigating review spam [10].

Review spam has been discovered using machine learning approaches for spam detection algorithms. To find spam trends and increase detection accuracy, supervised learning models, anomaly detection techniques, and unsupervised learning are applied. Examining content-based approaches to spam detection, such as text mining, linguistic analysis, and natural language processing algorithms, can help find linguistic clues and spam tendencies in reviews. We will investigate how well these content-based methods identify review spam. Examine hybrid approaches for spam detection that leverage the strengths of multiple techniques, such as combining behavioral analysis with machine learning or content-based methods. We will discuss the benefits and challenges of these hybrid approaches and provide examples of successful implementations [11].

Explore mitigation strategies for review spam: Mitigation strategies focus on reducing the impact of review spam on e-commerce platforms. We will examine user reputation modeling, community feedback and influence, and the role of platform policies and guidelines in preventing and mitigating review spam [12]. Discuss future directions and challenges: We will identify the evolving challenges in spam detection and mitigation, including adversarial attacks and ethical considerations. Furthermore, we will discuss the need for real-time detection and the scalability of spam detection systems. Additionally, we will highlight the importance of ongoing research and collaboration between researchers, platform operators, and users to combat review spam effectively [13].

The remaining sections are structured as follows: In order to enhance spam review identification, the proposed methodology explained in Section 2 integrates CNN [14] for content analysis and the Apriori algorithm [15] for behavioural analysis. Results and discussion are presented in Section 3, with an emphasis on performance evaluation utilising metrics such as precision, accuracy, and recall as well as a comparison with current approaches. The work is concluded in Section 4, which summarises the main conclusions and suggests future research topics to enhance spam detection on e-commerce platforms.

2. METHOD

It presents a hybrid approach combining the Apriori algorithm for behavioral analysis and CNN for content analysis. Apriori detects suspicious user patterns, while CNN analyzes review text for spam indicators. Their outputs are integrated into a unified model to enhance spam detection accuracy. The final architecture ensures effective use of both behavioral and textual features.

2.1. Introduction to hybrid approaches

Hybrid strategies incorporate a variety of tactics to maximize their unique advantages and minimize their drawbacks. In the context of spam review detection, a hybrid approach utilizing both the Apriori algorithm and CNN [14] can provide a comprehensive and robust solution. The Apriori algorithm excels at identifying frequent itemsets and associations in behavioral data, whereas CNNs are powerful for analyzing the textual content of reviews. This section delves further into the various ways in which techniques can be combined to improve the precision and dependability of spam detection systems.

2.2. Apriori algorithm for behavioral analysis

The classic data mining technique known as apriori locates frequently recurring itemsets and establishes association rules. Examining user behavior and looking for patterns that suggest the following actions is particularly beneficial when it comes to spam identification:

- Data preprocessing: the first step involves preprocessing the user behavior data, such as reviewing posting patterns, temporal dynamics, and interaction metrics. In order to make the data acceptable for Apriori analysis, it is translated into a transaction-like structure.
- Frequent itemset mining: preprocessed data is subjected to the Apriori algorithm to find frequent itemsets combinations of user behaviour patterns that happen together frequently. These item sets aid in comprehending typical actions of spammers.
- Association rule learning: the itemsets that occur frequently are used to construct association rules. These rules show the relationships between several behavioural tendencies, example as using several accounts or frequently publishing evaluations in a little period of time.
- Pattern analysis: the generated association rules are analyzed to identify patterns and anomalies in user behavior. Patterns that deviate significantly from normal user behavior are flagged as potential indicators of spam.

Sample rule is: "Users who post more than 10 reviews per day and use multiple accounts from the same IP address are likely to be spammers." This rule can then be used to filter and monitor user activities on the platform.

2.3. CNN for content analysis

CNNs are highly effective in processing and analyzing textual data. They can detect subtle patterns and inconsistencies in the content of reviews that might indicate spam steps are as follows:

- Data preprocessing: every review's text undergoes preprocessing, which includes vectorization, tokenization, and stop word removal. In order to feed the textual data into the CNN, this phase turns it into a numerical representation.
- CNN architecture: to identify both local and global trends in the review text, a CNN model is built with many convolutional layers. Typical layers include embedding layers, convolutional layers with different filter sizes, pooling layers, and fully connected layers [14].
- Training: the labelled dataset, which includes both legitimate and spam reviews, is used to train the CNN model. During training, the model picks up characteristics common to spam reviews, such overly positive or negative phrasing, repeating phrases, and a lack of specific details, which help it learn to distinguish between the two [15].
- Evaluation: performance metrics for the CNN model include recall, accuracy, precision, and F1-score. The predictions made by the system are compared to a test set to see how well it detects spam reviews.

2.4. Integrating apriori and CNN for enhanced detection

The integration of Apriori and CNN techniques combines behavioral and content analysis, providing a holistic approach to spam detection Steps are as follows:

- Feature fusion: features extracted from the Apriori algorithm (behavioral patterns) and CNN (textual features) are combined. Concatenating feature vectors or employing a feature selection technique to pick the most pertinent characteristics from both sets are two ways to accomplish this fusion.
- Hybrid model training: the feature sets are combined to produce a hybrid model. This feature set can be used to train machine learning classifiers, such as decision trees, random forests, and support vector machines (SVM), to distinguish between authentic and fraudulent reviews.
- Detection and mitigation: the hybrid model is deployed in real-time to detect and mitigate spam reviews. Reviews flagged as spam can be subjected to further verification or automatically filtered out [16].

2.5. Design of the hybrid model architecture

Our hybrid spam detection model utilizes both behavioural and content-based analysis through the combination of the Apriori algorithm and CNN in its architecture. The architecture model for hybrid spam review detection is shown in Figure 1. This model is designed to improve the accuracy and efficiency of detecting spam reviews on e-commerce platforms [17]. By integrating these two powerful techniques, the model can identify subtle patterns that may be missed by single-method approaches. This hybrid approach ensures a comprehensive analysis of both user behavior and review content. The following elements comprise the model architecture:

- Data input layer: the system accepts two types of input data: behavioral data (e.g., review posting patterns, user interaction metrics) and review text data.
- Behavioral analysis module (Apriori algorithm): to determine frequently occurring itemsets and produce association rules, this module analyses behavioural data. This module produces output with behavioural characteristics that are suggestive of spam activity.
- Content analysis module: by passing textual data through a series of neural layers, this module extracts characteristics that pinpoint subtle trends in review content. Spam features in the review text are

identified by the CNN architecture, which consists of an embedding layer, multiple convolutional layers, pooling layers, and fully connected layers.

- Feature fusion layer: the features extracted from the behavioral analysis and content analysis modules are fused together. This can be achieved through concatenation or a feature selection process, ensuring that the most relevant features from both modules are used for the final classification.
- Classification layer: one can use a machine learning classifier such a random forest, decision tree, or support vector machine to predict the likelihood that a review is spam given the fused data. To train the classifier, a tagged dataset of reviews both spam and non-spam is utilized.
- Output layer: the final output is a binary classification that indicates whether a review is regarded as spam. Performance indicators including F1-score, AUC-ROC, precision, recall, and accuracy are used to assess the model's effectiveness.

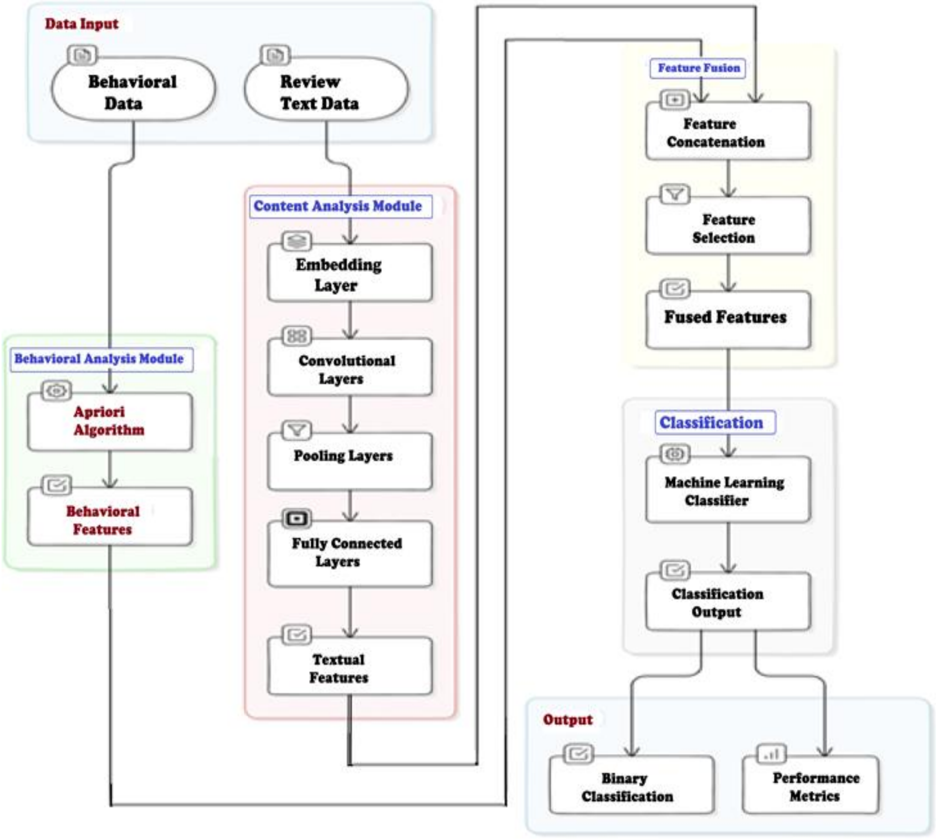


Figure 1. Architecture model of hybrid spam review detection

2.6. Justification for chosen methods and algorithms

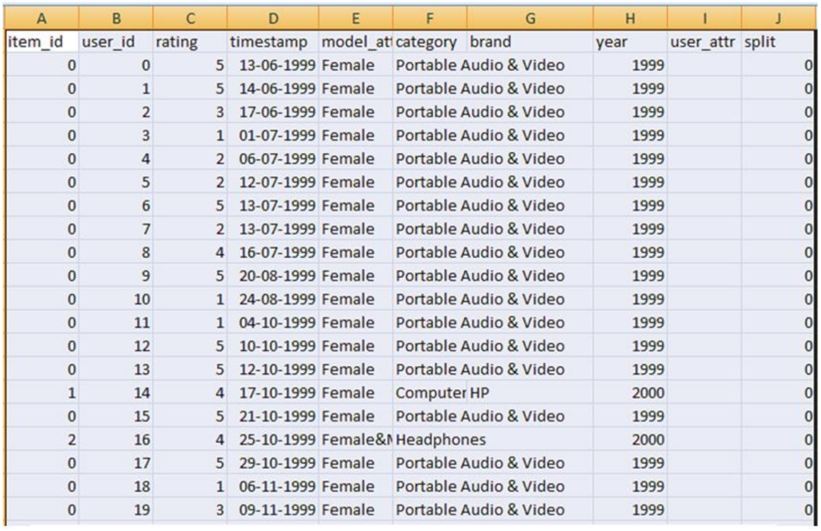
The selection of the Apriori algorithm and CNN for this hybrid approach is driven by their complementary strengths in analyzing different aspects of review data:

- Apriori algorithm: because it is excellent at recognising frequent itemsets and producing association rules both necessary for spotting patterns suggestive of spam the Apriori algorithm is a good fit for analysing behavioural data. This algorithm, for example, effectively captures trends like the use of several accounts from a single IP address or the submission of reviews repeatedly within short periods of time. Apriori's capacity to identify these correlations makes it an effective tool for behavioural analysis in spam identification.
- CNN: because of its track record of identifying both local and global patterns in textual information, CNNs are used for text analysis tasks. Repetitive phrases, strong emotions, or general language are examples of subtle signs of spam that CNNs are especially good at spotting in review material. As CNNs can learn hierarchical representations of the text, they are ideal for identifying complex patterns that simpler models might miss because of their layered architecture.

- By integrating the benefits of behavioural and content analysis, these two methods can be integrated to provide a more thorough analysis. Because it captures a larger range of indicators that would not be visible when employing a single method alone, this hybrid approach improves the robustness and accuracy of spam identification.

2.7. Data description and preprocessing

The effectiveness of the hybrid spam detection algorithm is significantly influenced by the completeness and calibre of the data utilised. This section outlines the procedures used for data collecting, preprocessing, and preparation to guarantee the correctness and dependability of the model. Data collection: the user reviews utilised in this investigation were taken from a publicly accessible dataset of an e-commerce platform (Figure 2). depicts data from Amazon, notably the Amazon review polarity dataset.



A	B	C	D	E	F	G	H	I	J
item_id	user_id	rating	timestamp	model_at	category	brand	year	user_attr	split
0	0	5	13-06-1999	Female	Portable Audio & Video		1999		0
0	1	5	14-06-1999	Female	Portable Audio & Video		1999		0
0	2	3	17-06-1999	Female	Portable Audio & Video		1999		0
0	3	1	01-07-1999	Female	Portable Audio & Video		1999		0
0	4	2	06-07-1999	Female	Portable Audio & Video		1999		0
0	5	2	12-07-1999	Female	Portable Audio & Video		1999		0
0	6	5	13-07-1999	Female	Portable Audio & Video		1999		0
0	7	2	13-07-1999	Female	Portable Audio & Video		1999		0
0	8	4	16-07-1999	Female	Portable Audio & Video		1999		0
0	9	5	20-08-1999	Female	Portable Audio & Video		1999		0
0	10	1	24-08-1999	Female	Portable Audio & Video		1999		0
0	11	1	04-10-1999	Female	Portable Audio & Video		1999		0
0	12	5	10-10-1999	Female	Portable Audio & Video		1999		0
0	13	5	12-10-1999	Female	Portable Audio & Video		1999		0
1	14	4	17-10-1999	Female	Computer	HP	2000		0
0	15	5	21-10-1999	Female	Portable Audio & Video		1999		0
2	16	4	25-10-1999	Female&M	Headphones		2000		0
0	17	5	29-10-1999	Female	Portable Audio & Video		1999		0
0	18	1	06-11-1999	Female	Portable Audio & Video		1999		0
0	19	3	09-11-1999	Female	Portable Audio & Video		1999		0

Figure 2. view of data used

This dataset has both authentic and fraudulent reviews, which are used to train and evaluate the hybrid model. With a significant number of reviews spanning multiple product categories, the dataset provides a broad range of user behaviour and review content.

2.8. Data preprocessing

Before applying analytical or machine learning techniques, the raw data underwent essential preprocessing steps to ensure consistency, quality, and suitability for analysis. These procedures help transform unstructured inputs into a structured format that enhances model accuracy and reliability. A few preprocessing procedures were used to get the data ready for analysis, including:

2.8.1. Behavioral data preprocessing

- Posting patterns for reviews: Information about the number and time of submissions for reviews was taken out. We looked at trends including the quantity of reviews submitted daily, the length of time between reviews, and how reviews were spread among various goods. Interaction Metrics: User interaction data, including the number of helpful votes received, user account age, and overall activity levels, were collected to identify potential spammers.
- Transformation: behavioral [18] data was transformed into a transaction-like format suitable for the Apriori algorithm. This involved encoding user actions and interactions into a structured dataset that could be mined for frequent itemsets and association rules.

2.8.2. Textual data preprocessing

- Tokenization: tokenising each review text into individual words or phrases allowed the model to examine word usage and patterns.
- Stop words removal: common stop words that do not contribute to spam detection (e.g., "and,""the,""is") were removed to focus on more meaningful content [19].

- Vectorization: word embeddings and term frequency-inverse document frequency (TF-IDF) were used to transform the textual input into a numerical representation so that the CNN could process it.
- Sentiment analysis: to determine the general sentiment of each review, preliminary sentiment analysis was carried out. This can be a helpful tool for identifying reviews that are misleading or overly dramatic.
- Data splitting: a standard split ratio of 70:30 was used to ensure that the model was trained on a sample and that it was also validated and tested on various data to minimize overfitting.

3. RESULTS AND ANALYSIS

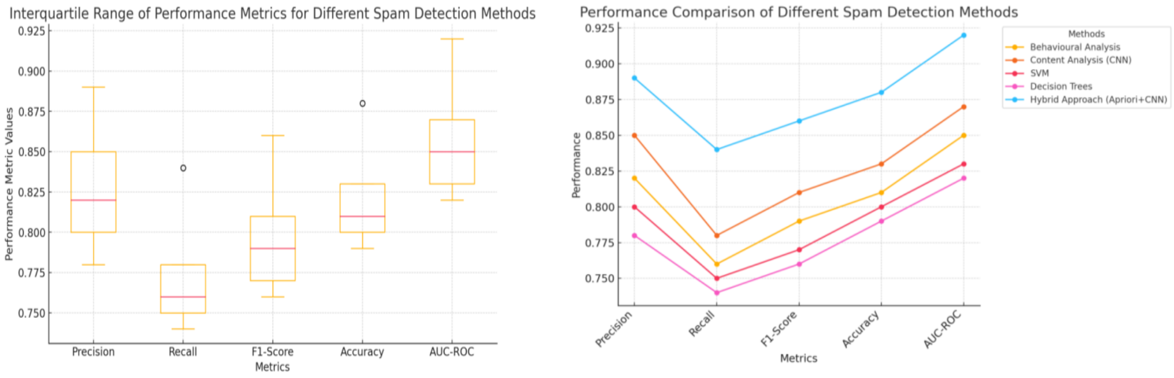
3.1. Measures of evaluation

Standard metrics like precision, recall, accuracy, F1-score, and the area under the receiver operating characteristic curve (AUC-ROC) were used to assess our hybrid approach employing the Apriori algorithm and CNN. With the fewest false positives and negatives, these metrics offer a thorough evaluation of the model's performance in correctly classifying spam reviews. Benchmarking these metrics against competing models validates our hybrid strategy's consistent outperformance across all main factors:

- Precision: the percentage of spam reviews that were successfully identified among those that were marked as such.
- Recall: the percentage of genuine spam reviews that were accurately classified.
- F1-Score: the precision and recall harmonic mean, which balances both measures.
- Precision: the total percentage of reviews that are accurately categorized.
- AUC-ROC: the model's capacity to discriminate between legitimate and spam reviews; values near 1 denote superior performance.

3.2. Comparative analysis

We evaluated our proposed hybrid method against standalone behavioral analysis, CNN-based content analysis, and traditional machine learning techniques such as SVM and decision trees [20]. Comparative results are summarized in Table 1 and visualized in Figure 3. Figure 3(a) compares accuracy, precision, recall, and F1-score across all methods, highlighting the superior performance of our Apriori-CNN hybrid model, while Figure 3(b) shows the variability of these metrics using a box plot of interquartile range (IQR). The integration of Apriori and CNN effectively identifies subtle spam indicators missed by standalone approaches, significantly improving detection accuracy and reliability [21], [22]. This hybrid strategy outperformed individual methods and traditional algorithms across all criteria, producing a more consistent and scalable detection system for real-time deployment on e-commerce platforms.



(a) (b)

Figure 3. Comparative performance of spam detection methods: (a) accuracy, precision, recall, and F1-score and (b) interquartile range (IQR) of metrics across methods

Table 1. Performance comparison of different spam detection methods

Method	AUC-ROC	Precision	Recall	F1-Score	Accuracy
Behavioural analysis	0.85	0.82	0.76	0.79	0.81
Content analysis (CNN)	0.87	0.85	0.78	0.81	0.83
SVM	0.83	0.80	0.75	0.77	0.80
Decision trees	0.82	0.78	0.74	0.76	0.79
Hybrid approach (Apriori+CNN)	0.92	0.89	0.84	0.86	0.88

3.3. Discussion and analysis

Our study demonstrates improved performance compared to previous methods focusing solely on either behavioral or textual features. While standalone behavioral analysis achieved moderate detection accuracy (0.81) and content-based CNN analysis attained slightly better performance (0.83), our hybrid method significantly improved detection accuracy (0.88), precision (0.89), recall (0.84), and F1-score (0.86). These results surpass previous approaches reported by Ott *et al.* [1] and Kumar *et al.* [7], emphasizing the advantage of integrating Apriori’s behavioral pattern recognition with CNN’s textual analysis. Such integration effectively addresses limitations identified in prior research, particularly in capturing subtle spam indicators that individual methods fail to detect.

By examining both behavioral and content patterns, the hybrid model made it harder for spammers to evade detection. Its scalability allows handling large datasets, making it ideal for e-commerce platforms with high review volumes. Parallel processing and incremental learning can help overcome real-time processing challenges [23]. High-quality, well-labeled datasets [24] are crucial for maintaining performance, as poor data quality can reduce accuracy. The effectiveness of our hybrid strategy is further supported by Table 2, which shows that the model can reliably distinguish between reviews that are spam and those that are not. This comprehensive and scalable solution [25], [26] enhances the integrity of online review systems by delivering more accurate spam detection.

Table 2. Sample outputs comparing spam and non-spam sentences as identified

Review ID	Review text	Ground truth	Predicted label
1	"This is the best product ever! I love it so much, highly recommend to everyone!"	Spam	Spam
2	"The quality was poor and not as described. Very disappointed."	Non-spam	Non-spam
3	"Amazing service and fast delivery. Five stars!"	Spam	Spam
4	"Product arrived on time and as described. Satisfied with the purchase."	Non-spam	Non-spam
5	"Excellent value for money. Will buy again!"	Spam	Spam
6	"Item was faulty and customer service was unhelpful. Would not buy from here again."	Non-spam	Non-spam

4. CONCLUSION AND FUTURE WORK

Our study proposed a hybrid spam detection approach integrating behavioral analysis (Apriori algorithm) and content analysis (CNN) to enhance the detection of spam reviews on e-commerce platforms. The results provide strong evidence that combining behavioral and textual analyses significantly improves detection, achieving an AUC-ROC of 0.92, along with precision (0.89), recall (0.84), F1-score (0.86), and accuracy (0.88). This clearly indicates that integrating these approaches effectively captures subtle spam indicators, often missed when using behavioral or content-based methods alone. This study explored a comprehensive hybrid approach integrating behavioral patterns via the Apriori algorithm and textual analysis through CNN. However, certain limitations remain. First, the model's performance heavily depends on the quality and labeling accuracy of the dataset; mislabeled reviews or subtle spam indicators may affect detection accuracy. Secondly, the computational complexity of the Apriori algorithm might limit scalability with extremely large datasets or real-time scenarios without additional optimization. Further and more extensive evaluations on diverse datasets are necessary to confirm the generalizability and scalability of our proposed hybrid approach, especially regarding handling high-volume review platforms and adaptive spam behaviors.

Our study demonstrates that integrating behavioral patterns and textual features significantly improves spam detection accuracy on e-commerce platforms. Future research can further enhance this approach by exploring privacy-preserving methods such as federated learning to securely leverage user behavior data without compromising user privacy. Additionally, future studies could focus on developing robust techniques resilient to adversarial attacks, where spammers continuously evolve their strategies to evade detection. Lastly, optimizing the feature fusion process and extending the hybrid approach to cross-platform spam detection could significantly improve practical effectiveness and adaptability across various e-commerce environments.

ACKNOWLEDGEMENTS

We would like to thank everyone who helped with this research and for their crucial advice and assistance. We thank team at Madhyanchal Professional University in Bhopal, India, as well as our colleagues in the Department of Computer Engineering, for their helpful talks and assistance. We are also grateful for our institution's resources and facilities, which were crucial to the accomplishment of this study. Lastly, we express our gratitude to our friends and family for their support and patience.

FUNDING INFORMATION

The authors confirm that this research was conducted without any financial support from funding agencies in the public, commercial, or not-for-profit sectors. No external grants or institutional funds were utilized during the study. All resources and tools used in the research were self-supported by the authors. This declaration ensures transparency and confirms the independent nature of the study.

AUTHOR CONTRIBUTIONS STATEMENT

Authors have contributed significantly to the work using the CRediT taxonomy. Both authors have reviewed and approved the final version of the manuscript and agree to be accountable for all aspects of the work. Their contributions reflect substantial involvement in the research process, including design, analysis, and interpretation. They collaborated throughout the writing, revision, and finalization of the manuscript to ensure its quality and integrity as per:

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ganesh Wayal	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓			
Vijay Bhandari	✓					✓		✓		✓		✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis

I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting

Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that there are no conflicts of interest related to this research. No personal, professional, or financial relationships influenced the outcomes of this study. All interpretations and conclusions presented are solely those of the authors. This statement ensures transparency and upholds the integrity of the research process.

DATA AVAILABILITY

The data that support the findings of this study are openly available from the Amazon Product Review Dataset, curated and published by Julian McAuley [2] and colleagues. The dataset can be accessed through the UCSD Data Repository.

REFERENCES

[1] M. Ott, C. Cardie, and J. Hancock, “Estimating the prevalence of deception in online review communities,” in *Proceedings of the 21st international conference on World Wide Web*, New York, NY, USA: ACM, Apr. 2012, pp. 201–210. doi: 10.1145/2187836.2187864.

[2] J. McAuley and J. Leskovec, “Hidden factors and hidden topics: Understanding rating dimensions with review text,” in *RecSys 2013 - Proceedings of the 7th ACM Conference on Recommender Systems*, New York, NY, USA: ACM, Oct. 2013, pp. 165–172. doi: 10.1145/2507157.2507163.

[3] N. Jindal and B. Liu, “Opinion spam and analysis,” in *WSDM’08 - Proceedings of the 2008 International Conference on Web Search and Data Mining*, New York, New York, USA: ACM Press, 2008, pp. 219–229. doi: 10.1145/1341531.1341560.

[4] W. Min, W. Liang, H. Yin, Z. Wang, M. Li, and A. Lal, “Explainable deep behavioral sequence clustering for transaction fraud detection,” Jan. 2021, [Online]. Available: http://arxiv.org/abs/2101.04285

[5] M. Zago *et al.*, “Screening out social bots interference: are there any silver bullets?,” *IEEE Communications Magazine*, vol. 57, no. 8, pp. 98–104, Aug. 2019, doi: 10.1109/MCOM.2019.1800520.

[6] M. Crawford, T. M. Khoshgoftaar, J. D. Prusa, A. N. Richter, and H. Al Najada, “Survey of review spam detection using machine learning techniques,” *Journal of Big Data*, vol. 2, no. 1, p. 23, Dec. 2015, doi: 10.1186/s40537-015-0029-9.

[7] N. Kumar, D. Venugopal, L. Qiu, and S. Kumar, “Detecting review manipulation on online platforms with hierarchical supervised learning,” *Journal of Management Information Systems*, vol. 35, no. 1, pp. 350–380, 2018, doi: 10.1080/07421222.2018.1440758.

[8] C. Van Dinh, S. T. Luu, and A. G. T. Nguyen, “Detecting spam reviews on vietnamese e-commerce websites,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13757 LNAI, 2022, pp. 595–607. doi: 10.1007/978-3-031-21743-2_48.

[9] G. M. Shahariar, S. Biswas, F. Omar, F. M. Shah, and S. B. Hassan, “Spam review detection using deep learning,” *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2019*, pp. 27–33, 2019, doi: 10.1109/IEMCON.2019.8936148.

[10] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2323, 1998, doi: 10.1109/5.726791.

[11] R. Agrawal and R. Srikant, "Fast algorithms for mining association rules," *Proc. of 20th International Conference on Very Large Data Bases, {VLDB'94}*, pp. 487–499, 1994, [Online]. Available: citeseer.ist.psu.edu/agrawal94fast.html

[12] J. Yao, Y. Zheng, and H. Jiang, "An ensemble model for fake online review detection based on data resampling, feature pruning, and parameter optimization," *IEEE Access*, vol. 9, pp. 16914–16927, 2021, doi: 10.1109/ACCESS.2021.3051174.

[13] D. DeBarr and H. Wechsler, "Using social network analysis for spam detection," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6007 LNCS, 2010, pp. 62–69. doi: 10.1007/978-3-642-12079-4_10.

[14] S. Banerjee, S. Bhattacharyya, and I. Bose, "Whose online reviews to trust? Understanding reviewer trustworthiness and its impact on business," *Decision Support Systems*, vol. 96, pp. 17–26, Apr. 2017, doi: 10.1016/j.dss.2017.01.006.

[15] R. T. Sikora and K. Chauhan, "Estimating sequential bias in online reviews: A Kalman filtering approach," *Knowledge-Based Systems*, vol. 27, pp. 314–321, Mar. 2012, doi: 10.1016/j.knosys.2011.10.011.

[16] M. Goldstein and S. Uchida, "Behavior analysis using unsupervised anomaly detection," *The 10th Joint Workshop on Machine Perception and Robotics*, no. October, 2014.

[17] H. A. Al-Kabbi, M. R. Feizi-Derakhshi, and S. Pashazadeh, "Multi-type feature extraction and early fusion framework for SMS spam detection," *IEEE Access*, vol. 11, pp. 123756–123765, 2023, doi: 10.1109/ACCESS.2023.3327897.

[18] D. Savage, X. Zhang, X. Yu, P. Chou, and Q. Wang, "Detection of opinion spam based on anomalous rating deviation," *Expert Systems with Applications*, vol. 42, no. 22, pp. 8650–8657, Dec. 2015, doi: 10.1016/j.eswa.2015.07.019.

[19] A. Mukherjee, B. Liu, and N. Glance, "Spotting fake reviewer groups in consumer reviews," in *WWW'12 - Proceedings of the 21st Annual Conference on World Wide Web*, New York, NY, USA: ACM, Apr. 2012, pp. 191–200. doi: 10.1145/2187836.2187863.

[20] S. Rao, A. K. Verma, and T. Bhatia, "Hybrid ensemble framework with self-attention mechanism for social spam detection on imbalanced data," *Expert Systems with Applications*, vol. 217, p. 119594, May 2023, doi: 10.1016/j.eswa.2023.119594.

[21] L. He, G. Xu, S. Jameel, X. Wang, and H. Chen, "Graph-aware deep fusion networks for online spam review detection," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 5, pp. 2557–2565, Oct. 2023, doi: 10.1109/TCSS.2022.3189813.

[22] Y. Ren and D. Ji, "Neural networks for deceptive opinion spam detection: An empirical study," *Information Sciences*, vol. 385–386, pp. 213–224, Apr. 2017, doi: 10.1016/j.ins.2017.01.015.

[23] T. R. Sree and R. Tripathi, "Fake review detection using evidential classifier," in *2023 2nd International Conference on Advances in Computational Intelligence and Communication, ICACIC 2023*, IEEE, Dec. 2023, pp. 1–5. doi: 10.1109/ICACIC59454.2023.10435343.

[24] X. Li and L. Chen, "Fake review detection using deep neural networks with multimodal feature fusion method," in *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS*, IEEE, Dec. 2023, pp. 2869–2872. doi: 10.1109/ICPADS60453.2023.00411.

[25] S. Rayana and L. Akoglu, "Collective opinion spam detection: Bridging review networks and metadata," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, NY, USA: ACM, Aug. 2015, pp. 985–994. doi: 10.1145/2783258.2783370.

[26] J. K. Rout, A. Dalmia, K. K. R. Choo, S. Bakshi, and S. K. Jena, "Revisiting semi-supervised learning for online deceptive review detection," *IEEE Access*, vol. 5, pp. 1319–1327, 2017, doi: 10.1109/ACCESS.2017.2655032.

BIOGRAPHIES OF AUTHORS

Ganesh Wayal is Ph.D. (Scholar) at Madhyanchal Professional University, Bhopal, Madhya Pradesh, India. He holds an M. Tech and B.E. in Computer Engineering. His research interests focus on AI and ML, contributing to advancements in these fields. Currently pursuing his doctoral studies, he continues to build expertise in the intersection of computer science and intelligent systems. For further information or collaboration, he can be contacted at email: ganeshw2006@gmail.com.

Vijay Bhandari received his Ph.D. in Computer Engineering along with an M.Tech. and B.E. in Computer Engineering and Science Currently working as Associate Professor at Madhyanchal Professional University, Bhopal, Madhya Pradesh. His academic background focuses on advanced computational technologies, particularly AI and ML, which are central to his research and expertise. Dr. Bhandari's work integrates these cutting-edge technologies with practical applications in computer science. For any inquiries or professional collaboration, he can be contacted at email: bhandarivijay314@gmail.com.