

Detecting and Characterizing Extremist Reviewer Groups in Online Product Reviews

Viresh Gupta¹, Aayush Aggarwal¹, and Tanmoy Chakraborty¹, *Member, IEEE*

Abstract—Online marketplaces often witness opinion spam in the form of reviews. People are often hired to target specific brands for promoting or impeding them by writing highly positive or negative reviews. This often is done collectively in groups. Although some previous studies attempted to identify and analyze such opinion spam groups, little has been explored to spot those groups who target a brand as a whole, instead of just products. In this article, we collected the reviews from the Amazon product review site and manually labeled a set of 923 candidate reviewer groups. The groups are extracted using frequent itemset mining over brand similarities such that users are clustered together if they have mutually reviewed (products of) a lot of brands. We hypothesize that the nature of the reviewer groups is dependent on eight features specific to a (group, brand) pair. We develop a feature-based supervised model to classify candidate groups as extremist entities. We run multiple classifiers for the task of classifying a group based on the reviews written by the users of that group to determine whether the group shows signs of extremity. A three-layer perceptron-based classifier turns out to be the best classifier. We further study behaviors of such groups in detail to understand the dynamics of brand-level opinion fraud better. These behaviors include consistency in ratings, review sentiment, verified purchase, review dates, and helpful votes received on reviews. Surprisingly, we observe that there are a lot of verified reviewers showing extreme sentiment, which, on further investigation, leads to ways to circumvent the existing mechanisms in place to prevent unofficial incentives on Amazon.

Index Terms—Behaviour, electronic commerce, machine intelligence, machine learning, reviews, social computing, web mining.

I. INTRODUCTION

IN TODAY'S world dominated by online marketplaces, review portals and websites play a crucial role in the buyer's decision for their next purchase.

"It is a virtuous cycle—the more reviews, the more buys. The more buys, the more reviews. The more buys, the higher your rank in search and the more sales you get," says Alice [1], the owner of online cosmetic brand Elizabeth Mott.

Undoubtedly, it is highly likely that some people write reviews that are less than truthful to manipulate widespread decision of buyers in their favor. These people act either individually or in groups. While individual reviewers write such

reviews in a matter of frustration or joy, they do not influence the overall opinion on a product to a large extent but help other buyers by stating their experiences. However, a more compelling case is when multiple individuals form an intricate web, and due to sheer higher number of people reviewing (and certain other techniques, discussed in Section VIII), they end up being a major influence on the overall sentiment of the product. The extent of such influence is not just limited to the reviews by opinion spam. Previous work [2] has shown that 10%–15% reviews are essentially echoing the earliest reviews, and thus, a misleading early review has an even higher influential potential.

This is widespread opinion spam, and every review website must be aware of this activity and take appropriate measures for the identification and/or prevention of this phenomenon. This is a classic example of collective fraud behavior, where several users are part of a business network and work together to target and influence a particular product. This is a lesser known phenomenon, and most groups work following certain techniques to not make their collaboration obvious. However, since such groups are economically or otherwise incentivized, and several of these are generally run by a given organization, they have several targets for opinion spam, which often share certain common characteristics in their nature of reviews. These characteristics can be exploited to classify them better using a robust and thorough analysis technique. Amazon India, to prevent opinion spam, has brought about a new policy that limits the number of reviews on a product in a day, as stated in [3].

In order to still be effective, we claim that certain groups target brands in general and postextreme reviews across multiple products for a given target brand. This is a higher level of opinion spamming, deliberately writing highly positive or negative reviews for a brand in general in order to promote or demote them in the cut-throat competition of the online marketplace. Studies have been conducted to identify such groups that try to influence a product [4]–[6]; however, groups exhibiting a brand-based opinion spamming is a phenomenon that remains widely unexplored. A detailed discussion is required for these brand-related activities because these practices are against the code of conduct of these review websites since they negatively skew the brand-based competition, giving innate (dis)advantages to certain brands.

Since only the nonverified reviews are limited by the policies,¹ reviewers from these groups can often purchase the

















Manuscript received November 9, 2019; revised February 26, 2020; accepted April 7, 2020. This work was supported in part by Ramanujan Faculty Fellowship (SERB), and Early Career Award under Grant ECR/2017/001691, and in part by the Infosys Centre of AI, IIIT-Delhi, India. (Corresponding author: Viresh Gupta.)

The authors are with the Department of Computer Science and Engineering, IIIT-Delhi, New Delhi 110020, India (e-mail: viresh16118@iiitd.ac.in; aayush16002@iiitd.ac.in; tanmoy@iiitd.ac.in).

This article has supplementary downloadable material available at <http://ieeexplore.ieee.org>, provided by the authors.

Digital Object Identifier 10.1109/TCSS.2020.2988098

¹<https://www.amazon.in/gp/help/customer/display.html?nodeId=201930110>

 <p>★★★★★ Five Stars 30th March 2018 Flavour Name : Chocolate Size: 1 Kg / 2.2 lb Verified Purchase This is amazing product</p> <p>Product Name: MuscleBlaze Mass Gainer XXL - 1 kg (Chocolate)</p>	 <p>★★★★★ Five Stars 30th March 2018 Flavour Name : Chocolate Size: 1 Kg / 2.2 lb Verified Purchase I like this product. Really good</p> <p>Product Name: MuscleBlaze Mass Gainer XXL - 1 kg (Chocolate)</p>	 <p>★★★★★ Five Stars 30th March 2018 Flavour Name : Chocolate Size: 1 Kg / 2.2 lb Verified Purchase Good quality product worth for money</p> <p>Product Name: MuscleBlaze Mass Gainer XXL - 1 kg (Chocolate)</p>	 <p>★★★★★ Five Stars 30th March 2018 Flavour Name : Chocolate Size: 1 Kg / 2.2 lb Verified Purchase Good quality product worth for money</p> <p>Product Name: MuscleBlaze Mass Gainer XXL - 1 kg (Chocolate)</p>
 <p>★★★★★ Five Stars 31st March 2018 Verified Purchase Good quality product. Affordable And best deal</p> <p>Product Name: PES 3D Premium Edge to Edge Full Glue , No Rainbow , Full Front Body Cover Tempered Full Glass Screen Protector Guard for OnePlus 5T - Pure Black</p>	 <p>★★★★★ Five Stars 31st March 2018 Verified Purchase Good quality product. Worth for money</p> <p>Product Name: PES 3D Premium Edge to Edge Full Glue , No Rainbow , Full Front Body Cover Tempered Full Glass Screen Protector Guard for OnePlus 5T - Pure Black</p>	 <p>★★★★★ Five Stars 30th March 2018 Verified Purchase Nice product. Full protection</p> <p>Product Name: PES 3D Premium Edge to Edge Full Glue , No Rainbow , Full Front Body Cover Tempered Full Glass Screen Protector Guard for OnePlus 5T - Pure Black</p>	 <p>★★★★★ Five Stars 31st March 2018 Verified Purchase Full protection with affordable price</p> <p>Product Name: PES 3D Premium Edge to Edge Full Glue , No Rainbow , Full Front Body Cover Tempered Full Glass Screen Protector Guard for OnePlus 5T - Pure Black</p>
 <p>★★★★★ Great product. Affordable 30th March 2018 Verified Purchase Great product. Affordable and original</p> <p>One person found this helpful</p> <p>Product Name: Noor Secrets Hair Fall Control & Hair Growth Oil, 100ml</p>	 <p>★★★★★ This is a great deal. I love this product awesome quality 30th March 2018 Verified Purchase This is a great deal. I love this product awesome quality</p> <p>Product Name: Noor Secrets Hair Fall Control & Hair Growth Oil, 100ml</p>	 <p>★★★★★ Five Stars 30th March 2018 Verified Purchase Good quality product worth for money.</p> <p>One person found this helpful</p> <p>Product Name: Noor Secrets Hair Fall Control & Hair Growth Oil, 100ml</p>	 <p>★★★★★ Five Stars 30th March 2018 Verified Purchase Good product. I recommend this to everyone</p> <p>Product Name: Noor Secrets Hair Fall Control & Hair Growth Oil, 100ml</p>
 <p>★★★★★ The product is really good. Its taste and effects are also fabulous and ... and original 3rd April 2018 Verified Purchase The product is really good. Its taste and effects are also fabulous and it doesn't contain any harmful substance. My gym trainer recommend Natuzy product to me. Many gyms provide this bcaa to their gym because of their results. finally it comes on amazon after much time and the price which they giving is amazing</p> <p>One person found this helpful</p> <p>Product Name: Natuzy Instantized BCAA Energy Blast with 7000 BCAA, Glutamine, Citrulline & Beta Alanine (Blueberry Mojito Flavor) - 450Gms</p>	 <p>★★★★★ Amazing Product, mostly other bcaa brands have 5000 or ... 3rd April 2018 Verified Purchase Amazing Product, mostly other bcaa brands have 5000 or 6000 mg of bcaa but natuzy have given amazingly 7000 BCAA and also the ratio is too good as scientifically proven 2:1:1. I just love the product the result shows itself. I surely recommend this to others.</p> <p>2 people found this helpful</p> <p>Product Name: Natuzy Instantized BCAA Energy Blast with 7000 BCAA, Glutamine, Citrulline & Beta Alanine (Blueberry Mojito Flavor) - 450Gms</p>	 <p>★★★★★ Five Stars 30th March 2018 Verified Purchase After trying a few brands before this, I can say Natuzy BCAA is the best bcaa I have tried. The price they are giving its value for money. Taste is also good, the powder doesn't dissolve immediately which shows the BCAA is genuine and also get free shaker that is also good overall 5 star to this product</p> <p>3 people found this helpful</p> <p>Product Name: Natuzy Instantized BCAA Energy Blast with 7000 BCAA, Glutamine, Citrulline & Beta Alanine (Blueberry Mojito Flavor) - 450Gms</p>	 <p>★★★★★ The taste is fine. The product is also good 3rd April 2018 Verified Purchase It's high quality BCAA. The taste is fine. The product is also good. Good if u want to gain and maintain lean muscle mass. For best results take 15 grams or 2 Scoops. Its also good thing guys we are getting shaker with every pack.</p> <p>Product Name: Natuzy Instantized BCAA Energy Blast with 7000 BCAA, Glutamine, Citrulline & Beta Alanine (Blueberry Mojito Flavor) - 450Gms</p>

(a)

(b)

(c)

(d)

Fig. 1. Sample extremist group. The reviews are all positive for different brands and also have a verified purchase sign with all of them done on nearly the same dates. For example, in the first row, all reviewers have reviewed the product on the same date and have given a five-star rating with the review text having extremely similar content. (a) User 1. (b) User 2. (c) User 3. (d) User 4.

product via Amazon in exchange for unofficial discounts (e.g., cash backs) and postverified reviews since they did not receive a discount via Amazon's mechanisms (e.g., coupons) (see further discussed in Section VIII).

Fig. 1 shows an example of such extremist groups (taken from our annotated data set as mentioned in Section III). Four rows correspond to the products belonging to four different brands. Four columns represent four different reviewers who, according to our annotation, are part of the same group. Each box represents the review information. This is an example of reviewers showing extreme likeliness toward these products/brands as can be seen from the extreme ratings, similar comments, and almost the same date [7]. It is clear that this group of reviewers had extreme sentiments toward the brands reviewed, both in terms of the ratings and the review content. While this has a large overlap with the classic collision in which reviewers target a product to bring up its ratings, this kind of extremism in reviews is not in order to promote/demote the ranking of a product, but rather to influence the perception of people for a brand.

It is worth noting that such a kind of characterization is different from just combining the groups of people who provide extreme reviews on a product, because while the groups focusing on a product may be extreme in their opinion, they do not necessarily intend to influence the brand image. This, coupled with the fact that the same product may be sold by different sellers, reduces the chance that a product-level opinion spamming reviewer group would target products of the same brand. Sellers may not have any inclination toward promoting any particular brand's products; rather, they would prefer to gain a better revenue on all products (may belong to different brands) by their promotional campaigns. Hence, such a group is more likely to have a very narrow and specialized

source, e.g., the competing brands or the manufacturing brand itself. (Additional results of experiments for distinguishing between the product level and the brand level are available in Section IV of the Supplementary Material).

In this article, we identify and study the behavioral characteristics of extremist reviewer groups. We also build a feature-based classifier based on the brand-specific activities of reviewer groups to identify the extremist groups on the Amazon India marketplace. We then further analyze our methodology to unfold behaviors that best signify such activities and compare and analyze the overall trend of these groups viz-a-viz their behaviors.

The major contributions of this article are fourfold:

- 1) a manually labeled data set of 923 reviewer groups that are classified into "extremist" and "moderate" categories;
- 2) the first-ever characterization and study of the novel problem of identifying brand-level extremism;
- 3) detailed characterization of extremist reviewer groups;
- 4) design supervised approach to detect extremist reviewer groups.

To encourage reproducible research, we have made the codes publicly available at <https://github.com/virresh/extremist-reviewers>.²

This article is organized as follows. We briefly survey the various studies related to review extremism, applications developed using reviews, and fake review detection in Section II. Section III outlines the details of the collected data set and annotation methodology. Section IV presents the modeling of features at brand level and features that relate to

²We could not release the original Amazon Data due to the copyright issue. Instead, we have released the scraper to collect the data. We have also released the annotated data and feature values of individual groups.

brand-level extremism in groups along with the experimental setup. Section V briefly discusses the results obtained by various classifiers. Sections VI and VII characterize extremist users based on the features and expert annotation. Section VIII discusses the implications of the study. Finally, we conclude in Section IX.

II. BACKGROUND AND RELATED WORK

We divide the existing literature into two parts: general studies on e-commerce services and detection of fake reviews.

A. General Studies on E-Commerce Reviews

There have been extensive studies on mining online reviews and classifying them based on user sentiment [8]–[11]. Reviews have also been extensively used in developing and augmenting recommendation systems [12]–[15] and extracting product features [16]–[18]. Another study has also shown the utility of product reviews in explaining the recommendations given by a recommendation system [19]. Pang *et al.* [20] showed the progression of reviews as an important part of the decision-making process with the advent of Web 2.0 and studied them from retrieval perspective. Since it is difficult for the buyer to wade through volumes of reviews, researchers have conducted studies on summarizing reviews based on user sentiment [21] and other features [22]–[24] as well under the umbrella of opinion summarization. All these studies indicated that product reviews are an invaluable resource for determining the quality of a product. Various marketing studies have also shown that reviews play an important role in maintaining the online reputation of a brand as well [25], [26].

A review usually consists of a star rating that helps to influence a product's overall ratings, but a review becomes even more impactful when people read it. It has been found that people read a review only when it is perceived as helpful by them, which may be through various means—the helpful upvotes by other consumers, the length of the review, star ratings, readability, and so on. [27], [28]. There have been several efforts to understand what makes a review helpful to people [27], [29], [30]. Based on these results, attempts have been made to construct systems that can recommend reviews to users [31] by predicting the perceived helpfulness of a review. An important point to note is that all these studies emphasize that review extremity is an important factor for assessing the impact made by the reviews.

Extensive work has been done on assessing how review extremity affects users [32]–[34] and the relation between star ratings given by a reviewer and the reviewer's attitude [35]. A moderate review can arise out of indifference or ambivalence [36], [37] and could prove to be useful for buyers seeking in-depth knowledge [32], and an extreme review provides quick validation for experience goods, such as movies and books [33], [34]. It has been observed that moderate reviews can affect “brand attitude” [27]. All the work indicates extremity in reviews on a product level, which affects the brand as a whole. We make an attempt to understand extremity in reviews directly at the brand level and associate it with groups involved in the same.

B. Studies on Fake Reviews

Since reviews are such an impactful resource, it is to be expected that the review space is infested with malpractices as well. There have been various efforts to uncover these practices and understand them in-depth, broadly called opinion spam. These studies can be broadly classified into three categories.

1) *Studies on Reviews*: Jindal and Liu [38] made a pioneering effort to detect fake reviews. They introduced the problem of opinion spam and analyzed online reviews in three varieties—untruthful opinions, seller/brand only reviews (no product involved), and nonreviews using near-duplicate content as an indicator of fake reviews. Other studies dealing with the detection of review-level spam explored linguistic features of text [39], handmade rules [40], and combination of review and reviewer features [41]. A probabilistic framework for the same has also been proposed in [42]. Ott *et al.* [39] synthesized fake hotel reviews using Amazon Mechanical Turk, whereas Jindal and Liu [38] worked on data scraped from Amazon and used content duplicity as ground truth. Both of them worked with features at a review level. Jindal *et al.* [40] and Li *et al.* [41] mentioned the role of brands briefly, but the main focus was on fake reviews rather than extreme reviews.

2) *Studies on Reviewers*: Studies involved in detecting reviewer fraud consider rating behavior [7], [43], trust scores based on a relationship graph among reviewers, reviews, and stores [44]. Other studies [45]–[47] provided various other methods exploiting behavioral footprints to identify fraud reviewers such as bursts of popularity and use Bayesian approaches. Notably, Wang *et al.* [44] introduced the usage of a review graph for identifying such spammers. Mukherjee *et al.* [45] tried to uncover features used by Yelp filters for abnormal behaviors and revealed that reviewers involved in writing fake reviews showed behavioral features and psychological patterns of overuse of top common words. Mukherjee *et al.* [46] and Fei *et al.* [47] employed strategies, such as Bayesian modeling of spamicity as latent behavior and loopy belief propagation on modeled Markov random fields. However, in all the approaches, the indicators for a fake reviewer, especially when characterizing a reviewer by their rating behaviors [43], highly positive or highly negative reviewers were more often a suspect than a moderate rating. This may indicate that extremism in reviews might also be related to opinion spam; however, this front has not been explored yet.

3) *Studies on Reviewer Groups*: The effect of fraud reviewer groups is more detrimental and subtle than individual fraud reviewers. The issue of manual labeling was addressed by considering a group of reviewers instead of individual reviews. Mukherjee *et al.* [4] showed that labeling a group of reviewers is considerably easier than labeling individual reviews. Other interesting studies that leverage metadata to characterize different entities in e-commerce sites can be observed in [5] and [6], where products, reviews, and users are classified simultaneously. Fei *et al.* [47] and Kakhki *et al.* [48] showed that synchronicity is an important group behavior; Xu and Zhang [49] further used this signal as a temporal indicator alongside combining several other measures and

TABLE I
DESCRIPTION OF THE COLLECTED AND ANNOTATED DATA SETS

Category	# Reviews	# Reviewers	# Brands	# Products
All	17,24,656	10,77,027	30,486	1,88,298
Filtered by reviewer history	3,41,081	10,379	28,437	1,81,596
Annotated set	45,892	366	8,005	33,892

proposed a completely unsupervised model for detecting group collusion. Several graph-based approaches have also shown the potential to detect both spam reviewers and spam reviews simultaneously [5]. Wang *et al.* [50] and Dhawan *et al.* [7] extended the reviewer graph to detect collusive users, i.e., a temporary group of users who work in unison to spam. Again, there has been no study about any phenomenon of extremism at a group level, especially with respect to a brand, since extremism ultimately affects “brand attitudes.”

C. How Our Work Is Different From Others?

Our work is different from the existing studies in the following ways.

- 1) We introduce the problem at a brand level, which was not considered in any of the previous studies.
- 2) Unlike other studies that majorly focus on fake review/reviewer detection, we here focus on extremist reviewer detection, which may not be fake. Moreover, we attempt to identify “groups” instead of detecting “individual user.”
- 3) We investigate the effect of Amazon’s 2016 changes in reviewing policy and the review scenario postpolicy changes.

III. DATA SET

To the best of our knowledge, no data set of consumer reviews (on Amazon) that consists of brand information exists so far. Thus, we attempted to create the first data set of its kind by crawling reviews from Amazon.in, the Indian counterpart of the e-commerce giant. In this data set, along with the regular metadata, we also obtained the brand on which a review was posted. Other metadata per-review include reviewer id, product id (ASIN), brand, rating, review text, date, and the number of helpful votes a review has received. (Details on dealing with individual reviewer data are mentioned in Section I of the Supplementary Material.)

The data were crawled during August–October 2018. The data set containing review history of reviewers consists of 341081 reviews from 10379 unique reviewers, spanning across 181596 products from 28437 brands. Table I shows the statistics of the complete data set.

Since the data set contains brand information associated with each review, these reviews can be used to identify the groups of reviewers targeting a particular brand. This problem can be seen as an extension of the existing data mining techniques such as frequent itemset mining (FIM) by considering itemset as a sequence of reviewer IDs, where each transaction contains the IDs of reviewers who have reviewed several products of the same brand. (Details on detecting candidate groups and selecting parameter for FIM are mentioned in Sections II and III of the Supplementary Material.)

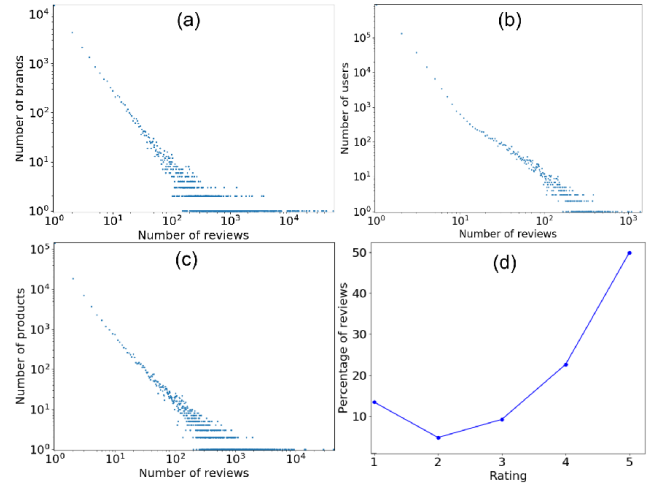


Fig. 2. Preliminary analysis. Variation of reviews with (a) number of brands, (b) number of reviewers, and (c) number of products. We observe a power-law distribution in all cases. (d) Percentage of reviews having a given rating. Also, as a general trend, the number of one- and two-star reviews is less than four- or five-star reviews.

A. Preprocessing the Data Set

On Amazon, usually, a brand does not directly sell its products. There are sellers that post their products and post them up for sale. Thus, the scraped data with brand names had an inherent issue. Different sellers might not give the exact same brand name to the products they list. Thus, identifying which products belong to the same group needs some preprocessing since the brand name may have subtle differences such as different cases (e.g., Whirlpool versus WhirlPool) or different acronyms (e.g., LG versus L.G. Electronics). We apply NLP normalization techniques as preprocessing to avoid such cases (more details in Section I of the Supplementary Material).

B. Preliminary Observation

We perform an analysis of our data to understand the relationships between brand and reviews. To this end, we draw the log–log plots of the number of reviews against brands, products, and reviewers (see Fig. 2). We observe a power-law distribution for not only products and reviewers (as reported in [38]) but also for brands [Fig. 2(a)–(c)]. This suggests the possibility that similar methods for detecting extremism at the brand level might work. Also, a distribution of the ratings given to reviews is shown in Fig. 2(d). We observe that the number of reviews with a low rating (one and two stars) is comparatively less than that of high rating (four and five stars).

C. Human Annotation

The technique used in previous studies for labeling fake reviews/reviewers was recrawling to detect the deleted reviews [51] and employing human judges for manual labeling [4], [5], [39], [43], [52], [53].

Some crucial insights while manually annotating reviewer groups are mentioned in [54], such as review length, similarity, excessive use of capitalization, brand pin-pointing, and personal relationship with brands. The labeling was done

TABLE II
FACTORS KEPT IN MIND BY THE ANNOTATORS
WHILE ANNOTATING THE DATA SET

Criterion	Information focused on
Brand mentions	Individual review
Excessive use of superlatives in text	Individual review
Excessively positive or negative sentiment	Individual review
Similarity in product description and review	Individual review
Rating variety	Reviewer profile
Number of reviews written	Reviewer profile
Rating deviation from the average rating	Reviewer profile
Reviewer's active duration	Reviewer profile
Similarity in reviews among group members	Group
Time of reviews of group members	Group
Rank of reviewers the group has	Group

keeping in mind these insights regarding the ratings, review title, review text, date posted, the number of helpful votes received, and also in some cases the product and reviewer ids. We leverage this information to perform manual labeling. These have been summarized in Table II.

Once the pruning is completed by recursive elimination [55], we made $(group, brand)$ tuples based on what brands the group has reviewed. This gave us around 180 000 pairs. Since there were too many candidate groups, our annotators could only manage to label 923 candidate $(group, brand)$ pairs as either 0 or 1, based on if they are genuine/moderate or extreme (brand critical or brand positive); 469 and 454 groups were marked as extreme and moderate groups, respectively. We employed three annotators who were within the age group of 20–35 years and were experts in e-commerce service policies. Out of 1000 reviews labeled, there was disagreement by the three annotators in around 77 groups. Therefore, we considered only 923 groups which all the three annotators agreed upon. The interannotator agreement is $\kappa = 0.86$ (Cohen's κ). We then use this as a ground truth to draw insights about extremist user groups, train classifiers to detect extremist groups, and identify the most important features that such extremist groups exhibit.

One may argue that the annotated data set is small in size. We would like to emphasize that such annotation is extremely challenging and time-consuming since the annotators need to go through each group separately and analyze the review patterns of all the constituent members of the group. In our case, the entire annotation took two-and-a-half months to finish. As suggested in [4], [56], we did not use Amazon Mechanical Turk (MTurk) for this annotation task because MTurk is normally used to perform simple tasks that require human judgments. However, our task is highly challenging, and the annotators required access to our data. Also, we needed annotators who had proper domain knowledge on the product review domain. Thus, we believe that MTurk was not suitable in our case. Due to the same problem, Mukherjee *et al.* [4] also did not use MTurk for the annotation of fake reviewer groups.

IV. CLASSIFICATION MODEL

We follow a feature-based classification technique to determine whether a candidate group is an extremist group with

respect to a given brand. For classification, we use state-of-the-art classifiers, such as SVM, random forest, logistic regression, decision tree, Gaussian Naive Bayes, K nearest neighbors (KNN), stochastic gradient descent (SGD), three-layer perceptron (MLP), and XGBoost (as suggested in [57]). We additionally test with an additional layer in the MLP-based architecture that consists of two fully connected hidden layers followed by a dense layer with a softmax activation as an output layer, forming a four-layer perceptron. Note that this four-layer perceptron is just to test the effect of increased depth.

A. Features Used for Classification

Previous studies proposed useful features for detecting group spam. For example, Mukherjee *et al.* [4] proposed eight features that are highly useful for detecting group spam. We extend these features into the brand level and identify groups of extremist users. The features we used are as follows.

- 1) *Average Rating*: It captures the average rating given by the group G to a certain brand B . We aggregate the reviews given by group members to products of the given brand and take the mean of these ratings. We hypothesize that an extreme group may give an average rating value at the extremes, i.e., closer to five stars or one star

$$\text{avg_rating}(G, B) = \text{avg}_{m \in G, p \in B} \text{rating}(m, p)$$

where $\text{rating}(m, p)$ is the rating given by member m to product p .

- 2) *Average Upvotes*: It captures how many upvotes the given group receives with respect to the given brand. This is the mean of upvotes taken across reviews posted by the group members, for products belonging to the given brand

$$\text{avg_upvotes}(G, B) = \text{avg}_{m \in G, p \in B} \text{upvote}(m, p)$$

where $\text{upvote}(m, p)$ is the number of upvotes of the reviews for product p posted by reviewer m .

- 3) *Average Sentiment*: We analyze the review text for the given $(group, brand)$ pair and find out the average sentiment of these reviews. We use SentiWordNet 3.0 [58] for the sentiment analyzer, which returns an overall sentiment for the review text between -1 and 1 . An extremist group may write reviews having an overall sentiment of being highly positive ($+1$) or highly negative (-1) toward a particular brand

$$\text{avg_sentiment}(G, B) = \text{avg}_{m \in G, p \in B} \text{sentiment}(m, p)$$

where $\text{sentiment}(m, p)$ indicates the sentiment of the review on product p posted by reviewer m .

- 4) *Group Time Window (GT)*: It indicates the difference between the latest review posted by the group and the earliest review posted by the group for the given brand. A lower value of GT may suggest that the group is

closely linked together and indulges in spamming the reviews together

$$\begin{aligned} & \text{GT}(G, B) \\ &= \begin{cases} 0, & \text{if } L(G, B) - F(G, B) > \tau \\ 1 - \frac{L(G, B) - F(G, B)}{\tau}, & \text{Otherwise} \end{cases} \end{aligned}$$

where $L(G, B)$ and $F(G, B)$ are the last and the first dates of any review posted by any member of group G on any product of brand B , respectively. Empirically, $\tau = 0.28$ was found to produce the best result.

- 5) *Review Count*: This feature captures how many reviews are written by the group for the particular brand. An extremist group is more likely to write more reviews collectively than other users

$$\text{RC}(G, B) = \sum_{m \in G} |\text{reviews}(m, B)|$$

where $|\text{reviews}(m, B)|$ is the number of reviews written by reviewer m on all products belonging to brand B .

- 6) *Rating Deviation*: It captures how much does the (*group*, *brand*) deviate from the mean rating. The reviewers of an extremist group are expected to possess a lesser deviation since they must write highly coherent opinions for the brand

$$\sigma(G, B) = \frac{|\langle r_{G,B} \rangle - \langle \bar{r}_{G,B} \rangle|}{4}$$

where $\langle r_{G,B} \rangle$ and $\langle \bar{r}_{G,B} \rangle$ represent the average rating given by group G on products belonging to brand B and average rating given by anyone not belonging to group B on products of brand B . The deviation is normalized by 4 since the rating ranges from 1 to 5; the maximum rating deviation can be 4.

- 7) *Early Time Window (ET)*: It measures the time gap since the product spawned on the marketplace, and the last review posted on for it by the group. The mean value is taken across all the products for the brand

$$\begin{aligned} & \text{ET}(G, B) \\ &= \text{avg}_{p \in B} \text{TW}(G, p) \\ & \text{TW}(G, p) \\ &= \begin{cases} 0, & \text{if } L(G, p) - \alpha(p) > \beta \\ 1 - \frac{L(G, p) - \alpha(p)}{\beta}, & \text{Otherwise} \end{cases} \end{aligned}$$

where $L(G, p)$ is the latest review date for a review done by any member of group G on a product p and $\alpha(p)$ is the earliest review date for product p . Empirically, $\beta = 0.28$ was found to produce the best result.

- 8) *Verified Purchase*: A review where the product was actually bought by the reviewer holds more credibility than the opposing case. This feature determines the fraction of reviews posted by the group for the brand corresponding to amazon-verified-purchase reviews

$$\text{VP}(G, B) = \frac{|\text{verified}(G, B)|}{\text{RC}(G, B)}$$

where $|\text{verified}(G, B)|$ is the number of verified reviews done by any member in G for a product belonging to brand B and $\text{RC}(G, B)$ is the review count as mentioned earlier.

B. Experimental Setup

We utilize a standard grid search for hyperparameter optimization (as suggested in [57]). For better reproducibility, we also report the parameters used for each classifier: MLP—logistic function as activation function, learning rate of $1e-5$, two hidden layers each with 100 neurons; KNN with $K = 5$; CART with Gini gain criteria for Decision Tree and Random Forest; for SGD learning rate of $1e-5$, modified Huber as loss function, maximum iteration of 200, and L2 norm as penalty function, XGBoost with a maximum tree depth of 4, a learning rate of 0.1, and a total of 100 estimators. The results are reported after tenfold cross validation with suitable hyperparameter optimization. To report the accuracy of the classifiers, we use standard evaluation metrics, i.e., precision, recall, F1-score, and area under the ROC curve (ROC-AUC), with both microaveraging and macroaveraging.

V. CLASSIFICATION RESULTS

Table III summarizes the classification accuracy. We observe that all the methods performed decently in predicting the label of the given candidate (*group*, *brand*) pair. However, the performance of neural network-based methods (three- and four-layer perceptron) is superior compared with the rest of the classifiers. This may be due to the data being accurately mapped by deep learning methods. Three-layer perceptron seems to be the best method with an accuracy of 0.98 across all the metrics used to evaluate the performance. Decision Tree seems to be the worst among all the classifiers since it is extremely sensitive to small variations that are prevalent in our data set. Nevertheless, we conduct the rest of the experiment with three-layer perceptron as the default classifier (see Table IV).

VI. FEATURE IMPORTANCE

To estimate and interpret how much each feature is indicative of extremist behavior, i.e., how much a feature governs the overall extremity of a group, we use the optimal feature weight distribution of our random forest classifier (Table V) as it is an established fact that Random Forest is a highly interpretable classifier. Alternatively, we run our three-layer perceptron, omitting each feature in isolation, and note down the drop in classification accuracy, which should also tell us how important each feature is to determine the extremity of a group. The observations are shown in Table IV.

The review count, i.e., how much a group writes about a brand, seems to be the strongest indicator of extremism. It shows that most of the time the activity involves writing a lot about a brand compared to moderate reviewers, which can be attributed to the fact that the group promotes/demotes a target brand by an overwhelming number of reviews. This trend can be explained by both the experiments: as given by random forest, and dropping this feature causes a significant drop in the three-layer perceptron's classification accuracy.

TABLE III
PERFORMANCE OF VARIOUS CLASSIFIERS. THE TASK IS OF BINARY CLASSIFICATION, AND THUS, THE VALUES OF MACROAVERAGE AND MICROAVERAGE ARE BOTH EXTREMELY CLOSE DIFFERING ONLY BECAUSE OF AVERAGING OVER FOLDS

Classifier	Micro Average				Macro Average			
	Precision	Recall	F1	ROC-AUC	Precision	Recall	F1	ROC-AUC
SVM	0.930	0.930	0.930	0.930	0.940	0.927	0.933	0.927
Logistic Regression	0.803	0.803	0.803	0.802	0.803	0.802	0.802	0.802
Random Forest	0.780	0.780	0.780	0.782	0.784	0.782	0.783	0.782
Decision Tree	0.699	0.699	0.699	0.701	0.704	0.701	0.703	0.701
Gaussian Naive Bayes	0.563	0.563	0.563	0.576	0.737	0.576	0.647	0.576
SGD	0.824	0.824	0.824	0.829	0.866	0.829	0.847	0.829
KNN	0.814	0.814	0.814	0.816	0.818	0.816	0.817	0.816
3-Layer Perceptron	0.982	0.982	0.982	0.982	0.982	0.982	0.982	0.982
4-Layer Perceptron	0.914	0.914	0.914	0.917	0.925	0.917	0.921	0.917
XGBoost	0.710	0.710	0.710	0.713	0.722	0.713	0.718	0.713

TABLE IV
ACCURACY OF THE THREE-LAYER PERCEPTRON AFTER DROPPING EACH FEATURE IN ISOLATION

Feature	Micro Average				Macro Average			
	Precision	Recall	F1	ROC-AUC	Precision	Recall	F1	ROC-AUC
Review count	0.640	0.640	0.640	0.641	0.647	0.641	0.644	0.641
Rating deviation	0.915	0.915	0.915	0.914	0.928	0.914	0.921	0.914
Avg. upvotes	0.955	0.955	0.955	0.956	0.957	0.956	0.956	0.956
Group time window	0.962	0.962	0.962	0.962	0.963	0.962	0.963	0.962
Verified purchase	0.966	0.966	0.966	0.967	0.967	0.967	0.967	0.967
Avg. sentiment	0.969	0.969	0.969	0.969	0.969	0.969	0.969	0.969
Early time window	0.971	0.971	0.971	0.971	0.972	0.971	0.972	0.971
Avg. rating	0.973	0.973	0.973	0.973	0.973	0.973	0.973	0.973

TABLE V
WEIGHTS GIVEN TO FEATURES BY RANDOM FOREST CLASSIFIER

Feature	Weight
Review Count	0.456
Early time window	0.154
Verified purchase	0.133
Avg. rating	0.105
Avg. sentiment	0.055
Rating deviation	0.051
Avg. upvotes	0.044
Group Time window	0.001

The rating deviation of the group seems to be another important feature for distinguishing two types of groups. Random Forest assigns it a decent score (Table V), and four-layer perceptron also exhibits an accuracy drop on removing this feature. This conforms to the past studies that associate extremism in review to the rating associated with the review [27].

Also, a major difference between extreme and moderate reviews is whether the product being reviewed was actually bought by the reviewer or not, as shown by the Amazon verified purchase tag next to the review. It shows a consistent value of importance in both our experiments.

Ratings are generally coupled with a similar sentiment in the review text itself. Therefore, it is not a very surprising observation that the average sentiment of a group to a brand also plays a minor role in the classification process, as given by the feature weight. However, since sentiment is a bit correlated with the rating, dropping this feature does not produce a great loss of accuracy since the missing information is nevertheless captured by the rating.

Unsurprisingly, average upvote count does not seem to have much impact on the nature of the group since, for different

product types, both kinds of reviews are helpful. Interestingly, “Average Rating” does not have any significant impact on the extremist and moderate review detection. This might be attributed to both kinds of groups that have a similar average over their group.

The overall trend of the extremist versus moderate reviewers is summarized in Fig. 3 and explained in the following section.

VII. CHARACTERIZATION OF EXTREMIST GROUPS

In this section, we attempt to characterize extremist reviewer groups and distinguish them from moderate groups. Fig. 3(a) shows that on an average, the extremist group writes a lot of five-star reviews, while moderate users are spread around the four stars. This is due to the nature of the problem itself that extremist groups tend to give extreme ratings to the target brand. The lack of reviews on the extreme negative side would be discussed in the later sections.

Fig. 3(b) shows that extremist groups tend to give similar ratings to the brand, giving a very small rating deviation. On the other hand, moderate users have some variance in the given ratings. The fact is that the rating deviations are about 1 and not higher may be attributed to the fact that generally people naturally tend to write positive reviews, with reviews generally not falling in the extreme negative side of the spectrum.

Fig. 3(c) shows that most of the reviews written by extremist users are about verified purchases. This distribution is significantly skewed compared to moderate users. Apparently, this observation may seem counterintuitive; however, this trend can be explained by the existence of several Blackmarket services which give products for free or heavily discounted rates (we will discuss it later).

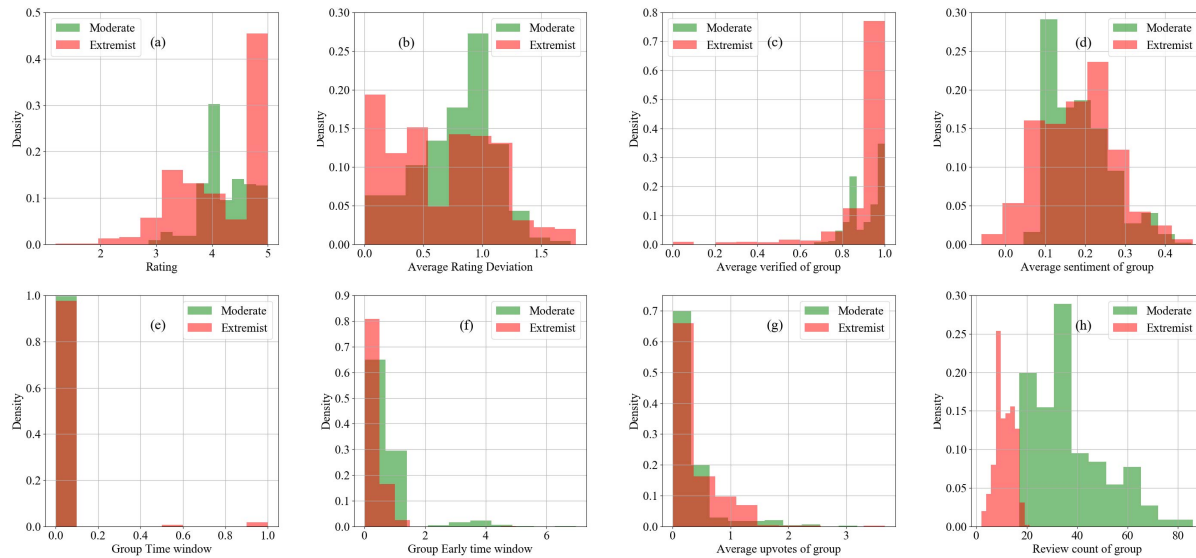


Fig. 3. (Color online) Comparison of extremist and moderate groups based on different features used in the classification.

Fig. 3(d) shows that moderate users tend to write reviews using a neutral or near-neutral tone, with extremists writing reviews using a positive sentiment in their writing.

Fig. 3(e) shows a similar trend of group time window distribution for both types of groups. Therefore, this may not be a good feature to predict the nature of a given (*group*, *brand*) pair.

Fig. 3(f) shows that extremist groups have a higher chance of reviewing the product of the target brand earlier compared to the moderate users.

Fig. 3(g) infers that the number of upvotes does not play a significant role, and the trend justifies the phenomenon. This may be attributed to the fact that either people do not take their time to upvote meaningful reviews, and upvotes given by the group members in case of extremist groups are nullified by upvotes given by users to moderate reviews.

Fig. 3(h) shows that extremist groups tend to write more reviews for a target brand compared to the moderate reviewers.

VIII. DISCUSSION

During labeling and classification, we found a fair number of spam groups showing extremist behavior. This is a strong indicator for our hypothesis that extremism is widely prominent at the brand level, with groups aiming to promote or demote brands, due to various reasons that may include economic incentives either directly or indirectly by the brand itself.

A closer look at the target brands reveals that most of them are not widely popular with little recognition among the general public. This is not surprising since these brands may be part of start-ups that might have a constraint on resources for marketing or publicity and thus interested in unethical practices to boost their growth. Also, since they have a relatively small consumer base and, thus, a small number of moderate reviews, reviews from spam groups influence their brand image more strongly.

The well-established and more reputed brands do not appear to be a target of these malicious activities due to several

reasons: 1) they already have a huge customer base and followers; 2) reviews by spam groups would be suppressed by the sheer number of moderate reviews for other customers; and 3) they have lot of reputation and popularity to lose if caught indulging in malicious activities.

There exist premium services that offer plans at different costs ranging from different reviews. Another crowdsourcing technique is also popular on websites, such as *Ripple Influence*³ or *Product Elf Coupons*⁴ where a seller puts his/her products along with a discount coupon, which the customer (the influencer) uses to purchase the product at a discounted price and post their reviews. Doing this, they gain more reputation on these sites and then can “unlock” higher discount coupons. Such kinds of reviews, though effective, will not qualify as a verified-purchase review since they were received at discounted rates, and systems can easily prevent spammer groups by using only verified reviews. Therefore, spammers now require a different strategy.

Since Amazon had restricted reviews recently in 2016, the services for obtaining reviews are forced to modify their mode of operation. A way to circumvent the restriction imposed on the system is to provide discount/refund off-site (e.g., a cashback). For example, we show a dashboard for a cashback-based website (cashbackbase.com) in Fig. 4. At the bottom, we can see their process for issuing cashback: A reviewer needs to “claim” the discount on the site, purchase the product within a time limit, and upload information proving the purchase on Amazon. After verifying the purchase, the website sanctions a cashback into the buyer’s account. Thus, the buyer was effectively incentivized for the product purchase. Although the website does not mandate reviews from the buyers, they do claim that their websites can help in gathering reviews (on the merchant portal). On further investigation, we came to know that this is indeed the case. One such confession by an anonymized top reviewer was seen

³<https://www.rippleinfluence.com>

⁴<http://productelf.com>

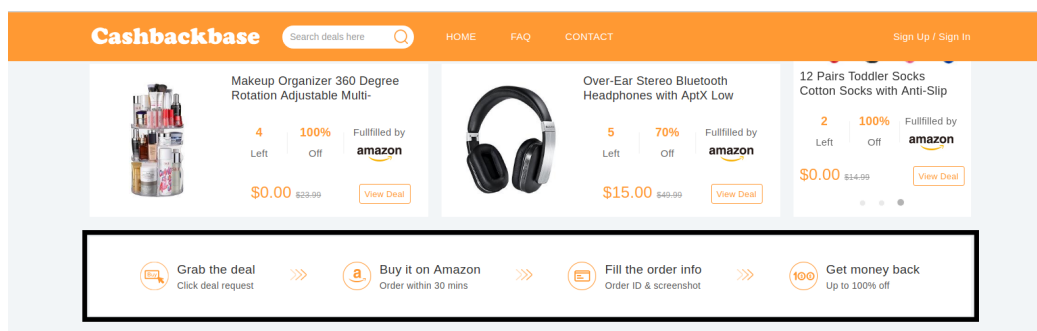


Fig. 4. Dashboard for a cashback-based website.

in a blog post [59]. Thus, it is to be expected that the online marketplace will be infested with manipulated extreme review instances. It is even more difficult to distinguish such cases due to the off-site nature, but by relating brand-level group, extremism activities to designing robust and feasible systems becomes possible.

Finally, we find that almost all the extremist groups are involved in promoting their target brand instead of demoting others. This observation may be attributed to the reason that it is more effective and profitable to edge out the competition by boosting their own brand image, rather than working to hinder the competition since that would require influencing a lot of brands, requiring a lot more resources and time.

IX. CONCLUSION

In this article, we discussed an unexplored form of opinion spam, where spammers target brands as a whole, posting extreme reviews, to change the overall sentiment about the brand. These groups are often part of a complex business Web that is capable of influencing the overall popularity and reputation of several brands on review websites. This article is the first step toward linking brand-level group activities and extremism in reviews, which uncovers important insights about marketplace activities. These insights would help in developing a better recommendation that makes use of online reviews.

A set of candidate spam groups was retrieved using FIM, and extremist groups were identified by observing their actions as a group based on various features, using a supervised learning technique based on a ground truth of manually annotated labels. We then classified extremist and moderate groups and compared the accuracy across multiple classification methods.

After classifying these groups, we observed the behaviors for extremist groups in detail to gain further insights about the phenomenon and the overall trends of how these groups target these brands. We have also released the codes and annotated data set for further studies.

REFERENCES

- [1] A. Kim. (2017). *That review you wrote on Amazon? Priceless.* [Online]. Available: <https://www.usatoday.com/story/tech/news/2017/03/20/review-you-wrote-amazon-prices/99332602/>
- [2] E. Gilbert and K. Karahalios, "Understanding deja reviewers," in *Proc. ACM Conf. Comput. supported Cooperat. Work (CSCW)*, 2010, pp. 225–228, doi: [10.1145/1718918.1718961](https://doi.org/10.1145/1718918.1718961).
- [3] Amazon.in. (2018). *Review Community Guidelines.* [Online]. Available: <https://www.amazon.in/gp/help/customer/display.html?nodeId=201929730>
- [4] A. Mukherjee, B. Liu, and N. Glance, "Spotting fake reviewer groups in consumer reviews," in *Proc. 21st Int. Conf. World Wide Web (WWW)*, 2012, pp. 191–200.
- [5] Y. Lu, L. Zhang, Y. Xiao, and Y. Li, "Simultaneously detecting fake reviews and review spammers using factor graph model," in *Proc. 5th Annu. ACM Web Sci. Conf. (WebSci)*, 2013, pp. 225–233.
- [6] S. Rayana and L. Akoglu, "Collective opinion spam detection: Bridging review networks and metadata," in *Proc. 21th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2015, pp. 985–994.
- [7] S. Dhawan, S. C. R. Gangireddy, S. Kumar, and T. Chakraborty, "Spotting collective behaviour of online frauds in customer reviews," 2019, *arXiv:1905.13649*. [Online]. Available: <http://arxiv.org/abs/1905.13649>
- [8] K. Dave, S. Lawrence, and D. M. Pennock, "Mining the peanut gallery: Opinion extraction and semantic classification of product reviews," in *Proc. 12th Int. Conf. World Wide Web (WWW)*, 2003, pp. 519–528.
- [9] B. Pang, L. Lee, and S. Vaithyanathan, "Thumbs up? Sentiment classification using machine learning techniques," in *Proc. Conf. Empirical Methods Natural Lang. Process.*, 2002, pp. 79–86.
- [10] K. Mouthami, K. N. Devi, and V. M. Bhaskaran, "Sentiment analysis and classification based on textual reviews," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2013, pp. 271–276.
- [11] Q. Ye, Z. Zhang, and R. Law, "Sentiment classification of online reviews to travel destinations by supervised machine learning approaches," *Expert Syst. Appl.*, vol. 36, no. 3, pp. 6527–6535, Apr. 2009.
- [12] M. Chelliah and S. Sarkar, "Product recommendations enhanced with reviews," in *Proc. 11th ACM Conf. Recommender Syst.*, Aug. 2017, pp. 398–399.
- [13] L. Chen and F. Wang, "Preference-based clustering reviews for augmenting e-commerce recommendation," *Knowl.-Based Syst.*, vol. 50, pp. 44–59, Sep. 2013.
- [14] J. Feuerbach, B. Loepp, C.-M. Barbu, and J. Ziegler, "Enhancing an interactive recommendation system with review-based information filtering," in *Proc. IntRS@RecSys*, 2017, pp. 10–55.
- [15] A. Almahairi, K. Kastner, K. Cho, and A. Courville, "Learning distributed representations from reviews for collaborative filtering," 2018, *arXiv:1806.06875*. [Online]. Available: <http://arxiv.org/abs/1806.06875>
- [16] A.-M. Popescu and O. Etzioni, "Extracting product features and opinions from reviews," in *Proc. HLT*, 2005, pp. 339–346.
- [17] B. Liu, M. Hu, and J. Cheng, "Opinion observer: Analyzing and comparing opinions on the Web," in *Proc. 14th Int. Conf. World Wide Web (WWW)*, 2005, pp. 342–351.
- [18] M. Hu and B. Liu, "Mining opinion features in customer reviews," in *Proc. AAAI*, 2004, pp. 755–760.
- [19] T. Donkers, B. Loepp, and J. Ziegler, "Explaining recommendations by means of user reviews," in *Proc. 1st Workshop Explainable Smart Syst. (ExSS)*, 2018. [Online]. Available: <http://ceur-ws.org/Vol-2068/exss8.pdf>
- [20] B. Pang *et al.*, "Opinion mining and sentiment analysis," *Found. Trends Inf. Retr.*, vol. 2, nos. 1–2, pp. 1–135, 2008.
- [21] M. Hu and B. Liu, "Mining and summarizing customer reviews," in *Proc. ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2004, pp. 168–177.
- [22] G. Somprasertsri and P. Lalitrojwong, "Mining feature-opinion in online customer reviews for opinion summarization," *J. UCS*, vol. 16, no. 6, pp. 938–955, 2010.
- [23] L. Zhuang, F. Jing, and X.-Y. Zhu, "Movie review mining and summarization," in *Proc. 15th ACM Int. Conf. Inf. Knowl. Manage. (CIKM)*, 2006, pp. 43–50.

- [24] S. Pecar, "Towards opinion summarization of customer reviews," in *Proc. Student Res. Workshop (ACL)*, 2018, pp. 1–8. [Online]. Available: <https://www.aclweb.org/anthology/P18-3001>
- [25] N. N. Ho-Dac, S. J. Carson, and W. L. Moore, "The effects of positive and negative online customer reviews: Do brand strength and category maturity matter?" *J. Marketing*, vol. 77, no. 6, pp. 37–53, Nov. 2013.
- [26] P. K. Chintagunta, S. Gopinath, and S. Venkataraman, "The effects of online user reviews on movie box office performance: Accounting for sequential rollout and aggregation across local markets," *Marketing Sci.*, vol. 29, no. 5, pp. 944–957, Sep. 2010.
- [27] S. Mudambi and D. Schuff, "Research note: What makes a helpful online review? A study of customer reviews on Amazon.com," *MIS Quart.*, vol. 34, pp. 185–200, Mar. 2010.
- [28] G. Yin, L. Wei, W. Xu, and M. Chen, "Exploring heuristic cues for consumer perceptions of online reviews helpfulness: The case of Yelp.com," in *Proc. PACIS*, 2014, Art. no. 52. [Online]. Available: <https://aisel.aisnet.org/pacis2014/52/>
- [29] S.-M. Kim, P. Pantel, T. Chklovski, and M. Pennacchiotti, "Automatically assessing review helpfulness," in *Proc. Conf. Empirical Methods Natural Lang. Process. (EMNLP)*, 2006, pp. 423–430. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1610075.1610135>
- [30] Y. Wang, J. Wang, and T. Yao, "What makes a helpful online review? A meta-analysis of review characteristics," *Electron. Commerce Res.*, vol. 19, no. 2, pp. 257–284, Jun. 2019, doi: [10.1007/s10660-018-9310-2](https://doi.org/10.1007/s10660-018-9310-2).
- [31] M. Salehan, M. Mousavizadeh, and M. Koohikamali, "A recommender system for online consumer reviews," *Assoc. Inf. Syst.*, Fort Worth, TX, USA, Tech. Rep. 12, 2015. [Online]. Available: <https://aisel.aisnet.org/ficis2015/proceedings/DecisionAnalytics/12/>
- [32] M. Eisend, "Two-sided advertising: A meta-analysis," *Int. J. Res. Marketing*, vol. 23, no. 2, pp. 187–198, 2006.
- [33] P. A. Pavlou and A. Dimoka, "The nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation," *Inf. Syst. Res.*, vol. 17, no. 4, pp. 392–414, Dec. 2006.
- [34] C. Forman, A. Ghose, and B. Wiesenfeld, "Examining the relationship between reviews and sales: The role of reviewer identity disclosure in electronic markets," *Inf. Syst. Res.*, vol. 19, no. 3, pp. 291–313, Sep. 2008.
- [35] J. A. Krosnick, D. S. Boninger, Y. C. Chuang, M. K. Berent, and E. Al, "Attitude strength: One construct or many related constructs?" *J. Personality Social Psychol.*, vol. 65, no. 6, pp. 1132–1151, 1993, doi: [10.1037/0022-3514.65.6.1132](https://doi.org/10.1037/0022-3514.65.6.1132).
- [36] K. J. Kaplan, "On the ambivalence-indifference problem in attitude theory and measurement: A suggested modification of the semantic differential technique," *Psychol. Bull.*, vol. 77, no. 5, pp. 361–372, 1972.
- [37] S. Presser and H. Schuman, "The measurement of a middle position in attitude surveys," *Public Opinion Quart.*, vol. 44, no. 1, pp. 70–85, 1980, doi: [10.1086/268567](https://doi.org/10.1086/268567)
- [38] N. Jindal and B. Liu, "Opinion spam and analysis," in *Proc. Int. Conf. Web Search Web Data Mining (WSDM)*, 2008, pp. 219–230.
- [39] M. Ott, Y. Choi, C. Cardie, and J. T. Hancock, "Finding deceptive opinion spam by any stretch of the imagination," in *Proc. 49th Annu. Meeting Assoc. Comput. Linguistics*, 2011, pp. 309–319.
- [40] N. Jindal, B. Liu, and E.-P. Lim, "Finding unusual review patterns using unexpected rules," in *Proc. 19th ACM Int. Conf. Inf. Knowl. Manage. (CIKM)*, 2010, pp. 1549–1552.
- [41] F. Li, M. Huang, Y. Yang, and X. Zhu, "Learning to identify review spam," in *Proc. 22nd Int. Joint Conf. Artif. Intell.*, 2011, pp. 2488–2493.
- [42] A. Fayazi, K. Lee, J. Caverlee, and A. Squicciarini, "Uncovering crowdsourced manipulation of online reviews," in *Proc. 38th Int. ACM SIGIR Conf. Res. Develop. Inf. Retr. (SIGIR)*, 2015, pp. 233–242.
- [43] E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, "Detecting product review spammers using rating behaviors," in *Proc. 19th ACM Int. Conf. Inf. Knowl. Manage. (CIKM)*, 2010, pp. 939–948.
- [44] G. Wang, S. Xie, B. Liu, and P. S. Yu, "Review graph based online store review spammer detection," in *Proc. IEEE 11th Int. Conf. Data Mining*, Dec. 2011, pp. 1242–1247.
- [45] A. Mukherjee, V. V. Venkataraman, B. Liu, and N. S. Glance, "What yelp fake review filter might be doing?" in *Proc. 7th Int. Conf. Weblogs Social Media*, 2013, pp. 409–418.
- [46] A. Mukherjee et al., "Spotting opinion spammers using behavioral footprints," in *Proc. 19th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2013, pp. 632–640.
- [47] G. Fei, A. Mukherjee, B. Liu, M. Hsu, M. Castellanos, and R. Ghosh, "Exploiting burstiness in reviews for review spammer detection," in *Proc. ICWSM*, Jan. 2013, pp. 175–184.
- [48] A. Molavi Kakhki, C. Kliman-Silver, and A. Mislove, "Iolau: Securing online content rating systems," in *Proc. 22nd Int. Conf. World Wide Web*, 2013, pp. 919–930.
- [49] C. Xu and J. Zhang, "Towards collusive fraud detection in online reviews," in *Proc. IEEE Int. Conf. Data Mining*, Nov. 2015, pp. 1051–1056.
- [50] Z. Wang, S. Gu, X. Zhao, and X. Xu, "Graph-based review spammer group detection," *Knowl. Inf. Syst.*, vol. 55, no. 3, pp. 571–597, Jun. 2018.
- [51] C. Xu, "Detecting collusive spammers in online review communities," in *Proc. 6th workshop Ph.D. Students Inf. Knowl. Manage. (PIKM)*, 2013, pp. 33–40.
- [52] D. Liang, X. Liu, and H. Shen, "Detecting spam reviewers by combing reviewer feature and relationship," in *Proc. Int. Conf. Informative Cybern. Comput. Social Syst. (ICCSS)*, Oct. 2014, pp. 102–107.
- [53] S. Xie, G. Wang, S. Lin, and P. S. Yu, "Review spam detection via temporal pattern discovery," in *Proc. 18th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2012, pp. 823–831.
- [54] A.-T. Pieper, "Detecting review spam on amazon with reviewalarm," M.S. thesis, Dept. Behavioural, Manage. Social Sci., Univ. Twente, Enschede, The Netherlands, 2016.
- [55] C. Borgelt, "Frequent item set mining," *Wiley Interdiscipl. Rev., Data Mining Knowl. Discovery*, vol. 2, no. 6, pp. 437–456, 2012.
- [56] H. S. Dutta, V. R. Dutta, A. Adhikary, and T. Chakraborty, "HawkesEye: Detecting fake retweeters using Hawkes process and topic modeling," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2667–2678, Jan. 2020. [Online]. Available: <https://ieeexplore.ieee.org/document/8976235/authors#authors>
- [57] H. Fulara, G. Singh, D. Jaisinghani, M. Maity, T. Chakraborty, and V. Naik, "Use of machine learning to detect causes of unnecessary active scanning in WiFi networks," in *Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2019, pp. 1–9.
- [58] S. Baccianella, A. Esuli, and F. Sebastiani, "Sentiwordnet 3.0: An enhanced lexical resource for sentiment analysis and opinion mining," in *Proc. LREC*, 2010, pp. 1–5.
- [59] Y. Chen. *Confessions of a Paid Amazon Review Writer*. Accessed: Nov 4, 2019. [Online]. Available: <https://digiday.com/marketing/vendors-ask-go-around-policy-confessions-top-ranked-amazon-review-writer/>



Viresh Gupta is currently pursuing the B.Tech. degree with the Department of Computer Science and Engineering, IIIT-Delhi, New Delhi, India.

His research focuses on natural language processing, complex network analysis, graph mining, representation learning, multimodal analysis and applications of data-driven artificial intelligence methods like machine learning and deep learning in problems across diverse domains.

Mr. Gupta has received recognition in the form of dean's list award for both academics and research and development at IIIT-Delhi.



Aayush Aggarwal is currently pursuing the B.Tech. degree with the Department of Computer Science and Engineering, IIIT-Delhi, New Delhi, India.

His research interests include data mining, natural language processing, and artificial intelligence, who is also exploring domains related to theoretical computer science and mathematics.



Tanmoy Chakraborty (Member, IEEE) is currently an Assistant Professor and a Ramanujan Fellow with the Department of Computer Science and Engineering, IIIT-Delhi, New Delhi, India, where he leads a Research Group, called LCS2. His primary research interests include social network analysis, data mining, and natural language processing.

Mr. Chakraborty has received several awards including Google Indian Faculty Award, Early Career Research Award, DAAD Faculty Award.