CG-HC: Candidates Grouping and Hierarchical Clustering based Group shilling Attacks detection in Recommender System

Ch. Rathan Kumar

Research Scholar, Department of Computer Science and Engineering

Osmania University, Hyderabad, Telangana, India

Corresponding email: rathankumaroucse@gmail.com

Radhika Kavuri

Department of Information Technology, CBIT, Telangana, 500075, India.

kradhika_it@cbit.ac.in

Article Info
Page Number: 10477-10491
Publication Issue:
Vol. 71 No. 4 (2022)

ABSTRACT

In the past ten years, a variety of techniques for spotting shilling assaults in recommender systems have been put forth. The current strategy for detecting shilling attacks focuses on detecting single attackers, but rarely addresses group shilling attacks, whereas team of attackers uses false profiles to manipulate a digital recommender system's results. In some technique's researchers used users individual and group features separately to form the groups. In this article, we developed a three-phase technique for identifying group shilling attacks. In first phase, we build tight candidate groups using user behaviour features. In second phase, we determined the degree of suspicion for each user in the group and using a hierarchical clustering technique splitted each group into two clusters. Finally, we applied group suspicious measures to find the attack groups. On real-world datasets like Netflix and Amazon reviews, the developed technique beats the baseline when compared with baseline detection methods.

Article History
Article Received: 12 October 2022
Revised: 24 November 2022
Accepted: 18 December 2022

1. INTRODUCTION

As internet stuff has proliferated quickly, information overload has become a major concern [1]. In some cases, Online Recommender Systems (RS) may help reduce information overload due to their suggestions for their users. However, RS have a history of being exposed to profile injection or shilling attacks [2, 3]. Such assaults have the potential to undermine user confidence in the recommender system and degrade the effectiveness and caliber of recommenders. Traditional attack models have received much study during the past decade like random, average, bandwagon attacks, etc. In the mentioned attacks, Attackers often aim to promote or demote target goods or individually inject attack profiles into RS. In Group shilling attacks [4, 5], this shilling behavior is performed with the intention of making the system more vulnerable. It is difficult for conventional detection methods to detect a conventional attack when attackers collaborate and develop attack profiles purposefully. As a result, improving performance of group shilling assaults detection is a critical issue in recommender systems.

Previous techniques developed by several authors on shilling attacks hardly take into account the collusive shilling behaviours among attackers and instead concentrate primarily on identifying individual attackers in RS. Although a few detection techniques [6, 7, 8, 9, 10] for group shilling assaults have been put out recently, they often need information of the attacks prior (such as the count of shilling groups or perpetrators). If not, they have an accuracy issue. On review websites, there have recently been several stated methods for identifying spammer groups [11, 12]. The in-group shilling tactics used by spammer teams on review sites are different from those used by recommendation systems.

To circumvent the above mentioned restrictions, the proposed technique Candidate Groups and Hierarchical Clustering (CG-HC) uses group behavioral features applied on candidate groups to detect group shilling attacks using Hierarchical Clustering method. The suggested method focuses on attack user's cooperative behaviours and successfully identifies group of shilling attackers.

As a summary, this article contributes the following:

1. In contrast to current approaches for creating user connection graphs, which emphasize relationships between users directly, we generate tight Candidate Groups based on neighbourhood properties like a) Reviewed products b) ratings given to products c) time spent on reviewing products among group members.
2. In each group, Individual Users Suspicious Degree (IUSD) is calculated using the behavioral features of users and based on the degree divided each group into two clusters using Ward's Hierarchical Clustering method.
3. Next, identified group attackers based on Group Suspicious Degree (GSD) by applying item and user related behavioral group attack features on each cluster.
4. Based on Netflix and Amazon datasets, we test our method on comprehensive datasets and compare its detection performance to baseline approaches.

Table 1: Group shilling attack summary

Version	**Model Attack**	**IS**	**IF items**	**IF rating**	**Target item rating**
GSAGens	Random	Zero	Randomly selected & In shilling group only rated by single attacker	Mean of the system	r_{max}/r_{min}
	Average	Zero	Randomly selected & In shilling group only rated by single attacker	Mean of the Item	r_{max}/r_{min}
GSAGenl	Random	Zero	Randomly selected & Two attackers can rate each shilling item.	Mean of the system	r_{max}/r_{min}

ISSN: 2094-0343
2326-9865

	Average	Zero	Randomly selected & Two attackers can rate each shilling item.	Mean of the Item	r_{max}/r_{min}

Furthermore, we are inspired by the works of Fuzhi Zhang et al. (2020), HongyunCai et al. (2021) on recommendation system group shilling detection to carry out this work.

Afterwards, the article is structured as follows. An overview of literature is presented in section 2. An outline of proposed technique (CG-HC) for detecting group shilling attacks is provided in section 3. Evaluation reports are included in section 4 and we conclude our findings and recommendations in the final section.

2. LITERATURE SURVEY

There have been an enormous number of algorithms developed over the last decade to detect and eliminate shilling attacks in recommender systems related to ratings, time, and item popularity. Wang et al. [7] developed a challenging group shilling assault model contains GSAGens and GSAGenlversions to produce successful group shilling profiles while avoiding detection of current approaches. Among them, GSAGenl will produce a shilling group with more shilling profiles than GSAGens because GSAGenl has fewer rigorous restrictions to generate. Table 1 outlines the group shilling assault models.

Hao et al. [10] created a user-user graph using rating behaviorlikeness and identified the attacker group using highest item filling rate. As a result of this approach, attacker communities can be identified where they are heavily linked to one another. The greater the maximum fill rate of the item within the group, the less precise the detection.Su et al. [13] introduced group shilling attack detection along with two attack scenarios. Multiple attackers are highly planned in these instances to mask their intentions. It depends on the scenario whether the shilling group's attackers collaborate to promote or demote the target goods or attack just some items in the target set.

Shilling attacks detection using supervised manner in recommender systems, Hao et al. [14] gathered multidimensional detection characteristics from several viewpoints like ratings, time of rating and item popularity degree, before training an SVM-based classifier to identify shilling assaults. This approach is more successful than the baseline methods; however it does not function well when the attack size is below than 10%.

A deep-learning-based technique for detecting classic shilling assaults in RS described by Zhou et al. [15]. The handmade features are not used in this technique, but it does require a validation set to discover the ideal hyper parameters. In [16] Zhang et al. present a supervised classifier capable of detecting attacks based on user representations and assessing their likelihood. Through this approach, extensive user side information can be utilized and integrated to increase detection performance, but certain hyper parameters must be configured.

Using LSTM-based deep learning, [17] suggested a hybrid convolutional neural network to detect attack characteristics. As filler size increases, the F1-measure of this approach declines because six different assault models can be recognized. Wu et al. [18] have suggested a method for identifying shilling profiles in recommender systems, in their approach the classifier was trained using both labelled and unlabeled profiles. This approach detects hybrid shilling assaults effectively, but it has lower detection efficiency than C4.5 decision trees. In order to detect known forms of shilling assaults, supervised detection approaches require that a classifier be trained using the labelled profiles in the training set.

A group based ranking technique based on ratings and classification was proposed by Gao et al. [19] for detecting unsupervised shilling attacks in RS.Although this method performs well when the dataset contains a few distorted ratings with only few attackers, its precision deteriorates when the dataset contains more original distorted ratings. Zhang et al. [20] investigated the differences in item popularity between authentic and malicious profiles and developed a unique detection technique based on a HMM and hierarchical clustering. It performs well in identifying various types of attacks; however, it fails to detect AoP attacks.

Zhang et al. provided an unsupervised detection strategy for detecting different assaults in Ref. [21] by analysing the diversity of real and attack users in rating behaviors. The key to assessing suspicious behavior is to dynamically discover the crucial point of evaluation, but if the attacks size is small, it is difficult to discern the critical point.

Another unsupervised technique of detection is presented in [22]; abisecting K-means algorithm is used to find shilling groups based on the suspicious groups in the candidate groups, after dividing the rating tracks for each item.On the Synthesis dataset, this method detects group attacks quite well. However, its accuracy on the real-world dataset needs to be increased.

3. CG-HC GROUP ATTACKERS DETECTION FRAMEWORK

When several attackers work together to take down the RS, attackers grade not only the intended product(s), but also certain unintended products over a predetermined period of time using identical reviewing practices. Based on these assumptions, the figure1 depicts a Candidate Groups and Hierarchical Clustering based shilling group attack detection (CG-HC) approach. A three-phased approach is proposed to detect the shilling attacks. Creating candidate groups, it begins with groups consisting of people who score the same item simultaneously. The user and item features are extracted in the next stage. Each group's level of individual usage is identified. and using hierarchical clustering approach suspicious groups are created. Finally identified group attackers based on Group Suspicious Degree (GSD) by applying item and user related behavioral group attack features on each cluster.

3.1 Generation of Candidate Groups:

A group of spammers have similar properties in terms of: a) Reviewed products b) ratings given to products c) time spent reviewing products. By incorporating above three factors generated suspicious groups based on following steps:

i) Initially constructed a graph – G (V, E), which segregates the users based on the products reviewed; then, it generated sub-groups based on the similar reviews given by the different users.
ii) Next, based on neighborhood properties like users behaviour (similar ratings and similar time), the graph is mapped in to the candidate groups.

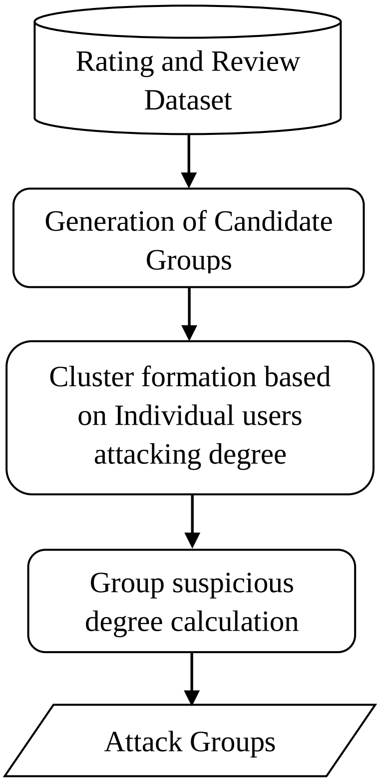

Figure 1. Proposed System Architecture

From Algorithm1 line 1-3 is used to eliminate isolated nodes in graph G, those users are treated as individual users. Line 4-11 is used to construct candidate groups based on edge values as, Edge $e_{(ij,mn)} = (u_{ij}, v_{mn}) \in E$, it explains two ratings (j, n) and two products (i, m) co-rating & co-reviewing patterns. The edge attribute $a^{e}_{(ij,mn)}$ represents the co-reviewers $R_{(ij,mn)}$ who gave review on same Γ_t time with similar ratings r_j and r_n on p_i and p_m products. It is important to note that an edge linking the same product with various rating values will not exist in G since we consider that a reviewer is not entitled to provide many reviews/ratings for a single product.

Algorithm 1: Generate Candidate Groups

Input:

P – Set of Products

R – Set of Reviewers

G (V, E) – Product – Product Graph

CGgroups – Empty set of Candidate Groups

Output:

Candidate Groups

Begin

i. **for** every isolated node v_i in G **do**
ii. CGgroups ← remove (v_i), add v_i from Graph G
iii. **end for**
iv. **for** every pair $(e_i, e_j) \in E \times E$ do
v. **if** $a_i^e \subset a_j^e$ **then**
vi. **if** $J(P_{a_j^e}, P_{a_j^e}) > 0.5$ **then**
vii. CGgroups.add$\left(a_i^e\right)$
viii. remove a_i^e from G
ix. **end if**
x. **end if**
xi. **end for**

End

3.2 Clusters creation based on Ward's Hierarchical clustering method

3.2.1 Ward's Hierarchical clustering:

Hierarchical clustering produces a group of clusters based on the hierarchical structure of data samples. For this, an agglomerative or divisive approach may be used. The error sum of squares is the foundation of Ward's approach [23]. Using this technique, clusters are agglomerated as a result of merging two clusters together; minimize the dispersion within the clusters. When creating clusters, Ward's technique takes into account both within and between cluster distances, which can improve the classification impact. Ward's technique, however, does not require prior knowledge of the number of clusters.

3.2.2 Individual Users Suspicious Degree (IUSD) calculation:

From the Algorithm1 we identified groups based on the users similar of rated items and similar time. To find group attackers there must be a need of generating cluster with equal kind of users. In order to find similarity among users, we calculated the Individual Users Suspicious Degree by using the following item and user behavioral four indicators showned in Table 2 to measure the suspicious degree. The IUSD is the average of all four indicators.

Algorithm 2 gives the process of generation of clusters, which contains two parts. In first section (lines 3-10), are used to calculate every user's suspicious degree in each group related to the items. In second part (lines 11-20), using hierarchical clustering method based on individual scores of user every group is divided into two clusters.

Algorithm 2 Clusters Generation

Input: Candidate Groups

Output: HC - Set of clusters

Begin

i. G ← call Algorithm 1
ii. HC ← ∅
iii. **for** each g ∈ G **do**
iv. **for** each user u ∈ U **do**
v. **for** each item i ∈ I do
vi. calculate ARD, ABRD, ER, ETF
vii. IUSD (u) = getAvg (ARD, ABRD, ER, ETF)
viii. **end for**
ix. **end for**
x. **end for**
xi. **for** each g ∈ G **do**
xii. N ← | IUSD(g)|
xiii. Let every user suspicious degree in IUSD be a cluster, denoted as C = {C_1, C_2… C_K}
xiv. r**epeat**
xv. N ← N − 1
xvi. Make a new from clusters C_i & C_j using the min SSE
xvii. Calculate SSE between new & other clusters.
xviii. **until** N = 2
xix. HC←HC ∪ (C_i & C_j)
xx. **end for**
xxi. return HC

End

3.3 Group (Cluster) Suspicious Degree Calculation

Over the last decade, several types of individual attack characteristic features are proposed. However, the detecting characteristics that are useful for shilling groups are restricted. And most of the techniques used items related [22] and users behaviour related [24] group features for degree calculation independently, but to improve the identification more clearly we are using both types of features to measure the suspicious degree for each group. The model calculates Suspicious Groups degree value using the average of four group spam indicators on each group (cluster).

Table 2: Users & Item features

Indicator	**Description**
ARD	Average Rating Deviation of user (product) i's reviews [26, 27]
ABRD	Product average ratings Absolute Rating Deviation [28]
ER	Extremity of Ratings [29]: xEXT = 1 if ratings 4, 5 else 0
ETF	Early Time Frame [29].

i. Group Product Tightness (GPT): If a group just analyses a small number of items and has never assessed any other products, it is likely that it is an actual opinion spammer group. The total number of products that group g members have all evaluated in common divided by all products reviewed by group members is the product tightness of group g and is presented in equation (1):

$$GPT(g) = \frac{|\bigcap_{r \in R_g} \mathrm{P_r}|}{|\bigcup_{r \in R_g} \mathrm{P_r}|} \qquad (1)$$

ii. Group Rating Variance (GRV): Members of the group intend to target components are elevated or decreased, thus their rating scores should be equal or alike. GRV is calculated as shown in equation (2):

$$GRV(g) = 2\left(1 - \frac{1}{1+\mathrm{e}^{\mathrm{k}}}\right)L(g) \qquad (2)$$

Where, $k = -avg_{(p \in P_g)} \operatorname{var}(p, g)$

Spamicity is lower when variance is higher.

iii. Group Neighbor Tightness (GNT): Compared with genuine reviewer groups the collusion relationship among reviewers in spammer groups is stronger. The GNT is given in equation (3)

$$GNT(g) = avg_{r_1, r_2 \in R_g} \frac{|\mathrm{P_{r1}} \cap \mathrm{P_{r2}}|}{|\mathrm{P_{r1}} \cup \mathrm{P_{r2}}|} \qquad (3)$$

iv. Group Reviewer Ratio (GRR) on Product: GRR is described as, highest proportion of product reviewers in Rg on product p where all the reviewers of p $\in$Pg and is represented in equation (4):

$$GRR(g) = \max_{p \in P_g} \frac{|R_{\mathrm{gp}}|}{|R_{\mathrm{p}}|} \qquad (4)$$

The algorithm 3 consists primarily of two parts. It takes the set of clusters created by algorithm 2. In the first part (lines 3–10), based on the above mentioned group behavioral

ISSN: 2094-0343
2326-9865

indications calculated each clusters suspicious degree. As a result of line 11, we are calculating the total of standard deviation of all clusters as well as mean of each. Then the second part (lines 13-17) identifies attack groups based on threshold value of supicious degree.

Algorithm 3 Attack Groups Detection

Input: HC - Set of clusters

Output: GA: Set of Attacking Groups

Begin

i. C ← call Algorithm 2
ii. GA ← Ø
iii. **for** each c ∈ C **do**
iv. **for** each item i ∈ I do
v. calculate GPT (c, i), GRV (c, i) from eq 1, 2
vi. **end for**
vii. **for** each user u ∈ U **do**
viii. calculate GNT (c, u), GRR (c, u) from eq 3, 4
ix. **end for**
x. CSD (c) is calculated as the sum of 1,2,3,4 equation values of cluster c
xi. **end for**
xii. TCSD = getAverage(C) + getStdev(C)
xiii. **for** each c ∈ C **do**
xiv. **if** CSD (c) >= TCSD **then**
xv. GA ← GA ∪ c
xvi. **end if**
xvii. **end for**
xviii. return GA

End

4. EXPERIMENTAL EVALUATION

4.1 Datasets:

To evaluated proposed CG-HC technique, two data sets [20, 22, 24] Netflix Data Set, Amazon Review Datasetare used to conduct experiments. Table 3 provides the description about datasets.

Table 3: Datasets description

Dataset Name	**Users**	**No of Ratings / reviews**	**items / products**
Netflix Data Set	4,80,186	10,32,97,638	17,770
Amazon Review Dataset	6,45,072	12,05,125	1,36,785

This article's experiment is broken up into two sections. The experiment's initial phase uses artificial data sets to generate results. With the reference of [20, 22, 24] we assumed Netflix dataset users are genuine users, we also used attack profiles and they are injected into Netflix dataset to find the attacker groups. From this dataset we constructed sampled dataset of 2,15,884 rating data for 4,000 goods from 2000 users. In the second part we used Amazon Review Dataset. A sampling dataset of Amazon reviews is constructed using the tagged reviewers as part of experimental assessment [25] it has 53,777 rating data for 17,610 goods from 5055 customers.

4.2 Evaluation Metrics:

Recall, precision and F1 – measure are used to evaluate the performance of our CG-HC method, which are defined as follows:

$$F1 - measure = \frac{2 * precision * recall}{precision + recall}$$

$$precision = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}$$

$$recall = \frac{TP}{TP + FN}$$

Table 4: Performance detection comparison on Netflix Dataset

	Precision	**Recall**	**F1- measure**
GB-BKM	0.9720	0.9888	0.9803
UD-HMM	0.851	0.99	0.915
TF-GBF	0.9903	0.9983	0.9942
CG-HC	0.9923	0.991	0.9916

4.3 Compared baselines and Experimental Analysis

We assessed the effectiveness of the proposed technique with baseline methods like UD-HMM [20], GD-BKM [22], and TP-GBF [24]. Performances of these methods are evaluated on Netflix and Amazon Review Datasets.

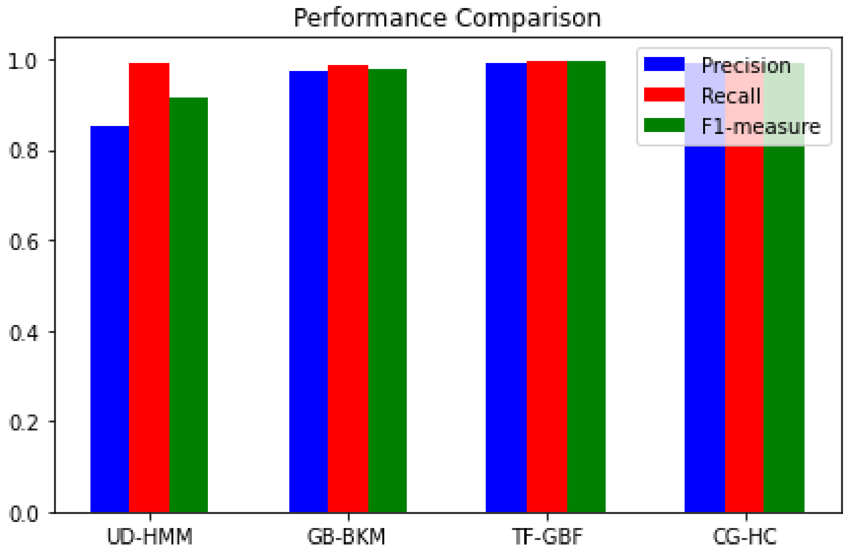

Figure 4: Comparison of four methods on Netflix Dataset

Comparison of performance on both Netflix and Amazon Review Datasets:

Figure 4 and 5 lists the performance of precision, recall and F1-measure for UD-HMM, GD-BKM, TF-GBF and CG-HC on Netflix and Amazon Datasets. As represented in Table4, the precision, recall and F1-measure for UD-HMM is 0.851, 0.99 and 0.915. Similarly GD-BKM, TF-GBF models achieved precision 0.9720, 0.9903, recall as 0.9888, 0.9983 and F-1measure as 0.9803, 0.9942. Compared with these models our CG-HC achieved better precision compared to baseline models as 0.9923 and small less recall and F1-measure as 0.991. 0.9916 on Netflix dataset.

Table 5: Performance detection comparison on Amazon Review Dataset

	Precision	**Recall**	**F1- measure**
GB - BKM	0.823	0.673	0.7404
UD - HMM	0.376	0.419	0.3963
TF - GBF	0.9283	0.6467	0.7623
CG - HC	0.952	0.6828	0.7956

As represented in Table5, UD-HMM, GD-BKM, TF-GBF models achieved precision 0.376, 0.823, 0.9283, recall as 0.419, 0.673, 0.6467 and F-1measure as 0.3963, 0.7404, 0.7623. Compared with these models our CG-HC achieved better precision, recall and F1-measure as 0.952, 0.6828, and 0.7956. This states that our model performed well compared with baseline models.

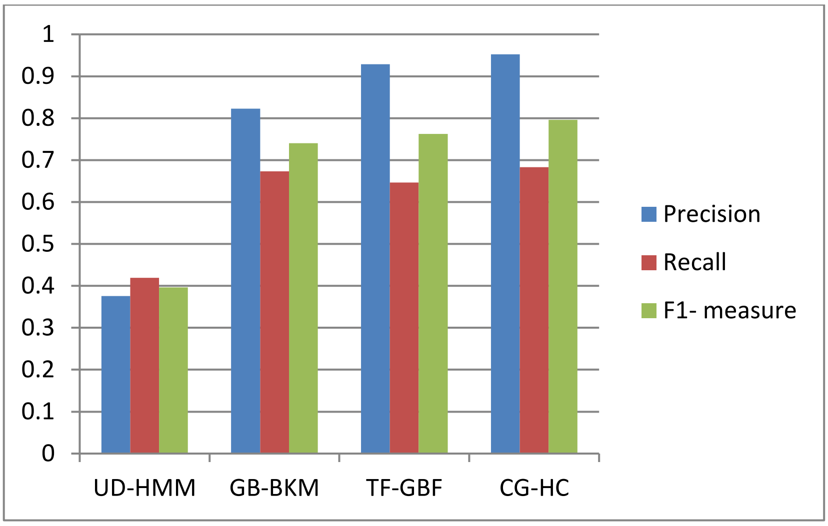

Figure 5: Comparison of four methods on Amazon Dataset

5. CONCLUSION

Group shilling attacks on RS are more dangerous and harder to identify than conventional shilling attacks. Previous approaches mainly concentrated on the individual attacker's detection but compared with group attackers individual attacking has less impact. In order to find group attackers previous works focused on item and user level features separately and applied clustering approaches to create attacker groups. We introduced a three stage detection methodology to enhance the efficacy of group level spammers detection called CG-HC based on both individual and group behavioral features.

Initially we generated tight Candidate Groups using users reviewed products, ratings given on products and time spent on reviewing products. Then calculated Individual Users Suspicious Degree (IUSD) for each group using the behavioral features of users and based on the degree divided each group into two clusters using Ward's Hierarchical Clustering method. Finally, identified group attackers based on Group Suspicious Degree (GSD) by applying item and user related behavioral group attack features on each cluster. Netflix and Amazon datasets have demonstrated that the CG-HC provides better precision, recall, and F1- measure than three baseline methods.

ACKNOWLEDGMENT

We thank R&D department of Osmania University, Hyderabad, India institute for funding.

CONFLICT OF INTEREST

Authors declare that there are no conflicts of interest in regarding the publication of this paper.

REFERENCES

1. [1] T. L. Ngo-Ye and A. P. Sinha. (2012). "Analyzing online review helpfulness using a regressional relief F- Enhanced text mining method," ACM Trans. Manage. Inf. Syst., vol. 3, no. 2, pp. 10:1–10:20. https://doi.org/ 10.1145/2229156.2229158
2. [2] I. Gunes, C. Kaleli, A. Bilge, and H. Polat. (2014). "Shilling attacks against recommender systems: A comprehensive survey," Artif. Intell. Rev., vol. 42, no. 4, pp. 767–799. https://doi.org/ 10.1007/s10462-012-9364-9.
3. [3] M. Si and Q. Li. (2020) "Shilling attacks against collaborative recommender systems: a review," Artificial Intelligence Review, vol. 53, no. 1, pp. 291–319. https://doi.org/ 10.1007/s10462-018-9655-x
4. [4] X. Su, H. Zeng, and Z. Chen.(2005) "Finding group shilling in recommendation system," in Proceedings of the Special Interest Tracks & Posters of the International Conference onWorld Wide Web, pp. 960-961, New York, NY, USA. https://doi.org/10.1145/1062745.1062818
5. [5] Y. Wang, Z. Wu, J. Cao, and C. Fang. (2012). "Towards a tricksy group shilling attack model against recommender systems," Advanced Data Mining and Applications, vol. 7713, pp. 675–688. https://doi.org/10.1007/978-3-642-35527-1_56
6. [6] J. Gao, Y. Dong, M. Shang, S. Cai, and T. Zhou. (2015). "Group-based ranking method for online rating systems with spamming attacks," EPL (Europhysics Letters), vol. 110, no. 2, Article ID 28003. https://iopscience.iop.org/article/10.1209/0295-5075/110/28003/meta
7. [7] W. Zhou, Y. Koh, J. Wen, S. Alam, and G. Dobbie. (2014). "Detection of abnormal profiles on group attacks in recommender systems," in Proceedings of the 37th international ACM SIGIR conference on Research & Development in information retrieval, pp. 955–958, Gold Coast Queensland Australia. https://doi.org/ 10.1145/2600428.2609483
8. [8] G. Gabriel, L. Robson, and F. Jose. (2017). "ORFEL: efficient detection of defamation or illegitimate promotion in online recommendation," Information Sciences, vol. 379, pp. 274–287. https://doi.org/10.1016/j.ins.2016.09.006
9. [9] F. Zhang and S. Wang. (2020). "Detecting group shilling attacks in online recommender systems based on bisecting K-means clustering," IEEE Transactions On Computational Social Systems, vol. 7, no. 5, pp. 1189–1199. https://doi.org/ 10.1109/TCSS.2020.3013878
10. [10] Y. Hao and F. Zhang. (2021). "An unsupervised detection method for shilling attacks based on deep learning and community detection," Soft Computing, vol. 25, no. 1, pp. 477–494. https://doi.org/ 10.1007/s00500-020-05162-6
11. [11] Y. Wang, Z. Wu, Z. Bu, J. Cao, and D. Yang. (2016). "Discovering shilling groups in a real e-commerce platform," Online Information Review, vol. 40, no. 1, pp. 62–78. https://doi.org/ 10.1108/OIR-03-2015-0073
12. [12] Z. Wang, S. Gu, X. Zhao, and X. Xu. (2018). "Graph-based review spammer group detection," Knowledge and Information Systems, vol. 55, no. 3, pp. 571–597. https://doi.org/10.1007/s10115-017-1068-7

13. [13] X.-F. Su, H.-J. Zeng, and Z. Chen. (2005). “Finding group shilling in recommendation system,” in Proc. Special Interest Tracks Posters 14th Int. Conf. WWW, pp. 960–961. https://doi.org/10.1145/1062745.1062818
14. [14] Y. Hao, P. Zhang, and F. Zhang. (2018). “Multiview ensemble method for detecting shilling attacks in collaborative recommender systems,” Security and Communication Networks, vol. 2018,no. 4, 33 pages, Article ID 8174603. https://doi.org/10.1155/2018/8174603
15. [15] Q. Zhou, J. Wu, and L. Duan. (2020). “Recommendation attack detection based on deep learning,” Journal of Information Security and Applications, vol. 52, Article ID 102493. https://doi.org/10.1016/j.jisa.2020.102493
16. [16] S. Zhang, H. Yin, and T. Chen. (2020). “GCN-Based representation learning for unifying robust recommendation and fraudster detection,” in Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval, pp. 689–698, Xi’an, China. https://doi.org/10.1145/3397271.3401165
17. [17] K. Vivekanandan and N. Praveena. (2021). “Hybrid convolutional neural network (CNN) and long-short term memory (LSTM) based deep learning model for detecting shilling attack in the social-aware network,” JAIHC, Springer, vol. 12, no. 1, pp. 1197–1210. https://doi.org/10.1007/s12652-020-02164-y.
18. [18] Z. Wu, J. Cao, Y. Wang, Y. Wang, L. Zhang, and J. Wu. (2020). “hPSD: a hybrid PU-Learning- Based spammer detection model for product reviews,” IEEE Transactions on Cybernetics, vol. 50, no. 4, pp. 1595–1606. https://doi.org/ 10.1109/TCYB.2018.2877161
19. [19] J. Gao, Y. Dong, M. Shang, S. Cai, and T. Zhou,. (2015). “Group-based ranking method for online rating systems with spamming attacks,” EPL (Europhysics Letters), vol. 110, no. 2, Article ID 28003. https://iopscience.iop.org/article/10.1209/0295-5075/110/28003/meta

    [20] F. Zhang, Z. Zhang, P. Zhang, and S. Wang. (2018). “UD-HMM: an unsupervised method for shilling attack detection based on hidden Markov model and hierarchical clustering,” Knowledge-Based Systems, vol. 148, pp. 146–166. https://doi.org/10.1016/j.knosys.2018.02.032
20. [21] F. Zhang, Z. Ling, and S. Wang. (2019). “Unsupervised approach for detecting shilling attacks in collaborative recommender systems based on user rating behaviours,” IET Information Security, vol. 13, no. 3, pp. 174–187. https://doi.org/10.1049/iet-ifs.2018.5131
21. [22] F. Zhang and S. Wang. (2020). “Detecting group shilling attacks in online recommender systems based on bisecting K-means clustering,” IEEE Transactions On Computational Social Systems, vol. 7, no. 5, pp. 1189–1199. https://doi.org/ 10.1109/TCSS.2020.3013878
22. [23] F Murtagh, P Legendre. (2011). Ward's hierarchical clustering method: clustering criterion and agglomerative algorithm. https://doi.org/10.1007/s00357-014-9161-z
23. [24] H. Cai and F. Zhang. (2021). “An Unsupervised Approach for Detecting Group Shilling Attacks in Recommender Systems Based on Topological Potential and Group

Behaviour Features," Hindawi Security and Communication Networks, Article ID 2907691. https://doi.org/10.1155/2021/2907691

24. [25] Zhuo Wang, Runlong Hu, Qian Chen, Pei Gao , Xiaowei Xu. (2020). ColluEagle: collusive review spammer detection using Markov random fields, Data Mining and Knowledge Discovery, Springer. https://doi.org/10.1007/s10618-020-00693-w