Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 6, 154 – 163

A NOVEL APPROACH FOR IDENTIFYING GROUP SHILLING ATTACKS IN RECOMMENDATION SYSTEMS

[1]S. Thavasi, [2]Dr. T. Revathi, [3]T. Raja Sushmitha

[1]sktthavasi@mepcoeng.ac.in, Assistant Professor/CSE, Mepco Schlenk Engineering College (Autonomous), Sivakasi – 626005, India
[2]trevathi@mepcoeng.ac.in, Sr.Professor and Head/IT, Mepco Schlenk Engineering College (Autonomous), Sivakasi – 626005, India
[3]rajasushmitha10_cs@mepcoeng.ac.in,PG Scholar/CSE, Mepco Schlenk Engineering College (Autonomous), Sivakasi – 626005, India

Abstract

Existing shilling attack detection algorithms are largely focused on identifying individual attackers in online recommender systems, and they seldom handle group shilling assaults, in which a group of attackers colludes to influence an online recommender system's output by providing fraudulent profiles. In this paper present a method for identifying shilling as a group assaults that incorporates both bisecting K-means clustering and hierarchical clustering methods in this research. First the rating track is extracted from each item's and divides it into candidate groups based on a predetermined time period. Second, the degree of item's attention and user interaction parameters are used to determine candidate group suspicious degrees. Finally, this work generate attack groups by grouping candidate groups based on their suspicious degrees using the bisecting K-means approach and the hierarchical clustering algorithm. Experiments are carried out using Amazon datasets. There are 103,297,638 ratings from 480,186 users on 17,770 products in the dataset. The proposed solution outperforms traditional approaches. The performance metrics used to evaluate the proposed systems are accuracy, precision, recall and f1-score.The proposed system provides 98% of accuracy, 90 % of precision, 98% of recall and 99% of f1-score.The goal of this research is to compare the bisecting k-means method with hierarchical clustering method and the results show hierarchical clustering based (proposed) method out performs bisecting k-means clustering method.

Keywords: Group shilling attack, bisecting k-means clustering, hierarchical clustering, attack detection.

1. INTRODUCTION

T The problem of information overload has arisen as a prominent concern with the fast proliferation of internet information. Users can get ideas from online recommender systems, which can aid with information overload. Attacks known as shillings, in which attackers use shillings to introduce a huge proportion of attacking profiles to impact the output of a recommender system, render online recommender systems susceptible. Push and nuke assaults can be used to promote or demote target objects (e.g., products) accordingly, to be proposed. Unprecedented attack, median assault, typical shifting attack, average-noise injecting attack, bandwagon assault, reverse juggernaut assault, and other well-studied shilling attacks are only a few examples. Attackers frequently insert attack recommender systems based on profiles individually in these assaults. In reality, a gang of assailants could plan a tactical attack together. As a result,

figuring out how to spot group shilling assaults has been a thing of the past an important a problem that must be resolved.

Various ways to identify shilling attacks have been published during the last decade to defend recommender systems. Current recommender system solutions, on the other hand, are mostly focused on identifying individual assailants and seldom explore collusive shilling by a group of people offenders. Although several methods for detecting shilling activities at the group level have been presented, they split detect assault groups and potential group that is based on profile similarity. There are a number of different group assault models that can result in a broad range of attack characteristics. As an outcome of this methods are unable to identify all assailants, resulting in low accuracy and recall. Some strategies for spotting spammer groups on review websites have recently been presented. Spammer groups on review websites are not the same as shilling tactics in recommendation system in groups. As a result, detection of fraudster gangs techniques are ineffective in detecting shilling as a grouping assaults. To circumvent the aforementioned restrictions, in this work bisecting K-means clustering and hierarchical clustering are used to identify Attacks on online recommendation system by a group of people. The proposed method uses the temporal concentration features of group shilling assaults to detect more effective group attacks with antitrust shilling behavior.

The following are the main contributions of this article

- This study presents a candidate group classification method that analyzes item rating records and then divides users in IRTs in time-based groups. The suggested grouping of candidates' strategy is much more prone to break up the assailants in an attack grouping collectively that can also help identify group shilling attacks, so the assailants a rating system must be used in an attack group targeted item in a specific length of time.
- The degree of item's attention and Activity of user (UA) measures for analyzing groups of candidates, resulting in more accurate attack group assessment. For each candidate group, the degree of item's attention and UA are calculated using the divided candidate groups, and the suspicious degrees of these groupings are determined. The candidate groups are then clustered according to their suspicious degrees using the bisecting K-means and hierarchical clustering techniques, providing the attack groups.
- Experiments on Amazon data sets are utilized to evaluate the technique's performance.

Moreover we are inspired by the works carried out by Mukhtar, Aet al.,(2022), Malarvizhi, A et al.,(2022) the proposed work on recommendation system and social media sentiment analysis which motivates us to carry out this work.

2. RELEATED WORKS

K. Vivekanandan.et al., (2020) Proposed a Shilling attack detection in recommender systems using a hybrid convolutional neural network (CNN) and long-short term memory (LSTM)-based deep learning model (CNN–LSTM). Netflix dataset, Amazon review, Movielens. The shilling attackers compute recommendation rankings using reviews, user ratings, and falsified user created content data. Prediction, recall, and f-measure are performance metrics utilised in this research.

Cai, Hongyun et al., (2021) proposed an identifying group shilling assault, researchers presented a a three-stage identification method based on strong group lockstep actions and group dynamics qualities. The datasets utilized in this study come from Netflix and Amazon reviews. F1-measure is a performance metric employed in this article.

A. M. Turk et al., (2019) proposed a using thorough experimental study, assess the resilience of baseline multi-criteria recommendation systems in relation to various similarity aggregation processes against proposed attacking strategies. This study

employed the YM5 and YM20 datasets. There are Shilling assaults tactics that inject harmful however this approach fails to locate them in collaborative filtering system in order to encourage one's own things or services while denigrating those of competitors. This paper's performance measurements include detection shift value.

B.Sharmila et al., (2021) proposed a dB scan technique is used to identify group shilling attacks. Netflix Data Set was utilised in this work. In the user's standpoint and in the realm of consumer use, fake reviews and ratings are always bothersome. Some people create and implant phoney user profiles with skewed ratings, skewing the recommendation ranking and influencing the user's decision. Prediction shift value is one of the performance indicators utilized in this work.

Chao Tong1.et.al., (2017) CNNSAD is a new CNN-based approach that uses a modified network topology to utilize the deep-level characteristics of user rating profiles. The 100K Netflix and MovieLens datasets were used in this study. When examining larger and more diverse data sets, the deep accumulation neural network model fails. Accuracy, recall, and F-measure were the performance measures used in this study.

3. System Design and Architecture

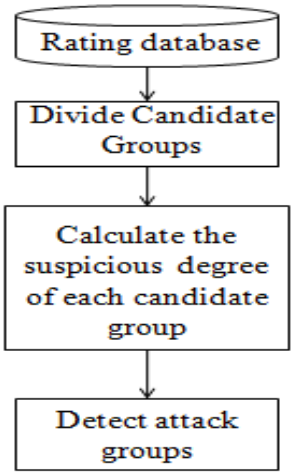

Figure 1: *system Architecture of the proposed system*

The figure 1 shows the work flow of the proposed system. When a group of attackers join forces to take down the recommendation systems, they rate not only the targeted item(s), as well as some non-target items. Furthermore, assailants in order to accomplish the intended assault impact, the group must complete their rating tasks within a specified amount of time. On the basis of these assumptions, the above diagram presents a group shilling attack detection method based on bisecting K-means clustering and hierarchical clustering. The propose diagram consists of three phases. The first stage is to create candidate groups, which are made up of individuals that score the same thing at the same time. In the second stage, the user and item characteristics are retrieved. The degree of suspicion for each application group is determined by combining these criteria. The bisecting K-means method and hierarchical clustering are then used to differentiate assault clustering on how suspicious they appear.

4. METHODOLOGY

The proposed methodology involves identification of candidate groups followed by identifying attack groups by identifying suspicious degree. The detailed descriptions of the modules proposed are as follows:

4.1. IDENTIFICATION OF CANDIDATE GROUPS

The rating track for each item is built in this part. The candidate groups are created depending on the tracks that have been rated and a specific time interval length (TIL) criterion.

4.1.1. IRT (Item Rating Track): The item i ∈ I(Item set)rating track is a set of user-time pairings specified by the user..

$$IRTi = \{(uin1,t1), (uin2,t2), \ldots, (uins,ts)\} \quad (1)$$

Users who rate item i are uin1, uin2,..., uins, and t1,t2,...,ts are timestamps when the item I is rated by users un1, un2,..., uns and ts> •••t2>t1. Users will be placed in the same candidate group if they rate the same item and their rating

timestamps are near. Furthermore, a group's starting time is dynamically determined. The steps for separating the applicant pool are as follows.

- In the data gathering, find all users who evaluate item I as well as the corresponding rating time for every items I then arrange them in sequential order to create the item I ratings track.
- The original user's ratings time is obtained and placed as a beginning point in items i's rating track; individuals whose rating time should be within TIL hours of the beginning point are then retrieved and separated into a candidates group.
- In the rating track for item I the ratings time of first individual who is not in a group is picked as the new beginning, and users who rating times are within TIL days of a new beginning point are eliminated and separated into a candidates group.
- Repeat steps 3–4 until all users on the item I ratings track are allocated to candidate groups.
- Continue with steps 1–4 until all of your items have been processed.

4.2. CALCULATION OF SUSPICIOUS DEGREE OF CANDIDATE GROUP

An attack group's goal, from the point of view of the item, is to raise the target item's recommended likelihood. The attention degree of an item will be high if the attackers agree to promote or dismiss each other it. Attackers in an attack group must accomplish their rating jobs within a certain time it takes to get the intended attack effect, hence the length of time required to achieve the desired attack effect throughout at this point frame. As a result, if a group of user's rates products with a high degree of attention and they are all online at the same time, it's more likely that the group is an assault group. On the basis of this analysis, human attributes and object characteristics are retrieved, and the degree of suspicion among the candidate groups is assessed.

4.3. DETECTION OF ATTACK GROUPS

The system clusters the candidates are divided into categories based on their level of suspicion. using bisecting K-means and hierarchical clustering and based on the separated candidate groups, determine the assault groups from the produced groupings of candidate groups. In more detail, it uses the collection of GSDs (Group Suspicious Degrees) as data samples, then use K-means clustering to bisect them and grouping in a hierarchical manner between them. This establishes the mean of GSDs for each of the K clusters after generating K clusters of groupings of candidates. If the cluster's mean value is more than or equivalent to the mean suspicious degrees of the candidate organizations plus overall statistical significance of the candidates groups' suspicious degrees, the groupings in this cluster are considered attack groups. The number of clusters K is necessary in k-means clustering, however with hierarchical clustering, no previous knowledge of the clustering is necessary.

$$GSD_{i,m}=GIAD_{i,m} \text{ X } GA_{i,m} \quad (2)$$

Where the suspicious degree of any group gi,m ∈ G(candidate group set) represented by the product of the group gi,m's degree of item's attention and the group's activity, gi,m is the mth candidate group of the item i.

$$GIAD_{i.m}=\frac{|g_{i,m}|}{|IRT_i|} \quad (3)$$

The group gi,m's degree of item's attention is the amount of users' count who have rated the item i in the mth group to the total users who have rated the item i.

The group item attention degree (GIAD) is indeed a way of measuring of how evenly the rating count is distributed over time intervals for a given item. When an item is attacked, it will receive more ratings over the course of the attack, resulting in high levels of group attention for the attacked item.

$$GA_{i,m}=\frac{\sum_{u\in g_{i,m}}.UA_{i,m}^{u}}{|g_{i,m}|} \quad (4)$$

Where the group's activity of mth candidate of item i is the mean of every users' activity in the group gi,m.

If it is a malicious group, its members will be active throughout this time span, resulting in a high group activity (GA).

$$UA_{i,m}^{u}=\frac{USRC_{i,m}^{u}}{|URIS_u|} \quad (5)$$

where the user activity is calculated mentioned above formula for each user u ∈ U(users set), let |URISu| be the sum of user u's rating counts.

Whenever a group shilling assault is carried out, the attackers are usually required to complete their respective tasks in a short period of time. As a result, hackers can rate additional items throughout this time frame than at other times, and intruder activity is high.

$$USRC_{i,m}^{u}=\left|\{(i,t) \in URIS_u / t \in [ST_{i,m,}ST_{i,m}+TIL]\}\right| \quad (6)$$

Where t is the user rating timestamp and ST i,m is the Starting Timestamp when the first user rated the item i in the mth candidate group of item i.

The quantity of goods rated by given user in item i's period increment [STi,m, STi,m+ TIL] is referred to as the sequential rating count of user u.

$$URIS_u=\{(i_{n1}^{u},t_1), (i_{n2}^{u},t_2),\ldots., (i_{ns}^{u},t_s)\} \quad (7)$$

A user's rating item series u ∈ U (User set) is a collection of item, time as key, value pairs.

where iun1,iun2,...,iuns are items rated by user u, and t1,t2,...,ts are user rated timestamps of the items in1,in2,...,ins and t1 < t2 < ⋯ <ts.

4.4. BISECTING K-MEANS CLUSTERING ALGORITHM

The following are the major steps in the bisecting K-means method.

Algorithm: Bisecting k-means

Create a list of clusters to fit the whole cluster

repeat

A cluster gets removed from of the cluster list

Perform a number of "trial" bisections of the cluster of interest

for i = 1 to the total number of trials do

Divide the selected clusters using simple K-means method

end for

Choose the two clusters with the lowest total SSE from the bisection.

until 'K' clusters are included in the cluster list

4.5 HIERARCHICAL CLUSTERING

Hierarchical clustering, also known as hierarchical clustering, is a technique for categorizing similar objects into clusters. The endpoint refers to a collection of cluster, each of which is distinct from the others contains broadly similar objects. There are primarily two types:

- divisive (top-down)
- agglomerative (bottom-up)

4.5.1 Divisive Approach

Algorithm: Divisive Clustering

Input: Dataset of size N (d1, d2, d3,....dN)

Initial Setup - all the data are in one cluster at the top

Separate the cluster by K-Means Clustering algorithm.

repeat

Choose the finest cluster from many of the clusters to split once more

the flat clustering technique separated that cluster

until every piece of data has its own singleton cluster

4.5.2. Agglomerative Approach

Algorithm: Agglomerative Clustering

Input:Dataset of size N (d1, d2, d3,....dN)

for i=1 to N:

for j=1 to i:

dis_mat[i][j] = distance[di, dj]

a singleton cluster is each data point

repeat

combine the two different groups which are close to each other.

update the distance matrix

until there is only one cluster left

5. EXPERIMENTAL EVALUATION

Assessing the proposed procedure the following the experiments are carried out using Amazon Dataset. Amazon Dataset: There are 103,297,638 ratings from 480,186 users on 17,770 products in the data set. The ratings are made up of numbers ranging from 1 to 5, with 1 indicating hate and 5 indicating the most liked. The experimental results set consists of 215 884 ratings drawn at random from 2000 people across 3985 products.

5.1. IDENTIFICATION OF CANDIDATE GROUPS

The rating track for each item is built. The candidate groups are created based on the user rating and a particular time interval length (TIL) threshold which shown in Table1.

Table 1: *Identification of Candidate Groups*

Item_Id	Group_Id	User_Id	Ratings	Timestamp
528881469	G1	A1H8PY3QHMQQA0,AMO214LNFCEI4,	2 1	1290556800 1290643200
	G2	A2CPBQ5W4OGBX'	2	1277078400
439886341	G1	A1GI0U4ZRJA8WN, A2NWSAGRHCP8N5	1 1	1334707200 1367193600

5.2. CALCULATION O F THE SUSPICIOUS DEGREE OF EACH CANDIDATE GROUP

By constructing the GSD (Group Suspicious Degree) to determine the fake ratings made by a group of users is identified. It is a computation of user activity based on the user rating time and rating to each item i.e. the time slot is used to group users with the same time slot together. To assess group activity, individual user behavior is examined. With this procedure, the GSD is computed as shown in Table 2.

Table 2: *Calculation of The Suspicious Degree Of Each Candidate Group*

Item Id	User ID	G1	G2	G3
321732944	A2CX7LUOHB2NDG	1	0	0
511189877	A89DO69P0XZ27	0.333333	0	0.23
511189877	A34ATBPOK6HCHY	0.333333	0	0
511189877	A3J3BRHTDRFJ2G	0	0.5	0.1
511189877	A2TY0BTJOTENPG	0	0.5	0

511189877	A1QGNMC6O1VW39	0	0.5	0.2
528881469	A1DA3W4GTFXP6O	1	0	0
528881469	A29LPQQDG7LD5J	1	0	0

5.3. DETECTION OF ATTACK GROUPS

The mean and standard deviation calculated using the GSD technique were calculated. GSTH is calculated by adding the mean and standard deviation. Bisecting K-means and hierarchical clustering algorithms were used to calculate the mean. The group is considered an attack group if the average value is bigger than GSTH as shown in Table 3.

Table 3: *Detection of Attack Groups*

Algorithms	**Group**	**User_id**	**Attack (Y/N)**
Bisecting K-Means Clustering	G1	Cluster 0 A1H8PY3QHMQQA0 AMO214LNFCEI4	Y
		Cluster 1 A89DO69P0XZ27 A34ATBPOK6HCHY	
Hierarchical Clustering	G1	Cluster 0 A1H8PY3QHMQQA0 AMO214LNFCEI4	N
		Cluster 1 A89DO69P0XZ27 A34ATBPOK6HCHY	

6. EXPERIMENTAL RESULT AND ANALYSIS

The proposed scheme is evaluated using two methods in order to demonstrate the usefulness. UD-HMM [11]: The use of hidden Markov chains in an unstructured method for detecting shilling assaults models to explain the differences in behavior between attackers and real users and Ward's hierarchical using clustering to identify attackers. On the Amazon data set, the parameters N and UD-HMM are set to 15 and 0.7, respectively, in the experiments. DPTS [12]: The addition to being an important series is dynamic partitioned first based on important points, and afterwards the chi-square distribution (2) is employed to find abnormal intervals in order to identify shilling attacks.

On the Amazon data set, proposed approaches (Bisecting k-means clustering and hierarchical clustering) with various attack size and filler size combinations. The following performance measures are used to evaluate the system.

$$Accuracy = \frac{TP + TN}{(TP + FP + FN + TN)}$$

$$Precision = \frac{TP}{(TP + FP)}$$

$$Recall = \frac{TP}{(TP + FN)}$$

$$F1 - Score = 2 * \left(\frac{(Precision * Recall)}{(Precision + Recall)}\right)$$

Table 4: *Comparison of Precision and Recall*

S. No.	Method	Precision	Recall
1.	Proposed Method [Hierarchical Clustering]	0.991	0.988
2.	Proposed Method [Bisecting k-means Clustering]	0.984	0.992
3.	GD-BKM	0.823	0.673
4.	UD-HMM	0.376	0.419
5.	DPTS	0.727	0.644

On the Amazon data set, researchers compared the precision and recall of the proposed technique, GD-BKM, UD-HMM, and DPTS. On the Amazon data set, Table 4 shows recall and precision for the proposed technique, GD-BKM, UD-HMM, and DPTS. So because Amazon set of data has a 99.9% sparsity level, the accuracy and recall values of UD-HMM on it are 0.376 and 0.419, respectively, as shown in Table 4. Furthermore, the amount of items co-rated by legitimate users is smaller than the amount of items co-rated by attack users, making the target products popular. DPTS has an accuracy of 0.727 and a recall of 0.644. This is due to the large variety of time periods in the Amazon set of data, which allows DPTS to perform rather well. GD-BKM has precision and recall value of 0.823 and 0.673, respectively, while the suggested approach has precision and recall values of 0.934 and 0.817, which are superior than GD-BKM, DPTS, and UD-HMM. These findings demonstrate that the suggested technique may be used to detect group assault characteristics inside the Amazon collected data.

TABLE 5: *Comparison of Performances*

S.No.	Method	Precision	Recall	F1 measure
1.	Proposed Method[hierarchical]	**0.991**	0.988	**0.990**
2.	Proposed Method[bisecting]	0.984	**0.992**	0.988
3.	GDBKM	0.823	0.673	0.74
4.	GDKM	0.482	0.882	0.623

On the Amazon Data Set, researchers compared the detection performance of the suggested approaches, GD-BKM [1] and GD-KM. To demonstrate the results of our detection model both using bisecting K-means (called GD-KM) and hierarchical clustering, we ran an experiment on the Amazon data set and compared its detection performance to that of the Proposed method using precision, recall, and F1-measure (i.e., the harmonic average of precision and recall) metrics. On the data set, Tables 5 exhibit a comparative of detection algorithms for the proposed technique, GD-BKM, and GD-KM. On the Amazon data set, the accuracy and F1-score values of suggested approaches are better than GDBKM and GD-KM, but the recall of GD-KM is greater than that of GD-BKM, as shown in Table 5. Overall, the suggested approaches outperform GD-BKM on the Amazon data set, demonstrating the efficiency of our classification models with bisecting K-means and Hierarchy clustering.

TABLE 6: *Performance Evaluation on the Amazon Dataset*

Method	Filler size	2.5%				5%			
	Attack	5%	10%	15%	50%	5%	10%	15%	50%

	Size								
Bisecting K-means clustering	**Accuracy**	0.9849	0.9864	0.9881	0.989	0.941	0.948	0.953	0.967
	Precision	0.9084	0.9482	0.9734	0.982	0.906	0.919	0.922	0.934
	Recall	0.9919	0.9923	0.9924	0.992	0.907	0.921	0.927	0.939
	F1-score	0.9455	0.9688	0.9825	0.987	0.943	0.951	0.967	0.977
Hierarchical clustering	**Accuracy**	0.9883	0.9884	0.9932	0.989	0.954	0.967	0.975	0.989
	Precision	0.9872	0.9923	0.9963	0.993	0.922	0.932	0.940	0.949
	Recall	0.9837	0.9777	0.9521	0.960	0.927	0.935	0.944	0.953
	F1-score	0.9911	0.9847	0.9730	0.976	0.958	0.964	0.972	0.981

As shown in Table 6, we compare the results for both Bisecting k-means clustering and Hierarchical clustering with different percentage of filter size and attack size. The analysis shows that the overall performance of the hierarchical clustering is better when compared to bisecting k-means algorithm.

7. CONCLUSTION

Shilling assaults in groups pose a significant danger to recommender systems. The bisecting K-means-based group assault detection model and hierarchical clustering technique to detect such assaults. When attackers have a few co-rated items, the suggested detection approach can solve the problem of low performance. The beginning time point for dividing every item's rating track to split candidate groups is dynamically determined using a set time duration. The features of objects and users are mixed to compute the GSD. The bisecting K-means technique is used to separate candidate groups are being attacked using GSDs. Our technique's success is demonstrated by the results of our testing on Amazon data sets. When the methods bisecting K-means and hierarchical clustering are compared, the hierarchical clustering algorithm outperforms the bisecting K-means clustering algorithm.

References

[1] Fuzhi Zhang et al.,(2020), "Detecting Group Shilling Attacks in Online Recommender Systems Based on Bisecting K-Means Clustering", IEEE Transactions on computational social systems.

[2] Shuo Qiu, Student Member, IEEE, Boyang Wang, Ming Li, Member, IEEE, Jiqiang Liu, and Yanfeng Shi(2020), "Toward Practical Privacy-Preserving Frequent Itemset Mining on Encrypted Cloud Data", IEEE Transactions on Cloud Computing.

[3] Cai, Hongyunetal., (2021) , "An Unsupervised Approach for Detecting Group Shilling Attacks in Recommender Systems Based on Topological Potential and Group Behaviour Features", Security & Communication Networks , p1-18. 18p.

[4] M. Si et al.,(2020), "Shilling attacks against collaborative recommender systems: a review," springer Artificial Intelligence Review, vol. 53, no. 1, pp. 291–319.

[5] A. M. Turketal.,(2019), "Robustness analysis of multi-criteria collaborative filtering algorithms against shilling attacks," Elsevier Expert Systems with Applications, vol. 115, pp. 386–402.

[6] K. Vivekanandanetal.,(2020), "Hybrid convolutional neural network (CNN) and long-short term memory (LSTM) based deep learning model for detecting shilling attack in the social-aware network," Springer Journal of Ambient Intelligence

and Humanized Computing, vol. 12, no. 1, pp. 1197–1210.
[7] B.Sharmila et al.,(2021),“Detecting Group Shilling Attacks In Online Recommender Systems”,journal of engineering science, Vol 12, Issue 05.
[8] Fuzhi Zhang et al(2020), “Graph embedding-based approach for detecting group shilling attacks in collaborative recommender systems”, Elsevier Knowledge-Based Systems.
[9] T. L. Ngo-Ye et al(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.
[10] D. Jiaetal.,(2012), “A user preference based automatic potential group generation method for social media sharing and recommendation,” (in Chinese) JisuanjiXuebao, vol. 35, no. 11, pp. 2382–2391.
[11] F. Zhang et al(2018), “UD-HMM: An unsupervised method for shilling attack detection based on hidden Markov model and hierarchical clustering,” Knowl.-Based Syst., vol. 148, pp. 146–166.
[12] M. Gao et al(2015), “Item anomaly detection based on dynamic partition for time series in recommender systems,” PLoS ONE, vol. 10, no. 8.
[13] C. A. Williamsetal(2007), “Defending recommender systems: Detection of profile injection attacks,” Service Oriented Comput. Appl., vol. 1, no. 3, pp. 157–170.
[14] Z. Wang et al(2018), “Graph-based review spammer group detection,” Knowl. Inf. Syst., vol. 55, no. 3, pp. 571–597.
[15] Mukhtar, A., Mehta, H. R., Abirami, S., & Adi, S. (2022), “Mood Based Music Recommendation for a Mall using Real-time Image”, Journal of Positive School Psychology, 6(3), 2975-2981.
[16] Malarvizhi, A. (2022),“An assessment of data mining technique’s reliability in predicting social media sentiments”, Journal of Positive School Psychology, 7254-7263.
[17] Dr.M.S.Bhuvaneswar et.al.,(2021) "A Parallel Approach for Web Session Identification to make Recommendation Efficient" International Journal of Business Intelligence and Data Mining Vol.19, Issue.2, pp.189-213.