2022 International Conference on Inventive Computation Technologies (ICICT) | 978-1-6654-0837-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICICT54344.2022.9850464

Shilling Attack Detection System for Online Recommenders

[1]Dr. J. R.V. Jeny, [2]R. Sowmya, [3]G. Sai Kiran, [4]M. Kiran Babu, [5]Ch. Arjun,
[1]Professor, [2,3,4,5]UG Student
[1,2,3,4,5]Department of Computer Science and Engineering
[1]jeny.navagar18@gmail.com
Vignan Institute of Technology and Science, Deshmukhi (v), Hyderabad

Abstract- The shilling attack detection methods or approaches that are previously proposed keep emphasis on identifying the shillers or the attackers that act individually. There is a lack of focus on the attackers or shillers that act as a group. A shilling attack is an attack in which fake profiles are injected. When such profiles are present in an online recommendation system, the output that is generated by the online recommendation system will be biased. This results in inaccuracy of the online recommendation system. Here, we are proposing a shilling attack detection system in which we can not only identify individual shillers but also group shillers. In this system, the candidate groups are generated with an interval of time and are then grouped according to a degree called group suspicion degree. Then by making use of the DBSCAN algorithm and clustering of the groups which are suspicious is done. These groups are the shilling groups.

Index Terms- DBSCAN clustering algorithm, Detecting Group Shilling attacks, Group Shilling attacks, Recommender System, Online recommendation system.

I. INTRODUCTION

Now a days there is a lot of information which is online and there comes the serious issue of information overload [1]. The recommendations that are made by online recommender systems for their users, which makes it easy for the user to choose among the abundant amount of data. But these online recommender systems are vulnerable to many attacks, one of them being shilling attacks. The Shilling attacks take place when, attackers attach a large-amount of profiles also called as attacking profiles, to affect or change the recommendation of the recommender system [3], [4]. Shilling attacks of two kinds mainly the push and the nuke attacks, which are used for the promotion or demotion of any item which is being targeted, respectively [5]. The shilling attacks that are well-known over many researches such as random [6],[7]and many more attacks. But even attackers that form as a group can also make a planned attack. These kind of shilling behaviours are called as group shilling attacks. These kinds of attacks are more dangerous than any other type of attacks of shilling [8]. So, the issue of identifying these attacks and solve them efficiently has to be addressed.

Over the past decade many studies have been conducted regarding the identification of the shilling attacks. But these studies only focus on the individual attackers. But shilling can be both individual and a group attack. When only individual attackers are identified, all of the shilling profiles are not identified. That means the group of shilling attackers working together cannot be identified. They individually don't seem to be suspicious.

They can easily pass through and not be identified as shilling profiles. So, this does not ensure complete reliability of the system of recommendation that is being used. Hence, we put forth a methodology for detection of group shilling attacks, which not only identifies the individual attackers but also group attacks. In this project we use DBSCAN clustering algorithm.

The approach that is proposed makes use of the time intervals of attacking shilling groups and it efficiently detects the shilling profiles with similarity. This can be done as follows

1) We use a method in which candidate groups are made. These groups are generated based on the time interval. We use this because, if the

attackers want to target a particular item, they must rate it in a particular interval of time. Hence, we obtain the groups in this step.

2) After obtaining the groups mentioned in the first step, we calculate the activity of the user. This is calculated to see if the behaviour of the user is suspicious. Then after obtaining the degree of suspicion based on the above calculated factors, we make use of the DBSCAN algorithm of clustering for finding the groups of shilling profiles. DBSCAN algorithm works by clustering the data on the basis of density. DBSCAN clustering algorithm proceeds efficiently even when the data is of different shapes and sizes and also deals with the data containing outliers and noise. DBSCAN calculates the number of clusters based on the data automatically without the need of specifying the number of clusters that need to be formed. The points of close distance are considered to be in a cluster.

II. RELATED WORK

The internet consists of large amount of data that is continuously changed, which makes it very much difficult to the users to find the information that is useful to them. The data can be very confidential such as personal data, health profiles etc. Many machine learning techniques are used for identifying these diseases using this important data [14] and even for many other recognition purposes [15]. The data regarding the customer can also be sued in real time for many purposes [17] [18]. Hence the security of that data is also very important [13]. Recommendation System, is a system which filters the information and is widely used by online marketers and sellers to give accurate suggestions according to the requirements of the users [9] [16]. These sellers often use e-commerce websites as their medium and use it for easy marketing [19]. Collaborative filtering is the type of recommendation system the is used most of the time. But unfortunately, it is highly prone to shillers. These kinds of attacks affect the recommendation system for the promotion or demotion of an item of their choice. Various models of attacks and the techniques to detect them have been developed to reduce the problem. With the increasing use of the world wide web social media platforms, reviews given by the customers online act as crucial factors in obtaining meaningful information, promoting an e-commerce market or increase sales. The large number of reviews that are given by the customer about any product lead to a lot of confusion and huge burden to go through each and every review. Hence, it is really important to design a system that solves the above problem and assists in going through the reviews according to the interests of the customers. The Social media applications are becoming the main part of the Web application [10]. The content that is generated by the users which is user specific is also very important. Sharing of data and the approaches used for recommendation are important in dealing with the problem of information overload in the online/web environment. Here, the analyzing the flaws of current group-based information sharing mechanism and the common problem of traditional recommender approaches, and here is an ideal approach of group automatic generating for social media sharing and recommendation. Fraud detection also plays a vital role in this area [12]. The essential idea of this approach is that we switch user's preference from the media objects to the interest elements which media objects imply. Then we gather the users who have common preference, namely users have the same interestingness in a set of interest elements, together as Common Preference Group (CPG) [11]. We also propose a new social media data sharing and recommendation system architecture based on CPG and designs a CPG automatic mining algorithm. By compare our CPG mining algorithm with other algorithm which has similar functionality, it is shown that our algorithm could be applicable to real social media application with massive users.

III. IMPLEMENTATION

In *Dual view* module we eliminate the profiles that have dual view reviews. Reviews are said to be dual viewed if the heading and the body of the review have different sentiment (positive, negative, neutral).

In *Targeted promotion or demotion* module we consider the profiles to be shilling profiles if they are continuously posting negative or positive about a particular item.

In *Many profiles with same ip address* module we verify if there are many profiles and are used on same Ip address. Such profiles are considered to be shilling profiles.

In *Flooding reviews with same profile* module, many reviews from the same profile on the same day with same sentiment (positive, negative) are to be eliminated. So, we consider them to be shilling profiles. Here by the activity of the user we can know if they are genuine or shilling.

In *Flooding reviews with different profiles but same ip* module, many reviews are from different profiles on the same day with same sentiment (positive, negative) but from same Ip address are considered to be shilling profiles.

In *Similar pattern* module, reviews that are posted from different profiles pattern is considered to be shilling profiles.

In *Irrelevant reviews* module, the reviews in which the reviewer is writing his own story.

In *Group shilling profiles* module, using DBSCAN algorithm we remove all the group shilling profiles.

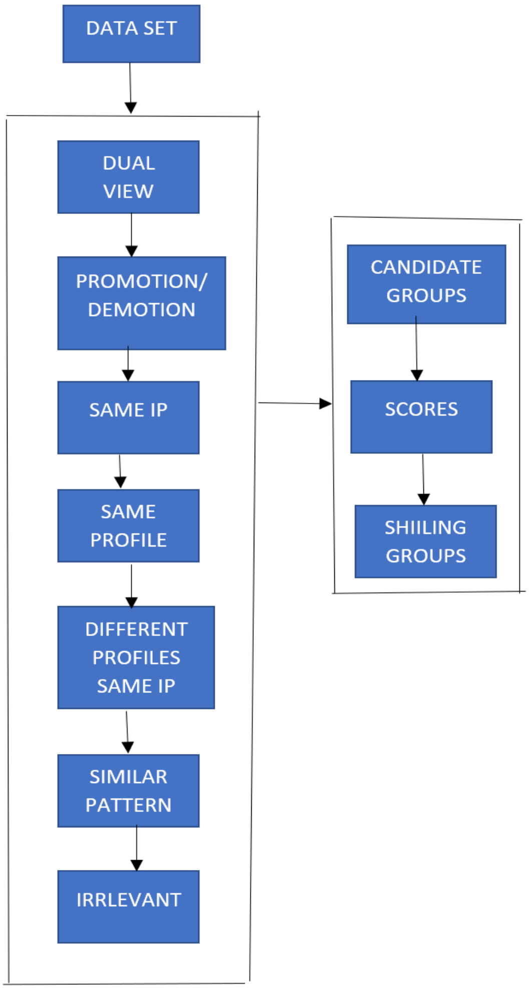

Fig.1 Process Flow

The Fig 1 shows the data passes through each of the modules. When the data is passed, according to the rules that are present in each module, some of the profiles are deemed to be shilling profiles.

When we use the group shilling module, according to the time and the activity of the user that is calculated in the previous steps, the profiles are clustered into groups. Here, as we are using the DBSCAN algorithm there is no need to calculate or determine any value of the clusters. Depending on calculated data's density, the clusters are formed.

IV. EXPERIMENTAL RESULTS

The following are the experimental results of our model. Here the shilling profiles are detected. And the reviews that are posted via these shilling accounts are removed. The reviews from these accounts are deemed non-credible. These shilling profiles could be either individual shilling profiles or group shilling profiles. This is the sample of the execution of our model. We consider a dataset. Here, the dataset is from Amazon reviews. Here the considered sample dataset consists of 26 Amazon reviews. These Amazon reviews are stored in Microsoft Excel file. We input these reviews to our program directly. The output of this program will be another Excel file.

This Excel file consists of the reviews which are deemed credible. That means the reviews are from the genuine users.

The reviews from the shilling profiles are removed. Only a set of genuine reviews are obtained.

We took the original sample dataset consisting of the 26 Amazon reviews. The output file is obtained after running the program. Hence, it consists of the genuine reviews. With the help of this any online recommendation system can be improved. All the non-credible reviews that means the reviews from shillers can be removed and this results in the improvement of the online recommendation system.

Here in this system, that we have proposed we conducted experiments many times and found out that the algorithm that we are using for detecting the shilling profiles is working well.

Table 1. Experimental Values of SADS

No. of Record s	No. of Shillin g profiles	No. of genuin e profiles	Shilling profiles detecte d by SADS	Genuin e profiles after running SADS
10	3	7	2	8
40	13	27	10	30
60	25	35	18	42
100	37	63	37	63
150	50	100	41	109
500	227	273	230	270

By using the above experimental data obtained, we calculate the accuracy of the SADS.

$$Accuracy = \frac{CS + CG}{CS + CG + WS + WG}$$

Where,

CS is Correctly identified shilling profiles

CG is Correctly identified genuine profiles

WS is Wrongly identified shilling profiles

WG is Wrongly identified genuine profiles

Table 2. Accuracy of SADS

No. of records taken	Accuracy Percentage
10	81.81
40	86.04
60	79.10
100	100
150	88.67
500	98.80

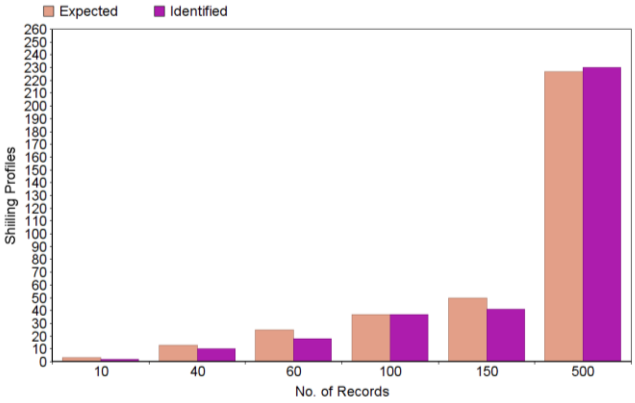

Fig. 2. Graph of expected values and SADS

The Fig 2 shows the extent to which the SADS was able to detect the shilling profiles when compared with the expected results.

The Accuracy of the SADS according to the experimental results is 89.07.

So, the system efficiently identifies the shilling profiles from the data which is given to the system. This is the data from the online recommender systems. This helps in the efficient functioning of the online recommender systems.

V. CONCLUSION

Group shilling attacks are being common these days. These attacks can be very disadvantageous to the systems which make recommendations to us. Hence, the detection of these attacks is very important. In this paper, the approach proposed by us which is based on DBSCAN ++ algorithm detects these group shilling attacks. We calculate and make use of the suspicion degree to cluster out the shilling attack groups. So, by the detection of these shilling attack groups, we can improve the performance of the online recommendation system. With this, we achieve the goal of protecting the integrity of the online recommender systems, without compromising on anything. Hence we have an efficient SADS [Shilling Attack Detection System].

REFERENCES

[1]. Sundar, A.P., Li, F., Zou, X., Gao, T. and Russomanno, E.D., 2020. Understanding shilling attacks and their detection traits: A comprehensive survey. *IEEE Access*, *8*, pp.171703-171715.

[2]. Ngo-Ye, T.L. and Sinha, A.P., 2012. Analyzing online review helpfulness using a Regressional ReliefF-enhanced text mining method. *ACM Transactions on Management Information Systems (TMIS)*, *3*(2), pp.1-20.

[3]. Jia, Da-Wen, Cheng Zeng, Zhi-Yong Peng, Peng Cheng, Zhi-Min Yang, and Zhou Lu. "A user preference based automatic

[6]. Jeny, J. R. V., Reddy, N. S., & Aishwarya, P. (2021, October). A Classification Approach for Heart Disease Diagnosis using Machine Learning. In *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 456-459). IEEE.

[7]. J. Prince Antony Joel, R. Joshua Samuel Raj and N. Muthukumaran, "Review on Gait Rehabilitation Training Using Human Adaptive Mechatronics System in Biomedical Engineering," 2022 International Conference on Computer Communication and Informatics, pp. 1-5, 2022.

[8]. Jeny, J. R. V., Anjana, A., Monica, K., Sumanth, T., & Mamatha, A. (2021, June). Hand Gesture Recognition for Sign Language Using Convolutional Neural Network. In *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 1713-1721). IEEE.

[9]. S Amutha, S S Vinsley, "Phase-based frame interpolation method for videos with high accuracy using odd frames", Int. J. Biomedical Engineering and Technology, Vol. 33, No. 3, 2020 .

[10]. R. Nafeena Abdul Munaf, K. Karthikeyan, S. Joe Patrick Gnanaraj, T.A. Sivakumar, N. Muthukumaran, "An ML Approach for Household Power Consumption," 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), 2022, pp. 784-791.

[11]. J. Prince Antony Joel, R. Joshua Samuel Raj and N. Muthukumaran, "Cognitive and Cybernetics based Human Adaptive Mechatronics System in Gait Rehabilitation Therapy," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, March 2021, pp. 516-521.

[12]. S. Anantha Babu, R. Joshua Samuel Raj, Arul Xavier V.M and N. Muthukumaran, "DCT based Enhanced Tchebichef

potential group generation method for social media sharing and recommendation." *Jisuanji Xuebao(Chinese Journal of Computers)* 35, no. 11 (2012): 2381-2391.

[4]. Jeny, J. R. V., & Joshi, C. A. (2013). Flexible Data Streaming In Stream Cloud. *International Journal of Innovative Research in Science, Engineering and Technology*, *2*(4), 1127-1131.

[5]. Yogita Gunjal, J.Rethna Virgil Jeny, "Data Security And Integrity Of Cloud Storage In Cloud Computing", *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 2, Issue 4, April 2013, ISSN: 2319-8753, pp:1166-1170.

Moment using Huffman Encoding Algorithm (ETMH)," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, March 2021, pp. 522-527.

[13]. Jeny, J. R. V., Shraddha, B., Ashritha, B., Sai, D. S., & Naveen, M. (2021, June). Deep Learning Framework for Face Mask Detection. In *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 1705-1712). IEEE

[14]. Sekaran, K., Chandana, P., Jeny, J. R. V., Meqdad, M. N., & Kadry, S. (2020). Design of optimal search engine using text summarization through artificial intelligence techniques. *Telkomnika*, *18*(3), 1268-1274.

[15]. Gautham A Nagendran, Harshmeet Singh, R Joshua Samuel Raj and N. Muthukumaran, "Input Assistive Keyboards for People with Disabilities: A Survey," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, March 2021, pp. 829-832.

[16]. Joshua Samuel Raj. R, M. A. Sreema, Sudarson Rama Perumal T, Muthukumaran N, "A Low Complex and Scalable Reconfigurable Simulation for Orthogonal Approximation using DCT," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 541-545.

[17]. Dr.J.Rethna Virgil Jeny, *A Framework for Dynamic Facet Ordering Search in E-commerce*, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3, issue 8, November-December 2018, ISSN: 2456-3307.