International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025

Research Paper

DETECTING GROUP SHILLING ATTACKS IN ONLINE RECOMMENDER SYSTEMS BASED ON BISECTING K-MEANS CLUSTERING

[1] K.ANUKSHIT KRISHNA,[2] B.SAI SANTHOSH,[3] A. PRABHAS GOUD,[4] K. SHIVA KRISHNA,[5] Dr. J. PRAVEEN KUMAR
[1234] Students, [5] Associate Professor
Department Of Computer Science and Design
Teegala Krishna Reddy Engineering College, Meerpet, Balapur, Hyderabad-500097

ABSTRACT

Existing shilling attack detection approaches focus mainly on identifying individual attackers in online recommender systems and rarely address the detection of group shilling attacks in which a group of attackers colludes to bias the output of an online recommender system by injecting fake profiles. In this article, we propose a group shilling attack detection method based on the bisecting K-means clustering algorithm. First, we extract the rating track of each item and divide the rating tracks to generate candidate groups according to a fixed time interval. Second, we propose item attention degree and user activity to calculate the suspicious degrees of candidate groups. Finally, we employ the bisecting K-means algorithm to cluster the candidate groups according to their suspicious degrees and obtain the attack groups. The results of experiments on the Netflix and Amazon data sets indicate that the proposed method outperforms the baseline methods.

Received: 10-7-2025 Accepted: 18-8-2025 Published: 25-8-2025

I. INTRODUCTION

With the explosive growth of online information, the phenomenon of information overload becomes a key issue. Online recommender systems make recommendations for their users, which can alleviate the information overload problem to some extent. However, the online recommender systems are vulnerable to shilling attacks in which attackers inject a large number of attack profiles to bias the output of the recommender system, . Shilling attacks can be divided into push attacks and nuke attacks, which are used for promoting and demoting target items (e.g., movies or products) to be recommended, respectively. The well-studied shilling attacks include random attack, average attack, bandwagon attack, reverse bandwagon attack, average- target shift attack, average-noise injecting attack, and so on. In these attacks, attackers usually separately inject attack profiles into recommender systems. In fact, a group of attackers might collude to make a tactical attack. Such shilling behaviors have been termed group shilling attacks, which are more threatening to the system than traditional shilling attacks. Therefore, how to effectively identify group shilling attacks has become a key issue needed to be addressed.

1.1 Motivation

With the rapid expansion of online platforms, users often experience information overload, making recommender systems essential for guiding them to relevant content. However, these systems are increasingly targeted by shilling attacks, where malicious users inject fake profiles to manipulate recommendations, either boosting or demoting certain items. While much research has focused on detecting individual attackers, group shilling attacks, where multiple attackers collaborate to deceive the system, pose a greater threat due to their coordinated behavior. Identifying and mitigating these group-based attacks is crucial

to preserving the trustworthiness and effectiveness of online recommendation platforms. This project is motivated by the need to develop a more robust detection mechanism that can effectively recognize and counteract the sophisticated strategies employed in group shilling attacks.

1.2 Problem Statement

Online recommender systems are highly susceptible to manipulation through shilling attacks, where attackers inject fraudulent user profiles to influence the system's suggestions. While traditional detection methods mainly focus on identifying individual attackers, they fall short when dealing with group shilling attacks, where multiple attackers coordinate their actions to mimic normal user behavior. This coordination makes the detection process far more challenging, leading to decreased precision and recall rates in existing solutions. There is an urgent need for an effective approach that can accurately detect and separate these attack groups without relying solely on profile similarity, as attackers often introduce significant diversity in their fake profiles to evade detection. The goal of this project is to address these challenges and develop a reliable method capable of uncovering group shilling activities in large-scale online recommendation environments.

1.3 Scope and Objective Scope:

This project is focused on enhancing the security and reliability of online recommender systems by detecting group shilling attacks—a form of coordinated profile injection that manipulates recommendation results. The work encompasses analyzing user rating behavior over time, forming candidate user groups based on temporal patterns, and evaluating their likelihood of being attackers. It is applicable to various recommendation platforms, such as e-commerce and streaming services, where trust in suggestions is critical. The solution is designed to be scalable, allowing integration with large datasets like those from Netflix or Amazon.

Objective:

The primary objective of this project is to design and implement an effective method for detecting group shilling attacks using the bisecting K-means clustering algorithm. This involves:

- Extracting and organizing rating data based on user activity over specific time intervals.
- Computing metrics like item attention and user activity to assess the suspiciousness of user groups.
- Clustering these groups to accurately isolate those exhibiting coordinated shilling behavior.
- Evaluating the method against established datasets and comparing its performance with existing techniques..

II. LITERATURE SURVEY

Feng Li designed a framework that systematically analyzed various shilling attacks and their detection mechanisms in collaborative filtering recommender systems. His system emphasized identifying key traits in injected profiles to enhance detection accuracy. The study provided a classification of attack models and detection attributes, helping to lay the groundwork for building more robust defenses against profile injection attacks.

Thomas Ngo-Ye developed a system that utilized Regressional ReliefF-enhanced text mining techniques to assess the helpfulness of online reviews. By selecting meaningful features from customer reviews and applying regression models, his system successfully identified influential reviews, thus improving information filtering in e- commerce platforms.

Da-Wen Jia, Cheng Zeng, Zhi-Yong Peng, and Peng Cheng proposed an automatic group generation method based on users' shared interests in social media platforms. Their system focused on clustering users who displayed similar preferences toward content elements, forming Common Preference Groups (CPGs) for efficient content sharing and recommendation.

Su et al. introduced the concept of group shilling attacks, highlighting two main scenarios where attackers either mixed biased ratings with normal behavior or collaborated through organized gray groups to target multiple items. Their work emphasized the complexity and threat level of group-based manipulations in recommendation systems.

Bryan Mehta and Wolfgang Nejdl proposed an unsupervised strategy for detecting shilling attacks by applying principal component analysis (PCA) on user rating profiles. Their system identified anomalous profiles based on their deviation from the normal user behavior, enabling early detection without the need for labeled training data.

Wang et al. developed a group shilling attack detection system that enhanced traditional individual attack detection features. Their method ranked candidate groups using principal component analysis after manually labeling groups with high minimum support, successfully identifying collusive attacks with high similarity among attackers.

Williams, Mobasher, and Burke created a detection system that analyzed the obfuscation tactics used in shilling attacks. Their approach relied on clustering techniques to identify hidden attack profiles and proposed methods to enhance recommender system resilience through robustness against sophisticated attackers.

EXISTING SYSTEM

To cover recommender systems, colorful approaches have been presented to descry shilling attacks over the once decade. still, these approaches concentrate substantially on detecting individual bushwhackers in recommender systems and infrequently consider the collusive shilling actions among bushwhackers. Although some approaches have been proposed to descry shilling actions at the group position, they divide seeker groups and identify attack groups according to profile similarity. There are some group attack models that can induce attack biographies with great diversity. As a result, these approaches cannot completely decrease attack groups, which beget poor perfection and recall. lately, some approaches have been presented to decrease spammer groups in review websites. still, the group shilling attacks in recommender systems are different from the spammer groups in review websites. thus, the spammer group discovery approaches aren't applicable to the discovery of group shilling attacks.

PROPOSED SYSTEM

To overcome the abovementioned limitations, we propose a system to descry group shilling attacks in online recommender systems through intersecting K- means clustering. The proposed approach takes advantage of the time attention characteristics of group shilling attacks, which has a better performance in detecting group attacks with collusive shilling actions. The major benefits of this composition are listed as follows. We propose a seeker group division system, which first mines the standing tracks of particulars and also divides the druggies in the point standing tracks(Its) into multiple groups according to a certain length of time. Since the bushwhackers in an attack group must rate the target point(s) within a certain period, the proposed seeker group division system is more likely to divide the bushwhackers in an attack group together, which can lie a good foundation for the group shilling attack discovery. We propose criteria of point attention degree and stoner exertion(UA) to dissect the seeker groups, making the judgment of attack groups more accurate. Grounded on the divided seeker groups, the point attention degree and the UA for each seeker group are calculated, and the suspicious degrees of these groups are attained. Grounded on this, the intersecting K-means algorithm is employed to cluster the seeker groups according to their suspicious degrees, and the attack groups are attained. To estimate the performance of our system, we conduct trials on the Netflix and Amazon data sets and compare the proposed system with four birth styles.

III. MODULE DESCRIPTION

The proposed system is structured into the following key modules, each contributing to

the detection of group shilling attacks in online recommender systems:

Candidate Group Division Module

This module scans each item's rating history and segments users into groups based on rating timestamps. Users who rate the same item within a predefined time interval are placed into the same candidate group. This approach captures the time-synchronized behavior often seen in coordinated attacks

Feature Extraction and Suspicion Scoring Module

Each candidate group is analyzed using two custom metrics:

Item Attention Degree (IAD): Evaluates how frequently an item is rated across groups, indicating its visibility or potential targeting.

User Activity (UA): Measures how active group members are during the rating window. These features are combined to calculate a suspicion score for each group.

Clustering and Attack Detection Module

Using the suspicion scores as input, this module applies the bisecting K-means algorithm to cluster candidate groups. Clusters with significantly high average suspicion scores are flagged as potential attack groups. This unsupervised clustering approach allows for the detection of previously unseen attack patterns.

Result Evaluation and Output Module

This final module cross-verifies the detected groups against known metrics like precision and recall. The results are then output for further action—such as filtering, alerting admins, or improving recommendation trust.

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE

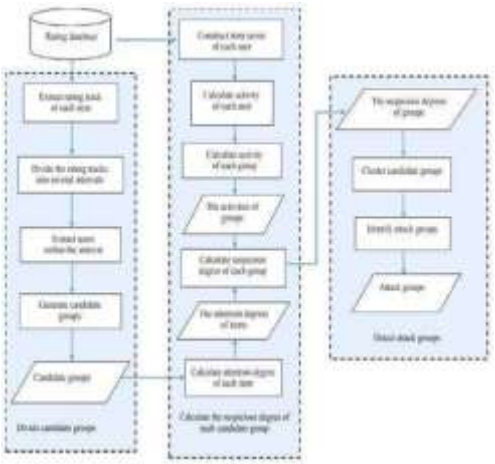

Fig. System Architecture

V. OUTPUT SCREENS

Fig : Registration

Fig : Login

Fig : Admin Add Product

Fig : Admin View Products

Fig : Admin Manage Products

Fig : Admin View Transactions

Fig : User Search Products

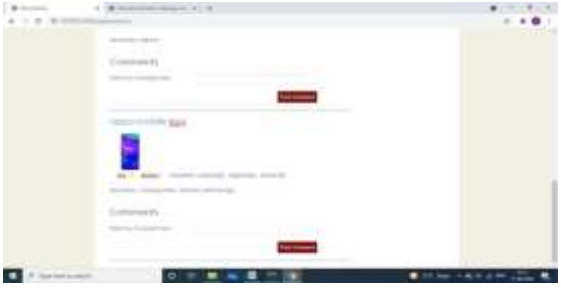

Fig : User Buy Products

Fig : User Buy Product

Fig : User View Transactions

Fig : Database Admin Login

Fig : Database Tables

VI. CONCLUSION

Group shilling attacks are a great threat to recommender systems. To detect such attacks, we propose a group attack detection model based on the bisecting K-means algorithm. The proposed detection model can overcome the problem that the performance is poor when attackers have a few curated items. In order to divide candidate groups, we use the fixed time length and dynamically select the

starting time point to divide each item's rating track. We combine the features of items and users to calculate the GSDs. Based on the GSDs, the bisecting K-means algorithm is utilized to identify attack groups from the candidate groups. The experimental results on two data sets illustrate the effectiveness of our method.

REFERENCE

1. T. L. Ngo-Ye and A. P. Sinha, "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, Jul. 2012.
2. B Kundan, Sangaralingam P. Combining Machine Learning and Deep Learning in the Retinopathy Diagnostic Algorithm for Enhanced Detection of DR and DME. J Neonatal Surg [Internet]. 2025Apr.2 [cited 2025Apr.9];14(5):128-40. Available from: https://www.jneonatalsurg.com/index.php/jns/article/view/2914.
3. I. Gunes, C. Kaleli, A. Bilge, and H. Polat, "Shilling attacks against recommender systems: A comprehensive survey," Artif. Intell. Rev., vol. 42, no. 4, pp. 767–799, Dec. 2014.
4. S. K. Lam and J. Riedl, "Shilling recommender systems for fun and profit," in Proc. 13th Conf. World Wide Web WWW, 2004, pp. 393–402.
5. B. Mobasher, R. Burke, R. Bhaumik, and J. J. Sandvig, "Attacks and remedies in collaborative recommendation," IEEE Intell. Syst., vol. 22, no. 3,pp. 56–63, May 2007.
6. B. Mobasher, R. Burke, R. Bhaumik, and C. Williams, "Toward trustworthy recommender systems: An analysis of attack models and algorithm robustness," ACM Trans. Internet Technol., vol. 7, no. 4, p. 23, Oct. 2007.
7. C. Williams, B. Mobasher, R. Burke, J. Sandvig, and R. Bhaumik, "Detection of obfuscated attacks in collaborative recommender systems," in Proc. 17th Eur. Conf. Artif. Intell., 2006, pp. 19–23.
8. X.-F. Su, H.-J. Zeng, and Z. Chen, "Finding group shilling in recommendation system," in Proc. Special Interest Tracks Posters 14th Int. Conf. World Wide Web WWW, 2005, pp. 960–961.
9. R. Burke, B. Mobasher, C. Williams, and R. Bhaumik, "Classification features for attack detection in collaborative recommender systems," in Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining KDD, 2006, pp. 542–547.
10. Y. Wang, Z. Wu, J. Cao, and C. Fang, "Towards a tricksy group shilling attack model against recommender systems," in Proc. 8th Int. Conf. Adv. Data Min. Appl., Nanjing, China, 2012, pp. 675–688.
11. K. Murugesan and J. Zhang, "Hybrid bisect K-Means clustering algorithm," in Proc. Int. Conf. Bus. Comput. Global Informatization, Jul. 2011, pp. 216–219.
12. C. A. Williams, B. Mobasher, and R. Burke, "Defending recommender systems: Detection of profile injection attacks," Service Oriented Comput. Appl., vol. 1, no. 3,pp. 157–170, Oct. 2007.
13. W. Zhou, J. Wen, Q. Xiong, M. Gao, and J. Zeng, "SVM-TIA a shilling attack detection method based on SVM and target item analysis in recommender systems," Neurocomputing, vol. 210, pp. 197–205, Oct. 2016.
14. W. Li, M. Gao, H. Li, Q. Xiong, J. Wen, and B. Ling, "An shilling

attack detection algorithm based on popularity degree features," (in Chinese) Acta Automatica Sinica, vol. 41, no. 9, pp. 1563–1575, Sep. 2015.

15. B. Mehta and W. Nejdl, "Unsupervised strategies for shilling detection and robust collaborative filtering," User Model. User-Adapted Interact., vol. 19, nos. 1–2, pp. 65– 97, Feb. 2009.