Detecting Group Shilling Attacks In Online Recommender Systems Based on Bisecting K-Means Clustering

Dr. P. D. R. Vijayakumar[1], Jamal veve.M[2], Umar farook. P[3], Ashok kumar. A[4], Jeeva. M[5]

[1]HOD, Dept of Computer Science Engineering
[2, 3, 4, 5]Dept of Computer Science Engineering
[1, 2, 3, 4, 5]Kovilpalayam, Sarkar Samakulam, Coimbatore.

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.*

Keywords- K-means, suspicious degrees, clustering algorithm

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, band- wagon 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.

To protect recommender systems, various approaches have been presented to detect shilling attacks over the past decade. However, these approaches focus mainly on detecting individual attackers in recommender systems and rarely consider the collusive shilling behaviors among attackers. Although some approaches have been proposed to detect shilling behaviors at the group level, they divide candidate groups and identify attack groups according to profile similarity. There are some group attack models that can generate attack profiles with great diversity. As a result, these approaches cannot fully detect attack groups, which causes poor precision and recall. Recently, some approaches have been presented to detect spammer groups in review websites. However, the group shilling attacks in recommender systems are different from the spammer groups in review websites. Therefore, the spammer group detection approaches are not applicable to the detection of group shilling attacks.

II. LITERATURE REVIEW

Shuo Qiu, Student Member, IEEE, Boyang Wang, Ming Li, Member, IEEE, Jiqiang Liu, and Yanfeng Shi, **“Toward Practical Privacy-Preserving Frequent Itemset Mining on Encrypted Cloud Data”**, IEEE Transactions on Cloud Computing, 2020. In this project, group shilling attack detection can be achieved based on bisecting K-means clustering algorithm. Time based manipulation is the base idea – 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. Experiments on the Netflix and Amazon data sets with the algorithm implementation indicate that the proposed method outperforms the baseline methods." Fake reviews and ratings becomes annoying forever in the user perspective and in the field of consumer utilization. Some users crate and inject fake user profiles consisting of biased ratings which affects the recommendation ranking and manipulate the user's decision. Attacks on recommender system behaviour is known as a "shilling" attack or "profile injection" attack. The fake Users involved in shilling attacks were coined as shillers. Existing shilling attack detection doesn't have a clear approach 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.

Cai, Hongyun; Zhang, Fuzhi " **An Unsupervised Approach for Detecting Group Shilling Attacks in Recommender Systems Based on Topological Potential and Group Behaviour Features**.", Security & Communication Networks . 9/27/2021, p1-18. 18p. First, we construct a weighted user relationship graph by combining direct and indirect collusive degrees between users. Second, we find all dense sub graphs in the user relationship graph to generate a set of suspicious groups by introducing a topological potential method. Finally, we use a clustering method to detect shilling groups by extracting group behaviour features. Extensive experiments on the Netflix and sampled Amazon review datasets show that the proposed approach is effective for detecting group shilling attacks in recommender systems, and the F1-measure on two datasets can reach over 99 percent and 76 percent, respectively. To protect recommender systems against shilling attacks, a variety of detection methods have been proposed over the past decade. However, these methods focus mainly on individual features and rarely consider the lockstep behaviours among attack users, which suffer from low precision in detecting group shilling attacks. In this work, we propose a three-stage detection method based on strong lockstep behaviours among group members and group behaviour features for detecting group shilling attacks.

M. Si and Q. Li, **"Shilling attacks against collaborative recommender systems: a review,"** Artificial Intelligence Review, vol. 53, no. 1, pp. 291–319, 2020. Due to their popularity and importance, we survey about shilling attacks in CFRSs. We first briefly discuss the related survey papers about shilling attacks and analyze their deficiencies to illustrate the necessity of this paper. Next we give an overall picture about various shilling attack types and their deployment modes. Then we explain profile injection attack strategies, shilling attack detection schemes and robust recommendation algorithms proposed so far in detail. Moreover, we briefly explain evaluation metrics of the proposed schemes. Last, we discuss some research directions to improve shilling attack detection rates robustness of collaborative recommendation, and conclude this paper. Collaborative filtering recommender systems (CFRSs) have already been proved effective to cope with the information overload problem since they merged in the past two decades. However, CFRSs are highly vulnerable to shilling or profile injection attacks since their openness. Ratings injected by malicious users seriously affect the authenticity of the recommendations as well as users' trustiness in the recommendation systems. In the past two decades, various studies have been conducted to scrutinize different profile injection attack strategies, shilling attack detection schemes, robust recommendation algorithms, and to evaluate them with respect to accuracy and robustness.

A. M. Turk and A. Bilge, **"Robustness analysis of multi-criteria collaborative filtering algorithms against shilling attacks,"** Expert Systems with Applications, vol. 115, pp. 386–402, 2019. Nowadays there is a growing research area focused on the design of robust machine learning methods to neutralize malicious profiles inserted into the system. This paper proposes an innovative robust method, based on matrix factorization, to neutralize shilling attacks. Our method obtains the reliability value associated to each prediction of a user to an item. Monitoring unusual reliability variations in the items prediction we can avoid promoting shilling predictions to erroneous recommendations. This paper open provides more than thirteen thousand individual experiments involving a wide range of attack strategies, both push and nuke, in order to test the proposed approach. Results show that the proposed method is able to neutralize most of the existing attacks; its performance only decreases in the not relevant situations: when the attack size is not large enough to affect effectively the recommendations provided by the system. As the use of recommender systems becomes generalized in society, the interest in varying the orientation of their recommendations increases. There are Shilling attacks strategies that introduce malicious profiles in collaborative filtering recommender systems in order to promote the own products or services, or to discredit those of the competition. Academic research against shilling attacks has been focused in statistical approaches to detect unusual patterns in user ratings.

K. Vivekanandan and N. Praveena, **"Hybrid convolutional neural network (CNN) and long-short term memory (LSTM) based deep learning model for detecting shilling attack in the social-aware network,"** Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 1, pp. 1197–1210, 2021. In this paper, a hybrid convolutional neural network (CNN) and long-short term memory (LSTM)-based deep learning model (CNN–LSTM) is proposed for detecting shilling attack in recommender systems. This deep learning model utilizes the transformed network architecture for exploiting the deep-level attributes derived from user rated profiles. It overcomes the limitations of the existing shilling attack detection methods which mostly focuses on identifying spam users by designing features artificially in order to enhance their efficiency and robustness. It is also potent in elucidating deep-level features for efficiently detecting shilling attacks by accurately elaborating the user ratings. The experimental results confirmed the significance of the proposed CNN–LSTM approach by accurately detecting most of the obfuscated attacks compared to the state-of-art algorithms used for investigation. In social aware network (SAN) paradigm, the fundamental activities concentrate on exploring the behavior and attributes of the users. This investigation of user characteristic aids in the design of highly efficient and suitable protocols. In particular, the shilling attack introduces a high degree of vulnerability into the recommender systems. The shilling attackers use the reviews, user ratings and forged user generated content data for the computation of recommendation rankings. The detection of shilling attack in recommender systems is considered to be essential for sustaining their fairness and reliability. In specific, the collaborative filtering strategies utilized for detecting shilling attackers through efficient user behavior mining are considered as the predominant methodologies in the literature.

Z. Wu, J. Cao, Y. Wang, Y. Wang, L. Zhang, and J. Wu,
“hPSD: a hybrid PU-Learning-Based spammer detection
model for product reviews,” IEEE Transactions on Cybernetics,
vol. 50, no. 4, pp. 1595–1606, 2020

Z. Wu, J. Cao, Y. Wang, Y. Wang, L. Zhang, and J. Wu**, “hPSD: a hybrid PU-Learning-Based spammer detection model for product reviews,”** IEEE Transactions on Cybernetics, vol. 50, no. 4, pp. 1595–1606, 2020. In this paper, we propose a hybrid semi supervised learning model titled hybrid PU-learning-based spammer detection (hPSD) for spammer detection to leverage both the users' characteristics and the user-product relations. Specifically, the hPSD model can iteratively detect multi type spammers by injecting different positive samples, and allows the construction of classifiers in a semi supervised hybrid learning framework. Comprehensive experiments on movie dataset with shilling injection confirm the superior performance of hPSD over existing baseline methods. The hPSD is then utilized to detect the hidden spammers from real-life Amazon data. A set of spammers and their underlying employers (e.g., book publishers) are successfully discovered and validated.

III. EXISTING SYSTEM

The existing system is developed to identify attacks from individual users of the recommendation system. The existing system is designed such a way that it is useful for finding attacks from individual users to alleviate the results produced by the recommendation system. But in recent time, groups of users work on to alleviate the results of the recommendation system. So the existing system is not sufficient enough to detect such attacks. So we need a new system that detects the group shilling attacks in the recommender system.

IV. PROPOSED SYSTEM

The proposed system is designed to detect the group shilling attacks that occurs in the recommender system. Here a group of users creates their profiles and enters the recommendation system and purposely tend to change the original rating given by the users for the products in the recommender system. So the original rating of the product is tend to be changed and the fake rating is produced to the users. First, the proposed system extract the rating track of each item and divide the rating tracks to generate candidate groups according to a fixed time criteria. Second, it proposes item attention degree and user activity to calculate the suspicious degrees of candidate groups. By this method it filters the fake ratings given by group shilling attacks and displays the original rating of the products in the recommender system.

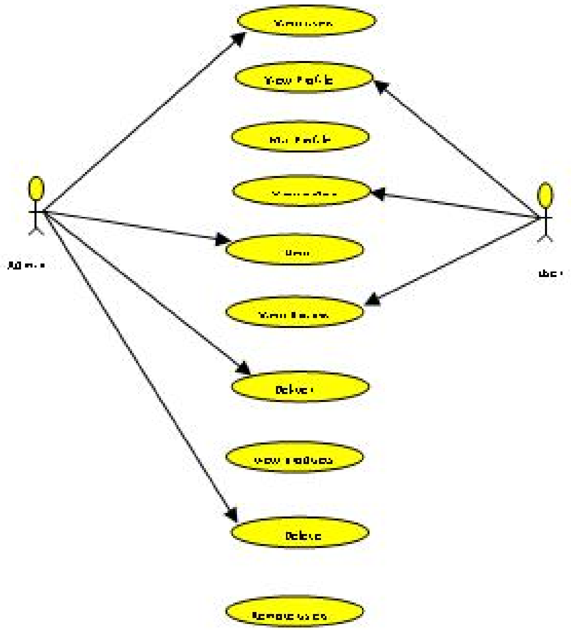


Figure 1: Proposed System

V. METHODOLOGY

K - Means clustering algorithm

1. k-means is one of the simplest unsupervised learning algorithms that solve the well known clustering problem.
2. The procedure follows a simple and easy way to classify a given data set through a certain number of clusters (assume k clusters) fixed apriori.
3. The main idea is to define k centers, one for each cluster. These centers should be placed in a cunning way because of different location causes different result. So, the better choice is to place them as much as possible far away from each other.
4. The next step is to take each point belonging to a given data set and associate it to the nearest center.
5. this algorithm aims at minimizing an objective function know as squared error function given by:

$$J(V) = \sum_{i=1}^{c} \sum_{j=1}^{c_i} (\|x_i - v_j\|)^2$$

where,

'$||x_i - v_j||$' is the Euclidean distance between x_i and v_j.
'c_i' is the number of data points in i^{th} cluster.
'c' is the number of cluster centers.

Place:
We use Euclidean distance in similarity form

VI. TECHNOLOGY USED

PHP

The past five years have been fantastic in terms of the explosive growth of the Internet and the new ways in which people are able to communicate with one another. Spearheading this phenomenon has been the World Wide Web (WWW), with thousands of new sites being launched daily and consumers being consistently offered numerous outstanding services via this new communications medium. With this exploding market has come a great need for new technologies and developers to learn these technologies. Chances are that if you are reading this paragraph, you are one of these Web developers or are soon to become one. Regardless of your profession, you've picked this book up because you've heard of the great new technology called PHP.

This chapter introduces the PHP language, discusses its history and capabilities, and provides the basic information you need to begin developing PHP enabled sites. Several examples are provided throughout, hopefully serving to excite you about what PHP can offer you and your organization. You will learn how to install and configure the PHP software on both Linux/UNIX and Windows machines, and you will learn how to embed PHP in HTML. At the conclusion of the chapter, you will be ready to begin delving into the many important aspects of the PHP language. So light the fire, turn on your favorite jazz album, and curl up on the lazyboy; you are about to learn what will be one of the most exciting additions to your resume: PHP programming.

PHP is best summarized as an embedded server-side Web-scripting language that provides developers with the capability to quickly and efficiently build dynamic Web applications. PHP bears a close resemblance, both syntactically and grammatically, to the C programming language, although developers haven't been shy to integrate features from a multitude of languages, including Perl, Java, and C++. Several of these valuable borrowed features include regular expression parsing, powerful array-handling capabilities, an object-oriented methodology, and vast database support. For writing applications that extend beyond the traditional, static methodology of Web page development (that is, HTML), PHP can also serve as a valuable tool for creating and managing dynamic content, embedded directly beside. Likes of JavaScript, Stylesheets, WML (Wireless Markup Language) and many other useful languages. Providing hundreds of predefined functions, PHP is capable of handling just about anything a developer can dream of Extensive support is offered for graphic creation and manipulation, mathematical calculations, ecommerce, and burgeoning technologies such as Extensible Markup Language (XML), open database connectivity (ODBC), and Macromedia Shockwave.

This vast range of capabilities eliminates the need for the tedious and costly integration of several third-party modules, making PHP the tool of choice for developers worldwide. One of the main strengths of PHP is the fact that because it can be embedded directly alongside HTML code, there is no need to write a program that has many commands just to output the HTML. HTML and PHP can be used interchangeably as needed, working alongside one another in unison. With PHP, we can simply.

Characteristics of PHP:

As you may have realized, the PHP language revolves around the central theme of practicality. PHP is about providing the programmer with the necessary tools to get the job done in a quick and efficient fashion. Five important characteristics make PHP's practical nature possible

- Familiarity
- Simplicity
- Efficiency
- Security
- Flexibility

One final characteristic makes PHP particularly interesting: it's free!

Familiarity

Programmers from many backgrounds will find themselves already accustomed to the PHP language. Many of the language's constructs are borrowed from C and Perl, and in many cases PHP code is almost indistinguishable from that found in the typical C or Pascal program. This minimizes the learning curve considerably.

Simplicity

A PHP script can consist of 10,000 lines or one line: whatever you need to get the job done. There is no need to include libraries, special compilation directives, or anything of the sort. The PHP engine simply begins executing the code after the first escape sequence (<?) and continues until it passes the closing escape sequence (?>). If the code is syntactically correct, it will be executed exactly as it is displayed.

Efficiency

Efficiency is an extremely important consideration for working in a multi-user environment such as the WWW. PHP 4.0 introduced resource allocation mechanisms and more pronounced support for object-oriented programming, in addition to session management features. Reference counting has also been introduced in the latest version, eliminating unnecessary memory allocation

Security

PHP provides developers and administrators with a flexible and efficient set of security safeguards. These safeguards can be divided into two frames of reference: system level and application level.

Flexibility

Because PHP is an embedded language, it is extremely flexible towards meeting the needs of the developer. Although PHP is generally touted as being used in conjunction solely with HTML, it can also be integrated alongside languages like JavaScript, WML, XML, and many others. Additionally, as with most other mainstream languages, wisely planned PHP applications can be easily expanded as needed. Browser dependency is not an issue because PHP scripts are compiled entirely on the server side before being sent to the user. In fact, PHP scripts can be sent to just about any kind of device containing a browser, including cell phones, personal digital assistant (PDA) devices, pagers, laptops, not to mention the traditional PC.

MYSQL

MySQL (http://www.mysql.com) is a robust SQL database server developed and maintained by T.c.X DataKonsultAB of Stockholm, Sweden. Publically available since 1995, MySQL has risen to become one of the most popular database servers in the world, this popularity due in part to the server's speed, robustness, and flexible licensing policy. (See note for more information regarding MySQL's licensing strategy.)

Given the merits of MySQL's characteristics, coupled with a vast and extremely easy-to-use set of predefined interfacing functions, MySQL has arguably become PHP's most-popular database counterpart.

Installation:

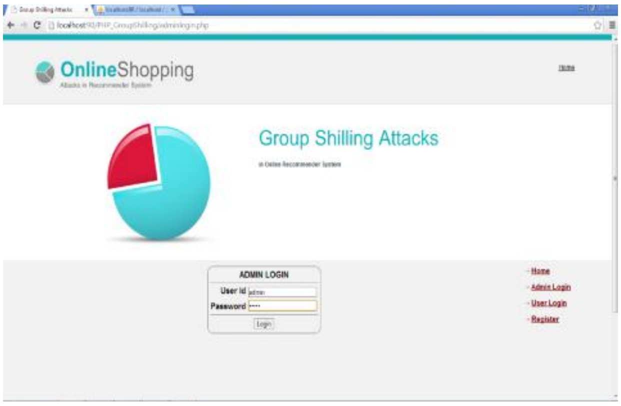
MySQL is so popular among PHP users that support for the db server is automatically built into the PHP distribution. Therefore, the only task that you are left to deal with is the proper installation of the MySQL package. MySQL is compatible with practically every major operating system, including, among others, FreeBSD, Solaris, UNIX, Linux, and the various Windows versions. While the licensing policy is considerably more flexible than that of other database servers, I strongly suggest taking some time to read through the licensing information found at the MySQL site (http://www.mysql.com).

You can download the latest version of MySQL from one of the many worldwide mirrors. A complete listing of these mirrors is at http://www.mysql.com/ downloads/mirrors.html. At the time of this writing the latest stable version of MySQL was 3.22.32, with version 3.23 in beta. It is in your best interest to always download the latest stable version.

V. EXPERIMENTAL RESULTS AND DISCUSSION

Administrator Module

Administrator is the controller of the system. He is in charge of adding products to this site. The admin can view the rating which was given by the users for the products they orders



ADMIN LOGIN

User id: admin

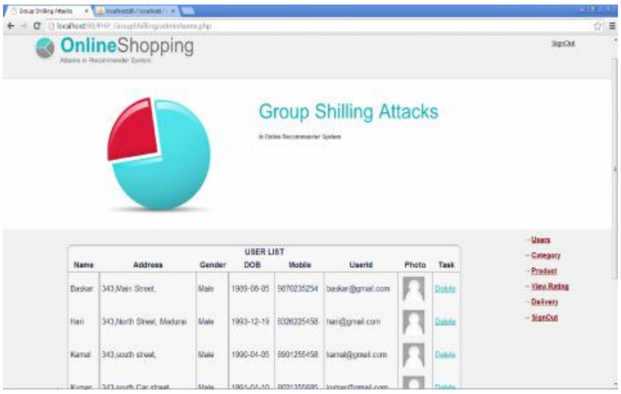
Password: -----

Login

Figure 2: Admin login

1. User List

The administrator can view the registered users in this module. It displays the name, address, gender, photo etc… Unwanted users can be removed from the system using this module.



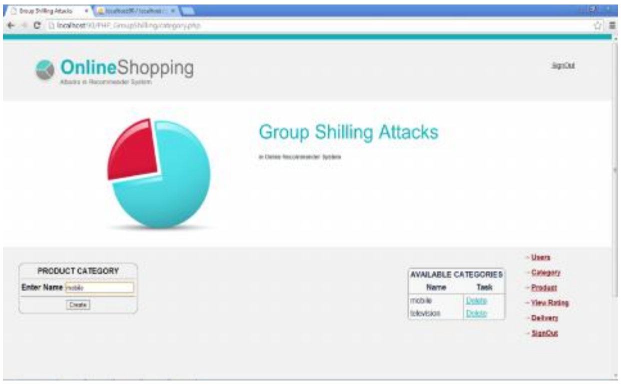
USER LIST

Name	Address	Gender	DOB	Mobile	Userid	Photo	Task
Baskar	343,Main Street,	Male	1989-06-05	9870235254	baskar@gmail.com		Delete
Hari	343,North Street, Madurai	Male	1993-12-19	8328225458	hari@gmail.com		Delete
Kamal	343,south street,	Male	1990-04-05	8901255458	kamal@gmail.com		Delete
Kumar	343,south Car street,	Male	1991-04-10	8021355695	kumar@gmail.com		Delete

Figure 3: User List

2. New Category

The new product category can be created in this module. The created category is displayed in the table format. Unwanted categories can be removed from the system.



PRODUCT CATEGORY

Enter Name: mobile

Create

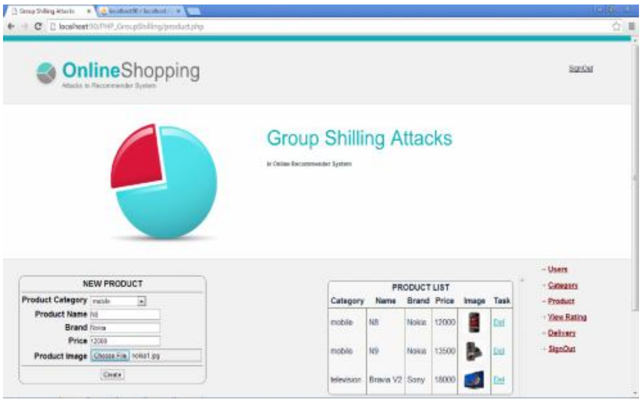
AVAILABLE CATEGORIES

Name	Task
mobile	Delete
television	Delete

Figure 4: Product Category

3. New Product

The administrator can create new product in this module. The admin enters the product category, product name, brand, price, product image and submits the form. It is stored in the server and is used in the user purchase module. Then the created products are shown in the table format and unwanted list can be removed from the system.



NEW PRODUCT

Product Category: mobile

Product Name: N8

Brand: Nokia

Price: 12000

Product Image: Choose File nokia1.jpg

Create

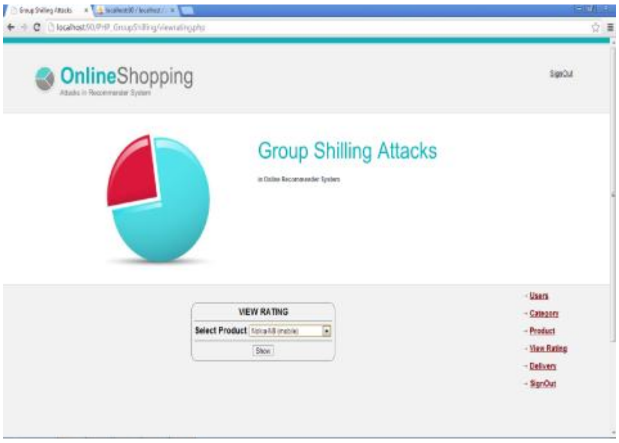
PRODUCT LIST

Category	Name	Brand	Price	Image	Task
mobile	N8	Nokia	12000		Del
mobile	N9	Nokia	13500		Del
television	Bravia V2	Sony	18000		Del

Figure 5: New Product

4. View Rating

The administrator can view the product rating in this module. After selecting the product for which the rating needs to be view the administrator submits the form. Then the rating of the product for both including shilling attack and excluding shilling attacks are shown. Then the administrator can remove the shilling attack ratings from the system if necessary. So the administrator can easily view that if the product rating is alleviated using the group shilling attacks.



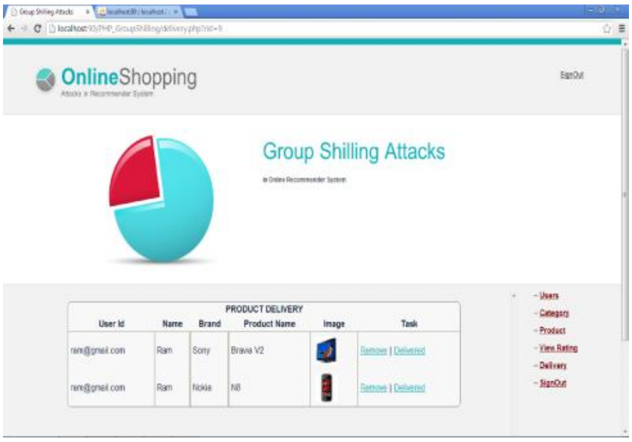
VIEW RATING

Select Product: Nokia N8 (mobile)

Figure 6: View Rating

5. Product Delivery

In this module, the administrator can view the ordered products by the users. The module displays the user id who ordered the items and user name, product brand, product name, image of the product etc… Then the administrator can deliver the product or cancel the product if the order is not delivered.



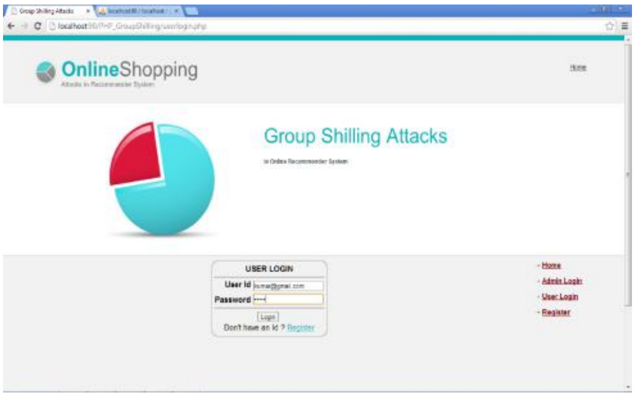
PRODUCT DELIVERY

User Id	Name	Brand	Product Name	Image	Task
ram@gmail.com	Ram	Sony	Bravia V2		Remove | Delivered
ram@gmail.com	Ram	Nokia	N8		Remove | Delivered

Figure 7: Product delivery

User Module

The users can register with the web site and can login the system. They can order the products and can give the rating for the products.



USER LOGIN

User Id: kumar@gmail.com

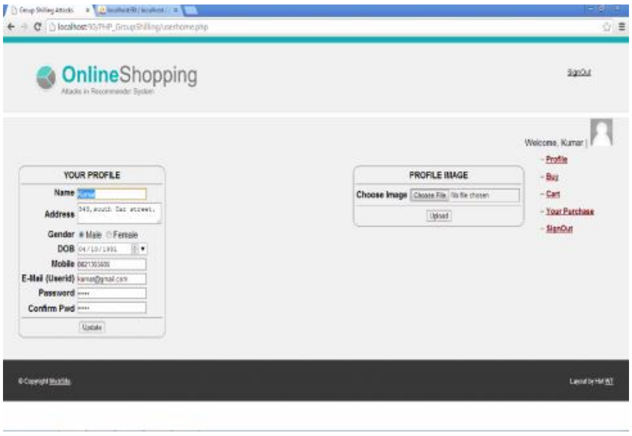
Password: ·····

Don't have an id ? Register

Figure 8: User Login

1. Profile

The user can view their profile in this module. The user can update the profile image in this module. Also the users can update their profile if necessary.



YOUR PROFILE

Name: Kumar

Address: 343,south Car street,

Gender: ● Male ○ Female

DOB: 04/10/1991

Mobile: 0821365606

E-Mail (Userid): kumar@gmail.com

Password: ·····

Confirm Pwd: ·····

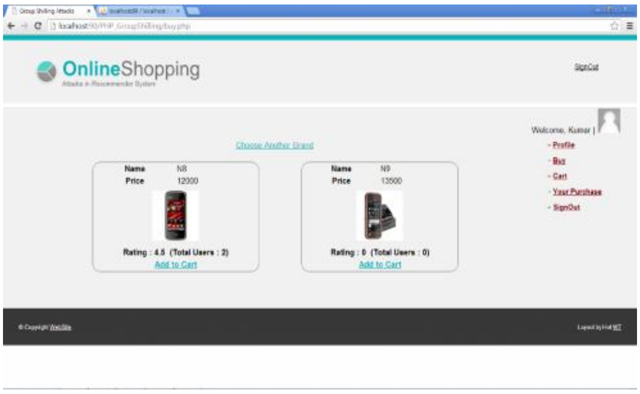
PROFILE IMAGE

Choose Image: No file chosen

Figure 9: User Profile

2. Purchase

The user needs to select the product for purchase. The user is listed the product list available in the brand. It shows the product name, price, image and the rating of the products etc… Then the user can add the item to the cart if necessary. Then it is added to the user cart.



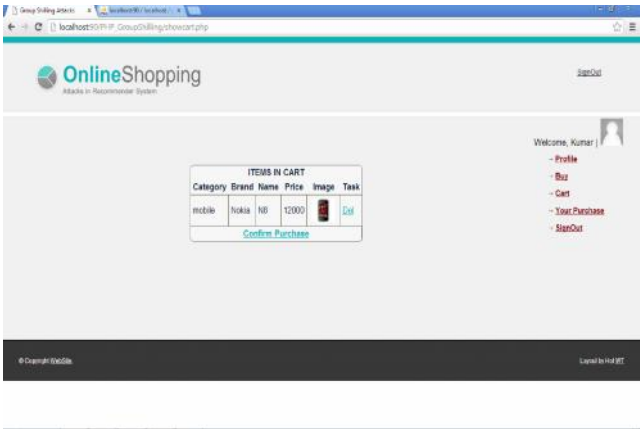
Name N8
Price 12000
Rating : 4.5 (Total Users : 2)

Name N9
Price 13500
Rating : 0 (Total Users : 0)

Figure 10: Purchase Products

3. View Cart

The purchased items are stored in the user cart. The user can view the cart items in this module. Then they can remove the product from the cart or can confirm the purchase if necessary. After confirming the product the user can give rating for the product and send the order to the server.



ITEMS IN CART

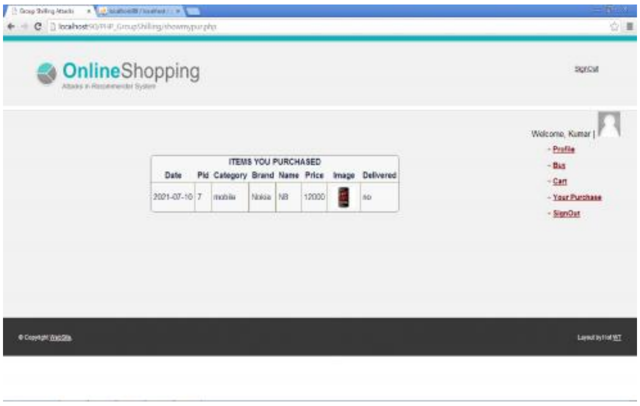
Category	Brand	Name	Price	Image	Task
mobile	Nokia	N8	12000		Del

Confirm Purchase

Figure 10: Items in cart

4. Purchased Items

In this module the purchased items by the user is displayed. It displays the date of purchase, product brand, name, price, product image and delivery status etc… So the user can view the product information which was ordered by him.



ITEMS YOU PURCHASED

Date	Pid	Category	Brand	Name	Price	Image	Delivered
2021-07-10	7	mobile	Nokia	N8	12000		no

Figure 11: Purchased Products

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 in the existing system which detects attacks from single users. So we have developed a system that detects the group shilling attacks from a group of users who tend to alleviate the results produced by the recommender system.

VII. FUTURE ENHANCEMENT

We Enhance 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.

REFERENCES

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

[2] Cai, Hongyun; Zhang, Fuzhi " An Unsupervised Approach for Detecting Group Shilling Attacks in Recommender Systems Based on Topological Potential and Group Behaviour Features.", Security & Communication Networks . 9/27/2021, p1-18. 18p.

[3] M. Si and Q. Li, “Shilling attacks against collaborative recommender systems: a review,” Artificial Intelligence Review, vol. 53, no. 1, pp. 291–319, 2020.

[4] A. M. Turk and A. Bilge, “Robustness analysis of multi-criteria collaborative filtering algorithms against shilling attacks,” Expert Systems with Applications, vol. 115, pp. 386–402, 2019.

[5] K. Vivekanandan and N. Praveena, “Hybrid convolutional neural network (CNN) and long-short term memory (LSTM) based deep learning model for detecting shilling attack in the social-aware network,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 1, pp. 1197–1210, 2021.

[6] Fuzhi Zhang, Weiqi Meng, Ru Ma, Dingli Gao, Shilei Wang, "User embedding-based approach for detecting group shilling attacks", 2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), pp.639-643, 2021

[7] Shilei Wang, Hui Wang, Hongtao Yu, Fuzhi Zhang, "Detecting shilling groups in recommender systems based on hierarchical topic model", 2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), pp.832-837, 2021

[8] Hongtao Yu, Shengyu Yuan, Yishu Xu, Ru Ma, Dingli Gao, Fuzhi Zhang, "Group attack detection in recommender systems based on triangle dense subgraph mining", 2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), pp.649-653, 2021

[9] Hongtao Yu, Haihong Zheng, Yishu Xu, Ru Ma, Dingli Gao, Fuzhi Zhang, "Detecting group shilling attacks in recommender systems based on maximum dense subtensor mining", 2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), pp.644-648, 2021

[10] Zhongying Zhao, Hui Zhou, Liang Qi, Liang Chang, MengChu Zhou, "Inductive Representation Learning via CNN for Partially-Unseen Attributed Networks", IEEE Transactions on Network Science and Engineering, vol.8, no.1, pp.695-706, 2021.

[11] Yassine Himeur, Aya Sayed, Abdullah Alsalemi, Faycal Bensaali, Abbes Amira, Iraklis Varlamis, Magdalini Eirinaki, Christos Sardianos, George Dimitrakopoulos, "Blockchain-based recommender systems: Applications, challenges and future opportunities", Computer Science Review, vol.43, pp.100439, 2022.

[12] Hongyun Cai, Fuzhi Zhang, "An Unsupervised Approach for Detecting Group Shilling Attacks in Recommender Systems Based on Topological Potential and Group Behaviour Features", Security and Communication Networks, vol.2021, pp.1, 2021.

[13] Zhihai Yang, Qindong Sun, Zhaoli Liu, Jinpei Yan, Yaling Zhang, "Rating behavior evaluation and abnormality forensics analysis for injection attack detection", Journal of Intelligent Information Systems, 2021.

[14] Pradeep Kumar Singh, Esam Othman, Rafeeq Ahmed, Awais Mahmood, Habib Dhahri, Prasenjit Choudhury, "Optimized recommendations by user profiling using apriori algorithm", Applied Soft Computing, vol.106, pp.107272, 2021.

[15] D. Jia, C. Zeng, Z. Y. Peng, P. Cheng, Z. M. Yang and Z. Lu, "A user preference based automatic potential group generation method for social media sharing and recommendation", Jisuanji Xuebao, vol. 35, no. 11, pp. 2382-2391, Nov. 2012.

[16] 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.

[17] 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

[18] S. K. Lam and J. Riedl, "Shilling recommender systems for fun and profit", Proc. 13th Conf. World Wide Web WWW, pp. 393-402, 2004.