IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 August 2023, accepted 24 September 2023, date of publication 2 October 2023, date of current version 13 October 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3321322*

RESEARCH ARTICLE

# Using Ensemble Method to Detect Attacks in the Recommender System

**REDA A. ZAYED[1,2], LAMIAA FATTOUH IBRAHIM[1], HESHAM A. HEFNY[1], (Member, IEEE), HESHAM A. SALMAN[2], AND ABDULAZIZ ALMOHIMEED[3]**

[1]Faculty of Graduate Studies for Statistical Research, Cairo University, Giza 12613, Egypt
[2]College of Informatics, Midocean University, Moroni, Comoros
[3]College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11564, Saudi Arabia

Corresponding author: Lamiaa Fattouh Ibrahim (lfattouh@cu.edu.eg)

This work was supported in part by Cairo University, Egypt; and in part by Midocean University, Comoros.

**ABSTRACT** Shill attacks are a serious threat to the stability of filtering and recommendation systems. These attacks involve the injection of fake profiles into the system, which can compromise the reliability of system output. Several shilling attack detection techniques have been proposed, but they often have limitations in terms of accuracy. This works presents a enhanced method for detecting attacks in collaborative recommender systems. The proposed method is based on a combination of statistical and machine learning techniques. The statistical techniques are used to identify anomalous user behavior, while the machine learning techniques are used to classify users as either malicious or benign. The main contribution of the proposed method is the use of a hybrid approach that combines the strengths of statistical and machine learning techniques. The statistical techniques are able to identify anomalous user behavior that is not easily detected by machine learning techniques. The machine learning techniques are able to classify users as either malicious or benign with a high degree of accuracy. The proposed method was evaluated on a real-world dataset. The results showed that the proposed method was able to detect attacks with a high degree of accuracy. The proposed method uses a combination of ensemble learning and feature selection to achieve better accuracy than previous methods. The results of the experiments show that the proposed method can achieve an accuracy of up to 99%.

**INDEX TERMS** Shilling attack detection, profile injection, recommender system, machine learning, ensemble method.

## I. INTRODUCTION

Recommender systems are becoming increasingly popular as a way to help users find content that they are likely to enjoy. These systems use machine learning algorithms to learn about user preferences and then make recommendations based on that data. One of the most common types of recommender systems is collaborative filtering. This type of system works by finding users who have similar interests and then recommending items that those users have rated highly. For example, if you have rated a number of movies highly, a collaborative filtering system might recommend other movies that have been rated highly by people who have similar tastes to you [1].

Another type of recommender system is content-based filtering. This type of system works by analysing the content of items and then recommending items that are like those that the user has previously interacted with. For example, if you have watched several movies about superheroes, a content-based filtering system might recommend other movies about superheroes [2].

Recommender systems are a powerful tool that can help users find content that they are likely to enjoy. These systems are becoming increasingly sophisticated, and they are now used by a wide variety of websites and applications [1].

Collaborative filtering systems use the relationships between users and items to make recommendations. The

The associate editor coordinating the review of this manuscript and approving it for publication was Hua-Wei Shen.

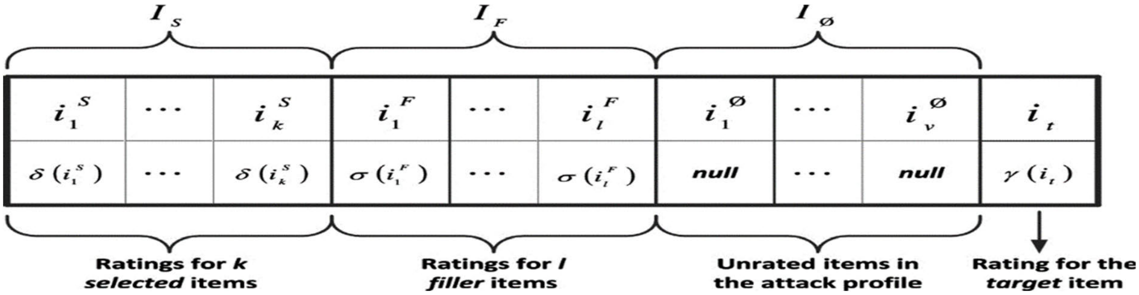
$I_S$
$I_F$
$I_\emptyset$
$i_1^S$ ... $i_k^S$
$i_1^F$ ... $i_l^F$
$i_1^\emptyset$ ... $i_v^\emptyset$
$i_t$
$\delta(i_1^S)$ ... $\delta(i_k^S)$
$\sigma(i_1^F)$ ... $\sigma(i_l^F)$
null ... null
$\gamma(i_t)$
Ratings for *k* *selected* items
Ratings for *l* *filler* items
Unrated items in the attack profile
Rating for the *target* item

**FIGURE 1.** The shilling attack profile structure in its most basic version [1].

similarity of items is determined by the similarity of ratings from users who have rated both items.

The Recommender systems (RSs) are one of the most important components in providing predictions for decision-making. They have efficient methods and procedures for handling large amounts of data [2].

Recommender systems can help people make decisions by suggesting relevant options. These systems can be used to rate articles and products, and it is important to protect rating organizations from manipulation. Collaborative recommender systems are one of the most active and effective types of recommender systems, and they can provide excellent suggestions and recommendations [3]. Techniques and classifications of recommender systems can be divided into content-based, collaborative, and hybrid Filtering Methods.

Collaborative filtering algorithms use user associations to create neighborhoods of similar users. However, this introduces a vulnerability to shilling attacks, in which attackers create and inject fake profiles into the system in order to manipulate the results of the recommendations.

Shill attacks are a serious problem for collaborative filtering systems, and recent research has shown that these systems are vulnerable to this type of attack. There are several techniques that can be used to detect and prevent shilling attacks, but no single technique is perfect [4]. Shill attacks are a type of attack in which attackers create and inject fake profiles into a system to manipulate the results of the recommendations. Collaborative recommendation applications are vulnerable to this type of attack, and recent research has shown that the vulnerability is increasing.

Detecting shilling attacks is typically thought of as a binary classification problem. This means that the goal is to classify each profile as either an active creative user or an anomalous (fake) user, also known as an attacker [2].

The detection method uses machine learning to detect and classify attackers from sophisticated active profiles. In this work, we evaluate well-known shilling attack detectors in collaborative recommendation systems through experimental research. This white paper provides a comprehensive overview of attack models and detection methods for shilling recommender system attacks. We also propose an enhanced shilling attack detection method and develop a roadmap for assessing the current state of research on recommender system attacks and detection techniques.

## II. BACKGROUND

Attacks are performed on the recommendation system by adding a shilling profile to induce distortion of the target element, the goal of shilling attacks is to artificially inflate the ratings of target items in order to increase their sales. Almost all attack models use the same type of profile when creating malicious users.

structure of shilling attack profile contains four sets of items as $I_s$, $I_F$, $I_t$ and $I_\emptyset$ figure 1 shows the shilling attack profile structure [5].

Selected items ($I_s$): these items are chosen based on their correlation and association to the target item.

Filler items ($I_F$): a set of items randomly selected and rating given based on attack properties

Unrated items ($I_\emptyset$: this set of items have no ratings.

Target item ($I_t$): the target item which attacker demote or promote.

Shilling attacks are a type of attack where malicious users attempt to manipulate the recommendations of a recommender system by artificially inflating the ratings of certain items. Attacks are mainly classified into flow attacks, push attacks, and nuclear attacks, and are classified according to the purpose of the attack, nuclear attacks that downgrade items, and the minimum rating given to the target item. next two points clarify the main types of attacks and categorize them into standard attacks and Obfuscated Attacks [2], [6].

Standard attacks are straightforward and easy to carry out. They typically involve creating fake accounts and rating the target item highly. These attacks can be detected using a variety of techniques, such as anomaly detection and trust networks.

Obfuscated Attacks are designed to be more difficult to detect. They may involve using legitimate accounts, rating the target item in a subtler manner, or using other techniques to obscure their intent. These attacks can be more difficult to detect, as they are designed to blend in with legitimate user behavior. However, there are a number of techniques that can be used to detect obfuscated attacks, such as clustering analysis and machine learning.

**TABLE 1.** Comparison of standard attacks and obfuscated attacks in recommender systems [7], [8].

| Feature | Standard Attacks | Obfuscated Attacks |
|---|---|---|
| Definition | These are attacks that are carried out in a straightforward manner. They typically involve creating fake accounts and rating the target item highly. | These are attacks that are designed to be more difficult to detect. They may involve using legitimate accounts, rating the target item in a subtler manner, or using other techniques to obscure their intent. |
| Detection | Standard attacks can be detected using a variety of techniques, such as anomaly detection and trust networks. | Obfuscated attacks can be more difficult to detect, as they are designed to blend in with legitimate user behavior. However, there are a number of techniques that can be used to detect obfuscated attacks, such as clustering analysis and machine learning. |
| Avoid and Mitigation | Standard attacks can be mitigated by using a variety of techniques, such as user verification, rating decay, and trust networks. | Obfuscated attacks can be more difficult to mitigate, as they are designed to evade detection. However, there are a number of techniques that can be used to mitigate obfuscated attacks, such as clustering analysis, machine learning, and game theoretic approaches. |

Standard shilling attacks are those that are easily detectable by existing shilling attack detection methods. These attacks typically involve a small number of malicious users who artificially inflate the ratings of certain items.

Obfuscated attacks are more difficult to detect and defend against than standard attacks. However, there are many techniques that can be used to mitigate the risk of these attacks.

Table 1 shows the comparison of standard attacks and obfuscated attacks in recommender systems.

Using social media to spread ratings: An attacker can use social media to spread their ratings to real users. This can help to make the ratings appear more legitimate.

## III. RELATED WORKS

Large amounts of labeled data are required to improve the performance of supervised algorithms. Training a classifier with a classification-based approach typically requires a balanced combination of attack and normal profiles. Attack profile signatures are used in most early detection algorithms. Others have used "decision trees, rule-based classifiers, Bayesian classifiers, neural network classifiers, or SVMs". A second strategy attempts to address this problem by using unlabeled data to train an unsupervised detection algorithm. These methods require much less computation than supervised methods. The main advantages are easier online learning and improved recognition accuracy. There is a lot of interest in unsupervised methods of detecting attack profiles in the research community. Clustering, association rules, and statistical techniques are some of the techniques used [9].

Jiang et al. proposed [3] a trust-based collaborative filtering algorithm for E-commerce recommendation systems. The algorithm is based on the idea that users' ratings can be trusted more if they are from users who are similar to the current user. The algorithm uses a combination of statistical and machine learning techniques to identify similar users and to calculate the trust between users. The algorithm was evaluated on a real-world dataset, and the results showed that it can achieve a high degree of accuracy

Rincy and Gupta [10]. provides a comprehensive survey of ensemble learning techniques. The work discusses the different types of ensemble learning techniques, the advantages and disadvantages of each technique, and the application of ensemble learning techniques in different domains.

Zayed et al. [11] presents an experimental and theoretical study of the popular shilling attacks detection methods in collaborative recommender systems. The authors evaluated the performance of these methods on a real-world dataset and compared their results with the results of other methods. They also proposed a new hybrid method that combines behavior-based and content-based methods.

Alonso et al. [12] proposed a novel method for detecting shilling attacks in collaborative filtering recommender systems. The method is based on a combination of statistical and machine learning techniques. The statistical techniques are

**TABLE 2.** Summary of existing papers on ensemble methods for detecting shilling attacks.

| Paper | Strengths | Weaknesses | How to Enhance |
|---|---|---|---|
| Ensemble-based Detection of Shilling Attacks in Recommender Systems [15] | - Can effectively detect shilling attacks with different attack strategies. | - Requires a large amount of training data. | - Use transfer learning.<br>- Use data augmentation.<br>- Use a small learning rate.<br>- Use a regularization technique. |
| An ensemble method for detecting shilling attacks based on ordered item sequences [16] | - Uses a variety of features to characterize attack profiles.<br>- Uses an ensemble framework to improve the detection performance. | - The features may not be discriminative enough for some attack types.<br>- The ensemble framework may be computationally expensive. | - Use more discriminative features.<br>- Use a more efficient ensemble framework. |
| Shilling attack detection for collaborative recommender systems: a gradient boosting method [17] | - Uses a gradient boosting algorithm to improve the detection performance.<br>- Can detect both small-scale and large-scale attacks. | - The algorithm may be sensitive to the hyperparameters.<br>- The algorithm may not be able to detect all attack types. | - Use a more robust gradient boosting algorithm.<br>- Use a more comprehensive set of features. |
| Multiview Ensemble Method for Detecting Shilling Attacks in Collaborative Recommender Systems [18] | - Uses a Multiview ensemble framework to improve the detection performance.<br>- Can detect both single-item and group shilling attacks. | - The framework may be computationally expensive.<br>- The framework may not be able to detect all attack types. | - Use a more efficient Multiview ensemble framework.<br>- Use a more comprehensive set of features. |

used to identify anomalous user behavior, while the machine learning techniques are used to classify users as either malicious or benign. The main contribution of the paper is the use of a hybrid approach that combines the strengths of statistical and machine learning techniques

Zayed et al. [13] provides an enhanced method for detecting attack in collaborative recommender systems. The proposed method used the ensemble method based on behaviour-based and content-based methods to improve the accuracy of detection. The experimental results showed that the proposed method is effective in detecting shilling attacks.

Yassine et al. [14] they present Comprehensive survey on security and privacy in recommender systems (RSs). It analyzes recent frameworks and investigates different security aspects. The study describes the strengths and weaknesses of existing contributions. It also discusses the importance of privacy preservation and security in RSs from the application perspective, including e-commerce, healthcare, energy, e-learning, IoT and smart city, and social networks and finally the study conducts a critical discussion and extracts the important findings.

Table 2 summarizes the existing papers on ensemble methods for detecting shilling attacks in recommender systems, including their strengths, weaknesses, and how they can be enhanced.

## IV. DETECTION ALGORITHMS

The proposed approach requires modifying and changing the rating dataset according to the attacker's goals in order to influence the results of the recommendation system. The targets of the proposed method are to classify and recognize attack profiles. The proposed method is divided into three main phases.

*Phase 1 (Feature Engineering):* This phase involves extracting features and attributes from the dataset. The goal of this phase is to create a set of features that are relevant to the task of attack detection.

*Phase 2 (Construction of a Recognition Classifier):* This phase involves constructing a classifier that can be used to detect attacks. The classifier is constructed using an ensemble learning algorithm called the voting method. The voting method combines the predictions of multiple classifiers to improve the accuracy of the overall prediction.

*Phase 3 (Attack Detection):* This phase involves using the classifier to detect attacks. The classifier is given a new dataset, and it predicts whether the dataset contains an attack or not.

Ensemble learning is a machine learning technique that combines the predictions of multiple models to improve overall accuracy. There are many different ensemble learning methods, but they all share the same basic principle:

**TABLE 3.** Summarizes the key differences between bagging and boosting algorithms [10].

| Feature | Bagging | Boosting |
|---|---|---|
| How models are created | Multiple models are trained on different subsets of the training data. | Models are trained sequentially, with each model being trained to correct the mistakes of the previous models. |
| How variance is reduced | By training on different subsets of the training data. | By training each model to correct the mistakes of the previous models. |
| Overall accuracy | Can be higher than individual models, but not always. | Can be higher than individual models, especially for difficult problems. |
| Computational complexity | Lower than boosting algorithms. | Higher than bagging algorithms. |

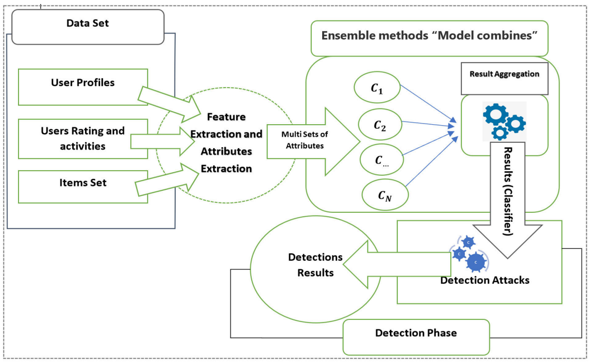

**FIGURE 2.** The proposed detection attacks model.

combining the predictions of multiple models to reduce variance. This is because different models are often susceptible to different types of errors, so by combining their predictions, we can reduce the overall error rate. Some of the most common ensemble learning methods include

*Bagging:* This method creates multiple copies of the same model, each trained on a different subset of the training data. The predictions of the individual models are then aggregated using a voting classifier.

*Boosting:* This method creates a sequence of models, each of which is trained to correct the errors of the previous models. The predictions of the individual models are then aggregated using a weighted voting classifier [10].

*Random Forests:* This method creates a forest of decision trees, each of which is trained on a different subset of the training data. The predictions of the individual trees are then aggregated using a voting classifier [10].

Ensemble learning is a powerful technique that can significantly improve the accuracy of machine learning models. It is a versatile technique that can be used with a variety of different machine learning algorithms [10]. Voting classifiers are not standalone classifiers.

They are wrappers that combine the predictions of multiple machine learning algorithms. This is done by training and evaluating the algorithms simultaneously. The predictions of the individual algorithms are then combined to make a final prediction [19].

Voting classifiers are a powerful way to improve the accuracy of machine learning models. This is because different algorithms are often susceptible to different types of errors. By combining the predictions of multiple algorithms, we can reduce the overall error rate.

Table 3 summarizes and compares the two main categories of ensemble learning algorithms: bagging and boosting.

### A. ATTRIBUTES EXTRACTION

In this phase, we extract attributes from user profiles and activities. These attributes are used to classify user profiles as genuine or attacker. We use a set of calculation methods, including RDAM, WDA, cosine similarity, LenVar, TF-IDF, RDMA similarity, RDMA_LenVar, and degree of similarity, figure 2 shows the proposed system.

### B. BUILDING THE DETECTION CLASSIFIER

in this phase, we divide the data into training and testing sets. The training set is used to train a voting classifier to recognize non-genuine profiles. The testing set is used to evaluate the performance of the classifier.

The voting classifier is a type of ensemble learning model that combines the predictions of multiple base classifiers. The base classifiers in this case are RDAM, WDA, cosine similarity, LenVar, TF-IDF, RDMA similarity, RDMA_LenVar, and degree of similarity.

## V. EVALUATION METRICS

To measure and evaluate the performance of any proposed model, we use several evaluation metrics, including false positive rate, detection rate, precision, and recall [9].

*False Positive Rate:* This is the percentage of non-attack profiles that are incorrectly classified as attack profiles.

*Detection Rate:* This is the percentage of attack profiles that are correctly classified as attack profiles.

**TABLE 4.** Statistical information of data sets are used.

| Data Set | Rating | Users | Movies | Rating |
|---|---|---|---|---|
| Movie Lens | 1,000,209 | 6040 | 3900 | Integer (1 to5) |

*Precision:* This is the percentage of attack profiles that are correctly classified as attack profiles out of all the profiles that are classified as attack profiles.

*Recall:* This is the percentage of attack profiles that are correctly classified as attack profiles out of all the attack profiles in the dataset.

In this work, "attacks" refers to the number of attack profiles in the dataset, and "detections" refers to the number of attack profiles that are correctly classified as attack profiles. [9].

$$DetectionRate = \frac{\#Detection}{\#Attacks} \tag{1}$$

The number of bogus genuine profiles is known as "False Positives," whereas the number of true genius profiles is known as "Actual Profiles."

$$\text{False Positive Rate} = \frac{\#\text{False Positives}}{\#Genuine\ Profiles} \tag{2}$$

many proposed methods are used precision, recall and F-measure [20]:

$$Precision = \frac{True\ positive}{True\ positive + False\ positive} \tag{3}$$

$$\text{Recall} = \frac{True\ positive}{True\ positive + False\ Negative} \tag{4}$$

$$\text{F1} - \text{Measure} = \frac{2.Precision * \text{Recall}}{Precision + \text{Recall}} \tag{5}$$

## VI. DISCUSSIONS AND EXPERIMENTS

In this section, we conduct in-depth experiments on the benchmark dataset using four detecting algorithms: RDAM, WDA, Cosine Similarity, and LenVar. The MovieLens datasets were used. The dataset specifications are listed in Table 4. We evaluate the performance of the four algorithms using the following valuation metrics: Precision, Recall, and f-measure.

Users rate items on a scale of 1 to 5, with 1 being the lowest (unhappy) and 5 being the highest (satisfied and happy). In each movie dataset, all ratings are numerical values between 1 and 5, with the lowest value representing unhappy and the highest value representing happy. For attacker profiles: We created a dataset of fake users to simulate attacker profiles. We used various attack models to create different attack profiles. As a result, we created an attack dataset containing attack ratings for different malicious users) for various attacks.

Generation method of three types of push attacker profiles. Then, these shilling attack profiles are injected into datasets, table 5 shows the generation method of five types of push attacker profiles. For feature extraction we give the definitions of popularity profile and popularity distribution of a user, which are the output of data preprocessing phase. For detection purpose, it is not necessary to operate on all possible values of the popularity distribution [21]. Instead, it is appropriate to consider only a small number of accumulated probabilities over some intervals. Therefore, we bucket the range of popularity distribution into several intervals to get accumulated probability as features. The mean popularity of a user (MPU) refers to the mean value of popularity profile, or the mean value of rated items popularity in a user profile. Figure 3 to figure 6 show the performance of the used detectors. The filler item set by 5% to 50%, attack size set by 25 and 50%, which means the ratio of the injected spammer to active genuine profiles, target item score set by 5, item has an average score lower than threshold may be one of the target items. Items that have rating count larger than min count may be chosen as one of the target items. For the training phase, we used 10 K-fold cross validation to train and test the classifiers. We used the classification report[1] visualizer displays the precision, recall, F1, and support scores for the model.

**TABLE 5.** Generation methods for the shilling attack models.

| Attack Model | Generation methods |
|---|---|
| Random Attack | Rate 5 to a target item; give filler items random ratings conforming to a Gaussian distribution with mean 3.6 and standard deviation 1.1 |
| Average Attack | Rate 5 to a target item; the ratings for filler items are distributed around the mean for each item |

To create attacker profiles, we created a dataset of fake users. We used various attack models to create different attack profiles. This resulted in an attack dataset containing attack ratings for different malicious users for various attacks. The list of attacked items in an attack consists of movies that are among the top 25% to 50% of user-rated movies to perform the User Shifting attack, we selected a subset of ratings from each profile and decreased them by one. We first calculated the standard normal distribution of the dataset, multiplied it by the ratings, and then divided the result by the noise injection attack threshold of 0.4. We then inserted the attack profiles into the dataset to create the test set. This study only discusses the User Shifting attack.

The performance of the proposed algorithm was evaluated against several classifiers in multiple trials. The following tables and graphs present the comparative results of the proposed algorithm.

Table 6 shown the result of the proposed voting classifier.

[1] https://www.scikit-yb.org/en/latest/api/classifier/classification_report.html

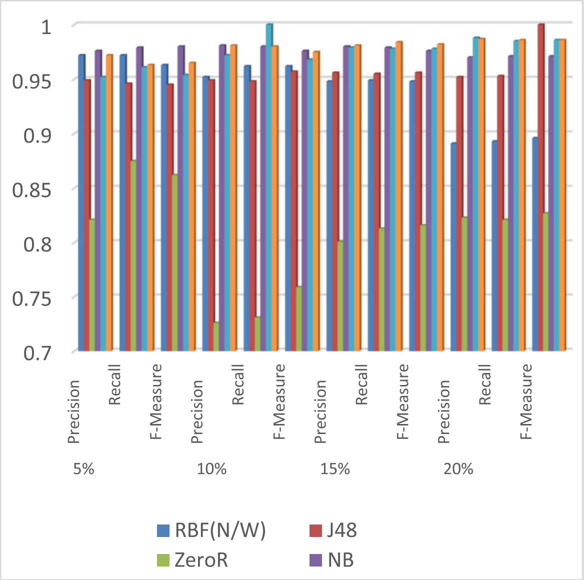

**FIGURE 3.** Peromance analysis for random attack at 5% to 20% filler size.

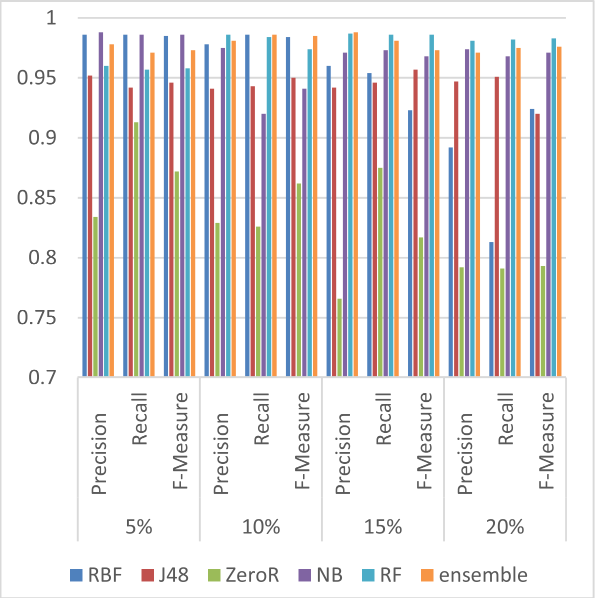

**FIGURE 4.** Peromance analysis of model for average attack at 50% filler size.

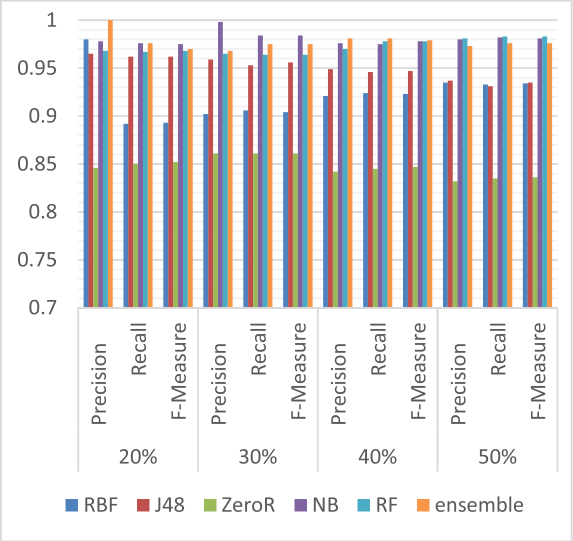

**FIGURE 5.** Peromance analysis for random attack at 20% to 50% filler size.

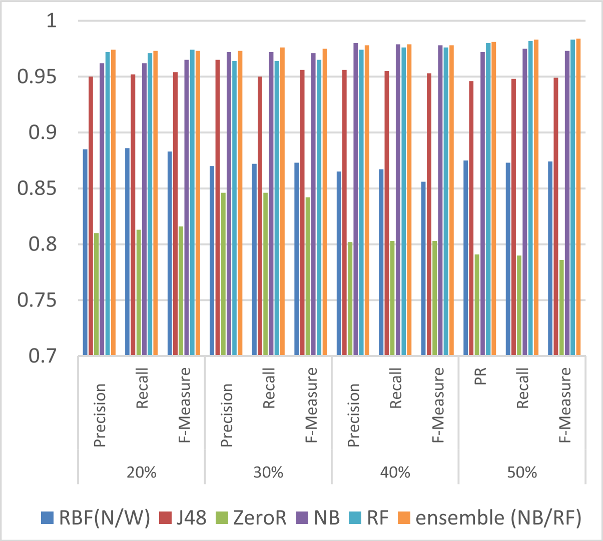

**FIGURE 6.** Peromance analysis of model for average attack at 20% to 50% filler size.

**TABLE 6.** The performance of the majority voting classifier.

| | TP | FP | Precision | Recall | F1 |
|---|---|---|---|---|---|
| | 0.968 | 0.0 | 1.0 | 0.968 | 0.985 |
| | 1.0 | 0.032 | 0.75 | 1.0 | 0.856 |
| Weighted AVG | 0.971 | 0.003 | 0.978 | 0.971 | 0.973 |

Experiments have shown that voting classifiers achieve the highest detection accuracy for shilling attacks in collaborative recommender systems.

The Experiments results have shown the Voting ensemble classifiers are more robust to noise in the data in recommender system. Noise in the profiles can cause individual classifiers to make incorrect predictions. However, voting ensemble classifiers are less likely to be affected by noise because they combine the predictions of multiple classifiers.

The Voting ensemble classifiers can learn more complex relationships in the data. Individual classifiers may have difficulty learning complex relationships in the data, especially if the data is noisy or high-dimensional. However, voting ensemble classifiers can learn more complex relationships by combining the predictions of multiple classifiers and the Voting ensemble classifiers are easier to tune than individual classifiers. Tuning a classifier involves adjusting its hyperparameters to achieve the best possible performance. Tuning an individual classifier can be difficult and time-consuming, especially if the classifier is complex. However, tuning a voting ensemble classifier is typically easier because the hyperparameters of the individual classifiers can be tuned independently. Ensemble learning is a powerful technique for improving model performance by combining different base models to create a more robust and reliable model. This technique can also be used on real-world datasets to improve performance.

## VII. CONCLUSION

The detection of attacks in recommender systems is an important and challenging research area. We conducted experiments using the well-known MovieLens benchmark rating dataset and compared the results in terms of accuracy, F1-measure, recall, precision, macro-average, and weighted-average. The proposed method for detecting attacks in collaborative recommender systems is a enhanced hybrid approach that combines the strengths of statistical and machine learning techniques. The statistical techniques are used to identify anomalous user behavior, while the machine learning techniques are used to classify users as either malicious or benign. The proposed method was evaluated on a real-world dataset, and the results showed that it can achieve an accuracy of up to 99

The main contribution of the proposed method is the use of a hybrid approach that combines the strengths of statistical and machine learning techniques. The statistical techniques are able to identify anomalous user behavior that is not easily detected by machine learning techniques. The machine learning techniques are able to classify users as either malicious or benign with a high degree of accuracy. The proposed method uses a combination of ensemble learning and feature selection to achieve better accuracy than previous methods. Ensemble learning combines the predictions of multiple models to improve the overall accuracy. The results of the experiments show that the proposed method is a promising approach for detecting attacks in collaborative recommender systems. The method is able to achieve a high degree of accuracy, and it is able to detect attacks that are not easily detected by other methods. Future work includes improving model performance and applying these methods across various domains using multiple datasets with different sparsity levels.

## ACKNOWLEDGMENT

The authors would like to thank Cairo University, Egypt, and Midocean University, Comoros, for technical and financial support.

## REFERENCES

[1] R. A. Zayed, L. F. Ibrahim, H. A. Hefny, and H. A. Salman, "Shilling attacks detection in collaborative recommender system: Challenges and promise," in *Proc. Workshops Int. Conf. Advanced Inf. Netw. Appl.*, 2020, pp. 429–439.

[2] Y. Hao, F. Zhang, J. Wang, Q. Zhao, and J. Cao, "Detecting shilling attacks with automatic features from multiple views," *Secur. Commun. Netw.*, vol. 2019, pp. 1–13, Aug. 2019.

[3] L. Jiang, Y. Cheng, L. Yang, J. Li, H. Yan, and X. Wang, "A trust-based collaborative filtering algorithm for e-commerce recommendation system," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 8, pp. 3023–3034, Aug. 2019.

[4] Z. Batmaz, B. Yilmazel, and C. Kaleli, "Shilling attack detection in binary data: A classification approach," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 6, pp. 2601–2611, Jun. 2020.

[5] K. Chen, P. P. K. Chan, F. Zhang, and Q. Li, "Shilling attack based on item popularity and rated item correlation against collaborative filtering," *Int. J. Mach. Learn. Cybern.*, vol. 10, no. 7, pp. 1833–1845, Jul. 2019.

[6] W. Zhou, J. Wen, Y. S. Koh, Q. Xiong, M. Gao, G. Dobbie, and S. Alam, "Shilling attacks detection in recommender systems based on target item analysis," *PLoS ONE*, vol. 10, no. 7, 2015, Art. no. 0130968.

[7] 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.

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

[9] M. Liu, C. Xu, C. Xu, and D. Tao, "Fast SVM trained by divide-and-conquer anchors," in *Proc. 26th Int. Joint Conf. Artif. Intell.*, Aug. 2017, pp. 2322–2328.

[10] T. N. Rincy and R. Gupta, "Ensemble learning techniques and its efficiency in machine learning: A survey," in *Proc. 2nd Int. Conf. Data, Eng. Appl. (IDEA)*, Feb. 2020, pp. 1–6.

[11] R. A. Zayed, L. F. Ibrahim, H. A. Hefny, H. A. Salman, and A. AlMohimeed, "Experimental and theoretical study for the popular shilling attacks detection methods in collaborative recommender system," *IEEE Access*, vol. 11, pp. 79358–79369, 2023.

[12] S. Alonso, J. Bobadilla, F. Ortega, and R. Moya, "Robust model-based reliability approach to tackle shilling attacks in collaborative filtering recommender systems," *IEEE Access*, vol. 7, pp. 41782–41798, 2019.

[13] R. A. Zayed, H. A. Hefny, L. F. Ibrahim, and H. A. Salman, "An enhanced method for detecting attack in collaborative recommender system," in *Proc. 1st Int. Conf. Adv. Innov. Smart Cities (ICAISC)*, Jeddah, Saudi Arabia, Jan. 2023, pp. 1–5.

[14] Y. Himeur, S. S. Sohail, F. Bensaali, A. Amira, and M. Alazab, "Latest trends of security and privacy in recommender systems: A comprehensive review and future perspectives," *Comput. Secur.*, vol. 118, Jul. 2022, Art. no. 102746.

[15] Y. Hao, F. Zhang, and J. Chao, "An ensemble detection method for shilling attacks based on features of automatic extraction," *China Commun.*, vol. 16, no. 8, pp. 130–146, Aug. 2019.

[16] F. Zhang and H. Chen, "An ensemble method for detecting shilling attacks based on ordered item sequences," *Secur. Commun. Netw.*, vol. 9, no. 7, pp. 680–696, May 2016.

[17] C. Shao and Y. Z. Y. Sun, "Shilling attack detection for collaborative recommender systems: A gradient boosting method," *Math. Biosciences Eng.*, vol. 19, no. 7, pp. 7248–7271, 2022.

[18] Y. Hao, P. Zhang, and F. Zhang, "Multiview ensemble method for detecting shilling attacks in collaborative recommender systems," *Secur. Commun. Netw.*, vol. 2018, pp. 1–33, Oct. 2018.

[19] X. Dong, Z. Yu, W. Cao, Y. Shi, and Q. Ma, "A survey on ensemble learning," *Frontiers Comput. Sci.*, vol. 14, pp. 241–258, Apr. 2020.

[20] W. Zhou, J. Wen, Q. Qu, J. Zeng, and T. Cheng, "Shilling attack detection for recommender systems based on credibility of group users and rating time series," *PLoS ONE*, vol. 13, no. 5, May 2018, Art. no. e0196533.

[21] C. Krügel, T. Toth, and E. Kirda, "Service specific anomaly detection for network intrusion detection," in *Proc. ACM Symp. Appl. Comput.*, Mar. 2002, pp. 201–208.

**REDA A. ZAYED** received the M.Sc. degree in computer science from the Faculty of Graduate Studies for Statistical Research, Cairo University, in 2017, where he is currently pursuing the Ph.D. degree in computer science. He has over 16 years of experience working in product management and data science. He is currently the Head of the Software Development Department, Ministry of Justices in Egypt, and the College of Informatics, Midocean University. His research interests include artificial intelligence, machine learning, advanced database management, knowledge-based systems, big data, and data science.

**LAMIAA FATTOUH IBRAHIM** received the B.Sc. degree from the Computer and Automatic Control Department, Faculty of Engineering, Ain Shams University, in 1984, the master's degree from Ecole National Superieur de Telecommunication (ENST), Paris, in 1987, the master's degree from the Computer and Systems Engineering Department, Faculty of Engineering, Ain Shams University, in 1993, and the Ph.D. degree from the Faculty of Engineering, Cairo University, in 1999. She was the Vice Dean for Education and Student Affairs with the Faculty of Information Systems and Computer Science, October 6 University. She was the Head of the Department of Computer Science, Faculty of Graduate Studies for Statistical Research, Cairo University. She was with the Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University. She has over 39 years of experience in the fields of network design engineering and artificial intelligence, with a focus on applying knowledge base and data mining techniques to wired and wireless network planning. She has published papers in many international journals and international conferences in the areas of networks, data mining, and wired and mobile network planning.

**HESHAM A. HEFNY** (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in electronics and communication engineering from Cairo University, in 1987, 1991, and 1998, respectively. He is currently a Professor of computer science with the Faculty of Graduate Studies for Statistical Research (FGSSR), Cairo University. He is also the Vice Dean of Graduate Studies and Research with FGSSR. He has authored more than 160 papers in international conferences, journals, and book chapters. His major research interests include computational intelligence (neural networks, fuzzy systems, genetic algorithms, and swarm intelligence), data mining, and uncertain decision-making. He is a member of the following professional societies: IEEE Computer Society, IEEE Computational Intelligence Society, and IEEE System, Man, and Cybernetics Society.

**HESHAM A. SALMAN** received the master's degree in engineering from Ain Shams University, in 1996, and the Ph.D. degree from the Faculty of Computing and Information Systems, Ain Shams University. He was with the Information System Department, Faculty of Computing and Information Technology, King Abdulaziz University. He was the General Manager of the Technology Competency Center, Ministry of Commerce and Industry, Cairo, Egypt. He is currently with the College of Informatics, Midocean University, and the Higher Institute of Computer and Information Technology, Alshrouk Academy, Cairo. Throughout his working life, he has participated in many studies and works related to information systems. He has over 37 years of experience in the fields of network engineering, computer security, and programming applications. He has published in the area of networks, data mining, and wire and mobile network planning.

**ABDULAZIZ ALMOHIMEED** received the master's degree from Monash University, Australia, and the Ph.D. degree from the University of Southampton, England, U.K. He is currently an Assistant Professor with the College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia. His research interests include natural language processing, artificial intelligence, data science, the Internet of Things, and network security. He is passionate about leveraging technology to create innovative solutions.