EAI Endorsed Transactions
on Scalable Information System

Research Article EAI.EU

Hybrid CNN and RNN-based shilling attack framework in social recommender networks

Praveena Narayanan[1,*], Vivekanandan.K[2]

[1]Research Scholar, Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India.
[2]Professor, Department of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India.

Abstract

INTRODUCTION: Recommender system is considered to be widely utilized in diversified domain for the purpose of effectively handling information overload. But, recommender systems are prone to vulnerabilities that are significantly exploited by malicious attacks. In particular, shilling attack is determined to crucial in the recommender system due to its openness characteristics and data dependence.
OBJECTIVES: Authors focused on detecting shilling attack by using hybrid deep learning techniques.
METHODS: Hybrid CNN and RNNs-based shilling attack framework is proposed for shilling attack detection based on the selection of dynamic features for attaining maximized detection accuracy.
RESULTS: The proposed CNN-RNNs-based shilling attack framework was determined to improve the recall with different filler size under Netflix dataset by 4.48% and 6.14%, better than the benchmarked HDLM and RMRA frameworks. The proposed CNN-RNNs-based shilling attack framework was determined to minimize the false positive rate by 4.82% and 5.94%, better than the benchmarked HDLM and RMRA frameworks.
CONCLUSION: This framework integrated user popularity and rating-based indicators in order to consider the deviations that happens, when the users select items. It also included information entropy for dynamically choosing the detection indicators in order to improve the reliability in attack detection. It was proposed with three different attack detection models that contextually handles different shilling attacks.

Keywords: Recommender System, Shilling Attack, Recurrent Neural Networks (RNN), Convolutional Neural Network (CNN), Interference Immunity.

Received on 24 April 2021, accepted on 31 October 2021, published on 02 November 2021

doi: 10.4108/eai.2-11-2021.171754

*Corresponding author. Email: praveenan@pec.edu

1. Introduction

In this information age, the data generated by governments, companies and individuals create information overhead. The internet is the common platform through which the generated information can be stored and shared with different parties that need this information [1]. From the past decades, multiple number of e-commerce platforms have emerged in the market for the objective of selling different categories of products and services [2]. However, identifying the required content by the online users have become more crucial and increasing difficult due to the information overload [3]. This problem of information overhead is handled by the websites through the benefits derived from the recommender systems [3]. In general, recommender systems refer to an information filtering mechanism that facilitates their potential customers or users with service of products based on their requirements [4]. At this juncture, multiple number of recommender system was employed for supporting different categories of requirements needed in different websites. Over the number of years, there has been a considerable growth in the methods used for enhancing the results of recommendation derived for different objectives [5]. The recommendation systems are categorized into two types such as content-based filtering scheme and collaborative filtering scheme

[6]. The content-based filtering recommender schemes recommends the products to its users by comparing the products' content based on the user profiles [7]. However, this content-based filtering possesses the limitations of over specialization, and they exhibit the behaviour of recommending the products whose characteristics are very similar to that of the product which is already consumed by the user [8]. On the hand, collaborative filtering schemes concentrate on the process of resolving the issues of over specialization inherent with content-based filtering approaches. This collaborative recommender system operates by exploring the user past behaviour into account [9]. The key idea behind this collaborative recommender system completely depends on the users, who possess similar interests and needs. Moreover, collaborative filtering-based recommendations completely depends on te associated between the items and its consuming users [10]. However, this collaborative filtering-based recommender systems are unfortunately prone to shilling attack due to its dependency and openness on the ratings of the user. This shilling attack launched over this collaborative filtering-based recommender systems are also named as a profile-injection attack. In specific, shilling attack refers to a particular category of attack through which a malicious user profile is intentionally inserted into an existing collaborative dataset in order to change the recommender systems' outcome. The profiles that are injected explicitly rate the items, such that items under target can never be promoted and demoted.

A diversified number of research contributions were proposed in the literature over the decades for determining different and potential challenges in this domain of collaborative filtering-based recommender systems [11]. Some of them concentrated exclusively on the development of a reliable collaborative filtering scheme, but have failed to focus on determining attack strategies or detection techniques. Few of these approaches focused on the identification of statistical measures that attribute towards the detection of the shilling attack methods [12]. As a whole, these detection scheme based on the detection of attack profiles is categorized into classification, clustering, graph mining and statistical methods. Unfortunately, these existing shilling attacks detections approaches inherited some inadequacies that do not consider the difference between the attacker and normal users or confines to the attackers ratings pattern, attack size sensitivity and restricted attack types [13]. When the difference between the normal and the attacker is not identified by the shilling attack detection approach, then mis-classification rate and false rate will surely get increased. Recently, a number of shilling attack detection schemes are propounded in the literature based on the merits of machine learning models. But, the classical machine learning approaches maximally depends on the process of feature engineering that essentially necessitates time-consuming and complex feature extraction phenomenon [14]. Hence, more robustly performing deep learning models are required for attaining end-to-end attack detection in real time environment. In this context, recurrent neural networks and convolutional neural networks are considered to the robust categories of deep learning methods that have wide applicability and suitability in detecting shilling attack with maximized accuracy [15]. A number of different architectures that integrates the merits of RNN and CNN were propounded for the purpose of detecting shilling attacks in different application and contexts. Some of the predominant combinations of RNN and CNN considered in the literature for detecting shilling attacks are CNN-LSTM, cascade CNN-RNN, CNN-GRU and CNN-LSTM-AM. At this juncture, CNN failed to include the items rating time distribution in scenarios where abnormal patterns are revealed through ratings order, even though it is useful for the detection of shilling attacks. Further, the propounded RNN approaches only and distinctly relied upon the ratings of separate items that generally ignored the data correlation. Thus, shilling attack in collaborative recommender systems need the use of integrating RNN and CNN models for achieving acceptable accuracy.

1.1 Motivation

Recommender systems manage huge amount of data and recommend desirable items to the users. The customers in the online platform are fulfilled with different choices of services or products with corresponding rapid advancement in the field of e-commerce. The marketing activities, on the other hand are facing struggle in providing more customized offers to the customers. This increase in the options diversity introduces the problem of information overload. Recommender systems handle the issue of options diversity by facilitating personalized recommendations that attribute towards the enhancement of customers' purchasing experience. This recommendation systems are classified into geographic recommenders, social filtering, demographic filtering, utility-based recommenders, knowledge-based recommenders, content-based filtering, collaborative filtering, and hybrid systems. Among the recommender systems, collaborative filtering-based recommender systems is determined to be potent in establishing the association between the new and old users of the systems with respect to items of recommendation determined based on similar interests. Collaborative filtering-based recommender systems is vulnerable to shilling attacks, both by individuals and groups. Forged user-generated content data, such as user ratings and reviews, are used by attackers to manipulate recommendation rankings. This shilling attack either promote or demote the target items, contributing towards push and nuke attacks in the recommender systems. This shilling attack utilize the filler ratings in attaining the objective of pushing or nuking the items of target. Attackers inject ratings and exploit fake profiles associated with the targeted items and remaining items set for increasing the influence of attacks in the system. In this context, the shilling attacks are classified into random, average bandwagon, average over popular, segment attack and love/hate attack. These attack categories evolved sue to the rated items' set such as selected items, filler items, unrated

items, and target items. At this juncture, shilling attack detection in recommender systems is of great significance to maintain the fairness and sustainability of recommender systems. The current studies have problems in terms of the poor universality of algorithms, difficulty in selection of user profile attributes, and lack of an optimization mechanism. Previous research focuses only on the differences between genuine profiles and attack profiles, ignoring the group characteristics in attack profiles. In this research, machine learning and deep learning-based shilling attack detection schemes are proposed for efficient detection by eliminating the limitations of the existing approaches.

In specific, deep learning models are considered to perform well in the detection of obfuscated and hybrid attacks (standard and obfuscated attacks). Deep learning models such as Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) is determined to be ideal and can be potentially applied to the problem of shilling attack detection. The significant deep learning models including C-LSTM, cascade CNN and RNN model, CNN-GRU model are potential in feature extraction and classify the attack patterns into genuine and fake profiles. CNN layers with possibly integration with RNN layers aids in attaining the objective of establishing correlation between different temporal sequences of users and item profiles. Moreover, the outputs of CNN's can act as the input to LSTM and, thus the integrated CNN and RNN models such as CNN-LSTM, CNN-GRU and CNN-BiLSTM-Attention Model (AM) can be significantly applied towards shilling attack detection. This hybrid models are considered to exhibit superior detection accuracy on par with the classical methods with respect to different datasets of diversified configurations and sizes. Motivated by the above facts, three different deep learning shilling attack mechanisms-based CNN-LSTM, CNN-GRU and CNN-BiLSTM-Attention models with an integrated framework is proposed for achieving local feature extraction and estimate long-distance dependencies.

1.2 Research Problem

In the digital world, recommendation systems play an anchor role in preventing the issue of information overload. This recommendation systems facilitates suggestions to the users depending on the behaviour or symmetric activities achieved in the past. These systems have the maximum probability of being attack by shilling attacks as they heavily rely on the behavior of the users. Thus, preventing the recommender systems from shilling attacks' influence is highly essential. In this context, deep learning methods are considered as the ideal and suitable options for attaining accurate detection of shilling attack, since these attacks possesses features with increasing complexity and huge number of ratings. In specific, hybridizing CNN and RNN (LSTM, GRU and BiLSTM with AM model) helps in achieving efficient detection of shilling attacks. This hybrid deep learning model uses the transformed network architecture for deriving the attributes such as user and item-related traits from the user-rated profiles for shilling attack detection. It is capable of modelling and handling the spatial and temporal information inherent with the ratings of the recommendation systems. It enhances the robustness and efficiency of the recommendation systems by alleviating the limitations that are inherent with the state-of the art shilling attack deep-learning methods It also possess the potential of handling the influence of standardized, obfuscated and hybrid attack with the tendency to sustain better accuracy, prediction, recall and F-measure on par with the existing deep learning models that could be used for shilling attack mitigation.

The core focus of this research targets in the design and development of three deep learning models such as CNN-LSTM, CNN-GRU and CNN-BiLSTM-AM for detecting shilling attacks with maximized accuracy in social recommender systems. This research concentrates on the possibility of integrating the proposed deep learning models into a reliable framework using the benefits of RNN and CNN integration feasibility. This research targets on the estimation the potential of the proposed deep learning models such as CNN-LSTM, CNN-GRU and CNN-LSTM-AM using accuracy, precision, recall and F-measure with respect to different attack and filler sizes. This research also concentrates on detecting almost all categories of shilling attack through the benefits of the utilized deep learning models.

In this paper, Hybrid CNN and RNNs-based shilling attack framework is proposed for shilling attack detection based on the selection of dynamic features for attaining maximized detection accuracy. In this framework, CNN model is responsible for local feature extraction, while RNNs models play a vital. Roles in determining long distance dependencies. In specific, RNN instance, such as LSTM, CNN and LSTM-AM are integrated with CNN in this shilling attack framework. The investigations conducted over the integrated model show better detection accuracy on par with the classical RNN and CNN architectures over the datasets that include different configuration and sizes. The major contributions of this proposed Hybrid CNN and RNNs-based shilling attack framework is listed as follows.

i) An integrated novel architecture that combined the merits of CNN and RNNs instance, such as LSTM, CNN and LSTM-AM is developed for achieving better accuracy during the detection of shilling attacks in collaborative filtering-based recommendation systems.
ii)This CNN and RNNs integrated framework are developed as a robust architecture for handling different attack types and sizes.
iii) It is developed with the inclusion of spatial and temporal information that could be possibly derived from the

collaborative filtering-based recommendation systems with an adaptive time segmentation process.

The remaining sections of the paper are organized as follows. Section 2 presents the background and related work of the deep learning-based shilling attack detection schemes propounded for collaborative filtering-based recommendation systems. Section 3 details the complete architecture and the steps involved in the deployment of this CNN and RNNs integrated framework. Section 4 demonstrates the experimental results of the proposed CNN-RNNs shilling attack detection framework with justifications behind its superior performance over the benchmarked approaches. Section 5 concludes the paper and innovates future scope of research directions.

2. Related Work

A Federated collaborative filtering-based Shilling attack detection scheme was proposed Jiang by et al. [16] for facilitating user privacy in social recommendation systems. This shilling attack detection scheme was the first approach propounded in the context of federated learning. It first exhibited the merits of detecting shilling attacks in the Federated collaborative filtering based on the utilization of four important features determined based on exchanged gradients among the clients. It included the advantages of semi-supervised Bayes classifier for training the extracted gradient-based features in order to identify shilling attackers effectively. The extensive experiments of this FCF framework conducted using real-world datasets confirmed better accuracy of 0.90 with respect to Netflix dataset. Then, an integrated binary collaborative and stand-alone rating-based framework was proposed for better detection of shilling attack [17]. This integrated framework was proposed with the dimensions of robustness and binary collaborative filtering for detecting shilling attack. The precision and recall of this framework was determined to be better than the baseline approaches.

An Adaboost-based shilling attack detection framework was proposed for automatic extraction of robust features in order to prevent the re-extraction of features that incurred high knowledge cost [18]. This framework determined robust representation with prior knowledge, which is completely contrasting to the uniform corruption rate included in the marginalized linear denoising autoencoder. It then calculated different corruption rates associated with the items based on the distribution of the ratings. It further weighted the mapping matrix for estimating ratings sparsity in order to extract low-dimensional representation. It also extracted robust and stable user features in order to set the uniform corruption rate. It finally added Adaboost-based detection scheme for preventing the issue of imbalanced classification. The results of this framework confirmed better classification accuracy compared to the baseline frameworks. A dual deep learning shilling attack detection framework was proposed for deriving deeper level features for better classification process [19]. It was proposed as a collaborative filtering-based recommendation method that prevented the use of hand-designed features during shilling attack detection process. It was proposed with the benefits of automatic extracted features in order to reduce the time incurred in detecting shilling attacks in collaborative recommender systems. The rate of misclassification is completely prevented in this shilling attack scheme, such that maximized accuracy can be derived with least amount of communication overhead.

Further, CNN model-based shilling attack detection scheme was proposed for exploiting deep-level features that aided in differentiating genuine profiles from attack profiles with improved accuracy [25]. It adopted the benefits of transformed network structure for deriving deep-level features on par with the artificially designed features, since they can detect shilling attack with efficiency and robustness. The results of CNN model-based detection scheme were proved to be capable enough in precisely detecting most of the obfuscated attacks within minimized time and reduced complexity on par with existing approaches. Then, an integrated CNN-RNN model was proposed for efficient detection of shilling attacks by utilizing the transformed network architecture to handle the potential of the attributes that could be extracted from the user-rated profiles [26]. The included architecture guaranteed the process of modelling the spatial and temporal information from the ratings of the recommender systems. It was proposed for resolving the limitations of the existing deep learning -based shilling attack approaches for improving the robustness and efficiency of the recommender systems. The results of this CNN-RNN model confirmed better classification accuracy, precision, recall and F-Measure compared with the experiments conducted with Netflix and MovieLens 100K datasets by detecting majority of the obfuscated attacks on par with the existing deep learning-based shilling attack detection models of the literature.

Another CNN model that constructs detection method without restoring the hand-designed features is proposed for determining attack user profiles with maximized efficiency [27]. It was proposed with the capability of directly learning the low-level rating data for the purpose of classifier training and ignored the issues incurred during the process of handling hand-crafted features. It included the method of rating matric generation for converting the rating vector into rating matrix for every individual user. It included the merits of bicubic interpolation algorithm for resizing the dimensionality of the rating matric for sparsity reduction over the rating matrix. Extensive experiments of this proposed CNN model conducted with respect to the MovieLens dataset confirmed better classification accuracy of 23.19%, better than the existing deep learning models. A stack denoising autoencoders-based shilling attack detection model was proposed for automatic extraction of user features during detection of shilling attacks even under different filler rates [28]. It was proposed as ensemble detection approach that extracted automated features from multiple dimensional views. It adopted a strategy that

collaboratively identifies the attacker profiles from which the user characteristics are explored from the views of use-user graph, item popularity and ratings. It was significant enough in attaining data pre-processing of features from multiple views, such that PCA can be used for features in integration. It detected attacks by generating and integrating weak classifiers depending on the features derived with varying rates of corruption. Extensive experiments of this proposed CNN model conducted with respect to the Netflix, Amazon and MovieLens dataset confirmed better.

3. Proposed Hybrid CNN and RNNs-based shilling attack framework elated Work

This Hybrid CNN and RNNs-based shilling attack framework is proposed based on the characteristic features of CNN and RNNs. This proposed framework comprises of three layers as depicted in Figure 1.

In the proposed framework, the rating matrix is first transformed into a three-dimensional array consisting of days, items and users in the first input layer. Then, a CNN model in the second layer is employed to the data input, whose input is conveyed into the output by the included LSTM, GRU and LSTM-AM model. Finally, the framework aided classified users into two categories such as genuine and attack users in the input layer based on the RNN model. In this integrated architecture, the CNN layer is mainly responsible for feature selection. The RNN layer plays an anchor role in iterating the operation in order to construct the internal state. This proposed framework was developed with the three different integrated models such as LSTM, GRU and LSTM-AM that inherits the CNN and RNN layers. The first model included into the framework is the LSTM model. The second model included into the framework for shilling attack detection is the GRU model, since it is determined that GRU performs well compared to the LSTM model. In this framework, user ratings associated with each item are aggregated on a daily basis, which is completely different from the previous studies that employed the merits of RNN and CNN individually on item or user-based data. A three dimensional array of users' items and days are constructed and utilized in the proposed framework. Moreover, time features existing in the constructed three dimensional array is considered for deriving the rating sequences in the RNNs. Then, the ratings are daily aggregated and further included into the framework as the input. It further facilitated an adaptive time segmentation, such that level of aggregation can be extended and selected based on the properties of the dataset. In this context, the segmentation is attained by changing the ratings level aggregation determined over time, such as the data derived over hours, daily, weekly, etc. It utilized the time distributed in Keras for extracting the feature ratings and investigate them over specified period of time for the purpose for constructing a hybrid model of RNNs and CNNs. This wrapper facilitates the model for applying he layer for every individual input temporal slice. This framework network architecture has been developed with the time-distributed wrapper that employed a two-dimensional convolutional layer with Relu activation function, 32 hidden neurons and 3x3 kernel size. The input goes through the max-pooling layer, drop out and flatten layer before the process of detecting shilling layer attacks in order to classify them into its actual type such as random, average, bandwagon attacks.

`

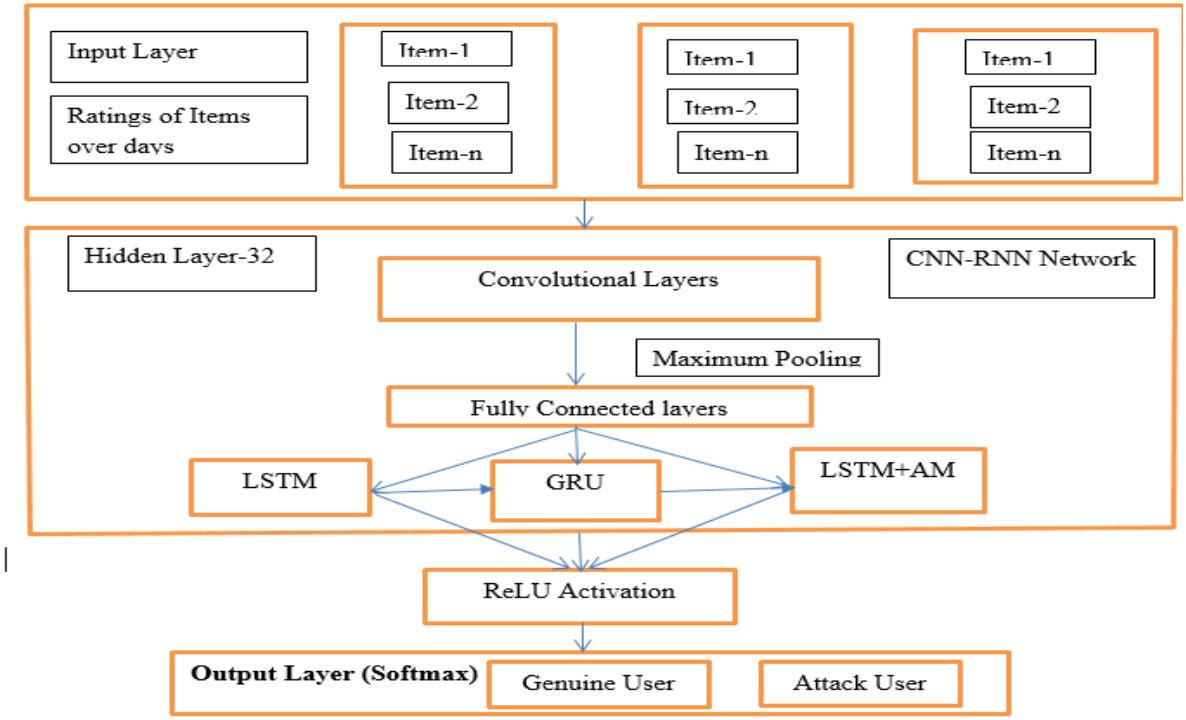

Figure 1. Proposed Hybrid CNN and RNNs-based shilling attack framework

In the first utilized CNN-LSTM model, the LSTM layer comprises of 32 hidden neurons, Relu activation function inherited dense layer, a layer of drop out and an additional dense layer with the function of Softmax to achieve better classification of users into the attacker and genuine user profiles. In the second incorporated CNN-GRU model, a structure of the previous CNN-LSTM model is used with a GRU layer consisting of 32 hidden neurons in the layer of RNN in supplement to the Relu activation functions, a Softmax activation function-based dense layer and one layer of drop out. In the third employed CNN-LSTM-AM model, the previous configurations of CNN-LSTM and CNN-GRU are utilized with a meagre amount of modifications for attaining its maximized functionality. In all the three models, the merits of categorical cross entropy and Adam optimized is used as the loss function and optimizer, respectively. The process of feature extraction is performed over the two dimensional array of ratings associated with the items determined on a daily basis, such that RNN layer uses the result in order to categorize the users into attack and genuine profiles. The attack profiles are injected through different attack parameters and models, assuming that the existing users in the dataset are completely genuine users. Further, selected item set, filter item set and a target item set are defined for every individual attack profile. The attacks that are injected into the user profiles pertains to the type of push attack. But, the only difference between the nuke and push attack type is the target items ratings. The push attack completely depends on the maximum possible rate of the users about an item existing in the recommendation system. While, the nuke attack depends on the minimum possible rate of the users about an item existing in the recommendation system. This proposed shilling attack detection framework is applicable to both push and nuke attacks. Furthermore, Table 1 explains the logic which is involved in the process of generating attack profiles.

Table 1. Attack model logic considered in this CNN-RNNs framework

Attack Model	Filler Item Set		Selected Item Set		Target Item Set
	Items	Ratings	Items	Ratings	
AOP	x% of popular items	$N(Ar_{(i)}, SD_{(i)})$	Not used		Maximum possible users rate
Bandwagon	Randomly selected	$Ar_{(i)}$	Popular Items	Maximum possible users rate	Maximum possible users rate
Average	Randomly selected	$N(Ar_{(i)}, SD_{(i)})$	Not used		Maximum possible users rate
Random	Randomly selected	$N(Ar_{(i)}, SD_{(i)})$	Not used		Maximum possible users rate

Moreover, the parameters of attack size and filler items are defined before the process of the attack profiles injection process. The filler item parameter aids in selecting a number of filler items and the attack size parameters affect the fake users count. In addition, the target items are randomly selected and their related values are set to a fixed value. In this proposed framework, the value of randomly selected target items is set to 100. In the bandwagon attack model, the popular items refers to the set of items that are rated by a huge user group. At this juncture, and refers to the mean and standard deviation of all the ratings existing in the complete dataset. Moreover, and pertains to the mean and standard deviation of all the ratings associated with an item 'i'. In the experimental process, the value of Maximum possible user's rate is set to 5. In the case of the average over popular (AOP) attack, the number of filler items is determined based on x% of the popular items. In specific, 1% of the popular items are considered in determining the number of filler items in the AOP attack. In the shilling attack mitigation framework, four important attacks such as AOP, bandwagon, average and random are randomly selected and they are assigned to a fixed value. The total number of randomly selected items in the framework for individual exploration is set to 100.

4. Simulation Results and Discussions

The simulation experiments of the proposed CNN-RNNs-based shilling attack framework is conducted based on the benchmarked datasets of MovieLens 100 K and Netflix. In the MovieLens 100 K dataset, 100000 number of ratings about 1682 movies rated by 943 users are provided. The ratings provided by the users range between the values of 1 to 5, in which the best movie is indicted through the rating value of 5 by the users. The dataset of Netflix comprises of ratings of movies provided by 470748 users. Only a subset of Netflix dataset is considered for experimental purposed as the size of the MovieLens 100 K dataset is comparatively very small in size. The subset of the Netflix dataset considered for experimentation comprises of at least 60 rates that are determined randomly from 1238 users over a period of seven months. The MovieLens 100 K and Netflix dataset considered for experimentation are partitioned for the purpose of training and testing, by considering 30% of the dataset as the test data. This proposed CNN-RNNs-based shilling attack framework is evaluated based on the performance metrics of accuracy, precision, recall, F1-measure and false positive rate [19-20].

In the first part of the investigation, Figure 2 and 3 exemplars the potential of the proposed CNN-RNNs-based shilling attack framework and the benchmarked HDLM and RMRA frameworks evaluated based on accuracy and precision determined under different filler size considered with the Netflix dataset. The classification accuracy of the proposed CNN-RNNs-based shilling attack framework with different filler size (Netflix dataset) was determined to be improved by 4.59% and 5.84%, better than the benchmarked HDLM and RMRA frameworks. The precision value of the proposed CNN-RNNs-based shilling attack framework was also identified to be improved by 4.59% and 5.82%, superior to the baseline HDLM and RMRA frameworks.

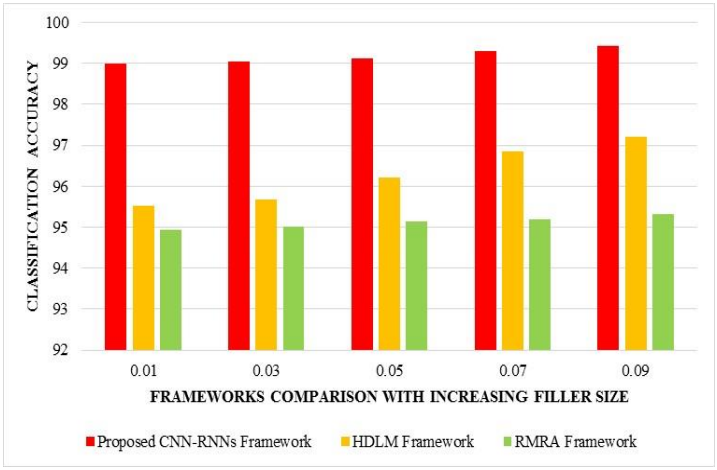

Figure 2. Proposed CNN-RNNs-based shilling attack framework-accuracy-Movielens 100k

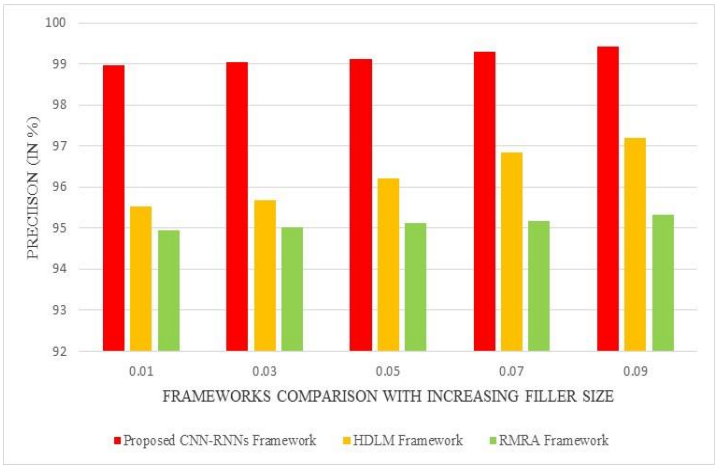

Figure 3. Proposed CNN-RNNs-based shilling attack framework-Precision-Movielens 100k

Figure 4. Proposed CNN-RNNs-based shilling attack framework-Recall-Movielens 100k

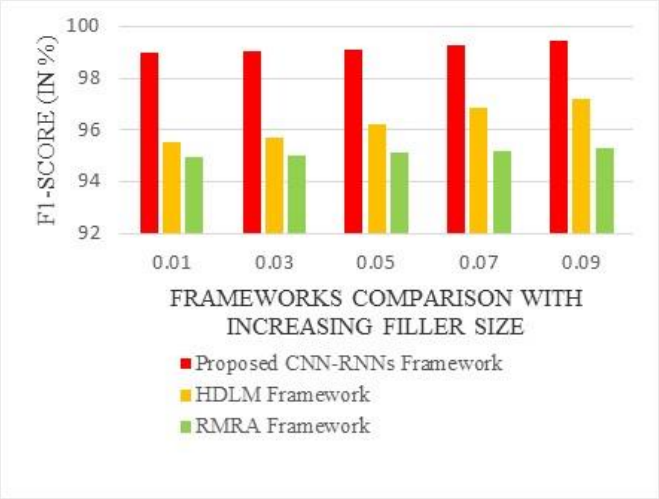

Figure 5. Proposed CNN-RNNs-based shilling attack framework-F1-Score-Movielens 100k

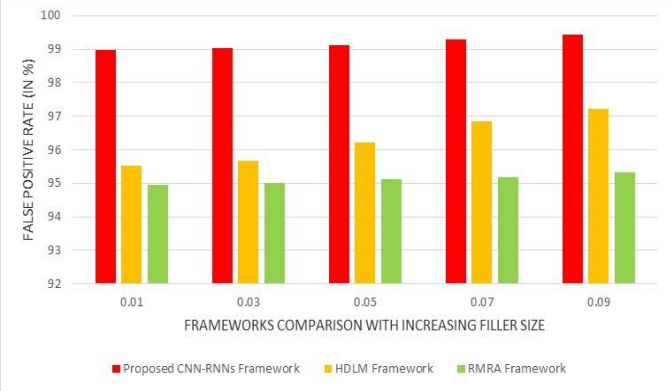

Figure 6. Proposed CNN-RNNs-based shilling attack framework-False Positive Rate-Movielens 100k

Figure 4 and 5 portrays the potential of the proposed CNN-RNNs-based shilling attack framework and the benchmarked HDLM and RMRA frameworks based on the false positive rate under different filler size considered during shilling attack detection. The proposed CNN-RNNs-based shilling attack framework was determined to improve the recall with different filler size under Netflix dataset by 4.48% and 6.14%, better than the benchmarked HDLM and RMRA frameworks. The proposed CNN-RNNs-based shilling attack framework was determined to improve the F1-measure by 5.26% and 6.72%, better than the benchmarked HDLM and RMRA frameworks. In addition, Figure 6 depicts the performance of the proposed CNN-RNNs-based shilling attack framework and the benchmarked HDLM and RMRA frameworks based on the false positive rate under different filler size considered during shilling attack detection. The proposed CNN-RNNs-based shilling attack framework was determined to minimize the false positive rate by 4.82% and 5.94%, better than the benchmarked HDLM and RMRA frameworks.

In the second part of the investigation, Figure 7 and 8 demonstrates the predominance of the proposed CNN-RNNs-based shilling attack framework and the benchmarked HDLM and RMRA frameworks evaluated based on accuracy and precision determined under different filler size considered with the Netflix dataset. The classification accuracy of the proposed CNN-RNNs-based shilling attack framework with different filler size (Netflix dataset) was determined to be improved by 4.59% and 5.84%, better than the benchmarked HDLM and RMRA frameworks. The precision value of the proposed CNN-RNNs-based shilling attack framework was also identified to be improved by 4.59% and 5.82%, superior to the baseline HDLM and RMRA frameworks.

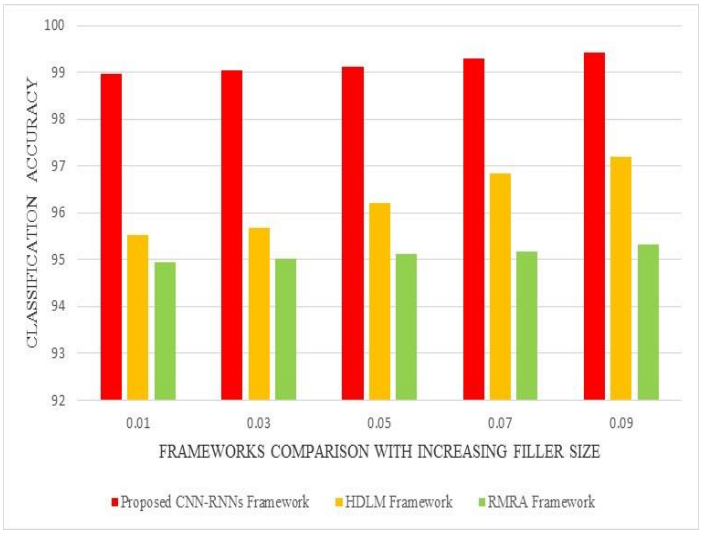

Figure 7. Proposed CNN-RNNs-based shilling attack framework-accuracy- Netflix

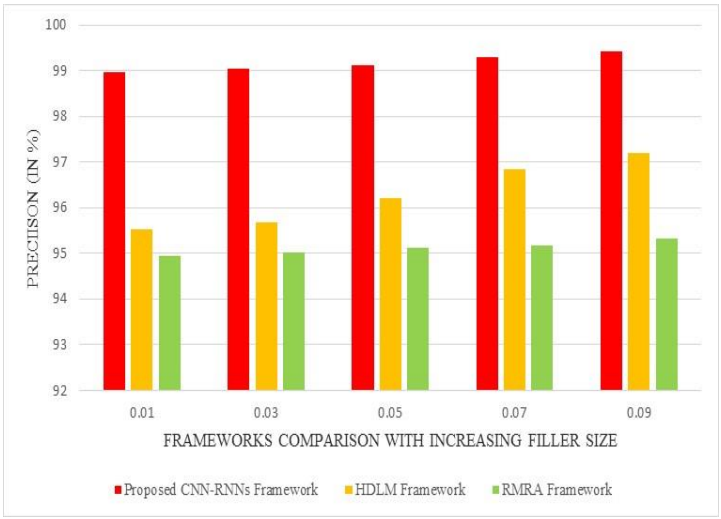

Figure 8. Proposed CNN-RNNs-based shilling attack framework-Precision- Netflix

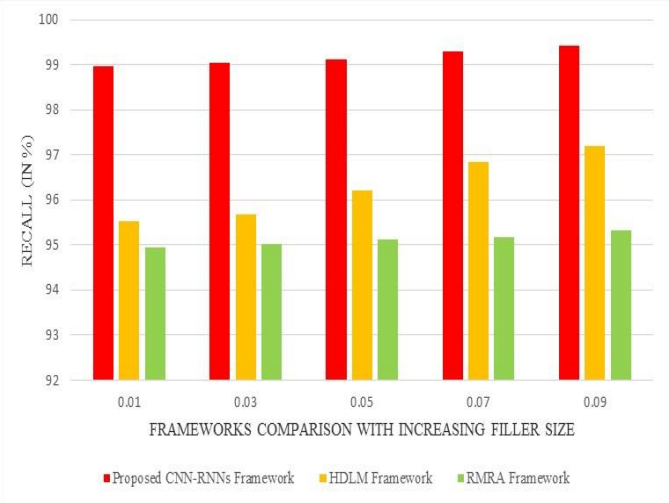

Figure 9. Proposed CNN-RNNs-based shilling attack framework-Recall- Netflix

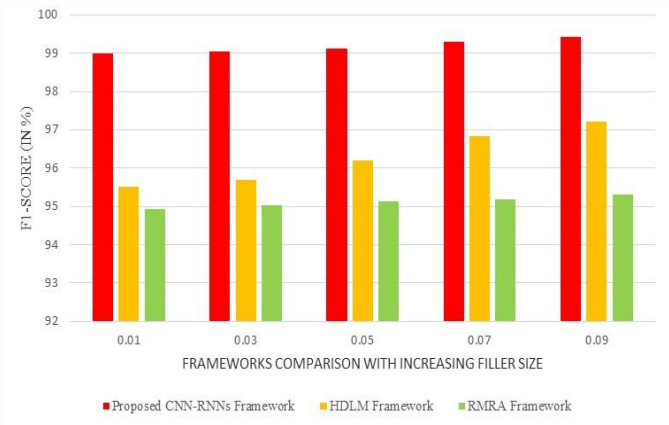

Figure 10. Proposed CNN-RNNs-based shilling attack framework-F1-Score- Netflix

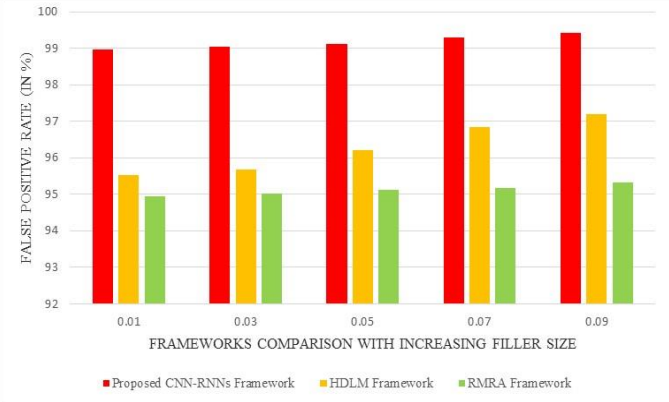

Figure 11. Proposed CNN-RNNs-based shilling attack framework-False Positive Rate-Netflix

Figure 9 and 10 highlights the potential of the proposed CNN-RNNs-based shilling attack framework and the benchmarked HDLM and RMRA frameworks based on the false positive rate under different filler size considered during shilling attack detection. The proposed CNN-RNNs-based shilling attack framework was determined to improve the recall with different filler size under Netflix dataset by 4.48% and 6.14%, better than the benchmarked HDLM and RMRA frameworks. The proposed CNN-RNNs-based shilling attack framework was determined to improve the F1-measure by 5.26% and 6.72%, better than the benchmarked HDLM and RMRA frameworks. In addition, Figure 11 present the performance of the proposed CNN-RNNs-based shilling attack framework and the benchmarked HDLM and RMRA frameworks based on the false positive rate under different filler size considered during shilling attack detection. The proposed CNN-RNNs-based shilling attack framework was determined to minimize the false positive rate by 4.82% and 5.94%, better than the benchmarked HDLM and RMRA frameworks.

5. Conclusion

In this paper, the Hybrid CNN and RNNs-based shilling attack framework is proposed for shilling attack detection based on the selection of dynamic features for attaining maximized detection accuracy. This framework integrated user popularity and rating-based indicators in order to consider the deviations that happens, when the users select items. It also included information entropy for dynamically choosing the detection indicators in order to improve the reliability in attack detection. It was proposed with three different attack detection models that contextually handles different shilling attacks. The proposed CNN-RNNs-based shilling attack framework was determined to improve the recall with different filler size under Netflix dataset by 4.48% and 6.14%, better than the benchmarked HDLM and RMRA frameworks. The proposed CNN-RNNs-based shilling attack framework was determined to minimize the false positive rate by 4.82% and 5.94%, better than the benchmarked HDLM and RMRA frameworks.

References

[1] Kaur, P., & Goel, S. (2016, August). Shilling attack models in recommender system. In *2016 International conference on inventive computation technologies (ICICT)* (Vol. 2, pp. 1-5). IEEE.

[2] Qi, L., Huang, H., Li, F., Malekian, R., & Wang, R. (2019). A novel shilling attack detection model based on particle filter and gravitation. *China Communications*, *16*(10), 112-132.

[3] Deng, Z. J., Zhang, F., & Wang, S. P. (2016, July). Shilling attack detection in collaborative filtering recommender system by PCA detection and perturbation. In *2016 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR)* (pp. 213-218). IEEE.

[4] Cai, H., & Zhang, F. (2019). An unsupervised method for detecting shilling attacks in recommender systems by mining item relationship and identifying target items. *The Computer Journal*, *62*(4), 579-597.

[5] Yuan, W., Xiao, Y., Jiao, X., & Ming, Y. (2019, November). Neural Network Detection of Shilling Attack Based on User Rating History and Latent Features. In *2019 International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI)* (pp. 229-232). IEEE.

[6] Qi, L., Huang, H., Wang, P., & Wang, R. (2018, August). Shilling Attack Detection Based on Data Tracking. In *2018 13th International Conference on Computer Science & Education (ICCSE)* (pp. 1-4). IEEE.

[7] Luo, Z., & Liang, C. (2016, August). An insider attack on shilling attack detection for recommendation systems. In *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)* (pp. 277-280). IEEE.

[8] Zhang, F., & Wang, S. (2020). Detecting Group Shilling Attacks in Online Recommender Systems Based on Bisecting K-Means Clustering. *IEEE Transactions on Computational Social Systems*, *7*(5), 1189-1199.

[9] Li, X., Gao, M., Rong, W., Xiong, Q., & Wen, J. (2016, June). Shilling attacks analysis in collaborative filtering based web service recommendation systems. In *2016 IEEE International Conference on Web Services (ICWS)* (pp. 538-545). IEEE.

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

[11] Jiang, Y., Zhou, Y., Wu, D., Li, C., & Wang, Y. (2020, September). On the detection of shilling attacks in federated collaborative filtering. In *2020 International Symposium on Reliable Distributed Systems (SRDS)* (pp. 185-194). IEEE.

[12] Bansal, S., & Baliyan, N. (2019, September). Evaluation of Collaborative Filtering Based Recommender Systems against Segment-Based Shilling Attacks. In *2019 International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 110-114). IEEE.

[13] Hao, Y., Zhang, F., & Chao, J. (2019). An ensemble detection method for shilling attacks based on features of automatic extraction. *China Communications*, *16*(8), 130-146.

[14] Ebrahimian, M., & Kashef, R. (2020, December). Efficient Detection of Shilling's Attacks in Collaborative Filtering Recommendation Systems Using Deep Learning Models. In *2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)* (pp. 460-464). IEEE.

[15] Alonso, S., Bobadilla, J., Ortega, F., & Moya, R. (2019). Robust model-based reliability approach to tackle shilling attacks in collaborative filtering recommender systems. *IEEE Access*, *7*, 41782-41798.

[16] Chichani, A., Golwala, J., Gundecha, T., & Gawande, K. (2018, July). Advancing Recommender Systems by Mitigating Shilling Attacks. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.

[17] Hu, D., Xu, B., Wang, J., Han, L., & Liu, J. (2020, November). A Shilling Attack Model Based on TextCNN. In *2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE)* (pp. 282-289). IEEE.

[18] Cai, H., & Zhang, F. (2019). BS-SC: An Unsupervised Approach for Detecting Shilling Profiles in Collaborative Recommender Systems. *IEEE Transactions on Knowledge and Data Engineering*.

[19] Lu, W., Li, J., Wang, J., & Qin, L. (2021). A CNN-BiLSTM-AM method for stock price prediction. *Neural Computing and Applications*, *33*(10), 4741-4753.

[20] Ebrahimian, M., & Kashef, R. (2020). Detecting Shilling Attacks Using Hybrid Deep Learning Models. *Symmetry*, *12*(11), 1805.

[21] Xie, Q., Huang, J., Peng, M., Zhang, Y., Peng, K., & Wang, H. (2019, November). Discriminative Regularized Deep Generative Models for Semi-Supervised Learning. In *2019 IEEE International Conference on Data Mining (ICDM)* (pp. 658-667). IEEE.

[22] Subramani, S., Michalska, S., Wang, H., Du, J., Zhang, Y., & Shakeel, H. (2019). Deep learning for multi-class identification from domestic violence online posts. *IEEE Access*, *7*, 46210-46224.

[23] Zhang, F., Wang, Y., Liu, S., & Wang, H. (2020). Decision-based evasion attacks on tree ensemble classifiers. *World Wide Web*, *23*(5), 2957-2977.

[24] Jiang, H., Zhou, R., Zhang, L., Wang, H., & Zhang, Y. (2019). Sentence level topic models for associated topics extraction. *World Wide Web*, *22*(6), 2545-2560.

[25] Tong, C., Yin, X., Li, J., Zhu, T., Lv, R., Sun, L., & Rodrigues, J. J. (2018). A Shilling attack detector based on convolutional neural network for collaborative recommender system in social aware network. The Computer Journal, 61(7), 949-958.

[26] Ebrahimian, M., & Kashef, R. (2020). Detecting Shilling attacks using hybrid deep learning models. Symmetry, 12(11), 1805.

[27] Zhou, Q., Wu, J., & Duan, L. (2020). Journal of Information Security and Applications, 52(2), 102493.

[28] Hao, Y., Zhang, F., Wang, J., Zhao, Q., & Cao, J. (2019). Detecting Shilling attacks with automatic features from multiple views. Security and Communication Networks, 2019(1), 1-13.