International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No. 44, May 2024 – www.ijais.org

Data Security Concerns in Approaches to Overcome Cold Start Problem in Recommender Systems - A Survey

Kanishkar Indira
Department of Computer Science and Engineering,
SRM University, Chennai, India

Kiruthi Thaker
School of Business Economics & Technology,
Campbellsville University, USA

ABSTRACT
In the subject of recommendation engines, the cold start problem is a significant research topic. Due to a lack of knowledge about the user and/or services, the recommendation system is unable to predict the user's preferences or interested products, resulting in a cold start. Many people have sought to overcome the cold start problem in recommending generic domains such as music, movies, E-Commerce, and travel websites using different types of machine learning models. This work provides a survey of the most recent to the traditional methods used for solving the cold start problem and also provides a holistic view of the adversarial attacks that are possible on the machine learning models used while trying to solve the cold start problem using the machine learning models.

General Terms
Data Security, Recommender Systems, Cold Start Problem

Keywords
Cold start, Recommendation Engine, Recommender Systems, Natural Language Processing, NLP, Adversarial attacks, Security, Machine Learning, Cloud Computing, Distributed Systems

1. INTRODUCTION
Most online content platforms such as e-commerce websites contain recommender systems for both items and services recommendation that return the top-K things in response to a natural-language query, given the user context, which could include the user's traits and personal information [1].

The output item space may be the same for both, but the input feature spaces are different. For example, it may be easy to gather information or make inferences of a user's preferences for personal or common items recommendations like a handbag or a book. However, it will be very difficult to make inferences to recommend domain specific services like the cloud services [2] which may involve various complications like the multiple functional and nonfunctional requirements to be met for recommending a useful recommendation to the user. The domain specific nature of the service may also require various natural language processing techniques to be applied to extract domain knowledge required to generate recommendations like the taxonomy, ontology, or the knowledge graph [3] of the domain to make a relevant recommendation to the user. These complex scenarios when comes with lack of user preference data leads to the cold start problem. Cold start problem in the application of recommender systems, this generally relates to modeling new users (no past interactions with the system) or new items (no records of being eaten by users). Most methods assume that some user or item side feature information is available, allowing the representation of a new user or item to be inferred. Recommending new services to new customers, recommending new services to existing users, and recommending existing services to new users are all examples of the cold start problem.

Most research efforts have used various approaches independently and in combination with other known techniques to tackle the cold start problem, as seen by the techniques listed above in the literature. This strategy is primarily focused on resolving the cold start issue for generic Business to Customer (B2C) E-Commerce domains. These approaches, on the other hand, could not be employed to solve the cold start problem in B2B E-Commerce domains such as cloud services. This is because data regarding user preferences is sparse for these types of domain-specific services, and recommending a service frequently necessitates the fulfillment of numerous criteria. Furthermore, the cost of losing a customer is significant. Knowledge graphs play a vital role in understanding the relationship between the various entities to be recommended in a domain specific environment. A taxonomy of the entities belonging to the domain is essential to capture the relationship between the various entities. The taxonomy is then converted to an ontology-based knowledge graph which can be further queried to get the information related to the entity. Thus, collaborative filtering methods cannot be used to recommend technical services such as the new type of cloud services, since user requirements for each project may differ, and it would be difficult to discover users with comparable interests or requirements during the cold start phase. This work also covers the adversarial attacks that need to be taken care of while designing the machine learning approaches to overcome the cold start problem and in designing the recommender system in general.

This work discusses on the following topics: a) A detailed survey of the techniques used to overcome the cold start problem in the recommender systems is given in section I b) The methods in which Adversarial attacks are carried out on Machine Learning models used in Recommender Systems is explained in section II c) The techniques used to attack the recommender system itself versus the machine learning model used in recommender system is explained in detail in section III d) Section IV provides a detailed discussion and conclusion.

2. METHODS FOR DEALING WITH THE COLD START PROBLEM IN RECOMMENDER SYSTEMS
Wang H et al [4] offer DotMat, a novel algorithm based on the Zipf Distribution and a reformulation of the RankMat algorithm, in this study. The method can achieve high accuracy and fairness metrics while requiring no information from the user item rating matrix.

Zhao X et al [5] developed the model-agnostic CVAR for item cold start in this research, which employs latent variables to learn a distribution across side information and then uses a conditional decoder to build acceptable ID embeddings. CVAR generates enhanced warmed-up embeddings with superior quality by learning the pattern in past data as well as leveraging the continuously updating item ID embedding from the backbone for better cold-start performance. In terms of industrial practice, we believe that the more stringent data requirements of cold-start approaches will make the deployment process in an online context more complex. As a result, CVAR is built to be trained using the same raw samples as the main prediction model. It's important to note that the suggested CVAR is a generic framework that can be used with a variety of backbones. Finally, numerous offline testing on public datasets as well as online A/B tests demonstrates CVAR's efficacy and compatibility.

With the CGAN framework and matrix injection method, Xu Y et al [6] have proposed GS2 -RS, a unique framework for addressing cold-start and filter-bubble problems. We demonstrated that GS2 -RS is effective in dealing with both difficulties using empirical trials on public datasets: When compared to SOTA RS models, GS2 -RS improves accuracy, diversity, and serendipity. We hope to expand GS2 -RS in the future to include photos (with GCN), social networks (with KG), and context (with NLP)

SRLGAN, a unique Cold-Start Recommendation model, is proposed by Shah AA et al [7], which takes advantage of the sparsity in the user purchase behavior distribution during training. The SRLGAN model uses a sparse penalty based on KL-divergence to reduce the dissimilarity between the ground truth user buy behavior distribution and the produced user purchase behavior distribution, resulting in robust collaborative filtering for highly sparse datasets. Extensive tests on two well-known benchmark datasets show that the SRLGAN outperforms other methods. It also confirms that the sparse penalty we proposed prevents the model from overfitting and collapsing into mode collapse. We want to test the SRLGAN's performance on the related problem of item-based Cold-Start recommendation in the future, which is comparable to the user-based problem in that the item-user interaction data is sparse.

In this study, Wang H et al [8] offer ZeroMat, a new method for solving the cold start problem that requires no data input as the starter. By a wide margin, our method outperforms the random recommendation. Even when compared to traditional matrix factorization, the method is competitive in terms of MAE and fairness. There are two implications: 1. It is an excellent tool for dealing with the cold-start issue. 2. Matrix factorization approaches are woefully inadequate. In this paper, Feng X et al [9] propose a contextual modulation meta learning framework with many algorithmic possibilities for handling cold-start recommendation problems. The cold-start recommendation problem is formulated as a meta learning problem. The system can easily adapt to new objectives, even with minimal interaction examples, thanks to its context encoder, hybrid context generator, and modulation network. Extensive studies on real-world datasets have proven that CMML is effective in terms of computational performance and interpretability. Furthermore, the entire framework is fully compatible with the existing actual industrial framework, allowing for a wider range of applications.

Wang Z et al [10] highlights two issues of user cold start recommendation in travel platforms in this paper: I It's difficult to identify a cross-domain user who behaves similarly in trip scenarios. ii) Users' LBS information has received insufficient attention. To solve this issue, we offer a heterogeneous relations model based on LBS. To establish the heterogeneous relations between people and items, LHRM uses user's LBS information and behavior information in the Taobao domain and user's behavior information in the Fliggy domain. In addition, to extract latent characteristics of users and items, an attention-based multi-layer perceptron is used. The efficiency of LHRM is demonstrated by experimental findings using real data from Fliggy's offline log.

Contrastive Learning-based Cold-start Recommendation is a broad cold-start recommendation framework that includes contrastive pair organization, contrastive embedding network, and contrastive optimization proposed by Wei Y et al [11]. We do thorough tests on four datasets to prove the effectiveness and efficiency of our proposed technique, which outperforms state-of-the-art baselines in both warm- and cold-start scenarios by a considerable margin. Briand L et al [12] present the approach that was recently installed on the music streaming service Deezer to address this challenge in this applied paper. The approach employs a semi-personalized recommendation strategy based on a deep neural network architecture and user grouping from disparate information sources. Through both offline and online large-scale tests, we demonstrate the practical impact of this method and its effectiveness at predicting the future musical preferences of cold start users on Deezer.

Our goal in this research by Zhang Y et al [13] is to see if social media background can be used as additional contextual information to improve recommendation algorithms. They have proposed a way to describe temporal social media background as embeddings and merge them as an extra component in the model based on an existing deep neural network model. On a real-world e-commerce dataset and a Twitter dataset, Zhang Yet al [14] have conducted experimental evaluations. The results demonstrate that combining social media background with an existing algorithm improves recommendation performance in general. After fusing with social media background, the suggestion accuracy assessed by hit-rate@K doubles in some circumstances. Our findings may be useful in the development of future recommender systems that take into account complex temporal information expressing social interests. ColdGAN, a unique end-to-end GAN-based model, is initially introduced in this research by Lai PL et al [15] to infer experienced user ratings from their cold-start states without using side information for tackling new user cold-start challenges.

A knowledge graph and content-based machine learning algorithm-based method has been proposed to overcome cold start problems in multicriteria recommendation systems [16]. The proposed work also recommends the domain specific cloud renderfarm services to render medical image files by ranking the services using multi criteria decision making algorithms [17]. Zhou Y et al [18] used users' item ratings are restored to their cold-start conditions by the suggested time-based rejuvenation function, which is then incorporated into the GAN model for efficient model training. Furthermore, they change the original GAN's loss function to address the Mode collapse issue. Extensive studies on two real-world datasets show that rejuvenation and relevant loss greatly beat state-of-the-art techniques in the cold-start recommendation system, not only in terms of accuracy but also in terms of effectiveness. Notably,

the presented model also paves the way for future research into using GAN to solve new item cold-start issues. In this study, they focused on "Cold Start" customers who have a detrimental impact on the recommender's performance.

The Continuous Cold Start Problem exists in the travel site's recommendation area, and Lucas Bernardi et al [19] have sought to solve it. The Context aware collaborative filtering strategy was utilized in this study to overcome the cold start problem, which takes into account the visitor's current context as well as the behavior of other users in similar situations. Using multi criteria ranking algorithms used in expert systems domain like the AHP, TOPSIS etc to rank the cloud services [20] based on the various functional requirements of the cloud services like the security adherence or data center location to ensure privacy protection has been explored to overcome the cold start problem in recommending domain specific services like the cloud renderfarm services has been explored by Ruby et al [21].In E-Commerce, Jin-Hu Liu et al [22] proposed approaches for promoting commodities in cold-start scenarios. The Top-k closest neighbor algorithm was utilized to achieve Item based Collaborative filtering in this study. Michele Trevisiol et al [23] developed a strategy to solve the cold start problem in news item recommendation. To tackle the cold start problem, topical filtering and content-based filtering methods were applied in this study. Ruby et al have worked on applying the content-based machine learning and collaborative filtering machine learning methods to overcome the cold start problem in recommending cloud renderfarm services. Xavier Amatriain et al [24] investigated the approach of mining large streams of user data for personalized recommendations. They used collaborative filtering approaches to estimate the movie rating in this study. Martin Saveski et al. [25] propose using the Multiplicative update rules-based learning algorithm to learn Local Collective Embeddings to overcome the cold start problem in E-Commerce. Xiwang Yang et al [26] employed the Bayesian-inference Based Recommendation technique in Online Social Networks to overcome the cold start problem. Users share their content ratings with peers, and the similarity between two friends is calculated as part of their job.

The method proposed by Chien Chin Chen et al [27] integrates a user model with trust and distrust networks to identify trustworthy users for movie recommendation using the clustering method. Christopher Krauss et al [28] employed the strategy of using customers viewing behavior and explicit user ratings to estimate user preference for a TV program. Katrien Verbert et al. [29] investigate information visualization strategies for interacting with recommender systems and using collaborative filtering for recommending conferences, whereas Pankaj Gupta et al. [30] employ graph recommendation algorithms for Twitter's user recommendation service. Jesus et al. [31] used Jaccard similarity measures to produce movie recommendations for people who had submitted fewer votes. In order to solve the cold-start problem, N.M.Heung et al [32] used collaborative error-reflected models.

For cold start movie recommendations, S.T.Park et colleagues [33] used a regression technique. To tackle the cold start problem, S. Loh et al [34] used collaborative filtering methods and similarity function methods to select scientific publications. Whereas in the work of L. Martnez et al. [35], a knowledge-based filtering method was utilized to smooth out the cold-start in collaborative recommender systems using the Collaborative filtering algorithm. Item taxonomies and item preference data are suggested by LT. Weng et al [36] for recommending books. Ruby et al have worked creating a taxonomy [37] of the entities belonging to the cloud renderfarm services domain which is essential to capture the relationship between the various entities in the animation domain. The taxonomy is then converted to an ontology [38] based knowledge graph which can be further queried to get the information required to recommend the cloud renderfarm services. The content was integrated into collaborative filters to propose movies using the Cross-Level Association RulEs (CLARE). In contrast, S.T. C.W. Leung et al. [39] offered a method for overcoming the cold start problem based on an empirical investigation of cross-level association rule mining.

To improve Collaborative Filtering algorithms, Park et al [40] investigates filterbots or surrogate users' rating methods. P.B. Ryan et al [41] employed Formal Concept Analysis (FCA) for collaborative filtering when proposing movies. A. Schein et al [42] combined content and collaborative data into a single probabilistic framework for movie recommendation. Knowledge graphs play a vital role in understanding the relationship between the various entities to be recommended in a domain specific environment. A taxonomy of the entities belonging to the domain is essential to capture the relationship between the various entities. The taxonomy is then converted to an ontology-based knowledge graph which can be further queried to get the information related to the entity in the work of Ruby et al [43].

3. ADVERSARIAL ATTACKS ON MACHINE LEARNING MODELS USED IN RECOMMENDER SYSTEMS

Deep learning (DL) breakthroughs have significantly improved the intelligence of machine learning (ML) models in a variety of predictive tasks, such as predicting items to be recommended for buying. Despite their widespread popularity, recent research has revealed that ML/DL models are not immune to security vulnerabilities posed by hostile AI use. Attacks can be classified using three primary dimensions: attack timing, attack goal, and ML model. An adversary can target a machine learning model at two stages of the learning pipeline: training and production. These two types of attacks are called a) training-time attack or causal or poisoning attack and (b) inference-time attack or exploratory or evasion attack [44]

The purpose of data poisoning attacks is to distort or degrade the model by adding fake data points into the training data. Poisoning attacks have been investigated in the literature for a variety of tasks [45], like binary classification attacks for tasks like label flipping or against kernelized SVM [46], (ii) unsupervised learning attacks like clustering and anomaly detection [47]. In their work [48], for example, the authors propose a poisoning approach based on features of the SVM optimal solution that could dramatically reduce classification test accuracy.

Attack of evasion or evasion attacks, unlike poisoning attacks, do not affect training data. During the inference phase, they alter harmful samples. These assaults are also known as decision-time attacks since they try to avoid the learned model's decision at test time [45]. Evasion attacks, for example, can be used to get through spam [49] and network intrusion [139] detectors. Recently, evasive attacks have been carried out by adding adversarial examples to original data, which are minor but non-random human-invisible alterations that lead the learnt model to give incorrect output.

Attacks are carried out for a variety of goals. There are two types of assault goals: a) untargeted attack and b) targeted attack. We formally define adversarial attacks and defense tactics for a classification assignment [45] to give the reader an intuitive understanding of the process behind them. In an untargeted adversarial attack or misclassification, the attacker's purpose is to inject a small amount of disturbance to the input sample to induce inaccurate classification. Whereas, in targeted adversarial attack, the attacker's goal is to disrupt the input with a small amount of perturbation so that the model misclassifies the disturbed sample into an illegitimate target class and to mis-classify the label. A detailed survey on this topic is given in the work of Deldjoo et al [50]. The differences between the adversarial attacks on recommender systems and machine learning models used for classification and recommendation learning tasks is discussed in detail below.

3.1 Shilling attacks in Recommender Systems

The recommender systems attacks are primarily focused on hand-engineered phony user profiles that resulted in shilling assault to manipulate the rating-based Collaborative Filtering [51, 52]. The purpose of a shilling attack, given n legitimate users and m items, is to add a fraction of malicious users with each malicious use profile including ratings to a maximum number of products. The final purpose is to capture recommendation outcomes for an illegal benefit, such as market penetration by pushing some specified goods onto the top-K list of users.

3.2 Attacks on Classification Models

Attacks on classification tasks are aimed at enforcing incorrect predictions of specific data instances. The popular attacks in RS, on the other hand, rely on collaborative filtering principles to compute suggestions using the similarities in the opinions of like-minded individuals. This dependency between users and things might improve predictions, but on the other hand, since predictions are based on a group of examples rather than a single one, it can generate cascading effects, where an attack on one user can affect other users [53, 54].

3.3 Granularity Attack

In image classification-based recommender systems, the adversarial samples are empowered based on a continuous real-valued representation of image data, but in recommender systems, the raw values are user/item identification numbers and discrete ratings. This difference in the granularity considered in the machine learning tasks may cause attack/defense techniques in training the machine learning models. Where, for example, the Generative Adversarial Networks, may change the semantics of the input, for example, applying ID + can result in a new user ID. As a result, existing adversarial attacks in the field of machine learning are not easily convertible to recommender system challenges. Hence these possible adversarial attacks should also be considered in the light of recommender systems to identify the appropriate possible attacks in the machine learning techniques chosen and proper measures should be taken to secure the recommender from such adversarial attacks.

4. DISCUSSION AND CONCLUSION:

The collaborative filtering and content-based filtering methods are the common algorithms used to tackle the cold start problem in the historic studies. The collaborative filtering method aims to find users who have similar likes and predicts which things should be recommended based on similar user referrals. This method of recommendation is effective for recommending items in generic domains such as music, movies, E-Commerce, and travel sites, because obtaining user preference data and identifying users with similar tastes is relatively simple, and data can be retrieved from a variety of sources such as social networks, blogs, and the user's search histories, among others. However, collaborative filtering methods cannot be used to recommend technical services such as the new type of cloud services, since user requirements for each project may differ, and it would be difficult to discover users with comparable interests or requirements during the cold start phase. This drawback has led the researchers to come up with a plethora of ideas to tackle the cold start problem and this work covers the new trends in tackling the cold start problem. Also, the possible adversarial attacks related to recommender systems discussed in this work should also be considered to identify the appropriate possible attacks in the machine learning techniques chosen and proper measures should be taken to secure the recommender from such adversarial attacks.

5. REFERENCES

[1] Wahab OA, Rjoub G, Bentahar J, Cohen R. Federated against the cold: A trust-based federated learning approach to counter the cold start problem in recommendation systems. Information Sciences. 2022 Jul 1;601:189-206.

[2] Annette J, Ruby, Aisha Banu W, Subash Chandran "Classification and Comparison of Cloud Renderfarm Services for Recommender Systems". Lecture Notes on Data Engineering and Communications Technologies, Springer, 2019.

[3] Ruby Annette et al. “A Cloud Service Providers Ranking System Using Ontology” International Journal of Scientific & Engineering Research 6 (4), 41-45, 2015.

[4] Wang H. DotMat: Solving Cold-start Problem and Alleviating Sparsity Problem for Recommender Systems. arXiv preprint arXiv:2206.00151. 2022 May 31.

[5] Zhao X, Ren Y, Du Y, Zhang S, Wang N. Improving Item Cold-start Recommendation via Model-agnostic Conditional Variational Autoencoder. arXiv preprint arXiv:2205.13795. 2022 May 27.

[6] Xu Y, Yang Y, Wang E. Generating Self-Serendipity Preference in Recommender Systems for Addressing Cold Start Problems. arXiv preprint arXiv:2204.12651. 2022 Apr 27.

[7] Shah AA, Venkateshwara H. Sparsity Regularization For Cold-Start Recommendation. arXiv preprint arXiv:2201.10711. 2022 Jan 26.

[9] Wang H. ZeroMat: Solving Cold-start Problem of Recommender System with No Input Data. In2021 IEEE

4th International Conference on Information Systems and Computer Aided Education (ICISCAE) 2021 Sep 24 (pp. 102-105). IEEE.

[10] Feng X, Chen C, Li D, Zhao M, Hao J, Wang J. CMML: Contextual Modulation Meta Learning for Cold-Start Recommendation. In Proceedings of the 30th ACM International Conference on Information & Knowledge Management 2021 Oct 26 (pp. 484-493).

[11] Wang Z, Xiao W, Li Y, Chen Z, Jiang Z. LHRM: A LBS Based Heterogeneous Relations Model for User Cold Start Recommendation in Online Travel Platform. In International Conference on Neural Information Processing 2020 Nov 18 (pp. 479-490). Springer, Cham.

[12] Wei Y, Wang X, Li Q, Nie L, Li Y, Li X, Chua TS. Contrastive learning for cold-start recommendation. In Proceedings of the 29th ACM International Conference on Multimedia 2021 Oct 17 (pp. 5382-5390).

[13] Briand L, Salha-Galvan G, Bendada W, Morlon M, Tran VA. A Semi-Personalized System for User Cold Start Recommendation on Music Streaming Apps. In Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining 2021 Aug 14 (pp. 2601-2609).

[14] Zhang Y, Maekawa T, Hara T. Using Social Media Background to Improve Cold-start Recommendation Deep Models. In2021 International Joint Conference on Neural Networks (IJCNN) 2021 Jul 18 (pp. 1-8). IEEE.

[15] Lai PL, Chen CY, Lo LW, Chen CC. ColdGAN: Resolving Cold Start User Recommendation by using Generative Adversarial Networks. arXiv preprint arXiv:2011.12566. 2020 Nov 25.

[16] Ruby Annette J, Aisha B W, Subash CP. A Multi Criteria Recommendation Engine Model for Cloud Renderfarm Services. International Journal of Electrical and Computer Engineering. 2018 Oct 1;8(5):3214.

[17] Annette J, Ruby, Aisha Banu W. “Ranking and Selection of Cloud Renderfarm Services”, Sadhana, 44:7, 2019.

[18] Zhou Y, Nadaf A. Embedded collaborative filtering for" cold start" prediction. arXiv preprint arXiv:1704.02552. 2017 Apr 9.

[19] Bernardi, Lucas Kamps, Jaap Kiseleva, Julia Mueller and Melanie, "The continuous cold start problem in e-commerce recommender systems”, CEUR Workshop Proceedings, Vol. 29, pp. 41-47, 2015.

[20] Ruby, Annette J., Banu W. Aisha, and Chandran P. Subash. "RenderSelect: a cloud broker framework for cloud renderfarm services." arXiv preprint arXiv:1611.10210 (2016).

[21] Ruby Annette J, and Aisha Banu. "A service broker model for cloud based render farm selection." arXiv preprint arXiv:1505.06542 (2015).

[22] Liu, Jin-Hu, Tao Zhou, Zi-Ke Zhang, Zimo Yang, Chuang Liu, and Wei-Min Li, "Promoting cold-start items in recommender systems”, PloS one, Vol. 9, 2014.

[23] Trevisiol, Michele, "Cold-start news recommendation with domain-dependent browse graph." Proceedings of the 8th ACM Conference on Recommender systems, ACM, 2014.

[24] Amatriain, Xavier. "Mining large streams of user data for personalized recommendations." ACM SIGKDD Explorations Newsletter , Vol 14, pp.37-48, 2013.

[25] Saveski, Martin, and Amin Mantrach, "Item cold-start recommendations: learning local collective embeddings." Proceedings of the 8th ACM Conference on Recommender systems, ACM, 2014.

[26] Yang, Xiwang, Yang Guo, and Yong Liu, "Bayesian-inference-based recommendation in online social networks." IEEE Transactions on Parallel and Distributed Systems, Vol 24, pp. 642-651, 2013.

[27] Chen, Chien Chin, Yu-Hao Wan, Meng-Chieh Chung, and Yu-Chun Sun, "An effective recommendation method for cold start new users using trust and distrust networks”, Information Sciences, Vol. 224, pp. 19-36, 2013.

[28] Krauss, Christopher, Lars George, and Stefan Arbanowski, "TV predictor: personalized program recommendations to be displayed on SmartTVs." Proceedings of the 2nd international workshop on big data, streams and heterogeneous source mining: Algorithms, systems, programming models and applications, ACM, 2013.

[29] Verbert, Katrien, Denis Parra, Peter Brusilovsky, and Erik Duval. "Visualizing recommendations to support exploration, transparency and controllability." In Proceedings of the 2013 international conference on Intelligent user interfaces, ACM, pp. 351-362, 2013.

[30] Gupta, Pankaj, Ashish Goel, Jimmy Lin, Aneesh Sharma, Dong Wang, and Reza Zadeh. "Wtf: The who to follow service at twitter." In Proceedings of the 22nd international conference on World Wide Web, ACM, pp. 505-514, 2013.

[31] Bobadilla, Jesus, Fernando Ortega, Antonio Hernando, and Jesus Bernal. "A collaborative filtering approach to mitigate the new user cold start problem", Knowledge-Based Systems, Vol. 26, pp. 225-238, 2012.

[32] Kim, Heung-Nam, Abdulmotaleb El-Saddik, and Geun-Sik Jo, "Collaborative error-reflected models for cold-start recommender systems”, Decision Support Systems, Vol. 51,pp. 519-531, 2011.

[33] Park, Seung-Taek, and Wei Chu, "Pairwise preference regression for cold-start recommendation”, Proceedings of the third ACM conference on Recommender systems, ACM, pp. 21-28, 2009.

[34] S. Loh, F. Lorenzi, R. Granada, D. Lichtnow, LK. Wives and J.P. Oliveira, “Identifying similar users by their scientific publications to reduce cold start in recommender systems”, Proceedings of the 5th International Conference on Web Information Systems and Technologies (WEBIST2009),pp. 593-600, 2009.

[35] L. Martínez, L.G. Pérez and M.J. Barranco, “Incomplete preference relations to smooth out the cold-start in collaborative recommender systems”, Proceedings of the 28th North American Fuzzy Information Processing Society Annual Conference (NAFIPS2009), pp. 1-6, 2009.

[36] LT. Weng, Y. Xu, Y. Li and R. Nayak, "Exploiting item taxonomy for solving cold-start problem in recommendation making", Proceedings of the 20th IEEE International Conference on Tools with Artificial Intelligence (ICTAI2008), USA, pp. 113-120, 2008.

[37] Annette, J. Ruby, W. Aisha Banu, and P. Subash Chandran. "Rendering-as-a-Service: Taxonomy and Comparison". Procedia Computer Science 50 (2015): 276-281, Elsevier.

[38] Ruby Annette J, Aisha Banu W, and Shriram. "A Taxonomy and Survey of Scheduling Algorithms in Cloud: Based on task dependency." International Journal of Computer Applications, 82.15 (2013): 20-26.

[39] C.W. Leung, S.C. Chan and F.L Chung, "An empirical study of a cross-level association rule mining approach to cold-start recommendations", Knowledge Based Systems, Vol. 21, pp. 515-529, 2008.

[40] S.T. Park, D.M. Pennock, O. Madani, N. Good and D. Coste, "Naive filterbots for robust cold-start recommendations", Proceedings of Knowledge Discovery and Data Mining (KDD2006), pp. 699-705, 2006.

[41] P.B. Ryan, D. Bridge, "Collaborative recommending using formal concept analysis", Knowledge Based Systems, Vol. 19, pp. 309-315, 2006.

[42] Schein, Andrew I., Alexandrin Popescul, Lyle H. Ungar, and David M. Pennock. "Methods and metrics for cold-start recommendations", Proceedings of the 25th annual international ACM SIGIR conference on Research and development in information retrieval, ACM, pp. 253-260, 2002.

[43] Ruby Annette J., Banu W. Aisha, and Chandran P. Subash. "Comparison of multi criteria decision making algorithms for ranking cloud renderfarm services." arXiv preprint arXiv:1611.10204 (2016).

[44] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian J. Goodfellow, and Rob Fergus. 2014. Intriguing properties of neural networks. In ICLR

[45] Yevgeniy Vorobeychik and Murat Kantarcioglu. 2018. Adversarial Machine Learning. Morgan & Claypool Publishers.

[46] Han Xiao, Huang Xiao, and Claudia Eckert. 2012. Adversarial Label Flips Attack on Support Vector Machines. In ECAI (Frontiers in Artificial Intelligence and Applications).

[47] Battista Biggio, Konrad Rieck, Davide Ariu, Christian Wressnegger, Igino Corona, Giorgio Giacinto, and Fabio Roli. 2018. Poisoning Behavioral Malware Clustering. arXiv (2018).

[48] Battista Biggio, Blaine Nelson, and Pavel Laskov. 2012. Poisoning Attacks against Support Vector Machines. In ICML. icml.cc / Omnipress.

[49] Zach Jorgensen, Yan Zhou, and W. Meador Inge. 2008. A Multiple Instance Learning Strategy for Combating Good Word Attacks on Spam Filters. J. Mach. Learn. Res. 9 (2008), 1115–1146

[50] Deldjoo Y, Noia TD, Merra FA. A survey on adversarial recommender systems: from attack/defense strategies to generative adversarial networks. ACM Computing Surveys (CSUR). 2021 Mar 5;54(2):1-38.

[51] Annette R, Banu A. Sriram,"Cloud Broker for Reputation-Enhanced and QoS based IaaS Service Selection". InProc. of Int. Conf. on Advances in Communication, Network, and Computing, CNC, Elsevier 2014 (pp. 815-824).

[52] Ruby Annette J., Banu W. Aisha, and Chandran P. Subash. "Comparison of multi criteria decision making algorithms for ranking cloud renderfarm services." arXiv preprint arXiv:1611.10204 (2016).

[53] Yashar Deldjoo, Tommaso Di Noia, and Felice Antonio Merra. 2020. How Dataset Characteristics Affect the Robustness of Collaborative Recommendation Models. In Proc. of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval.

[54] Konstantina Christakopoulou and Arindam Banerjee. 2019. Adversarial attacks on an oblivious recommender. In Proc. of the 13th ACM Conference on Recommender Systems, RecSys 2019, Copenhagen, Denmark, September 16-20, 2019. 322–330.