Exploring Unlearning Methods to Ensure the Privacy, Security, and Usability of Recommender Systems

Jens Leysen
University of Antwerp
Antwerp, Belgium
jens.leysen@uantwerpen.be

ABSTRACT

Machine learning algorithms have proven highly effective in analyzing large amounts of data and identifying complex patterns and relationships. One application of machine learning that has received significant attention in recent years is recommender systems, which are algorithms that analyze user behavior and other data to suggest items or content that a user may be interested in. However useful, these systems may unintentionally retain sensitive, outdated, or faulty information. Posing a risk to user privacy, system security, and limiting a system's usability. In this research proposal, we aim to address these challenges by investigating methods for machine "unlearning", which would allow information to be efficiently "forgotten" or "unlearned" from machine learning models. The main objective of this proposal is to develop the foundation for future machine unlearning methods. We first evaluate current unlearning methods and explore novel adversarial attacks on these methods' verifiability, efficiency, and accuracy to gain new insights and further develop the theory of machine unlearning. Using our gathered insights, we seek to create novel unlearning methods that are verifiable, efficient, and limit unnecessary accuracy degradation. Through this research, we seek to make significant contributions to the theoretical foundations of machine unlearning while also developing unlearning methods that can be applied to real-world problems.

CCS CONCEPTS

• **Information systems** → **Recommender systems**.

KEYWORDS

Recommender Systems, Machine Unlearning, Research Proposal

ACM Reference Format:
Jens Leysen. 2023. Exploring Unlearning Methods to Ensure the Privacy, Security, and Usability of Recommender Systems. In *Seventeenth ACM Conference on Recommender Systems (RecSys '23), September 18–22, 2023, Singapore, Singapore.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3604915.3608862

RecSys '23, September 18–22, 2023, Singapore, Singapore

ACM ISBN 979-8-4007-0241-9/23/09.
https://doi.org/10.1145/3604915.3608862

1 INTRODUCTION

Machine learning algorithms have been shown to be highly effective at analyzing large amounts of data and identifying complex patterns and relationships. One application of machine learning that has received significant attention in recent years is recommender systems, which are algorithms that analyze user behavior and other data to suggest items or content that a user may be interested in. Recommender systems are now used in various online industries, including e-commerce, social media, and entertainment [14]. For example, 80% of movies watched on Netflix come from recommendations [7], and 60% of video clicks on YouTube come from home page recommendations [5]. Recommender systems are also increasingly finding applications in new contexts, such as healthcare, where doctors can use them to suggest personalized treatments based on patient data [23].

Recommender systems have become an indispensable part of our daily lives. However, these systems can unintentionally retain sensitive, outdated, or faulty information, posing a risk to user privacy, system security, and possibly limiting a system's usability. In many cases, it can be difficult or even impossible to remove certain information from these algorithms once they have learned from their training data [3, 11]. This creates a significant challenge for the development of more responsible recommender systems. Therefore, the development of techniques and methods for machine "unlearning", that would allow information to be "forgotten" or "unlearned" from machine learning models, is an important research area [2].

In this proposal, we undertake fundamental research into machine unlearning for recommender systems, with the aim of deepening our understanding of this important area of study and identifying new approaches for removing information from recommendation models. Our research objectives are as follows:

1. To develop a comprehensive framework for evaluating machine unlearning methods for recommender systems, focusing on the verifiability, efficiency, and accuracy of these methods.
2. To explore adversarial attacks on machine unlearning methods for recommender systems, in order to better understand these methods and develop more robust approaches.
3. To develop new machine unlearning methods for recommender systems, ranging from traditional collaborative filtering models to deep learning.

Through our research, we aim to make significant contributions to the theoretical foundations of machine unlearning, while also developing practical techniques and methods that can be applied to real-world problems. By doing so, we hope to enable the development of more secure, trustworthy, and responsible recommender systems.

2 BACKGROUND

2.1 Introducing: Machine Unlearning

We first discuss the problem formulation of machine unlearning according to Mercuri et al. [19]. Formally, the goal of an unlearning algorithm is to remove the influence of a subset $D_u \subseteq D \in Z^*$ of m samples from the trained model $h \in H$. Whereby H is the space of all hypothesis functions, and Z^* is the space of datasets. To do so, we need to develop a removal mechanism, which is a map $U : H \times Z^* \times Z^* \longrightarrow H$. Which takes as input a model h, the original dataset D and data to be removed D_u, and outputs a new model $U(h, D, D_u) \in H$. For every algorithm, there exists a simple, trivial removal mechanism: retrain the model on the dataset that doesn't include D_u. The main problem with this naïve removal mechanism is its efficiency. In many situations, it would simply take too long or require too many computational resources to retrain a model in its entirety. Because of this inefficiency, there's an active research effort to develop more efficient, often *approximate*, unlearning methods. These methods attempt to efficiently approximate what the parameters of the model would have looked like if the data points to be unlearned (D_u) hadn't been part of the original training dataset.

2.2 Rationale for Machine Unlearning

In the following paragraphs, we discuss three justifications for the development of unlearning methods for recommender systems.

Privacy. From a privacy standpoint, legislation such as the European Union's GDPR acknowledges an individual's right to be forgotten and requires businesses to delete personal data without undue delay [16]. This legislation is vital because users might want their sensitive data to be forgotten to prevent persecution or be perpetually stigmatized [16]. Alas, machine learning models are susceptible to model inversion and membership inference attacks, which can leak private information from the model's training data [12]. Because of these privacy concerns, model owners should be able to quickly remove private, learned information at the request of the user. Training machine learning models is expensive and time-consuming, which makes it prohibitive to continuously retrain models each time a user invokes their right to be forgotten [8]. Hence the need for efficient unlearning methods.

Usability. Users of recommender systems may also want some of their data to be unlearned from the system for usability reasons. For instance, users might need to remove incorrect data or explicitly indicate a shift in their preferences. Since recommender systems learn from user behavior, incorrect or noisy training data may lead to poor recommendations. In addition, another important reason is to mitigate the impact of concept drift. Concept drift refers to the phenomenon that the underlying patterns in the data may change over time, which can cause the model to become less accurate or even completely obsolete [18]. This is especially relevant for recommender systems, as user preferences may change over time, item perception may change, or external events may influence the system's performance. By unlearning outdated information and incorporating new data, the recommender system can efficiently adapt to changing conditions and maintain its usability over time [18].

Security. From a security perspective, machine learning models are vulnerable to external attacks that seek to force them to output wrong predictions [2]. In the context of recommender systems, data poisoning attacks have been discussed most frequently [9]. In such an attack, attackers inject fake users (bots) to influence the behavior of a recommender system. This way, the system will make recommendations that the attacker desires. For example, an attacker-chosen item is recommended to the other (non-malicious) users. Once such an attack has been identified, there is a need for a mechanism to efficiently delete the influence of the adversary on the model.

In conclusion, having efficient unlearning methods to remove private, faulty, outdated, or adversarial information from a model is in the best interest of both users and online platforms that employ recommender systems.

3 RELATED WORK

3.1 Unlearning for Recommender Systems

Various unlearning approaches have been developed for specific recommendation algorithms (model-intrinsic) or as model-agnostic methods. For instance, RecEraser and LASER are model-agnostic unlearning methods developed by Chen et al. and Li et al [3, 11]. Schelter has developed a model-intrinsic unlearning method for item-based collaborative filtering [21]. Wang and Schelter have also proposed unlearning methods for next basket recommendations [24]. Liu et al. proposed an influence-based unlearning method for neural matrix factorization, while Yuan et al. have developed unlearning methods for federated recommendations [13], [25]. Additionally, Matuszyk et al. have developed forgetting methods for matrix factorization [18].

Despite the growing interest in developing unlearning methods for recommender systems in recent years, several classes of recommender systems still require the development of unlearning methods. The reason for this research gap is that unlearning methods have mainly been studied in the context of classification applications, while other unlearning applications, such as recommender systems, have not been extensively investigated [20].

3.2 Approximate Unlearning Methods

Influence functions are the dominant research direction for approximate machine unlearning as they solve the central problem of quantifying the effect of individual data points on the model parameters [20]. However, the existing influence-based methods suffer from several issues. First, they have been shown to be fragile for deep neural networks [1]. Second, they are computationally intensive since they require the calculation of the inverse-Hessian [1]. Third, as influence functions use second-order Taylor expansions, they are only accurate for estimating small perturbations to the model.

A recent study by Thudi et al. has also raised concerns about the validity of these approximate unlearning methods [22]. They show that it's possible for two different samples from the training data to have the same effect on the model parameters. In addition, they also show that two non-overlapping datasets can lead to similar model parameters. They call this phenomenon dataset "forgeability". Essentially, their results show we can find subsets in our training data that would have led to a similar final model. These insights have fundamental implications for approximate unlearning methods. Thudi et al. argue we cannot prove unlearning simply by comparing points in the model's parameter space. Rather, we need novel unlearning methods that reason on the level of the learning trajectory [22].

3.3 Evaluation of Unlearning Methods

Previously, studies have resorted to different forms of evaluation, resulting in limited comparability between studies. Most studies on machine unlearning have also neglected at least one of our proposed evaluation dimensions: verifiability, efficiency, and accuracy. This introduces uncertainty about the practicality of the proposed unlearning methods. This is problematic as in a real-world context, unlearning methods will not only be chosen based on their privacy-preserving abilities. We first discuss metrics related to verifiability.

Verifiability. These metrics are used to verify that for any dataset D and subset D_u , the model $U(A(D), D, D_u)$ contains a sufficiently small amount of information about D_u. Chen et al. have discussed membership inference attacks as a measurement of privacy degradation [4]. Similarly, Graves et al. have discussed both membership inference and model inversion attacks to verify unlearning [8]. Both attacks evaluate unlearning through a malicious adversary that mounts an attack and attempts to learn private information that was meant to be removed. They differ in that the former seeks to determine the presence of a sample in a model's training data, whereas the latter seeks to extract all training information from a trained model. In essence, these are both privacy attacks. Jagielski et al. have formalized this concept of privacy attacks into a measure named α-forgetting [10]. In summary, a model has achieved α-forgetting on a sample, if a privacy attack cannot achieve a higher success rate than α. This kind of measure captures the intuition that a model has unlearned a training point if an attack cannot reliably detect whether that point was ever used during training. Some authors have also presented a proof of exactness or bounds on the information that is retained in the model after unlearning [6]. With the derivation of these bounds being rooted in the theory of differential privacy.

Efficiency. The time efficiency of an unlearning method is usually measured as the time to unlearn using naïve retraining over the time to unlearn using the proposed unlearning method, averaged over several deletion requests [19]. The existing literature currently lacks studies that focus on the analysis of computational overhead for these unlearning methods. Clearly, some unlearning methods need to store additional data and wouldn't scale well with growing dataset size or increasing model complexity. As an example, the DeltaGrad method for unlearning in linear models stores the original SGD steps [15]. Some competing methods don't require storing the original training steps and would therefore be more space efficient.

Accuracy. Machine unlearning methods should also be evaluated according to their accuracy, to ensure that the model hasn't forgotten more than it should, leading to unnecessary accuracy degradation. As such, we should compare the test set performance of the unlearned model against that of the naïve and original model. Recommender systems interact with billions of people each day and consequently learn from enormous amounts of data. Because of this reason, unlearning methods need to be efficient, be able to deal with enormous deletion volumes, and not result in severe accuracy degradation after a few unlearning requests.

Value of Adversarial Attacks. A recent paper by Marchant et al. has explored attacks that maximize the computational cost to remove a sample of data from a model [17]. Their results show that unlearning methods should be developed with other characteristics in mind, such as time and computational efficiency. Thudi et al. developed another kind of attack named a "forgeability" attack [22]. In essence, they showed that in some circumstances, a model owner can plausibly deny having learned or unlearned on a data sample. In such a case, the current formulation of machine unlearning is ill-defined. These two examples illustrate the value of adversarial attacks in evaluating recommender systems and their unlearning methods, these attacks can help us discover new insights and potential shortcomings.

4 RESEARCH OBJECTIVES

The main objective of this proposal is to study and develop the foundation for future machine unlearning methods. To gain new insights and develop the theory on unlearning, we first evaluate current unlearning methods and explore adversarial attacks on these methods' verifiability, efficiency, and accuracy. Using our gathered insights, we seek to develop novel unlearning methods that are verifiable, efficient and don't lead to unnecessary accuracy degradation.

4.1 Evaluate Current Unlearning Methods for Recommender Systems

Previously, researchers have mostly evaluated unlearning methods according to their privacy-preserving capabilities. In general, there is a lack of discussion about applying machine unlearning in practice. We believe there exist trade-offs between verifiability, efficiency, and accuracy. Each of these dimensions is important to apply unlearning methods to real-world problems of security, privacy, and usability. The goal of this first objective is thus to compare current unlearning methods according to verifiability, accuracy, and efficiency metrics. As well as highlight any trade-offs between these evaluation dimensions in order to contribute to the theory on machine unlearning.

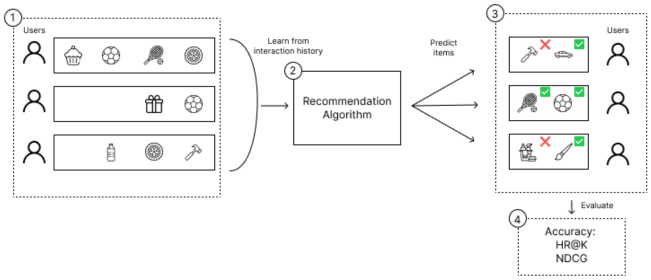

Figure 1: Offline evaluation of recommender systems. User history and item information (1) are used by the recommender system (2) to predict candidate items for different users (3). In offline evaluation (4), algorithms are evaluated by leaving items out of the history and evaluating the accuracy based on whether the correct items appear in the top-K predicted items.

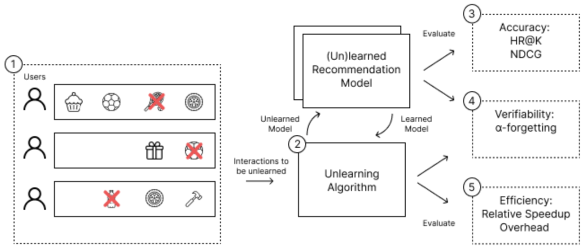

Figure 2: Offline evaluation of unlearning methods. In the case of interaction removal, an unlearning request is issued which specifies the data that needs to be unlearned: D_u (1). The unlearning algorithm (2) receives D_u and the learned model. It returns an unlearned model to be used for inference. The accuracy of the unlearned model is tested, as well as the verifiability and efficiency of the unlearning method (3)(4)(5).

4.2 Explore Adversarial Attacks on the Verifiability, Efficiency, and Accuracy of Unlearning Methods

In addition to evaluation metrics, we will explore a variety of attacks on machine unlearning methods. Previous studies have mainly discussed attacks that target the verifiability of unlearning methods. We believe that adversarial attacks on machine unlearning can help us gain a better understanding of unlearning algorithms and can help us better protect recommender systems. Therefore, our goal is to investigate new attack scenarios on the efficiency, and accuracy of unlearning methods.

4.3 Develop State-of-the-art Unlearning Methods for Recommender Systems

As we have discussed, approximate unlearning methods face significant challenges that we must address. Influence functions have been the dominant research direction for machine unlearning, but there is still significant room for improvement. Our goal is to research new unlearning algorithms that are efficient, have good privacy guarantees, and ensure the model doesn't experience severe accuracy degradation.

5 RESEARCH METHODOLOGY

Traditionally, recommender systems have been evaluated and compared through an offline evaluation design. The use of standardized benchmark datasets allows us to compare various algorithms across a variety of scenarios. Figure 1 shows a simplified illustration of the offline evaluation of a recommender system's accuracy. To test the accuracy, metrics for top-N ranking are often used, such as NDCG, Precision, or Recall.

To achieve our research objectives, we will develop an offline experimentation framework for unlearning methods. It will incorporate unlearning algorithms, adversarial attacks and metrics that measure the efficiency, accuracy and privacy of (un)learning methods. Figure 2 roughly illustrates our proposed experimentation framework.

Our first objective is to evaluate current unlearning methods. We will do this by simulating different kinds of deletion scenarios. In other words, we will investigate different sampling distributions to select which interactions need to be unlearned. We will implement several unlearning methods for recommender systems to compare to our unlearning methods and further improve upon. For example, considering a deep learning recommendation algorithm, we would implement the influence-based method proposed by Golatkar et al [6], as well as other applicable unlearning methods.

This unlearning method is then evaluated according to efficiency, verifiability, and accuracy. Time efficiency will be measured as the time to unlearn these sampled interactions using naïve retraining over the time to unlearn these items using the proposed unlearning method. We will also analyse the computational overhead of each unlearning algorithm. Our framework will include and later expand on state-of-the-art privacy attacks. These will be used to measure α-forgetting, which tests the privacy-preserving capabilities of an unlearning algorithm. An unlearning algorithm is said to be α-verified for a specific attack if this attack cannot achieve a higher success rate than α on a sufficiently large sample. The accuracy of the (un)learned model will be tested using the evaluation method discussed in Figure 1. We will evaluate the unlearning methods under identical conditions on datasets from different domains such as the MovieLens, Netflix, and 30Music datasets. While previous research has mainly evaluated unlearning methods based on their privacy-preserving capabilities, we take a broader approach by evaluating the methods based on verifiability, efficiency, and accuracy. By highlighting the trade-offs between these dimensions, we hope to develop a more nuanced understanding of the strengths and weaknesses of different unlearning methods.

Our second objective will be to expand our experimentation framework with adversarial attacks on the efficiency and accuracy of unlearning methods. We first conduct a study on accuracy degradation. We believe that approximate unlearning methods can drastically degrade the accuracy of the recommendation model. We would like to research an adversarial attack, that can discover data points whose unlearning would lead to severe accuracy degradation.

Afterwards, we will investigate attacks that can effectively slow down or increase the computational overhead of an unlearning method. While previous research has discussed attacks that target the verifiability of unlearning methods, we plan to explore a variety of attacks on the efficiency and accuracy of these methods. By doing so, we hope to gain a better understanding of how unlearning methods can be compromised and develop more robust unlearning algorithms.

For the third objective, we will use our insights from the evaluation of current unlearning methods and our study of adversarial attacks to develop new unlearning algorithms. The goal of our proposed methodology is to support our research on unlearning methods for recommender systems by allowing for correct, reproducible experimentation on standardized datasets. We believe this methodology will allow us to easily evaluate our newly developed unlearning methods on several classes of recommender systems.

6 CONCLUSION

Modern recommender systems are faced with several challenges, we discussed three of these: privacy, security and usability. We propose to address these challenges through the development of "unlearning" or "forgetting" methods for recommender systems. These methods would allow information to be efficiently removed from a trained model, without the need to fully retrain a recommendation model from scratch. We propose to evaluate the current unlearning methods for recommender systems and explore adversarial attacks on the verifiability, efficiency and accuracy of unlearning methods. Finally, we will develop novel unlearning methods for a range of recommendation algorithms.

ACKNOWLEDGMENTS

This work was conducted under the supervision of Prof. dr. Bart Goethals. This research received funding from the Flemish Government through the “Onderzoeksprogramma Artificiële Intelligentie (AI) Vlaanderen” programme.

REFERENCES

[1] Samyadeep Basu, Phillip Pope, and Soheil Feizi. 2021. Influence Functions in Deep Learning Are Fragile. In *International Conference on Learning Representations 2021*. Virtual Event. https://openreview.net/forum?id=xHKVVHGDOEk

[2] Yinzhi Cao and Junfeng Yang. 2015. Towards Making Systems Forget with Machine Unlearning. In *2015 IEEE Symposium on Security and Privacy*. IEEE, San Jose, CA, 463–480. https://doi.org/10.1109/SP.2015.35

[3] Chong Chen, Fei Sun, Min Zhang, and Bolin Ding. 2022. Recommendation Unlearning. In *Proceedings of the ACM Web Conference 2022*. ACM, Virtual Event, Lyon France, 2768–2777. https://doi.org/10.1145/3485447.3511997

[4] Min Chen, Zhikun Zhang, Tianhao Wang, Michael Backes, Mathias Humbert, and Yang Zhang. 2021. When Machine Unlearning Jeopardizes Privacy. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. ACM, Virtual Event Republic of Korea, 896–911. https://doi.org/10.1145/3460120.3484756

[5] James Davidson, Benjamin Liebald, Junning Liu, Palash Nandy, Taylor Van Vleet, Ullas Gargi, Sujoy Gupta, Yu He, Mike Lambert, Blake Livingston, and Dasarathi Sampath. 2010. The YouTube video recommendation system. In *Proceedings of the fourth ACM conference on Recommender systems*. ACM, Barcelona Spain, 293–296. https://doi.org/10.1145/1864708.1864770

[6] Aditya Golatkar, Alessandro Achille, Avinash Ravichandran, Marzia Polito, and Stefano Soatto. 2021. Mixed-Privacy Forgetting in Deep Networks. In *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, Nashville, TN, USA, 792–801. https://doi.org/10.1109/CVPR46437.2021.00085

[7] Carlos A. Gomez-Uribe and Neil Hunt. 2016. The Netflix Recommender System: Algorithms, Business Value, and Innovation. *ACM Transactions on Management Information Systems* 6, 4 (Jan. 2016), 1–19. https://doi.org/10.1145/2843948

[8] Laura Graves, Vineel Nagisetty, and Vijay Ganesh. 2021. Amnesiac Machine Learning. *Proceedings of the AAAI Conference on Artificial Intelligence* 35, 13 (May 2021), 11516–11524. https://doi.org/10.1609/aaai.v35i13.17371

[9] Hai Huang, Jiaming Mu, Neil Zhenqiang Gong, Qi Li, Bin Liu, and Mingwei Xu. 2021. Data Poisoning Attacks to Deep Learning Based Recommender Systems. In *Proceedings 2021 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2021.24525 arXiv:2101.02644 [cs].

[10] Matthew Jagielski, Om Thakkar, Florian Tramèr, Daphne Ippolito, Katherine Lee, Nicholas Carlini, Eric Wallace, Shuang Song, Abhradeep Thakurta, Nicolas Papernot, and Chiyuan Zhang. 2023. Measuring Forgetting of Memorized Training Examples. In *International Conference on Learning Representations 2023*. Kigali, Rwanda. https://openreview.net/pdf?id=7bJizxLKrR arXiv:2207.00099 [cs].

[11] Yuyuan Li, Xiaolin Zheng, Chaochao Chen, and Junlin Liu. 2022. Making Recommender Systems Forget: Learning and Unlearning for Erasable Recommendation. http://arxiv.org/abs/2203.11491 arXiv:2203.11491 [cs].

[12] Bo Liu, Ming Ding, Sina Shaham, Wenny Rahayu, Farhad Farokhi, and Zihuai Lin. 2022. When Machine Learning Meets Privacy: A Survey and Outlook. *Comput. Surveys* 54, 2 (March 2022), 1–36. https://doi.org/10.1145/3436755

[13] Wenyan Liu, Juncheng Wan, Xiaoling Wang, Weinan Zhang, Dell Zhang, and Hang Li. 2022. Forgetting Fast in Recommender Systems. http://arxiv.org/abs/2208.06875 arXiv:2208.06875 [cs].

[14] Jie Lu, Dianshuang Wu, Mingsong Mao, Wei Wang, and Guangquan Zhang. 2015. Recommender system application developments: A survey. *Decision Support Systems* 74 (June 2015), 12–32. https://doi.org/10.1016/j.dss.2015.03.008

[15] Ananth Mahadevan and Michael Mathioudakis. 2021. Certifiable Machine Unlearning for Linear Models. http://arxiv.org/abs/2106.15093 arXiv:2106.15093 [cs].

[16] Alessandro Mantelero. 2013. The EU Proposal for a General Data Protection Regulation and the roots of the ‘right to be forgotten’. *Computer Law & Security Review* 29, 3 (June 2013), 229–235. https://doi.org/10.1016/j.clsr.2013.03.010

[17] Neil G. Marchant, Benjamin I. P. Rubinstein, and Scott Alfeld. 2022. Hard to Forget: Poisoning Attacks on Certified Machine Unlearning. *Proceedings of the AAAI Conference on Artificial Intelligence* 36, 7 (June 2022), 7691–7700. https://doi.org/10.1609/aaai.v36i7.20736

[18] Pawel Matuszyk, João Vinagre, Myra Spiliopoulou, Alípio Mário Jorge, and João Gama. 2015. Forgetting methods for incremental matrix factorization in recommender systems. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*. ACM, Salamanca Spain, 947–953. https://doi.org/10.1145/2695664.2695820

[19] Salvatore Mercuri, Raad Khraishi, Ramin Okhrati, Devesh Batra, Conor Hamill, Taha Ghasempour, and Andrew Nowlan. 2022. An Introduction to Machine Unlearning. http://arxiv.org/abs/2209.00939 arXiv:2209.00939 [cs].

[20] Thanh Tam Nguyen, Thanh Trung Huynh, Phi Le Nguyen, Alan Wee-Chung Liew, Hongzhi Yin, and Quoc Viet Hung Nguyen. 2022. A Survey of Machine Unlearning. http://arxiv.org/abs/2209.02299 arXiv:2209.02299 [cs].

[21] Sebastian Schelter. 2019. “Amnesia” – Towards Machine Learning Models That Can Forget User Data Very Fast. In *1st International Workshop on Applied AI for Database Systems and Applications*. Los Angeles CA USA, 4. https://ssc.io/pdf/amnesia.pdf

[22] Anvith Thudi, Hengrui Jia, Ilia Shumailov, and Nicolas Papernot. 2022. On the Necessity of Auditable Algorithmic Definitions for Machine Unlearning. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 4007–4022. https://www.usenix.org/system/files/sec22fall_thudi.pdf

[23] Thi Ngoc Trang Tran, Alexander Felfernig, Christoph Trattner, and Andreas Holzinger. 2021. Recommender systems in the healthcare domain: state-of-the-art and research issues. *Journal of Intelligent Information Systems* 57, 1 (Aug. 2021), 171–201. https://doi.org/10.1007/s10844-020-00633-6

[24] Benjamin Longxiang Wang and Sebastian Schelter. 2022. Efficiently Maintaining Next Basket Recommendations under Additions and Deletions of Baskets and Items. http://arxiv.org/abs/2201.13313 arXiv:2201.13313 [cs].

[25] Wei Yuan, Hongzhi Yin, Fangzhao Wu, Shijie Zhang, Tieke He, and Hao Wang. 2022. Federated Unlearning for On-Device Recommendation. http://arxiv.org/abs/2210.10958 arXiv:2210.10958 [cs].