International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ADVANCING CROSS-DOMAIN RECOMMENDATION FOR SECURE RATING PREDICTION THROUGH FEDERATED LEARNING: A SYSTEMATIC REVIEW

Pratibha Patil[1], Anuradha Kanade[2*]

[1] [a]Research Scholar, Department of Computer Science and Applications, Dr. Vishwanath Karad MIT World Peace University, Pune, India
[b]Assistant Professor, School of Computer Studies, Sri Balaji University Pune (SBUP), Survey no. 55/2-7, Tathawade, Opp. Mumbai-Bangalore Bypass Pune - 411033, Maharashtra, India
[2*]Department of Computer Science and Applications, Dr. Vishwanath Karad MIT World Peace University, Pune, India

Abstract

Aim: This study evaluates the efficacy of federated cross-domain system recommendations in comparison to conventional recommendation systems for privacy-preserving rating prediction. Through the investigation of the interaction between recommendation systems and federated learning, this research can reduce the privacy issue, data security, and the barriers brought by integration of cross-domain data, and further evaluate the potential for more personalized and secure recommendation systems.

Methodology: A thorough literature review with focus on employing multi-domain recommendation systems to federated learning was conducted. Search on multiple academic platforms provided relevant data and publications on this subject matter. The selected studies and datasets were reviewed based on set inclusion and exclusion criteria to enable comparison with classical recommendation systems. Data was then compiled and used to evaluate the limitations, privacy-preservation methods, and performance of federated recommendation systems.

Results: Following an initial search of 1188 records, 71 studies were deemed eligible for publication. Relative to traditional methods, federated learning does hold great promise for enhanced security and privacy in recommendation systems. On data heterogeneity, scalability, and model performance across domains, the picture was not as bright. Among the key issues raised were data integration across domains, algorithmic bias, and the need for more robust privacy-preserving technology.

Findings: The work illustrates that federated cross-domain recommendation systems may effectively reconcile privacy protection with recommendation accuracy, particularly when using privacy-preserving techniques like differential privacy and safe multi-party computing.
Although federated systems have more robust privacy protection than conventional recommendation methods, they have more challenges in data sparsity and domain adaption.

Conclusion: This paper offers insightful analysis of how federated learning can be utilized to produce cross-domain recommendation systems with the maintenance of privacy. For the sake of ensuring the universal acceptance and effectiveness of federated recommendation systems, especially compared to traditional models, future studies must focus on enhancing privacy-maintaining methods, boosting cross-domain fusion, and expanding empirical verification into real-world use. should concentrate on improving privacy-preserving techniques, enhancing cross-domain integration, and extending empirical validation to real-world applications.

Keywords: Federated Learning, Cross-Domain Recommendation, Privacy-Preserving, Rating Prediction, Traditional Recommendation Methods, Data Security, Customized Recommendations

1 Introduction

In the age of the Internet, recommendation systems (RSs) are essential for dealing with information overload [1] [2][3]. Traditional RSs are usually built on a single domain [4–6], where users only interact with one kind of object. Furthermore, due to the dearth of user behaviour data, these single-

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

domain recommendation systems often fall short in making correct suggestions for new users, also known as cold-start users. On the other hand, the difficulty of accurately determining a user's or item's closest neighbour might result in a significant decline in recommendation quality due to the data sparsity issue [6].

These problems may be resolved by using the Cross-Domain Recommendation (CDR) [7]. CDR successfully addresses employing a source domain that is reasonably rich in information to solve difficulties handle cold starts and little data, and enhance the calibre of recommendations in the information-sparse destination domain. For instance, people only rate books on the well-known community website Douban1, but not films. The Douban recommendation algorithm might suggest films to users based on their book reviews since users tend to have similar tastes across multiple domains. The premise of the majority of current CDRs is that data is shared between domains [8]. The Combined Matrix Factorisation (CMF) [9] approach, for instance, learns item and user embeddings Simultaneously from several domains' interaction matrices. However, it is undeniable that the source and destination sites share raw data is necessary since user activity on websites is sensitive to privacy would result in a considerable risk of privacy leakage. Additionally, many users are anticipated to decline sharing data with web servers as a result of new privacy laws being implemented globally (such as the CCPA3 and GDPR2).

To minimize privacy breaches, care should be made to avoid disclosing user interaction data. There are very few CDR techniques now in use that take privacy protection into account. For instance, CCMF [10] recommends giving the target domain access to protected data. After using differential privacy to hide genuine a confidence matrix and utilize data from the source domain to enhance the efficacy of the perturbation data. In order to prevent user-related information from leaking, NATR [8] suggests that source and target domains instead of sharing user embeddings, just item embeddings. This method uses neural networks' potent representation capability to extract valuable information from item embeddings. It should be noted that although these techniques provide some degree of privacy protection for users, they are still predicated on a centralised learning methodology, and if the data is kept on the server side, it is still vulnerable to attack [11].

FedCDR is a CDR that incorporates Federated Learning (FL) [12] to allow for collaborative model training without requiring central storage of user behaviour data for high-level privacy protection. The fundamental tenet of FL, which Google advocated in recent years, is that users' own devices store data locally. The server receives only intermediate results, such weights or gradients. Compared to traditional centralised machine learning techniques, FL lowers expenses and the possibility of privacy leaks. Federated Learning (FL) is a revolutionary privacy-preserving technique that tackles common privacy and data security issues in machine learning applications. FL enables models to be trained locally on the user's device, as contrast to conventional centralised models that transport and analyse raw data centrally. Data transmission is significantly reduced since the system is trained on the data sources in a decentralised fashion, sending only model changes to a central server for aggregation. As a result, there is less chance of data breaches and leaks. By keeping sensitive data local, this paradigm not only protects data privacy but also lessens the need for data centralisation, lowering the danger of a single point of failure.

With FL, advancing RSs have a viable approach that protects user privacy. Significant privacy and security concerns are raised by RSs, which are essential in customising user-specific content yet rely heavily on user data for their functions. FL's distributed machine learning technique reduces privacy threats by keeping data local on the user's device. Having local models on each device and sharing model updates only offers two advantages: it eliminates the need to compile and process large amounts of user data centrally, which lowers the cost of data transmission and storage, and it automatically protects data privacy because private user information never leaves the local device. Using FL in RSs provides a practical way to use data's potential while protecting user privacy at a time when data privacy is becoming a more pressing issue. We can achieve a balance between privacy and personalisation by advancing RSs with FL, which is essential for winning over users and improving

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

the user experience in general.
Thus, Federated Learning provides a promising path towards improving Cross-Domain Recommendation systems, which have the potential to provide superior recommendations without compromising user's privacy. With the age of personalised information, this incorporation of FL into CDR systems ensures a secure and optimal user experience while also addressing the escalating issues on data privacy.

Objectives
[1]To create and execute a federated learning framework specifically designed for cross- domain recommendation systems.
[2]To integrate privacy-enhancing methods, such as differential privacy and secure aggregation, into the federated learning architecture.
[3]To perform tests utilising actual datasets from various domains to assess the effectiveness of the suggested federated cross-domain recommendation method.
[4]To evaluate the efficacy of the federated cross-domain recommendation strategy in relation to traditional recommendation methods and other federated learning systems.
[5]To validate the feasibility and effectiveness of federated cross-domain recommendation for privacy-preserving rating prediction through empirical validation.

2 Literature review

2.1 Cross-domain recommendation

The objective of cross-domain recommendation is to mitigate cold start problems and data sparsity in the target domain by using data obtained from the source domain. Through a combined study of the two datasets, the potential for leveraging their correlations to get a deeper understanding of the dataset's fundamental nature and provide more insightful information to increase recommendation accuracy is investigated. For instance, it is suggested that CMF [9]be used to accomplish knowledge integration across domains via the examination with two datasets with user components from separate domains and a low-rank subspace in their linked dimension. By using identical with the target domain being latent rating patterns from another domain, CBT [13] seeks to enhance recommendations in one domain. Through establishing entity correlation between the target and source domains via active transfer learning, MMMF [14] outperforms CBT. Due of the unfamiliar user environment, CDTF [15] uses tensor factorisation to represent the triadic connection of the user-item-domain.
Few research on privacy protection in the context of CDRs have been carried out in recent years. In order to satisfy the differential privacy condition, CCMF [10] adds noise to raw data as part of an obfuscation technique. Then, in the target domain, confidence-aware collective matrix factorisation is carried out to take advantage of the transmitted obfuscated interaction matrix. 27] proposed FedCDR is a recommendation system that spans domains using federated learning that preserves user-specific parameters and raw data on users' devices while training the recommendation model. Both a transfer module as well as a private module respond to the wildly different data on participating devices compared to traditional CDR models. For every user, the personal module retrieves private user data, whereas the transfer module transfers information across domains. We create a personalised update method for each client and a personalised server aggregation technique to give personalised suggestions with minimal storage and communication expenses while respecting privacy. To test FedCDR, we do extensive trials on sample three well-known rate prediction projects use datasets from Amazon 5-cores. FedCDR outperforms cutting-edge methods in MAE and RMSE. FedCDR improves MAE and RMSE by 65.83% and 55.45%, respectively, for new movie consumers in job Movie & Music. By randomly selecting unrated objects, giving virtual ratings, and batch and randomly federating several decomposition-based recommendation models, [28] presented the FedCDR a way to score predictions in the context of generalised federated recommendation systems that gives clear feedback. This method can make it harder for the server to figure out the user's identity in order to

Received: August 14, 2025

Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

protect user privacy preferences for some products. However, it also To prevent user data from leaking, NATR [8] recommends communicating item-side information and moving the item embedding across domains. Nevertheless, the previously stated CDR techniques depend on user behaviour data that is centrally maintained and completely transferable between domains. They need gathering data on user behavior and storing it centrally on the servers of the service providers, where it is very vulnerable to intrusions [26]. adds more noise to the interaction, raising access and computing costs. [29] provided the primary privacy-preserving methods of FRSs, which are encryption, perturbation, and masking, after a search in the relevant literature for survey studies on federated recommender systems. The paper tries to address every present and upcoming issue in FRSs and just briefly discusses privacy. The most recent study by [30] similarly examines the numerous FedRS communication architectures, listing the primary methods for protecting privacy, such as homomorphic encryption, differential privacy, etc., as well as the primary attack types, without placing much attention on the fundamentals of Federated Learning. The article offers a list of generic datasets that are often used for recommender system training and evaluation, as well as an analysis of the communication cost component. In addition to listing the different architectural options, Yang et al.'s previous review [30] offers a more thorough discussion and formal definition of Federated Learning in Recommender Systems. Additionally, the study outlines research paths and future difficulties, but it makes no mention of task-specific datasets or applications. Finally, a more comprehensive description of the FedRS procedures and the potential architectural choices is given by the work of [31], which omits many specifics. In addition to discussing the primary issues that are also thought of as potential areas for future study, they highlight privacy-preserving strategies and provide a list of applications and general-purpose datasets. **Privacy-preserving work in recommendation**

Related to protecting users' privacy, a number of studies have been done in the area of recommendation [20]. [21] proposed a collaborative filtering approach based on a probabilistic factor analysis model with privacy protection provided by peer-to-peer protocols [23] presents a systematic study that exploits the trade-off between users' interest- functionality interactions and privacy preferences to make personalized privacy-preserving App recommendations. [24] proposed a privacy-preserving recommendation method that applies differential privacy to matrix factorization. DMF[25] is a distributed MF framework based on a distributed training technique of a random wandering algorithm to train MF models on each user's end for POI recommendation. The aforementioned studies are based on a single- domain recommendation. In recent years, a limited number of studies are conducted on privacy protection in the area of CDRs. CCMF [10] applies an obfuscation mechanism to raw data by adding noise to meet the criterion of differential privacy, and then performs confidence-aware collective matrix factorization in the target domain to exploit the transferred obfuscated interaction matrix. NATR [8] proposes sharing information on the item side and transferring the item embedding between domains, which avoids the leakage of user-related data. However, the aforementioned CDR methods rely on centrally stored user-behavior data, which can be fully shared across domains. They require collecting user behavior data and then centrally storing them in the service providers' central servers, and the data are at significant risk of being attacked [26].

2.2 Federated Learning for Cross-Domain Recommendation for Rating Prediction [27] proposed FedCDR, a federated learning-based cross-domain recommendation system that trains the recommendation model while maintaining users' raw data and confidential user- specific parameters on their devices. A personal module and a transfer module respond to the exceedingly varied data on participating devices, unlike conventional CDR models. The personal module pulls private user characteristics for each user, whereas the transfer module transfers information across domains. We create a personalised update method for each client and a personalised server aggregation technique to give personalised suggestions with minimal storage and communication expenses while respecting privacy. To test FedCDR, we do extensive trials on sample Amazon 5-cores datasets for three

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

prominent rating prediction tasks. FedCDR beats state-of-the-art approaches in MAE and RMSE. FedCDR improves MAE and RMSE by 65.83% and 55.45%, respectively, for new movie consumers in job Movie & Music. [29]provided the primary privacy-preserving methods of FRSs, which are encryption, perturbation, and masking, after a search in the relevant literature for survey studies on federated recommender systems. The paper tries to address every present and upcoming issue in FRSs and just briefly discusses privacy. The most recent study by [30]similarly examines the numerous FedRS communication architectures, listing the primary methods for protecting privacy, such as homomorphic encryption, differential privacy, etc., as well as the primary attack types, without placing much attention on the fundamentals of Federated Learning. The article offers a list of generic datasets that are often used for recommender system training and evaluation, as well as an analysis of the communication cost component. In addition to listing the different architectural options, Yang et al.'s previous review [30]offers a more thorough discussion and formal definition of Federated Learning in Recommender Systems. Additionally, the study outlines research paths and future difficulties, but it makes no mention of task-specific datasets or applications. Finally, a more comprehensive description of the FedRS procedures and the potential architectural choices is given by the work of [31], which omits many specifics. In addition to discussing the primary issues that are also thought of as potential areas for future study, they highlight privacy-preserving strategies and provide a list of applications and general-purpose datasets.

3 METHODOLOGY

3.1 Protocol for Systematic Literature Review (SLR)

This study offers a methodical review of the literature (SLR) was conducted between 2014 and 2024 on the topic of Federated Cross-Domain Recommendation for Privacy-Preserving Rating Prediction. The SLR method used in this study corresponds with the recommendations made in [32] , offering an elaborate plan for understanding the relevant material. In contrast to other review publications, this study analyzes the benefits, data preparation methods, and various recommendation strategies applied across diverse datasets. A systematically organized collection of research articles, resulting from a structured literature review (SLR), provides a classification of the federated learning methodologies utilized for cross-domain recommendation. By identifying research gaps and limitations present in the literature, this work opens up novel and valuable opportunities for future research. Overall, this study offers a thorough and original approach to conducting an in-depth analysis of federated cross-domain recommendation methods for privacy-preserving rating prediction. Figure 1 presents an overview of the research methodology, which is detailed further below.

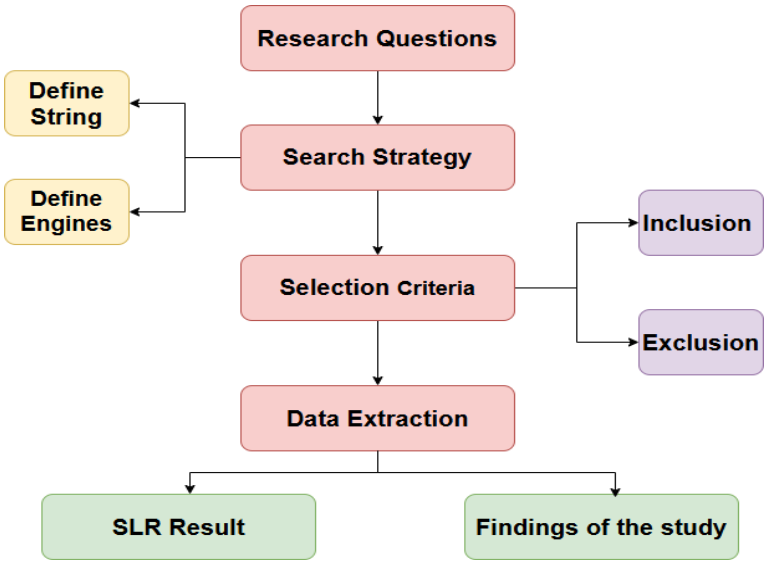


Figure 1 SLR protocol overview

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.1 Research techniques

This section describes a systematic analytical technique to assess cross-domain recommendation systems (CDRS) in federated learning (FL) and privacy-preserving deep learning (DL) models. Following criteria [33], our research is organised around methodology, specialised approaches, application areas, datasets, and assessment measures. Our study follows a systematic literature review (SLR) methodology: developing research objectives, conducting structured searches, choosing relevant publications, and synthesising essential data. This systematic methodology analyses FL and DL-driven CDRS, focussing on privacy and recommendation accuracy.

The primary contributions of this systematic literature review are highlighted as follows:

- This SLR provides a detailed review of FL and DL-based CDRS models to assist academics and practitioners understand new trends and find effective solutions to cross- domain recommendation difficulties.
- We provide thorough analyses of outstanding problems and potential paths forward in FL-based CDRS, emphasising privacy issues, calculation efficiency, and rating prediction accuracy.
- Our study covers advanced CDRS models' methodologies, common difficulties, evaluation measures, datasets, algorithms, and methodological approaches in both qualitative and quantitative ways. This study covers federated learning development and use in cross-domain recommendation systems.

3.2 Research questions

The following research questions are intended to directly address the primary obstacles to federated learning implementation for cross-domain recommendation systems (CDRS), with an emphasis on rating prediction and privacy protection. The purpose of these enquiries is to investigate the efficacy, privacy benefits, and usefulness of federated learning in CDRS. The developed research questions and their justifications are shown in Table 1, offering a thorough way for assessing and contrasting federated CDRS techniques with other federated learning models and conventional recommendation systems.

Table 1 Research questions

RQ No	Research question	Motivation
RQ1	What federated learning techniques and frameworks can be effectively applied to cross- domain recommendation systems?	To identify and explore effective techniques that enhance cross- domain recommendation, focusing on federated learning models.
RQ2	What privacy-enhancing methods, such as differential privacy and secure aggregation, have been integrated into federated learning for CDRS?	To assess privacy-preserving techniques integrated into federated learning to protect user data in cross-domain recommendations.
RQ3	How effective is the proposed federated cross- domain recommendation system on real-world datasets from multiple domains?	To validate the performance and adaptability of the federated cross-domain model on practical, multi-domain datasets.
RQ4	How does the federated cross-domain recommendation method compare to traditional and other federated learning-based recommendation systems?	To evaluate the advantages and limitations of the federated cross-domain approach in comparison to existing recommendation methods.
RQ5	Can federated learning be empirically validated for privacy-preserving rating prediction in cross- domain recommendation systems?	To confirm the feasibility and effectiveness of federated learning for maintaining privacy in rating predictions across domains.

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.3 Search strategy

The main digital libraries, including Elsevier, IEEE Explores, Springer, ScienceDirect, MDPI, and Google Scholar, were automatically searched in order to collect the papers that are pertinent to this SLR. Due to their acceptability, vast collection of research papers, and plenty of research articles pertaining to our study topics, the six libraries were chosen. The quantity of the chosen papers from each digital library is shown in Fig. 2. The search terms used were: ("Federated Learning" OR "Cross-Domain Recommendation Systems" OR "Privacy Preservation" OR "Rating Prediction" OR "Deep Learning in CDRS") AND ("Privacy-Preserving Techniques" OR "Differential Privacy" OR "Secure Aggregation" OR "Privacy in Machine Learning" OR "Data Security" OR "User Privacy") AND .

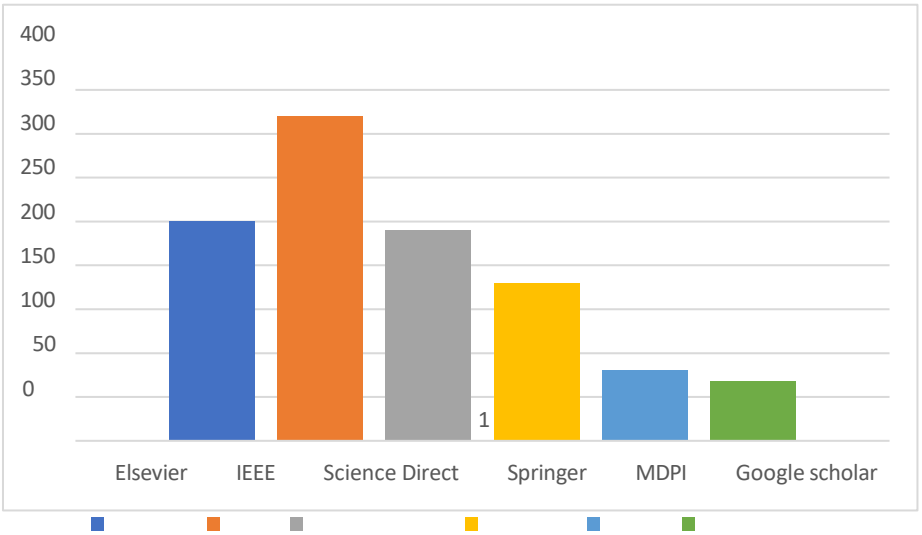


Figure 2 Publication digital libraries

("Recommendation Systems" OR "Cross-Domain Recommendations" OR "Federated Learning in Recommender Systems"). The search covered publications from 2014 to 2024 to ensure inclusion of the most recent advancements in the field.

3.4 Criteria for Inclusion and Exclusion

3.4.1. Inclusion Criteria

- Peer-reviewed journal articles, conference papers, and relevant industry reports.
- Papers published between 2014 and 2024 to capture the most up-to-date research.
- Studies that focus on federated learning, cross-domain recommendation systems (CDRS), privacy-preserving techniques in recommendation systems, and rating prediction using deep learning.
- Studies that use or suggest models based on deep learning, federated learning, and privacy-preserving algorithms within the framework of CDRS.
- Studies on rating prediction, cross-domain recommendation, and privacy protection that take into account federated learning models.

3.4.2 Exclusion Criteria

- Studies unrelated to CDRS, federated learning, or recommendation systems privacy- preserving strategies.
- publications from before 2014, since they could not accurately represent the most recent developments in CDRS and federated learning.
- Studies that are found to be duplicated across different databases or publications.

Reports, white papers, or preprints that have not undergone peer review. Data Extraction

Information that was crucial to our research was methodically filtered from the chosen articles according to established criteria during data extraction. Details pertaining to the study methodology,

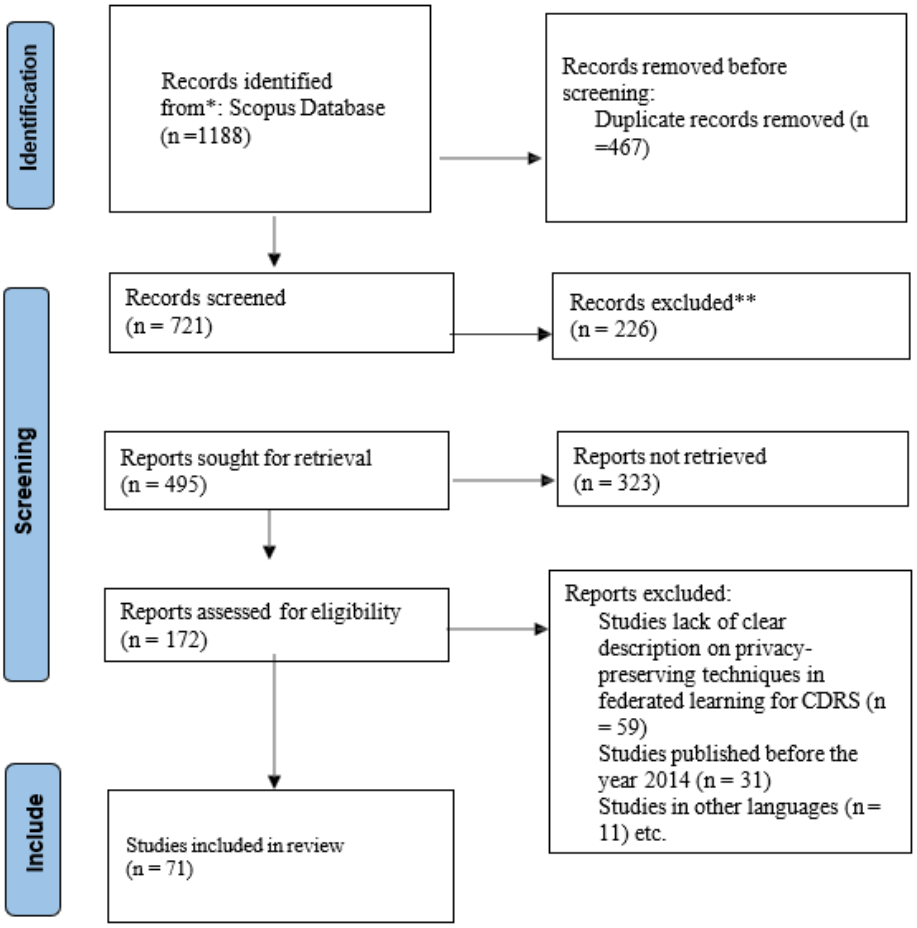
International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

privacy-preserving methodologies, dataset kinds, assessment metrics, and domain applications of cross-domain recommendation systems (CDRS) were the primary targets of the extraction. Furthermore, data on the federated CDRS models' performance results, including comparisons to conventional recommendation systems and other federated learning models, was mined. A thorough collection of pertinent data from all areas of federated learning for privacy protection and rating prediction was achieved via this procedure.

4 SLR Results

Initially, entries from the Scopus database were obtained in total: 1188 items. After duplicates were removed, 721 distinct records were screened. 226 records were excluded from consideration during the screening process based on predefined criteria. Excluded studies included those lacking clear descriptions of privacy-preserving techniques in federated learning for cross-domain recommendation systems (n = 59), those published before the year 2014 (n = 31), and studies published in languages other than English (n = 11). Furthermore, 323 records could not be retrieved for further evaluation. After evaluating the remaining 172 publications for eligibility, 71 research were included to the systematic review. The basis for a thorough examination of federated learning frameworks for privacy-preserving rating prediction in cross-domain recommendation systems was established by this selection, which satisfied the predetermined inclusion requirements.

PRISMA flow diagram outlining how the included studies were chosen.



Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5 Findings of the study

5.1 Design and Implementation of a Federated Learning Framework for Cross- Domain Recommendation Systems

Recommendation systems often use matrix decomposition because of its capacity to extract latent characteristics from user-item interactions. The approach's drawback, according to [34], is that matrix decomposition finds it difficult to extract intricate, deep information from latent characteristics. In order to overcome this, the Neural Collaborative Filtering (NCF) framework was put out. This framework substitutes a neural network for the inner product, enabling it to learn intricate functions from input data and capture more subtle user preferences. The inability to fully include an item's side characteristics is a problem with NCF, despite its usefulness. A new development in machine learning called federated learning has shown promise as a way to improve recommendation systems while protecting user privacy. One of the first to use a recommendation system based on federated learning was [35], who distributed a central model to clients for local training. User data is protected by keeping it on the client side, while model changes are compiled on a central server. The exact depiction of user preferences may be hampered by the data noise introduced by their method.

Numerous frameworks for federated learning have been created for recommendation systems, building on previous developments. FedRec is a federated architecture that uses explicit feedback for rating prediction, as presented by [28]. While increasing computational complexity, this approach federates decomposition-based recommendation models and masks user preferences by assigning virtual ratings to unrated objects. In order to preserve recommendation accuracy and increase privacy, [36] developed FedRec++, a lossless federated recommendation system that gathers denoised gradients from clients. Moreover, FedFast [37] speeds up model convergence by optimising parameter aggregation and customer screening. The evolution of privacy- preserving recommendation systems is shown by these federated learning frameworks, which work together to provide cross-domain suggestions that strike a compromise between accuracy, privacy, and computing efficiency.

5.2 Privacy-Preserving Techniques in Federated Learning

FRSs provide a distinct privacy issue because to their decentralised structure. Due to the distribution of training data across several nodes, ensuring data privacy is more challenging than in a centralised method. Current studies indicate that the central server may deduce sensitive information from the intermediate parameters. For example, a server may recognise things with which the user has engaged based on the non-zero gradients sent by the client [38]. Additionally, the server may deduce ratings from the user-uploaded gradients across two successive rounds [11]. In response to such issues, privacy-preserving approaches have been devised to safeguard user data privacy while enabling FRSs to function effectively. This section delineates the privacy-preserving mechanisms of FRSs and evaluates their benefits and drawbacks.

5.2.1 Differential Privacy

A method for protecting privacy that offers a mathematical assurance of privacy is differential privacy (DP) [39],[40]. It makes it challenging to distinguish distinct data within the dataset by introducing random noise to the data [41]. Recommendation systems are among the many areas in which this method has been used. As an example, the work in [42] used DP to safeguard user privacy in a collaborative filtering-based recommendation system.

On the other hand, federated learning makes advantage of local differential privacy (LDP), a kind of DP. LDP adds noise to each user's data before transmitting it to the server, as opposed to introducing noise to the whole dataset [44]. This guarantees that the server can still get valuable information even if it will never have access to the raw data. Numerous research have been carried out in this area; one of them, in [45], employed LDP to safeguard user privacy in a recommendation system based on matrix factorisation. In a similar vein, the authors of [46] enhanced matrix factorisation for recommender systems using LDP.

Received: August 14, 2025

Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Applying DP and LDP in FRS helps to protect user privacy while enabling the server to extract valuable data from the stream [47]. In addition, it ensure raw data is not accessed by the server, thus keeping user privacy intact. DP and LDP usage in FRSs possess some disadvantages like being the potential for spurious results from the added noise introduced to the data and the need for addition of the noise, which incurs longer computational periods [48].

5.2.2 Secure Multi-Party Computation

A cryptographic technique termed secure multi-party computing (SMPC) allows two or more parties to safely calculate a function over their private data without granting any of the parties access to the other parties' data [49]. To put it another way, SMPC guarantees the security of each party's private information while enabling the parties to access the computation's outcome across all the data without ever having to exchange the data.

Maintaining user data privacy, creating tailored recommendation platform are a few benefits of employing SMPC in FRSs [12]. However, there are some drawbacks of employing SMPC, such as the heavy to present a privacy preserving collaborative filtering system that allows several parties.

5.2.3 Homomorphic Encryption

A method of encryption that enables computations on encrypted data without necessitating decryption. Homomorphic encryption within a Federated Recommendation System (FRS) facilitates the sharing and encryption of data across several participants, enabling the calculation of recommendations based on the encrypted data Fully and partly homomorphic encryption (FHE and PHE) are the two primary types of homomorphic encryption used in FRSs. Specific computations like as addition or multiplication are only permitted by PHE, whereas FHE enables the execution of any function on encrypted data [22].

Homomorphic encryption has been used to recommendation systems in a number of research with encouraging outcomes. For instance, a recent work [23] used FHE to create a privacy- preserving matrix factorisation method. Another research [24] suggested employing homomorphic encryption to create a user-based recommendation system that protects privacy.

5.2.4 Tokenization

In FRSs, tokenisation facilitates the analysis and processing of data by dividing it into smaller units called tokens. This involves decomposing numerical data into integers and other values as well as text into words, sentences, and phrases [26]. By preventing sensitive user data, such preferences and personal information, from leaking, tokenisation also contributes to data security and privacy [27]. Tokenisation has been employed in FRSs in a number of experiments. To increase an FRS's performance, for instance, the authors used tokenisation in [28]. In order to enable the recommendation model to learn from dispersed data sources without jeopardising user privacy, they used a tokenisation technique based on the federated learning framework.

5.2.5 Anonymization

By hiding users' identity, anonymisation is a privacy-preserving approach in an FRS that protects their data privacy. The primary goal of this strategy is to preserve the data usefulness of users while masking their identifying information, including username, user ID, and other user-related data. This method enables the system to provide accurate and helpful suggestions while protecting users' personal data in the FRS. Numerous research have used the anonymisation approach in FRS, demonstrating the method's efficacy. The likelihood for data leakage and data distortion as a result of obscuring user identifying information are two drawbacks of utilising anonymisation in FRSs.

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6 Privacy-Preserving Rating Prediction Through Comparision

FRSs have made extensive use of the previously outlined privacy measures in order to provide more robust privacy protection. A comparison of these processes is shown in Table 2.

Table 2 Comparison between several privacy-preserving techniques

Reference	Privacy Type	Privacy Target	Privacy/ Accuracy	Communication/Computation Costs
[37]	Differential Privacy	Ratings	High	Low
[38]	Secure Multi-Party Computation	Ratings	Low	High
[11]	Homomorphic Encryption	High-Order Graphs Social Features Ratings	Moderate	High
[39]	Tokenization	Prediction	Low	Low
[40]	Anonymization	User's data	High	High
[41]	Pseudonymization	User's data	Moderate	Low

6.1 Publicly Available Datasets for Federated Recommendation Systems

A collection of publicly accessible datasets for Federated Recommendation Systems (FRSs) is given in the following section. These datasets address a variety of subjects, such as consumer preferences, music preferences, TV program ratings, and movie ratings. Every dataset has been meticulously selected to provide pertinent data for creating FRSs. These datasets may be used to train and evaluate FRS performance, and they are freely downloadable. The list of those datasets is shown in Table 3.

Table 3 Publicly available datasets that can be used for the development of Federated Recommendation Systems.

Name	Category	Variables	Data Type
Amazon	Reviews	Users, Reviews	Text, Numeric
MovieLens	Movies	Ratings, Genres	Numeric
Yelp	Reviews	Users, Reviews	Text, Numeric
Film Trust	Movies	Ratings, Genres	Numeric
Goodreads	Books	Reviews, Ratings	Text, Numeric
LastFM	Music	Listeners, Genres	Numeric
Douban	Movies/Books	Reviews, Ratings	Text, Numeric
BookCrossing	Books	Reviews, Ratings	Text, Numeric

Federated Recommendation Systems (FRSs) are developed and benchmarked using publicly accessible information in several research. These datasets allow researchers to develop and verify models across various recommendation settings since they span a variety of areas, such as user ratings, media preferences, and consumer behaviour. For instance, databases like Yelp, MovieLens, and Amazon provide a multitude of data on user reviews and ratings that may be used to evaluate and predict customer preferences. Others, like Goodreads and FilmTrust, focus on certain genres, such as movies and books, and provide useful data on genre preferences and rating patterns. While Douban and BookCrossing integrate many domains to enhance cross-domain recommendation capabilities, music databases such as LastFM provide information on user preferences. In order to facilitate reliable training, testing, and assessment of model performance, the datasets in Table 2 have been carefully selected for their applicability in FRS development.

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6.2 Comparing the Efficacy of Federated CDRS to Traditional Recommendation Systems

Traditional recommender systems include content-based strategies, collaborative filtering techniques, and hybrid approaches. Traditional recommender systems provide a number of benefits, but they may also have some disadvantages:

- **Cold-start problem:** This happens when an object or user is not sufficiently described to allow for the creation of relevant predictions. This may decrease the recommendation system's performance, especially for new goods or users.
- **Data sparsity:** Due to inadequate information in the system, collaborative filtering algorithms are vulnerable to data sparsity [48]. This produces a sparse user-item matrix, which may result in recommendations that are of low quality[49].

To solve issues with limited data and cold start, cross-domain recommender systems (CDRS) have been used in a number of applications [33]. Extracting common knowledge from one domain (the source domain) and applying it to another (the target domain) is the core idea of CDRS. Many publications have used various DL models or strategies in CDRS, such as matrix factorization-based methods that try to factorise many rating matrices from various domains in order to reduce data sparsity [48]. DL has recently been more well-liked in CDRS for deep feature extraction. DL-based approaches often use domain adaptation strategies and use nonlinear mapping functions to capture intricate interactions across domains. Neural networks were used by several writers to integrate other domains. According to certain writers, generative AI models have been used in CDRS almost as much as conventional approaches, and they provide superior results [49][50]. Providing tailored suggestions across several domains is a difficult challenge for CDRS.

6..2 Limitations of the study

This present review on federated cross-domain recommendation for privacy-preserving rating prediction suffers numerous constraints. The difficulty of guaranteeing robust data privacy across many fields is one key obstacle as improved privacy-preserving methods might raise computing costs and maybe lower model accuracy. Furthermore challenging the development of universally successful models is cross-domain data heterogeneity and sparsity, which usually calls for domain-specific modifications. The dependence on publicly accessible statistics also restricts real-world application as these datasets may not completely reflect the nuances of all user behaviour or industry-specific demands. Moreover, scaling is still difficult as federated learning systems might suffer with performance as domain complexity and data volume rise rise. At last, the absence of thorough empirical validation in many different real-world situations limits the generalisability of the suggested models, therefore suggesting a need for further research in many practical environments.

6.3 Future Scope

With several directions for future research, federated cross-domain recommendation systems intended for privacy-preserving rating prediction have great potential scope. First, without compromising model accuracy, improving privacy-preserving methods include homomorphic encryption, differential privacy, and secure multi-party computing can assist to boost data security. Moreover, improved strategies for cross-domain data integrationincluding domain adaptation and transfer learning can alleviate data sparsity and heterogeneity, hence enabling models to fit naturally across many domains. Testing these federated recommendation systems will assist to assess their adaptability and efficiency throughout multiple industries by means of real-world applications like healthcare, e-commerce, and tailored education. Comparative research using hybrid models and conventional recommendation approaches may assist find special performance advantages and trade-offs, therefore offering routes for optimisation. Moreover, initiatives to improve scalability by allowing models to handle more data and enable complex cross-domain interactions will greatly increase their value in big data environments, hence federated cross-domain recommendation is a progressively strong and

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

generally useful solution.

7 Conclusion

This systematic literature review (SLR) has studied, in general, the existing situation of federated cross-domain recommendation systems, especially with relation to privacy- preserving rating prediction. The review underlines the growing importance of federated learning techniques in safeguarding user data across various domains while maintaining high- quality recommendation performance by aggregating the findings of many studies. The study recognised important advances in privacy-preserving technologies such safe multi-party computing and differential privacy as well as challenges in controlling the heterogeneity and sparsity of cross-domain data. The review also emphasises how further research can widen real-world application testing, enhance data integration methods, and raise model scalability. Notwithstanding various disadvantages, including the reliance on publicly available datasets and the challenges in preserving strong privacy without compromising accuracy, the review offers a reasonable foundation for further research and development in this interesting topic. All things considered, the federated cross-domain recommendation technique offers enormous possibility for creating recommendation systems that are more secure, effective, and tailored for a range of companies.

References

[1] F. Ricci, L. Rokach, and B. Shapira, "Introduction to recommender systems handbook," in *Recommender systems handbook*, Springer, 2010, pp. 1–35.

[2] P. Nitu, J. Coelho, and P. Madiraju, "Improvising personalized travel recommendation system with recency effects," *Big Data Min. Anal.*, vol. 4, no. 3, pp. 139–154, 2021.

[3] Y. Zhang, C. Yin, Q. Wu, Q. He, and H. Zhu, "Location-aware deep collaborative filtering for service recommendation," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 51, no. 6, pp. 3796–3807, 2019.

[4] P. Cremonesi, A. Tripodi, and R. Turrin, "Cross-domain recommender systems," in *2011 IEEE 11th International Conference on Data Mining Workshops*, Ieee, 2011, pp. 496–503.

[5] M. M. Khan, R. Ibrahim, and I. Ghani, "Cross domain recommender systems: A systematic literature review," *ACM Comput. Surv.*, vol. 50, no. 3, pp. 1–34, 2017.

[6] X. Li, G. Cong, X.-L. Li, T.-A. N. Pham, and S. Krishnaswamy, "Rank-geofm: A ranking based geographical factorization method for point of interest recommendation," in *Proceedings of the 38th international ACM SIGIR conference on research and development in information retrieval*, 2015, pp. 433–442.

[7] C. Gao *et al.*, "Cross-domain recommendation without sharing user-relevant data," in *The world wide web conference*, 2019, pp. 491–502.

[8] A. P. Singh and G. J. Gordon, "Relational learning via collective matrix factorization," in *Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2008, pp. 650–658.

[9] C. Gao, C. Huang, Y. Yu, H. Wang, Y. Li, and D. Jin, "Privacy-preserving cross-domain location recommendation," *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 3, no. 1, pp. 1–21, 2019.

[10] D. Chai, L. Wang, K. Chen, and Q. Yang, "Secure federated matrix factorization," *IEEE Intell. Syst.*, vol. 36, no. 5, pp. 11–20, 2020.

[11] K. Bonawitz *et al.*, "Practical secure aggregation for privacy-preserving machine learning," in *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1175–1191.

[12] L. Zhao, S. Pan, E. Xiang, E. Zhong, Z. Lu, and Q. Yang, "Active transfer learning for cross-system recommendation," in *Proceedings of the AAAI Conference on Artificial Intelligence*, 2013, pp. 1205–1211.

Received: August 14, 2025

[13] L. Hu, J. Cao, G. Xu, L. Cao, Z. Gu, and C. Zhu, "Personalized recommendation via cross-domain triadic factorization," in *Proceedings of the 22nd international conference on World Wide Web*, 2013, pp. 595–606.
[14] B. W. Suter, "The multilayer perceptron as an approximation to a Bayes optimal discriminant function," *IEEE Trans. neural networks*, vol. 1, no. 4, p. 291, 1990.
[15] J. He, R. Liu, F. Zhuang, F. Lin, C. Niu, and Q. He, "A general cross-domain recommendation framework via Bayesian neural network," in *2018 IEEE International Conference on Data Mining (ICDM)*, IEEE, 2018, pp. 1001–1006.
[16] T. Man, H. Shen, X. Jin, and X. Cheng, "Cross-domain recommendation: An embedding and mapping approach.," in *IJCAI*, 2017, pp. 2464–2470.
[17] C. Zhao, C. Li, R. Xiao, H. Deng, and A. Sun, "CATN: Cross-domain recommendation for cold-start users via aspect transfer network," in *Proceedings of the 43rd international ACM SIGIR conference on research and development in information retrieval*, 2020, pp. 229–238.
[18] J. Canny, "Collaborative filtering with privacy via factor analysis," in *Proceedings of the 25th annual international ACM SIGIR conference on Research and development in information retrieval*, 2002, pp. 238–245.
[19] F. McSherry and I. Mironov, "Differentially private recommender systems: Building privacy into the netflix prize contenders," in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2009, pp. 627–636.
[20] B. Liu, D. Kong, L. Cen, N. Z. Gong, H. Jin, and H. Xiong, "Personalized mobile app recommendation: Reconciling app functionality and user privacy preference," in *Proceedings of the eighth ACM international conference on web search and data mining*, 2015, pp. 315–324.
[21] A. Berlioz, A. Friedman, M. A. Kaafar, R. Boreli, and S. Berkovsky, "Applying differential privacy to matrix factorization," in *Proceedings of the 9th ACM Conference on Recommender Systems*, 2015, pp. 107–114.
[22] C. Chen, Z. Liu, P. Zhao, J. Zhou, and X. Li, "Privacy preserving point-of-interest recommendation using decentralized matrix factorization," in *Proceedings of the AAAI conference on artificial intelligence*, 2018.
[23] Y. Zhang, J. Pan, L. Qi, and Q. He, "Privacy-preserving quality prediction for edge- based IoT services," *Futur. Gener. Comput. Syst.*, vol. 114, pp. 336–348, 2021.
[24] W. Meihan, L. Li, C. Tao, E. Rigall, W. Xiaodong, and X. Cheng-Zhong, "FedCDR: Federated Cross-Domain Recommendation for Privacy-Preserving Rating Prediction," in *Proceedings of the 31st ACM International Conference on Information \& Knowledge Management*, in CIKM '22. New York, NY, USA: Association for Computing Machinery, 2022, pp. 2179–2188. doi: 10.1145/3511808.3557320.
[25] Y. Wang, M. Gao, X. Ran, J. Ma, and L. Y. Zhang, "An improved matrix factorization with local differential privacy based on piecewise mechanism for recommendation systems," *Expert Syst. Appl.*, vol. 216, p. 119457, 2023.
[26] S. R. Pandey, L. D. Nguyen, and P. Popovski, "Fedtoken: Tokenized incentives for data contribution in federated learning," *arXiv Prepr. arXiv2209.09775*, 2022.
[27] E. Bandara, X. Liang, S. Shetty, R. Mukkamala, A. Rahman, and N. W. Keong, "Indy528—Federated learning model Tokenization with non-fungible tokens (NFT) and model cards," in *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, IEEE, 2022, pp. 195–201.
[28] Y. Tian, Y. Wan, L. Lyu, D. Yao, H. Jin, and L. Sun, "FedBERT: When federated learning meets pre-training," *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 4, pp. 1–26, 2022.
[29] X. Wu, Y. Zhang, M. Shi, P. Li, R. Li, and N. N. Xiong, "An adaptive federated learning scheme with differential privacy preserving," *Futur. Gener. Comput. Syst.*, vol. 127, pp. 362–372, 2022.
[30] K. V. Dudekula *et al.*, "Convolutional neural network-based personalized program

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

recommendation system for smart television users," *Sustainability*, vol. 15, no. 3, p. 2206, 2023.
[31] W. Ali, R. Kumar, Z. Deng, Y. Wang, and J. Shao, "A federated learning approach for privacy protection in context-aware recommender systems," *Comput. J.*, vol. 64, no. 7, pp. 1016–1027, 2021.
[32] M. Rahul, A. Singh, S. Verma, H. Shukla, and V. Yadav, "Content-Based Book Recommender System Using Supervised Learning," in *International Conference on Cyber Intelligence and Information Retrieval*, Springer, 2023, pp. 367–374.
[33] J. Nie, Z. Zhao, L. Huang, W. Nie, and Z. Wei, "Cross-Domain Recommendation Via User-Clustering and Multidimensional Information Fusion," *IEEE Trans. Multimed.*, vol. 25, pp. 868–880, 2021.
[34] S.-T. Zhong, L. Huang, C.-D. Wang, J.-H. Lai, and S. Y. Philip, "An autoencoder framework with attention mechanism for cross-domain recommendation," *IEEE Trans. Cybern.*, vol. 52, no. 6, pp. 5229–5241, 2020.
[35] Y. Ouyang, B. Guo, X. Tang, X. He, J. Xiong, and Z. Yu, "Mobile app cross-domain recommendation with multi-graph neural network," *ACM Trans. Knowl. Discov. from Data*, vol. 15, no. 4, pp. 1–21, 2021.
[36] T. Hirakawa, K. Maeda, T. Ogawa, S. Asamizu, and M. Haseyama, "Cross-domain recommendation method based on multi-layer graph analysis with visual information," in *2021 IEEE International Conference on Image Processing (ICIP)*, IEEE, 2021, pp. 2688–2692.
[37] Y. Li, J. Ren, J. Liu, and Y. Chang, "Deep sparse autoencoder prediction model based on adversarial learning for cross-domain recommendations," *Knowledge-Based Syst.*, vol. 220, p. 106948, 2021.
[38] S. Sahebi and P. Brusilovsky, "Cross-domain collaborative recommendation in a cold- start context: The impact of user profile size on the quality of recommendation," in *User Modeling, Adaptation, and Personalization: 21th International Conference, UMAP 2013, Rome, Italy, June 10-14, 2013 Proceedings 21*, Springer, 2013, pp. 289–295.
[39] A. Da'u and N. Salim, "Recommendation system based on deep learning methods: a systematic review and new directions," *Artif. Intell. Rev.*, vol. 53, no. 4, pp. 2709–2748, 2020.
[40] S. Natarajan, S. Vairavasundaram, S. Natarajan, and A. H. Gandomi, "Resolving data sparsity and cold start problem in collaborative filtering recommender system using linked open data," *Expert Syst. Appl.*, vol. 149, p. 113248, 2020.
[41] A. Agarwal, D. S. Mishra, and S. V Kolekar, "Knowledge-based recommendation system using semantic web rules based on Learning styles for MOOCs," *Cogent Eng.*, vol. 9, no. 1, p. 2022568, 2022.
[42] H. Kuang, W. Xia, X. Ma, and X. Liu, "Deep matrix factorization for cross-domain recommendation," in *2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, IEEE, 2021, pp. 2171–2175.
[43] J. Yang, J. Zhu, X. Ding, Y. Peng, and Y. Zhang, "A memory pool variational autoencoder framework for cross-domain recommendation," *Expert Syst. Appl.*, vol. 241, p. 122771, 2024.
[44] E. Q. Da Silva, C. G. Camilo-Junior, L. M. L. Pascoal, and T. C. Rosa, "An evolutionary approach for combining results of recommender systems techniques based on collaborative filtering," *Expert Syst. Appl.*, vol. 53, pp. 204–218, 2016.
[45] C.-D. Wang, Y.-H. Chen, W.-D. Xi, L. Huang, and G. Xie, "Cross-domain explicit– implicit-mixed collaborative filtering neural network," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 52, no. 11, pp. 6983–6997, 2021.
[46] P. K. Balasamy and K. Athiyappagounder, "An Optimized Feature Selection Method for E-Learning Recommender System Using Deep Neural Network based on Multilayer Perceptron.," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 5, 2022.
[47] J. Cao, J. Sheng, X. Cong, T. Liu, and B. Wang, "Cross-domain recommendation to cold-start users via variational information bottleneck," in *2022 IEEE 38th International Conference on*

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Data Engineering (ICDE), IEEE, 2022, pp. 2209–2223.
[48] S. Zhang *et al.*, "Personalized latent structure learning for recommendation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 8, pp. 10285–10299, 2023.
[49] S. Soundariya, S. V Manisekaran, S. Ramakrishnan, A. Ganesh, and R. Keerthi, "Cross Domain Movie Recommendation System using Personalized Preference Transfer," in *2022 International Conference on Edge Computing and Applications (ICECAA)*, IEEE, 2022, pp. 1650–1654.
[50] A. Ahmed, K. Saleem, O. Khalid, J. Gao, and U. Rashid, "Trust-aware denoising autoencoder with spatial-temporal activity for cross-domain personalized recommendations," *Neurocomputing*, vol. 511, pp. 477–494, 2022.

Received: August 14, 2025