SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I8P133

Volume 12 Issue 8, 384-394, August 2025
© 2025 Seventh Sense Research Group®

Original Article

A Privacy-Preserving Federated Recommender System with Neuro-Fuzzy Modeling and Local Differential Privacy

Thenmozhi Ganesan[1], Palanisamy Vellaiyan[2]

[1,2]*Department of Computer Applications, Alagappa University, Tamil Nadu, India.*

[1]*Corresponding Author : thenmozhigphd@alagappauniversity.ac.in*

Received: 18 June 2025 Revised: 19 July 2025 Accepted: 19 August 2025 Published: 30 August 2025

Abstract *- The increasing reliance on personalized recommender systems in e-commerce platforms has brought major challenges in terms of data privacy, interpretability, and the model's sturdiness. Traditional recommender systems are often mandated to access raw user data to predict relevant preferences, leading to severe privacy risks. Federated recommender system is a promising paradigm that enables decentralized model training to rectify the limitations by not exposing the unmodified user data, yet faces central server's inference attacks and lacks in defending predictions. To bridge these research gaps, this study attempts a novel hybrid neuro–fuzzy model that integrates the strength of fuzzy membership function with a deep neural network in the federated learning environment to enhance transparency in personalized recommendations. Additionally, local differential privacy is employed with Laplace noise injection to the locally trained model gradients, thereby maintaining user privacy without revealing sensitive information. The model has been collaboratively trained on local client devices, aligning with the concepts of decentralized learning. Extensive experiments were undertaken on the real-world MovieLens 100K and 1M datasets to examine the efficacy of the presented mechanism. Research findings highlight that the studied neuro-fuzzy architecture surpasses the conventional models in terms of Normalized discounted cumulative gain, precision, recall, root mean squared error and mean absolute error over multiple measurements of privacy budget. The proposed approach achieved a strong balance among relevancy accuracy (0.205 obtained for the 100 K dataset and 0.165 achieved for the 1 M dataset), privacy and interpretability.*

Keywords *- Collaborative filtering, Deep Neural Network, Federated learning, Fuzzy Logic, Laplace noise injection and recommender system.*

1. Introduction

In this digital world, recommender system becomes an integral part of the information technology to find the relevant user preferences from the vast volume of data with less time in fields like e-commerce, education, entertainment, etc. [1]. To find the exact match of the user's interest, the recommender system requires direct access to user data, which threatens user privacy. Predicting the relevant preferences without compromising the user's privacy is quite challenging yet essential, especially when personalized suggestions are involved [2].

To tackle these limitations, federated learning has been identified as a promising solution that enables collaborative model training in local devices without revealing the real data [3]. However, federated recommender systems face issues like inference attacks and a lack of mechanisms for defending their predictions [4]. Furthermore, a robust hybridized methodology is necessitated to predict the user preferences when the data is redundant and uncertain to maintain the interpretability. To ensure the user's privacy in the shared environment, asking for their local data with its parameters is efficient, yet the prediction accuracy is limited due to the data limitation [5]. Hence, it is necessary to provide accurate predictions; exclusion of personal users' data is essential.

This study exploits an innovative hybridized neural-fuzzy approach, which collaborates the strengths of fuzzy logic and deep neural networks that train the data locally to handle the data ambiguity and uncertainty. Federated learning is incorporated to prevent exposing raw user data to the global server to ensure user privacy. To preserve the global server inference of the shared data, Laplace noise is added to the model gradients before sending them to the central server. This hybrid approach rectified the shortcomings of the traditional deep learning methods and obtained accurate predictions without affecting the user's privacy.

The novel improvements of the model are as follows: Primarily, enhancing the predictive performance of the recommender system using the hybridized approach of neuro-fuzzy modeling to handle the ambiguity and vagueness in large data. Secondly, to guarantee the security of users in a global network, federated learning is incorporated, which considers intermediate gradients instead of the direct private data of users.

This method allows the model to learn on local devices and share only the gradients to the global server. Finally, local differential privacy is exploited on these gradients by injecting the Laplace noise into them prior to sending them to the central server. This dual privacy protocol augments users' privacy in a shared environment and enhances the suggestive relevancy.

The core contributions of the present study are detailed below:

- Built a robust neuro-fuzzy modeling to predict the most appropriate user preferences (top k recommendations) using fuzzification, fuzzy rules, and a fuzzy embedded deep neural network.
- For privacy preservation of the user, federated learning is incorporated into this architecture, which shares the model gradients with the global server instead of raw user data to prevent data inference by the global server.
- A local differential privacy mechanism is performed on these model gradients by injecting the Laplace noise into this trained model prior to feeding it into the global server to guarantee a secure environment.
- The model's trade-off between utility and privacy was illustrated under various privacy budgets(ε).

This paper is structured as follows: Section 2 reviews related works. Section 3 furnishes the proposed methodology. Section 4 outlines the experimental design. Section 5 demonstrates the results and discussion of this research, and Section 5 summarizes the work and proposes openings for future exploration.

2. Related Works

While various researchers have focused on enhancing recommendation and prediction accuracy, fewer have addressed the significance of user privacy. This section reviews relevant contributions in these areas and recognizes the research gaps that the studied work aims to address.

In [6], an improved fusion of fuzzy logic-based deep learning techniques is proposed to provide recommendations in industrial organizations. The author fuses fuzzy rules with a deep learning approach to enrich the interpretability and accuracy by handling ambiguity and uncertainty. CNN and RNN-based feature extraction techniques were exploited to extract the meaningful features that assist the prediction process.

A deep neural network model that depends upon federated learning is proposed in [7] to enhance the user privacy in the global server. This method utilizes a federated learning mechanism to share the data to the global server, which only shares the model parameters instead of the user's private information. Further, the author uses the pseudo-interaction filling approach to hide the real data to prevent server inference attacks.

In [8], the fuzzy-assisted Pearson correlation integration is studied to advance the recommendation in a social network environment. Labels, friendship and group memberships are utilized to determine similarity between users and movies.

Since the user preferences are not stable, it is hard to find the relevant match. To overcome this limitation, a fuzzy rules-based ontology is proposed in [9], in which fuzzy logic is employed to predict similar items in a dynamic manner. In addition, the author fused sentiment analysis to compute the sentimental score related to the end-user product.

In [10], federated learning based local differential privacy with security aggregation is proposed to equate the training efficacy and privacy protection in centralized environment. Though this clustering technique exploited the distributed training, it provides centralized training-like performance.

Local differential privacy enhanced matrix factorization proposed in [11] to ascertain the relevant items and provide privacy protection. Additionally, the author has employed a stochastic dimensionality reduction method, which drastically diminishes the perturbation error and stabilizes the generated recommendations.

In [12], a federated deep reinforcement learning recommender system is studied to overcome the balance between the communication overhead and potential threats to the user's private data. To acquire this, the SlateQ mechanism is leveraged to predict the long-term behavior of users and learn from a single-user multiple-platform approach.

A federated recommendation framework with differential privacy is proposed in [13], which leverages the training process performed in a global server without revealing the raw data and allows the local device to maintain it. To ensure the dual security differential privacy is implemented by obfuscating aggregated weights with calibrated noise prior to being sent to the central server.

In [14], a fuzzy logic-based recommendation for processing is proposed to build a robust condition monitoring system. It embeds the data along with the fuzzy algorithm within the processing system to predict the suggestions. The author achieved a higher accuracy on this hybrid model, ranging from 5% to 14.5% accuracy.

To handle data sparsity, cold start and improve relevancy, the author proposed a novel hybrid approach in [15] that collaborates with advancing technologies such as collaborative filtering, RNN and Singular Value Decomposition. This hybrid model necessitates an N-sample algorithm to suggest the top 10 relevant items to the users on the internet. RMSE and MAE are considered evaluation parameters and show substantial improvement in predicting personalized recommendations.

In [16], a novel federank approach is studied, which learns private factorization in a server by an asynchronous training process. The studied model provided the users with limited data sharing, which depends on the users' personal privacy control mechanisms. Yet this model offers personal security on a small portion of the data instead of the complete data that lacks security in a distributed environment.

Fuzzy C-means clustering and Shapley value are integrated [17] in a collaborative filtering recommender system to present the privacy-enriched predictions and performance. Pearson correlation is applied to predict the similarity, and the fuzzy incorporated Shapley demonstrated that the model achieved ε - ε-differential privacy.

In [18], Multimodal privacy-preserving federated learning is studied to alleviate the inadequacies of unimodal recommender systems, which are employed under various weight ratios under various modalities. Byzantine attacks are considered in this study by recognizing malicious clients in the distributed network by using a federated learning collaborative LDP mechanism.

Despite this literature, very few and limited works have employed the integration of a federated deep neural network with LDP. To the extent of the literature review, this is the first work to unify federated neuro-fuzzy modeling with a local differential privacy mechanism into a single recommendation framework. The studied method attempts to fill the existing gaps by incorporating a neuro-fuzzy architecture to ensure interpretability and strong privacy through local differential privacy within a federated learning environment. Further, the model guarantees the recommendation's transparency, relevancy, accuracy, and utility without affecting user privacy.

3. Proposed Methodology

Predicting the relevant and suitable items from the massive volume of data without compromising the user's privacy is a challenging task in a recommender system. To achieve this, the fuzzy approach is experimented with a local differential privacy mechanism in this study. When a fuzzy layer is embedded with deep neural network layers, it effectively handles the data ambiguity and vagueness, which provides the most accurate recommended list. To ensure the user's privacy, it is implemented using federated learning, in which user gradients are only shared instead of raw user data. Figure 1 depicts the functional framework of the neuro-fuzzy modeling.

The architecture of the neuro-fuzzy model consists of three key components: client-side fuzzy-DNN embedding, model gradient perturbation using LDP, and federated aggregator server-side. As an initial stage, preprocessing is done by the clients on the private data, then fuzzy rules are applied to them using a fuzzy membership function. These fuzzified inputs are then trained using DNN layers. The output of the DNN gradients is then perturbed by applying the LDP mechanism using Laplace noise injection. This noisy output is then fed to the central server for aggregation. Figure 2 demonstrates the workflow of the proposed privacy-preserving federated recommender system model.

3.1. Data Collection

Load the movie rating dataset into the system with user ID, movie ID, rating and timestamp.

3.2. Data Preprocessing

Redundant ratings and null values are checked and removed in this stage to maintain data integrity. In this modeling, the timestamp column is unnecessary and is eliminated.

3.3. Fuzzification of Ratings

To train the model using a fuzzy approach, the numerical input ratings are converted into fuzzy inputs using the fuzzy membership function to handle the uncertainty and ambiguity in user preferences. In this study, raw user-item ratings are interpreted into interpretable fuzzy categories using fuzzy rules before sending them into the DNN to enhance the robustness of sparseness in ratings and vagueness. The user input ratings for the fuzzy system range from 1 to 5, which are converted as follows:

Low (L) – weak preferences
Medium (M) – moderate preferences
High (H) – strong preferences
The formula for a triangular fuzzy membership function is given in Equation (1).

$$\mu_A\,(x) = \begin{Bmatrix} 0 & \text{if } x \le \alpha \\ \dfrac{x-\alpha}{\beta-\alpha} & \text{if } \alpha \le x \le \beta \\ \dfrac{\gamma-x}{\gamma-\beta} & \text{if } \beta \le x \le \gamma \\ 0 & \text{if } \gamma \le x \end{Bmatrix} \qquad (1)$$

Where α, β and γ denote the triangle's left base, peak and right base, respectively.

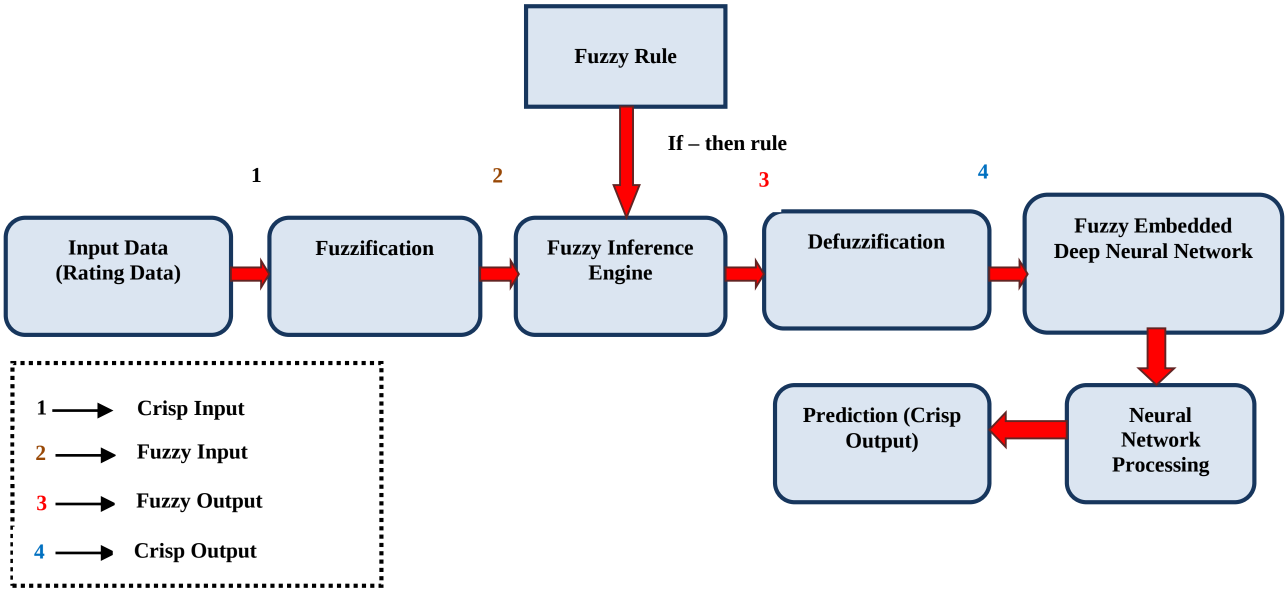

Fig. 1 Functional framework of the neuro-fuzzy modeling

The simplified equation is reported in Equation (2).

$$\mu_A\ (x) = \max\left(\min\left(\frac{x-\alpha}{\beta-\alpha}, \frac{\gamma-x}{\gamma-\beta}\right), 0\right) \tag{2}$$

Triangular member function for the user ratings from 1 to 5 can be written as follows:

For Low (x), the rating range is between 1 and 3, with peak 1.

$$\mu_A\ (L) = \max\left(\min\left(1, \frac{3-x}{2}\right), 0\right) \tag{3}$$

For Medium (x), the rating range is between 2 and 4, with a peak of 3.

$$\mu_A\ (M) = \max\left(\min\left(\frac{x-2}{1}, \frac{4-x}{1}\right), 0\right) \tag{4}$$

For High (x), the rating range is between 3 and 5, with a peak of 5.

$$\mu_A\ (H) = \max\left(\min\left(\frac{x-3}{2}, \frac{5-x}{5-5}\right), 0\right) \tag{5}$$

Here, $\frac{5-x}{5-5}$ is undefined. Hence, after dropping this, Equation (5) can be written as

$$\mu_A\ (H) = \max\left(\min\left(\frac{x-3}{2}, 0\right), 0\right) \tag{6}$$

3.4. Fuzzy Rules

The fuzzy rule is a small set of if-then rules that is used to map fuzzified categorical input into a user preference recommendation score. The following are the core rules of fuzzy for recommendation.

Rule 1: If the predicted rating is low, then the preference for the recommendation is weak.

Rule 2: If the predicted rating is medium, then preference for the recommendation is moderate.

Rule 3: If the predicted rating is high, then preference for the recommendation is strong.

These fuzzy rules act as a fuzzy inference engine, considered the supportive system of a deep neural network by feeding it with refined input as a data source. Table 1 represents the input values of the user ratings after the Fuzzification process.

Table 1. Input ratings after fuzzification

S.No	Rating	Low	Medium	High
1	1.0	1.0	0.0	0.0
2	2.0	0.5	0.0	0.0
3	2.5	0.25	0.5	0.0
4	3.0	0.0	1.0	0.0
5	3.5	0.0	0.5	0.25
6	4.0	0.0	0.0	0.5
7	5.0	0.0	0.0	1.0

3.5. Defuzzification

The fuzzified outputs from the fuzzy inference engine are converted into crisp numerical outputs. This serves as an input to the deep neural network for the training process.

3.6. DNN Training

Fuzzy membership values generated from the fuzzy inference engine are decoded into numerical output using the defuzzification process. These crisp rating vectors are then fed to the deep neural network architecture that features an input layer, comprising two latent layers and an output layer. This research uses a deep neural network to input numerically encoded crisp output. Dense latent layers are constructed, each fully connected and utilizing the ReLU activation function and dropout layers for regularization. Each dense layer consists of n neurons. Dropout layers (1 and 2) are used to prevent the issue of overfitting of the model to enhance the generalization. Further, these dropout layers normalise ReLU activation during training to stabilize the network learning for every mini-batch of learning. The crisp numerical output produced by the output layer represents the predicted user preferences. From this crisp output, the top k recommendation for the users is generated and predicted.

3.7. Local Differential Privacy Perturbation

Locally trained model gradients are injected with noise before being transferred to the global server to prevent user privacy. The federated learning environment shares only the model gradients instead of raw user data. A post-training local differential privacy noise injection mechanism is endeavoured in this study. After being trained with a fuzzy model, each client injects the Laplace noise into their model parameters (not to the model output) prior to sharing with the global server. $\mathrm{Lap}\left(\frac{\Delta w}{\varepsilon}\right)$ The added noise to each of the model's parameters Δ indicates the sensitivity, and ε denotes the privacy budget. Both guaranteed that the global aggregator cannot infer user privacy, even from the trained models. If the weights or the gradient of the trained model are w_i And the sensitivity added to the weight is Δw, then the equation for the Laplace noise injection is written as

$$w_i' = w_i + \mathrm{Lap}\left(\frac{\Delta w}{\varepsilon}\right) \tag{7}$$

These added weights of each client are then sent to the global server, and a secure aggregation is performed using a global aggregator using FedAvg to construct the global model. The updates from the global aggregator are being sent back to the local clients.

3.8. Algorithm

```
Steps:
Begin
Step 1:  Input the MovieLens 100K and 1M dataset. User ratings -R; Privacy budget – $\varepsilon$ and Total number of rounds – N.
Step 2:  Preprocessing of user data for null and redundant values, and dropping the field timestamp T.
Step 3:  For each user client, Apply a fuzzy if-then rule to fuzzify the numerical crisp input to the fuzzy categorical inputs.
         i.e.Low ($\mu_A$ (L)), Medium ($\mu_A$ (M)) and
         High ($\mu_A$ (H)).
Step 4:  Defuzzification of the fuzzy output into crisp output.
Step 5:  Train the data with a local deep neural network model with fuzzified numerical inputs to predict the top k recommendations(for $k = 5, k = 10$ and $k = 20$).
Step 6:  Gradient computation (g) using the incorporation of federated learning.
Step 7:  Perturb the locally trained model gradients by applying the LDP mechanism. i.e. Injecting Laplace noise into the trained weights ($w_i'$).
                $w_i' = w_i + \mathrm{Lap}\left(\frac{\Delta w}{\varepsilon}\right)$
Step 8:  Feed these perturbed weights into the global server.
Step 9:  Server aggregator aggregates these noisy gradients using FedAvg.
Step 10: Update the aggregated model and feed it to all the local endpoint devices.
Step 11: Repeat for N rounds.
End
```

4. Experimental Design

4.1. Dataset Specification

The studied model is evaluated using two real-world benchmark datasets, MovieLens 100K and MovieLens 1M, obtained from the GroupLens website. Both contain explicit numerical ratings ranging from 1 to 5, which are given by the users with User ID, Movie ID, Ratings, and Timestamp fields. Table 2 presents the descriptive statistics of the experimental datasets.

Table 2. Descriptive statistics of the experimental datasets

Dataset	Interaction	User	Movie	Sparsity
MovieLens 100K [19]	100,000	943	1700	93.69%
MovieLens 1M [20]	1,000,209	6,040	3952	95.53%

4.2. Software Description

The learning and implementation phases of the proposed model are performed using Python 3.8 managed through one of the IDEs of Python programming called Anaconda Navigator, which has inbuilt packages of machine learning libraries, including TensorFlow and scikit-learn. Jupyter Notebook is used as a coding editor, and Windows 10 Pro (64-bit) OS with Intel i5 Processor with RAM 8 GB DDR 512 GB SSD hardware environment is used for the computational processes.

4.3. Performance Parameters

The competence and efficiency of the presented approach are evaluated using the following quantitative measures: Precision, Recall and Normalized Discounted Cumulative Gain (NDCG) used for prediction and recommendation accuracy, whereas Root Mean Squared Error (RMSE) and Mean Absolute Error (MAE) are considered for error statistics.

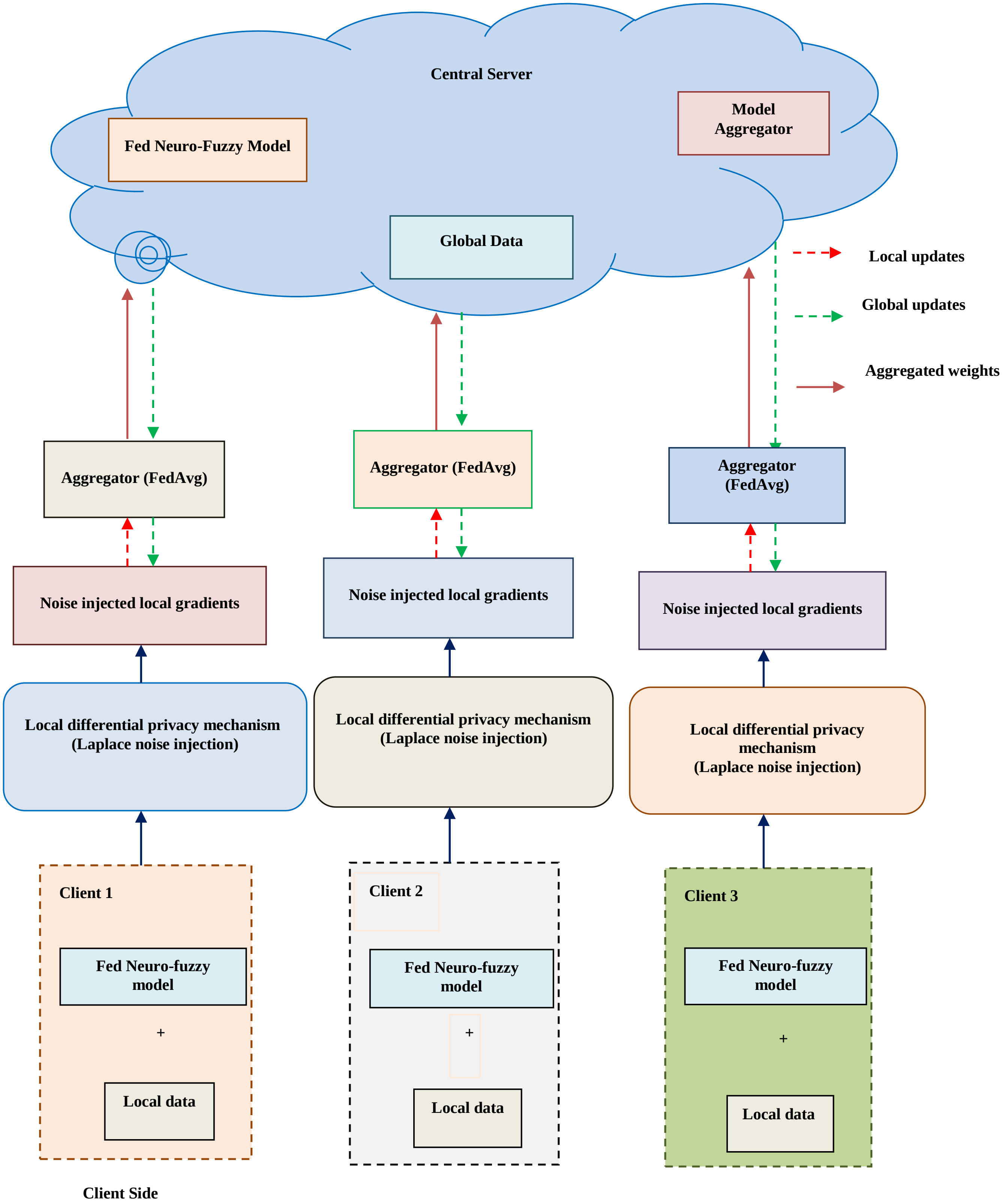

Fig. 2 Workflow of the proposed privacy-preserving federated recommender system model

4.3.1. Precision

It is the measure of the ratio of actual appropriate items of the top k suggested items. The higher values in precision indicate higher accuracy in the recommendation.

4.3.2. Recall

It measures the total count of appropriate items that are successfully suggested within the top k recommendation list. Like precision, the higher value of recall demonstrates better user preferences.

4.3.3. Normalized Discounted Cumulative Gain

NDCG quantifies the ranking quality of the recommended items in the list by providing higher scores to the appropriate items in the top k recommendation list.

4.3.4. Root Mean Squared Error

Root mean squared error computes the root of the mean squared deviations between the actual and predicted ratings. Lower RMSE values offer higher recommendation accuracy. The general equation to measure RMSE value is given in Equation (8).

$$\mathrm{RMSE} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}} (\hat{\mathrm{r}}_{\mathrm{i}} - \mathrm{r}_{\mathrm{i}})^2 \qquad (8)$$

Where N corresponds to the count of predicted user-item ratings and i represents the items. r_{i} and $\hat{\mathrm{r}}_{\mathrm{i}}$ are the actual ratings recorded by the user and the predicted item for item I, respectively.

4.3.5. Mean Absolute Error

Mean absolute measure quantifies the average difference between user-provided and predicted ratings. If the MAE value is low, then the recommendation accuracy will be high. The equation for the MAE calculation is presented in Equation (9).

$$\mathrm{MAE} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}} |\hat{\mathrm{r}}_{\mathrm{i}} - \mathrm{r}_{\mathrm{i}}| \qquad (9)$$

Where N is the count of predicted user-item ratings; i indicates the items; r_{i} and $\hat{\mathrm{r}}_{\mathrm{i}}$ are the true user ratings and predicted ratings, respectively.

5. Results and Discussion

This segment elaborates on the experimental outcomes derived from the introduced neuro–fuzzy model and presents the detailed discussion of the research findings. To measure the reliability of the model, various assessments are carried out on the experimental datasets, i.e. MovieLens 100K and MovieLens 1M. For the implementation, these datasets are partitioned into training data and evaluation data. Training data was leveraged to train the model parameters, comprising 80 % of the whole dataset for this research. The remaining 20% of the data is reserved for the evaluation and prediction processes of the model. To evaluate the efficacy of the proposed technique, it is compared against three baseline models, such as FNN [21], FedRec-DP [13] and FedDeepFM [7]. In Figures 3 and 4, accuracy measures such as NDCG, precision and recall comparison for the proposed model at various k values are demonstrated for MovieLens 100K and MovieLens 1M, respectively.

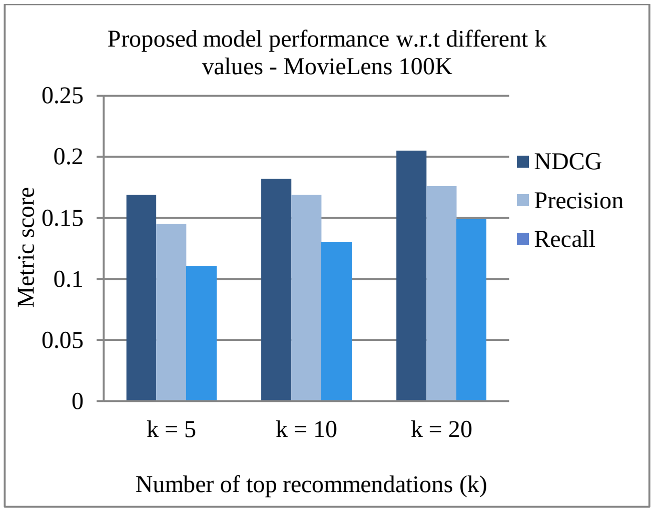

Fig. 3 Top k comparison of the proposed model for MovieLens 100K

Here, k represents the number of top movie recommendations, i.e. k = 5, k = 10 and k = 20. The comparison table of the top recommendation on two evaluation datasets is presented in Table 3. For the 100K dataset, the accuracy of the recommendation with 20 movies is relatively higher than the recommendation list with five movies, as the 1M dataset's accuracy measures are slightly lower than the 100K results due to its scalability, even though NDCG for the top 20 k recommendation is comparatively better for both datasets than the list with 5 recommendations.

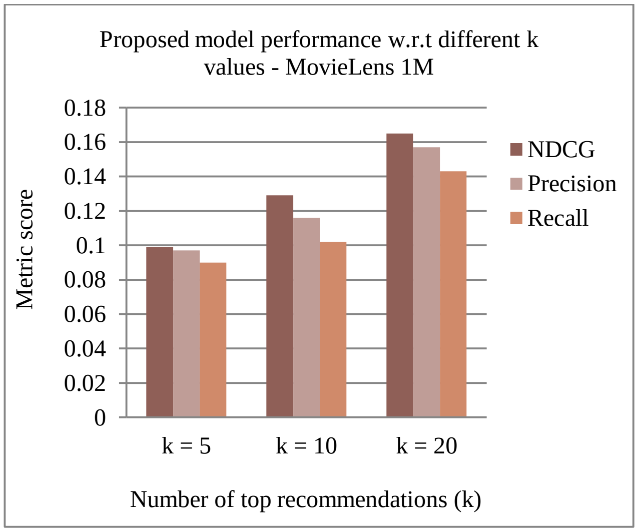

Fig. 4 Top k comparison of the proposed model for MovieLens 1M

A baseline comparison of the proposed federated neuro-fuzzy model is visualized in Figures 5 and 6. The comparison of both experimental datasets is given in Table 3 for k value 20 with three accuracy measures. FNN, FedRec-Dp and FedDeepFM are the three robust baseline models selected for this comparative study. Even though the baseline models perform well, the proposed study demonstrates the enhanced performance across top k (k=20), i.e. top 20 movie recommendations.

Table 3. Top k comparison of the proposed model on evaluation datasets

S. No	In this study	Dataset - MovieLens 100K			Dataset - MovieLens 1M		
		NDCG@k	Precision@ k	Recall@ k	NDCG@ k	Precision@ k	Recall@ k
1	k = 5	0.169	0.145	0.111	0.099	0.097	0.090
2	k = 10	0.182	0.169	0.130	0.129	0.116	0.102
3	k = 20	0.205	0.176	0.149	0.165	0.15	0.143

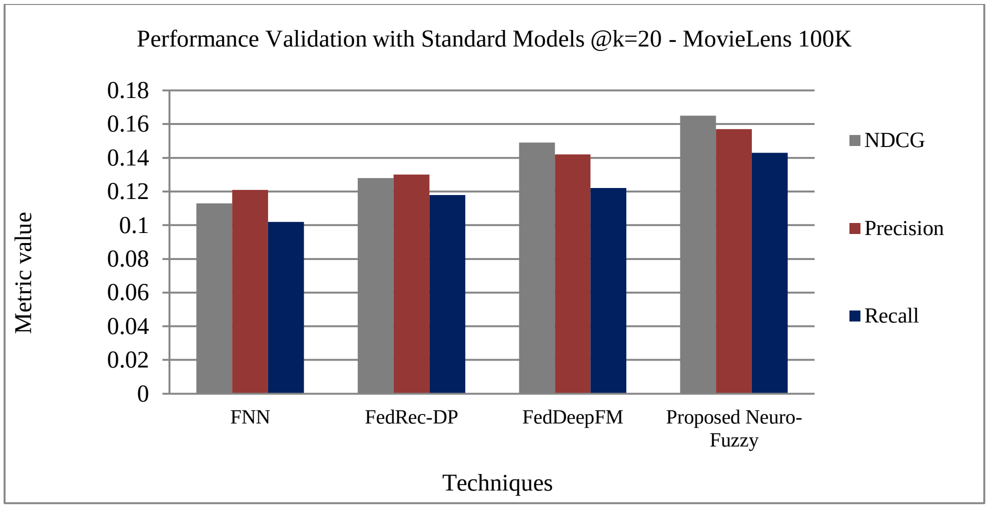

Fig. 5 Performance assessment of the studied model with baselines for MovieLens 100K

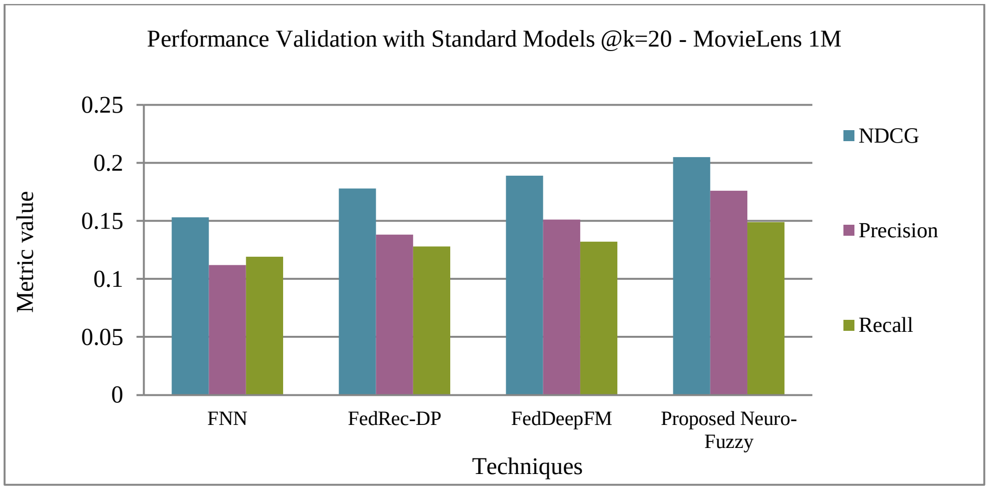

Fig. 6 Performance assessment of the studied model with baselines for MovieLens 100K

Table 4. Performance assessment of the studied approach with baselines on the evaluation dataset

S.No	Techniques	Dataset - MovieLens 100K			Dataset - MovieLens 1M		
		NDCG@k (k=20)	Precision@k (k=20)	Recall@k (k=20)	NDCG@k (k=20)	Precision@k (k=20)	Recall@k (k=20)
1	FNN	0.153	0.112	0.119	0.113	0.121	0.102
2	FedRec-DP	0.178	0.138	0.127	0.128	0.130	0.118

3	FedDeepFM	0.189	0.151	0.132	0.149	0.142	0.122
4	Proposed Neuro-fuzzy	0.205	0.176	0.149	0.165	0.157	0.143

Table 4 highlights the performance assessment of the proposed scheme with baselines on evaluation datasets. NDCG value obtained for the proposed model is 0.205 for 100K and 0.143 for 1M. Meanwhile, the FedDeepFM achieved 0.189 and 0.149. Among these three existing models, FedDeepFM achieved higher accuracy than the rest of the methods, yet not higher than the proposed model. A higher value in the NDCG indicates higher relevancy in the predicted top 20 movie recommendation list. Precision and recall values achieved for this study are also visibly higher than those of the conventional models. This represents that the prediction and recommendation of the studied model is more accurate and relevant than the existing approaches for the top 20 movie recommendation list.

To determine the capability of the proposed model, training and validation loss were monitored while training. Training loss reflects the suitability of the model to training data, whereas validation loss represents the model's overfitting issues, if any. Figures 7 and 8 are the graphical representations of training and validation loss of the studied mechanism on 100K and 1M datasets, respectively. The studied model achieved lower training and validation loss on both datasets; the training loss on the dataset decreased steadily over the 200 epochs, whereas the validation loss on the test set remained stable. This demonstrates the effective learning process and generalization of the model.

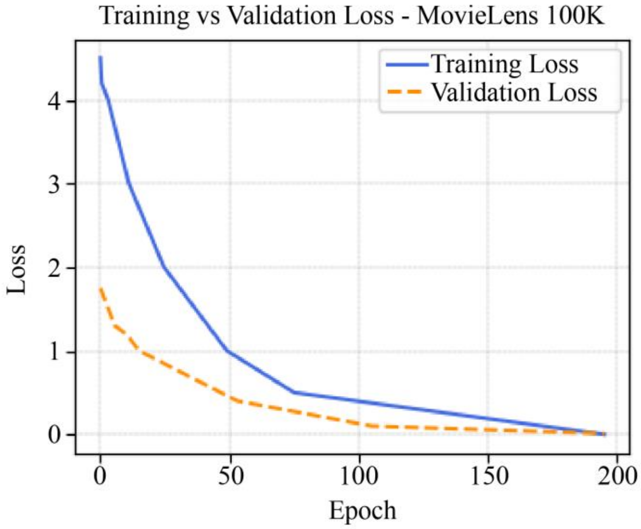

Fig. 7 Training vs. Validation loss on MovieLens 100K dataset

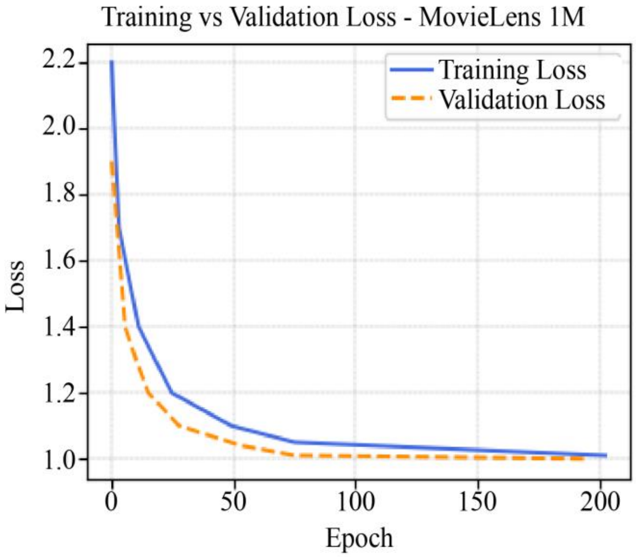

Fig. 8 Training vs. Validation loss on MovieLens 1M dataset

Table 5. Comparison of error metrics of the proposed model at various privacy budgets (ε) on evaluation datasets

S.No	Privacy Budget (ε)	Dataset - Movielens 100K				Dataset - Movielens 1M			
		MAE		RMSE		MAE		RMSE	
		DP	Proposed Neuro-fuzzy with LDP	DP	Proposed LDP	DP	Proposed Neuro-fuzzy with LDP	DP	Proposed LDP
1	0.5	2.549	1.721	2.414	1.351	2.152	1.620	1.946	1.012
2	1.0	2.382	1.257	2.102	0.712	1.921	1.391	1.731	0.897
3	1.5	2.199	1.104	1.844	0.657	1.597	0.249	1.428	0.721
4	2.0	1.824	0.772	1.630	0.470	1.249	0.187	1.223	0.585
5	2.5	1.632	0.485	1.542	0.323	0.809	0.116	1.118	0.359

Table 5 demonstrates the comparison of error metrics of the proposed federated neuro-fuzzy model with local differential privacy at various privacy budgets on the experimental datasets. Mean absolute error and root mean squared error are the error metrics considered for these measures, with privacy budget values $(\varepsilon) = 0.5$, $(\varepsilon) = 1$, $(\varepsilon) = 1.5$, $(\varepsilon) = 2$ and $(\varepsilon) = 2.5$. The table compares the neuro-fuzzy integrated with LDP and the differential privacy approach in terms of RMSE and MAE. Lower value in MAE and RMSE indicates the effectiveness of the model's prediction accuracy, i.e. utility. A higher value in the privacy budget indicates higher privacy and security. The proposed model achieved a lower MAE for the privacy budget (ε) = 2.5 for 100K dataset (MAE = 0.485) and for 1M dataset (MAE = 0.116). RMSE was achieved for the 100K dataset (RMSE = 0.323) and for the 1M dataset (RMSE = 0.359). This represented the model's robustness against privacy concerns without compromising its utility (prediction/recommendation accuracy). It is a critical task to balance both the utility and privacy concerns of the user at the same time. But the proposed model moderately balances them both to increase a better user experience.

6. Conclusion

This study proposes a novel federated neuro-fuzzy model with local differential privacy for a privacy-preserving federated recommender system. To combine the ambiguity and enhance the interpretability, a deep neural network is combined with the fuzzy system. Further, local differential privacy is incorporated to ensure user confidentiality and robustness of security.

Experimental evaluation on the real-world evaluation dataset demonstrated that the studied model achieves improved accuracy in terms of NDCG, precision and recall and provides enhanced security at multiple privacy budgets (ε) in terms of MAE and RMSE. The observed outcomes of the study on the MovieLens 100K dataset are NDCG = 0.205, precision = 0.176, recall = 0.149 and on MovieLen 1M dataset are NDCG = 0.165, precision = 0.157, recall = 0.143. On the other hand, privacy protection is achieved by the model, which is measured on the 100K dataset, with MAE = 0.485, RMSE = 0.323 and on the 1M dataset, MAE = 0.116, RMSE = 0.359 for the higher privacy budget (ε). Despite its promising performance, opportunities for improvement still exist in this study. Future work may involve heterogeneous data environments and increase the scalability of the experimental data. Hence, this study contributes a secure and user-convenient model for a privacy-aware federated recommender system in decentralized environments.

References

[1] Zehua Sun et al., "A Survey on Federated Recommendation Systems," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 36, no. 1, pp. 6-20, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Shivangi Gheewala, Shuxiang Xu, and Soonja Yeom, "In-Depth Survey: Deep Learning In Recommender Systems—Exploring Prediction and Ranking Models, Datasets, Feature Analysis, and Emerging Trends," *Neural Computing and Applications*, vol. 37, no. 17, pp. 10875-10947, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Yongjie Du et al., "Federated Matrix Factorization for Privacy-Preserving Recommender Systems," *Applied Soft Computing*, vol. 111, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Xinna Wang et al., "Federated Deep Recommendation System Based on Multi-View Feature Embedding," *IEEE 9th International Conference on Data Science and Advanced Analytics*, Shenzhen, China, pp. 1-9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Tribhuwan Kumar et al., "Fuzzy Logic and Machine Learning-Enabled Recommendation System to Predict Suitable Academic Program for Students," *Mathematical Problems in Engineering*, vol. 2022, no. 1, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Yasir Rafique et al., "An Enhanced Integrated Fuzzy Logic-Based Deep Learning Techniques (EIFL-DL) for the Recommendation System on Industrial Applications," *PeerJ Computer Science*, vol. 10, pp. 1-35, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Yue Wu et al., "FedDeepFM: A Factorization Machine-Based Neural Network for Recommendation in Federated Learning," *IEEE Access*, vol. 11, pp. 74182-74190, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Farzad Kaviani, "Recommender System in Social Networks Using Fuzzy Logic," *International Conference on Electrical, Computer, Communications and Mechatronics Engineering*, Tenerife, Canary Islands, Spain, pp. 1-7, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] R.V. Karthik, and Sannasi Ganapathy, "A Fuzzy Recommendation System for Predicting the Customers Interests Using Sentiment Analysis and Ontology in e-Commerce," *Applied Soft Computing*, vol. 108, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Weiqing Li et al., "A Federated Recommendation System Based on Local Differential Privacy Clustering," *Proceedings - 2021 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Internet of People, and Smart City Innovations, SmartWorld/ScalCom/UIC/ATC/IoP/SCI*, Atlanta, GA, USA, pp. 364-369, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Xiang Li et al., "LDPMF: Local Differential Privacy Enhanced Matrix Factorization for Advanced Recommendation," *Knowledge-Based Systems*, vol. 309, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Yongxin Deng et al., "FedSlate:A Federated Deep Reinforcement Learning Recommender System," *IEEE Transactions on Emerging Topics in Computational Intelligence*, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Zihang Xu, Chiawei Chu, and Shiyang Song, "An Effective Federated Recommendation Framework with Differential Privacy," *Electronics*, vol. 13, no. 8, pp. 1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Jakub Gorski et al., “Fuzzy-Logic-Based Recommendation System for Processing in Condition Monitoring,” *Sensors*, vol. 22, no. 10, pp. 1-32, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Amany Sami et al., “A Deep Learning Based Hybrid Recommendation Model for Internet Users,” *Scientific Reports*, vol. 14, no. 1, pp. 1-19, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Vito Walter Anelli et al., “FedeRank: User Controlled Feedback with Federated Recommender Systems,” *Lecture Notes in Computer Science*, vol. 12656, pp. 32-47, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Weiwei Wang, Wenping Ma, and Kun Yan, “FSPPCFs: A Privacy-Preserving Collaborative Filtering Recommendation Scheme Based on Fuzzy C-Means and Shapley Value,” *Complex and Intelligent Systems*, vol. 11, no. 1, pp. 1-18, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Chenyuan Feng et al., “Robust Privacy-Preserving Recommendation Systems Driven by Multimodal Federated Learning,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 36, no. 5, pp. 8896-8910, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] MovieLens 100K Dataset, GroupLens. [Online]. Available: https://grouplens.org/datasets/movielens/100k/

[20] MovieLens 1M Dataset, GroupLens. [Online]. Available: https://grouplens.org/datasets/movielens/1m/

[21] Stephan Bartl, Kevin Innerebner, and Elisabeth Lex, “Differentiable Fuzzy Neural Networks for Recommender Systems,” *Adjunct Proceedings of the 33rd ACM Conference on User Modeling, Adaptation and Personalization*, New York City USA, pp. 343-348, 2025. [CrossRef] [Google Scholar] [Publisher Link]