



Federated Contrastive Learning and Visual Transformers for Personal Recommendation

Asma Belhadi¹ · Youcef Djenouri^{2,3,4} · Fabio Augusto de Alcantara Andrade^{2,5} · Gautam Srivastava^{6,7,8}

Received: 24 October 2023 / Accepted: 10 April 2024
© The Author(s) 2024

Abstract

This paper introduces a novel solution for personal recommendation in consumer electronic applications. It addresses, on the one hand, the data confidentiality during the training, by exploring federated learning and trusted authority mechanisms. On the other hand, it deals with data quantity, and quality by exploring both transformers and consumer clustering. The process starts by clustering the consumers into similar clusters using contrastive learning and k-means algorithm. The local model of each consumer is trained on the local data. The local models of the consumers with the clustering information are then sent to the server, where integrity verification is performed by a trusted authority. Instead of traditional federated learning solutions, two kinds of aggregation are performed. The first one is the aggregation of all models of the consumers to derive the global model. The second one is the aggregation of the models of each cluster to derive a local model of similar consumers. Both models are sent to the consumers, where each consumer decides which appropriate model might be used for personal recommendation. Robust experiments have been carried out to demonstrate the applicability of the method using MovieLens-1M, and Amazon-book. The results reveal the superiority of the proposed method compared to the baseline methods, where it reaches an average accuracy of 0.27, against the other methods that do not exceed 0.25.

Keywords Personal recommendation · Federated learning · Contrastive learning · Transformers · Consumer electronics

Introduction

Electronics are designed for everyday use by individuals. These can include devices such as smartphones, laptops, televisions, cameras, headphones, and many other devices that people use daily [1, 2]. Consumer electronics have become an integral part of modern life, and their use is widespread across the world. They have revolutionized the way people communicate, work, and entertain themselves, providing new levels of convenience, connectivity, and entertainment [3–5]. As technology continues to advance, consumer electronics are becoming more sophisticated, powerful, and affordable. New devices are constantly being developed, offering new features and capabilities that make our lives easier and more enjoyable [6–8]. A personal recommendation in consumer electronics has attracted a lot of attention in the last decade [9, 10]. This recommendation is subjective and can be influenced by factors such as the user's needs, budget, and personal preferences. When someone makes a personal recommendation, they are sharing their personal experience with the product and how it has met their specific needs or preferences. This can be helpful for others who are considering purchasing

✉ Youcef Djenouri
youcef.djenouri@usn.no

Asma Belhadi
asma.belhadi@oslomet.no

Fabio Augusto de Alcantara Andrade
fabe@usn.no

Gautam Srivastava
srivastavag@brandonu.ca

- ¹ OsloMet University, Oslo, Norway
- ² University of South-Eastern Norway, Kongsberg, Norway
- ³ Norwegian Research Centre, Oslo, Norway
- ⁴ IDEAS NCBR, Warsaw, Poland
- ⁵ Norwegian Research Centre, Trømsø, Norway
- ⁶ Department of Math and Computer Science, Brandon University, Brandon, Canada
- ⁷ Research Centre for Interneural Computing, China Medical University, Taichung, Taiwan
- ⁸ Department of Computer Science and Math, Lebanese American University, Beirut, Lebanon

the same product and can provide valuable insights into the product's features, performance, and reliability.

Motivation

Solutions to personal recommendation in consumer electronics are divided into three categories:

1. **Collaborative filtering:** One of the most popular techniques for recommendation systems is collaborative filtering. Collaborative filtering uses the behavior of users to find similar users and recommends items that the similar users have liked in the past [11–14].
2. **Content-based filtering:** Another technique for recommendation systems is content-based filtering. Content-based filtering uses the features of items to find similar items and recommends items that have similar features to items the user has liked in the past [15–17].
3. **Hybrid approaches:** A hybrid approach combines collaborative filtering and content-based filtering to take advantage of the strengths of both approaches [18–20].

Even though these solutions provide high accuracy for non-complex data, they often require access to personal data such as browsing history, purchase history, and social network profiles. This raises privacy concerns and requires careful consideration of data protection regulations. Federated learning is a machine learning technique that allows multiple devices to collaboratively train a model without sharing their raw data with a central server [21, 22]. One possible direction to solve the aforementioned challenges of recommendation systems is to consider federated learning with a trust authority mechanism for improving the accuracy of recommendations while preserving user privacy. Another challenge of the existing solutions is the data quantity and quality. Indeed, these solutions are not able to efficiently learn from massive data. In order to tackle this challenge effectively, we delve into the realms of both clustering techniques and transformer models. By incorporating clustering into our approach, the recommendation system gains the capability to not only formulate a comprehensive global model encompassing all consumers but also to generate localized models tailored to specific clusters of similar consumers. This means that the system can discern nuanced patterns and preferences within different consumer segments, thereby enhancing the precision and relevance of its recommendations on a more granular level. In addition, and motivated by the success of transformers in training from massive data, this research work suggests the use of transformers for the recommendation system. The last challenge that we observe for the existing solutions in solving the personal recommendation problem is that they often face difficulty in capturing the fine-grained relationships between users and items, espe-

cially when dealing with sparse data. To address this issue, we propose a novel contrastive learning approach for feature embedding. Our method leverages the power of contrastive learning to learn meaningful representations of users and items in a shared embedding space. Thus, the contrastive learning framework ensures that user-item interactions are embedded in a way that positive pairs have higher similarities while negative pairs have lower similarities [23, 24]. This leads to a more compact and discriminative embedding space, where similar users and items are grouped, enhancing the recommendation performance. Contrastive learning leverages the abundance of negative samples to learn better embeddings, making it well-suited for handling sparse data scenarios in recommender systems.

Contributions

We suggest federated learning-based transformers for personal recommendations (FLT-PR), a smart hybrid approach that combines federated learning and transformers for use in personal recommendations. The following are the primary achievements of this research work:

1. We introduced a transformer-based approach to address personal recommendations in the consumer electronics domain. Initially, embedded features are extracted from the trained data. These derived features are subsequently inputted into transformers to facilitate the recommendation process. Additionally, we incorporate consumer clustering to develop localized models for groups of similar consumers, thereby enhancing the personalized nature of the recommendations.
2. We presented an innovative contrastive learning framework tailored specifically for feature embedding within recommender systems. This framework is designed to efficiently capture and represent intricate user-item interactions, ensuring a more comprehensive understanding of user preferences and item characteristics. By leveraging contrastive learning techniques, our approach aims to enhance the quality and relevance of recommendations by delving deeper into the dynamics of user-item relationships.
3. The approach is employed within the context of federated learning, where it serves to uphold the principle of a trusted authority. This principle plays a pivotal role in safeguarding the confidentiality and privacy of model data throughout the federated learning process. By adhering to the trusted authority framework, sensitive information remains protected, allowing for secure collaboration and model training across decentralized devices or entities.
4. We conducted thorough evaluations of FLT-PR using well-established recommendation system-based datasets.

Through these comprehensive tests, we demonstrate the effectiveness of our approach, showcasing its superiority over state-of-the-art algorithms in terms of both runtime efficiency and recommendation accuracy. Our results underscore the robustness and competitiveness of FLT-PR in addressing real-world recommendation challenges.

The rest of this work is structured as follows. The “[Personal Recommendation in Consumer Electronics](#)” section shows the basic concepts of the personal recommendation process in consumer electronics. Following a summary of the key relevant works for both the FL-based framework and traffic flow forecasting in the “[Related Work](#)” section, the “[FLT-PR: Federated Learning-Based Transformers for Personal Recommendation](#)” section provides specifics on the FLT-PR. After that, the “[Performance Evaluation](#)” section assesses our approach using extensive data. The research study’s conclusions and the future directions of FLT-PR are discussed in the “[Challenges and Future Directions](#)” section.

Personal Recommendation in Consumer Electronics

Personal recommendation in consumer electronics is made based on a user’s needs, preferences, and budget. There are several types of personal recommendations in consumer electronics, including:

1. **Expert Recommendations:** These recommendations are made by individuals who are considered experts in a particular field, such as technology, and are often sought after for their knowledge and experience.
2. **User Recommendations:** These recommendations are made by individuals who have personal experience using a particular product or device and can offer insights into its performance, features, and usability.
3. **Influencer Recommendations:** These recommendations are made by individuals who have a large following on social media platforms and are considered to be influencers in their respective niches. They may offer product reviews or endorsements, often in exchange for compensation or free products.

4. **Retailer Recommendations:** These recommendations are made by salespeople or customer service representatives working for a retailer, who are trained to offer advice and guidance to customers based on their needs and preferences.

The personal recommendation process in consumer electronics includes several steps as illustrated in Fig. 1, and described in the following:

1. **Identify Need:** The process begins when the consumer identifies a need or desire for a particular electronic product, such as a smartphone or laptop.
2. **Seek Recommendations:** The consumer then seeks out personal recommendations from various sources, such as experts, friends, family, online reviews, or influencers.
3. **Make Decision:** The consumer evaluates the recommendations based on factors such as the source’s credibility, expertise, and alignment with its need and preference. The consumer then decides on which product to purchase based on its preference.
4. **Provide Feedback:** After using the product for some time, the consumer may provide feedback to others in the form of a personal recommendation or product review, completing the cycle of personal recommendations in consumer electronics.

Related Work

Federated learning and personal recommendations are two major research areas that are connected. We will review the recent and pertinent works on both topics in the sections that follow.

Federated Learning

In the realm of industrial IoT, Fu et al. [25] proposed an innovative approach to address security concerns by introducing federated learning with evidence. Their method centers on verifying the accuracy of the cumulative gradients sent by a server, which is achieved through Lagrange interpolation. However, a potential issue arises with the possibility of the

Fig. 1 Personal recommendation process in consumer electronics



server producing counterfeit aggregation results. To counter this challenge, the authors put forward a solution involving a trustworthy public key generator, which distributes keys following the initialization of the model. Subsequently, each user takes the following steps: first, they locally train their model and then transmit their encrypted gradients to the server. This encryption step is vital to safeguarding privacy, as it ensures that the gradient remains confidential during transmission. The server, in turn, performs accumulation on this encrypted data. Importantly, this process eliminates the need for key exchange between participants, rendering collision attacks unfeasible. Upon receiving the collected ciphertexts from the server, each participating member verifies the integrity of the results before commencing the encryption process. This approach substantially reduces the effectiveness of deciphering counterfeit gradients. When compared to other state-of-the-art techniques, the authors' solution exhibits a lower vulnerability to potential assaults seeking to access private differentials. Furthermore, the introduced encryption only moderately impacts accuracy in contrast to a federated learning approach without gradient encryption. Lastly, it's worth noting that this method minimizes overhead costs related to encryption/decryption, verification, communication, and overall operational overhead. The verification overhead remains constant, regardless of the number of participants involved. In the context of fog computing, Zhou et al. [26] have introduced a federated security learning approach. Under this paradigm, each fog node is empowered to carry out learning tasks and gather data from IoT devices. This approach significantly enhances the efficiency of low-level training. To ensure the security of IoT device data and shield the model from a parameter server that may be trustworthy but overly inquisitive, the authors have implemented sophisticated encryption techniques. Specifically, when applied to an individual fog node, this innovative method effectively thwarts the server's attempts to deduce training set details from hyperparameters. Furthermore, it enables resistance against collusion attacks and safeguards the privacy of the mathematical model, even in situations where adversarial fog nodes or untrustworthy variables collaborate with other nodes. To mitigate vulnerabilities related to data and content disclosure during the training process, Yin et al. [27] have proposed a hybrid privacy-protection approach. Their methodology addresses these issues at multiple levels. First, during the weighted summing process, both the gradient weights of each participant and the characteristics of the information they provide are safeguarded using advanced function encryption techniques. Furthermore, they introduce a local quantification method to account for privacy loss due to Bayesian variability. This approach allows users to adjust their privacy budget in response to the data distributions within the datasets. Notably, Bayesian differential privacy outperforms the traditional differential privacy

framework, leading to improved service quality. Lastly, to enhance performance, a sparse distinction matrix is incorporated into the function encryption. This optimization ensures that each training cycle only necessitates modifications to incremental values similar to previous gradients, minimizing the server's computational load while significantly impacting the data transfer and storage capacities on the client side. Experimental results indicate that the use of sparse variance gradient techniques leads to improved model accuracy compared to traditional differential privacy measures.

Personal Recommendation

Personalized recommendations aim to alleviate the impact of data overload by minimizing ambiguity and the delivery of unwanted information to consumers. Traditional recommendation systems fall into three categories: content-based, collaborative, and a blend of both approaches. In the context of the Massive Open Online Course (MOOC) system, a personalized recommendation framework was developed by integrating deep learning and big data technologies, as proposed by Li et al. [28] in their work. This approach introduces several pertinent strategies leveraging the BERT network to enhance the precision of the recommendation system. Firstly, it outlines the acquisition and preprocessing of open datasets. Secondly, it establishes the groundwork for a recommendation model by employing the BERT model and incorporating a self-attention mechanism. To bolster the model's recommendation efficacy, a domain feature difference learning technique is implemented to extract profound network insights from the course content. In order to assess users' attitudes towards connected products, ascertaining whether they hold a positive, negative, or neutral viewpoint, Solairaj and their team conducted a comprehensive analysis of user opinions, beliefs, and sentiments, as documented in their study [29]. This proactive approach enables businesses to adapt and tailor their products to meet customer satisfaction. Many of the existing sentiment analysis methods suffer from inaccuracies and time-consuming processes. As a solution to these challenges, the authors developed EESNN-SA-OPR. In this framework, novel recommendation algorithms were applied, incorporating both Filtering Collaborative (FC) and product-to-product (P-P) similarity techniques. Collaborative filtering aims to "predict the best shops," while product-to-product similarity focuses on forecasting the best products. In a distinct research context, Swaminathan and colleagues, as documented in their study [30], advocate the utilization of collaborative filtering techniques for determining the optimal quantity of fertilizers required to promote sustainable crop development. Addressing the issue of imbalanced data concerning the unknown fertilizer quantities, they suggest incorporating auxiliary parameters such as soil fertilizer levels, land area,

and soil chemical characteristics. Of note, their work introduced an innovative wide matrix factorization technique that derived feature representations by linearly mapping integrated contextual information vectors. To comprehensively comprehend historical fertilizer recommendations for the land, they employed a fully connected multi-layer perceptron, preserving non-linear higher-order interactions among contextual information. In a related vein, the creation of the Knowledge Augmented User Representation (KAUR) network, as presented in the study by Ma et al. [31], is aimed at exploring contrastive learning within collaborative knowledge graphs. This approach enables the discovery of semantic neighbors and the derivation of ambiguous interest sets from such knowledge graphs. The KAUR network leverages a graph neural network to learn the representation of each node in the collaborative knowledge graph. It treats information from nodes and their propagated neighbors as positive contrastive pairs, enhancing node representations through contrastive learning. Users or items with similar profiles are identified as semantic neighbors and included as positive pairs for further exploration of user interests. This user representation is then amalgamated with fuzzy interest sets, enhancing interpretability. In their research, Walek et al. proposed a hybrid recommender system known as the Eshop recommender, as detailed in their study [18]. This innovative system combined a fuzzy expert system with a recommender module comprising three subsystems, each utilizing collaborative filtering and content-based techniques. It serves as an e-commerce recommendation system designed to provide well-suited product recommendations to users. The fuzzy expert system played a pivotal role in generating the list of recommended products. It took into account a wide array of user preferences and their online store behavior. The expert system considered various variables, including the similarity to previously rated products, the coefficient associated with purchased products, and the average product ratings, in order to compile the recommended product list.

Discussion

Certain major faults exist in the current recommendation systems, where they lack an accurate model from embedding to model training. Moreover, there is a lack of data privacy and model security. Particularly, the model data is distributed less securely and privately throughout the various entities of the recommendation platform. Table 1 offers the most recent research on recommendation systems and federated learning. In this research, we present an end-to-end architecture for a personal recommendation that integrates federated learning with the current transformers to overcome the aforementioned problems. We will show how our solution gives customers more precise product recommendations.

FLT-PR: Federated Learning-Based Transformers for Personal Recommendation

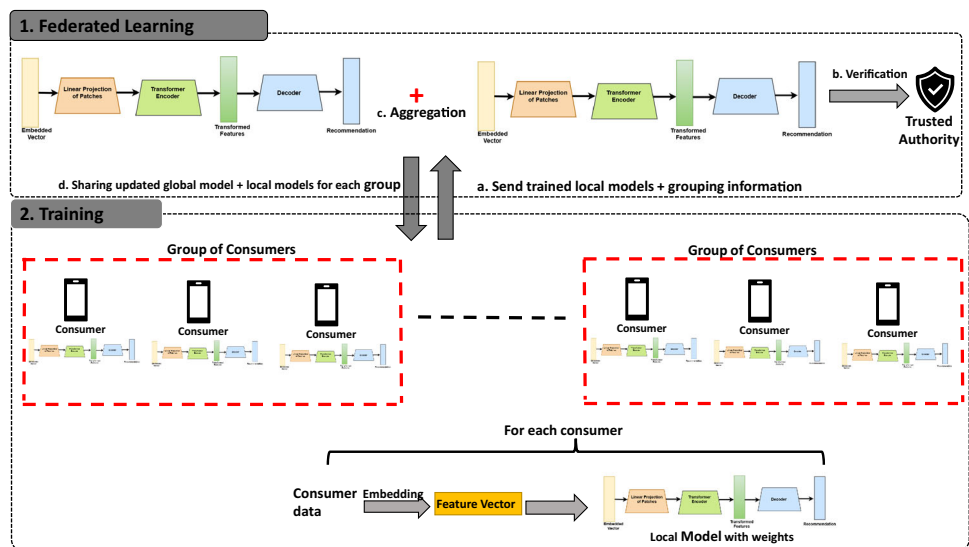
Principle

Figure 2 sketches the FTL-PR solution. It starts with consumer clustering, where the consumers that share similar features are merged into one group. Training is performed for each consumer, where the pre-trained model is used to train its proper data. This step includes embedding, which aims to map the consumer data to the feature vector. Additionally, it makes use of transformers to recommend items. By including the trusted authority principle, we create a federated learning framework for protecting model data during the federated learning stage. In this context, we define three types of models (local model for each consumer, local model for each group of consumers, and global model for all consumers). In the remainder of this section, we will go over each component of the FTL-PR approach in detail.

Table 1 Recent literature of federated learning, and personal recommendation systems

Category	Work	Limits
Federated Learning	Fu et al. [25]	Test the solution on a simple MNIST data.
	Zhou et al. [26]	Requires high time computing during the encryption phase.
	Yin et al. [27]	
Personal Recommendation	Li et al. [28]	Need to share data for multiple user recommendation.
	Solairaj et al. [29]	
	Swaminathan et al. [30]	Lack of advanced deep learning models in the training.
	Ma et al. [31]	
	Walek and Fajmon [18]	

Fig. 2 FTL-PR: Training is performed for each consumer, where the pre-trained model is used to train its proper data. By including the trusted authority principle, we create a federated learning framework for protecting model data during the federated learning stage



Contrastive Learning for Feature Embedding

This phase aims to embed the categorical attributes of the consumers to feature vectors to facilitate the training of our transformer. We also consider these feature vector to cluster the consumers into disjoint clusters, each of which contains similar consumers. For embedding, we consider embedding with contrastive learning [32]. Contrastive learning is an unsupervised learning technique that encourages similar instances to be close to each other in the embedding space while pushing dissimilar instances apart. In the context of recommender systems, we adapt this framework to create meaningful user and item embeddings.

Embedding Function Let:

- X is the set of all user-item interactions in the recommender system.
- U be the set of users, and I be the set of items.
- E be the embedding space with dimension d .
- $f_{\theta} : U \cup I \rightarrow E$ be the function that maps users and items to their corresponding embeddings in the space E , parameterized by $\theta \in \mathbb{R}^d$.

The goal of the embedding function is to project users and items into a common embedding space, where their interactions are better captured and represented. For example, we can represent each user u and item i as a low-dimensional vector in the embedding space, such as $f_{\theta}(u) \in \mathbb{R}^d$ and $f_{\theta}(i) \in \mathbb{R}^d$.

Similarity Function To measure the similarity between user and item embeddings, in addition to cosine similarity, we can introduce the “Angular Similarity” which takes into account

the angular distance between embeddings. The Angular Similarity “ \mathcal{AS} ” is defined as:

$$\mathcal{AS}(x, y) = \frac{\cos^{-1}(\text{cosine_similarity}(x, y))}{\pi} \tag{1}$$

\mathcal{AS} ranges from 0 to 1, where 0 indicates that the vectors are perfectly aligned (maximum similarity), and 1 indicates they are opposite (minimum similarity).

Angular Contrastive Loss

To leverage the Angular Similarity for contrastive learning, we propose the “Angular Contrastive Loss” that aims to maximize the angular similarity between positive pairs and minimize it between negative pairs.

Given a batch of anchor instances A , their corresponding positive instances P , and negative instances N , the Angular Contrastive Loss is defined as:

$$\mathcal{L} = -\frac{1}{|A|} \sum_{a \in A} \log \frac{\exp(\mathcal{AS}(a, P))}{\exp(\mathcal{AS}(a, P)) + \sum_{n \in N} \exp(\mathcal{AS}(a, n))} \tag{2}$$

The Angular Contrastive Loss encourages the embeddings of positive pairs to have lower angular distances (higher angular similarity) and embeddings of negative pairs to have higher angular distances (lower angular similarity). The Angular Contrastive Loss takes into account the angular distance between embeddings, which provides a more principled way of measuring similarity than the traditional cosine similarity. By maximizing the angular similarity for positive pairs, we ensure that similar user-item interactions are projected closer together in the embedding space. On the other hand, by minimizing the angular similarity for negative pairs,

we push dissimilar user-item interactions apart, making the embedding space more discriminative. Angular Contrastive Loss has the advantage of being more robust to variations in magnitude between embeddings, as it focuses on the relative angles between them. This property makes it well-suited for capturing fine-grained relationships in recommender systems, especially when dealing with sparse data.

Training

The goal of this step is to train the model on each network consumer. The k -means algorithm is first used to cluster the customers based on the extracted feature vectors. We then use Transformer to extract the recommendation from the feature vectors of the consumers. A detailed explanation is given in the following:

1. **Consumer clustering** — For clustering, we use the k -means algorithm with an Euclidean distance to measure the similarity between two different consumers. k -means is straightforward to implement and computationally efficient, making it suitable for clustering large consumer datasets commonly found in recommendation systems. Its simplicity enables quick experimentation and iteration, crucial for fine-tuning recommendation algorithms. Let $C = \{c_1, c_2, \dots, c_n\}$ be the set of n consumers, where each consumer c_i is represented as a d -dimensional vector:

$$c_i = (c_{i,1}, c_{i,2}, \dots, c_{i,d}) \in \mathbb{R}^d$$

Let K be the number of clusters we want to create. In the following, we will give the main insights of our consumer clustering algorithm:

- (a) **Initialization:** Randomly initialize K cluster centroids: g_1, g_2, \dots, g_K , where each centroid g_j is a d -dimensional vector:

$$g_j = (g_{j,1}, g_{j,2}, \dots, g_{j,d}) \in \mathbb{R}^d$$

- (b) **Assignment:** For each consumer c_i , calculate the Euclidean distance to each centroid g_j and assign c_i to the nearest centroid:

$$S(c_i) = \arg \min_{g_j \in G} \text{distance}(c_i, g_j)$$

where the Euclidean distance between c_i and g_j is given by:

$$\text{distance}(c_i, g_j) = \|c_i - g_j\|_2 = \sqrt{\sum_{k=1}^d (c_{i,k} - g_{j,k})^2}$$

- (c) **Update Centroids:** For each cluster $j = 1, 2, \dots, K$, update the centroid g_j as the mean of all consumers assigned to that cluster:

$$g_j = \frac{1}{|S^{-1}(g_j)|} \sum_{c_i \in S^{-1}(g_j)} x_i$$

- (d) **Convergence Check:** Repeat steps 2 and 3 until convergence, i.e., until the cluster assignments do not change significantly, or a maximum number of iterations is reached.

2. **Local training** — In this phase, we harness the capabilities of a transformer for our recommendation system. The transformer stands out as a neural network architecture that excels in capturing extensive dependencies within consumer data. Its noteworthy feature is the self-attention mechanism, empowering the model to focus on distinct segments of the input sequence when generating recommendations. Subsequently, we introduce our customized adaptation of the transformer to analyze the feature vectors extracted in the preceding phase:

- (a) **Patch Embeddings:** Initially, the input features are segmented into discrete, non-overlapping patches. Each patch \mathbf{X}_i of size $N \times N$ is transformed into a vector representation \mathbf{E}_i via a linear projection:

$$\mathbf{E}_i = \mathbf{X}_i \mathbf{W}_e + \mathbf{b}_e$$

where \mathbf{W}_e is the weight matrix and \mathbf{b}_e is the bias vector. These patch embeddings serve as input sequences for the transformer encoder.

- (b) **Encoder:** The transformer encoder consists of L identical layers, each equipped with multi-head attention and feedforward neural networks. The multi-head attention mechanism computes attention scores between each pair of input patches \mathbf{E}_i and \mathbf{E}_j , allowing the model to focus on various regions within the input patches simultaneously. The attention mechanism can be mathematically expressed as:

$$\text{Attention}(\mathbf{Q}, \mathbf{K}, \mathbf{V}) = \text{softmax} \left(\frac{\mathbf{Q}\mathbf{K}^T}{\sqrt{d_k}} \right) \mathbf{V}$$

where \mathbf{Q} , \mathbf{K} , and \mathbf{V} are the query, key, and value matrices, respectively, and d_k is the dimensionality of the key vectors.

- (c) **Positional Encoding:** Since transformers lack recurrent connections, preserving positional information is crucial. Positional encodings are added to the patch embeddings \mathbf{E}_i to incorporate positional information into the input sequence. The positional encoding can be computed using sine and cosine functions:

$$PE_{(pos,2i)} = \sin\left(\frac{pos}{10000^{2i/d_{model}}}\right)$$

$$PE_{(pos,2i+1)} = \cos\left(\frac{pos}{10000^{2i/d_{model}}}\right)$$

where pos is the position and i is the dimension.

- (d) **Output Head:** At the end of the encoder, an output head is integrated to transform the final hidden states into the model's output. This transformation is performed using a fully connected layer with a softmax activation function:

$$\text{Output} = \text{softmax}(\mathbf{HW}_o + \mathbf{b}_o)$$

where \mathbf{H} is the final hidden state, \mathbf{W}_o is the weight matrix, and \mathbf{b}_o is the bias vector.

- (e) **Local Recommendation Process:** After obtaining the output from the transformer encoder, the recommendation process begins. This output represents the features extracted from the input data and encoded by the transformer. A recommendation can be generated by computing the similarity between the extracted features of a given user and the features of each item in the dataset. This similarity can be calculated using cosine similarity, Euclidean distance, or other similarity metrics. The items with the highest similarity scores to the user's features are then recommended to the user. Additionally, the recommendation process can be enhanced by incorporating user preferences, feedback, and contextual information to personalize the recommendations further. This iterative process of feature extraction and recommendation generation enables the local model of each user to provide accurate and relevant recommendations based on its preferences and the characteristics of the items in the dataset.

Federated Learning

Three ongoing problems with the federated training process are addressed in this step. One is the validity check of the parameters that each consumer posts to the server. The server's validity verification of aggregated results is the next issue that needs to be addressed. Furthermore, to safeguard the rights and interests of the consumers, we will offer a plan for assuring the consistency of cumulative results attained by various consumers.

- **a. Sending trained local models** — The system initialization involves the establishment of public parameters, key generation, and data exchange among different system roles. The trusted authority takes charge of generating various codes essential for the transmission and

verification of model data. Consequently, the server receives the local models that consumers have individually trained, encompassing the models' architectures, weights, and the IDs of consumers within each cluster. These elements are homomorphically encrypted prior to transmission.

- **b. Checking model integrity** — In our designed federated learning system, the trusted authority plays a crucial role in maintaining the integrity and security of the recommendation process. Acting as the guardian of trust, this authority oversees the preservation, signing, and issuance of digital certificates. These certificates serve as a testament to the authenticity of each locally uploaded model to the central server. Furthermore, the trusted authority ensures the accuracy of these models through rigorous verification processes, thereby upholding the reliability and effectiveness of the designed federated learning system.
- **c. Model aggregation** — Two types of aggregation are used. The first one is the aggregation of the local model of each cluster of consumers $W^{(local)}_{C_j}$. The second one is the aggregation of all models to find the global model $W^{(global)}$. The detailed formulas are given as follows:

$$W^{(local)}_{C_j} = \sum_{u_i} \frac{|d_i|}{|\sum_{D^{C_j}} d_i|} W_i^{(local)} \quad (3)$$

and,

$$W^{(global)} = \sum_{u_i} \frac{|d_i|}{|\sum_{D} d_i|} W_i^{(local)} \quad (4)$$

where C_j is the j^{th} cluster of consumers. $\mathcal{U} = \{u_1, u_2 \dots u_k\}$ is the set of k users. $D = \{d_1, d_2 \dots d_k\}$ is the set of k datasets of traffic flow, one for each user in \mathcal{U} . $W_i^{(local)}$ is the weights of the local model of the consumer u_i .

- **d. Sharing updated global model** — Subsequently, the server transmits the aggregated results to all consumers. When consumers are influenced by similar individuals, such as friends, the aggregated local model for each cluster is employed for recommendations. In other cases, the aggregated global model is used.

It is worth noting that verification takes place during both the uploading and aggregation phases. For backup and recovery validation, we employ one-way hash mechanisms, along with a stratified random sampling technique that generates a unique random number on each iteration. These two stages can be iterated to enhance the model further. Upon receiving the newly generated weight parameters for the encrypted global model, each user in the system proceeds to conduct

local retraining using the designed transformer. The updated model can then be forwarded to the cloud server, and this process can be repeated as needed.

Performance Evaluation

Experimental Settings

We used the two following widely known recommendation system datasets for evaluation:

1. **MovieLens-1M**¹: The dataset comprising recommended movies encompasses a vast array of information, totaling approximately 1 million explicit ratings ranging from 1 to 5. These ratings have been provided by a diverse pool of 6041 consumers, offering a comprehensive perspective on their preferences and opinions. The dataset covers a wide spectrum of cinematic choices, incorporating feedback on 3707 distinct movies. This rich and expansive dataset provides a robust foundation for comprehensive analysis and the development of sophisticated recommendation systems tailored to the diverse tastes and preferences of the audience.
2. **Amazon-book**²: It is a widely utilized resource renowned for its extensive collection of metadata and consumer ratings pertaining to various books. Within this dataset, each book is accompanied by detailed information such as its description, category classifications, pricing details, and brand attributes. This comprehensive array of data offers valuable insights into the characteristics and qualities of each book, enabling in-depth analysis and exploration of consumer preferences, trends, and behaviors.

We contrast our suggested recommendation model with the following current state-of-the-art-based models to show its efficacy:

1. **KGAT** [33]: It is a model that combines graph learning, and knowledge graphs. To identify the significance of neighbor nodes throughout the propagation process, KGAT employs an attention mechanism. Then, it dynamically propagates embeddings from nearby nodes to update node representations.
2. **KAUR** [31]: The collaborative knowledge graph is represented by each consumer using a graph neural network, which views the information of consumers and the information of their propagating neighbors as positive contrastive pairs. The consumer representations are then improved using contrastive learning.

¹ <https://grouplens.org/datasets/movielens/>

² <https://www.cp.jku.at/datasets/LFM-1b/>

3. **RippleNe** [34]: This technique, which may automatically disseminate consumer preferences and investigate consumers' hierarchical interests in the knowledge graph, is comparable to memory network propagation.
4. **CFKG** [35]: It combines consumer behavior and item information into a single structure and suggests realistic predictions that have been turned into triples, which may then be used to explore paths in the feature embedding space to generate explanations about the recommended items.
5. **MKR** [35]: It is a framework for multi-task learning that helps recommendation by using feature embedding. It can transfer knowledge between tasks and automatically learn significantly greater interactions between item and consumer features.

We employ Recall@K and NDCG@K, two frequently used metrics, with $K = [10, 20, 50]$, to assess the efficacy of top-k recommendation and preference ranking (Table 2). A measure of the percentage of related things among all items is called recall@K. To explain the position of hits, the ranking quality NDCG@K (also called Normalized Discounted Cumulative Gain) gives higher scores to top-ranked hits.

Feature Embedding Comparison

To train our personalized recommendation model with contrastive learning, we sample positive and negative items for each user from the set of user-item interactions X . The number of negative samples per user, K , is an important hyperparameter that affects the model's performance. We then optimize the parameters θ of the embedding function f_θ to minimize the contrastive loss $\mathcal{L}_{\text{contrastive}}$ using stochastic gradient descent or other optimization algorithms. During training, the model learns to map similar user-item pairs close together in the embedding space while pushing dissimilar pairs apart. After training, the model can make recommendations by computing the similarity between a user's embedding and item embeddings to rank potential recommendations. We compare our feature embedding with dense embedding [36]. It is a mathematical representation of a consumer in a high-dimensional space, created using a dense embedding layer. The embedding captures important features and characteristics of the consumer, such as its genre, popularity, and historical interactions. A dense embedding is considered "dense" because it maps a consumer to a continuous vector space, where each element in the vector has a meaningful value, as opposed to a sparse representation where most elements are zero. This enables our clustering algorithm, and transformer to capture complex relationships between consumers that may be difficult to represent using simple features. Figure 3 presents T-SNE visualizations of both dense embeddings and embeddings generated using contrastive

Table 2 Performance of FLT-PR and state-of-the-art solutions in terms of Recall@K and NDCG@K

Dataset	Metrics	KGAT	KAUR	RippleNet	CFKG	MKR	FLT-PR
MovieLens-1M	Recall@10	0.17	0.18	0.12	0.16	0.14	0.19
	NDCG@10	0.27	0.28	0.20	0.25	0.22	0.32
	Recall@20	0.25	0.27	0.21	0.25	0.22	0.26
	NDCG@20	0.29	0.28	0.21	0.24	0.25	0.28
	Recall@50	0.43	0.42	0.35	0.40	0.40	0.46
	NDCG@50	0.32	0.31	0.24	0.31	0.27	0.35
Amazon-book	Recall@10	0.19	0.17	0.07	0.13	0.10	0.18
	NDCG@10	0.08	0.11	0.06	0.09	0.06	0.10
	Recall@20	0.20	0.25	0.12	0.18	0.17	0.29
	NDCG@20	0.10	0.15	0.07	0.11	0.09	0.19
	Recall@50	0.30	0.38	0.24	0.33	0.29	0.42
	NDCG@50	0.12	0.17	0.11	0.14	0.12	0.21
average	–	0.22	0.25	0.17	0.22	0.19	0.27

The bold value are best values observed in the running experiments

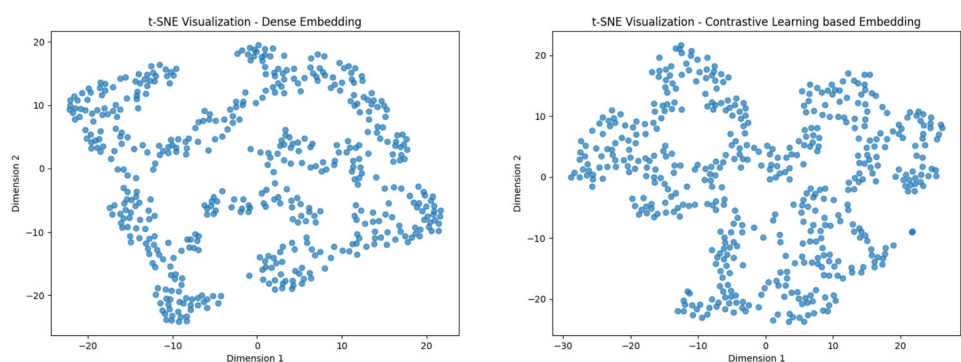
learning. In the dense embedding, the features obtained are dispersed widely across the 2D space without any discernible patterns or groupings. Consequently, T-SNE struggles to identify natural clusters or groupings of data points. Moreover, there is no clear separation between different clusters because this approach distributes points across the entire space without considering any underlying relationships. This results in high uncertainty or entropy in the feature space, where entropy refers to the level of disorder or unpredictability in the data distribution. In this scenario, the high entropy indicates that T-SNE fails to find any meaningful structure or patterns, leading to a lack of information about the underlying organization of the data. Additionally, the absence of structure and clear patterns makes it challenging to differentiate any signal from noise. Random noise in the features may dominate the visualization, making it difficult to interpret or draw meaningful conclusions. In contrast, the contrastive learning-based embedding generates features in a more organized manner, resulting in distinct clusters in the 2D space. The T-SNE algorithm successfully identifies similar features and groups them into clusters. Furthermore, different clusters

are well-separated, indicating that T-SNE captures the underlying similarities and differences between groups of features effectively. Our embedding exhibits low entropy, suggesting a more organized and structured representation. The T-SNE algorithm can unveil the inherent organization in the features, providing a clearer view of the feature's patterns and relationships. The clusters and separation in our embedding are meaningful representations of the features. Features within the same cluster are more similar to each other, while features in different clusters are more dissimilar. This enables better interpretation and analysis of the features.

Accuracy and Federated Learning Performance

To rigorously validate the performance of FLT-PR in terms of accuracy, we conducted robust experiments. We varied the top k recommendations retrieved from a set of values, namely {10, 20, 50}, and computed recall and NDCG values for two datasets, MovieLens-1M and Amazon-book. Our simulation accounts for the maximum accuracy of both the global model, applicable to all consumers, and the local

Fig. 3 Contrastive learning-based embedding vs. dense embedding



model within the respective consumer cluster. The results unequivocally demonstrated the superiority of FLT-PR when compared to baseline personal recommendation solutions. In fact, our solution outperformed other alternatives in eight out of twelve cases. Specifically, KAUR and KGAT achieved the best results in two cases each. Moreover, the average accuracy of our solution surpassed that of other solutions, including KAUR and KGAT. FLT-PR boasted an average accuracy of 0.27, while the other solutions failed to attain an average accuracy of 0.25. These achievements can be attributed to the fact that our solution capitalizes on both the global model, encompassing all consumers, and the local models within their respective clusters. Furthermore, the incorporation of the self-attention mechanism from transformer networks, which has demonstrated remarkable success in various applications, including natural language processing, also contributes to these commendable results. We can also explain the promising results of the competitive solutions (KAUR, and KGAT) in some cases by the fact that these solutions consider the knowledge graph in recommending the relevant items to the consumers. However, it is not always straightforward to design a knowledge graph in a real-world scenario. To evaluate the federated learning strategy used in this research work, we measure the stability metrics produced by trust value and information transmission success rate. Because hostile consumers may offer perturbation in terms of recommendation updates, we assign each consumer a trustworthiness score between 0 and 1. High-trust consumers are close to 1, whereas low-trust consumers are near 0. To withstand data manipulation and replay threats, the federated learning system built in this research effort is compared to FLT [37]. With a rigorous evaluation of the trust value of nodes, we can observe that the authority trust-based model employed in this research will lead to this tremendous achievement. Additionally, Figs. 4 and 5 show that their disruptive behaviors — which mainly consist of flooding attacks — are caused by repeatedly adding hostile consumers. The proposed hierarchical confidence model in this paper examines the overall stability of node trust value and is based on federated learning and trusted authority. The fundamen-

tal rationale is that the patterned trust scheme ensures that genuine models among the set of consumers receive reliable information even when adversaries are present. Consumers would consume more energy as a result of the flooding attack, and by analyzing edge energy consumption models, we might rapidly spot malicious consumers. The edge paradigm, which can decrease the energy use of the server, is the second concept we implement.

Challenges and Future Directions

Addressing the challenges and exploring future directions for using transformers and contrastive learning in a federated learning environment require a comprehensive and multidisciplinary approach. Researchers need to develop privacy-preserving communication protocols, enhance the adaptability of models to handle diverse data, promote fairness and explainability, and strike the right balance between exploration and exploitation in personalized recommendations. Solving the following challenges will lead to more robust and efficient personalized recommendation systems in the federated setting, benefiting users while safeguarding their privacy:

1. **Data Privacy and Security:** Data privacy is a critical concern in federated learning since the data remains on local devices, reducing the risk of centralized data exposure. However, the use of transformers and contrastive learning can potentially lead to privacy breaches. Transformers, especially large models like BERT and GPT, have a high capacity to memorize specific data samples during training [38]. If these sensitive details are incorporated into the model, they may be leaked through the model updates during federated learning. Differential Privacy offers a solution by adding carefully calibrated noise to the model updates before aggregation, ensuring that individual data points remain indistinguishable [39]. Secure Multi-Party Computation allows computations to be performed collaboratively across different devices

Fig. 4 Stability of trust evaluation of FTL-PR, and FLT framework with the MovieLens-1M data

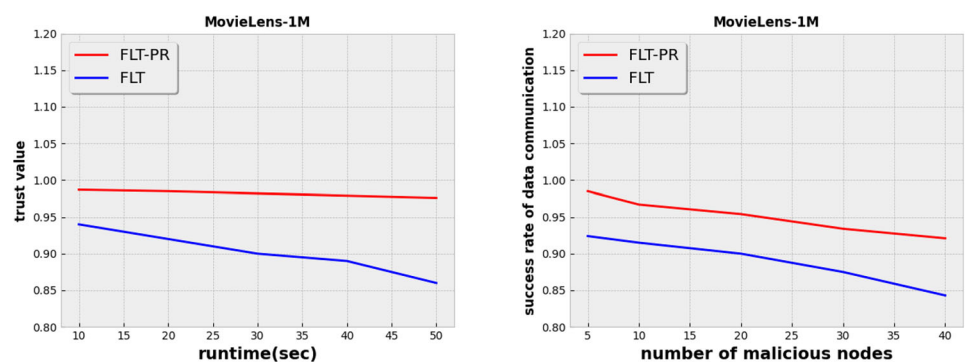
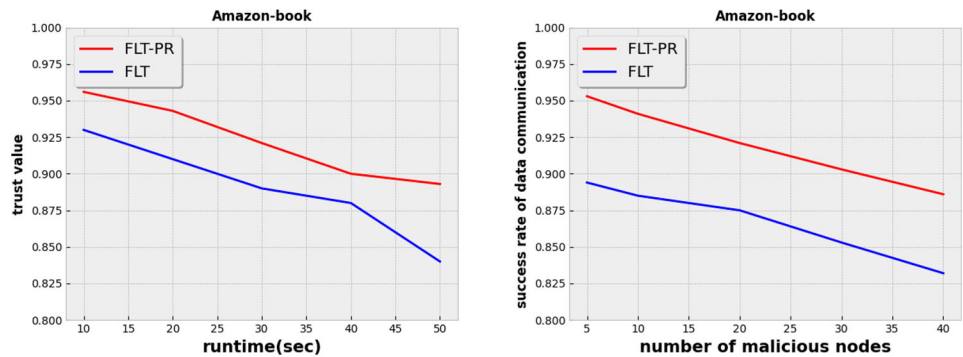


Fig. 5 Stability of trust evaluation of FTL-PR, and FLT framework with the Amazon-book data



without revealing raw data to other parties [40]. Federated Transfer Learning is another approach where pre-trained models are shared, and fine-tuning occurs locally with minimal data exposure [41].

2. **Communication Overhead:** Transformers have a large number of parameters, leading to substantial communication overhead when exchanging updates in a federated learning setting. This communication cost can impact the efficiency of the learning process, particularly in scenarios where communication is slow or resource-constrained. Model Compression techniques can be applied to reduce the model size without sacrificing performance significantly [42]. Knowledge distillation involves training a smaller model to mimic the behavior of a larger model, effectively transferring knowledge and reducing the number of parameters [43]. Quantization methods represent model parameters using a smaller number of bits, resulting in more efficient communication. Local training allows devices to perform multiple iterations of training on their local data before communicating with the central server, reducing the frequency of communication. Prioritizing communication based on the relevance of user data can ensure that updates from devices with more impactful data are transmitted more frequently.
3. **Heterogeneity of Data:** In federated learning, devices or servers may have data with different distributions, quality, and scale, making it challenging to train a consistent global model. Transformers and contrastive learning methods may struggle to generalize well in such a heterogeneous environment. Domain Adaptation techniques can be employed to adapt the model to different data domains, minimizing the discrepancies between them. Hybrid Models combine local and global modeling, leveraging both general patterns learned from the global model and user-specific preferences captured locally [44]. Personalized ensemble methods aggregate multiple personalized models, allowing the system to adapt to different user segments effectively [45].
4. **Cold Start Problem:** The cold start problem is a significant challenge in federated learning when new devices or users join the network with limited historical data. Transformers typically require substantial data to learn meaningful representations, which can hinder the personalization of new users. Meta-learning approaches can be explored to use information from other devices or servers to initialize models for new users, jump-starting the personalization process [46]. Active Learning techniques involve actively querying users for feedback to gather more relevant data and refine recommendations quickly [47]. Federated Knowledge Transfer aims to transfer knowledge from devices with more historical data to those with less data, mitigating the cold start problem [48].
5. **Bias and Fairness:** Transformers can inadvertently amplify biases present in the data, which can be exacerbated in a federated learning environment where data comes from multiple sources. This raises concerns about fairness in the recommendation process. Fair Aggregation methods aim to develop aggregation schemes that consider fairness constraints, ensuring that the final model does not disproportionately favor certain groups [49]. Fairness-aware Loss Functions incorporate fairness objectives in the recommendation learning process, guiding the model to make fairer recommendations. Bias Mitigation techniques, such as adversarial debiasing, can be employed to reduce bias in the learned representations and improve fairness [50].
6. **Adaptability to User Context:** Personalized recommendations should consider the user's current context and dynamic interests. Transformers, by nature, do not inherently handle real-time contextual information, which is crucial for a comprehensive personalized recommendation. Contextual transformers extend transformers to incorporate real-time context information (e.g., location, time, or user behavior) into the recommendation process [51]. Federated context aggregation allows the aggregation of context information along with user data during federated learning, enhancing the adaptability of

the model [52]. Contextual bandits in federated learning leverage contextual bandit algorithms to make dynamic and personalized recommendations in the federated setting [53].

7. **Interpretability and Explainability:** Interpreting the decisions made by transformer-based recommendation systems is challenging, especially in federated learning, where data comes from multiple devices and the model's reasoning may not be transparent. Attention visualization involves visualizing attention weights in the transformer to explain which parts of the input data are influential in the model's decision-making [54]. Rule-based post hoc explanations generate rule-based explanations for individual recommendations, providing insights into how specific recommendations were made [55]. Federated local explanations aim to provide explanations on individual devices without sharing raw data, enabling a more privacy-preserving approach to explainability [56].

Conclusion

In this research, an innovative approach to personalized recommendations in consumer electronic applications is presented. By investigating federated learning and trusted authority, it addresses the issue of data confidentiality during the training process. It also explores both transformers and consumer clustering to address both data quantity and quality. The consumers are first grouped into comparable groups using the dense embedding and k -means algorithms. Each consumer's local model is developed using data from their area. The server acquires the local models from consumers, along with the clustering information, and the integrity of these models is verified by a trusted authority. Instead of adhering to traditional federated learning systems, our approach employs two distinct types of aggregation. The first step involves amalgamating all consumer model data to establish the global model. The second step entails combining the models from each cluster to create a local model of similar consumers. The consumers receive both models, and they each choose which one should be utilized for personal recommendations. The method's applicability has been demonstrated by thorough trials utilizing MovieLens-1M and Amazon-book. The outcomes demonstrate the suggested method's superiority over the baseline approaches, where it achieves an average accuracy of 0.27 in comparison to approaches that do not exceed 0.25. As a future perspective, we plan to explore more advanced decomposition methods [57, 58] for consumer grouping. Exploring other consumer electronic-based applications with our method is also in our future agenda.

Author Contribution Conceptualization: Youcef Djenouri and Asma Belhadi. Methodology: Asma Belhadi, Fabio Augusto de Alcantara, and Gautam Srivastava. Validation: Asma Belhadi, Fabio Augusto de Alcantara, and Gautam Srivastava. Writing — original draft: Youcef Djenouri, Asma Belhadi, Fabio Augusto de Alcantara, and Gautam Srivastava. Writing — review and editing: Asma Belhadi, Fabio Augusto de Alcantara, and Gautam Srivastava. Supervision: Youcef Djenouri and Gautam Srivastava

Funding Open access funding provided by University Of South-Eastern Norway This work is co-funded by the Research Council of Norway under the project entitled "Next Generation 3D Machine Vision with Embedded Visual Computing" with grant number 325748.

Declarations

Competing Interest The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Beitz B, Roth R, Häser J, Wiegand T, Möller R. Improving the user experience for manual data labeling using a graph-based approach. In: 2022 IEEE International Conference on Consumer Electronics (ICCE). IEEE; 2022. pp. 1–4.
- Djenouri Y, Yazidi A, Srivastava G, Lin JCW. Blockchain: Applications, challenges, and opportunities in consumer electronics. IEEE Consum Electr Mag. 2023.
- Dong L, Hua Z, Huang L, Ji T, Jiang F, Tan G, Zhang J. The impacts of live chat on service–product purchase: Evidence from a large online outsourcing platform. Inf Manag. 2024:103931.
- Lim WM, Kumar S, Pandey N, Verma D, Kumar D. Evolution and trends in consumer behaviour: Insights from journal of consumer behaviour. J Consum Behav. 2023;22(1):217–32.
- Petchhan J, Su SF. High-intensified resemblance and statistic-restructured alignment in few-shot domain adaptation for industrial-specialized employment. IEEE Trans Consum Electr. 2023.
- Hilbel T, Frey N. Review of current ECG consumer electronics (pros and cons). J Electrocardiol. 2023;77:23–8.
- Zhang F, Chang Z, Xiong J, Ma J, Ni J, Zhang W, Jin B, Zhang D. Embracing consumer-level UWB-equipped devices for fine-grained wireless sensing. Proc ACM Interact Mob Wearable Ubiquitous Technol. 2023;6(4):1–27.
- Wu CJ. Special issue on environmentally sustainable computing. IEEE Micro. 2023;43(01):7–8.

9. Shen X, Jiang H, Liu D, Yang K, Deng F, Lui JC, Liu J, Dustdar S, Luo J. Pupilrec: Leveraging pupil morphology for recommending on smartphones. *IEEE Internet Things J.* 2022;9(17):15538–53.
10. Cao B, Zhao J, Lv Z, Yang P. Diversified personalized recommendation optimization based on mobile data. *IEEE Trans Intell Transp Syst.* 2020;22(4):2133–9.
11. Djenouri Y, Belhadi A, Srivastava G, Lin JCW. Toward a cognitive-inspired hashtag recommendation for twitter data analysis. *IEEE Trans Comput Soc Syst.* 2022;9(6):1748–57.
12. Mi F, Lin X, Faltings B. Ader: Adaptively distilled exemplar replay towards continual learning for session-based recommendation. In: *Proceedings of the 14th ACM Conference on Recommender Systems.* 2020. pp. 408–13.
13. Xu Y, Wang E, Yang Y, Chang Y. A unified collaborative representation learning for neural-network based recommender systems. *IEEE Trans Knowl Data Eng.* 2021;34(11):5126–39.
14. Afsar MM, Crump T, Far B. Reinforcement learning based recommender systems: A survey. *ACM Comput Surv.* 2022;55(7):1–38.
15. Djenouri Y, Belhadi A, Srivastava G, Lin JCW. Deep learning based hashtag recommendation system for multimedia data. *Inf Sci.* 2022;609:1506–17.
16. Wang D, Liang Y, Xu D, Feng X, Guan R. A content-based recommender system for computer science publications. *Knowl-Based Syst.* 2018;157:1–9.
17. Huang F, Wang Z, Huang X, Qian Y, Li Z, Chen H. Aligning distillation for cold-start item recommendation. 2023.
18. Walek B, Fajmon P. A hybrid recommender system for an online store using a fuzzy expert system. *Expert Syst Appl.* 2023;212:118565.
19. Belhadi A, Djenouri Y, Lin JCW, Cano A. A data-driven approach for twitter hashtag recommendation. *IEEE Access.* 2020;8:79182–91.
20. Djenouri Y, Belhadi A, Srivastava G, Lin JCW. An efficient and accurate GPU-based deep learning model for multimedia recommendation. *ACM Trans Multimed Comput Commun Appl (TOMM).* 2021.
21. Xie Y, Wang Z, Gao D, Chen D, Yao L, Kuang W, Li Y, Ding B, Zhou J. Federatedscope: A flexible federated learning platform for heterogeneity. *Proc VLDB Endowment.* 2023;16(5):1059–72.
22. Fu Y, Li C, Yu FR, Luan TH, Zhao P. An incentive mechanism of incorporating supervision game for federated learning in autonomous driving. *IEEE Trans Intell Transp Syst.* 2023.
23. Li B, Guo T, Zhu X, Li Q, Wang Y, Chen F. SGCCCL: Siamese graph contrastive consensus learning for personalized recommendation. In: *Proceedings of the Sixteenth ACM International Conference on Web Search and Data Mining.* 2023. pp. 589–97.
24. Xie X, Sun F, Liu Z, Wu S, Gao J, Zhang J, Ding B, Cui B. Contrastive learning for sequential recommendation. In: *2022 IEEE 38th International Conference on Data Engineering (ICDE).* IEEE; 2022. pp. 1259–73.
25. Fu A, Zhang X, Xiong N, Gao Y, Wang H, Zhang J. VFL: A verifiable federated learning with privacy-preserving for big data in industrial IoT. *IEEE Trans Industr Inf.* 2022;18(5):3316–26. <https://doi.org/10.1109/TII.2020.3036166>.
26. Zhou C, Fu A, Yu S, Yang W, Wang H, Zhang Y. Privacy-preserving federated learning in fog computing. *IEEE Internet Things J.* 2020;7(11):10782–93. <https://doi.org/10.1109/JIOT.2020.2987958>.
27. Yin L, Feng J, Xun H, Sun Z, Cheng X. A privacy-preserving federated learning for multiparty data sharing in social IoTs. *IEEE Trans Netw Sci Eng.* 2021;8(3):2706–18. <https://doi.org/10.1109/TNSE.2021.3074185>.
28. Li B, Li G, Xu J, Li X, Liu X, Wang M, Lv J. A personalized recommendation framework based on MOOC system integrating deep learning and big data. *Comput Electr Eng.* 2023;106:108571.
29. Solairaj A, Sugitha G, Kavitha G. Enhanced Elman spike neural network based sentiment analysis of online product recommendation. *Appl Soft Comput.* 2023;132:109789.
30. Swaminathan B, Palani S, Vairavasundaram S. Feature fusion based deep neural collaborative filtering model for fertilizer prediction. *Expert Syst Appl.* 2023;216:119441.
31. Ma Y, Zhang X, Gao C, Tang Y, Li L, Zhu R, Yin C. Enhancing recommendations with contrastive learning from collaborative knowledge graph. *Neurocomputing.* 2023;523:103–15.
32. Shuai J, Zhang K, Wu L, Sun P, Hong R, Wang M, Li Y. A review-aware graph contrastive learning framework for recommendation. In: *Proceedings of the 45th International ACM SIGIR Conference on Research and Development in Information Retrieval.* 2022. pp. 1283–93.
33. Wang X, He X, Cao Y, Liu M, Chua TS. Kgat: Knowledge graph attention network for recommendation. In: *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining.* 2019. pp. 950–8.
34. Wang H, Zhang F, Wang J, Zhao M, Li W, Xie X, Guo M. Ripplet: Propagating user preferences on the knowledge graph for recommender systems. In: *Proceedings of the 27th ACM International Conference on Information and Knowledge Management.* 2018. pp. 417–26.
35. Ai Q, Azizi V, Chen X, Zhang Y. Learning heterogeneous knowledge base embeddings for explainable recommendation. *Algorithms.* 2018;11(9):137.
36. Desai A, Chou L, Shrivastava A. Random offset block embedding (robe) for compressed embedding tables in deep learning recommendation systems. *Proc Mach Learn Syst.* 2022;4:762–78.
37. Wang D, Yi Y, Yan S, Wan N, Zhao J. A node trust evaluation method of vehicle-road-cloud collaborative system based on federated learning. *Ad Hoc Netw.* 2023;138:103013.
38. Acheampong FA, Nunoo-Mensah H, Chen W. Transformer models for text-based emotion detection: A review of Bert-based approaches. *Artif Intell Rev.* 2021:1–41.
39. Hassan MU, Rehmani MH, Chen J. Differential privacy techniques for cyber physical systems: A survey. *IEEE Commun Surv Tutor.* 2019;22(1):746–89.
40. Zhao C, Zhao S, Zhao M, Chen Z, Gao CZ, Li H, Tan YA. Secure multi-party computation: Theory, practice and applications. *Inf Sci.* 2019;476:357–72.
41. Liu Y, Kang Y, Xing C, Chen T, Yang Q. A secure federated transfer learning framework. *IEEE Intell Syst.* 2020;35(4):70–82.
42. Xu C, McAuley J. A survey on model compression and acceleration for pretrained language models. In: *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37. 2023. pp. 10566–75.
43. Wu G, Gong S. Peer collaborative learning for online knowledge distillation. In: *Proceedings of the AAAI Conference on artificial intelligence*, vol. 35. 2021. pp. 10302–10.
44. Liu H, Shao M, Fu Y. Structure-preserved multi-source domain adaptation. In: *2016 IEEE 16th International Conference on Data Mining (ICDM).* IEEE; 2016. pp. 1059–64.
45. Tang L, Jiang Y, Li L, Li T. Ensemble contextual bandits for personalized recommendation. In: *Proceedings of the 8th ACM Conference on Recommender Systems.* 2014. pp. 73–80.
46. Li X, Sun Z, Xue JH, Ma Z. A concise review of recent few-shot meta-learning methods. *Neurocomputing.* 2021;456:463–8.
47. Giancola S, Cioppa A, Georgieva J, Billingham J, Serner A, Peek K, Ghanem B, Van Droogenbroeck M. Towards active learning for action spotting in association football videos. In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.* 2023. pp. 5097–107.
48. Zhang J, Guo S, Guo J, Zeng D, Zhou J, Zomaya A. Towards data-independent knowledge transfer in model-heterogeneous federated learning. *IEEE Trans Comput.* 2023.

49. Cousins C. Revisiting fair-PAC learning and the axioms of cardinal welfare. In: International Conference on Artificial Intelligence and Statistics. PMLR; 2023. pp. 6422–42.
50. Omrani A, Ziabari AS, Yu C, Golazizian P, Kennedy B, Atari M, Ji H, Dehghani M. Social-group-agnostic bias mitigation via the stereotype content model. In: Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (ACL2023). 2023.
51. He J, Gao Y, Zhang T, Zhang Z, Wu F. D2former: Jointly learning hierarchical detectors and contextual descriptors via agent-based transformers. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2023. pp. 2904–14.
52. Zhou X, Ye X, Kevin I, Wang K, Liang W, Nair NKC, Shimizu S, Yan Z, Jin Q. Hierarchical federated learning with social context clustering-based participant selection for internet of medical things applications. *IEEE Trans Comput Soc Syst*. 2023.
53. Huang R, Zhang H, Melis L, Shen M, Hejazinia M, Yang J. Federated linear contextual bandits with user-level differential privacy. In: International Conference on Machine Learning. PMLR; 2023. pp. 14060–95.
54. Zhao C, Wang C, Hu G, Chen H, Liu C, Tang J. ISTVT: Interpretable spatial-temporal video transformer for deepfake detection. *IEEE Trans Inf Forensics Secur*. 2023;18:1335–48.
55. Jeyasothy A, Laugel T, Lesot MJ, Marsala C, Detyniecki M. A general framework for personalising post hoc explanations through user knowledge integration. *Int J Approx Reason*. 2023;160:108944.
56. Demertzis K, Iliadis L, Kikiras P, Pimenidis E. An explainable semi-personalized federated learning model. *Integr Comput Aided Eng*. 2022;29(4):335–50.
57. Djenouri Y, Belhadi A, Djenouri D, Lin JCW. Cluster-based information retrieval using pattern mining. *Appl Intell*. 2021;51:1888–903.
58. Djenouri Y, Lin JCW, Nørvåg K, Ramampiaro H. Highly efficient pattern mining based on transaction decomposition. In: 2019 IEEE 35th International Conference on Data Engineering (ICDE). IEEE; 2019. pp. 1646–9.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.