TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214
DOI: 10.26599/TST.2024.90100XX

FSRPCL: Privacy-Preserve Federated Social Relationship Prediction with Contrastive Learning

Hanwen Liu, Nianzhe Li, Huaizhen Kou, Shunmei Meng, and Qianmu Li*

Abstract: Cross-Platform Social Relationship Prediction (CPSRP) aims to utilize users' data information on multiple platforms to enhance the performance of social relationship prediction, thereby promoting socio-economic development. Due to the highly sensitive nature of users' data in terms of privacy, CPSRP typically introduces various privacy-preserving mechanisms to safeguard users' confidential information. Although the introduction mechanism guarantees the security of the users' private information, it tends to degrade the performance of the social relationship prediction. Additionally, existing social relationship prediction schemes overlook the interdependencies among items invoked in a user behavior sequence. For this purpose, we propose a novel privacy-preserve Federated Social Relationship Prediction with Contrastive Learning framework called FSRPCL, which is a multi-task learning framework based on vertical federated learning. Specifically, the users' rating information is perturbed with a bounded differential privacy technology, and then the users' sequential representation information acquired through Transformer is applied for social relationship prediction and contrastive learning. Furthermore, each client uploads their respective weight information to the server, and the server aggregates the weight information and distributes it purposes to each client for updating. Numerous experiments on real-world datasets prove that FSRPCL delivers exceptional performance in social relationship prediction and privacy preservation, and effectively minimizes the impact of privacy-preserving technology on social relationship prediction accuracy.

Key words: social relationship prediction; contrastive learning; vertical federated learning

1 Introduction

Presently, the swift progress and widespread utilization of smart devices, such as mobile phones and laptops, are significantly enhancing various aspects of people's daily lives, including entertainment, sports, and dining. Typically, users express their emotions and views by using a variety of intelligent devices to review and/or rate purchased items including clothing, food, electronics, etc. on various consumer platforms such as Tmall, Jingdong, and Taobao. According to existing homogeneous sociological theories[1], it is anticipated that users who share similar historical behavioral attributes, particularly in terms of consumption behavior, are expected to form new social relationships. Consequently, the proliferation of multiple platforms on various intelligent devices has contributed to the intricacy and unpredictability of online social networks. Moreover, there has been a notable focus on researching cross-platform social relationship prediction[2], which aims to leverage users' data from multiple platforms to enhance the accuracy of social relationship prediction, thus enabling users to

• Hanwen Liu, Nianzhe Li, Huaizhen Kou, Shunmei Meng, and Qianmu Li are with the School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China. E-mail: hanwenliu2020@njust.edu.cn; linianzhe@njust.edu.cn; huaizhenkou@njust.edu.cn; mengshunmei@njust.edu.cn; qianmu@njust.edu.cn.
* To whom correspondence should be addressed.
Manuscript received:

expand their communication networks rapidly and foster socio-economic development.

Sharing users' private data across different platforms is a challenging task due to the stringent privacy laws and regulations, such as GDPR[3] and CCPA, that impose strict requirements on data protection and privacy. As a result, integrating user data information from multiple consumer platforms that are distributed across different intelligent devices[4, 5] poses significant challenges for the cross-platform social relationship prediction model. Fortunately, the federated learning[6] paradigm introduced by Google[7, 8] provides a solution for sharing users' data information across different platforms. In practice, federated learning builds and trains a shared machine learning model, where each client simply uploads the trained weight information to the server for aggregation, while the users' data information[9] remains stored locally on the client without being transferred to other clients or servers. Currently, a widely accepted method for the aggregation of weight information is the Federal Average (FedAvg) algorithm[10]. Thus, the federated learning paradigm, as a distributed and privacy-preserving machine learning paradigm, is well suited for cross-platform social relationship prediction models.

While federated learning[11, 12] provides a certain level of protection for users' privacy information, attackers exploit the weight information uploaded by the client to perform inference attacks on the users' data. Therefore, the cross-platform social relationship prediction models usually introduce other privacy-preserving mechanisms[13, 14, 15] (e.g., differential privacy technology[16], homomorphic encryption) to further obscure the users' data information to achieve stronger privacy protection measures. Since the differential privacy technology allows the introduction of noise that conforms to either a Laplace or Gaussian distribution to perturb the users' data information, this privacy-preserving mechanism offers a designated level of privacy protection[17]. Despite the theoretical advantages and the assurance of users' data security on various platforms, the use of differential privacy technology consistently hampers the performance of social relationship prediction[16]. Indeed, the process of perturbation of the users' data by differential privacy technology can be considered as one of the data enhancement approaches in contrastive learning[18]. Consequently, the advancement of contrastive learning provides robust technical support for the solution of the performance degradation problem in the social relationship prediction process caused by using differential privacy technology.

Additionally, existing social relationship prediction methods[1, 19] typically assume that the users' historical data remains static and overlook the impact of interdependencies among items in the users' behavioral sequence on the users' characteristics. The comprehensive exploration and analysis of the sequence characteristics of the users' behavior is also hindered by this limitation. Recently, with the exploration and application of deep learning[20, 21, 22] in the field of artificial intelligence, Transformer[23, 24] has been proven to effectively capture the dependencies among items in a sequence of the users' behaviors, enabling dynamic modeling of the users' long sequences features. In essence, the Transformer is specifically designed to provide a solid technical foundation for extracting dependencies among items in the users' behavior sequence during the social relationship prediction.

Based on the aforementioned research, we present a novel privacy-preserve Federated Social Relationship Prediction with Contrastive Learning method named FSRPCL, which is a multi-task learning model that utilizes vertical federated learning. Specifically, FSRPCL consists of three primary components: The model applies the bounded differential privacy technology to perturb the users' rating information in each client during preprocessing, thus preventing attackers from attempting to deduce users' preference information through targeted attacks. On the client side, the model leverages the embedding technique and Transformer to learn the users' sequence representation information and thoroughly mines the dependencies among invoked items in the users' sequence for social relationship prediction and contrastive learning processes. Meanwhile, the impact of the bounded differential privacy technology on the social relationship prediction performance can be reduced by the contrastive learning process. Furthermore, the client uploads the weight information to the server and downloads the corresponding global weight information from the server. On the server side, the model gathers the parameter information uploaded by the client and updates the global parameter information using the federated averaging algorithm.

Below is a summary of the key contributions of our

work:

(1) **Novel:** Our research puts forward the privacy-preserve Federated Social Relationship Prediction with Contrastive Learning scheme, which is the first application of contrastive learning to the cross-platform social relationship prediction model.

(2) **Substantial:** In the FSRPCL model, the use of differential privacy technology introduces perturbations to the users' rating information. The embedding technique and Transformer are deployed to learn the users' sequence representation information that is leveraged in the social relationship prediction and contrastive learning processes.

(3) **Comprehensive:** We conduct a series of in-depth experiment analyses with the publicly accessible Epinions dataset. The detailed experimental analysis showcases the effectiveness and feasibility of FSRPCL in cross-platform social relationship prediction.

The remainder of the paper is divided as follows: Section 2 briefly summarizes previous research. The motivation behind the research is explained in Section 3. Section 4 outlines the specific details of the proposed multitask learning scheme based on vertical federated learning, known as FSRPCL. Section 5 describes the comprehensive experimental results and includes the corresponding analysis. Finally, there is a summary of our study and a discussion of possible future research directions in Section 6.

2 Related Work

Here, we will explore three pertinent topics: social relationship prediction, federated learning, and contrastive learning.

2.1 Social relationship prediction

There are currently two main types of methods used for predicting social relationships:

Historical behavior records-based social relationship prediction approaches. Kou et al.[25] and Liu et al.[26] both relied on information about users' historical behavior to predict social relationships, while both methods validated the established social relationships through the social balance theory. Furthermore, these two methods utilized the Simhash technique and the Locality-Sensitive Hashing technology to find a similar set of users, respectively. In addition, Tang et al.[1] proved that there was a strong internal correlation between social relationship prediction and users' similarity through the analysis of users' historical behavior information, thus indirectly showing that the homogeneity theory in sociology explained the reasons for the establishment of social relationships. Although the above methods have achieved certain achievements in social relationship prediction, all of them considered the users' historical behavior information as static information. In fact, the user's historical behavior information is dynamic and has a profound impact on social relationship prediction. For example, Xu et al.[27] utilized the LSTM (Long Short-Term Memory) network to extract the overall temporal characteristics of users to further predict the trust social relationships between users, and this social relationship prediction process fully exploited and analyzed the dynamic historical behavioral information of users. Furthermore, Xu et al.[28] designed an attention-based neural network model, GainTrust, by combining the users' trusted neighbors with the users' overall temporal characteristics obtained via the LSTM network to predict the trust social relationship among users. In addition, Ren et al.[29] proposed a collaborative filtering method based on dynamic trust decay, which not only adapted the neighbor selection mechanism but also redefined the neighbor effect by introducing the concept of trust decay.

Although the above investigations achieve overall favorable prediction results in the social relationship prediction process, these methods mainly consider the historical behavioral information of users on a single platform. In fact, in the big data environment, the users' data information for social relationship prediction is highly distributed among different smart application devices[30].

Social network structure-based social relationship prediction approaches. Drawing on the existing social network structure information[31], Liu et al.[32] proposed the OpinionWalk model, which focused on directly storing the trust social relationship between users by building an opinion matrix of the trust social network topology. Furthermore, the NeuralWalk algorithm, which constructed single-hop trust propagation and fusion in trust social networks based on the WalkNet neural network, has been proposed in Ref. [33]. Actually, the accuracy of social relationship prediction results in these two methods is not high, as the parameters in these two methods are empirically adjusted. Additionally, Lin et al.[19] proposed the Guardian model, which incorporated popularity trust and participation trust into the users' latent

representation through the graph convolutional neural network to learn and predict effective trust social relationships. Meanwhile, Liu et al.[26] and Xu et al.[28] also applied social network structure information in their social relationship prediction model to predict social relationships among users. Hence, within the big data environment, the aforementioned social relationship prediction methods relying on social network structure information also fall short of achieving cross-platform social relationship prediction scenarios.

2.2 Federated learning

The federated learning paradigm[10] was proposed by Google in 2016, which only enabled the transfer of weight parameter information between the client and the server without sharing the users' data information. The federated learning[34, 35] realizes the protection of the users' private information to some extent. According to the Literature [3], federated learning mainly comprises three forms, namely, vertical federated learning, horizontal federated learning, and federated transfer learning.

Recently, several federated recommendation algorithms[10, 36] have been developed with the aim of not only ensuring effective personalized recommendations but also safeguarding the privacy[37] of users' information. For example, Wu et al.[36] designed the Hierarchical Personalized Federated Learning (HPFL) approach to overcome the problem of inconsistent customer-user modeling in the federated learning framework. Although the federated learning paradigm can build and train federated models with the security of users' data to a certain extent, attackers are still able to infer the users' attribute information[38] by analyzing the weight or gradient information transmitted to the server. Therefore, the federated learning paradigm remains susceptible to privacy leaks. To prevent such situations, some researchers have incorporated privacy-preserving mechanisms, such as homomorphic encryption and differential privacy, into the federated learning paradigm. These mechanisms served to intentionally obscure users' data information, enhancing the overall protection of user privacy. As an illustration, FedRec[39] represented a federated recommendation model grounded in factorized explicit feedback, which introduced two strategies, namely user averaging and hybrid filling, to deliberately distort users' rating information and further thwart potential inference attacks by attackers. Furthermore, Chai et al.[40] proposed the FedMF framework, a secure matrix factorization framework built upon federated learning, which applied homomorphic encryption technology to enhance the security of gradient information. Meanwhile, Jiang et al.[41] proposed the FedNCF model, a privacy-preserving federated recommender system that used an adaptive differential privacy technology to perturb the gradient information in the model, successfully preventing attackers from carrying out inference attacks. In addition, Liu et al.[42] presented the FDRP model, which was a social relationship prediction model based on vertical federated learning and perturbed the users' history information by incorporating the graph attention network (GAT) strategy.

Although the aforementioned federated learning methods may serve as a suitable solution to the problem of users' privacy and security in recommender systems and social relationship prediction models, they neglect to take into account and mitigate the impact of the introduced privacy-preserving technologies on the performance of recommendations or social relationship predictions. Meanwhile, few existing research efforts have applied federated learning frameworks to the field of link prediction.

2.3 Contrastive learning

Currently, contrastive learning[43] finds extensive application across various domains of deep learning[44, 45, 46], including Computer Vision (CV), Natural Language Processing (NLP), and Recommender Systems (RS)[47, 48], primarily attributed to the effectiveness of self-supervised learning. For example, for the CV problem, He et al.[49] proposed the Momentum Contrast method for unsupervised learning of visual representations, i.e., MoCo, which was a model that used a contrastive learning-based approach to self-supervise the training of the image representer (encoder) to better encode the image and apply it to downstream tasks. In contrastive learning for language modeling, Yan et al.[50] proposed the ConSERT framework that employed the contrastive learning approach to fine-tune BERT, thus solving the problem of data augmentation methods to modify semantic information in the natural language model. In the realm of RS, Xie et al.[18] introduced the Contrastive Learning for Sequence Recommendation (CL4SRec) approach, which was a model that concentrated on

deriving self-supervised signals from raw users' behavior sequences using three different data augmentation methods to improve personalized recommendation performance. In the paper, contrastive learning is primarily adopted to reduce the impact of privacy-preserving schemes on social relationship prediction performance.

The aforementioned research on social relationship prediction, federated learning, and contrastive learning is not limited to what is described in this subsection. In light of the above research, we propose a multi-task learning model based on vertical federated learning, i.e., FSRPCL, which can reduce the impact of privacy-preserving technology on social relationship prediction performance. The details of the proposed cross-platform social relationship prediction model, FSRPCL, are outlined in Section 4.

3 Research Motivation

Figure 1 illustrates the motivation behind our research through a real-world application scenario. TikTok intends to create new social relationships among these three distinct users in the illustration to widen their circle of communication, share the short videos watched by each other, and further increase playback traffic on TikTok. As the data stored on TikTok related to users' video viewing is insufficient for a comprehensive analysis of users' preference information, it hinders the accurate prediction of social relationships among users. Therefore, TikTok seeks to combine users' consumption records on other platforms, such as JD and Tmall, to accurately predict social relationships between users. However, the consumption records (i.e., behavioral records) of the same users are not exchanged between the three platforms in the figure due to laws and regulations and users' need to protect their privacy. As a consequence, TikTok is unable to directly integrate and analyze the behavioral records of users located on other different platforms.

While current federated learning paradigms enable the training of model parameters without sharing the actual user data information, the potential for privacy violation persists. Therefore, there is a requirement to perturb the users' data information (e.g., rating information), using established privacy-preserving methods (e.g., differential privacy) to enhance overall privacy protection. In addition, existing social relationship prediction methods do not

take into account the dependencies among items invoked in the users' behavioral records when learning information about the users' behavioral sequence characteristics. For instance, the users u_i and u_j in Fig. 1 both purchased the same product on the JD platform, but the sequence of products they purchased differs in their behavioral records, implying that the learned behavioral sequence feature information for these two users may also differ.

The following daunting challenges to the social relationship prediction scenario arise intuitively:

(1) How to mitigate the risk of privacy violations present in the federated learning paradigm?

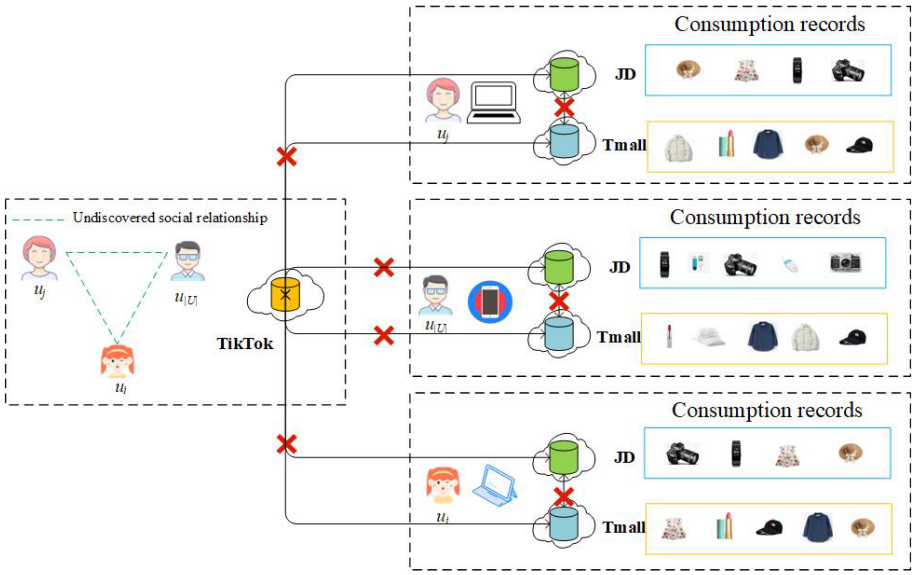


Fig. 1 Research motivation example.

(2) How to address the degradation of the social relationship prediction performance caused by privacy-preserving approaches?

(3) How to learn the dependencies among items invoked in the users' behavioral records?

Addressing the aforementioned challenges, this paper develops a novel social relationship prediction scheme called FSRPCL to better achieve the balance between privacy protection and social relationship prediction performance. The subsequent section delves into the specifics of the scheme. Furthermore, in consideration of the big data environment, our federated learning scenario and the corresponding problem can be specified as follows:

Definition 1 (Client). A single platform (e.g., Tmall) located on different intelligent application devices is defined as a local client that hosts the user data information. Each client c ($c \in Set\{c_1, ..., c_z\}$) is assigned to a set of the same users, i.e., U, but covering a different user behavioral space compared to the other clients.

Definition 2 (Server). A server is a device that coordinates model training among multiple clients and never collects original data from the clients, only the parameter information required to update the model.

Definition 3 (Problem Definition). In the big data environment, can we co-train a model to predict social relationships among users while minimizing the impact of privacy-preserving approaches on the performance of the social relationship prediction model, without accessing data from any local client (platform)?

4 Our Model: FSRPCL

In this section, we introduce the proposed social relationship prediction framework, i.e., FSRPCL. Unlike existing social relationship prediction models, our FSRPCL framework incorporates differential privacy technology[51, 52] to perturb users' ratings. Subsequently, we apply contrastive learning to mitigate the impact of performance degradation in social relationship prediction caused by the use of differential privacy technology. Secondly, during the social relationship prediction process, the raw data of user-item interactions are retained on each client instead of being uploaded to the server, thus further reducing users' privacy concerns.

As shown in Fig. 2, the entire FSRPCL model framework consists of the following three main parts:

(1) Pretreatment process: we utilize differential privacy technology to perturb the rating information of users on each client to thwart potential attackers from inferring attacks on users' preference information.

(2) Client-side: we employ Transformer to learn the users' representation information for both social relationship prediction and contrastive learning processes. Additionally, local and global parameter information is uploaded and downloaded to and from the server.

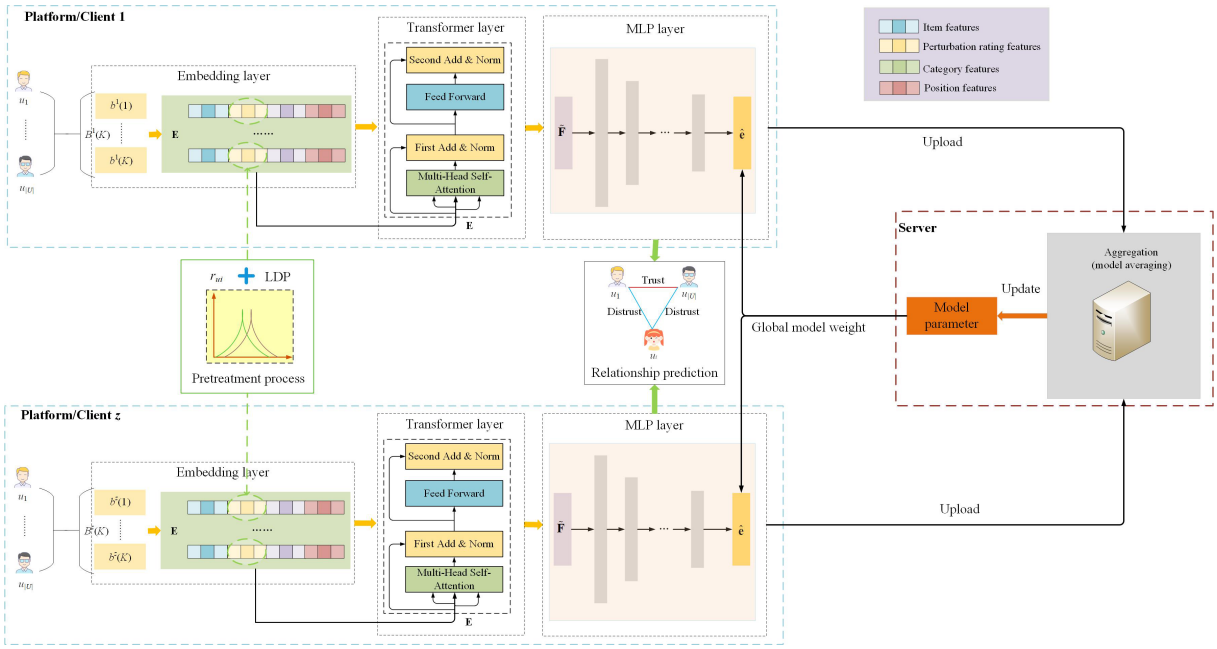


Fig. 2 Entire FSRPCL model framework.

(3) Server-side: the server gathers the parameter information uploaded by the client and updates the global parameter information.

We will delve into each of these three components in greater detail below. Additionally, the symbols related to the terms used in the paper are listed in Table 1.

4.1 Pretreatment process: perturbation rating

To safeguard the privacy information of users across various clients and prevent attackers from inferential attacks on users' preference information, according to the Literature[52], we employ differential privacy technology to carry out data perturbation of users' rating information. The perturbation process is shown below:

$$\tilde{r}_{ui} \triangleq r_{ui} + Lap(0, \lambda_i) \tag{1}$$

Where, $Lap(0, \lambda_i)$ represents the Laplacian noise with a mean of 0, and λ_i governs the intensity of the Laplacian noise. The larger λ_i is, the larger the noise is and the more favorable it is for privacy protection.

Table 1 Notation definition.

Notation	Definition
U	A set of users.
$Set\{c_1, ..., c_z\}$	A set of clients.
$\tilde{r}_{ui}$	Perturbation rating.
λ_i	Laplacian noise parameter.
$B^c{}_u()$	The behavioral sequence of the user u on the client c.
$I^c{}_u(k)$	The user u invokes the k-th ($1 \leqslant k \leqslant K$) item on the client c.
$R^c{}_u(k)$	The corresponding perturbation rating of the k-th item given by the user u on the client c.
$C^c{}_u(k)$	The corresponding category of the k-th item invoked by the user u on the client c.
$Po^c{}_u(k)$	The corresponding location information of the k-th item invoked by the user u on the client c.
$\mathbf{E}_u / e^c{}_u(K)$	The embedding representation of the embedding layer.
$\mathbf{S}_u$	The embedding representation of the multi-attention layer.
$\mathbf{F}_u$	The embedding representation of the feed-forward networks.
$\tilde{F}_u$	The final output embedding representation of the Transformer layer.
$\hat{e}_u$	The embedding representation of the multilayer perceptron layer.
w_c	The weight information that the client c uploads to the server.
$\bar{W}$	Aggregation parameter.
L_{cl}	The loss function of the contrastive learning process.
L_{rp}	The loss function of the social relationship prediction.
L_{mt}	The loss function of the multi-tasking training.

The introduction of noise[53] in the users' rating information can impact the learning and extraction of user feature information, subsequently influencing various downstream tasks such as item

recommendation and social relationship prediction. Additionally, the process of perturbing the users' rating information through the Laplace mechanism (i.e., setting different parameters λ_i) each time can be viewed as a rating enhancement operation in the context of contrastive learning. To perform the subsequent contrastive learning task, we will employ two distinct parameters λ_i, namely λ_1 and λ_2, to perturb the users' rating information, so that we will get two different rating enhancement views for each user on each client. It is worth noting that the bounded difference privacy technology[52] is implemented in the process of perturbing user rating information, meaning $\tilde{r}_{ui} \in [r^c{}_{max}, r^c{}_{min}]$.

Note that, for the sake of representing a user's rating information, we use a uniform symbol, i.e., R_u, to represent different rating perturbations in Section 4.2.

4.2 Client-side: social relationship prediction and contrastive learning

(1) Embedding layer. The embedding technique involves mapping objects from a high-dimensional space to a low-dimensional space while preserving their associated properties. Therefore, we initially convert the users' relevant data information (e.g., items, perturbation ratings) on each client into dense and continuous vectors using the appropriate embedding technique[2].

As shown in Fig. 2, on each client c ($c \in Set\{c_1, ..., c_z\}$), the behavioral sequence of a user u ($u \in U$) can be represented as $B^c{}_u(K)=\{ b^c{}_u(1), b^c{}_u(2), \ldots, b^c{}_u(K)\}$, where $b^c{}_u(k)=\{ I^c{}_u(k), R^c{}_u(k), C^c{}_u(k), Po^c{}_u(k)\}$. $Set\{I^c{}_u(k), R^c{}_u(k), C^c{}_u(k), Po^c{}_u(k)\}$ is detailed below:

$I^c{}_u(k)$ signifies that the user u invokes the k-th ($1 \leqslant k \leqslant K$) item on the client c.

$R^c{}_u(k)$ represents the corresponding perturbation rating of the k-th item.

$C^c{}_u(k)$ indicates the corresponding category of the k-th item.

$Po^c{}_u(k)$ describes the corresponding location information of the k-th item.

According to the Literature [54], Transformer records the relative positional relationships in a sequence through position encoding. Hence, we adopt the

original sinusoidal curve approach in Transformer for position encoding:

$$Po_{\sin}(index, 2i) = \sin(index/10000^{2i/d}) \quad (2)$$

$$Po_{\cos}(index, 2i+1) = \cos(index/10000^{2i/d}) \quad (3)$$

where *index* represents the location index and *i* represents the *i*-th dimension of the location encoding. $Po_{\sin}(index, 2i)$ and $Po_{\cos}(index, 2i+1)$ correspond to the $2i$ and $2i+1$ components of the encoding vector of the position *index*, respectively.

Based on the embedding technique, the embedding features of the user *u* are represented as follows:

$$E_u = e_u^c(K) = I_u^c(K) \circ R_u^c(K) \circ C_u^c(K) \circ Po_u^c(K) \quad (4)$$

Where $\circ$ is the connectivity operator, $I^c{}_u(K)$, $R^c{}_u(K)$, $C^c{}_u(K)$, $Po^c{}_u(K)$ belong to the space $\mathbb{R}^{K*d}$, d is the dimension size of the embedding, and $K=|I|$ is the number of items called by the user *u*. Thereby, $e^c{}_u(K)$ belongs to the space $\mathbb{R}^{4*K*d}$ and seamlessly integrates all the historical behavioral features of the user *u* on the client *c*.

(2) Transformer layer. As Transformer[55, 56] adeptly captures the dependencies between items in a sequence of the users' behaviors, it assists us in achieving a more profound representation learning of each item and further obtaining accurate embedding representations for each user on each client.

a. Self-attention layer. The scaled dot-product attention[23] is defined as follows:

$$\text{Attention}(\mathbf{Q}, \mathbf{K}, \mathbf{V}) = \text{softmax}\left(\frac{\mathbf{Q}\mathbf{K}^T}{\sqrt{d}}\right)\mathbf{V} \quad (5)$$

Where $\mathbf{Q}$, $\mathbf{K}$ and $\mathbf{V}$ represent query, key and value, respectively.

In our devised scheme, the self-attention mechanism takes the embedded information of the embedding layer as input and transforms it into three matrices by linear projection, which is then fed into the attention layer. Following the approach outlined in Ref. [23], for the user *u*, the multi-head attention mechanism is as follows:

$$\mathbf{S}_u = \text{MH}(\mathbf{E}_u) = \text{Concat}(head_1, head_2, ..., head_h)\mathbf{W}^H \quad (6)$$

$$head_j = \text{Attention}\left(\mathbf{E}_u\mathbf{W}^{\mathbf{Q}}, \mathbf{E}_u\mathbf{W}^{\mathbf{K}}, \mathbf{E}_u\mathbf{W}^{\mathbf{V}}\right) \quad (7)$$

Where the mapping matrix $\mathbf{W}^{\mathbf{Q}}$, $\mathbf{W}^{\mathbf{K}} \in \mathbb{R}^{4*K*d*d_k}$, $\mathbf{W}^{\mathbf{V}} \in \mathbb{R}^{4*K*d*d_v}$, $\mathbf{W}^H \in \mathbb{R}^{h*d_v*4*K*d*d_k}$, h is the number of heads. $d_k = d_v = 4*K*d/h$.

b. First Add&Norm. As depicted in Fig. 2, the embedding information from the embedding layer undergoes the multi-attention layer to derive the new embedding representation $\mathbf{S}_u$. Subsequently, the new embedding representation is subjected to the First Add&Norm manipulation. Meanwhile, we incorporate the dropout operation in the First Add&Norm to avoid overfitting, the process is as follows:

$$\mathbf{S}'_u = \text{LayerNorm}(\mathbf{E}_u + Dropout(S_u)) \quad (8)$$

Where the LayerNorm(.) is the standard normalized layer.

c. Feed-Forward Networks. Following the First Add&Norm operation, we add Feed-Forward Networks (FFN) to augment the nonlinearity of the user feature extraction process. In practice terms, the FFN contains a two-layer linear mapping network structure, and the network is activated by the activation function ReLU. The definition is as follows:

$$\begin{aligned}\mathbf{F}_u &= \text{FFN}(\mathbf{S}'_u) = \text{ReLU}\left(\mathbf{S}'_u W^1 + \mathbf{b}^1\right)\mathbf{W}^2 + \mathbf{b}^2 \\ &= \max\left(0, \mathbf{S}'_u\mathbf{W}^1 + \mathbf{b}^1\right)\mathbf{W}^2 + \mathbf{b}^2\end{aligned} \quad (9)$$

Where $\mathbf{W}^1$ and $\mathbf{W}^2$ are the linear layer weight parameters, $\mathbf{b}^1$ and $\mathbf{b}^2$ are the corresponding bias parameters.

d. Second Add&Norm. According to Fig. 2, the embedding representation learned by the FFN is subjected to the second Add&Norm operation. Again, the dropout operation is performed on the Second Add&Norm, the process outlined below:

$$\tilde{\mathbf{F}}_u = \text{LayerNorm}(\mathbf{S}'_u + Dropout(\mathbf{F}_u)) \quad (10)$$

In the Transformer layer, $\tilde{\mathbf{F}}_u$ is the ultimate output embedding representation of the user *u* on the client *c*.

(3) Multilayer perceptron (MLP) layer. The MLP network is applied on the output embedding representation of the Transformer layer to further extract and learn higher-dimensional features of the user *u* on the client *c*:

$$\begin{aligned}\mathbf{X}_0 &= \tilde{\mathbf{F}}_u \\ \mathbf{X}_1 &= \tanh(\mathrm{W}_1\mathbf{X}_0 + \mathrm{b}_1) \\ \mathbf{X}_2 &= \tanh(\mathrm{W}_2\mathbf{X}_1 + \mathrm{b}_2) \\ &\vdots \\ \mathbf{X}_n &= \tanh(\mathrm{W}_n\mathbf{X}_{n-1} + \mathrm{b}_n) \\ \hat{\mathbf{e}}_u &= \text{sigmoid}(w_u\mathbf{X}_n)\end{aligned} \quad (11)$$

Where W_n and b_n denote the trainable weight matrix and bias vector of the *n*-th layer in the MLP network,

respectively. The w_u denotes the weight of the user u at the output layer of the MLP network on the client c.

In our proposed scheme, each client holds $|U|$ number of users. Therefore, the weight of the client c uploading server is represented as follows:

$$w_c = \left[w_{u_1}, w_{u_2}, \cdots w_{u_{|U|}}\right]^{\mathrm{T}} \tag{12}$$

(4) Multi-tasking training process. Next, we will predict the trust/distrust social relationship among any two users on the client based on the parameter information aggregated by the server.

The server transmits (i.e., the backpropagate process) the aggregation parameter $\bar{\mathbf{W}}$ to each client. Based on Eq. (11) and Eq. (12), on the client c ($c \in Set\{c_1, ..., c_z\}$), the destination features of the user u ($u \in U$) are extracted as follows:

$$(\hat{\mathbf{e}}_t)_c = \left(\text{sigmoid}\left(\bar{\mathbf{W}}_v \mathbf{X}_n\right)\right)_t \tag{13}$$

Hence, the trust/distrust social relationship between users u_i and u_j is computed using the dot operation[2]. The formula is as follows:

$$\left(L_{spg}\left(u_i, u_f\right)\right)_e = \begin{cases} +1 & \text{sigmoid } ((\hat{\mathbf{e}}_k)_e \cdot (\hat{\mathbf{e}}_i)_e) > \sigma \\ -1 & \text{otherwise} \end{cases} \tag{14}$$

According to Eq. (1) and Eq. (13), for the same user u on each client c, utilizing two distinct differential privacy parameters will result in two different user feature representations in the MLP layer, namely $\left(\hat{\mathbf{e}}_u^{\lambda_1}\right)_c$ and $\left(\hat{\mathbf{e}}_u^{\lambda_2}\right)_c$. According to the Literature [18], the goal of the contrastive learning can be roughly summarized as maximizing consistency between positive pairs and minimizing consistency between negative pairs. To reduce the impact of degradation of the social relationship prediction performance caused by the differential privacy technology, we formulate the objective function for contrastive learning as follows:

$$L_{cl}\left(\left(\hat{\mathbf{e}}_u^{\lambda_1}\right)_c, \left(\hat{\mathbf{e}}_u^{\lambda_2}\right)_c\right) = -\log \frac{\exp\left(\text{sim}\left(\left(\hat{\mathbf{e}}_u^{\lambda_1}\right)_c, \left(\hat{\mathbf{e}}_u^{\lambda_2}\right)_c\right)\right)}{\exp\left(\text{sim}\left(\left(\hat{\mathbf{e}}_u^{\lambda_1}\right)_c, \left(\hat{\mathbf{e}}_u^{\lambda_2}\right)_c\right)\right) + \sum_{(\hat{\mathbf{e}}_u^*)_c} \exp\left(\text{sim}\left(\left(\hat{\mathbf{e}}_u^{\lambda_1}\right)_c, (\hat{\mathbf{e}}_u^*)_c\right)\right)} \tag{15}$$

Where $\left(\left(\hat{\mathbf{e}}_u^{\lambda_1}\right)_c, \left(\hat{\mathbf{e}}_u^{\lambda_2}\right)_c\right)$ denotes the positive sample pairs, and $(\hat{\mathbf{e}}_u^*)_c$ denotes the user feature representations generated by other users of the same client using the differential privacy technology.

To optimize the social relationship prediction process in the proposed model, in terms of Eqs. (1) and (14), we set the objective function for the social relationship prediction as:

$$L_{loss} = \sum_{LP_{type} \in \{S_e \cup S_u\}} \begin{pmatrix} \widehat{LP_{type}}\left(u_i, u_j\right) * \log\left(LP_{type}\left(u_i, u_j\right)\right) + \\ \left(1 - \widehat{LP_{type}}\left(u_{tar}, u_j\right)\right) * \\ \log\left(1 - LP_{type}\left(u_{tar}, u_j\right)\right) \end{pmatrix} \tag{16}$$

$$L_{rp} = L_{loss}^{\lambda_1} + L_{loss}^{\lambda_2} \tag{17}$$

Where $\{S_e \cup S_u\}$ is the set representing explicit social relationships and unobserved social relationships. Moreover, $\{S_e \cup S_u\}$ is considered as a training set.

For the single client c, the multi-tasking training objective is described as shown below:

$$L_{mt} = L_{rp} + \gamma L_{cl} \tag{18}$$

Most of the papers adopt the Adam optimizer[2] to batch update all the training parameters of the neural network, as its adaptive stochastic gradient descent combines the advantages of two optimization algorithms, AdaGrad and RMSProp.

4.3 Server-side: Aggregation parameters

The client uploads the updated parameters to the central server, which conducts federated aggregation using a specific aggregation algorithm (i.e., FedAVG[10]) to update the model parameters. The aggregation process can be represented as:

$$\bar{W} = \sum_{i=1}^{z} \frac{|c_i|}{|c|} w_{c_i}^{(m+1)} \tag{19}$$

Where $|c_i|$ denotes the number of clients selected to participate in model training in each round, $|c|$ indicates the total number of clients, i.e., $c \in Set\{c_1, ..., c_z\}$. m represents the training epoch of federated learning.

In general, the central server assigns the aggregated model weights to each client participating in the model training and then proceeds to the next round of training. Additionally, the primary process of the proposed FSRPCL is outlined in Algorithm 1.

4.4 Privacy analysis

The sub-section analyzes the ability of our FSRPCL framework to protect user privacy in the cross-platform social relationship prediction scenario. We initially introject the concept of vertical federated learning into the social relationship prediction model. Our proposed model guarantees that there is no interaction of raw

Algorithm 1 The whole executive process: FSRPCL.

Input: $B^c_u()$: The behavioral sequence of a user u on each client c

Output: The aggregation parameter: $\bar{\mathbf{W}}$

```
The user rating perturbation process via Eq. (1)
Server initializes the model parameters
For FL_E from 1 to 20 do
  Server-side performs:
    For each client c ∈ Set{c_1, ..., c_z} in parallel do
      set the aggregation parameter W̄
      sent the aggregation parameter W̄ to each client
    End for
  Client-side updates:
  For each local epoch C_E from 1 to 5 do
    execute the embedding features extraction
    capture the dependencies between items
      set the users' overall sequence features and the weight parameter w_u
    upload the model parameter w_c to the server
      download the aggregation parameter W̄ from the server
    execute the multi-tasking training
    optimize model parameters by the Adam optimizer
  End for
End for
```

data among clients and the server refrains from collecting raw data information from individual clients. Furthermore, our model's weight aggregation procedure is confined to the server. Thus, our social relationship prediction model ensures to some extent the protection of users' privacy information.

Even though the users' information contained in the model parameters is implicit, it is feasible for an aggressor to deduce the users' actual data from these model parameters. As stated in Literatures [51, 52], FSRPCL further performs a bounded differential privacy technology during the pretreatment process, whose perturbation ratings' upper bound is $max|\ r^c_{max} - r^c_{min}\ |$, and the corresponding upper bound of the privacy budget is $max|\ r^c_{max} - r^c_{min}\ |/\lambda$[57]. Obviously, a higher value of λ, representing the Laplacian noise intensity, results in a reduced privacy budget. Additionally, a privacy budget that is too small reduces the availability of data and therefore the performance of the social relationship prediction. Consequently, it is imperative to strike a balance between model performance and privacy protection in our devised scheme. Here, to achieve a more robust privacy-preserving effect, we concurrently employ two different views of data augmentation[58], generated by two distinct Laplacian noises, for social relationship prediction. Simultaneously, FSRPCL adopts contrastive learning to minimize the impact of differential privacy technology on the degradation of social relationship prediction performance.

5 Experiment

In this section, we conduct comprehensive experiments on the real-world Epinions dataset[26] to showcase the efficiency and usefulness of FSRPCL. Concurrently, we seek to answer the following research questions (RQs):

RQ1: Does FSRPCL outperform competing baseline approaches for the prediction of social relationships?

RQ2: What components of FSRPCL are essential and beneficial?

RQ3: How do the variations in the Laplacian noise parameter λ settings affect the privacy protection performances of the proposed social relationship prediction model?

RQ4: How is the influence of social relationship prediction performances achieved by the various threshold value σ settings in FSRPCL?

RQ5: What is the impact of the number of platforms on the performances of FSRPCL?

RQ6: How do other hyperparameters affect social relationship prediction performances?

5.1 Experimental environment

(1) Experimental dataset: Table 2 shows that Epinions records contextual information (e.g., category information) and users' behavioral information (e.g., consumption records and rating information). Additionally, the dataset's ratings range from 1 to 5, with 1 indicating low affinity to the item and 5 indicating a strong liking for the item. To simulate multiple clients, we divide different platforms (i.e.,

Table 2 Statistical description of Epinions dataset.

Feature	Numerical value
Users	85000
Items	7557600
Rating	13668319
Category	101140
Social relationships	841372
Start date	10/01/2001
End date	12/08/2003

Table 3 Configuration of FSRPCL.

Configuration	Numerical value
Embedding size	{4, 16, 32}
Number of heads	{1, 5, 8}
Number of platforms	{1, 2, 3}
FL_E	[1, 20]
Transformer block	{1, 2, 3}
λ	[0.1, 1, 10]
MLP shape	1024*512*256
Batch size	32
σ	{0.3, 0.5, 0.7}
Dropout	0.5
C_E	[1, 5]
Learning rate	{1e-3, 1e-5, 1e-7}

$Set\{c_1, ..., c_z\}$) based on the category information described in Table 2. Moreover, we filter out users whose behavioral sequence length is less than 2.

(2) Experimental setup: The paper configures the model parameters as follows:

The experimental running environment has a basic configuration consisting of Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz CPU, 16GB RAM, and an NVIDIA GeForce RTX 2060 GPU for hardware parameters. The software application parameters include Windows 10 and Python 3.7.

(3) Evaluation metrics: As stated in Ref. [25], to assess the performances of FSRPCL, evaluation measures like precision, recall, G_measure, F1-score, and accuracy are applied, where the larger the value in the experimental outcomes, the better the performance in the model.

(4) Comparison approaches: Select several representative comparison approaches to demonstrate and verify FSRPCL's effectiveness and feasibility, including the following:

a. FSRPCL-CL (Contrastive Learning): FSRPCL-CL involves setting the parameter γ in Eq. (18) to 0. The other configurations of this model are consistent with those of the FSRPCL model.

b. FSRPCL-FL (Federated Learning): FSRPCL-FL only leverages information about users' data on a single platform for the social relationship prediction process, without considering information about users' behavioral sequences on multiple platforms.

c. FDRP[42]: FDRP employs the Graph Attention Network to perturb the users' sequence information. Meanwhile, the method uses deep learning and federated learning to predict the social relationships among users.

d. CPSRP[2]: CPSRP applies deep learning networks to extract the temporal sequence features of users and subsequently predict the social relationships among users. Furthermore, the model adopts the improved Simhash technique and differential privacy technology to ensure users' privacy protection.

e. MemTrust[27]: MemTrust mainly applies Long- and Short-Term Memory and MLP networks to extract time-series features of users on a single platform, and further predicts the trust social relationships among users.

f. SHLP[25]: SHLP exclusively relies on information about users' ratings on a single platform to predict social relationships and types of relationships among users, and the method does not train the model using deep learning.

g. SRP-LSH[26]: SRP-LSH leverages only the information of the ratings of users on a single platform to predict the social relationships among users. Compared to SHLP, this method explores the use of social network structure information to further predict social relationships.

h. Guardian[19]: Guardian utilizes convolutional neural networks as its core technology, mining information on the latent traits of users and predicting trust social relationships between any two unrelated users.

5.2 Overall comparison (RQ1)

Figure 3 presents the experimental results positively answering the question **RQ1**. In Fig. 3, the vertical and horizontal axes denote the different performance metrics and the proportion of the training set, respectively, where the proportion of the training set is represented by the form of a set, i.e., {40%, 50%, 60%, 70%, 80%, 90%}.

As Guardian relies heavily on fusing two types of trusted neighbors for trust social relationship prediction, FSRPCL outperforms the method when evaluated on the Epinions dataset. In the majority of instances, the performance metrics of FSRPCL are slightly inferior to those of the other three deep learning-based social relationship models, namely FDRP, MemTrust, and CPSRP. This discrepancy can be attributed to the fact that FDRP, unlike our method, relies solely on the graph attention mechanism for data perturbation without incorporating strict privacy-preserving technologies (such as differential privacy

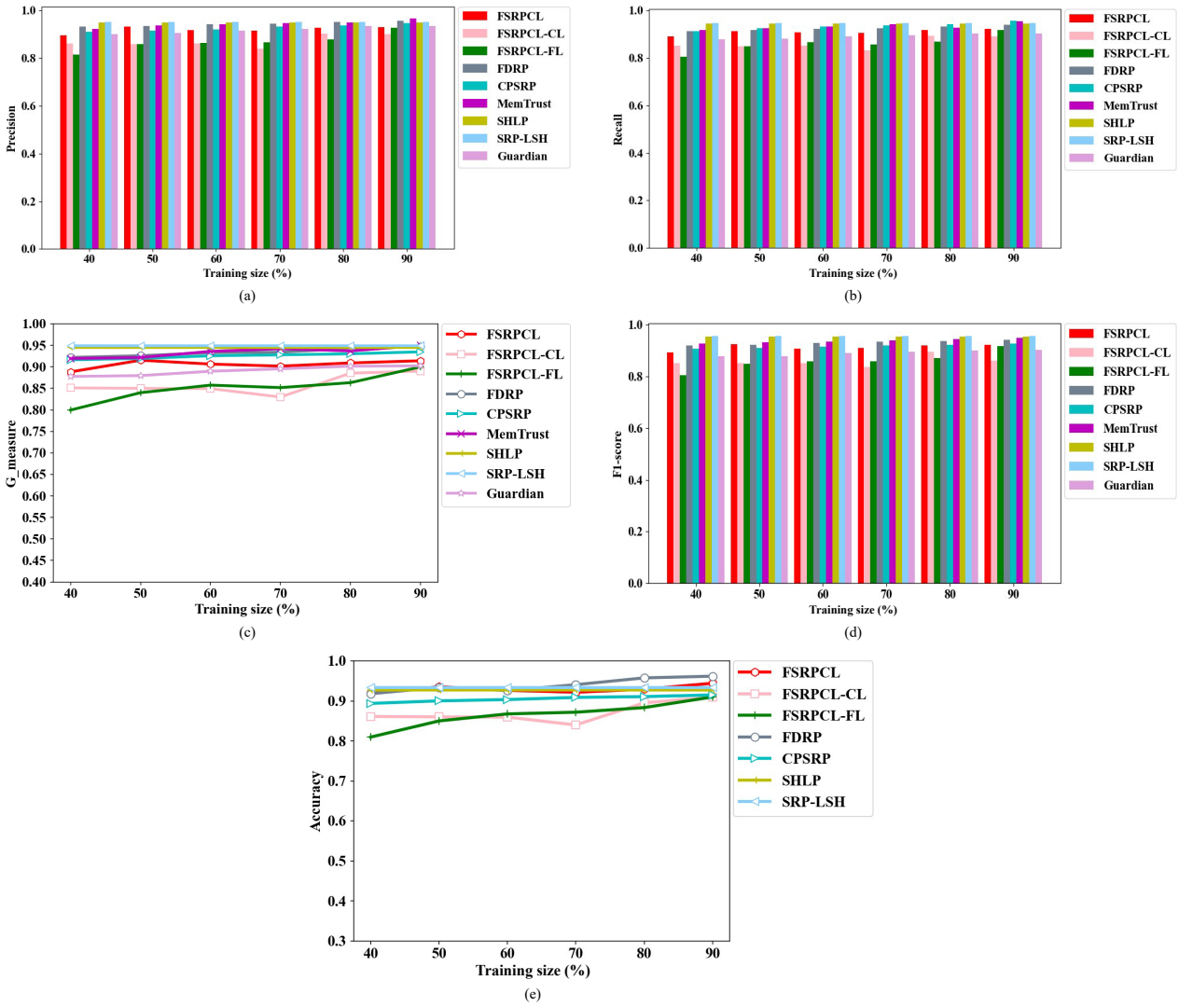


Fig. 3 Performances comparison of different approaches.

and homomorphic encryption) for perturbation. Consequently, the experimental results of FDRP are superior to those of our approach. Similarly, MemTrust attains better experimental results due to its omission of strict privacy-preserving technology for perturbation. Although CPSRP also applies differential privacy technology, it only perturbs groups of users with similar preferences. Furthermore, FSRPCL simultaneously performs two different differential privacy operations for social relationship prediction, so the corresponding experimental effectiveness is slightly lower than that of CPSRP. In addition, both SHLP and SRP-LSH mainly predict social relationships on user data stored in a centralized manner, and these two approaches neglect the implementation of stringent privacy-preserving technology. As a result, the overall performance metrics of our model are lower than those of these two models. Note that, we only evaluate four performance metrics (i.e., precision, recall, G_measure, and F1-score) for MemTrust and Guardian, due to the fact that these two methods are not utilized for predicting distrust social relationships among users.

In terms of ablation experiments, FSRPCL has shown better overall performances compared to its two variants, namely FSRPCL-CL and FSRPCL-FL. While both FSRPCL and FSRPCL-CL concurrently deploy two different differential privacy operations for social relationship prediction, FSRPCL additionally employs the contrastive learning process to pull the perturbation effects of the two different differential privacy operations. As such, FSRPCL achieves better experimental results, indirectly demonstrating that the contrastive learning process can effectively reduce the impact of differential privacy technology on the

performances of social relationship prediction. In addition, FSRPCL yields superior experimental outcomes compared to FSRPCL-FL because the federated learning framework enables the FSRPCL model to gather feature information from the same user across various platforms.

In Fig. 3, the overall performances of all social relationship prediction methods generally improve as the proportion of the training set increases. Indeed, the validity and feasibility of FSRPCL are further demonstrated by the experimental results of G_measure, F1-score and accuracy. As anticipated, the integration of differential privacy technology, contrastive learning, deep learning, and federated learning in the realm of big data can effectively model users' preference information from a cross-platform standpoint, and simultaneously implement more stringent protection measures for users' sensitive information, thereby providing secure and effective social relationship prediction services.

5.3 Effect of framework components (RQ2)

To provide additional evidence supporting the practicality of our model, we analyze the convergence of the two main components of our proposed model, namely FSRPCL-CL and FSRPCL-FL. This analysis is conducted using two evaluation metrics, F1-score and accuracy, on the Epinions dataset. Figure 4 describes the corresponding experimental results, with the vertical axis representing different performance metrics and the horizontal axis representing training epochs.

As shown in Fig. 4a, our model and its two variants (i.e., FSRPCL-CL and FSRPCL-FL) essentially reach a relatively stable state, also known

as a converged state, at a training epoch of 40. The three models depicted in Fig. 4b exhibit smooth fluctuations within the range of 0.8 to 0.95. Furthermore, during the later stages of the training epoch, the F1-score and accuracy values of the three methods exhibit minimal fluctuations, eventually achieving their optimal values. In combination, contrastive learning and federated learning facilitate the comprehensive integration of user preference information from various platforms, ensuring the safety and effectiveness of the task of predicting social relationships.

5.4 Effect of Laplacian noise parameters (RQ3)

In this analysis, we examine two distinct parameters of

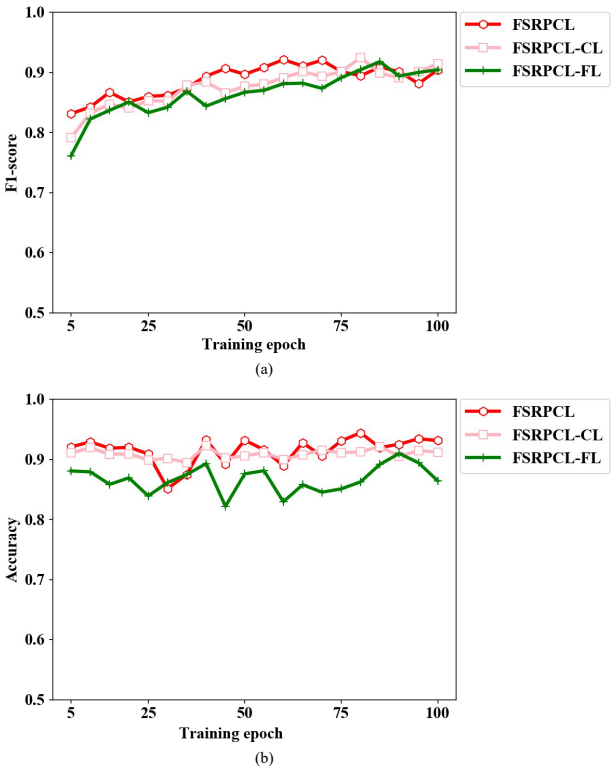


Fig. 4 Effect of framework components.

differential privacy in FSRPCL, as well as the security of our proposed model, in order to provide a more comprehensive response to **RQ3**. Essentially, our model applies the more stringent differential privacy technology, which effectively mitigates the risk of inference attacks by potential adversaries, specifically based on users' rating data. To highlight the impact of privacy-preserving parameters, specifically the Laplacian noise parameter, λ, on the performance of the proposed model, we conduct experiments using a series of various sets of parameters (i.e., $\{\lambda_1, \lambda_2\}$) and then evaluate the model's performance based on two criteria, i.e., F1-score and accuracy.

Table 4 shows the effect of the set of privacy-preserving parameters $\{\lambda_1, \lambda_2\}$ on the performance of FSRPCL, with the best outcomes in each column emphasized in bold. The privacy-preserving parameter λ ranges from the set $\{0.1, 1, 10\}$, and the higher value of λ indicates a greater level of perturbation applied by the differential privacy technology to the users' rating information, resulting in a more effective reduction in the authenticity of the users' data information. With different training set scales, Table 4 reveals that the optimal results in terms of F1-score and accuracy of our model are achieved when $\{\lambda_1, \lambda_2\} = \{0.1, 1\}$, compared to other scenarios. In addition, in

Table 4 Impact of the privacy-preserving parameter λ.

Training size		40%	50%	60%	70%	80%	90%
F1-score	$\{\lambda_1, \lambda_2\} = \{0.1, 1\}$	**0.8923**	**0.9234**	**0.9084**	**0.9105**	**0.9201**	**0.9211**
	$\{\lambda_1, \lambda_2\} = \{0.1, 10\}$	0.8857	0.9196	0.8898	0.9005	0.9153	0.9046
	$\{\lambda_1, \lambda_2\} = \{1, 10\}$	0.8813	0.9132	0.8974	0.8995	0.9004	0.8965
Accuracy	$\{\lambda_1, \lambda_2\} = \{0.1, 1\}$	**0.9183**	**0.9353**	**0.9264**	**0.9216**	**0.9291**	**0.9441**
	$\{\lambda_1, \lambda_2\} = \{0.1, 10\}$	0.9001	0.9257	0.9006	0.9107	0.9154	0.9287
	$\{\lambda_1, \lambda_2\} = \{1, 10\}$	0.8998	0.9102	0.9001	0.8999	0.9078	0.9201

conjunction with Fig. 4, contrastive learning can be proven to be effective in reducing the influence of two differential privacy operations on the performance of social relationship prediction. In conclusion, our proposed model is capable of achieving social relationship prediction more securely and effectively.

5.5 Effect of threshold values (RQ4)

To respond to **RQ4** more thoroughly, we investigate the effect of the threshold value σ on the prediction of users' social relationships according to Fig. 5. Theoretically, adjusting the thresholds in the social relationship prediction model to higher or lower values leads to more rigorous conditions for establishing trust or distrust among users in social relationships. Therefore, we only measure F1-score and accuracy with thresholds of 0.3, 0.5, and 0.7 during various training epochs, i.e., {5, 25, 50, 75,100}.

As shown in Fig. 5, the F1-score and accuracy values of FSRPCL increase with the increase of training epochs. Moreover, FSRPCL attains its highest performance when the threshold value is 0.5.

Therefore, setting the threshold value appropriately allows our proposed social relationship prediction model to achieve optimal experimental results.

5.6 Effect of the number of platforms (RQ5)

To respond to **RQ5**, we investigate the influence

of varying numbers of platforms in predicting social relationships, and consequently, the potential impact of federated learning on the proposed model. In Fig. 6, we evaluate three different evaluation criteria for F1-score, accuracy, and time, where the thresholds arefixed to {0.3, 0.5, 0.7}, the number of platforms is consistent with {1, 2, 3}, and the training size varies between {40%, 50%, 60%, 70%, 80%, 90%}.

In Figs. 6a and 6b, the F1-score and accuracy values of FSRPCL increase as the number of platforms increases, which is mainly due to the fact that the model can fully utilize user data from multiple

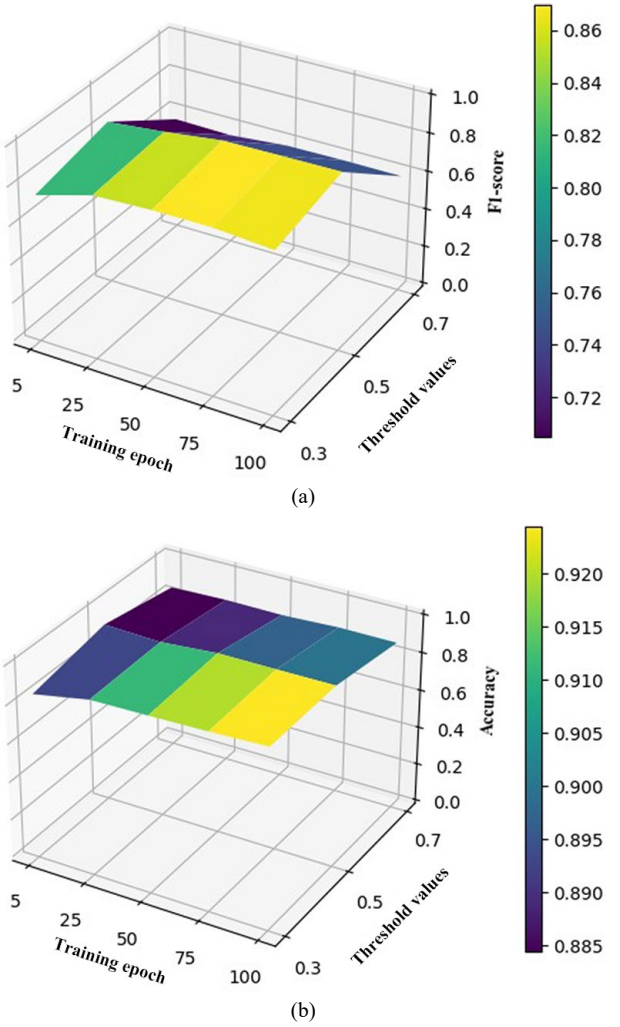


Fig. 5 Effect of threshold values.

platforms for users' feature extraction and the model parameter training. Thus, our model achieves optimal performance when the number of platforms is set to 3. Additionally, as the number of platforms and the training size increase, the time required by the FSRPCL also increases, as demonstrated in Fig. 6c. Similarly, when the number of platforms is 3, our model exhibits the longest processing time. In general, selecting more platforms for prediction, although time-

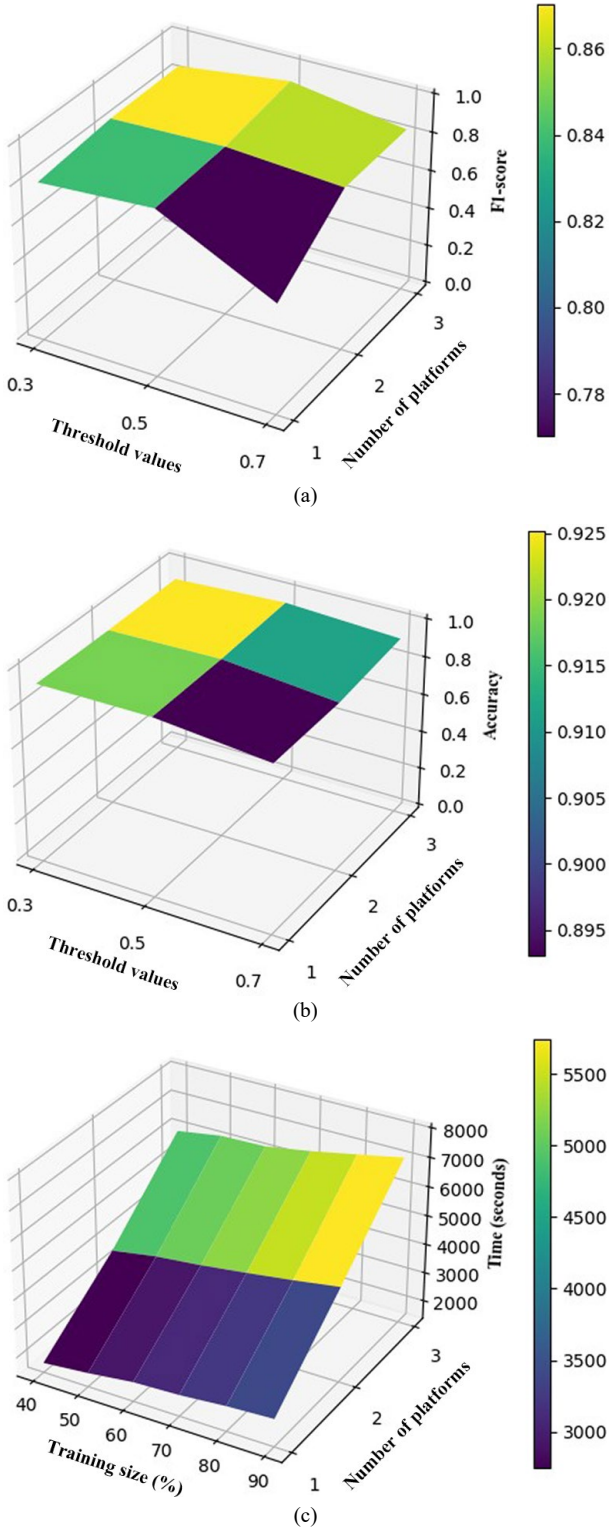


Fig. 6 Effect of the number of platforms.

consuming, can lead to improved prediction outcomes.

5.7 Effect of the hyperparameters (RQ6)

(1) Learning rate analysis. As the learning rate affects the training results achieved by deep learning and contrastive learning, as well as the prediction results achieved by the FSRPCL model, we evaluate the effect of different learning rates on the performance metrics (i.e., F1-score and accuracy). In Fig. 7, the vertical and horizontal axes represent the training ratio and the learning rate, respectively, where the learning rate varies within the range of {le-3, le-5, le-7}. According to Fig. 7, it can be observed that FSRPCL achieves the best experimental results when using the learning rate of 1e-3 compared to the other conditions. The feasibility and validity of our model are further demonstrated by these experiment results.

(2) Convergence analysis. According to Fig. 8, we examine two sets of parameter information (i.e., the training epoch and the training size) to further evaluate the convergence of FSRPCL. In Fig. 8, FSRPCL exhibits relatively stable growth at a training epoch of 80, thus reaching a stable convergence state. Furthermore, optimal performances can be achieved by appropriately adjusting the training epoch and the size

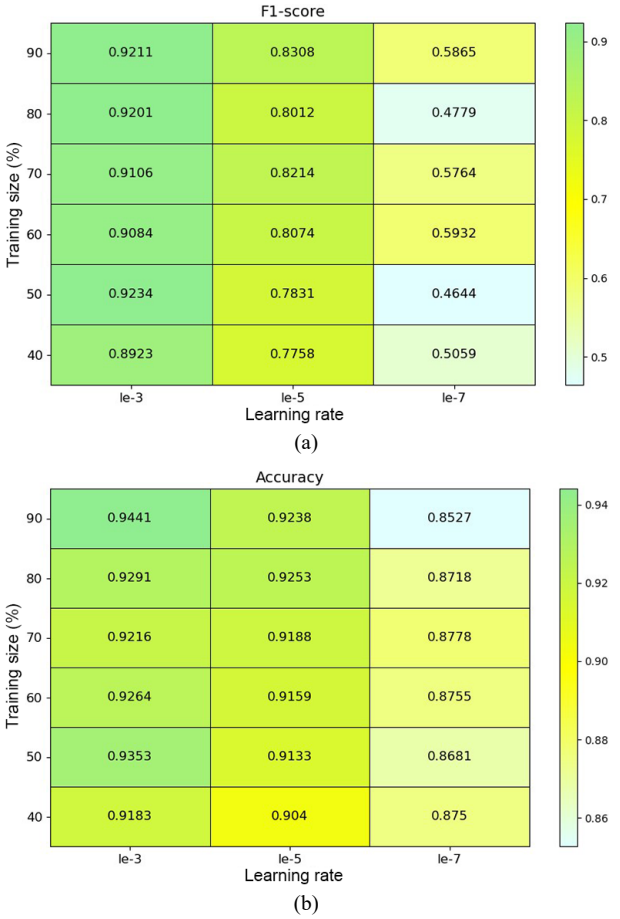
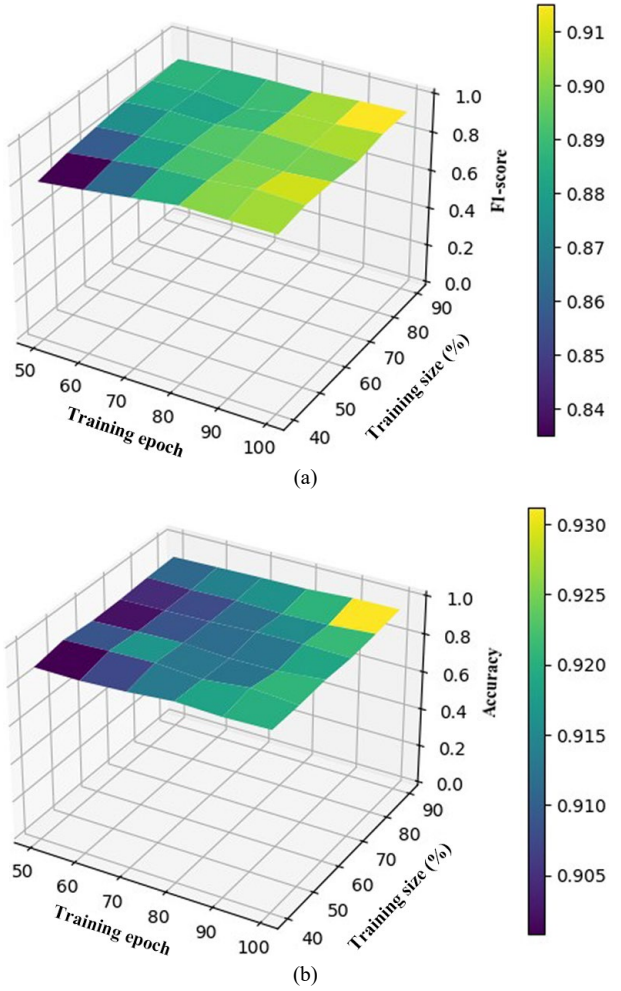


Fig. 7 Effect of the learning rate.



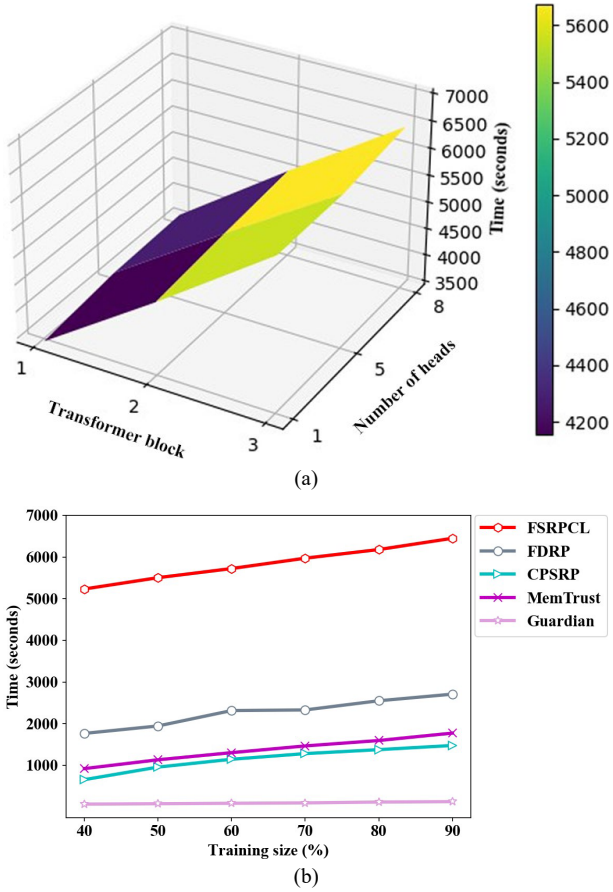
(a)

(b)

Fig. 8 Effect of the learning rate.

of the training set. This is evident from the highest F1-score and accuracy values obtained when the training epoch is set to 90 and the training set comprises 90% of the data.

(3) Time consumption analysis. As depicted in Fig. 9a, we experiment to examine how the number of heads and blocks in the Transformer affects the runtime of FSRPCL. As the number of heads and blocks increases, FSRPCL will require more time for the cross-platform social relationship prediction process. The maximum time taken by FSRPCL occurs when the Transformer has 8 heads and 3 blocks. In Fig. 9b, we further conduct measurements on the time required by various methods for predicting social relationships, where the time consumption of all social relationship methods increases with the size of the training set. Given that FSRPCL involves federated learning, its time overhead is significantly greater compared to the three social relationship prediction



(a)

(b)

Fig. 9 Time consumption.

models, namely Guardian, MemTrust, and CPSRP. Furthermore, when subjected to identical conditions, FSRPCL exhibits substantially higher time overhead than FDRP due to its utilization of contrastive learning.

To answer **RQ6**, we conduct additional research and analysis on the learning rate, convergence, and time consumption. Overall, reasonable parameter settings improve the performance of predicting social relationships among users.

6 Conclusion

In the scenario of predicting cross-platform social relationships, we introduce a new approach called FSRPCL (privacy-preserve Federated Social Relationship Prediction with Contrastive Learning), which is a multi-task learning model relying on vertical federated learning. Specifically, within the big data environment, FSRPCL consists of three main components: The model applies the bounded differential privacy technology to perturb the users' rating information in each client during the pre-processing stage, thus safeguarding against attackers

attempting to deduce the users' preference information through inference attacks. On the client side, the model employs the embedding technique and Transformer to acquire the users' sequence representation information and explore the dependencies among the invoked items in the sequence, which can be applied for the social relationship prediction and the contrastive learning processes. Meanwhile, the contrastive learning process can lessen the influence of the bounded differential privacy technology on the performance of social relationship prediction. Additionally, the client uploads the weighting information to the server and downloads the corresponding global weight information from the server. On the server side, the model gathers the parameter information uploaded by each client and updates the global parameter information via the federated averaging algorithm. The overall comparison of experimental results illustrates that our proposed approach effectively incorporates privacy-preserving mechanisms, deep learning and contrastive learning into the cross-platform social relationship prediction scenario, further demonstrating the effectiveness and stability of FSRPCL in securing users' privacy and ensuring accurate prediction of social relationships.

Although our cross-platform social relationship prediction scheme ensures the performance of social relationship prediction while protecting users' private information, it still suffers from the following weaknesses: (1) We have not taken into account the influence of the information about the network structure in social networks on the scenarios of cross-platform social relationship prediction. (2) We intend to explore cross-platform social relationship prediction schemes using horizontal federated learning and/or federated transfer learning. (3) We consider applying homomorphic encryption and secure multi-party computing to our model to better protect user privacy information. (4) Data imbalance problem: In a big data environment, the user data on each platform should be massive, and thus there should be an imbalance of data among various platforms. Moving forward, we will strive to overcome these limitations and enhance the practicality and precision of cross-platform social relationship prediction schemes.

Acknowledgment

This work was supported by the Jiangsu Province Special Funding for the Transformation of Scientific and Technological Achievements (No. BA2022011), and the Special Fund for Transformation and Upgrading of Industrial and Information Industry of Jiangsu Province (Tackling and Industrialization of Threat Detection and Response System for Industrial Internet Terminals).

References

[1] J. Tang, H. Gao, X. Hu, H. Liu. Exploiting Homophily Effect for Trust Prediction. Proceedings of the Sixth ACM International Conference on Web Search and Data Mining (WSDM'13). Association for Computing Machinery, New York, USA, 2013, pp. 53–62.

[2] H. Liu, L. Qi, S. Shen, A. Khan, S. Meng, Q. Li. Microservice-driven Privacy-aware Cross-Platform Social Relationship Prediction based on Sequential Information. Software: Practice and Experience, vol. 54, no. 1, pp. 85–105, 2024.

[3] Q. Yang, Y. Liu, T. Chen, Y. Tong. Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019.

[4] H. Dai, Y. Xu, G. Chen, W. Dou, C. Tian, X. Wu, T. He. ROSE: Robustly Safe Charging for Wireless Power Transfer. IEEE Transactions on Mobile Computing, vol. 21, no. 6, pp. 2180–2197, 2022.

[5] H. Dai, X. Wang, X. Lin, R. Gu, Y. Liu, W. Dou, G. Chen. Placing Wireless Chargers with Limited Mobility. IEEE Transactions on Mobile Computing, vol. 22, pp. 3589-3603, 2023.

[6] X. Xu, H. Li, Z. Li, X. Zhou. Safe: Synergic data filtering for federated learning in cloud-edge computing. IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1655–1665, 2023.

[7] R. Zeng, B. Mi and D. Huang. A Federated Learning Framework Based on CSP Homomorphic Encryption. 2023 IEEE 12th Data Driven Control and Learning Systems Conference (DDCLS). Xiangtan, China, 2023, pp. 196–201.

[8] J. Konecny, H. B. McMahan, D. Ramage, and P. Richtarik. Federated optimization: Distributed machine learning for on-device intelligence, 2016, doi: 10.48550/arXiv.1610.02527.

[9] X. Xia, F. Chen, Q. He, J. Grundy, M. Abdelrazek, H. Jin. Online Collaborative Data Caching in Edge Computing. IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 2, pp. 281–294, 2021.

[10] B. McMahan, E. Moore, D. Ramage, S. Hampson, B.A. y Arcas. Communication-Efficient Learning of Deep Networks from Decentralized Data, 2016, doi: 10.48550/arXiv.1602.05629.

[11] X. Zhou, X. Zheng, X. Cui, J. Shi, W. Liang, Z. Yan, L. T. Yang, S. Shimizu, and K. Wang. Digital Twin Enhanced Federated Reinforcement Learning with Lightweight Knowledge Distillation in Mobile Networks. IEEE Journal on Selected Areas in Communications, vol. 41, no. 10, pp.

3191–3211, 2023.

[12] P. Tiwari, A. Lakhan, R. H. Jhaveri and T. -M. Grønli. Consumer-Centric Internet of Medical Things for Cyborg Applications Based on Federated Reinforcement Learning. IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 756–764, 2023.

[13] X. Ye. Privacy preserving and delegated access control for cloud applications. Tsinghua Science and Technology, vol. 21, no. 1, pp. 40–54, 2016.

[14] N. A. Jalali, H. Chen. Federated Learning Security and Privacy-Preserving Algorithm and Experiments Research Under Internet of Things Critical Infrastructure. Tsinghua Science and Technology, vol. 29, no. 2, pp. 400–414, 2024.

[15] D. Xu, C. Peng, W. Wang, H. Liu, S. A. Shaikh, Y. Tian. Privacy-Preserving Dynamic Multi-Keyword Ranked Search Scheme in Multi-User Settings. IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 890–901, 2023.

[16] C. Wang, X. Wu, G. Liu, T. Deng, K. Peng, S. Wan. Safeguarding cross-silo federated learning with local differential privacy. Digital Commun. Netw., vol. 8, no. 4, pp. 446–454, 2022.

[17] P. Guo, B. Ye, Y. Chen, T. Li, Y. Yang, X. Qian, X. Yu. A Differential Privacy Protection Protocol Based on Location Entropy. Tsinghua Science and Technology, vol. 28, no. 3, pp. 452–463, 2023.

[18] X. Xie et al. Contrastive Learning for Sequential Recommendation. 2022 IEEE 38th International Conference on Data Engineering (ICDE), Kuala Lumpur, Malaysia, 2022, pp. 1259–1273.

[19] W. Lin, Z. Gao and B. Li. Guardian: Evaluating Trust in Online Social Networks with Graph Convolutional Networks. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, Toronto, ON, Canada, 2020, pp. 914–923.

[20] K. Nan, S. Liu, J. Du, H. Liu. Deep model compression for mobile platforms: A survey. Tsinghua Science and Technology, vol. 24, no. 6, pp. 677–693, 2019.

[21] S. Zhang, L. Yao, A. Sun, Y. Tay. Deep Learning based Recommender System: A Survey and New Perspectives. ACM Computing Surveys, vol. 52, no. 125, pp. 1–38, 2018.

[22] C. Yang, X. Xu, X. Zhou, L. Qi. Deep Q Network–Driven Task Offloading for Efficient Multimedia Data Analysis in Edge Computing–Assisted IoV. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 18, no. 2s, pp. 1–24, 2022.

[23] Q. Chen, H. Zhao, W. Li, P. Huang, W. Ou. Behavior sequence transformer for e-commerce recommendation in Alibaba. Proceedings of the 1st International Workshop on Deep Learning Practice for High-Dimensional Sparse Data. Association for Computing Machinery, New York, USA, 2019, pp. 1–4.

[24] G. F. Angelis, C. Timplalexis, A. I. Salamanis, S. Krinidis, D. Ioannidis, D. Kehagias, D. Tzovaras. Energformer: A New Transformer Model for Energy Disaggregation. IEEE Transactions on Consumer Electronics, vol. 69, no. 3, pp. 308–320, 2023.

[25] H. Kou, H. Liu, Y. Duan, W. Gong, Y. Xu, X. Xu, L. Qi. Building trust/distrust relationships on signed social service network through privacy-aware link prediction process. Applied Soft Computing, vol. 100, no. 5, p. 106942, 2021.

[26] H. Liu, S. Meng, J. Hou, S. Wang, Q. Li, C, Huang. Locality-Sensitive Hashing-based Link Prediction Process on Smart Campus Education or Online Social Platform. Journal of Circuits, Systems, and Computers, vol. 31, no. 9, p. 2250160, 2022.

[27] Y. Xu, Z. Feng, X. Xue, S. Chen, H. Wu, et al. MemTrust: Find Deep Trust in Your Mind. 2021 IEEE International Conference on Web Services (ICWS), Chicago, IL, USA, 2021, pp. 598–607.

[28] Y. Xu, Z. Feng, X. Zhou, M. Xing, H. Wu, X. Xue, S. Chen, C. Wang, L. Qi. Attention-based neural networks for trust evaluation in online social networks. Information Sciences, vol. 630, pp. 507–522, 2023.

[29] J. Ren, Z. Wu. Collaborative Filtering Algorithm Based on Dynamic Trust Attenuation. Proceedings of the 3rd International Conference on Big Data Technologies (ICBDT'2020). Association for Computing Machinery, New York, USA, 2020, pp. 121–125.

[30] L. Qi, X. Xu, X. Wu, Q. Ni, Y. Yuan, X. Zhang. Digital-Twin-Enabled 6G Mobile Network Video Streaming Using Mobile Crowdsourcing. IEEE Journal on Selected Areas in Communications, vol. 41, no. 10, pp. 3161–3174, 2023.

[31] Z. Li, X. Xu, T. Hang, H. Xiang, Y. Cui, L. Qi, X. Zhou. A knowledge-driven anomaly detection framework for social production system. IEEE Transactions on Computational Social Systems, pp. 1–14, 2022.

[32] G. Liu, Q. Chen, Q. Yang, B. Zhu, H. Wang, W. Wang. OpinionWalk: An efficient solution to massive trust assessment in online social networks. IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, Atlanta, GA, USA, 2017, pp. 1–9.

[33] G. Liu, C. Li, Q. Yang. NeuralWalk: Trust Assessment in Online Social Networks with Neural Networks. IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, France, 2019, pp. 1999–200.

[34] X. Zhou, X. Ye, K. Wang, W. Liang, N. K. C. Nair, S. Shimizu, Z. Yan, and Q. Jin. Hierarchical Federated Learning With Social Context Clustering-Based Participant Selection for Internet of Medical Things Applications. IEEE Transactions on Computational Social Systems, vol. 10, no. 4, pp. 1742–1751, 2023.

[35] X. Zhou, W. Liang, K. Wang, Z. Yan, L. T. Yang, W, Wei, J. Ma, and Q. Jin. Decentralized P2P Federated Learning for Privacy-Preserving and Resilient Mobile Robotic Systems. IEEE Wireless Communications, vol. 30, no. 2, pp. 82–89, 2023.

[36] J. Wu, Q. Liu, Z. Huang, Y. Ning, H. Wang, E. Chen, J. Yi, B. Zhou. Hierarchical personalized federated learning for user modeling. Proceedings of the Web Conference 2021. Association for Computing Machinery, New York, USA, 2021, pp. 957–968.

[37] F. Wang, G. Li, Y. Wang, W. Rafique, M. R. Khosravi, G. Liu, Y. Liu, L. Qi. Privacy-aware Traffic Flow Prediction based on Multi-party Sensor Data with Zero Trust in Smart City. ACM Transactions on Internet Technology, vol. 23, no. 3, pp. 1–19, 2023.

[38] K. Ganju, Q. Wang, W. Yang, C. A. Gunter, N. Borisov. Property Inference Attacks on Fully Connected Neural Networks using Permutation Invariant Representations. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Association for Computing Machinery, New York, USA, 2018, pp. 619–633.

[39] G. Lin, F. Liang, W. Pan, Z. Ming. Fedrec: Federated recommendation with explicit feedback. IEEE Intelligent Systems, vol. 36, no. 5, pp. 21−30, 2021.

[40] D. Chai, L. Wang, K. Chen, Q. Yang. Secure Federated Matrix Factorization. IEEE Intelligent Systems, vol. 36, no. 5, pp. 11−20, 2021.

[41] X. Jiang, B. Liu, J. Qin, Y. Zhang, J. Qian. FedNCF: Federated Neural Collaborative Filtering for Privacy-preserving Recommender System. 2022 International Joint Conference on Neural Networks (IJCNN), Padua, Italy, 2022, pp. 1−8.

[42] H. Liu, N. Li, H. Kou, S. Meng, Q. Li. FDRP: Federated Deep Relationship Prediction with Sequential Information. Wireless Network, 2023, doi: 10.1007/s11276-023-03530-2.

[43] J. Wu, X. Wang, F. Feng, X. He, L. Chen, J. Lian, X. Xie. Self-supervised Graph Learning for Recommendation. Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval. Association for Computing Machinery, New York, USA, 2021, pp. 726−735.

[44] R. Gu, Y. Chen, S. Liu, H. Dai, G. Chen, K. Zhang, Y. Che, Y. Huang. Liquid: Intelligent Resource Estimation and Network-Efficient Scheduling for Deep Learning Jobs on Distributed GPU Clusters. IEEE Transactions on Parallel and Distributed Systems, vol. 33, no. 11, pp. 2808−2820, 2022.

[45] R. Gu, K. Zhang, Z. Xu, Y. Che, B. Fan, H. Hou, H. Dai, L. Yi, Y. Ding, G. Chen, Y. Huang. Fluid: Dataset Abstraction and Elastic Acceleration for Cloud-native Deep Learning Training Jobs. 2022 IEEE 38th International Conference on Data Engineering (ICDE), Kuala Lumpur, Malaysia, 2022, pp. 2182−2195.

[46] X. Xu, S. Tang, L. Qi, X. Zhou, F. Dai, W. Dou. CNN Partitioning and Offloading for Vehicular Edge Networks in Web3. IEEE Communications Magazine, vol. 61, no. 8, pp. 36–42, 2023.

[47] Y. Cao, X. Chen, L. Yao, X. Wang, W. E. Zhang. Adversarial Attack and Detection on Reinforcement Learning based Recommendation System. Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval. Association for Computing Machinery, New York, USA, 2020, pp. 1669−1672.

[48] F. Wang, H. Zhu, G. Srivastava, S. Li, M. R. Khosravi, L. Qi. Robust Collaborative Filtering Recommendation with User-Item-Trust Records. IEEE Transactions on Computational Social Systems, vol.9, no. 4, pp. 986−996, 2022.

[49] K. He, H. Fan, Y. Wu, S. Xie, R. Girshick. Momentum Contrast for Unsupervised Visual Representation Learning. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, USA, 2020, pp. 9726−9735.

[50] Y. Yan, R. Li, S. Wang, F. Zhang, W. Wu, W. Xu. ConSERT: A Contrastive Framework for Self-Supervised Sentence Representation Transfer. Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing. Association for Computational Linguistics, USA, 2021, pp. 5065-5075.

[51] D. Yan, Y. Zhao, Z. Yang, Y. Jin, Y. Zhang. FedCDR: Privacy-preserving federated cross-domain recommendation. Digital Communications and Networks, vol.8, no. 4, pp. 552−560, 2022.

[52] A. Friedman, S. Berkovsky, M. A. Kaafar. A differential privacy framework for matrix factorization recommender systems. User Model User-Adap Inter 26, 2016, doi: 10.1007/s11257-016-9177-7.

[53] H. Dai, J. Yu, M. Li, W. Wang, A. Liu, J. Ma, L. Qi, G. Chen. Bloom Filter with Noisy Coding Framework for Multi-Set Membership Testing. IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 7, pp. 6710−6724, 2023.

[54] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, I. Polosukhin. Attention is all you need. Proceedings of the 31st International Conference on Neural Information Processing System. Association for Computing Machinery, New York, USA, 2017, pp. 6000–6010.

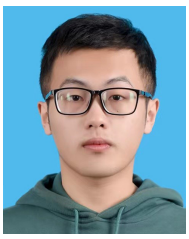
[55] S. Wang, X. Chen, D. Jannach, L. Yao. Causal Decision Transformer for Recommender Systems via Offline Reinforcement Learning. Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval. Association for Computing Machinery, New York, USA, 2023, pp. 1599–1608.

[56] W. Du, S. Tian. Transformer and GAN-Based Super-Resolution Reconstruction Network for Medical Images. Tsinghua Science and Technology, vol. 29, no. 1, pp. 197−206, 2024.

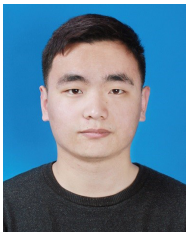
[57] W. -S. Choi, M. Tomei, J. R. S. Vicarte, P. K. Hanumolu, R. Kumar. Guaranteeing Local Differential Privacy on Ultra-Low-Power Systems. 2018 ACM/IEEE 45th Annual International Symposium on Computer Architecture (ISCA), Los Angeles, CA, USA, 2018, pp. 561−574.

[58] B. Zhang, L. Wang. False Negative Sample Detection for Graph Contrastive Learning. Tsinghua Science and Technology, vol. 29, no. 2, pp. 529−542, 2024.

Hanwen Liu received the MS degree from Qufu Normal University, China in 2020. He is now persuing the PhD degree at School of Computer Science and Engineering, Nanjing University of Science and Technology, China. His major is cyberspace security. His research interests include recommender systems, security & privacy, link prediction, social relationship prediction, and big data.



Nianzhe Li received the bachelor degree from School of Nanjing University of Posts and Telecommunications in 2022. He is now a master student at School of Computer Science and Engineering, Nanjing University of Science and Technology, China. His major is software engineering. His research interests include recommender systems, federated Learning, and big data.



Huaizhen Kou is currently a PhD candidate at Nanjing University of Science and Technology. He has received the BS and MS degrees in computer science from Qufu Normal University in 2018 and 2020, respectively. His research interests include Service Computing, Recommender Systems, and Link Prediction.

Shunmei Meng received the PhD degree in Department of Computer Science and Technology from Nanjing University, China, in 2016. Now, she is an assistant professor with School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing, China. She has published papers in international journals and international conferences such as *TPDS*, *TKDD*, *TII*, *WWWJ*, *FGCS*, *COSE*, *CIKM*, *AAAI*, *ICDM*, *ICWS*, and *ICSOC*. Her research interests include recommender systems, cloud computing, security, and privacy.

Qianmu Li received the BSc and PhD degrees from Nanjing University of Science and Technology, China, in 2001 and 2005, respectively. He is a professor with School of Cyber Science and Engineering, Nanjing University of Science and Technology, China. His research interests include information security, computing system management, and data mining. He received the China Network and Information Security Outstanding Talent Award and multiple Education Ministry Science and Technology Awards