Appendix

In this part, we provide an in-depth analysis of the FedPLF model's privacy preservation capabilities, examining two pivotal dimensions:

Part 1: *Resistance to Data Exfiltration*.

In traditional centralized hashing algorithms, each client needs the user's private data to be uploaded to a high-computing power cloud server for centralized training. However, the sharing of sensitive data and the uncontrollable flow of data lead to the model of centralized training that can be potentially risky for privacy leakage and security [1]. FedPLF is trained in the framework of FL, which saves the private data locally, and there will be no possibility of the raw data being captured by a malicious server.

Part 2: *Protection Against Parameter Inference*.

In the realm of related research [2-6], it is widely accepted that a client's raw data $r_{u,i}$ and the representation vector w_u that characterizes the user's preferences are considered as the user's private information. Zhu et al. [7] suggests that if the gradient information used for updating the global model, as uploaded by the client, becomes known, the client's raw data can potentially be inverted.

Within the framework of real-value-based FL, it is hypothesized that if a malicious attacker were to obtain the public model F according to (3) and captured the gradient information ∇y_i^u of all items uploaded by the client u, and obtained the items' representation matrix Y, then generate pseudo-representation $\dot{x}_u$ and pseudo-rating $\dot{r}_{u,i}$. These pseudo-values are iteratively refined by the following objective function, aiming to converge towards their real values and thus posing a risk of privacy leakage:

$$\arg\min_{\substack{\dot{x}_u \in \mathbb{R}^{|I| \times D} \\ \dot{r}_{u,i} \in \mathbb{R}}} \left\| \frac{\partial l\left(F\left(\dot{x}_u, y_i\right), \dot{r}_{u,i}\right)}{\partial y_i} - \nabla y_i^u \right\| \tag{18}$$

However, in our model, the objective function of FedPLF is non-derivable, and all parameters are discrete, which inherently prevents the use of gradient-based attacks. Additionally, an irreversible sign function is integrated into the framework to further obscure the true gradient information, thereby ensuring privacy. We can substantiate this through theoretical analysis.

Firstly, we set aside the regularization parameters α and β. Based on the (14), we can deduce that $\sum \Delta q_{l,k}^u(t)$ serves as the guidance factor $q_{i,k}^*(t)$. Suppose attackers obtain the binary representations $q_i^{(t)}$ and $q_i^{(t+1)}$ of item i in different iteration rounds, and also acquires the public "gradient-like" term $\Delta Q_{u,k}(t) = [\Delta \hat{q}_{1,k}^u(t), \Delta \hat{q}_{2,k}^u(t), \ldots, \Delta \hat{q}_{|I_u|,k}^u(t)]$ uploaded from clients. According to (19), we have the following equation:

$$\Delta \hat{q}_{i,k}^{u\,(t)} = sign\left(\Delta q_{i,k}^{u\,(t)}\right) \tag{19}$$

$$\Delta q_{i,k}^{u\,(t)} = \left(r_{u,i} - \left(w_{u,k'}{}^T q_{i,k'}{}^{(t)} - \sum w_{u,k'} + \sum q_{i,k'}{}^{(t)} - 1\right)\right)\left(w_{u,k} + 1\right) \tag{20}$$

Where sign(·)sign(·) denotes the sign function. It is evident that for each parameter, the value is either +1 or -1. Following this, we discuss why FedPLF can maintain the privacy of clients' local data. According to (19) and (20), even if an attacker attempts to derive $r_{u,i}$ and w_u from the following sets of equations:

$$\begin{cases} \Delta q_{i,k}^{u\,(1)} = \left(r_{u,i} - \left(w_{u,k'}{}^T q_{i,k'}{}^{(1)} - \sum w_{u,k'} + \sum q_{i,k'}{}^{(1)} - 1\right)\right)\left(w_{u,k} + 1\right) \\ \Delta q_{i,k}^{u\,(2)} = \left(r_{u,i} - \left(w_{u,k'}{}^T q_{i,k'}{}^{(2)} - \sum w_{u,k'} + \sum q_{i,k'}{}^{(2)} - 1\right)\right)\left(w_{u,k} + 1\right) \\ \quad \ldots \\ \Delta q_{i,k}^{u\,(R)} = \left(r_{u,i} - \left(w_{u,k'}{}^T q_{i,k'}{}^{(R)} - \sum w_{u,k'} + \sum q_{i,k'}{}^{(R)} - 1\right)\right)\left(w_{u,k} + 1\right) \end{cases} \tag{21}$$

If $\Delta \hat{q}_{i,k}^u(t) \neq 0$, the attacker can only determine that $\Delta q_{i,k}^u(t) > 0$ or $\Delta q_{i,k}^u(t) < 0$, but not the exact value. Thus, they cannot ascertain $r_{u,i}$ and w_u from (21). If $\Delta \hat{q}_{i,k}^u(t) = 0$, the only conclusion is that $\Delta q_{i,k}^u(t) = 0$. Even if the attacker expands (22) by the dimension D to (23):

$$\begin{cases} \Delta q_{i,1}^{u\,(t)} = \left(r_{u,i} - \left(w_{u,1'}{}^T q_{i,1'}{}^{(t)} - \sum w_{u,1'} + \sum q_{i,1'}{}^{(t)} - 1\right)\right)\left(w_{u,1} + 1\right) \\ \Delta q_{i,2}^{u\,(t)} = \left(r_{u,i} - \left(w_{u,2'}{}^T q_{i,2'}{}^{(t)} - \sum w_{u,2'} + \sum q_{i,2'}{}^{(t)} - 1\right)\right)\left(w_{u,2} + 1\right) \\ \quad \ldots \\ \Delta q_{i,D}^{u\,(t)} = \left(r_{u,i} - \left(w_{u,D'}{}^T q_{i,2'}{}^{(t)} - \sum w_{u,2'} + \sum q_{i,2'}{}^{(t)} - 1\right)\right)\left(w_{u,D} + 1\right) \end{cases} \tag{22}$$

$$\begin{cases} \Delta q_{i,1}^{u\,(t+1)} = \left(r_{u,i} - \left(w_{u,1'}{}^T q_{i,1'}{}^{(t+1)} - \sum w_{u,1'} + \sum q_{i,1'}{}^{(t+1)} - 1\right)\right)\left(w_{u,1} + 1\right) \\ \Delta q_{i,2}^{u\,(t+1)} = \left(r_{u,i} - \left(w_{u,2'}{}^T q_{i,2'}{}^{(t+1)} - \sum w_{u,2'} + \sum q_{i,2'}{}^{(t+1)} - 1\right)\right)\left(w_{u,2} + 1\right) \\ \quad \ldots \\ \Delta q_{i,D}^{u\,(t+1)} = \left(r_{u,i} - \left(w_{u,D'}{}^T q_{i,2'}{}^{(t+1)} - \sum w_{u,2'} + \sum q_{i,2'}{}^{(t+1)} - 1\right)\right)\left(w_{u,D} + 1\right) \end{cases} \tag{23}$$

However, it is worth noting that the premise of (22) and (23) hold on is that $\Delta \hat{q}_{i,k}^u(t) = q_{i,k}^*(t) = 0$, $\Delta \hat{q}_{i,k}^u(t+1) = q_{i,k}^*(t+1) = 0$, which is a scenario that highlights the infeasibility of the classical DCD optimization algorithm.

REFERENCES

[1] D. Hou, J. Zhang, J. Ma, X. Zhu, and K. L. Man, "Application of differential privacy for collaborative filtering based recommendation system: A survey," in *Proc. 12th Int. Symp. Parallel Architectures, Algorithms Program. (PAAP)*, Dec. 2021, pp. 97–101.

[2] D. Chai, L. Wang, K. Chen, and Q. Yang, "Secure Federated Matrix Factorization," *IEEE Intell. Syst.,* vol. 36, no. 5, pp. 11–20, Sep. 2021.

[3] Y. Lin *et al.*, "Meta Matrix Factorization for Federated Rating Predictions," in *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval*, in SIGIR '20. New York, NY, USA: Association for Computing Machinery, Jul. 2020, pp. 981–990.

[4] G. Lin, F. Liang, W. Pan, and Z. Ming, "FedRec: Federated recommendation with explicit feedback," *IEEE Intell. Syst.*, vol. 36, no. 5, pp. 21–30, Sep. 2021.

[5] M. M. Rahimi, H. I. Bhatti, Y. Park, H. Kousar, and J. Moon, "EvoFed: Leveraging Evolutionary Strategies for Communication-Efficient Federated Learning," in Advances in *Neural Information Processing Systems*, *A. Oh, T. Naumann, A. Globerson, K. Saenko, M. Hardt, and S. Levine, Eds., Curran Associates, Inc.*, 2023, pp. 62428–62441.

[6] H. Zhang, F. Luo, J. Wu, X. He, and Y. Li, "LightFR: Lightweight Federated Recommendation with Privacy-preserving Matrix Factorization," *ACM Trans. Inf. Syst.,* p. 3578361, Dec. 2023.

[7] L. Zhu, Z. Liu, and S. Han, "Deep Leakage from Gradients," *in Advances in Neural Information Processing Systems, Curran Associates, Inc.,* 2019.