A Lightweight Hashing-Based Approach for Privacy-Preserving IOT Service Recommendation

Erolla Abhinav, department of Computer Science and Engineering, GNITC, 22-584, 22wj1a0584gniindia.org@gmail.com
Dupally Bhanu Prasad Reddy, department of Computer Science and Engineering, GNITC, 22-577, 22wj1a0577@gniindia.org
Gaddam Srinitha, department of Computer Science and Engineering, GNITC, 22-585, 22wj1a0585@gniindia.org
Dr. N. Srihari Rao, Professor, department of Computer Science and Engineering, GNITC, sriharirao.csegnitc@gniindia.org

---***---

Abstract- Data about user-service interactions is frequently kept across several dispersed platforms in the context of the Internet of Things (IoT). In order to make a thorough recommendation decision in this scenario, recommender systems must integrate the dispersed user-service interaction data from several platforms, which likely exposes user privacy. Furthermore, the efficiency of recommendations is greatly diminished as user-service interaction records mount up over time. We suggest a lightweight, privacy-preserving service recommendation method called SerRecL2H to address these problems. To efficiently identify customers with similar preferences for precise suggestions, SerRecL2H uses Learning to Hash (L2H) to encapsulate sensitive user-service interaction data into less-sensitive user indices.

Key Words: Internet of Things (IoT), Service Recommendation, Privacy Preservation, Learning to Hash (L2H), Distributed Systems, Hashing Techniques.

1.INTRODUCTION

In the era of big data, recommender systems analyze user–service interaction data to identify user preferences and provide personalized recommendations. With the rapid growth of the Internet of Things (IoT), large volumes of interaction data are generated by smart devices and distributed across multiple platforms, creating challenges in data integration, privacy protection, and system efficiency. Integrating multi-source data may expose sensitive user information and increase computational complexity. To address these issues, this work proposes SerRecL2H, a lightweight privacy-preserving IoT service recommendation approach. The system uses the Learning to Hash (L2H) technique to transform sensitive interaction data into compact hashed user indices that preserve similarity while protecting privacy. Based on these hashed representations, the system efficiently identifies users with similar preferences and generates personalized recommendations. Experimental evaluation demonstrates that the proposed approach improves recommendation efficiency and scalability while ensuring user privacy in distributed IoT environments.

2. LITERATURE REVIEW

The rapid growth of Internet of Things (IoT) technologies has significantly increased the amount of user–service interaction data generated by smart devices, creating new opportunities and challenges for service recommendation systems. Researchers have proposed various techniques to improve recommendation accuracy and efficiency. Lin et al. (2024) introduced a deep neural collaborative filtering method that integrates multi-source interaction data from cloud and edge environments to enhance recommendation performance. Although the approach improves prediction accuracy, it requires high computational resources and centralized data processing, which may raise privacy concerns. Ma et al. (2023) proposed a social graph neural network–based recommendation scheme that utilizes social relationships and user–item interactions to generate personalized recommendations. While this approach improves recommendation quality, the use of graph neural networks increases computational complexity and memory requirements. Similarly, Li et al. (2024) developed a knowledge-driven anomaly detection framework that combines machine learning with domain knowledge to detect abnormal patterns in large-scale systems; however, it relies heavily on extensive domain knowledge and computational resources. Xu et al. (2023) proposed a federated learning–based framework called SAFE, which enables collaborative model training across cloud-edge environments without sharing raw data, thereby improving privacy protection. Despite these advancements, many existing approaches rely on complex deep learning models, centralized architectures, or heavy computational operations, which limit their applicability in distributed and resource-constrained IoT environments. To address these challenges, the proposed system introduces a lightweight hashing-based approach called SerRecL2H, which uses the Learning to Hash (L2H) technique to convert sensitive user–service interaction data into compact hashed user indices. This approach preserves similarity among users while protecting privacy and enables efficient service recommendation in distributed IoT systems.

3. RELATED WORK

Recent advancements in Internet of Things (IoT) technologies have led to the rapid growth of user–service interaction data, making service recommendation an important research area. Several studies have explored machine learning and deep learning techniques to improve recommendation accuracy and efficiency. Lin et al. (2024) proposed a deep neural collaborative filtering method for service recommendation in cloud–edge environments. Their approach integrates multi-source interaction data to capture complex relationships between users and services, resulting in improved recommendation performance. However, the reliance on deep neural networks increases computational complexity and requires centralized data processing, which may expose sensitive user information. Ma et al. (2023) introduced a social graph neural network–based recommendation system that utilizes social relationships and user–item interactions to generate personalized recommendations. By modeling user connections through graph neural networks, the method captures complex relational patterns and improves recommendation accuracy. Despite its advantages, the approach requires significant computational resources and memory, making it less suitable for resource-constrained IoT environments. Li et al. (2024) proposed a knowledge-driven anomaly detection framework that combines domain knowledge with machine learning techniques to identify abnormal behaviors in large-scale systems. Although the framework enhances detection accuracy and system reliability, its dependency on extensive domain knowledge and large computational resources limits scalability in distributed IoT environments. Xu et al. (2023) presented SAFE, a federated learning-based framework designed for cloud–edge collaboration. The framework filters low-quality or redundant data at the edge level to improve model training efficiency while preserving data privacy. Federated learning allows collaborative training without sharing raw user data; however, the approach mainly focuses on training optimization rather than efficient recommendation generation. Additionally, Yang and Esquivel (2024) proposed a time-aware Long Short-Term Memory (LSTM) model that captures temporal patterns in user behavior for dynamic recommendation systems. While this model improves prediction accuracy by considering time-based interactions, it requires high computational power and centralized processing of large datasets. Although these approaches contribute to improving recommendation quality and system intelligence, many of them rely on complex deep learning models or centralized architectures that may not be suitable for large-scale distributed IoT environments. Furthermore, heavy computation and high storage requirements can limit real-time performance in resource-constrained systems. To overcome these limitations, this work proposes a lightweight hashing-based recommendation framework called SerRecL2H. The proposed system utilizes the Learning to Hash (L2H) technique to transform sensitive user–service interaction data into compact hash-based user indices. These hashed representations preserve user preference similarity while protecting sensitive data and enabling efficient similarity search. As a result, the proposed approach provides a scalable, privacy-preserving, and computationally efficient solution for service recommendation in distributed IoT environments.

4. PROPOSED METHODOLOGY

The proposed system introduces SerRecL2H, a lightweight and privacy-preserving IoT service recommendation framework designed to address the challenges of privacy leakage, scalability, and computational efficiency in distributed IoT environments. In modern IoT systems, a large volume of user–service interaction data is generated by smart devices such as sensors, wearable devices, and mobile applications. These interaction records are often distributed across multiple platforms including cloud servers and edge devices. Integrating such distributed data is essential for accurate recommendation generation, but direct data sharing may expose sensitive user information and increase computational overhead. Therefore, the proposed methodology focuses on transforming sensitive interaction data into secure and compact representations that enable efficient recommendation without revealing raw user data.

The core component of the proposed framework is the **Learning to Hash (L2H)** technique, which converts high-dimensional user–service interaction data into compact hash-based user indices. Instead of storing or processing raw interaction records, the system generates hash codes that preserve similarity among users with similar preferences. This transformation significantly reduces data dimensionality while protecting user privacy. The architecture of the system includes several modules such as data collection, hashing transformation, similarity computation, and recommendation generation. In the initial stage, interaction data generated by IoT devices is collected and preprocessed. The L2H module then processes this data and converts it into compact hash representations that can be efficiently stored and compared for recommendation tasks.

To ensure data integrity and reliability, the system also incorporates a **file hashing mechanism using the SHA-256 algorithm**, which generates a unique hash value for each interaction record. These hash values act as digital fingerprints that help detect any unauthorized modification of stored data. After generating the hashed user indices, the system performs similarity search to identify users with similar preferences. By comparing hashed representations rather than raw interaction data, the recommendation engine efficiently generates personalized service recommendations. This approach improves computational efficiency, enhances scalability, and ensures strong privacy protection, making the proposed SerRecL2H framework suitable for large-scale IoT service recommendation environments.

5. RESULTS AND DISCUSSION

The proposed **SerRecL2H** framework effectively generates privacy-preserving IoT service recommendations. It converts sensitive interaction data into compact hashed indices using the **Learning to Hash (L2H)** technique. The results show improved efficiency, scalability, and privacy protection in distributed IoT environments.

Home Page

The **home page** serves as the main interface of the IoT service recommendation system. It displays the project title and provides navigation to modules such as Consumer Panel, Cloud Server Panel, User Panel, and Smart Contracts. The page offers a simple and interactive dashboard that allows users to access system features and manage services efficiently.

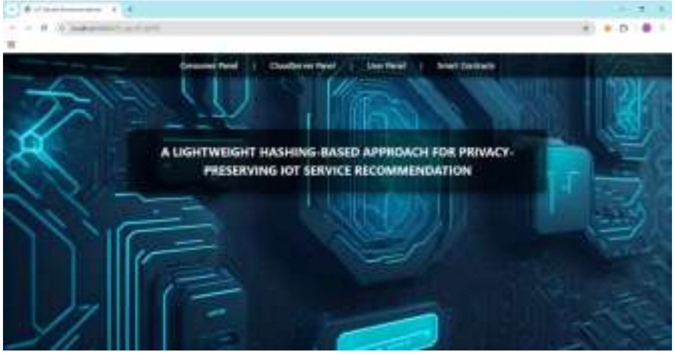
Consumer Panel
CloudServer Panel
User Panel
Smart Contracts
A LIGHTWEIGHT HASHING-BASED APPROACH FOR PRIVACY-PRESERVING IOT SERVICE RECOMMENDATION

Fig 1: Home page of the project

User Registration Page

The **User Registration page** allows new users to create an account by entering details such as name, email, password, phone number, age, gender, and address. After registration, users can securely access the system and use IoT service recommendation features.

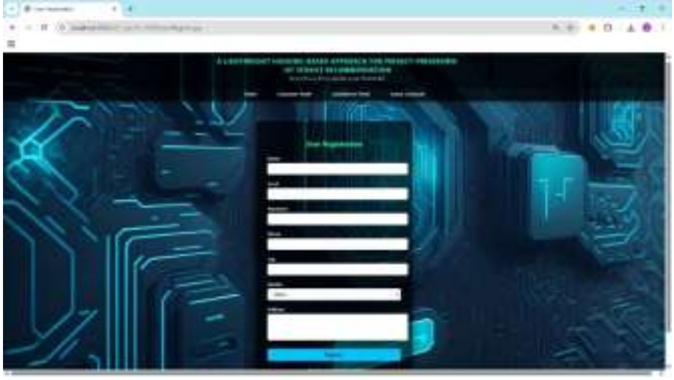

Fig 2: User registration interface

Consumer login Page

The Consumer Registration page enables consumers to create an account by entering details such as name, email, password, phone number, age, gender, and address. After registration, consumers can log in and upload IoT service data.

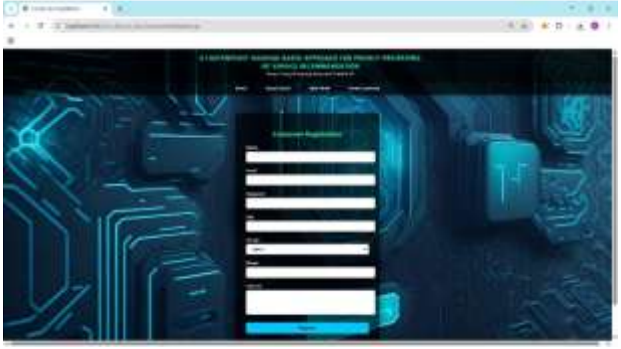

Fig 3: Consumer login interface

Employer Login Page

The Cloud Server Login page allows the administrator or cloud server to securely access the system by entering a valid email and password. After successful login, the cloud server can manage uploaded data, user requests, and recommendation processes.

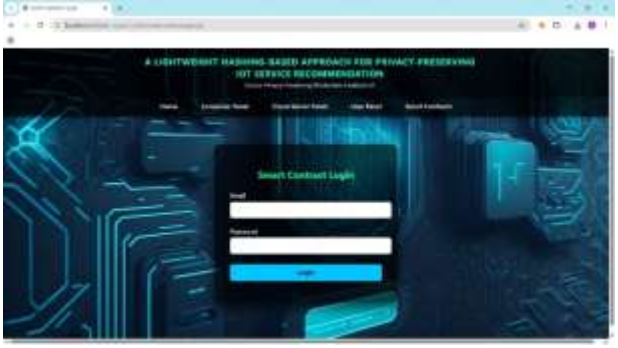
A LIGHTWEIGHT HASHING-BASED APPROACH FOR PRIVACY-PRESERVING
IOT SERVICE RECOMMENDATION
Smart Contract Login
Email
Password
Login

Fig 4: Smart Contract login interface

Smart Contract Portal

The user data requests page allows the cloud server to view and manage requests submitted by users for accessing uploaded data. The server can approve or reject requests, ensuring secure access control and proper management of system data.

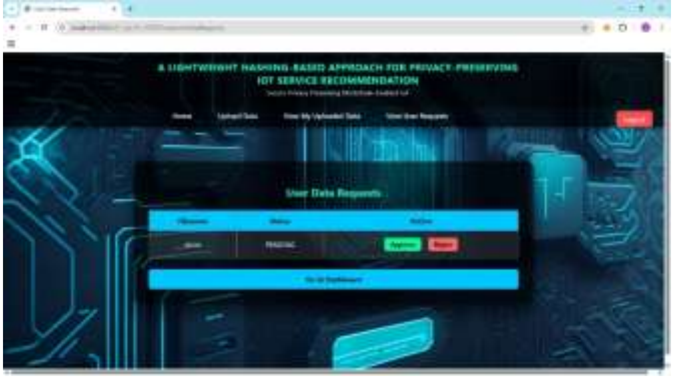
A LIGHTWEIGHT HASHING-BASED APPROACH FOR PRIVACY-PRESERVING
IOT SERVICE RECOMMENDATION
User Data Requests

Fig 5: Approve or Reject by Smart Contract

File Search Interface

The search file page allows users to search for uploaded files by entering the filename. After the search, the system displays the L2H transformed data and the encrypted file hash value. This feature helps users verify files securely and view protected data without revealing the original content.

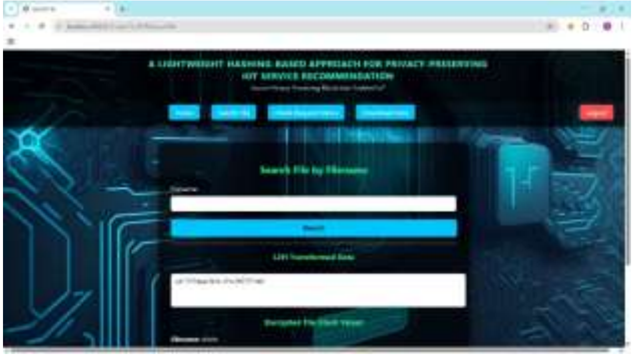
A LIGHTWEIGHT HASHING-BASED APPROACH FOR PRIVACY-PRESERVING
IOT SERVICE RECOMMENDATION
Search File by Filename
Search
L2H Transformed Data

Fig 6: Search by File Name

A LIGHTWEIGHT HASHING-BASED APPROACH FOR PRIVACY-PRESERVING
IOT SERVICE RECOMMENDATION
Private Key Released

Fig 7: Private Key will be Released

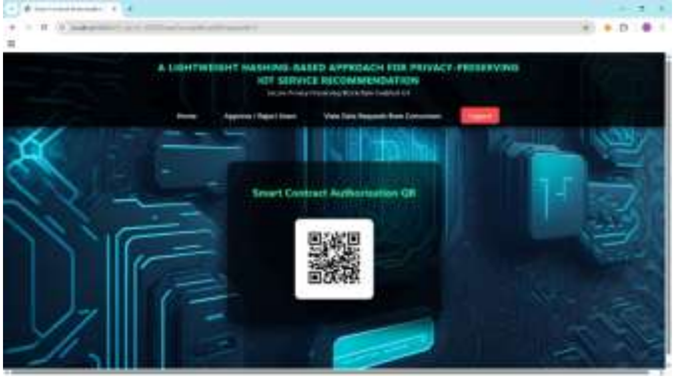
A LIGHTWEIGHT HASHING-BASED APPROACH FOR PRIVACY-PRESERVING
IOT SERVICE RECOMMENDATION
Smart Contract Authorization QR

Fig 8: The Smart Contract Authorization page displays a QR code used for secure authentication and access approval within the IoT service recommendation system.

User Detail Page

The approved users page displays the list of users who have been verified and authorized through the smart contract system. It shows important details such as user ID, name, email, phone number, age, gender, address, and smart contract ID. This page helps the cloud server monitor and manage authenticated users efficiently. It ensures that only approved users are allowed to access system services and data securely..

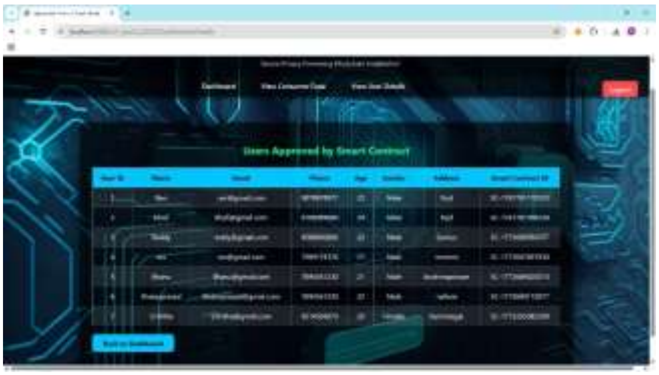

Fig 9: List of Details of the Users

6. CONCLUSION

This project presented a lightweight and privacy-preserving IoT service recommendation system designed to address the challenges of privacy protection, scalability, and computational efficiency in distributed environments. With the rapid growth of the Internet of Things (IoT), large volumes of user–service interaction data are continuously generated through smart devices such as sensors, wearable devices, and mobile applications. Traditional recommendation systems often rely on centralized data processing, which may expose sensitive user information and increase system complexity. Therefore, there is a strong need for efficient methods that can generate accurate service recommendations while maintaining user privacy and reducing computational overhead.

To overcome these challenges, the proposed system introduced SerRecL2H**,** a lightweight hashing-based recommendation framework. The core concept of the system is based on the Learning to Hash (L2H) technique, which transforms sensitive user–service interaction data into compact and less-sensitive hash-based user indices. Instead of storing or processing raw interaction data, the system operates on these hashed representations, which preserve similarity among users with similar preferences. This approach ensures that sensitive information remains protected while still enabling efficient similarity analysis for recommendation generation.

In addition to privacy preservation, the system also integrates a file hashing mechanism using the SHA-256 algorithm to ensure data integrity and authenticity. Each uploaded data file is assigned a unique hash value, which acts as a digital fingerprint. This mechanism allows the system to detect any unauthorized modification of stored data and guarantees the reliability of the information used in the recommendation process. The system architecture also includes modules such as user registration, consumer data upload, cloud server management, and smart contract-based authorization, which together provide a secure and organized environment for IoT service recommendation.

Overall, the proposed SerRecL2H framework provides a practical and efficient solution for privacy-aware IoT service recommendation. The system successfully balances recommendation accuracy, privacy protection, and computational efficiency, making it suitable for large-scale IoT applications. The proposed approach can serve as a strong foundation for future research in secure and scalable recommendation systems for emerging IoT environments.

7. FUTURE SCOPE

The proposed SerRecL2H framework can be further enhanced to support more advanced and intelligent IoT service recommendation systems. In the future, deep learning–based models can be integrated with the Learning to Hash technique to improve recommendation accuracy and adaptability to dynamic user behavior. The system can also be extended to support real-time data processing from large-scale IoT devices and edge computing environments. Additionally, integrating federated learning can further strengthen privacy protection by enabling collaborative model training without sharing raw data. Mobile application support and advanced analytics dashboards for monitoring recommendation trends can also be implemented to improve usability and scalability.

REFERENCES

[1] W. Lin, M. Zhu, X. Zhou, R. Zhang, X. Zhao, S. Shen, and L. Sun, A deep neural collaborative filtering based service recommendation method with multi-source data for smart cloud-edge collaboration applications, Tsinghua Science and Technology, vol. 29, no. 3, pp. 897–910, 2024.

[2] D. Ma, Y. Wang, J. Ma, and Q. Jin, SGNR: A social graph neural network based interactive recommendation scheme for e-commerce, Tsinghua Science and Technology, vol. 28, no. 4, pp. 786–798, 2023.

[3] Z. Li, X. Xu, T. Hang, H. Xiang, Y. Cui, L. Qi, and X. Zhou, A knowledge-driven anomaly detection

framework for social production system, IEEE Trans. Comput. Soc. Syst., vol. 11, no. 3, pp. 3179–3192, 2024.

[4] L. Qi, R. Wang, C. Hu, S. Li, Q. He, and X. Xu, Time aware distributed service recommendation with privacy preservation, Inf. Sci., vol. 480, pp. 354–364, 2019.

[5] X. Xu, H. Li, Z. Li, and X. Zhou, Safe: Synergic data filtering for federated learning in cloud-edge computing, IEEE Trans. Ind. Inf., vol. 19, no. 2, pp. 1655–1665, 2023.

[6] IEEE Trans. Ind. Inf., vol. 19, no. 2, pp. 1655–1665, 2023. [5] D. Li and J. A. Esquivel, Trust-aware hybrid collaborative recommendation with locality-sensitive hashing, Tsinghua Science and Technology, 2023, DOI: 10.26599/TST.2023.9010096.

[7] X. Xu, S. Tang, L. Qi, X. Zhou, F. Dai, and W. Dou, CNN partitioning and offloading for vehicular edge networks in web3, IEEE Commun. Mag., vol. 61, no. 8, pp. 36–42, 2023.

[8] F. Luo, J. Wu, and T. Wang, Discrete listwise personalized ranking for fast top-N recommendation with implicit feedback, in Proc. 31st Int. Joint Conf. Artificial Intelligence, Vienna, Austria, 2022, pp. 2159–2165.

[9] F. Wang, W. Liu, C. Chen, M. Zhu, and X. Zheng, HCFRec: Hash collaborative filtering via normalized flow with structural consensus for efficient recommendation, in Proc. 31st Int. Joint Conf. Artificial Intelligence, Vienna, Austria, 2022, pp. 2270–2276.

[10] H. Zhou, J. M. Alvarez, and F. Porikli, Less is more: Towards compact CNNs, in Proc. 14th European Conf. Computer Vision, Amsterdam, The Netherlands, 2016, pp. 662–677.

[11] H. Li, T. N. Chan, M. L. Yiu, and N. Mamoulis, FEXIPRO: Fast and exact inner product retrieval in recommender systems, in Proc. 2017 ACM Int. Conf. Management of Data, Chicago, IL, USA, 2017, pp. 835–850.

[12] D. Lian, H. Wang, Z. Liu, J. Lian, E. Chen, and X. Xie, LightRec: A memory and search-efficient recommender system, in Proc. Web Conf. 2020, Taipei, China, 2020, pp. 695–705.

[13] Y. Li, T. Chen, P. F. Zhang, and H. Yin, Lightweight self attentive sequential recommendation, in Proc. 30th ACM Int. Conf. Information & Knowledge Management, Virtual Event, Australia, 2021, pp. 967–977.

[14] J. W. Lee, M. Choi, J. Lee, and H. Shim, Collaborative distillation for top-N recommendation, in Proc. 2019 IEEE Int. Conf. Data Mining (ICDM), Beijing, China, 2019, pp. 369–378.

[15] W. Kweon, S. Kang, and H. Yu, Bidirectional distillation for top-K recommender system, in Proc. Web Conf. 2021, Ljubljana, Slovenia, 2021, pp. 3861–3871.

[16] X. Xu, J. Gu, H. Yan, W. Liu, L. Qi, and X. Zhou, Reputation-aware supplier assessment for blockchain enabled supply chain in industry 4.0, IEEE Trans. Ind. Inf., vol. 19, no. 4, pp. 5485–5494, 2023.

[17] L. E. Wang and X. Li, A graph-based multifold model for anonymizing data with attributes of multiple types, Comput. Secur., vol. 72, pp. 122–135, 2018.

[18] X. Y. Xia, Z. H. Bai, J. Li, and R. Y. Yu, A location cloaking algorithm based on dummy and stackelberg game, (in Chinese), Chin. J. Comput., vol. 42, no. 10, pp. 2216–2232, 2019.

[19] H. Liu, X. H. Li, B. Luo, Y. W. Wang, Y. B. Ren, J. F. Ma, and H. F. Ding, Distributed K-anonymity location privacy protection scheme based on blockchain, (in Chinese), Chin. J. Comput., vol. 42, no. 5, pp. 942–960, 2019.

[20] G. Qiu, D. Guo, Y. Shen, G. Tang, and S. Chen, Mobile semantic-aware trajectory for personalized location privacy preservation, IEEE Internet Things J., vol. 8, no. 21, pp. 16165–16180, 2021.

[21] K. Dou, B. Guo, and L. Kuang, A privacy-preserving multimedia recommendation in the context of social network based on weighted noise injection, Multimedia Tools Appl., vol. 78, no. 19, pp. 26907–26926, 2019.

[22] Y. Zhang, J. Pan, L. Qi, and Q. He, Privacy-preserving quality prediction for edge-based IoT services, Future Gener. Comput. Syst., vol. 114, pp. 336–348, 2021.

[23] A. Gionis, P. Indyk, and R. Motwani, Similarity search in high dimensions via hashing, in Proc. 25th Int. Conf. Very Large Data Bases, San Francisco, CA, USA, 1999, pp. 518–529.

[24] L. Qi, X. Zhang, S. Li, S. Wan, Y. Wen, and W. Gong, Spatial-temporal data-driven service recommendation with privacy-preservation, Inf. Sci., vol. 515, pp. 91–102, 2020.

[25] E. Yang, C. Deng, T. Liu, W. Liu, and D. Tao, Semantic structure-based unsupervised deep hashing, in Proc. 27th Int. Joint Conf. Artificial Intelligence, Stockholm, Sweden, 2018, pp. 1064–1070.

[26] L. Qi, Y. Liu, Y. Zhang, X. Xu, M. Bilal, and H. Song, Privacy-aware point-of-interest category recommendation in internet of things, IEEE Internet Things J., vol. 9, no. 21, pp. 21398–21408, 2022.

[27] Y. Liu, H. Wu, K. Rezaee, M. R. Khosravi, O. I. Khalaf, A. A. Khan, D. Ramesh, and L. Qi, Interaction-enhanced and time-aware graph convolutional network for successive point-of-interest recommendation in traveling enterprises, IEEE Trans. Ind. Inf., vol. 19, no. 1, pp. 635–643, 2023.

[28] Y. Liu, X. Zhou, H. Kou, Y. Zhao, X. Xu, X. Zhang, and L. Qi, Privacy-preserving point-of-interest recommendation based on simplified graph convolutional network for geological traveling, ACM Trans. Intell. Syst. Technol., vol. 15, no. 4, p. 76, 2024.

[29] K. Zhang, S. Fan, and H. J. Wang, An efficient recommender system using locality sensitive hashing, in Proc. 51st Hawaii Int. Conf. System Sciences, Waikoloa Village, HI, USA, 2018, pp. 780–789.

[30] Z. Zheng, Y. Zhang, and M. R. Lyu, Investigating QoS of real-world web services, IEEE Trans. Serv. Comput., vol. 7, no. 1, pp. 32–39, 2014.

[31] Z. Zheng, Y. Zhang, and M. R. Lyu, Distributed QoS evaluation for real-world web services, in Proc. 2010 IEEE Int. Conf. Web Services, Miami, FL, USA, 2010, pp. 83–90.

[32] L. Shao, J. Zhang, Y. Wei, J. Zhao, B. Xie, and H. Mei, Personalized QoS prediction forWeb services via collaborative filtering, in Proc. IEEE Int. Conf. Web Services (ICWS 2007), Salt Lake City, UT, USA, 2007, pp. 439–446.

[33] B. Sarwar, G. Karypis, J. Konstan, and J. Riedl, Item based collaborative filtering recommendation algorithms, in Proc. 10th Int. Conf. World Wide Web, Hong Kong, China, 2001, pp. 285–295.

[34] Y. Koren, R. Bell, and C. Volinsky, Matrix factorization techniques for recommender systems, Computer, vol. 42, no. 8, pp. 30–37, 2009.

[35] D. D. Lee and H. S. Seung, Learning the parts of objects by non-negative matrix factorization, Nature, vol. 401, no. 6755, pp. 788–791, 1999.

[36] S. Hashemi and S. Reda, Generalized matrix factorization techniques for approximate logic synthesis, in Proc. 2019 Design, Automation & Test in Europe Conf. Exhibition(DATE). Florence, Italy, 2019, pp. 1289–1292.

[37] L. Qi, X. Zhang, W. Dou, and Q. Ni, A distributed locality-sensitive hashing-based approach for cloud service recommendation from multi-source data, IEEE J. Sel. Areas Commun., vol. 35, no. 11, pp. 2616–2624, 2017.

[38] C. Yan, Y. Zhang, W. Zhong, C. Zhang, and B. Xin, A truncated SVD-based arima model for multiple QoS prediction in mobile edge computing, Tsinghua Science and Technology, vol. 27, no. 2, pp. 315–324, 2022.

[39] X. Yang and J. A. Esquivel, Time-aware LSTM neural networks for dynamic personalized recommendation on business intelligence, Tsinghua Science and Technology, vol. 29, no. 1, pp. 185–196, 2024.