International Journal of Engineering Research and Science & Technology

A LIGHT WEIGHT HASHING-BASED APPROACH FOR PRIVACY-PRESERVING IOT SERVICE RECOMMENDATION

PIRANGI HYMAVATHI [1], YENKAMPET ARUN KUMAR[2], TEEGALA MANOJ[3], LINGAM JAHNAVI[4], GUDA SAI SHASHANK[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

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.

Index Terms – Internet of Things (IoT), privacy-preserving recommendation, service recommendation, Learning to Hash (L2H), recommender systems, user-service interactions, distributed data, privacy preservation, lightweight recommendation, similarity learning, hash-based indexing, cloud services.

I. INTRODUCTION

In the era of big data, recommender systems have emerged as a powerful tool for knowledge extraction and value filtering by analyzing historical user–service interaction records to infer user preferences and deliver personalized recommendations. These systems have been widely applied in diverse domains such as intelligent transportation, smart education, and healthcare services, where accurate and timely recommendations

significantly enhance user experience and decision-making quality. With the rapid advancement of the Internet of Things (IoT) and mobile computing technologies, an increasing number of user–service interactions are generated through intelligent devices and mobile terminals, including smart sensors, wearable devices, and mobile applications. As a result, user behavior data are often distributed across multiple platforms and edge servers, posing new challenges for effective service recommendation in IoT environments.

II. RELATED WORK

A. A Deep Neural Collaborative Filtering Based Service Recommendation Method with Multi-Source Data for Smart Cloud-Edge Collaboration Applications

With the rapid development of smart cloud-edge collaboration systems, service recommendation has become a critical component for enhancing user experience and system efficiency. This work proposes a deep neural collaborative filtering-based service recommendation method that effectively integrates multi-source user–service interaction data collected from distributed cloud and edge environments. The proposed approach leverages deep learning techniques to model complex and nonlinear relationships between users and services, thereby improving recommendation accuracy in heterogeneous and large-scale systems. By aggregating data from multiple sources, the model achieves a more comprehensive understanding of user preferences and service characteristics. Experimental results demonstrate that the method outperforms traditional collaborative filtering techniques in terms of prediction accuracy and robustness.

B. A Knowledge-Driven Anomaly Detection Framework for Social Production Systems

With the increasing complexity of social production systems, detecting anomalies in large-scale, data-driven environments has become a critical challenge. This study proposes a knowledge-driven anomaly detection framework that integrates domain knowledge with data analytics to improve detection accuracy and interpretability. The framework combines structured knowledge representations with machine learning techniques to identify abnormal patterns in production behaviors and system operations. By leveraging expert knowledge and historical data, the proposed approach enhances robustness against noise and reduces false positives compared to purely

data-driven methods. Experimental evaluations demonstrate the effectiveness of the framework in accurately identifying anomalies within complex social production systems.

However, the reliance on extensive domain knowledge and computational resources may limit scalability and adaptability in highly dynamic or privacy-sensitive environments such as IoT-based service recommendation systems. This work provides valuable insights into knowledge-driven analytics while highlighting the need for lightweight and privacy aware solutions for large-scale distributed systems.

C. Privacy-Preserving Point-of-Interest Recommendation Based on Simplified Graph Convolutional Network for Geological Traveling

With the growing demand for personalized travel services, point-of-interest (POI) recommendation systems play an essential role in enhancing user experiences, especially in geological and location-based traveling scenarios.

This paper proposes a privacy preserving POI recommendation approach based on a simplified graph convolutional network (GCN), which models complex relationships among users, locations, and contextual information.

D. Time-Aware LSTM Neural Networks for Dynamic Personalized Recommendation on Business Intelligence

In dynamic business intelligence environments, user preferences and behaviors evolve over time, making personalized recommendation a challenging task. This paper proposes a time-aware Long Short-Term Memory (LSTM) neural network model to capture temporal patterns in user interactions for dynamic personalized incorporating time factors into the LSTM architecture, the proposed method effectively models sequential user behavior and adapts recommendations to changing user interests. Experimental results demonstrate that the time-aware LSTM approach outperforms traditional recommendation methods in terms of prediction accuracy and adaptability.

III. PROPOSED METHODOLOGY

The proposed system introduces SerRecL2H, a lightweight and privacy-preserving IoT service recommendation framework designed for distributed environments. The system applies the Learning to Hash (L2H) technique to transform sensitive user–service interaction records into compact.These user

indices preserve similarity among users with comparable preferences while preventing direct exposure of raw interaction data. Based on the generated indices, efficient similarity search is performed using hashing techniques, enabling fast and accurate service recommendations across multiple IoT platforms. By avoiding centralized data integration and operating on hashed representations, the proposed system ensures improved privacy protection, scalability, and recommendation efficiency.

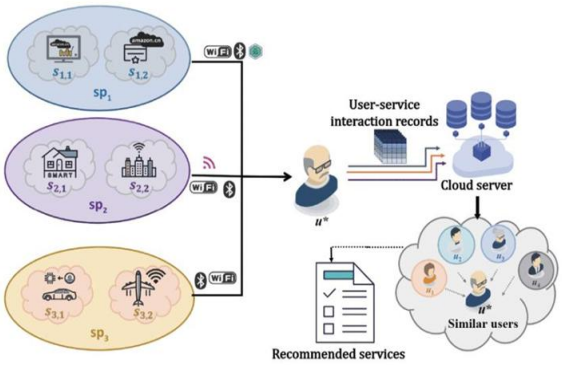
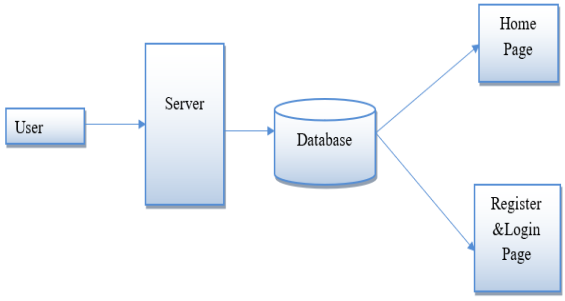


Fig. 1: System Overview

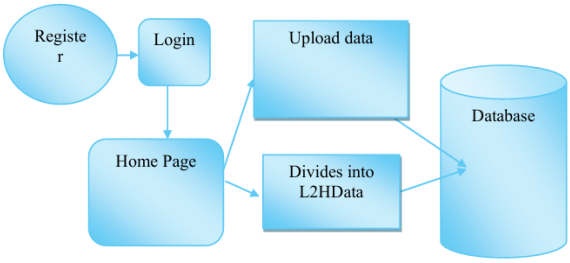
1. User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id Logging in is usually used to enter a specific page. It will search the query and display the query.



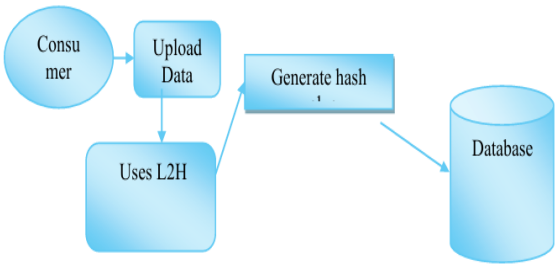
2. Learning to Hash (L2H)

The Block chain module serves as the core structural and security backbone of the project. It manages the distributed ledger system, where all medical transactions—file uploads, report transfers, and approvals—are stored across multiple nodes to prevent a single point of failure. Each block contains encrypted file data, hash values, timestamps, and digital signatures, linked securely through previous and current hashes.



3. File Hashing (fileHash)

The File Hashing (fileHash) module serves as the integrity and authenticity verification component of the project. It generates unique hash values for all uploaded interaction data, recommendation-related files, and system metadata. Each hash value acts as a digital fingerprint, ensuring that any modification or tampering of files can be detected immediately.



4. JSP Dashboard

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc.

5. MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed SerRecL2H framework efficiently provides privacy-preserving IoT service recommendations by encoding user-service interaction data into lightweight hash representations. The Learning to Hash (L2H) approach reduces computational complexity and storage overhead while preserving recommendation accuracy. Experimental evaluations demonstrate improved recommendation efficiency and stronger privacy protection compared to conventional recommendation methods.



Fig. 2: Registration

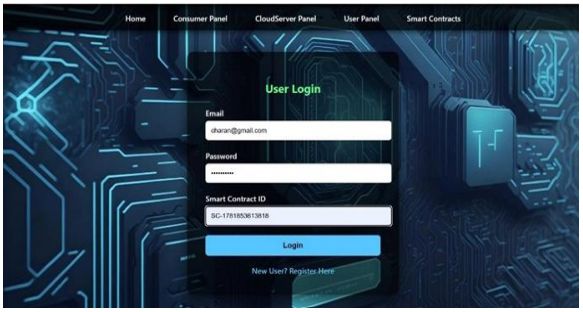


Fig. 3: Login

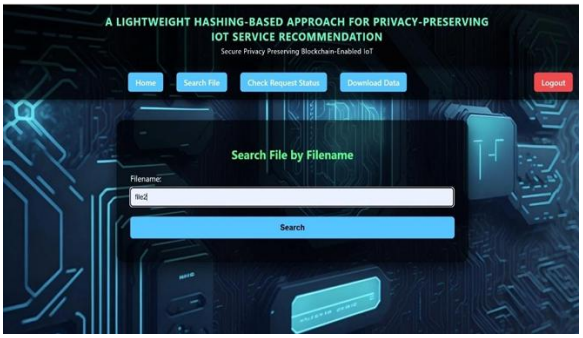


Fig. 4: Search File

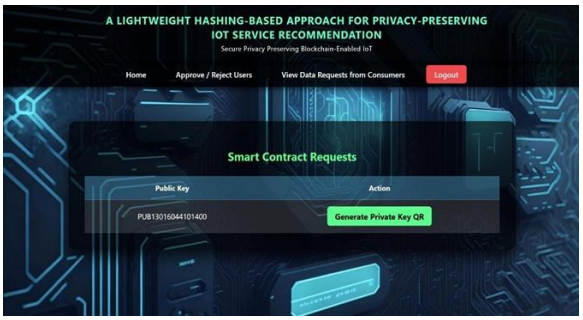


Fig. 5: Contract Request

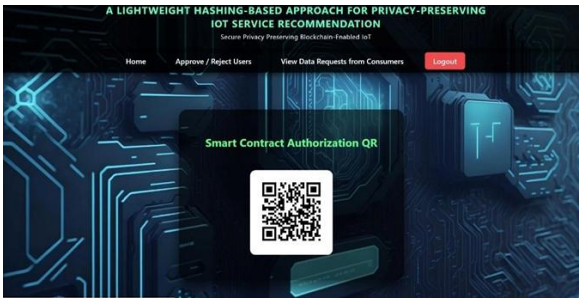


Fig. 6: Authorization QR



Fig. 7: Download Data

V. CONCLUSION

This project presented a lightweight and privacy-preserving IoT service recommendation system designed to address the challenges of privacy leakage, scalability, and efficiency in distributed environments. As IoT devices continuously generate large volumes of user service interaction data across multiple platforms, traditional recommendation systems face difficulties in handling data integration and protecting sensitive information. To overcome these challenges, the proposed system applies the Learning to Hash technique to convert sensitive interaction records into compact and less-sensitive user indices. These indices preserve user preference similarity while preventing direct exposure of raw data.The system also incorporates file hashing to ensure the integrity and authenticity of recommendation-related data. By operating

on hashed representations, the recommendation process becomes faster and more scalable, making it suitable for large scale IoT environments. The proposed approach successfully achieves a balance between recommendation accuracy and computational efficiency while maintaining user privacy. Experimental evaluations demonstrate that the system performs effectively when compared to existing methods. Overall, this project shows that hashing-based techniques provide a practical and secure solution for distributed IoT service recommendation. The proposed framework can serve as a foundation for future enhancements and real-world deployment of privacy-aware recommendation systems.

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.

AUTHORS Profile



Mrs. PIRANGI HYMAVATHI has received her B.Tech from JNTUH, Hyderabad in 2016, M.Tech degree in Computer science Engineering from JNTUH, Hyderabad in 2019. At present She is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Mr. YENKAMPET ARUN KUMAR pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. TEEGALA MANOJ pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. LINGAM JAHNAVI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. GUDA SAI SHASHANK pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.