**EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced**

**Encrypted Data**

**Priyadharshini S** (MCA) Department of MCA & Krishnasamy College of Engineering & Technology

**Dr. E. Ranjith, MCA., M.Phil., Ph.D.,** Assistant.Prof. Department of MCA & Krishnaswamy College of Engineering and Technology, Cuddalore.

# ABSTRACT

Location-based services (LBS) have lately gained popularity and importance due to the widespread use of smart phones. However, the privacy of a user's location could potentially be threatened by the use of LBS. In this research, we describe an effective and privacy-preserving location based query solution called EPLQ that targets spatial range query, a common LBS that provides information about POIs (Points of Interest) within a particular distance. We specifically present the first predicate only encryption system for inner product range to enable privacy-preserving spatial range queries. This scheme may be used to determine whether a position is inside a certain circular area. We also create a privacy-preserving tree index structure in EPLQ to decrease query time.

# I. INTRODUCTION

A few decades ago, location-based services (LBS) were used in military only. Today, thanks to advances in information and communication technologies, more kinds of LBS have appeared, and they are very useful for not only organizations but also individuals. Let’s take the spatial range query, one kind of LBS that we will focus on in this paper, as an example. Spatial range query is a widely used LBS, which allows a user to find POIs (Point of Interests) within a given distance to his/her location, i.e., the query point. As illustrated in Fig. 1, with this kind of LBS, a user could obtain the records of all restaurants within walking distance (say 500 meters). Then the user can go through these records to find a desirable restaurant considering price and reviews**.**

While location-based services are popular and vital, most of these services today including spatial range query require users to submit their locations, which raises serious concerns about the leaking and misusing of user location data. For Example, criminals may utilize the data to track potential victims and predict their locations. For another example, some sensitive location data of organization users may involve trade secret or national security. Protecting the privacy of user location in LBS has attracted considerable

interest. However**,**



**Admin**



**Register**



**Login**



**Upload Data**



**User**



**register**



**login**



**search data**



**Location**



<<



extend



>>

# Use case Diagrams



# II. LITERATURE SURVEY

In this paper, we present a solution called EPLQ (Efficient Privacy-Preserving Spatial Range Query) that addresses the challenges faced by existing methods in privacy-preserving spatial range queries. The goal of EPLQ is to enable queries over encrypted location-based service (LBS) data without compromising user privacy by disclosing their locations to the cloud or LBS provider.

To achieve this, we introduce a novel encryption scheme called Inner Product Range Encryption (IPRE). IPRE allows for testing whether the inner product of two vectors falls within a given range without revealing the vectors themselves. In predicate encryption, the key associated with a predicate, denoted as f, can decrypt a ciphertext only if the attribute of the ciphertext, denoted as x, satisfies the predicate, i.e., f(x) = 1. However, in predicate-only encryption, the focus is not on encrypting/decrypting messages but rather on determining whether f(x) = 1 or not.

While predicate-only encryption schemes supporting various types of predicates have been proposed for privacy-preserving query on outsourced data, there is currently no existing scheme that specifically supports inner product range predicates. Our IPRE scheme fills this gap and can have applications beyond privacy-preserving spatial range querying.

In addition to IPRE, we also introduce a privacy-preserving index structure called the ˆsstree (pronounced "hat sstree"). This index structure is designed to enhance the performance of EPLQ. The combination of IPRE and ˆsstree constitutes the core contributions of this paper.

To summarize, the main contributions of this paper can be outlined as follows:

1. Introduction of IPRE, a novel predicate-only encryption scheme for inner product range. This scheme enables testing the range of inner products without exposing the vectors themselves.
2. Demonstration of the applicability of IPRE in privacy-preserving spatial range querying, while acknowledging its potential for use in other applications.
3. Development of the ˆsstree, a privacy-preserving index structure that improves the overall efficiency of EPLQ.

By proposing EPLQ and its underlying components, this paper aims to provide an efficient and privacy-preserving solution for spatial range queries over encrypted LBS data, safeguarding user location privacy in the process.

# III. PROPOSED SYSTEM

The increasing use of Location-Based Services (LBS) raises concerns about the privacy of user locations. This paper addresses the specific scenario of spatial range queries, where an LBS provides information about Points of Interest (POIs) within a certain distance from a given location. To tackle this problem and ensure privacy preservation, we introduce a solution called EPLQ (Efficient Privacy-Preserving Location-Based Query).

The primary objective of EPLQ is to enable spatial range queries while protecting the privacy of user locations. To achieve this, we propose the first predicate-only encryption scheme for the inner product range. This encryption scheme allows for the detection of whether a position falls within a specified circular area without revealing the exact position in a privacy-preserving manner. By using this scheme, EPLQ ensures that user locations remain concealed from the LBS provider or any other third parties..

# IV. MODULE DESCRIPTION

I. Admin

A. Register and Login:

Administrators have the ability to register by providing their personal details and create an account within the system. Once registered, they can log in using their credentials to access the system's functionalities.

B. Upload Data:

After logging in, administrators are able to upload data to the system. These data may include various types of information such as points of interest, locations, or other relevant data. To ensure security, the uploaded data is encrypted before being stored in the system's database.

II. User

A. Register and Login:

Users have the option to register within the system by providing their personal details, along with their location information. Once registered, they can log in using their credentials to access the system.

# V. CONCLUSION

We have proposed “EPLQ: Efficient Privacy-Preserving Location-based Query over Outsourced Encrypted Data”, an efficient privacy preserving spatial range query solution for smart phones, which preserves the privacy of user location, and achieves confidentiality of LBS data. To realize EPLQ, we have designed a novel predicate-only encryption scheme for inner product range named IPRE and a novel privacypreserving index tree named ˆ ss-tree. EPLQ’s efficacy has been evaluated with theoretical analysis and experiments, and detailed analysis shows its security against known-sample attacks and ciphertext-only attacks. Our techniques have potential usages in other kinds of privacy-preserving queries. If the query can be performed through comparing inner products to a given range, the proposed IPRE and ˆ ss-tree may be applied to realize privacypreserving query. Two potential usages are privacy preserving similarity query and long spatial range query. In the future, we will design solutions for these scenarios and identify more usages.

# VI. FUTURE ENCHANCEMENT

. This project holds significant potential for future development and implementation on the internet. Its flexible nature allows for seamless updates and expansions to accommodate emerging requirements as they arise.

With the proposed software, which includes a robust database system and fully functional processes, administrators are empowered to efficiently manage and oversee the entire operation. This results in improved accuracy, streamlined workflows, and a reduced likelihood of errors.

As the project evolves and adapts to changing needs, it has the capability to become a comprehensive solution that effectively supports various aspects of the work at hand. By leveraging the power of technology, the project offers an enhanced platform for administrators to carry out their responsibilities, ultimately leading to smoother operations and improved outcomes.

# VII. REFERENCES

1. A. Gutscher, “Coordinate transformation - a solution for the privacy problem of location based services?” in 20th International Parallel and Distributed

Processing Symposium (IPDPS 2006),

Proceedings,25-29 April 2006, Rhodes Island, Greece, 2006. [Online]. Available.

1. W. K. Wong, D. W.-l. Cheung, B. Kao, and

N. Mamoulis, “Secure knncomputation on encrypted databases,” in SIGMOD. ACM, 2009,pp.139–152.

1. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, “Privatequeries in location based services: anonymizers are not necessary,” inSIGMOD. ACM, 2008, pp. 121– 132.
2. X. Yi, R. Paulet, E. Bertino, and V.

Varadharajan, “Practical k nearestneighbor queries with location privacy,” in ICDE. IEEE, 2014, pp.640–651.

1. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private information retrieval,” Journal of the ACM (JACM), vol. 45, no. 6, pp. 965–981, 1998.