WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Location-Based Query Over Outsourced Encrypted Data

Priyadharshini S ,Asst.Prof. Dr.E. RANJITH, MCA., MPhil., Ph.D.,

Krishnasamy College Of Engineering and Technology,Cuddalore.

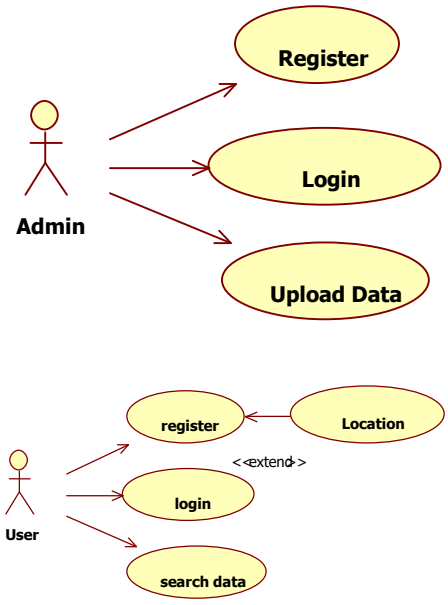
ABSTRACT

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

Location-based services (LBS) were only utilised by the military a few decades ago. More types of LBS have now emerged as a result of improvements in information and communication technology, and both individuals and organisations can benefit greatly from them. As an illustration, consider the spatial range question, one type of LBS that this study will concentrate on. A frequently used LBS called spatial range query enables users to locate POIs (Points Of Interest) that are close to their current position, or the query point. With this type of LBS, as shown in Fig. 1, a user might get the information about every restaurant within walking distance (let's say 500 metres). Once found, the user can search these records.

Use case Diagrams



LITERATURE SURVEY

For the privacy-preserving spatial range query, there are currently a few solutions [1]–[6]. However, as explained in Section VIII below, current methods cannot handle all of the aforementioned problems. In order to address this, we present an effective method for a spatial range query that

protects privacy, called EPLQ, in this work. EPLQ enables searches over encrypted LBS data without revealing user positions to the cloud or LBS provider. To the best of our knowledge, the first predicate/predicate-only scheme of this kind, we build a unique predicate-only encryption scheme for inner product range (IPRE scheme for short) to safeguard the privacy of user location in EPLQ. We also develop the ss-tree, a privacy-preserving index structure, to boost performance. The three primary contributions of this study are as follows:

First, we provide a brand-new inner product range predicate-only encryption scheme called IPRE, which enables checking the inner product of two vectors' range without releasing the vectors themselves. If and only if the characteristic of the cypher text, x, meets the predicate, as in $f(x) = 1$, the key corresponding to the predicate, f, can decrypt the cypher text in predicate encryption. A unique kind of predicate encryption called "predicate-only encryption" is not made to encrypt/decrypt messages. Instead, whether $f(x) = 1$ or not, it shows that.
For privacy-preserving queries on outsourced data, predicate-only encryption techniques supporting a variety of predicates [7, [8]] have been developed. To the best of our knowledge, there is no scheme enabling an inner product range that uses solely predicates. Although this study uses our approach for a privacy-preserving spatial range query, it can also be utilised for other purposes.

PROPOSED SYSTEM

The privacy of a user's location could also 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.

System Modules:

- **ADMIN**
  - Register
  - Login
  - Upload Data
- **USER**
  - Register
  - Login
  - Search Data(Decrypt data)

MODULE DESCRIPTION

I-admin

A. ***Register and login****:*

Admin enter this system and register their own information.

B. ***Upload Data:***

Data administrators can upload to this system. These data are kept in a database using encrypted storage.

II-user

A.***Register and login****:*

User registers their details and enters this system with location details.

B. ***SearchData:***

User enter this system and search their data
like Restaurant, Bank, Police Station and etc.,

System Requirement:

Hardware Requirements:-

- Windows Desktop

Software Requirements: -

Operating System : Windows OS

Tool : Java Eclipse

CONCLUSION

We have suggested "EPLQ: Efficient Privacy-Preserving Location-based Query over Outsourced Encrypted Data", an effective privacy-preserving spatial range query solution for smartphones that achieves confidentiality of LBS data while maintaining the privacy of the user's location. To implement EPLQ, we created a novel privacy-preserving index tree called ss-tree and a novel predicate-only encryption method for inner product range called IPRE. A thorough examination demonstrates EPLQ's security against known-sample attacks and cypher text-only assaults. Its effectiveness has been assessed through theoretical analysis and tests. Our methods could be used to various other privacy-preserving inquiries. The proposed IPRE and ss-tree may be used to realise privacy-preserving query if the query can be carried out by comparing inner products to a specified range.

FUTURE ENCHANCEMENT

The future of this project is really bright. Future online implementation of this idea is possible. The project is highly flexible in terms of expansion, therefore it can be upgraded in the near future as and when the need for the same arises. The administrator was able to manage and thereafter perform the entry job in a lot better, accurate, and error-free manner thanks to the provided software of database systems and completely functional process.

REFERENCES

1. Gutscher, “Coordinate transformation - a solution for the privacy problem of locationbased services?” in 20th International Parallel and Distributed
2. Processing Symposium (IPDPS 2006),
3. Proceedings,25-29 April 2006, Rhodes Island, Greece, 2006. [Online]. Available.
4. W. K. Wong, D. W.-l. Cheung, B. Kao, and
5. N. Mamoulis, “Secure knncomputation on encrypted databases,” in SIGMOD. ACM, 2009,pp.139–152.
6. 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.
7. X. Yi, R. Paulet, E. Bertino, and V.
8. Varadharajan, “Practical k nearestneighbor queries with location privacy,” in ICDE. IEEE, 2014, pp.640–651.
9. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private information retrieval,” Journal of the ACM (JACM), vol. 45, no. 6, pp. 965–981, 1998.