ISSN: 2096-3246
Volume 55, Issue 02, May, 2023

https://doi.org/10.5281/zenodo.12707497

EPLQ: Effective, confidential, location-based query on offsiteencrypted data

KALWAKURTHI SRI SANDHYA,K BALAJI SUNIL CHANDRA,TALARI SIVALAKSHMI
Assistant Professor[1,2,3],
k.srisandhya26@gmail.com, hod.cse@svitatp.ac.in, shivalakshmidinesh@gmail.com
department of CSE, Sri Venkateswara Institute of Technology,
N.H 44, Hampapuram, Rapthadu, Anantapuramu, Andhra Pradesh 515722

Keywords:

ABSTRACT

Due to the increasing number of people using smartphones, location-based services (LBS) have recently become more popular and significant. Nevertheless, a user's capacity to monitor their location might be compromised by using LBS. One popular location-based service (LBS) that gives information about POIs within a certain distance is spatial range query; in this study, we provide EPLQ, an efficient and privacy-preserving LBS solution for this purpose. We provide the first privacy-preserving spatial range inquiry using a predicate-only encryption scheme for inner product range (IPRE). With IPRE, it is possible to determine, without compromising privacy, if a given position is within a certain circular zone. Additionally, we suggest a privacy-preserving tree index structure in EPLQ to decrease query time. The security aspects of EPLQ have been validated by a comprehensive security audit. Additionally, comprehensive testing is conducted, and the results show that EPLQ excels at doing privacy-preserving geographic range searches on encrypted data that is outsourced. For example, in our tests, a commodity workstation acting as the cloud searches POIs in a matter of seconds, whereas a mobile LBS user on an Android phone takes around 0.9 seconds to generate a query.

ISSN: 2096-3246
Volume 55, Issue 02, Nov, 2023
https://doi.org/10.5281/zenodo.12707497

Introduction

Safeguarding mobile users' location data in Location Based Services is a critical yet challenging and mostly unresolved issue. It is essential to safeguard location data from both users and service providers that store and process it, without limiting the system's performance, to prevent unauthorised access. While location-based services (LBS) have expanded beyond their original military usage, they continue to pose serious problems, such as the fact that criminals may potentially track the whereabouts of any individual using the data collected. That they have access to sensitive information on the company, including its physical location, is also useful for business purposes. Therefore, the most critical one is safeguarding users' whereabouts. In this study, we will primarily focus on the spatial range query.Several obstacles must be overcome, such as the need to secure privacy and the encryption of accessing LBS data. Spatial range query has several existing implementations.

1. RELATED WORK

In. authors used an approach based on coordinate transformations. It looks to how location information can be rendered illegible in such a way that it is still possible to perform processingoperations required by LBS.in this approach all users share one single transformation function,it is thus only suitable for closed user groups in which all members trust each .it is basically possible to solve the major privacy problem of LBS and to protect the location data of mobileusers even against malicious location and event service providers. It gives a relatively ‘weak’ protection; it not a better solution and it cannot offer a perfect solution . in [3] Authors focuseson the outsourcing of spatial datasets.

Aim is to enforce the user authorization defined by the data owner, even when the service provider cannot be trusted. The method that protect location information from unauthorizes, provide authorized users to search spatial queries that are querying by the service provider. Given a set Q of data points, the data owner maps Q to another point set Q0 using a transformation with a secret key. The data owner uploads Q0 to the service provider and sendsthe key to authorized users through a secure channel. Since the service provider does not knowthe key. At query time, an authorized user maps a query X to another query X0 by using the key and then submits X0 to the service provider.

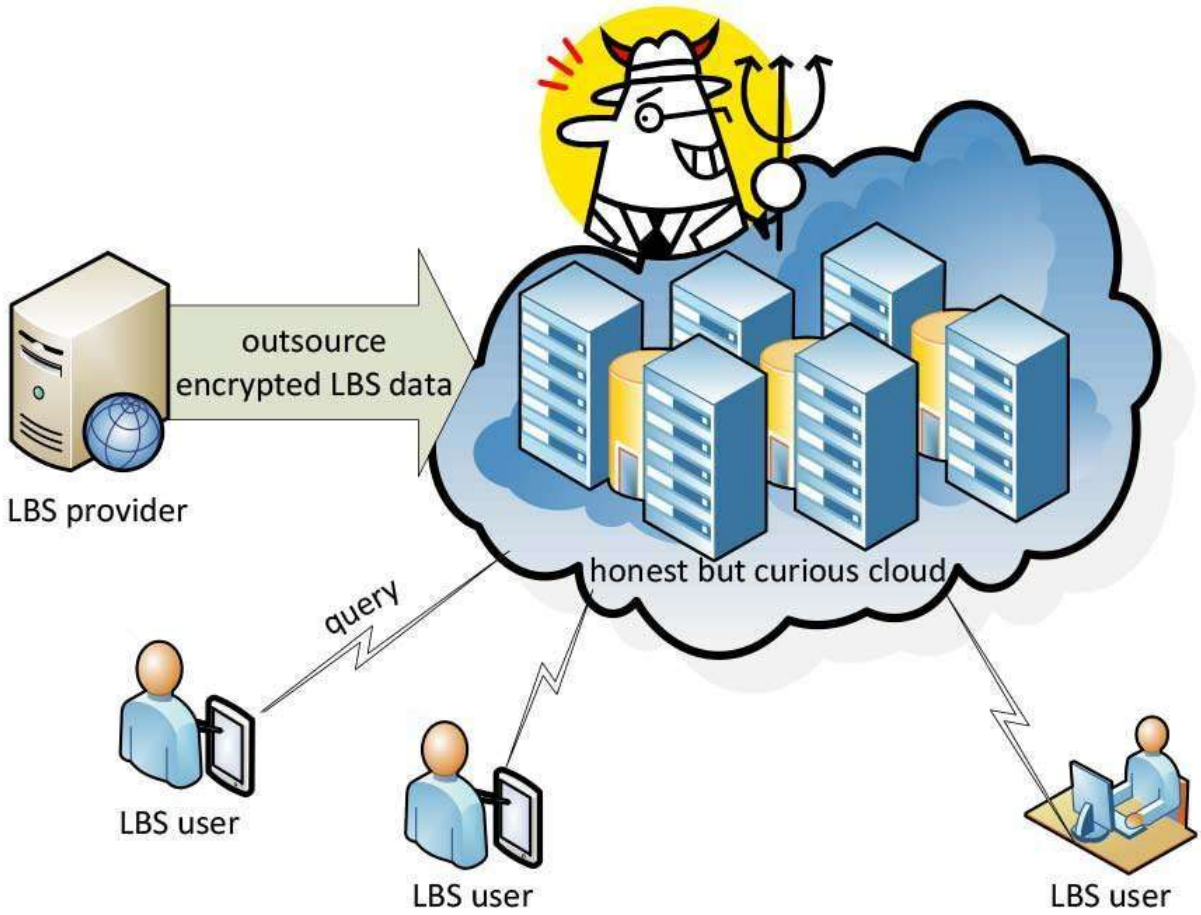
Then service provider executes X0 against Q0 and returns the result R0 P0 to U, who uses thekey to decode R0 and obtain the actual result R P. used an optimization function which considers nature of the packet, size of the packet and distance between the nodes, number of hops and transmission time are also considered for optimization. In Author look to anonymouscommunication technique to protect the location privacy of people using LBSs. In our proposedtechnique, a user sends true position data with several false position data (‘dummies’) to a service provider, who creates a reply message for each received position data. The user simplyextracts the necessary information from the reply message. In this manner, even if the service provider stores the set of position data, it cannot distinguish the true position data from the setof position

ISSN: 2096-3246
Volume 55, Issue 02, May, 2023
https://doi.org/10.5281/zenodo.12707497

data. To apply our anonymous communication technique in LBSs, the twoimportant issues are; Realistic dummy movements, Reduction of communication cost. In The author present Casper is new method in which mobile and stationary users can entertain location based services without revealing their location information. Casper consists of two main components, the location anonymizer and the privacy-aware query processor. Thelocation anonymizer blurs the users' exact location information into cloaked spatial regions based on user specified privacy requirements. The privacy-aware query processor is embeddedinside the location-based

database server in order to deal with the cloaked spatial areas rather than the exact location information. Experimental results show that Casper achieves high quality location-based services while providing anonymity for both data and queries. In Authors introduce new method basing on coordinate transformations. it shows how location information can be rendered illegible in such a way that it is still possible to perform processing operations requiredby LBS.

2. SYSTEM ARCHITECTURE:



ISSN: 2096-3246
Volume 55, Issue 02, Nov, 2023
https://doi.org/10.5281/zenodo.12707497

3. MODULES:

System Construction Module

- LBS User
- LBS Provider
- Privacy-Preserving Spatial Range Query

3.1 MODULES DESCSRIPTION:

System Construction Module

The LBS provider has abundant of LBS data, which are POI records. The LBS provider allows authorized users (i.e., LBS users) to utilize its data through location-based queries. Because of the financial and operational benefits of data outsourcing, the LBS provider offers the query services via the cloud. However, the LBS provider is not willing to disclosethe valuable LBS data to the cloud. Therefore, the LBS provider encrypts the LBS data, and outsources the encrypted data to the cloud.

The cloud has rich storage and computing resources. It stores the encrypted LBS data fromthe LBS provider, and provides query services for LBS users. So, the cloud has to search the encrypted POI records in local storage to find the ones matching the queries from LBSusers.

LBS users have the information of their own locations, and query the encrypted records ofnearby POIs in the cloud. Cryptographic or privacy-enhancing techniques are usually utilized to hide the location information in the queries sent to the cloud. To decrypt the encrypted records received from the cloud, LBS users need to obtain the decryption key from the LBS provider in advance.

LBS User

In this Module, the mobile user sends location-based queries to the LBS provider (or calledthe LBS server) and receives location-based service from the provider. The mobile user queries the location based service provider about approximate k nearest points of interest on the basis of his current location. In general, the mobile user needs to submit his locationto the LBS provider which then finds out and returns to the user the k nearest POIs by comparing the distances between the mobile user's location and POIs nearby. This revealsthe mobile user's location to the LBS provider.

LBS Provider

ISSN: 2096-3246
Volume 55, Issue 02, May, 2023
https://doi.org/10.5281/zenodo.12707497

In this Module, the LBS provider provides location-based services to the mobile user. LBSallows clients to query a service provider in a ubiquitous manner, in order to retrieve detailed information about points of interest (POIs) in their vicinity (e.g., restaurants, hospitals, etc.). The LBS provider processes spatial queries on the basis of the location of the mobile user. Location information collected from mobile users, knowingly and unknowingly, can reveal far more than just a user's latitude and longitude.

Privacy-Preserving Spatial Range Query

In EPLQ, user queries and the sensitive location information are encrypted with IPRE scheme. A query consists of two tokens associated with two predicate vectors, which contains the LBS user's location information. The LBS user generates two tokens for searching

POI records with the proposed IPRE scheme. The two tokens associated with the query area should be generated. Let Ks and Ks be the generated two tokens.

The user sends a query to the LBS Service Provider. The LBS Service Provider searches tofind all leaf nodes matching the query from the user. The LBS Service Provider returns thecorresponding POI records of matched leaf nodes to the user. The LBS user decrypts received POI records with the shared key of the standard encryption scheme.

4. SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 1GB.

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
  Coding Language : ASP.NET, C#.NET
- Tool : Visual Studio 2008
- Database : SQL SERVER 2005

5. CONCLUSION AND FUTURE WORK

This work presents an encryption strategy for the inner product range and a data structure called sstree. With these, mobile users may enjoy location-based services securely, without having to reveal their private location data.

ISSN: 2096-3246
Volume 55, Issue 02, Nov, 2023
https://doi.org/10.5281/zenodo.12707497

6. REFERENCES

[1] "EPLQ: Efficient Privacy-Preserving Location-BasedQuery Over Outsourced Encrypted Data" Published in the IEEE Internet of Things Journal, Volume 3, Issue 2, April 2016, by Lichun Li, Rongxing Lu, and Cheng Huang. "Coordinate transformation - a solution for the privacy problem of location base services?" was published in the proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS 2006), which took place on Rhodes Island, Greece, from April 25th to 29th, 2006. [On the web]. "The new casper: query processing for location services without compromising privacy," in VLDB, 2006, pp. 763, is authored by M. F. Mokbel, C.-Y. Chow, and W. G. Aref. In Data and Applications Security XXI, published by Springer in 2007, C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. Di Vimercati, and P. Samarati presented "Location privacy protection through obfuscation-based techniques." "Anonymous usage of location-based services through spatial and temporal cloaking," in Proceedings of the 1st international conference on Mobile systems, applications and services, by M. Gruteser and D. Grunwald, [5] found. 2003, ACM.

[6] "Location privacy protection through obfuscation-based techniques," in Data and Applications Security XXI. Spinger, 2007, pp. 47-60, by C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. Di Vimercati, and P. Samarati. [7] Ghinita, Panos, Kalnis, Ali, Cyrus, and Tan, Kian-Lee "Private Queries in Location Based Services Anonymizers are not Necessary"An anonymous communication strategy utilising dummies for location-based services was presented at the 2005 IEEE ICPS by H. Kido, Y. Yanagisawa, and T. Satoh, and can be found on pages 88 to 97. [9]Working with A. R. Beresford and F. Stajano.Article titled "Location privacy in pervasive computing" published in 2003 by IEEE ubiquitous Computing, with pages 46–55.The authors include G. Aggarwal and others. A Vision Paper on Giving Paranoids Their Own Personal Space. In the 2004 VLDB