International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1838110

Enhancing Privacy Preserving Query Retrieval Using Locality Sensitive Hashing

Archana M.S., K. Deepa

[1]Assistant Professor, Department of Computer Science, Nilgiri College of Arts and Science, Thaloor, The Nilgiris, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science, Providence College for Women, Coonoor, Ooty, Tamil Nadu, India

ABSTRACT

The usage of smart phones is tremendously increasing day by day. Due to this, Location Based Services (LBS) attracted considerably and becomes more popular and vital in the area of mobile applications. On the other hand, the usage of LBS leads to potential threat to user's location privacy. In this paper, the famous LBS provide information about points of interest (POI) in spatial range query within a given distance. For that, a more efficient and an enhanced privacy-preserving query solution for location based, Efficient Privacy-Location Query (EPLQ) is proposed along with Locality Sensitive Hashing (LSH) reduces the dimensionality of high dimensional data. Experiments are conducted extensively and the results show the efficiency of the proposed algorithm EPLQ in privacy preserving over outsourced encrypted data in spatial range queries. The proposed method performs in spatial range queries and similarity queries of privacy preserving.

Keywords: Location Based Services, points of interest, Efficient Privacy-Location Query, NICT

I. INTRODUCTION

Location Based Services (LBSs) are progressively in style in today's society. It's reportable that up to a 4.77 billion users are enjoying LBSs as of 2018 compared to 150 million during 2014 [1]. Users can get the required location information from LBS provider to get personalized services like restaurant recommendations, taxi reservations and map directions.

The idea of Location Based Services depends on long periods of advancement and intermingling of various advances and in addition a development of information society where context and customization of information is one of the principal needs for clients. Considering the background of LBS, it is a combination of various technologies such as Geographical Information System (GIS) and other spatial and situating advances, the Internet and the Web, and new data and correspondence advances (NICTs).

A framework is context-aware in the event that it utilizes context to give pertinent information as well as services to the client, where pertinence relies upon the client's task. Information or services can be activated with context information with several parameters mirroring the context of the client task. These parameters might be subdivided into spatial, personal, social, technical and physical context. The issueconnected with context- aware services is displaying those parameters in quantifiable and computable way. The spatiotemporal information about the client is one of few parameters that are clear and genuinely simple to quantify and utilize. This is connected to the term Location-Aware Services that may be characterized as context-aware services that use the location of the client to embrace the conduct of the services. It is a unique way of Location Based Services in a most broad sense as its services are connected with location data.

II. RELATED WORKS

M. Gruteser et al investigates a complimentary approach that concentrates on the principle of minimal collection. In this approach location-based services collect and use only de-personalized data that is practically anonymous data. But query encryption is not done and database is not outsourced.

M. F. Mokbel introduces Casper; a novel framework in which mobile users can entertain location based services without the need to disclose their private location information. Per query privacy and multi-location query are absent and inefficient in handling frequent attack are some of the drawbacks of this work.

R Shokri et al proposed an approach that protects the location privacy. In this approach, the mainstream approach to protecting the location-privacy of mobile users in location-based services (LBSs) is to alter the users' actual locations in order to reduce the location information exposed to the service provider. This method is inefficient in terms of handling frequent attacks. M. E. Andres et al.

G. Ghinita et al employed the Private Information Retrieval theory to guarantee privacy in location-dependent queries. The main drawback is query encryption is present but lacking in database outsourcing.

III. DESIGN GOAL

It is very challenging to propose a privacy preserving query for implementing LBS over the encrypted location data. Enhancing Processing of Query (EPQ) enables the cloud server to perform query processing without exposing client's location details. EPQ can insist on a client location coordinate query as per client's present location. Practically, the LBS application is mainly developed for the user who used to search his point of interest such as searching hotels nearest to him. In this work, the user query is secured with the keyword and encrypted. This will accurately identify the requested location and the distance between the target locations are classified and ranking will be given. Our system provides a multiuser environment as any number of users can log at a time. The following are the three main processes of our proposed work.

1. To propose a LBS query scheme which is more efficient and privacy preserving to protect the location data and the user's request. For this, a hybrid encryption technique to encrypt the outsourced location data is proposed. This scheme also supports multiuser cloud environment.
   - ✓ System Construction Module
   - ✓ LBS User Module
   - ✓ LBS Provider Module
   - ✓ Dimensionality Reduction Module – Locality Sensitive Hashing
   - ✓ Spatial Range Query For Privacy Preserving

1.1 POI Query Processing

POI query processing in privacy preserving is classified into two ways (i) Public LBS and (ii) Outsourced LBS. In public LBS, POI of spatial database is recorded by an LBS provider in plaintext. These queries are initiated at the provider's site. Outsourced LBS consists of three kinds of entities, LBS provider, Cloud and LBS users.

1) LBS data is abundant in LBS provider and these data are nothing but POI records. Authorized users are allowed by the LBS provider to access these data by passing location based queries. the LBS provider provides the query services through the cloud for getting operational and financial benefits of data outsourcing. But, the more valuable LBS data is not disclosed by LBS provider to the cloud. Hence, the LBS provider will outsource the encrypted LBS data to the cloud.

2) The cloud has abundant computing resources and storage. The encrypted LBS data from the LBS provider are stored and also provides query services for the users. So, in cloud, the encrypted POI records are searched in local storage for finding the data that matches the queries of LBS users.

IV. RESULT DISCUSSION

In the previous section, we have discussed about the modules for achieving the privacy preserving of location data. These modules are implemented using Java and MySQL. For accessing the location, we have implemented using J2ME as a mobile application. The experiments are carried out on Intel Core(TM) I3 Processor (2.27 GHz)

The system takes input from the users, processes it and produces an output. Input design is link that ties the information system into the world of its users. The system should be user-friendly to gain appropriate information to the user.

The project gives the low time consumption to make the sensitive application made simple. The fund that the company is willing to spend into the research and development of this system is very limited. The design of input covers all the phases of input from the creation of initial data to actual entering of the data to the system for processing.

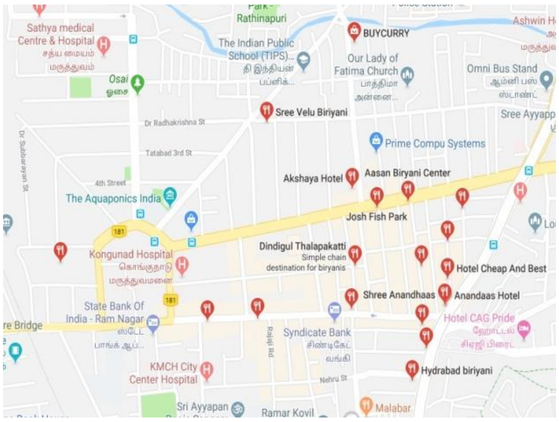

Figure 4.1 (a) POI in Coimbatore

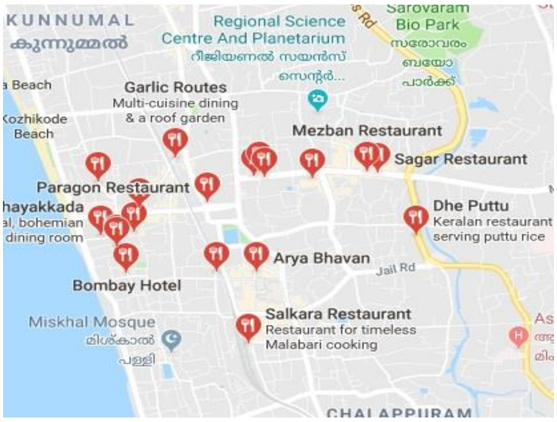

Figure 4.2 (b) POI in Calicut

V. CONCLUSION AND FUTURE WORK

In this paper, the famous LBS provide information about points of interest (POIs) in spatial range query within a given distance is discussed. For that, a more efficient and an enhanced privacy-preserving location-based query solution, Enhancing Privacy-Location Query (EPLQ) is proposed.

In specific, to obtain privacy preserving spatial range query, the first predicate-only encryption scheme for inner product range (IPRE) is proposed. This method is used to detect a privacy preserving way to find a position whether it is within a given circular area. The IPRE scheme has two vectors, attribute and predicate vectors. The problem with the proposed method is, when the numbers of attributes are increased, the latency time for retrieving data is also increased. Here, we apply locality sensitive hashing to reduce dimensionality thereby supporting k-nearest neighbor search.

VI. REFERENCES

[1]. Statista, "Number of location-based service users in the United States from2013 to 2018 (in millions)," Statista; 2017. https://www.statista.com/statistics/436071/location-based- service-users-usa

[2]. K. Xie, X. Ning, X.Wang et al., "Recover corrupted data in sensornetworks: a matrix completion solution," IEEE Transactions on Mobile Computing, vol. 16, no. 5, pp. 1434-1448, 2017.

[3]. M. Li, H. Zhu, Z. Gao et al., "All your Location are belong to us: breaking mobile social networks for automated user location tracking," in Proceedings of the 15th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2014, pp. 43-52, USA, August 2014.

[4]. J. Shao, R. Lu, and X. Lin, "FINE: a fine-grained privacy preserving location-based serviceframework for mobile devices," in Proceedings of the IEEE INFOCOM, pp. 244-252, IEEE, Ontario, Canada, May 2014.

[5]. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-Tan, "Private queries in location based services: anonymizers are not necessary," in Proceedings of the ACMSIGMOD International Conference on Management of Data (SIGMOD '08), pp. 121-132, ACM, 2008.

[6]. B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: architecture and algorithms," IEEE Transactions on Mobile Computing, vol. 7, no. 1, pp. 1- 18, 2008.

[7]. R. Paulet, M. G. Kaosar, X. Yi, and E. Bertino, "Privacy preserving and content-protecting location based queries," IEEE Transactions on Knowledge and Data Engineering, vol. 26,no.5, pp. 1200-1210, 2014.

[8]. L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10,no. 5, pp. 571-588, 2002.

Cite this article as :

Archana M.S, K.Deepa , "Enhancing Privacy Preserving Query Retrieval Using Locality Sensitive Hashing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 70-73 , January-February 2019.
Available at doi :
https://doi.org/10.32628/CSEIT1838110
Journal URL : http://ijsrcseit.com/CSEIT1838110