

Privacy Preserving Location Based Spatial Range Query over SS-Tree Index Structure

T. Shirisha, C. Shoba Bindu, P. Dileep Kumar Reddy

Department of CSE, JNTUA college of Engineering. Ananthapuramu, Andhra Pradesh, India

ABSTRACT

Based on IOT, the Location based services (LBS) and spatial range queries (SPG) have received great impact and became more popular and is absolutely needed in recent years. This leads to several issues such as increase in search latency, minimum numbers of queries for a user and known sample attacks. So, in order to overcome the issues in LBS, a coordinate transformation suite technique (CTS) based on ss-tree index structure has been proposed by Lichen et. al.,. They used Euclidean distance to calculate the distance between two locations. This paper replaces Euclidean distance with the great circle distance (GCD) to calculate the shortest distance between two locations. Using GCD in the scheme has increased the number of queries generated and the query latency has been decreased.

Keywords: Outsourced encrypted data, privacy-enhancing technology, SPG (spatial range query), coordinate transformation suite, LBS (Location-based services).

I. INTRODUCTION

Over the last few decades, LBS was used to control army force only. Today, with advances in technology LBS is used anywhere to find the location of any areas by using maps & navigation, tracking services, information services and applications also. SPG (spatial range query) is generally used in LBS, which allows user's interest (i.e.; location search for hotels, climate, traffic, weather reports, friend finders etc). It consists of GIS (geographic information system) service that is a collection of dimensional objects (points, lines, and polygons) related to point queries, range queries, k- nn queries and spatial join. Spatial query is supported by both geo-databases (database of geological data such as places, countries, official divisions and related information) and spatial databases (to load and concern data that execute objects describes in a dimensional space). GIS is an achieved system to maintain, store, manage, evaluate and execute geographic dimensional data. Spatial range query is an online mobile service in LBS, users are sensitive to query latency and it may be impossible to secure the query inspite of interruptions. There are many hacking techniques to find users location i.e.: Eye spy, find my friends, fake GPS fake

location, white pages, exposed installer etc. By utilizing these applications others can easily find where the particular user stayed in an area.

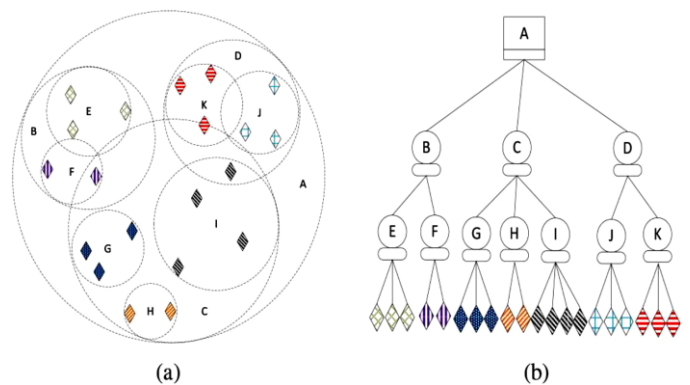


Figure 1: a) Point of distribution b) ss-tree structure[6]

Fig 1. (b) Shows the flow of users locations in ss-tree. It hides each node's location information using the predicate encryption technique proposed in [10] and removes unnecessary information. It provides two functions: detecting of matched nodes and intersection of circular areas. Euclidean distance is used to measure distance between two locations and generating minimum no. of queries by the user. With minimum no .of queries being generated the latency of finding a location is more. In order to reduce this latency, this

paper proposes a great circle distance between two points based on ss-tree index structure. This method generates more no. of queries for a user.

The rest of the paper is organized as follows: section 2 presents the related work: Section 3 presents the preliminaries: Section 4 presents the proposed approach: section 5 performance evaluation: Finally section 6 Concludes the paper.

II. RELATED WORK

Internet of things (IOT) is an advanced technology in which we can collect and exchange data by using some sensors in many areas. Here we encounter a problem as “How we protect user’s location to avoid hacking techniques in privacy way?”. If a user in current location wants to search another location, his location can be easily traced by hacker using fake GPS [7]. To overcome this problem many location based techniques were introduced by many researchers. Based on those techniques users can easily secure their information in an efficient way. PIR (private information retrieval) is a kind of technique in which the information of a particular user’s location can be protected against unauthorized PIR can be used to store all the users POI (point of interest) queries in privacy preserving manner [2].

To support spatial range query, an LBS user and provider should maintain minimum POIs queries by using PIR technique. But, recently CTS (coordinate transformation suite) is one of the techniques wherein it used to generate a encrypted query and calculates the distance between two locations of that query [1]. Actually, we can calculate the distance of two locations by using Euclidean distance (finding only straight line distance) [8]. At initial stage CTS will maintain the queries and store that query in LBS provider. By using the great circle distance instead of Euclidean distance we can calculate the distance in short period of time and generate the queries. To view that queries LBS user gets the secret key from LBS provider by using predicate encryption schema [10]. This schema generates the key for each and every query in the cloud and sends that key to users in an encrypted format. Otherwise, there is a chance of attack models such as cipher text attack, access pattern attack, plaintext attack, sample attack [4] and so on. In order to solve these problems similarity search structure [5] is needed as in

fig.1 for spatial range query. For indexing spatial data, there actually exist a few data structures such as multidimensional range search [3] and KNN search [9] used for privacy-preserving query, location data, e.g., the location data of points, circular areas, rectangular areas and single-dimension ranges must be concealed.

Lichen li et al [6] proposed the index structure for similar dimension which is used to determine whether a current position is within a given circular area in a secure preserving way. It allows testing the exactness of detecting matched records and the intersection of circular areas via inner product range without opening the user’s data in cloud (fig 1). However, ss-tree searches minimum no. of encrypted queries and increases the latency of a specific user location.

III. PRELIMINARIES

This section discusses some preliminaries required for proposed work. There are two different techniques used for LBS.

1) Coordinate transformation suite:

CTS help to find out a distance between two locations by using Euclidean distance. But Euclidean distance is used to measure only straight line distance. To overcome this problem we can replace the great circle distance instead of Euclidean distance. It helps to calculate the shortest distance between two locations. The following equation is used to find the GCD in a particular area.

$$D_{ns} = \frac{2r_E \Delta_{ns}}{360}$$

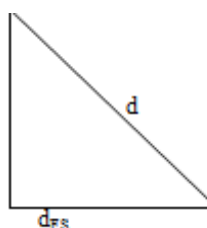
$$D = \sqrt{d_{ns}^2 + d_{ew}^2}$$


Fig2: Distances angle in GCD

D_{ns} represents distance from north to south, r_E represents radius of earth, Δ_{ns} represents angle between north to south likewise we can also calculate from east to west, D represents great circle distance.

2) SS-tree index structure:

As shown in fig 1.(b) SS-tree used to detect the matched records and intersection of circular areas. In this ss-tree hides each tree node’s location information using the predicate-only encryption

Scheme, and removes unnecessary information. Because of the encryption, detecting circular area intersection and matched records are also different when searching matched records with the tree.

IV. PROPOSED APPROACH

To implement CTS, the system model considers three entities: LBS provider, LBS user and cloud.

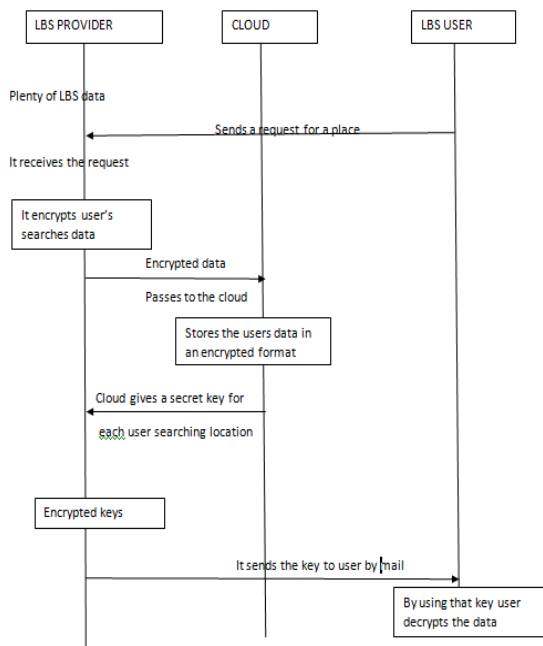


Figure 4: Sequence flow of LBS provider, cloud, LBS user

The system model shows that the CTS needed some basic applications to view the locations in a short period of time. There are two primary applications of coordinate system.

1. **Geographic information system:** GIS is a system achieves to collect, load, manage, evaluate, execute and present dimensional or geological data. Based on this GIS we can easily find the city map data and quickly identify where the user moves from one area to another.

2. **Projection:** It is nothing but transformations from one coordinate system to another.

To achieve the great circle distance we need some geo-data. To identify this geo-data, geodetic technique is used it gives the 2D and 3D dimensions on the spherical earth based tree structure. The UTM (Universal Transverse Mercator) is used to calculate Cartesian coordinate points present in 2D or 3D

dimension. By using this UTM, API key is used to generate the maps for particular location. Basically the queries must be increased in an encode format and reduces the latency by using this GCD.

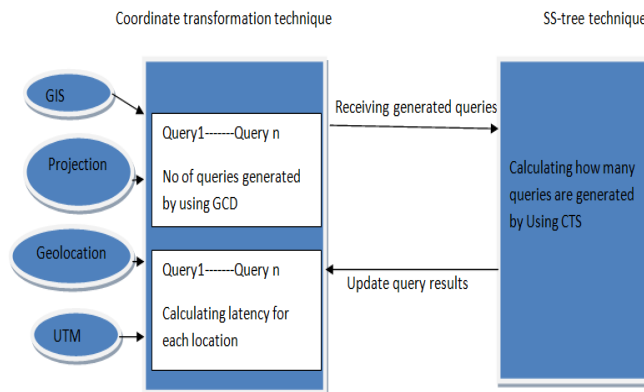


Fig 5: Coordinate transformation and ss-tree framework

The framework in fig. 5 shows the flow of calculating the generated query result by using applications of CTS. This paper uses the geometric objects from ESRI (environmental system research institute) in GIS, a software product for ARCGIS, web-GIS and geo-database management applications for experimentation. The geometric objects can also be obtained from various mapping frameworks such as ESRI, ARCGIS, JavaScript API and Google maps API.

V. PERFORMANCE EVALUATION

We tested this ss-tree and CTS technique using real time dataset on LBS providers. Dataset is downloaded from LBS geo location website [11] for GCD calculations. For experimental purpose, we considered four users locations for each LBS provider. As shown in Fig 2 we are calculated the shortest distance between two locations. By using GCD formula we get the final query result. The query result for four users searching locations at cloud side and user side.

Based on ss-tree and CTS techniques, the four users searches locations calculated by GCD to reduce the latency and increases the maximum number of queries. The final query result is very efficient to each and every user for searching their locations in a privacy preserving manner.

Users searches locations	SS-tree and CTS Technique using Euclidean	SS-tree and CTS Technique using Great Circle Distance
--------------------------	---	---

	Distance	
Hyderabad	20	35
Mumbai	22	34
Chennai	36	42
Delhi	42	48

Table 1: LBS users query efficiency at cloud side.

The above table shows the results after calculating query result using ss-tree and CTS techniques as well as ss-tree technique. We can observe that combining the two techniques the efficiency of the query result were clearly increased.

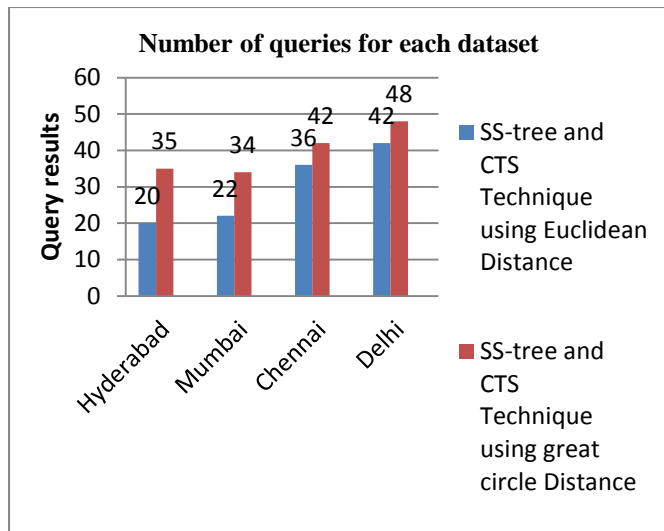


Figure 6 : Graphical representation of queries efficiency for each dataset.

Dataset	SS-tree latency using Euclidean distance	SS-tree latency using great circle distance
Hyderabad	3.5	2.8
Mumbai	4.3	3.2
Chennai	4.2	3.9
Delhi	4.2	3.7

Table 2: LBS users' latency at user's side

By combining the two techniques the latency of the query result were clearly reduced by using the GCD formula. The users query latency results for four LBS search locations based on real time analysis. The results are listed in above table.

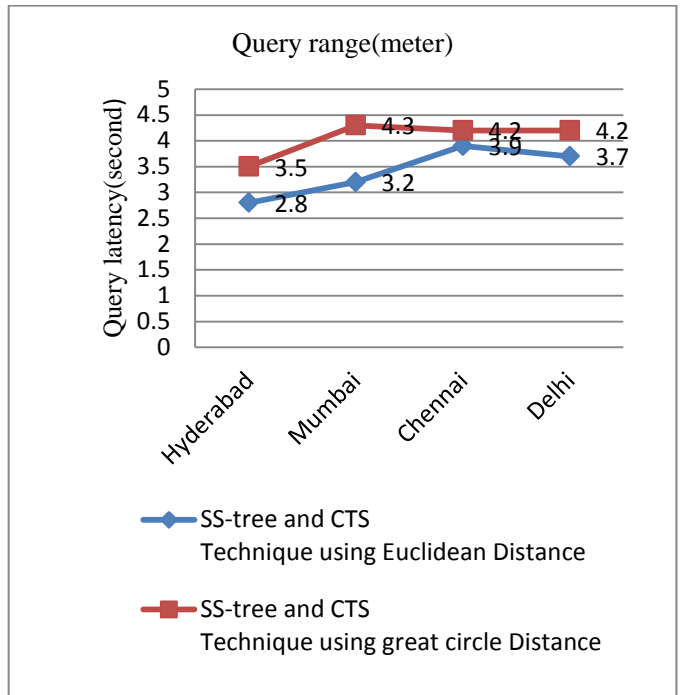


Figure 7 : Graphical representation of LBS users' latency at user's side.

VI.CONCLUSION

Coordinate transformation technique helps to calculate the distance between two locations. So, in this paper, we used a great circle distance to finding a shortest metric between two locations in order to enhance the efficiency of many queries and to reduce the query latency.

VII. REFERENCES

- [1]. A. Gutscher, "Coordinate transformation-A solution for the privacy problem of location based services?" in Proc. 20th Int. Parallel Distrib.
- [2]. Process. Symp. (IPDPS'06), Rhodes Island, Greece, Apr. 25-29, 2006, p. 424.
- [3]. A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," Pervasive Comput., vol. 2, no. 1, pp. 46-55, Jan./Mar. 2003
- [4]. B. Wang, Y. Hou, M. Li, H. Wang, and H. Li, "Maple: Scalable multidimensional range search over encrypted cloud data with tree-based index," in Proc. 9th ACM Symp. Inf. Comput. Commun. Secur., 2014, pp. 111-122.
- [5]. C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. Di Vimercati, and P. Samarati, "Location privacy protection through obfuscation-based

- techniques," in Proc. Data Appl. Secur. XXI, 2007, pp. 47–60.
- [6]. D. A. White and R. Jain, "Similarity indexing with the ss-tree," in Proc. 12th Int. Conf. Data Eng. (ICDE), 1996, pp. 516–523
- [7]. Lichuen Li, Rongxing Lu., IEEE, Senior Member and Cheng Huang Efficient searching Privacy Preserving Location-Based Query Over Outsourced Encrypted Data", in proc.7th,2016,pp.322-422.
- [8]. M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," VLDB J., vol. 19, no. 3, pp. 363–384, 2010.
- [9]. M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new Casper: Query processing for location services without compromising privacy," in Proc.32nd Int. Conf. Very Large Data Bases (VLDB'06), 2006, pp. 763–774.
- [10]. X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, "Practical k nearest neighbor queries with location privacy," in Proc. 30th Int. Conf. Data Eng. (ICDE), 2014, pp. 640–651
- [11]. Y. Elmehdwi, B. K. Samanthula, and W. Jiang, "Secure k-nearest neighbour query over encrypted data in outsourced environments," in Proc. IEEE 30th Int. Conf. Data Eng. (ICDE), 2014, pp. 664–675.
- [12]. Melia and Avenida, Madrid" LBS geolocation" <https://tmt.knect365.com/location-based-services/>, Accessed on june 2, 2017.