RESEARCH ARTICLE OPEN ACCESS

Geometric Range Queries For Security And Privacy Of Encrypted Spatial Data

M Uday Kumar [1] , S.DurgaPrasad [2]
Department of Computer Science Engineering,
Baba Institute of Technology and Sciences, AP

ABSTRACT
Spatial data comprise of geographic and geometric data primitives. Searching on spatial data is conveyed by geometric range queries. Nowadays, outsourcing the information to the cloud server is a trademark activity sold by a couple of cloud clients. The re-appropriated information may carry raw information. The cloud props are especially upgraded that pulls in various Location based Services associations. The general topic of the cloud information stays at the blocked off server is to be managed inconsequential calculation by information proprietor and information clients. The information is squeezed away in scrambled casing to maintain a strategic distance from mystery works out. Accomplish limit is one of the issues looked between cloud clients and LBS associations. Accessible encryption is a method to perform basic queries on scrambled data without uncovering security. Regardless, geometric range look on spatial data has not been completely dissected nor strengthened by existing open encryption plans. In this we plan a symmetric-key accessible encryption plot that can bolster geometric range ask for on scrambled spatial data. One of our certified obligations is that our structure is a general methodology, which can strengthen different sorts of geometric range queries. Constantly end, our system for scrambled data is free from the states of geometric range queries. In similar fashion, we besides broadening our plan with the additional function of tree structures to accomplish look multifaceted nature that is quicker than direct.

Keywords:- Geometric range queries, Spatial Data, Encrypted data.

I. INTRODUCTION

A spatial database, oversees multidimensional s, (for example, focuses, square shapes, and thus on.), and makes quick access to those items dependent on various selection criteria. The meaning of spatial databases is reflected by the accommodation of demonstrating elements of reality in a geometric fashion. For example, areas of eateries, lodgings, healing facilities, etc. are regularly talked to as focuses in a template, while bigger degrees, for example, parks, lakes, and scenes frequently as a mixture of square shapes. Numerous functionalities of a spatial database are helpful in different courses in explicit contexts. For instance, in a geology information framework, extend pursuit can be expressed to discover all eateries in a specific area, while closest neighbor recovery can find the eatery nearest to a fed position. Today, the boundless utilization of network search tools has made it practical to compose spatial queries in a fresh out of the box new way. Routinely, queries center around s' geometric properties just, for example, regardless of whether a point is in a square shape, or how close two points are from one another. We have found out some cutting edge applications that demand the capacity to choose objects depends on both of their geometric directions and their related writings. For example, it would be truly valuable if a web search tool can be used to find the closest restaurant that offers ―steak, spaghetti, and brandy‖ all in the interim. Note this isn't the ―globally‖ closest eatery (which would have been delivered by a conventional closest neighbor inquiry), yet the closest eatery among just those making all the requested nourishments and beverages. On that point are simple approaches to help queries that join spatial and high spots. For example, for the above question, we could initially bring every one of the eateries whose menus contain the arrangement of catchphrases {steak, spaghetti, brandy}, and after that from the recovered eateries, discover the most secretive one. Correspondingly, one could similarly do it conversely by focusing on first the spatial conditions—peruse every single of the eateries in climbing request of their separations to the inquiry point until experiencing one whose card has every one of the catch phrases. The real downside of these clear methodologies is that they will fail to give constant answers on troublesome data sources. A run of the mill precedent is that the genuine closest neighbor lies very far from the inquiry level, spell all the closer neighbors are missing no less than one of the question catchphrases. Spatial queries with

watchwords have not been broadly investigated. In the former age, the network has started eagerness by examining watchword seek in social databases.

II. RELATED WORK

An ordinary range seek has the accompanying structure: pre-prepared A lot of focuses for the hunt zone is located in the S-score can be exposed, or quickly. We take the ions of your scholarship and information abilities to portray scaly examine and different utilizations of related topics. Research territory is an wide variety of utilizations, which these information frameworks, PC designs, databases, states and times, various databases. Moreover, different events may have issues with the geometry zone fit as a violin. We ponder the mystery nearness tests: Alice and Bob to demonstrate that there is no information on some other pieces of the universe to unveil. We describe an assortment of conventions to guarantee private testing near the different dimensions of granularity. We have figured out how to utilize the area "labels" created by the designer to enhance the physical protection of the nearness test. In our framework we have actualized to educate Android, and its viability. Our framework utilizes interpersonal organizations (Facebook) to oversee open keys. With the entry of solid situating advancements and the pervasiveness of area based administrations, you can now precisely contemplate the spread of issues, for example, irresistible infections, malware and delicate information through a populace of versatile questions, for example, individuals, cell phones and vehicles. In such application situations, a protest goes between two s when the items are near enough (when they are equally far as anyone knows in contact) and once a question is begun, it can record the protest populace through the system the advancement of contacts between items, a arrangement of contacts called. In this we characterize and contemplate out of the blue the availability of the inquiry of a mass of data (which are on the circle) that enroll the development of a (conceivably vital) accumulation of points that are in a place for a more drawn out point. An inquiry for verification when two points are "open" by way of the contact organize spoken to by this advancing arrangement of ways. We provide two lists with contact subtleties that can be used to evaluate the sufficiency of these inquiries, regardless of the conceivably colossal size of all contact data. This all around acknowledged prologue to computational geometry is a reading material for undergrad and graduate college course of studies. The accent is on calculations and the book is perfect for PC and designing understudies. Divine guidance is offered in the fields of use: every one of the systems and strategies coming about because of computational geometry are identified with explicit applications in mechanical technology, realistic pictures, CAD/CAM and geographical information frameworks. This divine guidance is especially welcome for understudies. Present day information of computational geometry is applied to make organizations that are both feasible and straightforward and put to death. Every single fundamental strategy and disciplines of computational geometry, and likewise a little further developed themes, are studied. The book is to a great extent independent and can be used for self-contemplate by anybody with essential preparing in algorithmics. In this third release, notwithstanding updates to the second edition, new fields have been added to Voronoi outlines of course segments, the most remote Voronoi charts and reasonable information models.

III. METHODOLOGY

Client and server are two modules in our architecture. Client stores its spatial information on the waiter. In increase it also requires to perform geometric range queries over its outsourced data as presented in fig 1. The function of the geometric range query is to retrieve points inside the geometric range. The customer holds the secret key for both encryption and decoding of spatial information and geometric query. The server provides data warehousing and query processing services.

The host is required to correctly perform geometric range search on encrypted spatial data without decryption, means symmetric encryption and it returns results to the customer. Dynamic grid system, which divides user query into grids based on structure specified by the user and query server is identified as an intermediate between user and service supplier.

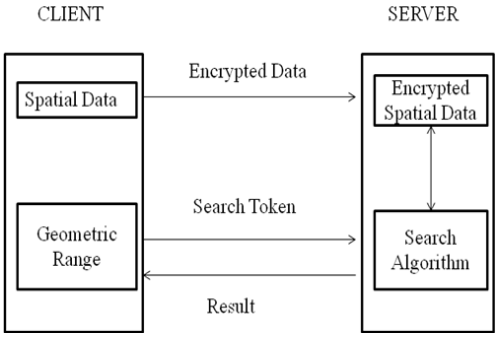

Figure 1: Model of GSE Scheme

Here we are using two techniques for searching the document

1) Restaurant Search,

2) Key Search.

Key Search: It means that the user can render the key in which dish that the restaurant is renowned for.This answers in the list of menu items displayed.

Restaurant Search: It means that the user can accept the list of eating houses which are situated very close. The list added up from the database.
O Map View

- Space Search
- Neighbor Search

A. ***Map View:-***

- The User can watch the position of their locality by Google Map (such as map view, satellite view).
- As our goal is to combine keyword search with the existing location-finding services to facilities such as hospitals, eating houses, hotels, and so on, we will focus on dimensionality 2, but our technique can be stretched out to arbitrary dimensionalities with no technical obstacle.
- Notice that the tilt of each word maintains a sorted order of point ids, which provides considerable convenience in query processing by permitting an efficient merge step. For instance, assume that we want to see the peaks that have words c and d. This is all important to calculate the convergence of the two words' inverted lists.

B. ***Space Search***

- The User can evaluate the distance and compute the time that leads them to arrive at the destination by giving speed. The chart will be developed by applying these values. None of these are done

By the utilization of Google Maps.

- The traditional nearest neighbor search returns the data point closest to a query point.
- We believe that the data set does not fit in memory, and asks to be indexed by efficient access methods in society to belittle the number of I/us in answering a question

C. ***Neighbor Search:***

- In this module we implement our neighbor Search. The other trouble with this search algorithm is that the indexing information has to be repeated in the broadcast cycle to enable twice scanning.
- The first scan is for determining the search range, and the second scan is for retrieving k objects based on the hunting range.
- Thus, we propose the Nearest Neighbor query approach to improve the preceding on-air query algorithm.
- The organization tries to affirm the validity of k

IV. PROPOSED METHOD

The suggested study is purely based on Symmetric Key Encryption scheme. The system model consists of three entities, namely, data owner, data user and cloud server. The chore of data owner is to preserve the data at cloud server, eventually focus on subduing the local cost searched by the data user. The task of cloud server is to offer services to the data owner and data users. Since, the cloud server is semi-trusted, the cloud service is dependable. The learning of range queries over the private a challenging project. The data owner stores the data in encrypted form, to preserve the is purely based on Symmetric Key The system model of our scheme is The system model consists of three entities, namely, data owner, data

user and cloud server. The project of keeping the data at cloud server, eventually focus on subduing the local price. The outsourced data will be looked for by the data user. The task of cloud server is to offer services to the data owner and data users. Since, the trustee, the cloud service is dependable. Range queries over the private information is a challenging job. The data owner stores the data in encrypted form, to keep the spatial data set. Our proposed algorithm supports range queries. The different geometric data is and then proceeded in the cipher text data. Algorithm eliminates the multiple cycles of communication between server and customer. Firstly, the points are denoted for data discs and then range queries are set from the set of geometric points.

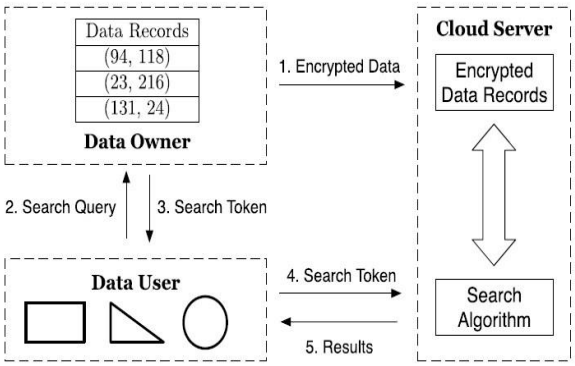

Fig. Proposed Architecture diagram

FastGeo Algorithm:

Input: Spatial data (D), geometric range queries (Q) and hidden key (SK).

Output: Returns points inside the geometric range.

STEP 1: Client generates secret key SK, and spatial data D, is conveyed in the form of dots.

STEP 2: Spatial information and geometric range queries Q, are converted into new form named equality-vector form instead of performing compute-then-compare operations.

STEP 3: Next building index for spatial data D, is created by considering spatial data as input and generates an index as output which is run by a customer.

STEP 4: Generated index need to be written in code by considering index and secret key SK, as an input and it operates on client side.

STEP 5: Geometric range query Q, which is converted into equality vector form is taken as an input for generating token with secret key SK, is sent to server.

STEP 6: client sends outsourced spatial data and search token T, to the server.

STEP 7:Server takes encrypted index end (T, SK), and search token T, as input and outputs set of identifiers IQ, in cipher text and the identifiers are transmitted to the customer.

STEP 8: Client learns the search results in the plain text by decrypting encrypted points locally.

STEP 9: Dynamic grid structure is used where query server QS, acts as an intermediate between user and service provider SP.

STEP 10: Finally, client generates points inside the geometric range specified by the user.

V. CONCLUSION AND FUTURE WORK

In this paper scheme is implemented, which supports geometric range search on encrypted spatial data without revealing data privacy and query privacy. Dynamic grid system is used in which provides better privacy guarantee by placing semi trusted third party termed query server (QS), which cannot drop or create a new message. Supports arbitrary geometric shapes and achieves sub linear search time and enables dynamic updates on encrypted spatial data.

Future research may include designing range searchable encryption achieving faster-than-linear search with regard to the number of data records, and studying searchable encryption schemes for other common geometric queries, such as simplex range (i.e., retrieving points that are inside a triangle).

References

[1] R. A. Popa, F. H. Li, and N. Zeldovich, “An ideal-security protocol for orderpreserving encoding,” in Proc. IEEE SP, May 2013, pp. 463–477.

[2] F. Kerschbaum and A. Schropfer, “Optimal average-complexity ideal- security order-preserving encryption,” in Proc. ACM CCS, 2014, pp. 275–286.

[3] B. Wang, Y. Hou, M. Li, H. Wang, H. Li, and F. Li, "Tree-based multi-dimensional range search on encrypted data with enhanced privacy," inProc. SECURECOMM, 2014, pp. 1–25.

[4] E.-O. Blass, T. Mayberry, and G. Noubir, "Practical forward-secure range and sort queries with update-oblivious linked lists," in Proc. PETS, 2015, pp. 81–98.

[5] B. Wang, M. Li, H. Wang, and H. Li, "Circular range search on encrypted spatial data," in Proc. IEEE ICDCS, Jun./Jul. 2015, pp. 794–795.

[6] [Online]. Available: http://aws.amazon.com/solutions/casestudies/

[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE SP, May 2000, pp. 44–55.

[8] C. Shahabi, L. Fan, L. Nocera, L. Xiong, and M. Li, "Privacy-preserving inference of social relationships from location data: A vision paper," in Proc. ACM SIGSPATIAL GIS, 2015, pp. 1–4.

[9] B. Chazelle, "Filtering search: A new approach to query-answering," SIAM J. Comput., vol. 15, no. 3, pp. 703–724, 1986.

[10] P. K. Agarwal and J. Erickson, "Geometric range searching and its relatives," Discrete Comput. Geometry, vol. 223, pp. 1–56, 1999.

AUTHOR DETAILS

M Uday Kumar is presently pursuing M.Tech (CST) Department of Computer Science Engineering from Baba Institute of Technology and Sciences,Visakhapatnam.

S.DurgaPrasad , M.TECH is working as an Associate Professor in the Department of Computer Science and Engineering in Baba Institute of Technology and Sciences, Visakhapatnam.