ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 8, August 2017

Fast Geo: Efficient Geometric Range Queries on Encrypted Spatial Data

A.S.Abdul Rahman[a], M.Phil and R. Banumathi[b], M.Phil. , M.Tech. (CSE)
[a]Research Scholar, Department of Computer Science, PRIST University, Thanjavur.
[b]Research Supervisor, Department of Computer Science, PRIST University, Thanjavur.

Abstract: Geometric range search is a fundamental primitive for spatial data analysis in SQL and NoSQL databases. It has extensive applications in location-based services, computer aided design, and computational geometry. Due to the dramatic increase in data size, it is necessary for companies and organizations to outsource their spatial data sets to third-party cloud services (e.g., Amazon) in order to reduce storage and query processing costs, but, meanwhile, with the promise of no privacy leakage to the third party. Searchable encryption is a technique to perform meaningful queries on encrypted data without revealing privacy. However, geometric range search on spatial data has not been fully investigated nor supported by existing searchable encryption schemes. In this paper, we design a symmetric-key searchable encryption scheme that can support geometric range queries on encrypted spatial data. One of our major contributions is that our design is a general approach, which can support different types of geometric range queries. In other words, our design on encrypted data is independent from the shapes of geometric range queries. Moreover, we further extend our scheme with the additional use of tree structures to achieve search complexity that is faster than linear. We formally define and prove the security of our scheme with in distinguish ability under selective chosen-plaintext attacks, and demonstrate the performance of our scheme with experiments in a real cloud platform.

Keywords: Geometric range, GPS, Symmetric key, encrypted data, queries.

I. INTRODUCTION

About ten years ago, the field of range searching, especially simplex range searching, was wide open. At that time, neither efficient algorithms nor nontrivial lower bounds were known for most range-searching problems. A series of papers by Haussler and We z [161], Clarkson [88, 89], and Clarkson and Shor [92] not only marked the beginning of a new chapter in geometric searching, but also revitalized computational geometry as a whole. Led by these and a number of subsequent papers, tremendous progress has been made in geometric range searching, both in terms of developing efficient data structures and proving nontrivial lower bounds. From a theoretical point of view, range searching is now almost completely solved. The impact of general techniques developed for geometric range searching "-nets, 1=r cuttings, partition trees, multi-level data structures, to name a few is evident throughout computational geometry. This volume provides an excellent opportunity to recapitulate the current status of geometric range searching and to summarize the recent progress in this area.

Range searching arises in a wide range of applications, including geographic information systems, computer graphics, spatial databases, and time-series databases. Furthermore, a variety of geometric problems can be formulated as a range-searching problem. A typical range-searching problem has the following form. Let S be a set of n points in Rd, and let R be a family of subsets of Rd; elements of R are called ranges. We wish to preprocess S into a data structure so that for a query range 2R, the points in S can be reported or counted efficiently. Typical examples of ranges include rectangles, half spaces, simplexes, and balls. If we are only interested in answering a single query, it can be done in linear time, using linear space, by simply checking for each point p 2 S whether p lies in the query range. Most applications, however, call for querying the same point set S several times (and sometimes we also insert or delete a point periodically), in which case we would like to answer a query faster by preprocessing S into a data structure. Range counting and range reporting are just two instances of range-searching queries. Other examples include emptiness queries, where one wants to determine whether S= ;, and optimization queries, where one wants to choose a point with certain property (e.g., a point in with the largest x1-coordinate). In order to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 4, Issue 8, August 2017

encompass all different types of range-searching queries, a general range-searching problem can be defined as follows. Let (S ;+) be a commutative semigroup1. For each point p 2 S, we assign a weight w (p) 2 S. For any subset S0 S, let w (S0)=Pp2S0 w(S), where addition is taken over the semigroup.2 For a query range 2R,we wish to compute w(S\). For example, counting queries can be answered by choosing the semi group to be (Z;+), where + denotes standard integer addition, and setting w(p) = 1 for every p 2 S; emptiness queries by choosing the semi group to be (f0;1g;) and setting w(p) = 1; reporting queries by choosing the semi group to be (2S;[) and setting w(p)=fpg; and optimization queries by choosing the semi group to be (R; max) and choosing w(p) to be, for example, the x1-coordinate of p. We can, in fact, define a more general (decomposable) geometric searching problem. Let S be a set of objects in Rd (e.g., points, hyper planes, balls, or simplexes), (S;+) a commutative semi group, w : S ! S a weight function, R a set of ranges, and S R a \spatial" relation between objects and ranges. Then for a range 2 R, we want to compute P pw (p). Range searching is a special case of this general searching problem, in which S is a set of points in Rd and =2. Another widely studied searching problem is intersection searching, where p if p intersects.

II. Related Works

(Log n) even when d = 1. Therefore, we would like to develop a linear-size data structure with logarithmic query time. Although near-linear-size data structures are known for orthogonal range searching in d into cells of dimensions .

III. System Analysis

While most of the searchable encryption schemes focus on common SQL queries, such as keyword queries and Boolean queries, few studies have specifically investigated geometric range search over encrypted spatial data. Wang et al. proposed a novel scheme to specifically perform circular range queries on encrypted data by leveraging a set of concentric circles. Some previous searchable encryptions handling order comparisons can essentially manage axis parallel rectangular range search on encrypted spatial data. Similarly, Order-Preserving Encryption, which has weaker privacy guarantee than searchable encryption, is also able to perform axis-parallel rectangular range search with trivial extensions. Ghinita and Rughinis particularly leveraged certain Functional Encryption with any ‘x’ ed dimension that can answer a query in poly logarithmic time, no similar bounds are known for range searching with more complex ranges such as simplexes or disks. In such cases, we seek a trade o between the query time and the size of the data structure How fast can a query be answered using O (n poly log n) space, how much space is required to answer a query in O (poly log n) time, and what kind of trade o between the size and the query time can be achieved? In this paper we survey the known techniques and data structures for range-searching problems and describe their applications to other related searching problems. As mentioned in the beginning, the quest for efficient range-searching data structure has led to many general, powerful techniques that have had a significant impact on several other geometric problems. The emphasis of this survey is on describing known results and general techniques developed for range searching, rather than on open problems. Let us consider a finite set H of lines in the plane. These lines divide the plane into convex sets called cells sometimes also the word faces is used of various dimension see. The cells of dimensions or cells for short are the intersections of the lines of H and we call them vertices If we remove all vertices lying on a line h H the line h is split into two open semi infinite rays and a finite number of open segments. These segments and rays form the cells or edges Finally by removing all the lines of H is the plane partitioned into open convex polygons also unbounded ones which are the cells Similarly a finite set H of hyper planes in IR d defines a decomposition of IR hierarchical encoding to efficiently operate axis-parallel rectangular range search on encrypted spatial data in the application of mobile users monitoring.

Disadvantages of Existing System:

- Most of the searchable encryption schemes focus on common SQL
- None of these previous works have particularly studied geometric range
- More importantly, there still lacks a general approach,

a. Proposed System

In this paper, we propose a symmetric-key probabilistic Geometric Range Searchable Encryption. With our scheme, a semi-honest (i.e., honest-but-curious) cloud server can verify whether a point is inside a geometric range over encrypted spatial datasets. Informally, except learning the necessary Boolean search result (i.e., inside or outside) of a geometric range search,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 4, Issue 8, August 2017

the semi-honest cloud server is not able to reveal any private information about data or queries.

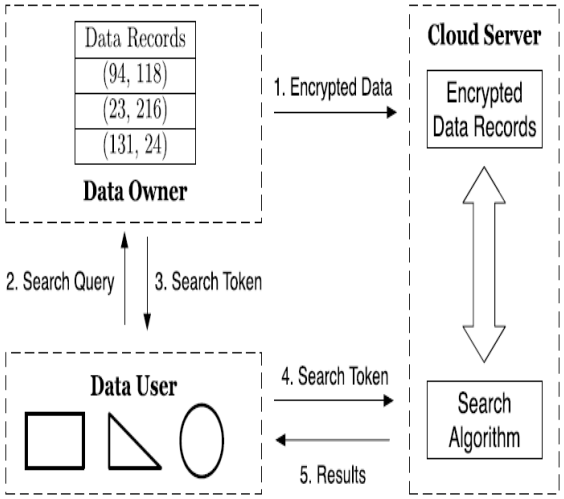
Our main contributions are summarized as follows:

- We present a symmetric-key probabilistic Geometric Range Searchable Encryption, and formally define and prove its security with in distinguish ability under Selective Chosen-Plaintext Attacks (IND-SCPA).
- The security of our scheme is formally defined and
- Our design has great potential to be used and implemented in wide applications,

Advantages of Proposed System:

than-linear search complexity regarding to the number of points in a dataset. The security of our scheme is formally defined and analyzed with in distinguish ability under Selective Chosen-Plaintext Attacks. Our design has great potential to be used and implemented in wide applications, such as Location-Based Services and spatial databases, where the use of sensitive spatial data with a requirement of strong privacy guarantee is needed.

b. System Architecture



IV. GEOMETRIC SEARCH

This paper considers an algorithmic problem called range searching. We describe the problem and outline current theoretical knowledge about it including the main ideas of several proofs and constructions Computational geometry general remarks The considered problems belong into the area of computational geometry In the rest of this section we brie y introduce this yield and mention some features and conventions which seem particular to it reader somewhat familiar with computational geometry may probably skip the rest of section safely Older computational geometry monographs of a wide scope are PS.

V. CONCLUSION

A general approach to securely search encrypted spatial data with geometric range queries. Specifically, our solution is independent with the shape of a geometric range query. With the additional use of R-trees, our scheme is able to achieve faster-

REFERENCES

[1]. D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," in Proc. of IEEE S&P'00, 2000.

[2]. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," in Proc. of ACM CCS'06, 2006.

[3]. S.Kamara,C.Papamanthou,and T.Roeder," Dynamic Searchable Symmetric Encryption," in Proc. of ACM CCS'12, 2012.

[4]. D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries," in Proc. of CRYPTO'13, 2013.

[5]. D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation," in Proc. of NDSS'14, 2014.

[6]. E. Stefanov, C. Papamanthou, and E. Shi, "Practical Dynamic Searchable Encryption with Small Leakage," in Proc. of NDSS'14, 2014.

[7]. G. Ghinita and R. Rughinis, "An Efficient Privacy-Preserving System for Monitoring Mobile Users: Making Searchable Encryption Practical," in Proc. of ACM CODASPY'14, 2014.

[8]. B. Wang, M. Li, H. Wang, and H. Li, "Circular Range Search on Encrypted Spatial Data," in Proc. of IEEE CNS'15, 2015.

[9]. H. Zhu, R. Lu, C. Huang, L. Chen, and H. Li, "An Efficient Privacy-PReserving Location Based Services Query Scheme in Outsourced Cloud," Ieee Trans. on Vehicular Technology.