Asia-pacific Journal of Convergent Research Interchange
Vol.2, No.3, September 30 (2016), pp. 21-28
http://dx.doi.org/10.21742/apjcri.2016.09.03

Data Encryption using Geometric Range

Bhargavi Nadella[1)]

Abstract

Geometric range scan is a key primitive for spatial information analysis in SQL and NoSQL databases. It has broad applications in area based administrations, PC aided design, and computational geometry. Due to the dramatic increase in information size, it is fundamental for organizations and associations to outsource their spatial informational indexes to outsider cloud administrations (e.g., Amazon) so as to decrease stockpiling and inquiry handling costs, at the same time, then, with the guarantee of no security spillage to the outsider. Searchable encryption is a system to perform significant inquiries on encoded information without uncovering security. In any case, geometric range seek on spatial information has not been completely researched nor upheld by existing searchable encryption plans. In this paper, we outline a symmetric-key searchable encryption plot that can bolster geometric range questions on encoded spatial information. One of our real commitments is that our plan is a general approach, which can bolster distinctive sorts of geometric range questions. At the end of the day, our plan on scrambled information is autonomous from the states of geometric range questions. In addition, we additionally develop our plan with the extra utilization of tree structures to accomplish look multifaceted nature that is speedier than straight. We formally characterize and demonstrate the security of our plan with indistinguishable capacity under specific picked plaintext assaults, and show the execution of our plan with trials in a genuine cloud stage (Amazon EC2).

Keywords : geometric, range search, spatial data, encrypted data, amazon.

1. Introduction

GEOMETRIC range search [1], [2] is a standout amongst the most basic inquiries performed on spatial information, where information are represented as points while queries can be depicted as geometric objects, such as triangles, circles, rectangles. It is an indispensable function, which is included in most SQL and NoSQL databases. For example, real database applications, for example, MySQL, Oracle, PostgreSQL (with extra utilization of PostGIS) andMongoDB, all give certain sorts of geometric range search. The reason for geometric range look on a spatial dataset is to recover focuses that are inside a specific geometric range (see some significant sorts of geometric range queries in Fig. 1).

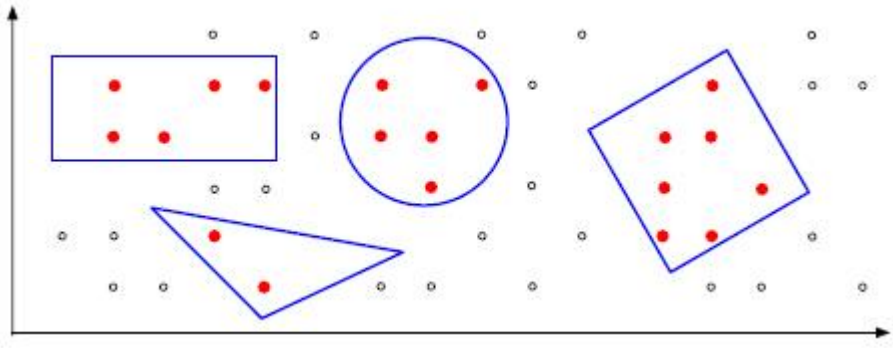
Geometric range search is a basic device for spatial information examination, and has wide

Received(April 25, 2016), Review Result(1st: May 13, 2016, 2nd: June 9, 2016), Accepted(September 10, 2016)

[1](Corresponding Author) Machine Intelligence Research Labs, India
email: nadella.bhargavi@gmail.com

ISSN: 2508-9080 APJCRI

applications in geometric data



[Fig. 1] (From left to right) axis-parallel rectangular range search, triangularrange search, circular range search, and non-axis-parallel rectangular rangesearch.

Systems, computer-aided design and computational geometry. For example, a versatile client can perform proximity testing to discover purpose of premiums, companions, bistros or approaching occasions near her in Location-Based Services, for example, Yelp and Foursquare, by running circular range search on spatial datasets [3]; an information analyzer can concentrate social reachability based on millions of users' location check-ins by evaluating multiple rounds of circular range queries [4]; a fashioner can make sense of what number of houses, structures and streets will be influenced if another air terminal will be set up by working geometric range look on a spatial dataset, where the state of this airplane terminal could be communicated as a rectangle or a triangle [5]; a medicinal analyst may need to inquiry a spatial dataset to gather data about patients with a specific malady (e.g., Ebola) in a specific geometric region (e.g., a city) to anticipate whether there will be a perilous episode.

With rapid advancements of social networks, Location-Based Services and mobile computing, the amount of information individuals make regular is developing drastically. It is no longer simple or even gainful for organizations/associations to keep up a huge measure of information locally[6-15]. In this way, it is regular to see organizations and associations, even real ones (e.g., Yelp, Expedia and NASA) [16], outsourcing their datasets (counting spatial datasets) to open cloud suppliers, for example, Google and Amazon. Be that as it may, since security and protection episodes continue occurring in the cloud, outsourcing datasets to open cloud benefits additionally builds protection worries from those organizations and their clients [17], [18]. Especially, by trading off cloud administrations, it is simple for an inside aggressor

(e.g., an inquisitive cloud director) to uncover information security of those organizations and inquiry protection of their clients, which ought to be kept classified because of legitimate and business issues or the affectability of information itself. For example, the leakage of spatial datasets outsourced by Foursquare by means of the break of Amazon Web Services would jeopardize millions of users' private location information.

2. Proposed system

2.1 Related work

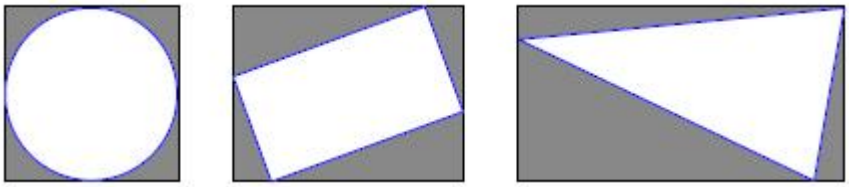
As we mentioned, the vast majority of the searchable encryption schemes [17], concentrate on keyword search (normally with the use of inverted indices or dictionaries), which are not appropriate for spatial information. In this area, we exhibit a few works that are firmly identified with geometric range search on encrypted information. Besides, we likewise clarify the test of planning a general answer for secure geometric range search.

2.1.1 Axis-Parallel rectangular range search

Some past searchable encryptions taking care of request examinations [6-9], [13], [14] can basically oversee axisparallel rectangular range look on encoded spatial information. Thus, Order-Preserving Encryption [10-12], which has weaker protection ensure than searchable encryption, is likewise ready to perform pivot parallel rectangular range look with unimportant augmentations. Ghinita and Rughinis especially utilized certain Functional Encryption [6] with various leveled encoding to productively work hub parallel rectangular range seek on scrambled spatial information in the utilization of portable clients checking.

Unfortunately, none of them are able to directly support different sorts of geometric range inquiries, for example, non-axisparallel rectangles, circles and triangles. Take note of that creating a negligible jumping hub parallel rectangle for any geometric question, e.g., a triangle, a circle or a non-axis-parallel rectangle, would be an option alternative for those previous plans to construct a general arrangement supporting distinctive sorts of geometric range inquiries. Be that as it may, this option strategy will present high false positive rates, where these false positives show focuses are inside the insignificant bouncing pivot parallel rectangle however are not inside the first geometric protest (see cases in Fig. 2). Besides, these false positives will turn out to be much more awful in higher dimensions.

ISSN: 2508-9080 APJCRI



[Fig. 2] Minimal bounding axis-parallel rectangles for different types of geometric objects, where dark areas represent all the false positives.

2.1.2 Circular Range Search

A very recent work [15] is able to particularly manage circular range search on encrypted spatial information. Its fundamental thought is to use an arrangement of concentric circles to speak to a roundabout range inquiry. All the more particularly, if an information point is on the limit of one of those concentric circles produced by the roundabout range inquiry, then it is a point inside the round range question. In any case, this thought with concentric circles is appropriate for round range inquiries however not for other geometric range queries.

2.1.3 Secure Multi-Party Computation on Computational Geometry

Past works in Secure Multi-party Computation on computational geometry are likewise firmly identified with the theme we contemplated in this paper. With these works, two gatherings (e.g., Alice and Bob) can secretly figure and test whether a point is inside a geometric range. So also, a portion of the current works [3], in private nearness testing, which can help two clients to safely check whether one client is inside a hover of another client based their private areas, are additionally worked from Secure Multi-party Computation. In any case, these works in view of Secure Multi-party Computation typically require broad rounds of communications between two gatherings. While we aiming at a design with no interactions during the evaluation on encrypted information.

2.2. Existing System

While the greater part of the searchable encryption plans concentrate on basic SQL inquiries,

such as keyword and Boolean inquiries, few reviews have particularly explored geometric range look over encrypted spatial information.

Wang et al.[13] proposed a novel plan to specifically perform circular range inquiries on encrypted information by utilizing an arrangement of concentric circles. Some past searchable encryptions taking care of request examinations can basically oversee pivot parallel rectangular range look on encrypted spatial information. Similarly, Order-Preserving Encryption, which has weaker security ensure than searchable encryption, is additionally ready to perform axis-parallel rectangular range search with trivial extensions.

Ghinita and Rughinis especially leveraged certain Functional Encryption with hierarchical encoding to productively work axis-parallel rectangular range look on encrypted spatial information in the utilization of mobile users monitoring[6].

2.2.1 Disadvantage of Existing System

Most of the searchable encryption schemes concentrate on basic SQL inquiries, such as keyword queries and Boolean queries, few reviews have particularly explored geometric range seek over encrypted spatial information.

Inevitably presents obstacles in terms of search functionalities over encoded information. None of these past works have especially concentrated geometric range inquiries which are communicated as non-axis-parallel rectangles or triangles.

More vitally, there still does not have a general approach, which can adaptably and safely bolster diverse sorts of geometric range inquiries over encoded spatial information regardless of their specific geometric shapes.

2.3 Proposed System

In this paper, we propose a symmetric-key probabilistic Geometric Range Searchable Encryption. With our plan, a semi-honest (i.e., honest-but-curious) cloud server can confirm whether a point is inside a geometric range over encrypted spatial datasets. Casually, aside from taking in the essential Boolean output (i.e., inside or outside) of a geometric range look, the semi-genuine cloud server is not ready to uncover any private data about information or questions.

Our primary contributions are outlined as takes after: We exhibit a symmetric-key probabilistic Geometric Range Searchable Encryption, and formally characterize and demonstrate

its security with indistinguishability under Selective Chosen-Plaintext Attacks (IND-SCPA).

In expansion, our inquiry procedure is non-intuitive on encoded information. As far as inquiry multifaceted nature, our benchmark plot acquires straight intricacy (concerning the quantity of information records), and its propelled variant acknowledges speedier than-direct hunt by incorporating with tree structures.

Our configuration is a general approach, which can safely bolster diverse sorts of geometric range questions on encoded spatial information paying little heed to their geometric shapes. Moreover, our plan is appropriate for geometric range inquiries, as well as perfect with other normal sorts of geometric questions, for example, crossing point inquiries and point nook inquiries, over encrypted spatial information.

2.3.1 Advantages of Proposed System

The security of our plan is formally characterized and analyzed with indistinguishability under Selective Chosen-Plaintext Attacks.

Our configuration can possibly be utilized and actualized in wide applications, such as Location-Based Services and spatial databases, where the utilization of delicate spatial information with a necessity of solid security assurance is required.

[Fig 3] System Architecture

3. Conclusion

We studied 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-than-linear

search complexity regarding to the number of points in a dataset. The security of our scheme is formally defined and analyzed with indistinguishability 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, wherethe use of sensitive spatial data with a requirement of strong privacy guarantee is needed.

References

[1] B. Chazelle, Filtering search: A new approach to query-answering, SIAM J. Comput., **(1986)**, Vol.15, No.3, pp.703-7240.

[2] P. K. Agarwal and J. Erickson, Geometric range searching and its relatives, Discrete Comput. Geometry, **(1999)**, Vol.223, pp.1-56.

[3] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, Location privacy via private proximity testing, Proc. NDSS, **(2011)**.

[4] H. Shirani-Mehr, F. Banaei-Kashani, and C. Shahabi, Efficient Reachability Query Evaluation in Large Spatiotemporal Contact Datasets, Proc. VLDB Endowment, **(2012)**, Vol.5, No.9, pp.848-859.

[5] M. de Berg, O. Cheong, M. van Kreveld, and M. Overmars, Computational Geometry: Algorithms and Applications, Springer-Verlag, **(2008)**; Berlin, Germany.

[6] D. Boneh and B. Waters, Conjunctive, subset, and range queries onencrypted data, Proc. Theory Cryptogr. (TCC), **(2007)**, pp.535-554.

[7] E. Shi, J. Bethencourt, T. H. H. Chan, D. Song, and A. Perrig, Multidimensional range query over encrypted data, Proc. IEEE SP, **(2007)** May, pp.350-364.

[8] Y. Lu, Privacy-preserving logarithmic-time search on encrypted data incloud, Proc. NDSS, **(2012)**, pp.1-17.

[9] B. Wang, Y. Hou, M. Li, H. Wang, and H. Li, Maple: Scalable multidimensional range search over encrypted cloud data with tree-based index, Proc. ACM ASIA CCS, **(2014)**, pp.111-122.

[10] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, Order preserving encryption for numeric data, Proc. ACM SIGMOD, **(2004)**, pp.563-574.

[11] R. A. Popa, F. H. Li, and N. Zeldovich, An ideal-security protocol fororder-preserving encoding, Proc. IEEE SP, **(2013)** May, pp.463-477.

[12] F. Kerschbaum and A. Schropfer, Optimal average-complexity ideal security order-preserving encryption, Proc. ACM CCS, **(2014)**, pp.275-286.

[13] B. Wang, Y. Hou, M. Li, H. Wang, H. Li, and F. Li, Tree-based multidimensional range search on encrypted data with enhanced privacy, Proc. SECURECOMM, **(2014)**, pp.1-25.

[14] E. O. Blass, T. Mayberry, and G. Noubir, Practical forward-securerange and sort queries with

update-oblivious linked lists, Proc. PETS, **(2015)**, pp.81-98.

[15] B. Wang, M. Li, H. Wang, and H. Li, Circular range searchon encrypted spatial data, Proc. IEEE ICDCS, **(2015)** Jun./Jul, pp.794-795.

[16] http://aws.amazon.com/solutions/case-studies/, July 22 **(2015)**.

[17] D. X. Song, D. Wagner, and A. Perrig, Practical techniques for searches on encrypted data, Proc. IEEE SP, (2000) May, pp.44-55.

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

[19] J. Katz and Y. Lindell, Introduction to Modern Cryptography: Principlesand Protocols. Boca Raton, FL, USA: CRC Press, **(2007)**.

[20] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, Publickey encryption with keyword search, Proc. EUROCRYPT, **(2004)**, pp.506-522.

[21] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, Searchable symmetric encryption: Improved definitions and efficient constructions, Proc. ACM CCS, **(2006)**, pp.79-88.

[22] S. Kamara, C. Papamanthou, and T. Roeder, Dynamic searchable symmetric encryption, Proc. ACM CCS, **(2012)**, pp.965-976.

[23] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, Expressive searchon encrypted data, Proc. ACM ASIA CCS, **(2013)**, pp.243-251.

[24] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking, Proc. ACM AISA CCS, **(2013)**, pp.71-82.