A Review: Fast-Geo Geometric Range Queries on Spatial Data

Jyoti[1], Neeraj Verma[2]
[1]*Student, Department of Computer Science Engineering, Prannath Parnami Institute of Management and Technology, Chaudharywas, Hissar, Haryana, India*
[2]*Assistant Professor, Department of Computer Science Engineering, Prannath Parnami Institute of Management and Technology, Chaudharywas, Hissar, Haryana, India*

Abstract- Spatial data have wide applications, e.g., location-based services, and geometric range queries (i.e., finding points inside geometric areas, e.g., circles or polygons) are one of the fundamental search functions over spatial data. The rising demand of outsourcing data is moving large-scale datasets, including large-scale spatial datasets, to public clouds. Meanwhile, due to the concern of insider attackers and hackers on public clouds, the privacy of spatial datasets should be cautiously preserved while querying them at the server side, especially for location based and medical usage.

Keywords- Fast-Geo, Geometric Range, Spatial Data etc.

I. INTRODUCTION

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 (Amazon EC2).

- 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 hierarchical encoding to efficiently operate axis-parallel rectangular range search on encrypted spatial data in the application of mobile users monitoring.

II. LITERATURE SURVEY

In [1], we examine protection safeguarding tests for nearness: Alice can test in the event that she is near Bob without either party uncovering whatever other data about their area. We portray a few secure conventions that help private vicinity testing at different levels of granularity. We examine the utilization of "area labels" created from the physical condition with a specific end goal to reinforce the security of vicinity testing. We actualized our framework on the Android stage and provide details regarding its viability. Our framework

utilizes an informal organization (Facebook) to oversee client open keys.

In [2], we present another system for tackling issues of the accompanying structure: pre-process an arrangement of items so those wonderful a given property as for a question protests can be recorded adequately. Among surely understood issues to fall into this class we discover go question, point fenced in area, crossing point, close neighbor issues, and so on. The approach which we take is extremely broad and lays on another idea called filtering look. We appear on various illustrations how it can be utilized to enhance the multifaceted nature of referred to calculations and improve their usage too. Specifically, sifting seek enables us to enhance the most pessimistic scenario many-sided quality of the best calculations known so far for taking care of the issues said above.

In [3], Searchable encryption is a promising technique enabling meaningful search operations to be performed on encrypted databases while protecting user privacy from untrusted third-party service providers. However, while most of the existing works focus on common SQL queries, geometric queries on encrypted spatial data have not been well studied. Especially, circular range search is an important type of geometric query on spatial data which has wide applications, such as proximity testing in Location-Based Services and Delaunay triangulation in computational geometry. In this paper, we propose two novel symmetric-key searchable encryption schemes supporting circular range search. Informally, both of our schemes can correctly verify whether a point is inside a circle on encrypted spatial data without revealing data privacy or query privacy to a semi-honest cloud server. We formally define the security of our proposed schemes, prove that they are secure under Selective Chosen-Plaintext Attacks, and evaluate their performance through experiments in a real-world cloud platform (Amazon EC2). To the best of our knowledge, this paper represents the first study in secure circular range search on encrypted spatial data.

In [4], Location-based service (LBS) is booming up in recent years with the rapid growth of mobile devices and the emerging of cloud computing paradigm. Along with the challenges to establish LBS and the user privacy issue becomes the most important concern. So successful privacy-preserving LBS must be secure and provide accurate query results. In this paper we present a solution to one of the location-based query problems that provide privacy for the user's location . This mainly focused spatial range query,. In this paper, aiming at spatial range LBS is giving the data about the interested area within a given boundary, here i present an efficient and privacy-preserving location based query solution (EPLQ). This mainly look to provide privacy preserving spatial range query, it use the predicate only encryption scheme for inner product range, that can find out whether a position is within a given circular area in a privacy-preserving way or not. This use tree model structure (ss^tree) for minimize searching time.

In [5], In recent years, database as a service (DAS) model where data management is outsourced to cloud service providers has become more prevalent. Although DAS model offers lower cost and flexibility, it necessitates the transfer of potentially sensitive data to untrusted cloud servers. To ensure the confidentiality, encryption of sensitive data before its transfer to the cloud emerges as an important option. Encrypted storage provides protection but it complicates data processing including crucial selective record retrieval. To achieve selective retrieval over encrypted collection, considerable amount of searchable encryption schemes have been proposed in the literature with distinct privacy guarantees. Among the available approaches, oblivious RAM based ones offer optimal privacy. However, they are computationally intensive and do not scale well to very large databases. On the other hand, almost all efficient schemes leak some information, especially data access pattern to the remote servers. Unfortunately, recent evidence on access pattern leakage indicates that adversary's background knowledge could be used to infer the contents of the encrypted data and may potentially endanger individual privacy.

In this paper, we introduce a novel construction for practical and privacy-aware selective record retrieval over encrypted databases. Our approach leaks obfuscated access pattern to enable efficient retrieval while ensuring individual privacy. Applied obfuscation is based on differential privacy which provides rigorous individual privacy guarantees against adversaries with arbitrary background knowledge.

III. APPLICATION OF FAST-GEO GEOMETRIC RANGE

♦ Spatial data have wide applications, e.g., location-based services, and geometric range queries (i.e., finding points inside geometric areas, e.g., circles or polygons) are one of the fundamental search functions over spatial data.

♦ The rising demand of outsourcing data is moving large-scale datasets, including large-scale spatial datasets, to public clouds. Meanwhile, due to the concern of insider attackers and hackers on public clouds, the privacy of spatial datasets should be cautiously preserved while querying them at the server side, especially for location-based and medical usage.

IV. CHALLENGES OF FAST-GEO GEOMETRIC RANGE

- The method incurs higher storage overhead and not guarantees the security.
- Confidentiality parameter is achieved, over encrypted data was unsuccessful.

V. EXISTING METHOD

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.

Axis-Parallel rectangular range search

Some past searchable encryptions taking care of request examinations [6-9], [13], [14] can basically oversee axis parallel 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-axis parallel 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. 1). Besides, these false positives will turn out to be much more awful in higher dimensions

Fig.1: Minimal bounding axis-parallel rectangles for different types of geometric objects, where dark areas represent all the false positives

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.

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 [16], 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 us aiming at a design with no interactions during the evaluation on encrypted information.

Search Algorithm:

A **search algorithm** is the step-by-step procedure used to locate specific data among a collection of data. It is considered a fundamental procedure in computing. In computer science, when **searching** for data, the difference between a fast

application and a slower one often lies in the use of the proper **search algorithm**.

Polynomial Time Algorithm:
An algorithm that is guaranteed to terminate within a number of steps which is a polynomial function of the size of the problem. See also computational time complexity. Search the data without loss of time to provide out stream for the process.

Sweeping Algorithm:
In computational geometry, a sweep line algorithm or plane sweep algorithm is an algorithmic paradigm that uses a conceptual sweep line or sweep surface to solve various problems in Euclidean space.

VI. CONCLUSION

We survey FastGeo an efficient two-level search scheme that can operate geometric ranges over encrypted spatial datasets. We studied a general approach to securely search encrypted spatial data with geometric range queries. Specifically, new solution is independent with the shape of a geometric range query. The security of our scheme is formally defined and analyzed with in distinguishability under Selective Chosen-Plaintext Attacks.

VII. REFERENCES

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

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

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

[4]. 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, 2015.

[5]. M. Kuzu, M. S. Islam, and M. Kassntarcioglu, "Efficient Privacy- Aware Search over Encrypted Databases," in ACM CODASPY'14, 2014, pp. 249–256.

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