International Journal of Research Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

Analysis Of Secure Geometric Range Search Over Encrypted Spatial Data

APARNA MITUKULA
PG Research Scholar
SR Engineering College
Warangal, telangana, India
Mitukulaaparna123@gmail.com

T. SAMPATH KUMAR
Senior Assistant Professor in CSE
SR Engineering College,
Warangal, telangana, India
tsk0707@gmail.com

ABSTRACT: The overall subject matter of the cloud data is existing on the remote server is to be controlled with minimal computation by means of data owner and data users. The data is stored away in encrypted form to save our anonymity activities. Reachability is one of the issues faced by cloud customers and LBS groups. A novel and light-weight scheme, named, Geometric Range Search Model (GRSM) that retrieves the quest data from cipher text dataset. The information is taken into consideration as factors and the group of factors denotes the cipher text database. Bloom filter is the that includes all viable combination of seeking tokens. The proposed GRSM comprise three levels, namely, Encryption segment, Token technology segment and Search Each section serves as input/ output to retrieve the search statistics. An investigational result shows the effectiveness of the proposed set of rules.

KEYWORDS-Data outsourcing, cloud technologies, location-based services(LBS), bloom filter and search tokens.

I. INTRODUCTION

Geometric range search [1], [2] is one of the maximum essential queries done on records, in which information are represented as points at the same time as queries can be described as geometric objects, inclusive of triangles, circles, rectangles. It is an integral function, that's blanketed in most SQL and NoSQL databases. For example, foremost database packages, together with MySQL, Oracle, PostgreSQL (with additional use of PostGIS) and MongoDB, all provide positive sorts of geometric range search. The reason of geometric range seek on a spatial dataset is to retrieve points which can be interior a selected geometric variety (see a few essential kinds of geometric variety queries in Fig. 1).Geometric range seek is a critical device for spatial data evaluation, and has extensive applications in geometric data systems, computer-aided design, and computational geometry. For instance, a cellular consumer can carry out proximity trying out to find factor of interests, buddies, coffee stores or incoming activities near her in Location-Based Services, such as Yelp and Foursquare, by using jogging round variety search on spatial datasets [3]; a facts analyzer can take a look at social reachability based totally on hundreds of thousands of customers' area check-ins by means of evaluating a couple of rounds of circular variety queries [4]; a dressmaker can determine out what number of homes, homes, and roads can be affected if a new airport can be installed with the aid of running geometric range search on a spatial dataset, in which the form of this airport could be expressed as a rectangle or a triangle [5]; a medical researcher can also want to query a spatial dataset to accumulate information about medical with a particular ailment (e.g., Ebola) in a sure geometric region (e.g., a city) to predict whether or not there might be a risky outbreak.

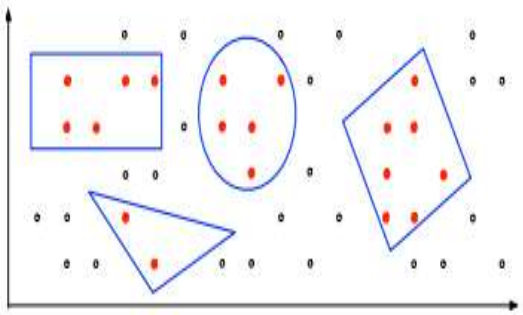

Fig. 1.(From left to right) axis-parallel rectangular range search, triangular range search, circular range search, and non-axis-parallel rectangular range search. with fast tendencies of social networks, location-based services, and mobile computing, a number of data humans create every day is growing dramatically. it is not longer easy profitable for organizations to hold a lot of quantity of statistics domestically. Thus it's far common place to see companies and corporations, even main ones (e.g., Yelp, Expedia, and NASA) [16], outsourcing their datasets (which include spatial datasets) to public cloud vendors, such as Google and Amazon. However, on the grounds that safety and privacy incidents maintain occurring in the cloud, outsourcing datasets to public cloud offerings additionally will increase privateness worries from the one's businesses and their users [17], [18]. Particularly, with the aid of compromising cloud services, it is simple for an internal attacker (e.g., a curious cloud administrator) to reveal records privacy of those organizations and query privacy in their users, which need to be saved confidential due to criminal and business troubles or the sensitivity of information itself. For example, the leakage of spatial datasets outsourced by using Foursquare thru the breach of Amazon Web Services would jeopardize thousands and thousands of users' personal region data.

Searchable encryption [3] is the stereotype of encryption technique which most recently studied by the research community. It executes search operations on the encrypted databases. By doing that, the privacy service of the data should be obtained from semi-trusted third party service providers. The cloud users are unaware of their data location. Thus, the client performs search the operation to the server and obtains its results. Prior work depicts that the server's execution from the result set of encrypted documents and its security parameters like data dimension and documents. Better the privacy design, better the search operation. Reachability is one of the parameters that depict that the server's execution from the result set of the search operation. location can notify from Location Based Services (LBS) [4] such as Google Maps, Foursquare etc. this scenario motivates to study about the reachability analysis of cloud data. Since, the data volume increases, the need for LBS companies are increased. In order to provide better information retrieval process, the security and privacy issues should be devised properly [5]. Though the concept of this searchable encryption is examined previously, the security and privacy challenges are not yet accomplished. Some additional security index was used for the data search process. In this paper, we suggest a geometric range search process over the encrypted data, so as to enhance the data privacy. Geometric queries are the queries that deal with spatial data. The data is denoted as 'points' and queries are portrayed as geometric objects like a triangle, spheres, and rectangles.

II. BACKGROUND WORKS

This section describes the prior work carried out by researchers. Previously, data utilization method is performed over the plaintext search. Due to an increase of the cloud users, the search operation is given importance. Usually, Boolean search operation [6] was performed by the server to yield better results. This search fails to give better security to the cloud data. The data is being stored in the cloud using 'inner- product similarity'. Search over encrypted data is still in its infancy. Initially, multi-keyword ranked search was introduced by Information Retrieval System (IRS). Latent Semantic Analysis (LSA) was used to retrieve the matched data. Latent values between terms and documents were used for finding the finding the association. Further, K-NN

classification technique is used for generating the security index.

Secure Multi-party Computation on Computational Geometry. Previous works in Secure Multi-party Computation on computational geometry are also closely related to the topic we studied in this paper. With these works, two parties (e.g., Alice and Bob) are able to privately compute and test whether a point is inside a geometric range. Similarly, some of the recent works [3in private proximity testing, which can help two users to securely verify whether one user is inside a circle of another user based their private locations, are also built from Secure Multi-party Computation. However, these works based on Secure Multi-party Computation normally require extensive rounds of interactions between two parties. While we are aiming at a design with interactions during the evaluation on encrypted data.Challenges for Building a General Solution. Normally, we have some standard methods to test whether a point is a geometric object in the plaintext domain [2]. For example, to check whether a point is inside an axis-parallel rectangle, we can respectively compare the X-axis and Y-axis of a point with the X-axis and Y-axis of the lower-left corner and upper-right corner of this axis-parallel rectangle. For circular range search, we can simply compute the distance between a point and the center of a query circle and then compare this distance with the radius of the query circle. For other geometric range search representing in more general forms of polygons, such as non-axis-parallel rectangles and triangles, we can compute cross products, and compare the results of cross products with 0 (i.e., positive or negative)[5]. Unfortunately, directly using different methods to operate these preceding geometric range queries on encrypted data will introduce challenges for designing a general geometric range searchable encryption, which is expected to flexibly support different types of geometric range queries.

First of all, due to the inefficiency of fully homomorphic encryption on arbitrary functions, practically evaluating different types of operations on encrypted data generally relies on different cryptography primitives. For instance, order-preserving encryption is only suitable for evaluating order comparisons; deterministic encryption (e.g., a pseudorandom function [19]) is only useful for quality checking; additive homomorphic encryption (e.g..paillier) only applies to additions. As a result, leveraging different cryptographic primitives in a parallel or onion manner (e.fg. cryptDBin) can support different operations over encrypted data simultaneously, but it inevitably introduces additional overheads for initializing the system, managing multiple secret keys, and generating multiple ciphertexts with different primitives.

III. PROPOSEDWORK

The proposed work is purely based on Symmetric Key Encryption scheme. The system model of our scheme is given in Fig.1. The system model consists of three entities, namely, data owner, data user and cloud server. The task of the data owner, data user, and cloud server. The task of data owner is to preserve the data at cloud server, eventually, focus on reducing the local cost. The task of the cloud server is to provide service is reliable. The learning of range queries over the private information is a challenging task. The data owner stores the data in encrypted form, to preserve the spatial dataset.

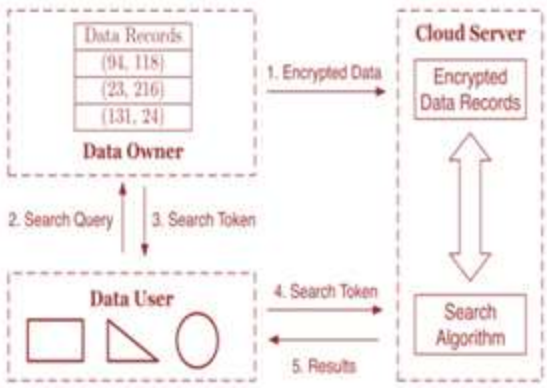

Fig.1 System Architecture

Our proposed algorithm support different and continuous range queries. the different geometric data is preprocessed then preceded in the cipher text data.

The proposed algorithm eliminates the multiple rounds of communication between server and client. firstly, the points are denoted for data records and then range queries are determined from the set of geometric points. The proposed algorithm is explained as follows:

i)Each record is symbolized as geometric points.

ii) Given the input 1^{λ}, the data owner generates the secret keys.

iii) Along the secret key, bloom filters are generated and outputs as {m, h_1….h_k} where m is the bloom filter length and h is the hash functions. In fact, the bloom filter contains all possible combination of ciphertext, which is further used as search token.

iv) Encryption phase: Afforded with secret key SK and a data set D, the data owner encrypts the data as follows:

BFD_i: =BF. Init (m)(2)

BFD_i :=BF. Add (D_i, BFD_i)(3)

The eq. (2) and (3) will process for all data points and the cipher text C_i will be estimated as:

$C_i \leftarrow$ SSW. Enc (S_K, U_k) (4)

Then, the encrypted dataset is C= (C_1… C_n)

v)Token Generation phase (S): The search token is generated from secret key SK and geometric query Q, the data owner calculates S=={S_1…S_t}:=Enumerate Inside Points (Q) BF_Q:=BF. Init (m)BFQ: = BF. Add (S_i, BF_Q), for 1≤i≤t, t is the possible points of Q. The search token TK calculates as

$$TK \leftarrow SSW.Gen(SK, \vec{v})$$

vi)Search phase: Afforded with TK and C, the cloud server returns the search results, IQ

Flag i←SSW. Query (TK, C_i) for $1 \leq i \leq n$.

For each flag, the identifier Ii is added to the set IQ.

The proposed algorithm works in the tree structure in order to improve the search complexity. By analyzing the size pattern, search pattern and access pattern, information leakage is reduced in the tree structure.

IV. CONCLUSION

In general, the four spatiotemporal points are adequate to recognize the location of the individual. In view of third party cloud, there is a chance of revealing the location of the individual to the anonymity.To resolve this issue, the researcher insisted on provide an end-to-end encryption. Each record is considered as the points and the set of points constitutes for range search.Based on the security parameter, the proposed algorithm consists of three important phases, encryption phase, token generation phase and search phase. All the three phases are interlinked with each other to perform the search over cipher text dataset.

REFERENCES

[1] B. Chazelle, “Filtering Search: A New Approach to Query-Answering,”SIAM J. Comput., vol. 15, no. 3, 1986.

[2] P. Agarwal and J. Erickson, “Geometric Range Searching and ItsRelatives,” Discrete and Computational Geometry, 1999.

[3] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh,“Location Privacy via Private Proximity Testing,” in Proc. of NDSS’11,2011.

[4] H. Shirani-Mehr, F. Banaei-Kashani, and C. Shahabi, “Efficient Reachability Query Evaluation in Large Spatiotemporal Contact Datasets,” inProc. of VLDB’12, 2012.

[5] M. de Berg, O. Cheong, M. van Kreveld, and M. Overmars, Computational Geometry: Algorithms and Applications. Springer-Verlag, 2008.

[6] D. Boneh and B. Waters, “Conjunctive, Subset, and Range Queries onEncrypted Data,” in the Proceedings of Theory of Cryptography (TCC).Springer-Verlag, 2007, pp. 535–554.

[7] E. Shi, J. Bethencourt, T.-H. H. Chan, D. Song, and A. Perrig, “MultiDimensional Range Query over Encrypted Data,” in Proc. of IEEES&P’07, 2007, pp. 350–364.

[8] Y. Lu, "Privacy-Preserving Logarithmic-time Search on Encrypted Data Cloud," in Proc. of NDSS'12, 2012.

[9] B. Wang, Y. Hou, M. Li, H. Wang, and H. Li, "Maple: Scalable MultiDimensional Range Search over Encrypted Cloud Data with Tree-basedIndex," in Proc. of ACM ASIACCS'14, 2014.

[10] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order PreservingEncryption for Numeric Data," in Proc. of ACM SIGMOD'04, 2004.

[11] R. A. Popa, F. H. Li, and N. Zeldovich, "An Ideal-Security Protocol forOrder-Preserving Encoding," in Proc. of IEEE S&P'13, 2013.

[12] F. Kerschbaum and A. Schroepfer, "Optimal Average-Complexity IdealSecurity Order-Preserving Encryption," in Proc. of ACM CCS'14, 2014.

[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," in Proc. of Securecomm'14, 2014.

[14] E.-O. Blass, T. Mayberry, and G. Noubir, "Practical Forward-SecureRange and Sort Queries with Updated-Oblivious Linked Lists," in InProc. of PETS'15, 2015.

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

[16] [Online]. Available: http://aws.amazon.com/solutions/case-studies/

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

[18] C. Shahabi, L. Fan, L. Nocera, L. Xiong, and M. Li, "Privacy-PreservingInference of Social Relationships from Location Data: A Vision Paper," in Proc. of ACM SIGSPATIAL GIS, 2015.

[19] J. Katz and Y. Lindell, Introduction to Modern Cryptography. CRCPress, 2007.

[20] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public KeyEncryption with Keyword Search," in Proc. of EUROCRYPT'04, 2004.