IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

Symmetric-Key Accessible Encryption to Secure Geometric Range Search Over Encrypted Spatial Data

P.Karthikeyan[1], Prof.B.Gopinathan M.E.,(Ph.D)[2]

P.G. Student, Department of Computer Science and Engineering, Adiyamaan College of Engineering , Hosur, Tamilnadu, India[1]

Associate Professor, Department of Computer Science and Engineering, Adiyamaan College of Engineering, Hosur, Tamilnadu, India[2]

Abstract*:* Nowadays, outsourcing the data to the cloud server is a natural activity auctioned by several cloud users. The outsourced data may contain sensitive information. The cloud technologies are very much improved that attracts many Location based Services companies. The overall theme of the cloud data resides at the distant server is to be managed with minimal computation by data owner and data users. The data is hired away in encrypted form to prevent anonymity activities. Reach ability is one of the issues faced between cloud users and LBS companies. Accessible encryption is a procedure to perform significant questions on encoded information without uncovering protection. Be that as it may, geometric range look on spatial information has not been completely examined nor bolstered by existing accessible encryption plans. In this we plan a symmetric-key accessible encryption conspire that can bolster geometric range inquiries on encoded spatial information. One of our real commitments is that our outline is a general approach, which can bolster diverse sorts of geometric range questions. At the end of the day, our outline on encrypted information is free from the states of geometric range questions. In addition, we additionally expand our plan with the extra utilization of tree structures to accomplish look multifaceted nature that is speedier than linear.

Keywords*:* Spatial data, geometric range queries, encrypted data, privacy

I. INTRODUCTION

Searchable Encryption (SE) is a promising technique to enable search functionalities over encrypted data at a remote server (e.g., a public cloud) without decryption. Specifically, with SE, a client (e.g., a company) can retrieve correct search results from an honest-but curious server without revealing private data or queries. Sequences of SE schemes have been proposed, where most of them focus on common SQL queries, such as keyword search and range search. Recently, a few SE schemes have drawn their attentions particularly to geometric range queries over spatial datasets, where a geometric range query retrieves points inside a geometric area, such as a circle or a polygon. However, how to enable arbitrary geometric range queries with sublinear search time while supporting efficient updates over encrypted spatial data remains open. Spatial data have extensive applications in location based services, computational geometry, medical imaging, geosciences, etc., and geometric range queries are fundamental search functionalities over spatial datasets. For instance, clients can find friends within a circular area in location-based services (e.g., Facebook); a medical researcher can predict whether there is a dangerous outbreak for a specific virus in a certain geometric area (e.g., Zika in Brazil) by retrieving patients inside this area. Many companies, such as Yelp and Foursquare, are now relying on public clouds (e.g., Amazon Web Services, AWS) to manage their spatial datasets and process queries. However, due to the potential threats of inside attackers and hackers, the privacy of spatial datasets in public clouds should be carefully taken care of, particularly in location-based and medical applications. For instance, a compromise of AWS by an inside attacker or hacker would put millions of Yelp users' sensitive locations under the spotlight.

Different from keyword search relying on equality checking and range search depending on comparisons, a geometric range query over a spatial dataset essentially requires compute-then-compare operations . For example, to decide whether a point is inside a circle, we calculate a distance from this point to the center of a circle, and then compare this distance with the radius of this circle; in order to verify whether a point is inside a polygon, we compute the cross product of this point with each vertex of this polygon, and compare each cross product with zero (i.e., positive or negative) . Unfortunately, this requirement of compute-then compare operations makes the design of a SE scheme supporting geometric range queries more challenging, since current efficient cryptographic primitives are not suitable for the evaluation of compute-then-compare operations in cipher text. More specifically, Pseudo Random Function (PRF) can only enable equality checking; Order-Preserving Encryption solely supports comparisons; Partially

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

Homomorphic Encryption (e.g., Paillier) can only compute additions (or multiplications). BGN calculates additions and at most one multiplication on encrypted data. On the other hand, Fully Homomorphic Encryption (FHE) could securely evaluate compute-then-compare operations in principle. However, the evaluation with FHE does not reveal search decisions (such as inside or outside) over encrypted data, which limits its usage in search. In this paper, we formalize the concept of Geometrically Searchable Encryption (GSE), which is evolved from the definitions of SE schemes but focuses on answering geometric queries. We propose a GSE scheme, named FastGeo, which can efficiently retrieve points inside a geometric area without revealing private data points or sensitive geometric range queries to a honest-butcurious server. Instead of directly evaluating compute then-compare operations, our main idea is to convert spatial data and geometric range queries to a new form, denoted as equality-vector form, and leverage a two-level search as our key solution to verify whether a point is inside a geometric range, where the first level securely operates equality checking with PRF and the second level privately evaluates inner products with She n-Shi-Waters encryption (SSW) . The major contributions of this paper are summarized as below: With the embedding of a hash table and a set of link lists in our two-level search as a novel structure for spatial data, FastGeo can achieve sub linear search and support arbitrary geometric ranges (e.g., circles and polygons). Compared to recent solutions , FastGeo not only provides highly efficient updates over encrypted spatial data, but also improves search performance over 100x. We formalize the definition of GSE and its leakage function, and rigorously prove data privacy and query privacy with indistinguishability under selective chosen plaintext attacks (IND-SCPA) . We implement and evaluate FastGeo in cloud platform (Amazon EC2), and demonstrate that FastGeo is highly efficient over a real-world spatial dataset. For instance, a geometric range query over 49,870 encrypted tuples can be performed within 15 seconds, and an update only requires less than 1 second on average.

II. LITERATURE SURVEY

[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.

[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 protest 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.

[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.

[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.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

[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. RELATED WORK

Some SE schemes that support comparisons, can perform rectangular range queries by applying multiple dimensions. However, those extensions do not work with other geometric range areas, e.g., circles and polygons in general. Wang at a proposed a scheme, which particularly retrieves points inside a circle over encrypted data by using a set of concentric circles. Zhu et al. also built a scheme for circular range search over encrypted spatial data. Unfortunately, these two schemes exclusively work for circles, and do not apply to other geometric areas. Ghinita and Rughinis designed a scheme, which supports geometric range queries by using Hidden Vector Encryption. Instead of encoding a point with a binary vector of T2 bits, where T is the dimension size, it leverages a hierarchical encoding, which reduces the vector length to 2log2 T bits. However, its search time is still linear with regard to the number of tuples in a dataset, which not only runs slowly over large-scale datasets but also disables efficient updates. Our recent work presents a scheme that can operate arbitrary geometric range queries. It leverages Bloom filters and their properties, where a data point is represented as a Bloom filter, a geometric range query is also formed as a Bloom filter, and the result of an inner product of these two Bloom filters correctly indicates whether a point is inside a geometric area. Its advanced version with R-trees can achieve logarithmic search on average. Although it also utilizes SSW as one of the building blocks, its tree-based index and unique design with Bloom filters are completely different from then two-level index introduced in this paper, where these significant differences prevent this previous scheme from supporting efficient updates and practical search time. Some other works study secure geometric operations between two parties (e.g., Alice and Bob), where Alice holds a secret point and Bob keeps a private geometric range. With Secure Multi-party Computation (SMC), Alice and Bob can decide whether a point is inside a geometric range without revealing secrets to each other. However, the model of these studies are different from ours (i.e., Alice and Bob both provide individual private inputs, while a client in our model has all the private inputs but the server has no private inputs). Besides, SMC introduces extensive interactions.

Data utilization method is performed over the plaintext search. Due to increase of the cloud users, search operation is given importance. Usually, Boolean search operation was performed over the server to yield better results. This search fails to give better security to the cloud data. 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 association. Further, k-NN classification technique is used for generating the security index. Secure index was obtained from mini-hash include cryptography, image processing and information retrieval. The schema contains hash functions and inverted visual words. It yields slow performance in inverted visual words. The theme of cryptographic provides secure systems. The method incurs higher storage overhead and not guarantees the security. A privacy preserving model search operation is carried out in two phases, namely, Ranked over keyword search, search over structured data. Though confidentiality parameter is achieved, over encrypted data was unsuccessful.

DISADVANTAGES:

- Boolean search operation was performed over the server to yield better results but this search fails to give better security to the cloud data.
- The method incurs higher storage overhead and not guarantees the security.
- Confidentiality parameter is achieved, over encrypted data was unsuccess

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

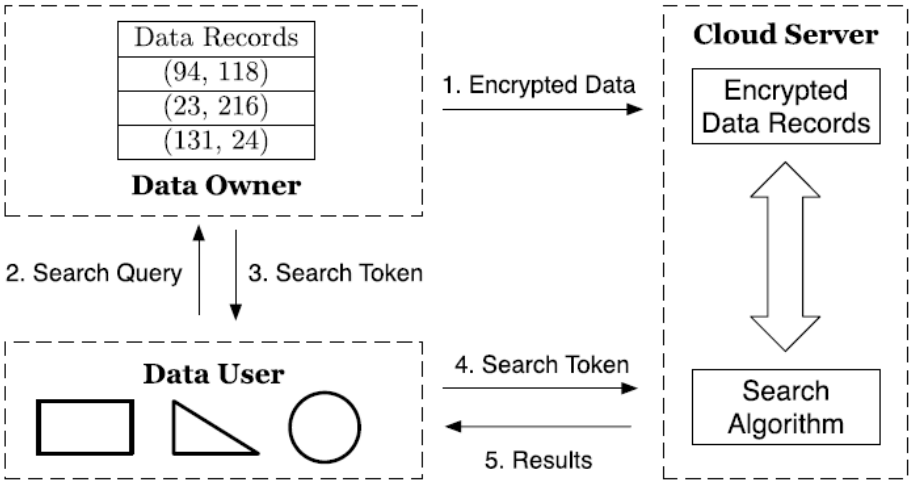
IV. PROPSED SYSTEM

The proposed work is purely based on Symmetric Key Encryption scheme. The system model consists of three entities, namely, 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 searched by the data user. The task of cloud server is to provide services to the data owner and data users. Since, the cloud server is semi-trusted, the cloud service is reliable. The learning of range queries over the private a challenging task. 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 task of preserve the data at cloud server, eventually focus on reducing the local cost. The outsourced data will be searched by the data user. The task of cloud server is to provide services to the data owner and data users. Since, the trusted, the cloud service is reliable. range queries over the private information is a challenging task. The data owner stores the data in encrypted form, to preserve the spatial dataset. Our proposed algorithm supports range queries. The different geometric data is and then preceded in the cipher text data. 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.

Advantages:

- The proposed algorithm works in tree structure in order to improve the search complexity.
- By analyzing pattern, search pattern and access pattern leakage is reduced in tree structure.
- The security of our scheme is formally defined and analyzed with in distinguishability 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.

V. SYSTEM ARCHITECTURE



VI. CONCLUSION

We contemplate a general way to deal with safely seek encoded spatial information with geometric range questions. In particular, our answer is autonomous with the state of a geometric range inquiry. With the extra utilization of R-trees, our plan can accomplish speedier than-direct inquiry many- sided quality in regards to the quantity of focuses in a dataset. The security of our plan is formally characterized and broke down with lack of definition under Selective Chosen-Plaintext Attacks. Our outline can possibly be utilized and executed in wide applications, for example, Location-Based Services and spatial databases, where the utilization of delicate spatial information with a necessity of solid protection ensure is required. In Future, a Hilbert-curve based cryptographic transformation scheme for preserving data privacy of the outsourced databases in the cloud system. To enhance the efficiency of the query processing, our HCT uses the newly designed HAI instead of using a tree structure. It reduces communication cost for query processing by performing local clustering based on Hilbert-curve order. From the performance analysis, we show that our system shows better performance than the existing CRT scheme.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

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. 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.
[7] E. Stefanov, C. Papamanthou, and E. Shi, "Practical Dynamic Searchable Encryption with Small Leakage," in Proc. of NDSS'14, 2014.
[8] G. Ghinita and R. Rughinis, "An Efficient Privacy-Preserving Sys- tem for Monitoring Mobile Users: Making Searchable Encryption Practical," in Proc. of ACM CODASPY'14, 2014.
[9] J. Sedenka and P. Gasti, "Privacy-Preserving Distance Computation and Proxitity Testing on Earth, Done Right," in Proc. of ACM ASIACCS'14, 2014.
[10] B. Wang, Y. Hou, M. Li, H. Wang, and H. Li, "Maple: Scalable Multi-Dimensional Range Search over Encrypted Cloud Data with Tree-based Index," in Proc. of ACM ASIACCS'14, 2014.