International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.6, pp.01-05, October (2018)

Research Paper

E-ISSN: 2320-7639

A Novel Two Level Search Scheme to Provide Security and Privacy of Encrypted Spatial Data

Ch.V.B.Neeraja[1*], S.S.S.N.Usha Devi N[2]

[1]Dept. of Computer Science and Engineering, University college of engineering JNTUK, Kakinada, India
[2]Dept. of Computer Science and Engineering, University college of engineering JNTUK, Kakinada, India

Available online at: www.isroset.org

Received: 04/Oct/ 2018, Accepted: 14/Oct/ 2018, Online: 31/Oct/2018

***Abstract*—**Spatial data consists of geographic and geometric data primitives. Searching on spatial data is carried by geometric range queries. FastGeo, an efficient two-level search scheme is introduced. The major contributions focus on two aspects. First, enrich search functionalities by designing new solutions to carry out fundamental geometric search queries, which are supported over encrypted data. Second, minimize the gap between theory and practice by building novel schemes to perform geometric queries with highly efficient search time and updates over large scale spatial data. Spatial data and geometric range queries are converted into a new form, denoted as equality-vector form and perform two-level search to verify whether a point is inside a geometric range. FastGeo is implemented using java as programming language on Net Beans IDE. An honest-but-curious server efficiently performs geometric range queries and returns data points that are inside the geometric region to the client without learning query or sensitive information. Better privacy can be achieved which cannot drop or create a new message. Experimental results on spatial data can achieve sublinear search time.

***Keywords*-** Geometric range queries, Spatial Data, Encrypted data

I. INTRODUCTION

Spatial data is the data where any information is mapped. It consists of points, lines and other geometric areas, these data is implemented extensively in many emerging applications [3]. Spatial Data Option is designed to make spatial data natural and easier to user for storage, retrieval and manipulation of data such as Geographic Information System (GIS). Geometric range queries [10] and Nearest neighbor queries are two major Geometric queries in practice. Geometric range query is a common and important type of query in spatial data. Here in Euclidean space the spatial locations are represented as data points and queries are described as geometric objects such as rectangles, circles etc. Due to dynamic increase in size of data, many organizations are outsourcing their spatial data to public clouds which is helpful in minimizing data storage and query processing costs.

However, due to attackers on remote servers, users are worried about their private data while storing and querying on public clouds. Solution to provide privacy to the outsourced data stored in public clouds is encryption of spatial data. Advanced Standard Encryption (AES) is a symmetric encryption algorithm.

Searchable Encryption (SE) is a technique, which enables search functionalities on remote server. Specifically, with searchable encryption, a client can get relevant search results from an honest-but curious server by not revealing any private data or queries. Sequence of SE schemes [8] have been proposed and most of them focus on common SQL queries such as range and keyword search [4]. Different from keyword search and range search depending on comparisons, a geometric range query over a spatial data essentially requires compute-then-compare operations. Recently, a few SE schemes have drawn their attention particularly towards geometric range queries, where a geometric range query retrieves points inside a geometric area, such as a circle or polygon. Unfortunately, this requirement of compute-then-compare [2] 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.

Therefore a new technique named FastGeo, an efficient two-level search scheme is proposed which operates geometric ranges over encrypted spatial data and return data points to a client without learning sensitive data points and also supports dynamic updates over encrypted spatial data. Dynamic grid system is used in which the query area is divided into equal sized grid cells based on structure specified by user. It provides better privacy guarantee by placing semi trusted third party termed query server (QS), which cannot drop or create a new message.

Section I consists of introduction of the paper, Section II contain related work, Section III contain existing system, Section IV contain proposed system, Section V contain system architecture, Section VI contain methodology, Section VII contain results and analysis, Section VIII contain conclusion and future work.

II. RELATED WORK

Wang et. al. [6] propose a scheme, which particularly retrieves points inside a circle over encrypted data by using set of concentric circles. Zhu et al. [7] also proposed a scheme for circular range search on encrypted spatial data but these two ideas do not work with other geometric areas and exclusively work for circles. OPE [5] and some SE schemes that support comparisons, can perform rectangular range queries by applying multiple dimensions. However, those dimensions do not work with other geometric areas, e.g, circles and polygons in general. Ghinita and Rughinis [11] designed a scheme, which supports geometric range queries by using Hidden Vector Encryption.

Instead of encoding a point with binary vector of T2 bits, where T is the dimension size, it leverages a hierarchical encoding, which reduces the vector length to 2 log2 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.

Recent work presents a scheme that can operate arbitrary geometric range queries. It leverages Bloom filter 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.

Some other works [9] 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).

III. EXISTING SYSTEM

Searchable encryption techniques concentrates on SQL queries, such as keyword queries and Boolean queries and some techniques focus on geometric range search on encrypted spatial data. Some schemes specifically perform circular range queries on encrypted data by leveraging a set of concentric circles.

Some previous encryption techniques handling order comparisons only manage axis parallel rectangular range search on encrypted spatial data. A new technique named Order Preserving Encryption is introduced, which has weaker privacy guarantee than searchable encryption and it is able to perform axis parallel rectangular range search with trivial extensions. Ghinita and Rughinis implements functional encryption technique with hierarchical encoding to efficiently perform axis parallel rectangular range.

Other existing system, uses Bloom filters and its properties, where a data point and geometric range query are formed as two different bloom filters and results whether a point is inside geometric area. In advanced version with R-tree can achieve logarithmic search on average.

DISADVANTAGES OF EXISTING SYSTEM

- Due to the potential threats of inside attackers and hackers, the privacy of spatial data 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.
- Does not reveal search decisions over encrypted data, which limits its usage in search.

IV. PROPOSED SYSTEM

In proposed system, Geometrically Searchable Encryption (GSE) scheme is formalized, which mainly focuses on answering geometric range queries and it is evolved from the definitions of SE schemes. A new GSE scheme named FastGeo, is proposed, without revealing private data points or sensitive geometric range queries to a honest-but-curious server, it efficiently retrieve points inside a geometric area. Generally SE schemes require compute-then-compare operations, instead of directly evaluating those operations, here the main idea is to convert spatial data and geometric range queries to a new form, denoted as equality-vector form. A novel two-level search scheme is introduced as a key solution to verify whether a point is inside a geometric range or not.

Here, in the first level, it securely operates equality checking with pseudo random function (PRF) and second level privately evaluates inner products with shen-shi-waters encryption (SSW) [12]. Spatial data points in the geometric region are displayed by considering point of interest and type of geometric query searched.

Dynamic grid system is also proposed, in which the query area is divided into equal sized grid cells based upon the structure specified by the user. Here, a semi trusted query server (QS) is placed as an intermediate between user and service provider which provides better privacy guarantee.

ADVANTAGES OF PROPOSED SYSTEM

- FastGeo can achieve sub linear search and support arbitrary geometric areas such as circles and polygons with the use of hash table and set of linked lists in our two-level search.
- Highly efficient updates over encrypted spatial data is possible in FastGeo and also improves search performance.
- Data privacy and query privacy is possible by formalizing the definition of GSE.

- FastGeo is highly efficient over a real-world spatial data.
- Dynamic grid system provides better privacy guarantee by using semi trusted third party termed query server and also reduces total burden on server.

V. SYSTEM ARCHITECTURE

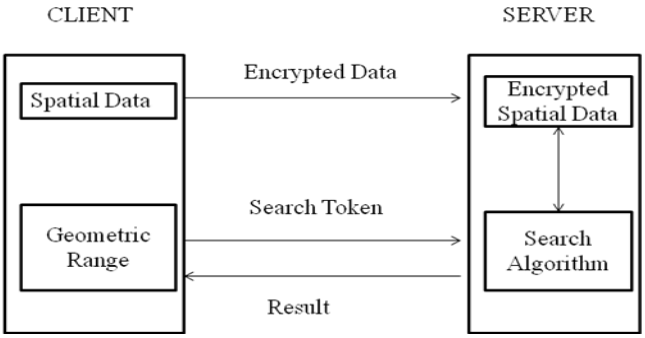

Figure 1: Model of GSE Scheme

Client and server are two modules in our architecture. Client stores its spatial data on the server. In addition it also wants to perform geometric range queries over its outsourced data as shown in fig 1. The purpose of geometric range query is to retrieve points inside the geometric range. Client has the secret key for both encryption and decryption of spatial data and geometric query. Server offers data storage and query processing services.

The server is required to correctly perform geometric range search on encrypted spatial data without decryption, means symmetric encryption and it returns results to the client. Dynamic grid system, which divides user query into grids based on structure specified by user and query server is placed as an intermediate between user and service provider.

VI. METHODOLOGY

FastGeo Algorithm:

Input: Spatial data (D), geometric range queries (Q) and secret key (sk).
Output: Returns points inside the geometric range.

STEP 1: Client generate secret key sk, and spatial data D, is taken in the form of points.
STEP 2: Spatial data and geometric range queries Q, are converted into new form named equality-vector form instead of performing compute-then-compare operations.
STEP 3: Next building index for spatial data D, is created by considering spatial data as input and generates index as output which is run by a client.
STEP 4: Generated index need to be encrypted by considering index and secret key SK, as an input and it runs on client side.
STEP 5: Geometric range query Q, which is converted into equality vector form is taken as an input for generating token with secret key SK, is sent to server.
STEP 6: client sends outsourced spatial data and search token T, to the server.
STEP 7:Server takes encrypted index enc(T,SK), and search token T, as input and outputs set of identifiers IQ, in cipher text and the identifiers are sent to the client.
STEP 8: Client learns the search results in the plain text by decrypting encrypted points locally.
STEP 9: Dynamic grid structure is used where query server QS, acts as an intermediate between user and service provider SP.
STEP 10: Finally, client generates points inside the geometric range specified by the user.

VII. RESULTS AND ANALYSIS

FastGeo is a GSE scheme, which performs operations between client and server. Client consists of spatial data and geometric range queries. Spatial data and geometric range queries are to be converted into equality-vector form. Client sends data along with search token to the server. Server accepts and performs searching algorithm by considering geometric range query and returns result to the client.

Authorizing Users

Client needs to login, but client can able to login only after the authorization of users by server. Client sends request to the server at the time of registration before login. Server accepts the request from client, view all the entered information and authorize users.

Figure 2: Authorizing users

Client Adding Spatial Data

Client adds all the spatial data details and the spatial data is considered as a point and it converted into equality vector form. Encryption is performed on it and send to the server,

which is shown in figure 3. Spatial Data is generally the location of the client.

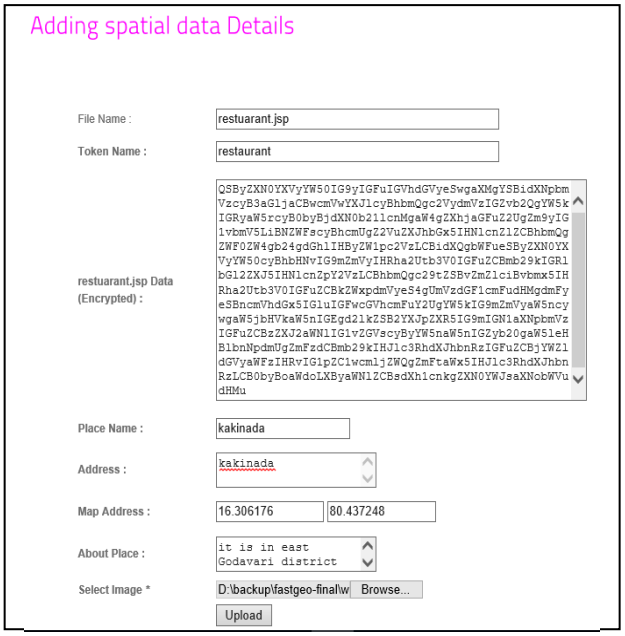

Figure 3: Adding Spatial Data at Client Side

The spatial data is encrypted automatically at client side before sending it to server. Spatial data includes all the data along with the token and file information and sends request to the server. Server accepts it in the encrypted format without decrypting it. AES is used for encrypting the spatial data.

Range query result

Client sends spatial data and geometric range query as an input to the server, where the spatial data is encrypted. Server accepts the encrypted spatial data and search token and search algorithm is performed.

Here, as a result client displays the geometric area queried for the searched token and displays all the data points related to the search token with in the geometric range, as shown in figure 4.

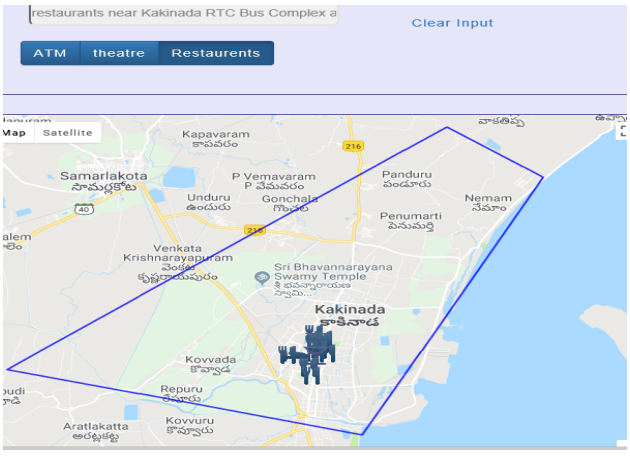

Fig 4: Polygon Range Query

Finally as a result, server efficiently performs geometric range queries and returns data points that are inside the geometric region to the client without learning query or sensitive information.

VIII. CONCLUSION AND FUTURE WORK

A novel two-level search scheme is implemented, which supports geometric range search on encrypted spatial data without revealing data privacy and query privacy. Dynamic grid system is used in which provides better privacy guarantee by placing semi trusted third party termed query server (QS), which cannot drop or create a new message. Supports arbitrary geometric shapes and achieves sub linear search time and enables dynamic updates on encrypted spatial data.

Future research may include designing range searchable encryption achieving faster-than-linear search with regard to the number of data records, and studying searchable encryption schemes for other common geometric queries, such as simplex range (i.e., retrieving points that are inside a triangle).

REFERENCES

[1] Boyang Wang, Ming Li, and Li Xiong, "*FastGeo: Efficient Geometric Range Queries on Encrypted Spatial Data"* IEEE Transactions on Dependable and Secure Computing, 2017.

[2] B. Wang, M. Li, and H. Wang, "*Geometric Range Search on Encrypted Spatial Data*", IEEE Transactions on Information Forensics and Security, vol. 11, no. 4, pp. 704–719, 2016.

[3] Shashi Shekhar, Stenven k. Feiner, and Walid G. Aref, "*Spatial Computing*," Communications of the ACM, 2016.

[4] Erik-Oliver Blass, Travis Mayberry, and Guevara Noubir, "*Practical Forward Secure Range and Sort Queries with Updated-Oblivious Linked Lists*", Proceedings of Privacy Enhancing Technology Symposium, 2015.

[5] Florian Kerschbaum, "*Frequency-Hiding Order-Preserving Encryption",* Proceedings of ACM, 2015.

[6] B. Wang, M. Li, H. Wang, and H. Li, "*Circular Range Search on Encrypted Spatial Data*", Proceedings of IEEE CNS, 2015.

[7] H. Zhu, R. Lu, C. Huang, L. Chen, and H. Li, "*An Efficient Privacy Preserving Location Based Services Query Scheme in Outsourced Cloud,"* IEEE Transactions on Vehicular Technology, 2015.

[8] V. Pappas, F. Krell, B. Vo, V. Kolesnikov, T. Malkin, S. G. Choi, W. George, A. Keromytis, and S. Bellovin, "*Blind Seer: A Searchable Private DBMS*," Proceedings of IEEE (S&P), 2014.

[9] J. Sedenka and P. Gasti, "*Privacy-Preserving Distance Computation and Proximity Testing on Earth, Done Right*," Proceedings of ACM ASIA Conference on Information, Computer and Communications Security (ASIACCS), 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*," Proceedings of ACM, 2014.

[11] G. Ghinita and R. Rughinis, "*An Efficient Privacy-Preserving System for Monitoring Mobile Users: Making Searchable Encryption Practical*," Proceedings of ACM

Conference on Data and Application Security and Privacy (CODASPY), 2014.

[12] E. Shen, E. Shi, and B. Waters, "*Predicate Privacy in Encryption Systems,"* Proceedings of Transactions on cloud computing (TCC), 2009.

Authors Profile

Ms. Ch.V.B.Neeraja pursed Bachelor of Technology from Vignan's Lara Institute of Technology and Science, Vadlamudi, Guntur in 2016 and Master of Technology from University College of Engineering, Jawaharlal Nehru Technological University Kakinada in 2018.

*Mrs. S.S.S.N.Usha Devi N***.** is currently pursuing Ph.D. She is currently working as Assistant Professor in Department of Computer Science and Engineering, University College of Engineering, Jawaharlal Nehru Technological University ,Kakinada since 2013.

