IJCSC 0973-7391
International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 9 • Issue 2 pp. 89-95 March 2018 - Sept 2018 www.csjournals.com

RapidGeo: Graphic Regional Range Queries on Encrypted Geographical Data in a Productive Mechanism

Mudassir Ahmed Khan[1], MdAteeq Ur Rahman[2]
[1]Research Scholar, Dept. of Computer Science & Engineering, SCET, Hyderabad
[2]Professor and Head, Dept. of Computer Science & Engineering, SCET, Hyderabad

Abstract: It is fascinating to store knowledge on knowledge storage servers such as mail servers and file servers in encrypted type to cut back security and privacy risks. however this sometimes implies that one has to sacrifice practicality for security. as an example, if a client desires to retrieve solely documents containing sure words, it absolutely was not antecedently known a way to let the info storage server perform the search and answer the question while not loss of knowledge confidentiality. In this paper, we tend to describe our cryptanalytic schemes for the matter of looking out on encrypted knowledge and supply proofs of security for the ensuing crypto systems. Our techniques have variety of crucial blessings. knowledge have wide applications, e.g., location-based services, and geometric vary queries (i.e., finding points within geometric areas, e.g., circles or polygons) square measure one amongst the elemental search functions over spatial knowledge. The rising demand of outsourcing knowledge is moving large-scale datasets, as well as large-scale spatial datasets, to public clouds. Meanwhile, owing to the priority of corporate executive attackers and hackers on public clouds, the privacy of spatial datasets ought to be cautiously preserved whereas querying them at the server aspect, particularly for location-based and medical usage. during this paper, we tend to formalize the conception of Geometrically Searchable Encryption, associate degreed propose an economical theme, named FastGeo, to shield the privacy of clients' spatial datasets keep and queried at a public server. With FastGeo, that could be a novel two-level seek for encrypted spatial knowledge, associate degree honest-but-curious server will with efficiency perform geometric vary queries, and properly come knowledge points that square measure within a geometrical vary to a consumer while not learning sensitive data points or this non-public question. FastGeo supports discretionary geometric areas, achieves sublinear search time, and allows dynamic updates over encrypted spatial datasets. Our theme is demonstrably secure, and our experimental results on real-world spatial datasets in cloud platform demonstrate that FastGeo will boost search time over a hundred times. They are provably secure: they supply demonstrable secrecy for encoding, in the sense that the untrusted server cannot learn anything concerning the plaintext once solely given the ciphertext; they provide question isolation for searches, meaning that the untrusted server cannot learn something additional concerning the plaintext than the search result; they supply controlled searching, so the untrusted server cannot rummage around for Associate in Nursing arbitrary word while not the user's authorization; they additionally support hidden queries, so the user might raise the untrusted server to look for a secret word while not revealing the word to the server. The algorithms we tend to gift area unit easy, fast (for a document of length , the encoding and search algorithms solely would like stream cipher and block cipher operations), and introduce virtually no house and communication overhead, and thus area unit sensible to use these days Spatial.

Index Terms: Spatial data, geometric range queries, encrypted data, privacy, Searchable symmetric encryption

I. Introduction

Today’s mail servers like IMAP servers [11], file servers and different information storage serverstypically should be absolutely
trusted—they have access to the information, and therefore should be trusted to not reveal it while not authorization—which introduces undesirable security and privacy risks in applications. Previous work shows the way to build encrypted file systems and secure mail servers, however generally one should sacrifice functionality to make sure security. the elemental drawback is that moving the computation to the information storage looks very tough once the information is encrypted, and plenty of computation problems over encrypted information antecedently had no practical solutions. In this paper, we tend to show the way to support looking out practicality without any loss of information confidentiality. An example is wherever a mobile user with restricted information measure desires to retrieve all email containing the word “Urgent” from associate untrusted mail-storage server within the infrastructure.

This is trivial to try and do once the server is aware of the content of the information, but however will we tend to support search queries if we tend to don't want toreveal all our email to the server?

Our answer is to gift cryptologic schemes that modify searching on encrypted information while not unseaworthy any info
to the untrusted serve Our techniques area unit demonstrably secure. Searchable cryptography (SE) [1] could be a promising technique to modify search functionalities over encrypted information at a foreign server (e.g., a public cloud) while not cryptography. Specifically, with SE, a shopper (e.g., a company) will retrieve correct search results from AN honest-but curious server while not revealing non-public information or queries. A sequence of SE schemes [1]–[7] are projected, wherever most of them specialize in common SQL queries, like keyword search and vary search. Recently, a couple of SE schemes have drawn their attentions significantly to geometric vary queries over abstraction datasets, wherever a geometrical vary question retrieves points within a geometrical space, like a circle or a plane figure. However, a way to modify whimsical geometric vary queries with sublinear search time whereas supporting economical updates over encrypted abstraction information remains open. abstraction information have in depth applications in locationbased services, process pure mathematics, medical imaging, geosciences, etc., and geometric vary queries ar basic search functionalities over abstraction datasets. as an example, a shopper will realize friends inside a circular space in location-based services (e.g., Facebook); a medical man of science will predict whether or not there's a dangerous eruption for a particular virus during a bound geometric space (e.g., Zika in Brazil) by retrieving patients within this area. several firms, like Yelp and Foursquare, ar currently looking forward to public clouds (e.g., Amazon internet Services, AWS) to manage their abstraction datasets and method queries.

However, because of the potential threats of within attackers and hackers, the privacy of abstraction datasets publically clouds ought to be fastidiously taken care of, significantly in location-based and medical applications. as an example, a compromise of AWS by an indoor assailant or hacker would place ample Yelp users’ sensitive locations beneath the spotlight. completely different from keyword search looking forward to equality checking and vary search betting on comparisons, a geometrical vary question over a abstraction dataset primarily needs compute-then-compare operations . for instance, to make a decision whether or not some extent is within a circle, we tend to calculate a distance from now to the middle of a circle, then compare this distance with the radius of this circle; so as to verify whether or not some extent is within a plane figure, we tend to calculate the vector of now with every vertex of this plane figure, and compare every vector with zero (i.e., positive or negative) . sadly, this demand of compute-then compare operations makes the look of a SE theme supporting geometric vary queries more difficult, since current economical crypto logic primitives aren't appropriate for the analysis of compute-then-compare operations in cipher text. a lot of specifically, Pseudo Random operate (PRF) will solely modify equality checking; Order-Preserving cryptography only supports comparisons; part Homo morphic cryptography (e.g., Paillier) will solely calculate additions (or multiplications). BGN calculates additions and at the most one multiplication on encrypted information.

On the opposite hand, absolutely Homo morphic cryptography (FHE) may firmly valuate compute-then-compare operations in essence. However, the analysis with FHE doesn't reveal search choices (such as within or outside) over encrypted information, that limits its usage in search. during this paper, we tend to formalize the conception of Geometrically Searchable cryptography (GSE), that is evolved from the definitions of SE schemes however focuses on responsive geometric queries. we tend to propose a GSE theme, named FastGeo, which may with efficiency retrieve points within a geometrical space while not revealing non-public information points or sensitive geometric vary queries to a honest-but curious server. rather than directly evaluating compute then - compare operations, our main plan is to convert abstraction information and geometric vary queries to a brand new kind, denoted as equality-vector kind, and leverage a two-level search as our key answer to verify whether or not some extent is within a geometrical vary, wherever the primary level firmly operates equality checking with PRF and also the second level in camera evaluates inner merchandise with Shen-Shi-Waters cryptography (SSW) . the main contributions of this paper ar summarized as below: nine With the embedding of a hash table and a collection of link lists in our two-level search as a completely unique structure for abstraction information, FastGeo are able to do sublinear search and support whimsical geometric ranges (e.g., circles and polygons). Compared to recent solutions [8], Fast Geo not solely provides extremely economical updates over encrypted abstraction information, however additionally improves search performance over 100x. nine we tend to formalize the definition of GSE and its outflow operate, and strictly prove information privacy and question privacy with identity beneath selective chosen plaintext attacks (IND-SCPA) . nine we tend to implement and valuate FastGeo in cloud platform (Amazon EC2), and demonstrate that Fast- Geo is very economical over a real-world abstraction dataset. as an example, a geometrical vary question over forty nine,870 encrypted tuples is performed inside fifteen seconds, and an update solely needs but one second on the average.

The techniques provide obvious secrecy for encoding, within the sense that the untrusted server cannot learn something regarding the plaintext given solely the ciphertext. The techniques provide controlled looking out, so the untrusted server cannot explore for a word while not the user’s authorization. The techniques support hidden queries, so the user might raise the untrusted server to search for a secret word while not revealing the word to the server. The techniques conjointly support question isolation, meaning that the untrusted server learns nothing more than the search result regarding the plaintext. Our schemes area unit economical and sensible. The algorithms we gift area unit straightforward and quick. a lot of specifically, for a document of length , the encoding and search algorithms solely want
variety of stream cipher and block cipher operations. Our schemes introduce essentially no house and communication overhead. They are conjointly versatile and may be simply extended to support a lot of advanced searches. Our schemes all take the shape of probabilistic searching:

a search for the word returns all the positions wherever occurs within the plaintext, in addition as probably another inaccurate positions. we tend to might management the amount of errors by adjusting a parameter within the encoding algorithm; each wrong position are going to be came with likelihood regarding, so for a -word document, we tend to expect to ascertain regarding false matches. The user are going to be ready to eliminate all the false matches (by decrypting), therefore in remote looking out applications, false matches mustn't be a drag farewell as they're not therefore common that they overwhelm the communication channel between the user and also the server. This paper is structured as follows. we tend to initial introduce the problem of looking out on encrypted information in Section a pair of and briefly review some vital background in Section three. We then describe our answer for the case of looking out with sequential scan in Section four. we tend to discuss any problems such as advanced search and search with index in Section five. We discuss connected add Section vi and eventually we tend to conclude in Section 7. Appendix A presents the proofs for all of proofs of security for these schemes

I. Related Works

We initial outline the matter of looking out on encrypted data. Assume Alice incorporates a set of documents and stores them on associate degree untrusted server Bob. for instance, Alice may well be a mobile user World Health Organization stores her email messages on associate degree untrusted mail server. as a result of Bob is untrusted, Alice needs to write her documents and solely store the ciphertext on Bob. Each document may be distributed into 'words'. every 'word' may be any token; it could also be a 64-bit block, an English word, a sentence, or another atomic amount, according to the applying domain of interest. For simplicity, we have a tendency to usually assume these 'words' have constant length (otherwise we can either pad the shorter 'words' or split longer 'words' to make all the 'words' to own equal length, or use some simple extensions for variable length 'words'; see Section 5.3). as a result of Alice could have solely a low-bandwidth network association to the server Bob, she needs to solely retrieve the documents that contain the word . In order to achieve this goal, we want to style a theme in order that after playacting sure computations over the ciphertext, Bob will confirm with some likelihood whether or not every document contains the word without learning the rest. There appear to be 2 varieties of approaches. One chance is to make up associate degree index that, for every word of interest, lists the documents that contain . another is to perform a successive scan while not associate degree index. The advantage of using associate degree index is that it's going to be quicker than the successive scan once the documents area unit giant. The disadvantage of using associate degree index is that storing and change the index may be of substantial overhead. therefore the approach of victimization associate degree index is a lot of appropriate for mostly-read-only knowledge. We initial describe our theme for looking out on encrypted data while not associate degree index. Since the index-based schemes appear to require less subtle constructions, we are going to defer discussion of looking out with associate degree index .

2.1 Existing System

OPE and a few SE schemes that support comparisons, will perform rectangular vary queries byapplying multiple dimensions. However, those extensions don't work with different geometric vary areas, e.g., circles and polygons generally. Wang et. al. planned a theme, that notably retrieves points within a circle over encrypted information by employing a set of concentrical circles.

Disadvantages:

Current economical cryptologic primitives aren't appropriate for the analysis of compute-then-compare operations in ciphertext. Due to the potential threatsof within attackers and hackers, the privacy of spatialdatasets publicly clouds ought to be rigorously taken careof, articularly in location-based and medical applications.

II. Proposed System

In this paper, we tend to formalize the thought of Geometrically Searchable cryptography (GSE), that is evolved from the definitions of SE schemes however focuses on responsive geometric queries. we tend to propose a GSE theme, named FastGeo, which may expeditiously retrieve points within a geometrical space while not revealing non-public information points or sensitive geometric vary queries to a honest-but curious server. rather than directly evaluating compute then-compare operations, our main plan is to convert abstraction information and geometric vary queries to a brand new type.

The major contributions of this paper area unit summarized as below:

With the embedding of a hash table and a group of link lists in our two-level search as a unique structure for spatial information, FastGeo can do sub-linear search and support capricious geometric ranges (e.g., circle sand polygons). Compared to recent solutions, FastGeo not solely provides extremely efficient updates over encrypted abstraction information, however conjointly improves search performance over 100x.

We formalize the definition of GSE and its leakage function, and strictly prove information privacy and query privacy with in distinguish ability beneath selective chosen plaintext attacks. We implement and judge FastGeo in cloud platform, and demonstrate that Fast-Geo is very economical over a real-world spatial dataset. OPE and a few SE schemes that support comparisons, will perform rectangular vary queries by applying multiple dimensions. However, those extensions do not work with alternative geometric vary areas, e.g., circles and polygons normally. Wang et. al. [9] projected a scheme, that notably retrieves points within a circle over encrypted information by employing a set of coaxial

circles. Zhu et al. conjointly designed a theme for circular range search over encrypted spacial information. sadly, these 2 schemes solely work for circles, and do not apply to alternative geometric areas. Ghinita and Rughinis designed a theme, which supports geometric vary queries by mistreatment Hidden Vector Encryption. rather than encryption some extent with a

binary vector of T2 bits, wherever T is that the dimension size, it leverages a gradable encryption, that reduces the vector length to two log2 T bits. However, its search time

is still linear with relevance the amount of tuples in a dataset, that not solely runs slowly over large-scale datasets however conjointly disables economical updates.

Our recent work [11] presents a theme which will operate arbitrary geometric vary queries. It leverages Bloom filters and their properties, wherever an information purpose is delineate as a Bloom filter, a geometrical vary question is also fashioned as a Bloom filter, and therefore the results of AN inner product of those 2 Bloom filters properly indicates whether some extent is within a geometrical space. Its advanced version with R-trees are able to do exponent search on average. though it conjointly utilizes point mutually of the building blocks, its tree-based index and distinctive style with Bloom filters area unit utterly completely different from the novel two-level index introduced during this paper, wherever these significant variations stop this previous theme from supporting economical updates and sensible search time. Some other works study secure geometric operations between 2 parties (e.g., Alice and Bob), where Alice holds a secret purpose and Bob keeps a non-public geometric vary. With Secure Multi-party Computation (SMC), Alice and Bob will decide whether or not some extent is inside a geometrical vary while not revealing secrets to each other. However, the model of those studies area unit different from ours (i.e., Alice and Bob each offer individual non-public inputs, whereas a shopper in our model has all the non-public inputs however the server has no non-public inputs). Besides, SMC introduces in depth interactions.

3.1 Advantages:

FastGeo not solely provides extremely economical updates over encrypted spatial information, however conjointly improvessearch performance over 100x.. Our style permits geometric vary queries with whimsical shapes, e.g., circles, polygons, etc.

III. System Architecture

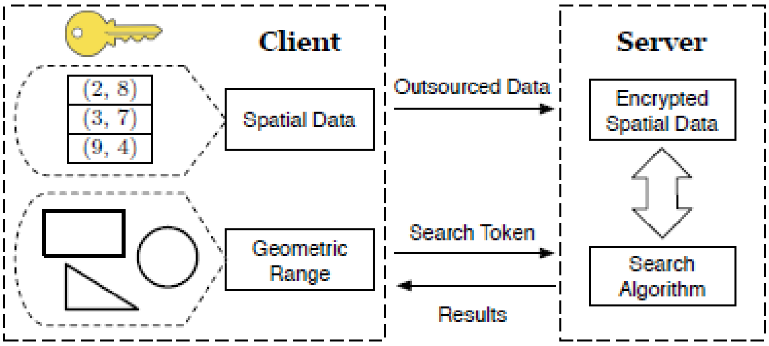

Fig. 1: The system model of a GSE scheme.

It is fascinating to store information on information storage servers like mail servers and file servers in encrypted kind to scale back security and privacy risks. however this typically implies that one has got to sacrifice practicality for security. as an example, if a shopper needs to retrieve solely documents containing bound words, it had been not antecedently illustrious a way to let the info storage server perform the search and answer the question, while not loss of knowledge confidentiality. we have a tendency to describe our cryptanalytic schemes for the matter of looking out on encrypted information and supply proofs of security for the ensuing crypto systems. Our techniques have variety of crucial benefits. they're incontrovertibly secure: they supply demonstrable secrecy for cryptography, within the sense that the untrusted server cannot learn something concerning the plaintext once solely given the ciphertext; they supply question isolation for searches, which means that the untrusted server cannot learn something additional concerning the plaintext than the search result; they supply controlled looking out, in order that the untrusted server cannot look for AN absolute word while not the user's authorization; they conjointly support hidden queries, in order that the user could raise the untrusted server to go looking for a secret word while not revealing the word to the server. The algorithms conferred area unit straightforward, quick (for a document of length n, the cryptography and search algorithms solely would like O(n) stream cipher and block cipher operations), and introduce nearly no area and communication overhead, and thus area unit sensible to use nowadays.

IV. Conclusion

We propose FastGeo, associate degree economical two-level search scheme that may operate geometric ranges over encrypted spatial datasets. Our experiment results over a realworld dataset demonstrate its effectiveness in apply. Moreover, our comparison with previous solutions indicates that the final plan of two-level search are often leveraged as a vital methodology to spice up search time and alter extremely economical updates over encrypted data once complicated operations, like compute-thencompare operations, square measure concerned in search.With FastGeo, that could be a novel two-level seek for encrypted spatial knowledge, associate degree honest-but-curious server will with efficiency perform geometric vary queries, and properly come knowledge points that square measure within a geometrical vary to a consumer while not learning sensitive data points or this non-public question. FastGeo supports discretionary geometric areas, achieves sublinear search time, and allows dynamic
updates over encrypted spatial datasets. Our theme is demonstrably secure, and our experimental results on real-world spatial datasets in cloud platform demonstrate that FastGeo will boost search time over a hundred times.

References

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” Nat. Instit. Standards Technol., vol. 53, no. 6, p. 50, 2009.

[1] D. Song, D. Wagner, and A. Perrig, “Practical Techniques for Searches on Encrypted Data,” in Proc. of IEEE S&P’00, 2000.

[2] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, “Searchable Symmetric Encryption: Improved Definitions and Efficient
Constructions,” in Proc. of ACM CCS’06, 2006.

[3] S. Kamara, C. Papamanthou, and T. Roeder, “Dynamic Searchable Symmetric Encryption,” in Proc. of ACM CCS’12, 2012.

[4] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, “Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries ,” in Proc. of CRYPTO’13, 2013.

[5] V. Pappas, F. Krell, B. Vo, V. Kolesnikov, T. Malkin, S. G. Choi, . George, A. Keromytis, and S. Bellovin, “Blind Seer: A Searchable Private DBMS,” in Proc. of IEEE S&P’14, 2014. 14 IEEE Transactions on Dependable and Secure Computing,Year: 2017, Volume: PP, Issue: 99

[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 System for Monitoring Mobile Users: Making Searchable Encryption Practical,” in Proc. of ACM CODASPY’14, 2014.

[9] B. Wang, M. Li, H. Wang, and H. Li, “Circular Range Search on Encrypted Spatial Data,” in Proc. of IEEE CNS’15, 2015.

[10] 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.

[11] S. Goldwasser and M. Bellare. Lecture notes on cryptography. Available online from http://wwwcse.ucsd.edu/users/mihir/papers/gb.html.