A REVIEW ON GEOMETRIC RANGE QUERIES ON ENCRYPTED SPATIAL DATA

K. Kumaraswamy[1] & Manohar Gosul[2]

M.Tech[1] & Assistant professor[2] Dept of CSE from Bharat Institute of Engineering and Technology

ABSTRACT

Spatial data has wide applications, for example, location-based services and geometric range queries (for example, finding points within geometric areas, for example, circles or polygons) are one of the fundamental functions of research on spatial data. The growing demand data outsourcing is moving large-scale data sets, including large-scale spatial data sets for public clouds. Meanwhile, due to concern intruders and hackers on public clouds, the privacy of spatial data sets should be stored with caution when on the server side, especially for medical and location-based use. In this paper, we have formalized the concept of Geometrically Searchable Encryption, and propose an efficient system called FastGeo, to protect the privacy of data of space customers stored and accessible in a public employee. With FastGeo, which is a new search for two-level encrypted spatial data, an honest-but-curious server can effectively perform geometric range queries and correctly return data points that are within a geometric range for a client without learning data points or private consultation.

KEYWORDS: Spatial data, geometric range queries, encrypted data, and privacy

INTRODUCTION

Searchable encrypted features data on a remote server (for example, a public cloud) without decryption. In particular, with SE, a customer (for example a company) can retrieve the correct search results from an honest curriculum without divulging data or private consultations. A series of sequences SE where most focuses on common SQL queries, such as like search by keywords and search for rank. Recently some SEs the programs have given particular emphasis to geometric queries in spatial data sets, where the geometric width query retrieves the points within a like a circle or a polygon. However, like enable geometric queries with underscores Search and support

time for effective updates the encrypted spatial data remains open. Spatial data has extensive applications in place services, computational geometry, medical images, geosciences, etc. and geometric issues of amplitude basic search functions in spatial data sets. For example, a customer can find friends in circular site-based services (for example, Facebook). a doctor the investigator can predict if there is a risk manifestation of a particular virus in a particular geometric region (eg zika in Brazil) who are recovering patients in the area Many companies, such as Yelp and Foursquare, now depends on public clouds (for example, Amazon Web AWS) to manage their spatial data sets and process requests. However, due to potential threats hackers and intruders, the privacy of space datasets in public clouds must be carefully especially in medical and localization applications. For example, an AWS commitment for a attacker or hacker would put millions of Yelp users places sensitive to honor Different from the keyword search that depends on equality analysis and scope search based on comparisons, a query of geometric range in a set of spatial data essentially it requires calculation and comparison operations. For example, to decide if a point is in a circle, calculate a distance from this point to the center of a circle and then compare that distance with the radius of this circle; check if there is a point in a polygon, we calculate the cross product of this point with each vertex of this polygon, and compare each cross produced with zero (that is, positive or negative).

LITERATURE REVIEW

[1] Art to solve problems for us things in it to give such satisfaction to the new heights include the property of some object, to pre-emulate a number of great weight issues. Difficulties and it is one very well-known that the genus is that we can find the query have agreed on the signing of the altar he will take off badly junction problems etc. A new search for federation called general strikes. In most studies, filtering allows us to improve the worst complexity of the most famous algorithms to solve the above mentioned problems.

[2] A typical range search has the following form: pre-processed A set of points for the search zone is located in the S-score can be revealed, or quickly. We study the arguments of your learning and information skills to describe scale research and other applications of related problems.

Research area is a wide range of applications, which these information systems, computer graphics, databases, states and times, a number of databases. In addition, other problems may encounter problems in the geometry zone in shape

[3] We study the secret proximity tests: Alice and Bob to show that there is almost no information on any other parts of the world to reveal. We describe a variety of protocols to ensure private testing close to the various levels of granularity. We have learned to use the location "tags" generated by the developer to improve the physical security of the proximity test. In our system we have implemented to inform Android, and its effectiveness. Our system uses social networks (Facebook) to manage public keys.

[4] With the arrival of reliable positioning technologies and the prevalence of location-based services, you can now accurately study the spread of issues such as infectious viruses, malware and sensitive information through a population of mobile objects such as people, mobile devices and vehicles. In such application scenarios, an object passes between two objects when the objects are close enough (when they are supposedly in contact) and once an object is started, it can enter the object population via the network the evolution of contacts between objects, a network of contacts called. In this article we define and study for the first time the accessibility of the query of large amounts of data (which are on the disk) that register the movement of a (possibly important) collection of objects that are in a space for a longer period. A query for authentication when two objects are "accessible" via the contact network represented by this evolving set of coordinates. We offer two indices with contact details that can be used to evaluate the effectiveness of these questions, despite the potentially enormous size of all contact information.

[5] This well-accepted introduction to computational geometry is a textbook for undergraduate and graduate undergraduate courses. The focus is on algorithms and the book is ideal for computer and engineering students. Motivation is offered by the fields of application: all the solutions and techniques resulting from computational geometry are related to specific applications in robotics, graphic images, CAD / CAM and geographical information systems. This motivation is particularly welcome for students. Modern knowledge of computational geometry is used to provide solutions that are both effective and easy to understand and implement. All basic techniques and topics of computational geometry, as well as several more advanced topics, are discussed. The book is largely self-contained and can be used for self-study by anyone with basic training in algorithmics. In this third edition, in addition to revisions to the second edition, new sections have been added to Voronoi diagrams of line segments, the most remote Voronoi diagrams and realistic input models.

PROBLEM STATEMENT

Although most searchable encryption plans focus on basic SQL requests such as Keyword and Boolean search, few revisions have explored the particular geometric range look beyond the encrypted spatial information. Wang et al. [13] proposed a new plan to specifically investigate the circular range encrypted information using an array of concentric circles. Some searchable from the past the cryptographies dealing with the request tests can fundamentally supervise the parallel scope to look for encrypted space information. In the same way, Order Preservation Encryption, which has weaker security ensures searchable encryption, is also ready to run the axis in parallel rectangular flow research with trivial extensions. Ghinita and Rughin particularly explored functional cryptography with hierarchical criteria coding to productively work the appearance of the rectangular band parallel to the axis in encrypted space information on the use of mobile user monitoring [6].

The most searchable encryption schemes focus on basic SQL queries like keyword queries and Boolean queries, few revisions have explored geometric coverage in particular search for encrypted space information. Inevitably it presents obstacles in terms of search functionality for the encoded information. None of these previous works focused in particular on the geometrical surveys tracked parallel rectangles or triangles not parallel to the axis. More importantly, there is not yet a general approach that can be various types of geometric queries on encoded spaces their specific geometric shapes

PROPOSED SYSTEM

In this paper, we propose a symmetric-key probabilistic Geometric Range Searchable Encryption. With our plan, a semi-honest (i.e., honest-but-curious) cloud server can confirm whether a point is inside a geometric range over encrypted spatial datasets. Casually, aside from taking in the essential Boolean output (i.e., inside or outside) of a geometric range look, the semi-genuine cloud server is not ready to uncover any private data about information or questions. Our primary contributions are outlined as takes after: We exhibit a symmetric-key probabilistic Geometric Range Searchable Encryption, and formally characterize and demonstrate its security with indistinguishability under Selective Chosen-Plaintext Attacks (IND-SCPA). In expansion, our inquiry procedure is non-intuitive on encoded information. As far as inquiry multifaceted nature,

our benchmark plot acquires straight intricacy (concerning the quantity of information records), and its propelled variant acknowledges speedier than-direct hunt by incorporating with tree structures. Our configuration is a general approach, which can safely bolster diverse sorts of geometric range questions on encoded spatial information paying little heed to their geometric shapes. Moreover, our plan is appropriate for geometric range inquiries, as well as perfect with other normal sorts of geometric questions, for example, crossing point inquiries and point nook inquiries, over encrypted spatial information. The security of our plan is formally characterized and analyzed with indistinguishability selected selective attacks in plain text. Our configuration can be used and updated in large applications, such as Location-based services and spatial databases, where the use of Information is necessary with the need for solid security.

CONCLUSION

We have studied a general approach for the secure scanning of encrypted spatial data with geometric data Interval query. In particular, our solution is independent in the form of a geometric range inquirer with the additional use of R trees; our scheme is able to achieve a faster search complexity than linear in relation to the number of points in a data set. The security of our scheme it is formally defined and analyzed with indistinguishability under Selective Chosen-Plaintext Attacks. Our design has great potential to be used and implemented in large applications such as location-based services and spatial databases, where the use of spatial data A strong requirement for privacy is required.

REFERENCES

[1] B. Chazelle, Filtering search: A new approach to query-answering, SIAM J. Comput., (1986), Vol.15, No.3, pp.703-7240.

[2] P. K. Agarwal and J. Erickson, Geometric range searching and its relatives, Discrete Comput. Geometry, (1999), Vol.223, pp.1-56.

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

[4] H. Shirani-Mehr, F. Banaei-Kashani, and C. Shahabi, Efficient Reachability Query Evaluation in Large Spatiotemporal Contact Datasets, Proc. VLDB Endowment, (2012), Vol.5, No.9, pp.848-859.

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

[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.