FASTGEO: EFFICIENT GEOMETRIC RANGE QUERIES ON ENCRYPTED SPATIAL DATA

ABSTRACT

- Spatial data have wide applications, e.g., location-based services, and geometric range queries (i.e., finding points inside geometric areas, e.g., circles or polygons) are one of the fundamental search functions over spatial data.
- The rising demand of outsourcing data is moving large-scale datasets, including large-scale spatial datasets, to public clouds. Meanwhile, due to the concern of insider attackers and hackers on public clouds, the privacy of spatial datasets should be cautiously preserved while querying them at the server side, especially for location-based and medical usage

- In this paper, we formalize the concept of Geometrically Searchable Encryption, and propose an efficient scheme, named FastGeo, to protect the privacy of clients' spatial datasets stored and queried at a public server.
- With FastGeo, which is a novel two-level search for encrypted spatial data, an honest-but-curious server can efficiently perform geometric range queries, and correctly return data points that are inside a geometric range to a client without learning sensitive data points or this private query.
- FastGeo supports arbitrary geometric areas, achieves sub linear search time, and enables dynamic updates over encrypted spatial datasets

EXISTING SYSTEM

- 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, a client 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.

PROPOSED SYSTEM

- 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)

HARDWARE REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS

- Operating system : Windows XP/7.
- Coding Language : java/Asp.net

CONCLUSION

- We propose FastGeo, an efficient two-level search scheme that can operate geometric ranges over encrypted spatial datasets. Our experiment results over a real-world dataset demonstrate its effectiveness in practice. Moreover, our comparison with previous solutions indicates that the general idea of two-level search can be leveraged as an important methodology to boost search time and enable highly efficient updates over encrypted data when complex operations, such as compute-then-compare operations, are involved in search.