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.

EXISTING SYSTEM

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. 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, 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. For instance, a compromise of AWS by an inside attacker or hacker would put millions of Yelp users' sensitive locations under the spotlight.

Disadvantages

- Its leakage functions, and rigorously not proves data privacy and query privacy with in distinguish ability under selective chosen plaintext attacks.
- It provides less security under selective chosen plaintext attacks with this leakage function.

PROPOSED SYSTEM

We propose FastGeo, an efficient two-level search scheme that can operate geometric ranges over encrypted spatial datasets. Our experiment results over a realworld 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-thencompare operations, are involved in search.

Advantages

- FastGeo not only provides highly efficient updates over encrypted spatial data, but also improves search performance over 100x.
- FastGeo in cloud platform (Amazon EC2), and demonstrate that Fast-Geo is highly efficient.

SOFTWARE REQUIREMENTS

Front-end	:	JSP
Back-End	:	MySQL
Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3
RAM	:	512MB-2GB
HARD DISK	:	40GB