

**CHENNAI – PONDICHERRY**

**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 sublinear search time, and enables dynamic updates over encrypted spatial datasets. Our scheme is provably secure, and our experimental results on real-world spatial datasets in cloud platform demonstrate that FastGeo can boost search time over 100 times.