

**CHENNAI – PONDICHERRY**

**QLDS: A Novel Design Scheme for Trajectory Privacy Protection with Utility Guarantee in Participatory Sensing**

**Abstract:**

Participatory sensing, leveraging on the ubiquity of cheap sensors in mobile devices, enables various promising applications of great social benefit. However, its ubiquitous sampling and openness results in serious privacy concerns. People’s activity trajectories may reveal their private information such as home and work place and thus requires proper protection. In this paper, we propose a novel design scheme, called query logics detached storage (QLDS), for trajectory privacy protection. The core idea of QLDS is to extract the query logics for personal trajectory retrieval and make actual trajectory tuples not clustered to any route-identity or user-identity at server end, which introduces fine-granularity anonymity. The QLDS design scheme stores the extracted query logics at users own client devices and the un-clustered location tuples at the backend server, guaranteeing trajectory reconstruction at client-end and privacy preservation at server-end. Besides,integration of QLDS with other privacy protection approaches can further enhance the protection strength and bring flexible configurations to meet individuals’ variable privacy concerns. The theoretical analytics is provided for the privacy and utility evaluation. The data retrieval performance of QLDS is experimentally evaluated in real-world internet environment.

**Existing System:**

PS is regarded as a promising solution to solve large-scale urban issues that require collection of data and feedback from people, and has been implemented in many domains such as transportation, environmental monitoring, information sharing, public health etc. While PS enables so many promising applications that bring value to people and society, its intrinsic ubiquitous sampling and openness poses serious privacy concerns. For instance, the spatiotemporal trajectory data (sequential GPS data) discussed in this paper is of high relevance with participants’ personal activity routines. If an adversary has a priori knowledge of these trajectory data, it is possible to mine out users’ private information such as users’ traveling pattern and home or work place etc. GPS data are commonly used in many PS applications. It is beneficial to design effective approaches for trajectory privacy protection.

**Proposed System:**

A novel design scheme, QLDS, is proposed for trajectory privacy protection whilst assuring both the client end’s and server end’s utilities through separating the storage of the discrete tuples (stored in the backend server) and the critical query logics of high relevance with personal privacy (stored in individuals’ clients).

• The trajectory privacy protection strength and the client-end & server-end utility of QLDS is theoretically discussed; meanwhile, we concretize the idea using a realworld PS dataset.

• QLDS breaks the symmetry in information retrieval between the participants and platform owner to guarantee 100% reconstruction at client end (to enable client-end utility) and privacy preservation at server end.

• The design scheme allows for integration with other privacy protection approaches of flexible configurations to meet individuals’ variable privacy concerns whist enhancing the privacy protection strength.

• For utility evaluation, the metrics are suggested to be considered according to the concrete application requirements. We for the first time propose a sub-utility oriented.