**Title:**

**Towards Privacy-Aware Location-Based Database Servers**

**What is the research problem?**

A lot of services offered to the end customers are location based. However these location based devices pose a serious threat to the user’s privacy like location, if it goes to untrusted hands. In the existing model either the user can avail the server and compromise the privacy or can turn off these services. The paper recommends a model using which location based services can be availed yet based on the user setting the privacy to not completely compromise.

**Overview/main points of the proposed approach/architecture**

* There has been a huge increase in the number of location based services and the amount of data around it.
* Location based services like find the nearest restaurant, nearest store, delivering weather report based on location, traffic information etc.
* The whole idea is based on spatial-temporal queries where accuracy and efficiency are very crucial like a small delay in response may completely render an obsolete answer.
* The service providers in these cases, although assure safety of data and privacy but for obvious reasons such services threaten the privacy of the user/customers.
* Such services continuously send the users location information to the server to provide better services.
* Such services can be misused to stalk or illegally record movements of the customers.
* The approach of pseudonymity (fake identity) cannot be applied to such services.
* Either the user can avail such services or altogether turn it off for privacy reason.
* This is where this papers recommends a location based services with high quality without compromising on the privacy.
* Using a trusted third party termed as Location Anonymizer the whole idea is achieved.
* The anonymizer receives the exact location of the of the end customer.
* It’s the responsibility of the Location Anonymizer to blur the user location based on the user settings, its termed as cloaked spatial region.
* This cloaked spatial region is than send to the local based service provider for further processing.
* Location privacy is suggested to be achieve in two ways. Scalability and Query processing. To achieve the above following approaches are recommended
  + False dummies: Send multiple user co-ordinates including the fake once. So the server never knows which one is the right user location.
  + Landmarks: Instead of exact user location, landmarks around can be used. But the accuracy/efficiency in this case is questionable.
  + Location perturbation: the idea is to blur the user location in a spatial region or location obfuscation.
  + Avoid user tracking and only when needed the user can share the location to avail the service.
* Database Privacy: Even before storing the data, its perturbed hence privacy is managed even before storing the data. In privacy-aware location based servers the aim is to protect the user who queries and not the data.
* K-anonymity in case of database privacy is feasible when the data is not updated frequently. In location based service environment the data and queries are bound to change continuously, which needs a new model to provide the kth-anonymity.
* Hence the idea of location anonymizer comes, which acts a third party between the mobile user and the location based service provider.
* The user set his/her own profile with preferences, accordingly the location Anonymizer cloaks the location of the user in the spatial region which satisfies the user preferences set, which is then finally sent to the location based service provider
* Privacy Profile of the user contain the following which set the user preferences:
  + The level of anonymity: A kth anonymity means the user cannot be distinguished among other k users.
  + Minimum Area: The minimum cloaked spatial region.
  + Maximum Area: The maximum cloaked spatial region.
  + Temporal constants: Based on the user preference the above parameters which differ from time to time based on the settings/preferences.
* Constructing the cloaked region will be dependent on the data-dependent or space-dependent
* Data and query Types: Data is divided into two type as below:
  + Public data: its location need not be hidden, available to all
  + Private data: Data contain personal information, comes under privacy purview.
* Accordingly two types of queries needs to be supported by the privacy aware location based database server:
  + Private queries over public data: person asking location of the nearest gas station. Person exact location not know (private), but the gas station (public) location is available.
  + Public query over private data: Administrator want to know about the number of active mobile users in a given area.
* Privacy aware location based database servers is a tradeoff between the user privacy preference and the amount of information the user is ready to release for the same.

**Conclusion:**

This paper highlights privacy related threats imposed by the location detection services and recommends research in the direction of privacy-aware location-based database servers. The idea here is to protect the sensitive user location and yet provide location based services with trade off in quality. It balances the amount of information released to the quality of the service desired by the end user. In addition query types were introduced Private queries over public data and Public query over private data.