In the last decade, mobile communication has enjoyed unprecedented growth all over the world. The recent advances in mobile communication technologies including Global Positioning System (GPS) and Radio Frequency Identification (RFID) have propelled the growth of a number of mobile services. A particularly thriving example is that of location-based services (LBS). LBS is to request usable, personalized information delivered at the point of need, which includes information about new or interesting products and services, promotions, and targeting of customers based on more advanced knowledge of customer profiles and preferences, automatic updates of travel reservations, etc. For example, a LBS provider can be designed to present users with targeted content such as clothing items on sale, based on prior knowledge of their profile, preferences and/or knowledge of their current location, such as proximity to a shopping mall. Additionally, LBS can provide nearby points of interests based on the real-time location of the mobile customer, advising of current conditions such as traffic and weather, deliver personalized, location-aware, and context-sensitive advertising, again based on the mobile customer profiles and preferences.

By definition, delivery of LBS requires knowledge of a mobile customer’s location. Along with the location information, their preference profiles must also be maintained. Effective delivery requires efficient processing of access requests on this data to find the past, present and future status of the mobile customers (or moving objects) that match a certain profile. Personalization and customization of such services, based on the profiles of mobile users, would significantly increase the value of such services. Whether LBS is delivered in a “push” or “pull” fashion, customization and personalization based on the location information, customer profiles and preferences, and vendor offerings are required. This is because, to be effective, targeted advertising should not overwhelm the mobile consumers and must push information only to a certain segment of mobile consumers based on their preferences and profiles, and based on certain marketing criteria. Obviously, these consumers should be targeted only if they are in the location where the advertisement is applicable at the time of the offer.

However, this creates significant challenges. Since effective delivery of LBS may need to locate and track a mobile customer, and gain access to his/her profile, a number of security and privacy concerns arise. Location information has the potential to allow an adversary to physically locate a person. As such, wireless subscribers carrying mobile devices have legitimate concerns about their personal safety, if such information should fall into the wrong hands. To deal with this, the concept of location $k$-anonymity has been advanced [2]. Instead of revealing the exact location, a bounding box is reported containing at least $k$ people. This provides for more physical security, since you cannot be individually identified within the bounding box. However, this ignores the fact that profile information may serve to further identify an individual. Since profile information is increasingly collected and used in services such as targeted advertising and personalized dating [1] to deliver the service based on the mobile users’ profile and preferences, privacy of mobile users can be compromised if the sensitive profile information of the mobile users is revealed to unintended users. Even though location privacy is protected through location $k$-anonymity, a person could be identified through their profile. For example, even if $k$ people, reside on the 10th floor, there may only be one Asian female. In this case, profile information can be used to distinguish between and uniquely identify a person, and the guarantee of location $k$-anonymity fails. Essentially, a person may still be identified based on his/her profile if the profiles of all $k$ people are not the same. Therefore, it is important that anonymity guarantees apply over location as well as profile information. We argue that it is necessary to extend the notion of $k$-anonymity by incorporating user profiles. We discuss different flavors of anonymization that guarantee anonymity even when profiles of mobile users are known to untrusted entities, that generalize both location and profiles to the extent specified by the user.

Services such as targeted advertising may deliver the
service based on the mobile customers’ profile and preferences. It is important to note here that user profile information may include both sensitive and non-sensitive attributes such as name, address, linguistic preference, age group, income level, marital status, education level, etc. However, certain segment of mobile consumers are willing to trade-off privacy by sharing such sensitive data with selective merchants, either to benefit from personalization or to receive incentives offered by the merchants. For example, a security policy may specify that a customer is willing to reveal his age in order to enjoy a 20% discount coupon offered on sports clothing. But he is willing to do this only during the evening hours and while close to the store. As such, privacy of mobile users can be compromised if the sensitive profile information of the mobile users is revealed to unintended users. Therefore, it is important that the sensitive profile information is revealed to the respective merchants only on a need-to-know basis, when allowed. As a result, the security policies in such an environment are characterized by spatial and temporal attributes of the mobile customers (location and time), as well as their profile attributes.

To ensure security, an appropriate access control mechanism must be in place to enforce the authorization specifications reflecting the security and privacy needs. One way to take these concerns into account is by establishing security policies and enforcing them for every access. A comprehensive security policy can encode spatiotemporal restrictions on access to location and profile. Serving an access request requires to search for the desired moving objects that satisfy the query, as well as identify and enforce the relevant security policies.

In addition to the security and privacy concerns mentioned above, there are a number of applications that call for securing resources based on the criteria of mobile objects. These include context (location)-sensitive access control, and the ubiquitous computing environment, where access is permitted based on the location of the subjects/objects during a specific time.

While LBS are often presumed as untrusted entities, the location services (LS) that capture and maintain mobile users’ location to enable communication are considered trusted, and therefore can capture and manage the profile information. The current location of moving objects are stored and updated accordingly in order to provide most up-to-date location information to a requester. Location information can be directly provided by users’ mobile devices using wireless communication periodically, or acquired from the installed sensors. LS is responsible for maintaining and enforcing the specified security and pri-
vacy policies. To efficiently enforce the access requests and perform anonymization, LS maintains the mobile object’s location, velocity, mobile user’s profile and the authorizations using a unified index, as shown in figure 1. The access requests are processed by the LS, which searches the index for the authorized data that adheres to the specified security policies. It also converts the user’s request to a generalized request by generalizing it based on the user’s privacy specifications.

While the above authorization enforcement and anonymization solve the security problem, they may create performance problems. Often, enforcing security incurs overhead, and as a result may degrade the performance of a system. However, the key insight is to realize that a lot of duplicate work is performed. Thus, one way to alleviate this problem and to effectively serve access requests, is to efficiently organize the mobile objects, authorizations as well as mobile customers’ profiles. In this talk, we discuss the different solutions proposed by researchers in a response to ensuring security and privacy. The solutions specifically propose unified index schemes for organizing moving object data, authorizations and profiles of users, which result in significant gain in performance during anonymization as well as query processing.

References
