Title: Securing Data in the Cloud – Challenges and Research Directions

Abstract:

Managing data is arguably one of the reasons for adopting cloud technologies. These technologies are very promising with respect to enhancing scalability, reducing costs, and rapidly adapting to changes in application demands. However the adoption of these technologies is not without risks. Data stored in a cloud would be accessible to a large variety of individuals, like the IT staff of the cloud providers. The cloud providers may in turn outsource data management functions to other providers. Data integrity and availability are critical issues. Physical protection, crucial for data security, may be difficult to assess for the organization owning the data as data may be stored in different countries, which makes difficult making inspections to the data storage location. In some cases, even being able to control the location of the data may be difficult. However, making sure that data is stored or not stored in certain locations is crucial for compliance. Data segregation is essential in the context of multi-tenant contexts in which data owned by different organizations may reside on the same systems. Support for disaster recovery, and accountability are also critical requirements. In the talk we will first elaborate on these issues. We will then present an overview of the MASK system, able to support fine-grained encryption of data while at the same time supporting identity-based privacy-preserving access control on encrypted data.