Simple searchable encryption framework for supporting complex queries

Murat Kantarcioglu, UT Dallas

Many efficient searchable encryption schemes have been developed over the years. Almost all of the existing searchable encryption schemes are developed for keyword searches and/or require running some code on the cloud servers. However, many of the existing cloud storage services (e.g., Dropbox, Box, Google Drive etc.) only allow simple data object retrieval and do not provide computational support needed to realize most of the searchable encryption schemes.

In this talk, we discuss how to enable efficient execution of complex search queries over wide range of encrypted data types (e.g., image files) without requiring customized computational support from the existing cloud servers. To this end, we provide an extensible framework for supporting complex search queries over encrypted multimedia data. Before any data is uploaded to the cloud, important features are extracted to support different query types (e.g., extracting facial features to support face recognition queries) and complex queries are converted to series of object retrieval tasks for cloud service. Our results show that this framework may support wide range of image retrieval queries on encrypted data with little overhead and without any change to underlying data storage services.

Later on, we discuss how some of the sensitive information leakage (e.g., data access patterns) in the above framework could be limited using differential privacy. Finally, we discuss how to leverage recent developments in trusted execution environments such as SGX to enable complex data analysis while hiding all the access patterns.