# Preserving Data Privacy Through Data Partitioning in Mobile Application

Mohammad Al-Mutawa and Shivakant Mishra
Department of Computer Science, University of Colorado Boulder
Campus Box 0430 Boulder, CO 80309-0430, USA.
{almutawm|mishras}@colorado.edu

A key concern in utilizing external resources for mobile application execution is a potential loss of data privacy. User data needs to be shipped to possibly untrusted remote nodes for execution. This work introduces the concept of data partitioning, where in the user can conveniently identify the sensitive parts of her data, which is then prevented from being shipped to untrusted remote servers. The overall execution consists of identifying sensitive data, shipping code and non-private data for remote execution and getting the results back, and then combining the results from local and remote executions on the mobile device. Data partitioning can be used for a variety of personal digital files that the users create and modify using applications. These include images, videos, audios, textual documents and spreadsheets. It allows mobile users to enjoy a better computing experience by not only further improving the performance and saving power, but also *preserving data privacy.*

We will demonstrate the data partitioning concept with an image processing app. The app takes pictures stored on a smartphone and applies digital filters to them. The app has two main components, one that runs on the phone and another one that runs on a remote node. The user draws a square to denote the private section of the picture, and the app will partition the image, shipping the public section of the picture to be processed on the remote node and processing private section on the phone. The results are combined on the phone and the filtered picture is shown on the screen.

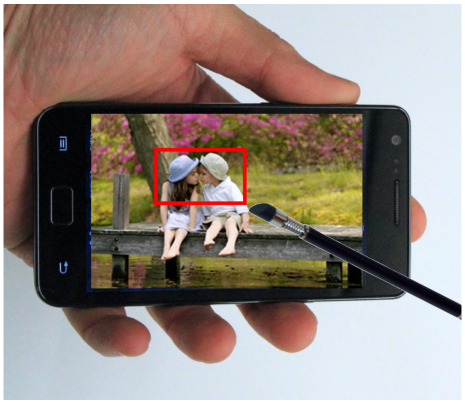

Figure 1: Denoting the private section of the picture