

به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه



محرم‌انگلی الگوی دسترسی به داده‌ی برون‌سپاری شده

Confidential Access to the Outsourced Data

الهه سادات نجم آبادی

زمان: شنبه ۱۵ شهریورماه ۱۳۹۳ ساعت ۳ عصر

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن ۴۰۴

امروزه بسیاری از افراد و سازمان‌ها برای رهایی از مشکلات نگهداری داده‌ها، آن‌ها را روی یک کارگزار خارجی قرار می‌دهند. یکی از بزرگترین چالش‌های پیش‌رو عدم اعتماد به کارگزارهاست. معمولاً فرض بر امین اما کنجکاو بودن کارگزار است. در سال‌های گذشته تحقیقات زیادی برای از بین بردن کنجکاوای کارگزار و محرمانه کردن داده‌ها به کار رفته است. دسته‌ی بزرگی از این تحقیقات، در راستای حفظ محرمانگی محتوایی و رمزنگاری داده‌ها بوده است. دسته‌ی دیگری از این تحقیقات که کمتر مورد توجه بوده در راستای حفظ محرمانگی دسترسی و الگوی دسترسی است. در این ارائه به بررسی این مهم پرداخته می‌شود. روشی که در این ارائه مطرح می‌شود روشی است که نسبت به سایر روش‌ها دارای هزینه نسبتاً کم و کارایی بیشتر است. در این روش محرمانگی دسترسی مورد نیاز در داده‌های برون‌سپاری شده تأمین می‌شود، در عین حال هزینه روش‌هایی که امنیت تئوری اطلاعاتی دارند پرداخت نمی‌کند.

حضور دانشجوین گرامی در این سمینار مورد انتظار است.