به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

پردازش آگاه از رمزنگاری پرس‌وجوها در برون‌سپاری داده

جواد قره چمنی

زمان: شنبه ۶ شهریور ماه ۱۳۹۵ ساعت ۹:۱۵

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهار، سالن خوارزمی

یکی از راهکارهای کاهش هزینه نگهداری داده‌ها و اطمینان از دسترس‌پذیری آنها، استفاده از خدمات ابری است. با برون‌سپاری داده‌ها به کارگزارها، نیازی به خرید تجهیزات گران‌قیمتِ ذخیره‌سازی و استخدام نیروهای خبره نیست. آنچه‌که تاکنون مانع استفاده‌ی مالکان داده از این خدمات شده، عدم وجود امنیت کافی در این حوزه است. اگرچه راه‌کارهایی مثل کریپت.دی.بی و اس.دی.بی سعی در رفع این نقصان نموده‌اند، اما بدلیل محدودیت‌های این روش‌ها، مالکان داده نتوانسته‌اند از آنها استفاده نمایند. یکی از مشکلات موجود در سامانه‌های برون‌سپاری داده، عدم توانایی آن‌ها در اجرای انواع پرس‌وجو، بر روی داده‌های رمز شده است. سربار محاسباتی روش‌های رمزنگاری کاملاً هم‌ریخت، موجب شده است که تنها روش‌های خاص‌منظوره‌ی رمزنگاری قابل استفاده باشند. همچنین برای بسیاری از انواع داده وعملگرهای مورد استفاده کاربران، روش رمزنگاری مناسبی که بتواند با روش‌های قبلی ترکیب شود، وجود ندارد. در این ارایه به بررسی ابعاد مختلف این موضوع خواهیم پرداخت.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.