بسمه تعالی

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه

اعمال کنترل دسترسی با استفاده از شاخص

هادی حلواچی

شنبه ۳۱ فروردین؛ ساعت ۹ صبح

دانشکده کامپیوتر، آزمایشگاه امنیت داده و شبکه

برون‌سپاری داده‌ها علاوه بر مزایای متعددی که دارد، با چالش‌های امنیتی زیادی مخصوصاً از بُعد حفظ محرمانگی داده‌های حساس همراه است. پرکاربردترین روش حفظ محرمانگی داده‌های برون‌سپاری شده، رمزنگاری داده‌ها است. بیشتر روش‌های رمزنگاری ارائه شده در سناریوی برون‌سپاری، یک فراداده به نام شاخص کنار داده رمز شده ایجاد می‌کنند. هدف از ایجاد شاخص، بهبود کارایی اجرای پرسجو روی داده رمزشده است.

تاکنون در روش‌های ارائه شده برای تولید شاخص، بدون توجه به خط‌مشی‌های کنترل دسترسی عمل شده است و اِعمال کنترل دسترسی با استفاده از روش‌هایی مانند رمزنگاری انتخابی و با مکانیزمی مجزا از تولید شاخص، تضمین می‌شود. این جدایی مکانیزم‌ها در تولید شاخص و اِعمال خط‌مشی‌های کنترل دسترسی، علاوه بر ایجاد سربار مضاعف، باعث افشای اطلاعات می‌شود. در این نشست روشی ارائه می‌دهیم که در آن ایجاد شاخص، با توجه به خط‌مشی‌های کنترل دسترسی صورت می‌گیرد. استفاده از این روش برای تولید شاخص، اِعمال کنترل دسترسی با ریزدانگی بالا را بدون نیاز به حضور برخط مالک داده، امکان‌پذیر کرده و امنیت را از طریق کاهش امکان استنتاج و نشت اطلاعات، افزایش می‌دهد.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.