به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

محرمانگی الگوی دسترسی به داده برون سپاری شده

Confidential Access to the Outsourced Data

الهه سادات نجم آبادی

زمان: شنبه ۹ آذرماه ۱۳۹۲ ساعت ۹ صبح

مکان: دانشکده مهندسی کامپیوتر، طبقه پنجم، آزمایشگاه امنیت داده و شبکه

با رشد روزافزون تمایل صاحبان داده به برون‌سپاری آن، چالش‌های امنیتی مرتبط با آن بسیار مورد توجه قرار گرفته‌است. در اکثر تحقیقات پیشین، دو مبحث محرمانگی محتوای داده برون‌سپاری شده و نیز کنترل دسترسی به آنها مورد بررسی قرار گرفته است ولی تحقیقات اندکی پیرامون محرمانگی الگوی دسترسی و محرمانگی دسترسی به داده‌ها انجام پذیرفته است در حالی که در مواردی نیاز است علیرغم اعمال مطلوب کنترل دسترسی، محتوای پرس و جو نیز از دید کارگزار مخفی بماند.

در این ارائه تلاش خواهیم نمود روش‌های حفظ محرمانگی الگوی دسترسی را معرفی نماییم. اغلب این روش‌ها بر اساس ترکیب سه تکنیک جست و جوی پوشا[1]، کش کردن[2] داده در سمت کارخواه و بُر زدن[3] داده می‌باشد. در این ارائه، ضمن معرفی این سه تکنیک، مثال‌هایی از نحوه به‌کارگیری عملی آن‌ها را در روش‌های حفظ محرمانگی دسترسی را بیان خواهیم کرد. در نهایت، به معرفی دسته دیگری از روش‌های حل این مشکل که مبتنی بر حافظه فراموشکار[4] هستند خواهیم پرداخت.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.

---

[1] Cover search
[2] Caching
[3] Shuffling
[4] Oblivious RAM