به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

برون‌سپاری امن داده مبتنی بر رویکرد تسهیم راز

A Secret Sharing Based Approach for Secure data Outsourcing

محمدعلی هادوی

زمان: شنبه ۲۴ مردادماه ۱۳۹۴ ساعت ۹:۱۵

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

برون‌سپاری داده رویکردی است که مدیریت داده را به‌عنوان یک خدمت به کارپذیر بیرونی واگذار می‌نماید. این رویکرد با توجه روزافزون به الگوی رایانش ابری که هدف آن تأمین مقرون‌به‌صرفه و منعطف منابع محاسباتی و ذخیره‌سازی است، اهمیت بیشتری پیدا کرده است. با این‌حال، ملاحظات امنیتی برون‌سپاری داده که ناشی از عدم اعتماد کامل به عملکرد کارپذیرهای بیرونی است، چالش جدی در پذیرش این رویکرد است.

در این ارائه روش‌هایی با رویکردی یکسان و قابل تجمیع مبتنی بر تسهیم راز برای برون‌سپاری امن داده معرفی می شوند. در این راستا، ابتدا روش‌های تسهیم راز جستجوپذیر برای تامین محرمانگی داده‌ها معرفی شده و سپس این روش‌ها، برای محیط‌های چندکاربره با سطوح دسترسی متفاوت گسترش یافته‌اند. در پایان روش‌هایی ارائه شده‌اند که می‌توانند هرگونه دست‌کاری غیرمجاز داده که منجر به پاسخ نادرست به پرس‌وجوهای کاربران می‌شود را تشخیص دهند. روش‌های مذکور می‌توانند در سامانه‌های مدیریت پایگاه داده‌ی موجود بدون تغییر در ساختارهای درونی آن‌ها مورد استفاده قرار گیرند که مزیت قابل توجهی از حیث کاربردپذیری روش‌ها محسوب می‌شود.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.