به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

جستوجوی عبارت منظم بر روی داده رمز شده

Regular Expression Search on Encrypted Data

رامین بهلولی

زمان: شنبه ۲۴ تیر ماه ۱۳۹۶ ساعت ۹:۱۵

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

خوارزمی

یکی از مشکلات برون‌سپاری امن داده، جستوجوی عبارت منظم بر روی داده‌های رمز شده می‌باشد. به عبارتی چنانچه قرار باشد داده‌های یک پایگاه‌داده برون‌سپاری شده رمز شوند، بایستی بتوان رمزگشایی داده در سمت کارگزار، جستوجوی عبارت منظم (دستور LIKE) را بر روی داده‌های رمز شده انجام داد.

با استفاده از الگوریتم‌های رمزنگاری موجود، این امکان در حال حاضر وجود ندارد اما در این سخنرانی یک روش رمزنگاری پیاده‌سازی شده ارائه می‌گردد که علاوه بر حفظ محرمانگی داده، امکان جستجوی عبارت منظم را بر روی داده‌ای رمز شده فراهم می‌نماید.

شرکت در این جلسه برای تمامی علاقه‌مندان آزاد است.