

به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه



جستجوی عبارت منظم بر روی داده رمز شده

Regular Expression Search on Encrypted Data

رامین بهلولی

زمان: شنبه ۲۳ آبان ماه ۱۳۹۴ ساعت ۹:۱۵

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

یکی از مشکلات برون سپاری امن داده، جستجوی عبارات منظم بر روی داده‌های رمز شده می‌باشد. به عبارتی چنانچه قرار باشد داده‌های یک پایگاه داده برون سپاری شده رمز شوند، بایستی بتوان بدون رمزگشایی داده در سمت کارگزار، جستجوی 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 داده‌های رمز شده فراهم می‌نماید.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.