

به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه



جستجوی مبتنی بر شاخص بر روی داده رمز برون سپاری شده

Indexing Based Search on Encrypted Outsourced Data

علی حبیبی

زمان: شنبه ۱۹ مهر ماه ۱۳۹۷ ساعت ۹:۱۵

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

اخیرا محاسبات ابری با سرعت روزافزون رو پیشرفت می‌باشد، یکی از کاربردهای اساسی محاسبات ابری، برون سپاری داده می‌باشد. برون سپاری داده بدین معنی می‌باشد که کاربران می‌توانند اطلاعات خود به سرور ابر بسپارند و از خدمات ذخیره سازی با کیفیت بالا استفاده نمایند، حال ممکن است ارائه دهندگان این خدمات مورد اعتماد نباشند، که در این صورت باعث ایجاد نگرانی برای امنیت داده ها می‌شود. ارائه دهندگان خدمات پایگاه داده های برون سپار اطلاعات را نگهداری می‌کنند و پاسخ پر سمان ها به کاربران می‌دهند. با توجه به این تفا سیر، حفظ محرمانگی در پایگاه داده های برون سپار برای پایگاه داده هایی که حاوی اطلاعات حساسی مانند اطلاعات مدارک مالی، اطلاعات پزشکی، اطلاعات مکان شخصی افراد، اطلاعات خانوادگی افراد و از این قبیل از اطلاعات هستند، بسیار ارزشمند و مورد توجه است. دومین چالش مطرح در برون سپاری داده، دستکاری داده و برگرداندن پاسخ اشتباه برای پرسمان های کاربران می‌باشد که در این صورت مسئله صحت، کامل بودن و تازگی پاسخ ها حائز اهمیت می‌شوند. مسئله اعمال کنترل دسترسی‌هایی در پایگاه داده‌های برون سپاری شده با توجه به خط‌مشی های قبلی در پایگاه داده محلی چالش سوم در برون سپاری داده می‌باشد، که کاربران باید از انجام کنترل دسترسی توسط ارائه دهنده خدمات اطمینان حاصل کنند و همچنین با توجه به این که در اکثر روش‌های حفظ محرمانگی، پایگاه داده رمز شده می‌باشد تغییر روش های کنترل دسترسی برای اعمال در پایگاه داده رمز شده نیز حائز اهمیت می‌باشد. در این جلسه سعی بر این خواهد شد این سه چالش و روش های حل ارائه شده بررسی شود .

شرکت در این جلسه برای تمامی دانشجویان علاقه مند آزاد است.