

به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه



# چالش‌های امنیتی برون‌سپاری داده و رویکرد امنیت اثبات‌پذیر

## Security Challenges of Data Outsourcing and Provably Secure Schemes

محمد علی هادوی

زمان: ۱۸ آبان ۱۳۹۲

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

برون‌سپاری داده در محیط رایانش ابری که از آن با تعابیر سرویس ذخیره‌سازی (Storage as a Service) و سرویس پایگاه داده (Database as a Service) نام برده می‌شود، با چالش‌های امنیتی روبرو است. این چالش‌ها ناشی از عدم اعتماد به میزبان داده و ارائه دهنده‌ی خدمات ذخیره‌سازی و مدیریت داده است. تاکنون روش‌های متعددی برای پاسخ به نیازمندی‌های امنیتی برون‌سپاری داده از جمله حفظ محرمانگی و اطمینان از درستی داده‌ها ارائه شده است که اثبات‌پذیری ویژگی‌های امنیتی در آن‌ها عموماً مدنظر نبوده است. در این ارائه، ضمن مرور چالش‌های امنیتی برون‌سپاری داده و راه‌حل‌های موجود، یک نمونه از روش‌های ارائه شده مبتنی بر رمزنگاری با دیدگاه امنیت اثبات‌پذیر بررسی می‌گردد.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.