به نام خدا

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه

استفاده از «رمزنگاری تابعی» در مدیریت داده‌های رمزشده

Using “Functional Encryption” to Manage Encrypted Data

روح‌اله محفوظی

زمان: شنبه ۲۳شهریور ماه، ساعت ۹ صبح

مکان: دانشکده‌ی مهندسی کامپیوتر، طبقه‌ی پنجم، آزمایشگاه امنیت داده و شبکه

اتاق ۵۰۲

امروزه بسیاری از سازمان‌ها برای رهایی از هزینه‌های نگه‌داری داده‌ها آن‌ها را نزد یک کارگزار خارجی برون‌سپاری می‌کنند. اما نبود اعتماد کافی به کارگزار خارجی برای اِعمال کنترل دسترسی مورد نظر مالک داده، به عنوان یک مشکل بزرگ برای برون‌سپاری داده‌های حساس مطرح است. در سال‌های اخیر پژوهش‌های مختلفی در زمینه کنترل دسترسی مبتنی بر رمزنگاری انجام شده است. در این ارائه روشی با استفاده از رمزنگاری تابعی برای اِعمال کنترل دسترسی توسط کارگزار غیر قابل اعتماد ارائه شده است. در این روش قابلیت پویایی در تغییر کنترل دسترسی در کنار راهبری خط‌مشی‌های دسترسی دیده شده است. بدین معنی که مالک داده ضمن امکان تغییر در خط‌مشی‌های دسترسی (اعطا و ابطال حق به کاربران) می‌تواند حق اعطا و ابطال حق را نیز به کاربران بدهد. این امکان در پژوهش‌های قبل کمتر مورد توجه بوده است. در پایان ارائه با ارائه‌ی نتایج مقایسه و تحلیل این روش با دیگر پژوهش‌ها نشان می‌دهیم روش ارائه شده برای تعیین حقوق دسترسی کاربران انعطاف‌پذیری بیشتری داشته و امکان اعطای حقوق مختلف دسترسی به مجموعه‌ای از کاربران در این روش ساده‌تر است. همچنین روش ارائه شده حافظ حریم خصوصی کاربران است و کارگزار نامعتمد از الگوی دسترسی کاربران مطلع نمی‌شود. وجود این مزایا به خاطر استفاده‌ی از رمزنگاری تابعی در اعمال کنترل دسترسی می‌باشد.