بسمه تعالی

جلسه‌ی ارائه‌ی هفتگی آزمایشگاه امنیت داده و شبکه

یک معماری امن پایگاه‌داده برای حفظ محرمانگی و صحت داده

هادی حلواچی

شنبه ۳۰ شهریور، ساعت ۹ صبح؛ دانشکده‌ی کامپیوتر، آزمایشگاه امنیت داده و شبکه

برون‌سپاری داده‌ها، افزون بر مزایای خود، چالش‌های امنیتی جدیدی را در راستای محرمانگی و صحت داده‌ها مطرح کرده است. اگرچه این چالش‌ها در مورد سناریوی برون‌سپاری مطرح می‌شوند اما نگرش مدیریت و نگه‌داری درون‌سازمانی نیز ــ شاید به گونه‌ای خفیف‌ترــ با این چالش‌ها روبروست. به هر حال، داده‌های ذخیره شده درون پایگاه‌داده، در معرض تهدیدات امنیتی قرار دارند؛ چرا که از طرفی سیستم‌های مورد استفاده، در برابر حملات مهاجمین آسیب‌پذیر بوده و از طرف دیگر، مدیران پایگاه‌داده ــ اگرچه قابل اعتماد ولیــ کنجکاو هستند.
نیازمندی‌های کلی یک پایگاه‌داده‌ی امن شامل محافظت از محرمانگی و صحت داده‌ها، حفظ حریم خصوصی کاربران، محرمانگی دسترسی به داده‌ها، اِعمال خط‌مشی‌های کنترل دسترسی و عدم افشای آن‌ها، پشتیبانی از اجرای انواع پرس‌وجوها و نوع داده‌های مختلف، و تحمیل سربار قابل قبول می‌شود. اگرچه روش‌های متفاوتی برای برطرف کردن هر کدام از نیازمندی‌های امنیتی پایگاه‌داده ارائه شده است، اما هنوز یک چارچوب عملیاتی امن که این نیازها را به صورت جامع در نظر گرفته و آن‌ها را با استفاده از روش‌های موجود برطرف نماید، ارائه نشده است.
در این ارائه، یک معماری برای مدیریت و نگه‌داری امن داده‌ها ارائه می‌کنیم که علاوه بر حفظ کارکردهای معمول سیستم‌های موجود، محرمانگی و صحت داده‌ها را حفظ، و اِعمال خط‌مشی‌های کنترل دسترسی را تضمین کند. معماری ارائه شده از دید کاربران و کارگزار پایگاه‌داده پنهان بوده و علاوه بر آن، انعطاف‌پذیری قابل توجهی را برای ایجاد مصالحه بین امنیت و کارایی، برای مالک داده فراهم می‌کند. در ادامه، یک روش اِعمال خط‌مشی‌های کنترل دسترسی در سناریوی برون‌سپاری ارائه می‌کنیم که می‌تواند خط‌مشی‌های ریزدانه‌ی کنترل دسترسی را که بر اساس محتوای داده‌ها بیان می‌شوند، در سمت کارگزار و بدون دخالت مالک داده به صورت برخط، اِعمال کند. روش ارائه شده از نشت غیرمجاز اطلاعات نیز جلوگیری می‌کند. سپس یک روش جدید برای ایجاد شاخص روی داده‌های رشته‌ای رمز شده ارائه می‌شود که با استفاده از احتمال رخداد کاراکترهای مختلف، شاخص‌های امن و با کارایی بالا ایجاد می‌کند. بهره‌برداری از اختلاف احتمال رخداد کاراکترهای مختلف درون رشته‌ها، توزیع شاخص‌های تولید شده را یکنواخت می‌کند که این ویژگی، علاوه بر کاهش امکان حملات استنتاجی، احتمال وقوع برخوردهای اشتباه را نیز تا حد مطلوبی کاهش می‌دهد.