15th International Conference on
Information Technology, Computer & Telecommunication

جستجوی مبتنی بر عبارات منظم در متن رمزشده

ریحانه حاج‌قاسم صابون‌پز
کارشناسی ارشد، مجتمع دانشگاهی فن‌آوری اطلاعات، ارتباطات و امنیت
پژوهشکده امنیت اطلاعات و ارتباطات، دانشگاه صنعتی مالک‌اشتر

رسول جلیلی
دانشیار، دانشگاه صنعتی شریف

چکیده
هزینه‌های زیرساختی مدیریت داده‌ها از یک سو و ظهور پدیده‌ی کلان‌داده از سوی دیگر، اشخاص و سازمان‌ها را به سمت برون‌سپاری داده سوق داده‌است. این رویکرد با چالش‌ها و مخاطرات امنیتی قابل توجهی مواجه است. یکی از مهمترین مخاطرات امنیتی در این رویکرد، عدم اطمینان به مدیریت سامانه ابری است؛ در این مقاله، فرض براین است که ارائه‌دهندگان خدمات ابری امین اما کنجکاو هستند؛ بنابراین به منظور اعمال تمهیدات امنیتی، باید داده‌ها در سمت کارسپار رمز شده و به سمت کارپذیر ارسال و ذخیره گردد، همچنین داده‌ها در مقابل حملات خارجی و نفوذهای داخلی محافظت خواهند شد هدف از این پژوهش، ارائه یک راهکار برای جستجوی عبارات منظم بر روی داده‌های رمزشده است (پیاده‌سازی عملگر LIKE رمزشده)، به گونه‌ای که عبارات منظم مورد درخواست کاربر به صورت رمزشده به سمت DBMS ارسال شده و روی داده‌های رمز شده اعمال می‌گردد، سپس وجود یا عدم وجود داده‌ها به کاربر مربوطه اطلاع داده می‌شود و در ضمن تلاش می‌شود ملاک‌های امنیتی و بهینگی در حد مطلوب برآورده شوند. منظور از ملاک‌های امنیتی، حفظ محرمانگی یا عدم نشت اطلاعات از داده‌های رمزشده و پرسمان کاربر می‌باشد و منظور از ملاک‌های بهینگی، وجود کم‌ترین سربارهای پردازشی و ذخیره‌سازی در سمت کاربر و عدم نیاز به تغییر زیرساخت کاربر و همچنین کاهش زمان پاسخ به پرسمان است. اگرچه در پژوهش‌های گذشته در این زمینه نیز فعالیت‌هایی صورت گرفته‌شده‌است، اما پیاده‌سازی آن‌ها در محیط واقعی چندان بهینه به نظر نمی‌رسد. در حالی که در ارزیابی‌های نمونه‌ی آزمایشگاهی این پایان‌نامه ملاحظه می‌شود، راهکار ارائه شده قابلیت استفاده در محیط واقعی را دارد.

واژگان کلیدی: برون‌سپاری داده، جستجوی عبارت منظم، امنیت، رمزنگاری