

جستجو در متن رمز شده

www.ketab.ir

مؤلف: ریحانه حاج قاسم صابون پر

حریم دانش

سرشناسه	: حاج قاسم صابون‌پز، ریحانه، ۱۳۶۷ -
عنوان و نام پدیدآور	: جستجو در متن رمز شده/مؤلف: ریحانه حاج قاسم صابون‌پز
مشخصات نشر	: تهران: حریم دانش، ۱۴۰۱.
مشخصات ظاهری	: ۱۱۳ص: مصور، جدول، نمودار.
شابک	: ۹۷۸-۶۲۲-۷۸۹۰-۱۸-۱
وضعیت فهرست نویسی: فیبا	
یادداشت	: کتابنامه: ص ۱۱۱-۱۱۳
موضوع	: داده کاوی -- رمزگذاری داده‌ها -- پایگاه‌های اطلاعاتی -- جستجو
موضوع	: Database searching -- Data encryption (Computer science) -- Data mining
رده‌بندی کنگره	: QA۷۶/۹
رده‌بندی دیویی	: ۰۰۶/۳۱۲
شماره کتابشناسی ملی	: ۸۴۶۵۴۲

www.ketab.ir

عنوان کتاب: جستجو در متن رمز شده
 مؤلف: ریحانه حاج قاسم صابون‌پز
 ویراستار: مهین بیات هاشمی
 ناشر: حریم دانش
 نوبت چاپ: چاپ اول ۱۴۰۱
 قیمت: ۸۰۰,۰۰۰ ریال
 تیراژ: ۱۰۰۰ جلد
 شابک: ۹۷۸-۶۲۲-۷۸۹۰-۱۸-۱

کلیه حقوق چاپ و نشر برای انتشارات حریم دانش و مؤلف محفوظ می‌باشد.

فروشگاه شماره ۱: میدان انقلاب، جنب بانک صادرات، پلاک ۱۳۵۷، کتاب فروشی محسن تلفن: ۶۶۴۹۲۶۶۲

فروشگاه شماره ۲: میدان انقلاب، روبروی سینما بهمن، پلاک ۱۳۷۰ کتاب فروشی بهنام تلفن: ۶۶۴۱۶۴۲۵

وب سایت: www.HarimeDanesh.com اینستاگرام: h.a.r.i.m.d.a.n.e.s.h

فهرست مطالب

پیشگفتار	۹
فصل اول: مقدمه	۱۱
فصل دوم: پژوهش‌های پیشین	۱۷
طبقه‌بندی پژوهش‌های پیشین	۱۹
۱. جستجو براساس وجود یا عدم وجود فراداده‌ها	۱۹
۲. جستجو براساس توانایی پاسخ به انواع پرسمان‌ها	۲۰
جستجو بر اساس وجود یا عدم وجود فراداده‌ها	۲۰
جستجو براساس توانایی پاسخ به انواع پرسمان‌ها	۲۳
توصیف و تحلیل پژوهش‌ها	۲۷
روش سانگ	۲۷
رمزنگاری با کلید عمومی، با قابلیت جستجوی کلمات کلیدی	۳۱
رمزنگاری متقارن قابل جستجو	۳۳
رمزنگاری تطبیق الگو	۳۵
جستجوی شباهت کارا بر روی داده‌ی رمز شده	۳۵
جستجوی عبارات منظم بر روی داده‌ی رمز شده	۳۶
جستجوی تطبیق الگوی رشته‌ای تعمیم یافته بر روی داده‌ی رمز شده در سیستم‌های ابری	۴۰
فصل سوم: راه‌کار پیشنهادی	۴۷
معماری راه‌کار پیشنهادی	۵۰
تبیین راه‌کار پیشنهادی	۵۲
نقطه ضعف راه‌کار پیشنهادی و ایده‌ای برای برطرف نمودن آن	۷۸

پیشگفتار

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 کتاب، 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 کارپدیس ارسال و ذخیره گردد، به این ترتیب کارپذیر از محتوی داده چیزی برداشت نمی‌کند، همچنین داده‌ها در مقابل حملات خارجی و نفوذهای داخلی محافظت خواهند شد. اگرچه معایبی مانند کاهش توانایی اجرای پرسمان‌ها، عملگرها و توابع رایج پایگاه‌داده، بر روی داده‌های رمز شده را به همراه خواهد داشت. منظور از پرسمان‌های رایج، دستورات موجود در سیستم‌های مدیریت پایگاه داده‌ها (مانند SQL) است که می‌توان از UPDATE, DELETE, INSERT, SELECT, AND, UNION, LIKE و OR اشاره نمود و از توابع نیز می‌توان SUM(), COUNT(), MAX() و MIN() را نام برد.

یکی از عبارات مورد استفاده در DBMS ها، عبارت WHERE است که قابلیت ایجاد فیلترگذاری بر روی خروجی بدست آمده از دستور SELECT را دارد و یکی از امکانات شرطی عبارت WHERE، عملگر LIKE است که عبارتی رشته‌ای را در قالب عبارات منظم، در خروجی بدست آمده جستجو می‌نماید. هدف از این کتاب، ارائه یک راه‌کار برای جستجوی

عبارات منظم بر روی داده‌های رمز شده است (پیاده‌سازی عملگر LIKE رمز شده)، به گونه‌ای که عبارات منظم مورد درخواست کاربر به صورت رمز شده 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 به عبارت بهتر، عدم نشت اطلاعات از داده‌های رمز شده و پرسمان کاربر می‌باشد که به منظور برآورده نمودن این خواسته، داده‌های رمز شده بین دو کاربری که هیچ اطلاعی از وجود یکدیگر ندارند توزیع گردید.

منظور از ملاک‌های بهینگی، وجود کم‌ترین سربارهای پردازشی و ذخیره‌سازی در سمت کاربر و عدم نیاز به تغییر زیرساخت کاربر می‌باشد که به منظور برآورده ساختن این خواسته، تمامی عملیات رمزنگاری و مدیریت عملیات به سامانه‌ی واسط محول گردید. از دیگر ملاک‌های بهینگی، کاهش زمان پاسخ به پرسمان است که از طریق بهینه‌سازی الگوریتم و بهره‌گیری از روشهای چندریشه‌ای برآورده گردید.

اگرچه در پژوهش‌های گذشته در این زمینه نیز فعالیت‌هایی صورت گرفته شده است، اما پیاده‌سازی آن‌ها در محیط واقعی چندان بهینه به نظر نمی‌رسد. در حالی که در ارزیابی‌های نمونه‌ای آزمایشگاهی این کتاب ملاحظه می‌شود، راه‌کار ارائه شده قابلیت استفاده در محیط واقعی را دارد.