عنوان مقاله:
رمزنگاری قابل جستجوی دارای دریچه یکبار مصرف با قابلیت جستجوی ترکیبی

محل انتشار:
دومین کنفرانس ملی محاسبات نرم (سال: 1396)

تعداد صفحات اصل مقاله: 10

نویسندگان:
آرین عرب نوری - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر،نرمافزار دانشگاه گیلان،گیلان،رشت،ایران*

رضا ابراهیمی آتانی - *دانشیار گروه مهندسی کامپیوتر دانشگاه گیلان،گیلان،رشت،ایران*

خلاصه مقاله:
امروزه فناوری ذخیرهسازی ابری بهعنوان راهکاری جهت مدیریت حجم بالایی از دادهها با هزینه پایین و دسترسی بالا)هر زمان و هر مکان(مطرح گردیده است. بااین وجود نگرانیهای فراوانی در حوزه حفظ حریم خصوصی در این فضا احساس میشود. جهت برآوردن نیاز به حفظ محرمانگی اطلاعات خصوصی افراد و سازمانها، از رمزنگاری استفاده میشود. علیرغم توانایی بالای تکنیکهای رمزنگاری اطلاعات در حفظ محرمانگی دادهها عملا امکان جستجو در رکوردهای رمزنگاری شده که یکی از نیازهای اساسی برای بازیابی اطلاعات است، پس از رمزنگاری کلاسیک غیر فعال میشود. جهت حل این مشکل و فعال نمودن امکان جستجو در دادههای رمزشده، ایده رمزنگاری قابل جستجو مطرح گردیده است. در این مقاله طرحی نوین برای جستجو در اطلاعات رمزشده پایگاه داده ارایه شده است. از ویژگیهای این طرح میتوان به قابلیت جستجوی عطفی، تامین امنیت دریچه در مقابل حملات حدس کلمات کلیدی با ارایه دریچههای یکبار مصرف، تامین محرمانگی سلسله مراتبی و تضمین صحت دادهها که یکی دیگر از نیازهای اساسی در فضای ابری است، اشاره نمود.

کلمات کلیدی:
رمزنگاری قابل جستجو، محرمانگی و صحت داده، زوجسازی دوسویه، حملات حدس کلمه کلیدی، دریچه