عنوان مقاله:
گمنام سازی جستجوی خصوصی در شبکه های کامپیوتری با استفاده از شبکه های مختلط

محل انتشار:
پنجمین کنفرانس بین المللی مهندسی برق و کامپیوتر با تاکید بر دانش بومی (سال: 1396)

تعداد صفحات اصل مقاله: 13

نویسندگان:
علیرضا افشاری - *گروه مهندسی کامپیوتر، واحد صفادشت، دانشگاه آزاد اسلامی، تهران، ایران*

علیرضا عموعابدینی - *گروه مهندسی کامپیوتر، واحد صفادشت، دانشگاه آزاد اسلامی، تهران، ایران*

احسان امینیان - *گروه مهندسی کامپیوتر، واحد صفادشت، دانشگاه آزاد اسلامی، تهران، ایران*

خلاصه مقاله:
با افزایش روز افزون مراکز داده و به علت پراکندگی در بین شبکه وسیع جهانی، جستجو را به یک امر ضروری تبدیل کرده است. توانایی به اشتراک گذاری اطلاعات حساس ذخیره شده در جوامع اطلاعاتی، بین طرفین غیر قابل اعتماد، یکی از مهمترین نگرانی های شبکه های کامپیوتری در دنیای امروزه است. به همین جهت جستجوی خصوصی به عنوان راه حلی برای این موضوع است که اجازه میدهد تا اطلاعات حساس بصورت رمزی بین کاربران مجاز با حفظ حریم خصوصی هر یک از کاربران جستجو شوند. تاکنون تکنیکهای متفاوتی برای جستجوی خصوصی ارایه شده است که از میزان حریم خصوصی متفاوتی برخوردار هستند. حریم خصوصی هر تکنیک براساس نیاز، اهداف و هزینه های آن طرح معین میشود. از طرفی ملاک مد نظر در این مقاله حداکثر حریم خصوصی است به این معنا که حریم خصوصی هر کاربر، حفاظت از محتوای پرسوجو، نتایج بدست آمده از آن و حفاظت از هویت کاربر در نظر گرفته میشود، به همین منظور در تکنیک های موجود با این میزان حریم خصوصی برای حفاظت از هویت کاربران از واسطی برای جستجو استفاده میکنند و آن واسط را صادق و امن تصور میکنند. در صورتی که اگر این واسط با هر یک از طرفین تبانی کند، منجر به نقض حریم خصوصی هر یک از کاربران میگردد (افشای هویت پرس وجوگر، افشای محتوای پرس وجو و نتایج مرتبط با آن و همچنین امنیت سایر اطلاعات). در این مقاله به ارایه راهکاری نوین از ترکیب سیستم های موجود برای گمنام سازی جستجوی خصوصی در شبکه های کامپیوتری با استفاده از شبکه مختلط به عنوان واسط ارتباطی بین کاربر و پایگاه داده میپردازیم. شبکه ت4 ر به عنوان واسط ارتباطی برای گمنام سازی جستجوی خصوصی ما مد نظر گرفته میشود به همین جهت روش ساخت یک کلیدواژه رمزی برای جستجوی خصوصی ما نیز تغییر میکند و ما در روش جستجوی خصوصی خود از ترکیب سیستم رمزنگاری RSA و AES بهره میبریم که منجر به حداکثر حفظ حریم خصوصی در جستجوی خصوصیمان میگردد. از این جهت مدل ما از لحاظ امنیتی، به علت استفاده از شبکه ت4ر و الگوریتم رمزنگاری RSA و AES، مدلی امن است و تاکنون هیچ یک از این رمزنگاری ها و شبکه ت4ر در جوامع اطلاعاتی شکسته نشده است.

کلمات کلیدی:
جستجوی رمز شده، گمنام سازی، شبکه های مختلط، حریم خصوصی کاربران، اطلاعات حساس