عنوان مقاله:
پیاده سازی موازی رمزنگاری هومومرفیک Somewhat با استفاده از تکنیک موازی سازی OpenMP جهت بالابردن امنیت در رایانش ابری

محل انتشار:
هفتمین کنفرانس بین المللی فناوری اطلاعات و دانش (سال: 1394)

تعداد صفحات اصل مقاله: 5

نویسندگان:
مارال مویدفرد - *دانشجوی کارشناسی ارشد نرم افزار، دانشگاه آزاد اسلامی واحد کرمان*

امیر صباغ ملاحسینی - *استادیار، دانشگاه آزاد اسلامی واحد کرمان*

خلاصه مقاله:
چشم انداز برون سپاری افزایش میزان ذخیره سازی داده ها و مدیریت در خدمات ابر، بسیاری از نگرانی های امنیتی و حریم خصوصی داده ها را برای افراد و شرکت های تجارتی افزایش می دهد. حال اگر کاربران داده ها را رمزنگاری کرده و سپس آن ها را به محیط ابر ارسال کنند، نگرانی های حریم خصوصی بطور رضایت بخشی برطرف خواهند شد. اگر طرح رمزنگاری هومومرفیک باشد، ابر می تواند بدون نیاز به رمزگشایی و بخطر انداختن حریم خصوصی، محاسبات با معنایی را روی داده ی رمزشده انجام دهد. در نتیجه بنابر افزایش نیاز روزافزون استفاده از رایانش ابری و عدم وجد امنیت در این محیط، رمزنگاری هومومرفیک و پیاده سازی آن از اهمیت ویژه ای برخوردار است. تاکنون استفاده از طرح رمزنگاری هومومرفیک بدلیل مدت زمان اجرای بالا و مشکل کمبود حافظه ممکن و عملی نبوده است و از طرفی طرح رمزنگاری هومومرفیک Somewhat بسیار سریع تر و فشرده تر از طرح رمزنگاری هومومرفیک کامل می باشد. در جهت کاهش مدت زمان اجرا، در این مقاله، اولین موازی سازی طرح رمزنگاری هومومرفیک Somewhat مبتنی بر اعداد صحیح توسط تکنیک موازی سازی OpenMP ارائه شده است. نتایج بدست آمده نشان دهنده ی بهبود سرعت 1/67،1/87 و 8/63 در الگوریتم های تولید کلید، رمزگذاری و ارزیابی اعمال توابع جمع و ضرب بر روی متن رمزشده، نسبت به پیاده سازی موازی بر روی پردازنده می باشد.

کلمات کلیدی:
طرح رمزنگاری هومومرفیک Somewhat، OpenMP، رایانش ابری، امنیت داده