عنوان مقاله:

تضمین امنیت محاسبات ابری با الگوریتم های رمز نگاری همریختی
Ensuring the security of cloud computing byHomomorphic encryption algorithms

محل انتشار:

اولین کنفرانس بین المللی دستاوردهای نوین پژوهشی در مهندسی برق و کامپیوتر (سال: 1395)

تعداد صفحات اصل مقاله: 25

نویسنده:

احسان فرزادنیا - *دانشجوی کارشناسی ارشد رایانش امن ، پژوهشکده امنیت اطلاعات ، مجتمع ICT دانشگاه صنعتی مالک اشتر تهران*

خلاصه مقاله:

با گسترش روز افزون کاربرد رایانه ها محققان همواره در تلاش برای یافتن راهی برای ارتقاء کیفیت و سرعت خدماتسیستم های نرم افزاری و ارائه الگویی تازه برای عرضه خدمات رایانشی به کاربران بوده اند . پردازش ابری این مسئله مهمو چالش انگیز را تا حدودی محقق ساخته اما هنوز چالش های اساسی در بعد امنیتی محاسباتی داده به قوت خودباقی است.بطوریکه چالش اصلی را می توان موازنه میان کارائی و امنیت دانست و در این کارزار مطمئناً به عملکرد و کارائی نبایدلطمه ای وارد شود . چراکه با رویکرد خصوصی سازی اقتصادی و آزادی اطلاعات ، کاربران در انتخاب سرویس مناسبدیگر نمی توانند مانند گذشته کاربردهای گوناگون را در قید و بند نظارت دولت ها یا غول های بزرگ نرم افزاری به انجامرسانند و این امر از سرویس های ابری نیز مستثنا نیست.به عبارت دیگر سرویس های ابری علیرغم برون سپاری پردازش ها ، نباید در حین اجرای عملیات محاسباتی به داده هایخصوصی کاربر به نحو آشکار، دسترسی داشته و حریم خصوصی را نقض کنند و تحقق این امر مرهون استفاده از تکنیک هاو روشهای قابل اثباتی چون «رمزنگاری همریختی» است. در این مقاله ابتدا ضمن معرفی معماری امن پردازش ابری و بیان مزیت ها، آسیب پذیری ها ، تهدیدات و چالش های اساسی در حفظ محرمانگی و حریم خصوصی این نوع پردازش ، بهارزیابی مهم ترین راهکارهای پژوهشی صورت گرفته در این زمینه در جهت رفع چالش ها پرداخته شده است. در ادامه باتعریف سیستم رمز نگاری همریختی و انواع آن ، برخی از ایده های مطرح در تضمین امنیت محاسبات مزایا و کاستی های آن با ترسیم مسیر پژوهشی آینده و مسائل باز در این حوزه طبقه بندی و ارزیابی شده است. در انتها نیز اهمیت وجود نوعی توازن منطقی میان دو مقوله مهم «مسیر تاریخی کشف اعداد اول بسیار بزرگ» و «توسعه تحقیقات در تضمین امنیت روشهای همریختی ضمن افزایش توان بالقوه رایانشی» با هدف ارائه دیدگاهی کلی از موضوع «امنیت محاسبات ابری آینده» نتیجه گیری و مورد تحلیل قرار گرفته است.

کلمات کلیدی:

تضمین امنیت محاسبات ، پتانسیل های رمزنگاری همریختی کامل DES, FHE ، رمزنگاری کلیدهمگانی RSA ، برون سپاری ، CSA ، سرورهای رمز نگاری ، حریم خصوصی ، محرمانگی ، مجازی سازی ، بوتاسترپ، اعداد اول