9th SASTech Symposium on Advances in Science & Technology (2014)
نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
بامحوریت
امنیت ملی و توسعه پایدار
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

الگوریتم جدیدی برای مدیریت کلید در محیط ابری

زهرا داردان، مصطفی حق جو سانیجی
دانشجوی کارشناسی ارشد دانشگاه پیام نور قشم
استاد یار مهندسی نرم لفزار دانشگاه پیام نور کیش
zahradardan@gmail.com
زهرا داردان

خلاصه

در این مقاله روش مدیریت کلید گروهی مبتنی بر چندجمله ای های ساده ارائه می گرددکه درآن اعمال سرویس های مدیریت کلید با کارآمدی بالا نسبت به روش های موجود انجام می گیرد. در سطح بین تهیه کننده ابر و مدیر پایگاه داده ابری از یک درخت کلید و در سطح بین کاربر و تهیه کننده ابر از یک درخت کلید دیگر استفاده می شود.به منظور کاهش بار محاسباتی و ارتباطی تهیه کننده ابر از کدگذاری گره‌های درخت کلید استفاده می شود.با اعمال این روش، بار محاسباتی به روز کردن کلیدها از تهیه کننده ابر به کاربران انتقال می یابد. ارزیابی الگوریتم رمز نگاری AES نشان می دهد که استفاده از این روش رمزنگاری هزینه های مربوط به مراکز داده را بالا می برد. همچنین میانگین زمان پاسخ توسط ماشین های مجازی در نظر گرفته شده در محیط ابری افزایش می یابد.در الگوریتم پیشنهادی هزینه محاسبات در تهیه کننده ابر در زمان وارد شدن کلید مرتبه o(5) و در زمان خروج log1+1 می باشد.

کلمات کلیدی:

محیط ابری،پایگاه داده ابری،پنهان سازی،مدیریت کلید

۱–مقدمه

سرویس پایگاه داده در ابر یکی از بخش‌های اساسی در تکنولوژی محاسبات ابری می باشد.مهاجرت پایگاه داده به محیط ابر مشکلات امنیتی برای سازمان‌ها به دنبال دارد و با توجه به باز بودن محیط ارتباطی، امنیت یکی از چالش های مهم در این محیط محسوب می شود. برای دستیابی به سرویس های امنیتی می توان از روش های رمز نگاری استفاده نمود.در روش های رمز نگاری از یک کلید محرمانه برای انجام عملیات استفاده می شود. از این رو در ارائه سرویس های محرمانگی در این محیط باید از یک سیستم مدیریت کلید بهره برد. (**۱۳۹۱،٤،فریده لطفی، تورج بنی رستم**). از وظایف یک سیستم مدیریت کلید