عنوان مقاله:
الگوریتم جدیدی برای مدیریت کلید در محیط ابری

محل انتشار:
همایش ملی علوم و مهندسی کامپیوتر با محوریت امنیت ملی و توسعه پایدار (سال: 1393)

تعداد صفحات اصل مقاله: 8

نویسندگان:
زهرا داردان - *دانجشوی کارشناسی ارشد دانشگاه پیام نور قشم*

مصطفی حق جو سانیجی - *استادیار مهندسی نرم افزار دانشگاه پیام نور کیش*

خلاصه مقاله:
در این مقاله روش مدیریت کلید گروهی مبتنی بر چند جمله ای های ساده ارائه می گردد که در آن اعتمال 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 گره های درخت کلید استفاده می شود. با اعمال این روش، بار محاسباتی به روز کردن کلی ها از تهیه کننده ابر به کاربران انتقال می یابد. ارزیابی الگوریتم رمزنگاری AES نشان می دهد که استفاده از این روش رمزنگاری هزینه های مربوط نه مراکز داده را بالا می برد. همچنین میانگین زمان پاسخ توسط ماشین های مجازی درنظر 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 log+1 می باشد.

کلمات کلیدی:
پایگاه داده ابری، پنهان سازی، مدیریت کلید