عنوان مقاله:
روشی جدید جهت اصلاح علامت گذاری در فضای رایانش ابری: روش Boneh-Lynn-Shacham

محل انتشار:
ششمین کنفرانس بین المللی پژوهش های کاربردی در علوم و مهندسی (سال: 1401)

تعداد صفحات اصل مقاله: 15

نویسندگان:
مهدی نژادفرحانی - *دانشجوی دکتری مهندسی کامپیوتر نرم افزار، دانشگاه آزاد اسلامی واحد قم، ایران*

حسین چاهخویی نژاد - *دانشجوی دکتری مهندسی کامپیوتر نرم افزار، دانشگاه آزاد اسلامی واحد قم، ایران*

شیوا روا - *دانشجوی مهندسی فن آوری اطلاعات و ارتباطات، دانشگاه عالیفرد ،هشتگرد، ایران*

آرش شیخی
محمد قلیزاده

خلاصه مقاله:
رایانش ابری جایگزینی برای برون سپاری متداول فناوری اطلاعات است. به عنوان یک نتیجه، مهاجرت به رایانش ابری در بین سازمان به سرعت در حال گسترش است. پذیرش این فناوری جنبه های مثبت بسیاری را به ارمغان می آورد اما خطرات و نگرانی های مختلفی را نیز ایجاد می نماید. سازمانی که به طور رسمی سرویس های ابری خود را در معرض ارئه دهندگان خارجی قرار می دهد، استدلال می کند که کارکردها و فرآیندهای فناوری اطلاعات خود را به ارائه دهندگان شخص ثالث سرویس های BPO برون سپاری کرده است. برای فرآیندهای بازرسی عمومی ایجاد کننده حریم خصوصی در ذخیره سازی دینامیکی داده های ابری، الگوریتم بازرسی اصلاح شده و پویای (MBLDSA Boneh-Lynn-Shachame) در این مقاله پیشنهاد داده شده است. الگوریتم پیشنهادی یک فرآیند بازرسی را برای چندین کاربر مبتنی بر نظارت شاخه ای به طور همزمان و موثر اجرا می کند تا بازرسی شخص ثالث (TPA) را امکان پذیر سازد. این مقاله احراز هویت همگن را در الگوریتم بازرسی دینامیکی ورود با علامت گذاری تصادفی برحسب فرآیند بازرسی عمومی با حفظ حریم خصوصی ادغام می کند. هنگامی که کاربر فضای ابری داده ها را ذخیره یا آپدیت می کند، آن ها را با استفاده از الگوریتم Rijndal رمزنگاری کرده و تولید امضاء Boneh-Lynn-Shacham برای تولید کلید مورد استفاده قرار می گیرد. در نهایت ترکیبی از نظارت دینامیکی و اصلاح شده ورود به نام Boneh-Lynn-Shacham داده ها را به منظور فراهم کردن امنیت مورد بازرسی قرار می دهد.

کلمات کلیدی:
رایانش ابری، بازرسی، امنیت، چند اجرایی و امنیت ابر

لینک ثابت مقاله در پایگاه سیویلیکا: