

عنوان مقاله:

امنیت مجازی سازی در محیط رایانش ابری مبتنی بر فناوری مجازی

محل انتشار:

کنفرانس بین المللی تحقیقات بین رشته ای در مهندسی برق، کامپیوتر، مکانیک و مکترونیک در ایران و جهان اسلام (سال: 1397)

تعداد صفحات اصل مقاله: 13

نویسندگان:

سیما احمدلو - مقطع کارشناسی ارشد، دانشگاه آزاد اسلامی واحد یادگار امام (ره)، تهران،

سارا نجف زاده

خلاصه مقاله:

در این تحقیق هدف بررسی راه کارهایی برای مقاوم سازی مجازی سازی در برابر مشکلات امنیتی با بررسی تهدیدها و ریسک های محیط های رایانش ابری است. مسایلی مانند زیر ساخت به عنوان یک سرویس laas پلتفرم به عنوان یک سرویس paas و نرم افزار به عنوان یک سرویس saas، محیط ابر را آسیب پذیر کرده اند. مهم ترین و بنیادی ترین نکته ی تکنولوژی ابر، مجازی سازی است. فناوری مجازی سازی امنیت ابر را به یک مبحث پیچیده تبدیل کرده است و آسیب ها و تهدیدهای جدید بسیاری در حال شکل گیری هستند. مجازی سازی به سیستم عامل های چندگانه این امکان را می دهد که بر روی یک ماشین فیزیکی بدون تداخل با یکدیگر قرار گیرند و از تخصیص منابع پویا بر روی یک سخت افزار بهره گیرند. از آنجایی که ماشین های مجازی متعددی بر روی یک سرور راه اندازی می شوند، عامل مخرب فرصتی برای حمله به لایه ی مجازی سازی، استفاده از حفره های امنیتی و دسترسی به تمام ماشین های مجازی پیدا می کند. علاوه بر این، یک ماشین مجازی به خطر افتاده می تواند برای ماشین های مجازی دیگر در یک سرور فیزیکی مشکل امنیتی ایجاد کند. اگر یک هکر زمانی را صرف حمله به یکی از ماشین های مجازی کند می تواند سایر ماشین های مجازی را نیز تهدید و در نهایت به میزبان دست یابد. در این پژوهش برای شبیه سازی از نرم افزار شبیه ساز Opnet مدل 17.5 استفاده شده است. در ابتدا یک سناریو از معماری ابر را مورد بررسی قرار می گیرد که 3 نوع حمله 1. MI 3. DDos 2. dos بر روی آن اعمال می گردد. سپس راهکارهای پیشنهادی خود را بر روی ساختار طراحی شده اعمال کرده و مجدداً این ساختار با 3 نوع تهدید بیان شده مورد حمله قرار داده می شود. در این پژوهش نشان داده شده که با برطرف سازی بعضی از مشکلات وجود در ابر می توان با تکنیک مجازی سازی امنیت بهتری را برای داده به ارمغان آورد.

کلمات کلیدی:

رایانس ابری، مجازی سازی، ماشین مجازی، امنیت، فناوری مجازی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/805304>

