

بررسی و مقایسه‌ی معماری‌های امنیتی رایانش ابری در راستای ارائه راهکارهایی جهت توسعه سازمان‌های امنیتی

زهرا سلیمی^{۱*}

۱- استاد حق‌التدریسی دانشگاه پیام نور واحد کرمانشاه

چکیده

رایانش ابری یک مقوله مهم در عصر نوین فناوری اطلاعات بدل شده است. از این رو جدیدترین تحقیقات در این حوزه پیرامون فناوری ابری صورت می‌گیرد. به همین دلیل شناخت چالش‌های پیرامون رایانش ابری از اهمیت بالایی برخوردار است. مفاهیم تعامل‌پذیری، امنیت، استانداردسازی و معماری‌های امنیتی مهم‌ترین چالش‌های فضای ابری هستند. از این رو، این مقاله با هدف بررسی معماری امنیتی رایانش ابری در سازمان‌های امنیتی سعی در توسعه مفاهیم امنیتی رایانش ابری دارد. به همین دلیل در ابتدا معماری‌های مختلف رایانش ابری تعریف و بررسی شده است. سپس با بررسی نقاط ضعف و قوت معماری‌های پیشنهادی، با ارائه راهکارهایی به توسعه سازمان‌های امنیتی در راستای بهبود معماری امنیتی رایانش ابری پرداخته شده است.

کلمات کلیدی: رایانش ابری، معماری امنیتی، سازمان‌های امنیتی، معماری رایانش ابری

۱. مقدمه

اگرچه ظهور رایانش ابری یک پیشرفت متأخر بشمار می‌آید، درک جنبه‌های حساس امنیتی می‌تواند از تجارب گزارش‌شده سازگارترهای اولیه و همچنین از محققین که سکوها را ایجادگر ابری موجود و فناوری‌های دست‌اندرکار را تحلیل و آزمایش می‌کنند، جمع‌آوری شود. بخش‌های ذیل مسئله مربوط به امنیت و حریم خصوصی را مشخص می‌کند که پنداشته می‌شود اهمیت بلندمدتی به رایانش ابری عمومی و در بسیاری از موارد به سایر مدل‌های سرویس رایانش ابری می‌دهند. در برخی از موارد این احتمال می‌رود که نمونه‌های مشکلات تعریف‌شده یا مشخص‌شده پیشین برای طرح مسئله‌ای ارائه نمودند. نمونه‌ها جامع نیستند و ممکن است که یک جنبه از یک موضوع کلی‌تر را پوشش دهند. در مسائل بسیاری، مشکلات خاص مطرح‌شده دوباره طرح و حل گشته‌اند. با این وجود مسئله وسیع‌تر در اکثر موارد از خود سماجت و مقاومت نشان می‌دهد و دارای پتانسیلی است که از راه‌های دیگری دوباره خود را در میان مدل‌های سرویس مختلف بروز دهد.

* Corresponding author: فارغ‌التحصیل کارشناسی ارشد مهندسی نرم‌افزار از دانشگاه گیلان

Email: zsalimi1360@yahoo.com