فصلنامه رویکردهای پژوهشی نوین در
مدیریت و حسابداری
سال هفتم، شماره ۸۹، تابستان ۱۴۰۲، ص ۶۰-۴۰

Journal of New Research Approaches
in Management and Accounting
ISSN: 2588-4573
http://www.majournal.ir

# ارائه و تحلیل کنترل امنیت در رایانش ابری با رویکرد افزایش پایداری مناسب در ذخیره سازی داده ها

**علی اکبر احمدی** [۱]
**میلاد حبیب نژاد** [۲]

تاریخ دریافت: ۱۴۰۲/۰۲/۱۷ تاریخ چاپ: ۱۴۰۲/۰۴/۱۰

## چکیده

هدف اصلی این تحقیق ارائه و تحلیل کنترل امنیت در رایانش ابری با رویکرد افزایش پایداری مناسب در ذخیره سازی داده ها است. فناوری اطلاعات و ارتباطات دارای تأثیر مستقیم در همه بخش‌های یک سازمان است. رایانش ابری به عنوان یک فناوری نوظهور توانسته با به اشتراک گذاری منابع و برنامه‌های کاربردی میان کاربران، محیط انعطاف‌پذیر و قدرتمندی را در سازمانها ایجاد نماید. رایانش ابری به مجموعه‌ای از سرورها اطلاق می‌گردد که می‌توانند از راه دور و از طریق اینترنت در زمان مناسب قابل‌دسترسی باشند. این فناوری بسیار کارآمد، محلی برای ایجاد، ذخیره‌سازی و دسترسی به اطلاعات شخصی کاربران است با افزایش استفاده از رایانش ابری، مسائل امنیتی در مقیاس رو به رشد نمایان می‌شوند. مهم این است که این مسائل امنیتی برای کمک به کاربردهای وسیع تر رایانش ابری حل شود افزایش تعداد حوادث مربوط به امنیت در ابرها، سازمان‌ها را ملزم می‌سازد تا به راهکارهای بهبود و ارتقای ابرهای مورداستفاده خود بپردازند و از اطلاعات حساس خود به‌طور فعال محافظت کنند. رایانش ابری پتانسیل قابل توجه و چشمگیری در ارائه منابع در جریان قدرتمند، مقرون به صرفه، منعطف و با قابلیت مدیریت آسان در اینترنت دارد. رایانش ابری به واسطه استفاده بهینه و مشترک قابلیت های منابع سخت افزاری را به میزان زیادی افزایش می دهد. ویژگی های مزبور سازمان ها و کاربران فردی را ترغیب نموده تا اپلیکیشن ها و سرویس های شان را به محیط ابری منتقل کنند. با توجه به رشد روز افزون تکنولوژی‌ها و تنوع نیاز کاربران در حوزه فناوری اطلاعات، جایگاه رایانش ابری نمود بیشتری پیدا می کند. چرا که گسترش زیر ساخت محاسباتی در هر سازمان نیازمند صرف هزینه و زمان و نیروی انسانی بسیاری است که گاهی در توان عملیاتی یک سازمان نمی‌گنجد. از این رو سازمان‌ها برای پیشبرد اهداف خود تمایل به استفاده از چنین تکنولوژی‌هایی دارند. در اصل پایگاه داده‌ها و برنامه‌های نرم‌افزاری به سمت مراکز داده بزرگ ابر حرکت داده می‌شوند که مدیریت داده و سرویس های آن به‌طور کامل قابل اعتماد نیست. به همین دلیل شرکت‌ها با وجود اینکه محاسبات ابری امکانات وسیعی در اختیار آن‌ها قرار می‌دهد، تمایلی به گسترش تجارت خود در ابر ندارند. امنیت داده در ابر یکی از موضوعات مهمی می‌باشد که اثرات آن مانع از به کار گرفته شدن محاسبات ابری می‌شود؛ اما علی رغم امکانات خوبی که رایانش ابری در اختیار کاربر می گذارد مسائل امنیتی است که در ابعاد مختلف آن را تحت تأثیر قرار می دهد که این تهدیدات شامل موارد مختلف از جمله حمله ی هکرها، آسیب پذیری ها، از دست دادن داده ها، حریم خصوصی و خیلی موارد دیگر است که از جمله موانع رشد و گسترش آن است. در واقع یکی از چالش های این فناوری نو ظهور امنیت آن است که در این تحقیق به این چالش پرداخته می شود.

## واژگان کلیدی

رایانش ابری، امنیت فناوری اطلاعات و ارتباطات، حریم خصوصی مراکز داده، تهدیدات امنیتی

۱ - هیئت علمی دانشگاه پیام نور، گروه مدیریت دولتی. aliakbarahmadi@pnu.ac.ir
۲ - دانشجوی کارشناسی ارشد پیام نور (تهران واحد غرب)، گروه مدیریت فناوری اطلاعات.

**مقدمه**

با پیشرفت فناوری اطلاعات و تغییر شیوه زندگی مردم نیازهای جدیدی از قبیل دسترسی آنی به اطلاعات، پردازش سریع، امنیت و کاهش هزینه ها برای کاربران به وجود آمده است؛ که فناوری رایانش ابری پاسخ خوبی برای نیازهای متعدد کاربران می باشد. رایانش ابری تکنولوژی جدیدی است که دسترسی کاربران را برای دریافت منابعی همچون منابع محاسباتی، شبکه ها، محیط ذخیره سازی، سرورها، سرویسها و کاربردها، بدون دستیابی فیزیکی کاربران به آنها و بدون پرداخت هزینه گزاف، فراهم می کند. در مقایسه با مدل رایانش قدیمی که در آن داده های کاربر نهایی و قدرت محاسباتی در رایانه کاربر واقع شده اند، منابع مدل رایانش ابری به صورت زیرساخت های مجازی تجمیع شده است که توسط ارائه دهندگان خدمات، مدیریت می شود. (تاکایی[3]،۲۰۱۲)

به طور کلی امنیت در مراکز داده به مجموعه ای از راه حل های فنی برای مشکلات غیرفنی گویند. زمان، پول و تلاش زیادی را می توان برای ایمن کردن سیستم ها صرف کرد؛ اما هرگز نمی توان نگران پاک شدن تصادفی داده ها یا تخریب عمدی اطلاعات نبود. با در نظر گرفتن مجموعه شرایط: اشکالات نرم افزاری، حوادث، اشتباهات، بداقبالی، آب و هوای بد یا یک مهاجم مجهز و با انگیزه، مشاهده می شود که هر مرکز داده ای ممکن است مورد حمله قرار بگیرد، برای مدتی از کار بیافتد، یا حتی کاملاً غیرفعال شود. در این تحقیق برای بالا بردن امنیت در مراکز داده و ایجاد یک مدیریت متمرکز بر روی کنترل دسترسی های تعریف شده در آن و با توجه به ماهیت مراکز داده که محلی امن جهت ذخیره سازی اطلاعات می باشد، ابتدا نیازهای امنیتی یک مرکز داده بیان می شود. از دیدگاه تشکیل دهنده سیستم های رایانش ابری به دو قسمت می شود که از دو قسمت فرانت اند و بک انـد تشکیل شده است: قسمت اول شامل کاربران و مشتریانی است که از خدمات آن بهره می برند که شامل سیستم هـاو تجهیزات مانند تبلت، موبایل و غیره است و برنامه های کاربردی مثل مرورگر وب کاربران که به وسیله دستگاه هـا از این خدمات بهره می برند. (رزمجو، ۱۳۸۶).

قسمت بعدی شامل خود ابر است که شامل کامپیوترهـا، سـرورها و سیسـتم هـای ذخیـره سازی است که با هماهنگی و کارکرد موازی همدیگر به مشتریان خدمات می دهند. تمـام سـرور هـا سیسـتم عامـل مستقل خود را دارند و مستقل از دیگر سیستم ها کار می کنند. محاسبات ابری مـی توانـد فنـاوری مجـازی سـازی جهت پیاده سازی ابر استفاده نماید که در مجموعه ای از سیستم های مجازی سازی شده است. مجازی سازی‌فناوری است که می تواند بر روی یک کامپیوتر معمولی و یا سرور پیاده سازی شود و این امکان را می دهد که چندین سیستم عامل به طور همزمان بر روی آن ها نصب گردد و همچنین به طور همزمان اجرا می گردنـد. سـروری مرکـزی بـر روی ترافیک و درخواست های کاربران جهت اطمینان از اجرای روان پردازش ها نظارت می کند که به وسیله ی یک سـری پروتکل ها و نرم افزار خاصی به نام میان افزار انجام می شود. میان افزار به سیستم های شبکه شـده اجـازه ارتبـاط بـه یکدیگر را می دهد. رایانش ابری توسط میان افزار تمام پردازش ها را طوری اجرا می کند که به نظر می رسد در یـک کامپیوتر معمولی اجرا می شوند. انواع رایانش ابری از لحاظ مدل استقرار ابری که خدمت رسانی می کنند به سه دسته تقسیم می شوند که شامل ابرهای عمومی، ابرهای خصوصی و ابرهای هیبریدی تقسیم می شوند. در ابرهـای عمـومی سرویس های ابری از طریق بستر اینترنت در دسترس هستند و کاربران از این طریق بـه راحتـی بـه آن هـا دسترسـی دارند؛ اما با این وجود از امنیت کمتر برخوردارند و هم چنین آسیب پذیرتر از ابرهای خصوصی هستند چون دسترسـی به آن ها سهل تر است و شبکه ی اینترنت شامل

3- Takai,M.

دستگاه های بی شماری است و شبکه های ابری عمومی می توانند به راحتی مورد حمله و سوء استفاده قرار گیرند زیرا همان طور که کاربران به راحتی به آن ها دسترسی دارند مـی تواننـد هدف در دسترسی برای افراد مهاجم باشد. ابرهای عمومی انواع مختلفی از سرویس ها را به کاربران ارائه می دهنـد. در ابرهای خصوصی سرویس ها و ساختارها در داخل شبکه خصوصی و داخلی نگهداری می شـوند کـه در نتیجـه امنیـت بالاتری نسبت به ابرهای عمومی دارند و کنترل بر روی آن ها راحت تر است. امـا آن شـرکت یـا سـازمان بایـد هزینـه خریداری و نگهداری نرم افزارها و سخت افزارهای مورد نیاز رایانش ابری را تقبل کنـد. ابرهـای هیبریـدی هـم شـامل ابرهای عمومی و هم شامل ابرهای خصوصی است که توسط چندین سرویس دهنده بـه کـاربران خـدمات رسـانی مـی کند، در حقیقت ابر هیبریدی، ابر خصوصی است که توسط لینک هایی به دیگر ابرها متصل است. (ادل[2] وانگر[3] و ویر[4] ۲۰۱۵).

## روش تحقیق

### اثر بخشی رایانش ابری بر پیشرفت فناوری اطلاعات:

دنیای فناوری اطلاعات و اینترنت که امروزه تبدیل به جزئی حیاتی از زندگی بشر شده، روز به روز در حال گسترش است. همسو با آن، نیازهای اعضای جوامع مانند امنیت اطلاعات، پردازش سریع، دسترسی پویا و آنی، قدرت تمرکز روی پروژه‌های سازمانی به جای اتلاف وقت برای نگهداری سرورها و از همه مهم‌تر، صرفه‌جویی در هزینه‌ها اهمیت زیادی یافته است. راه حلی که امروزه در عرصه فناوری برای چنین مشکلاتی پیشنهاد می‌شود فناوری است که این روزها با نام رایانش ابری (محاسبات ابری، پردازش ابری) پرداخته می‌شود. رایانش ابری مدلی است برای داشتن دسترسی فراگیر، آسان و بنا به سفارش شبکه به مجموعه‌ای از منابع پردازشی پیکربندی‌پذیر (مثل: شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) که بتوانند با کمترین کار و زحمت یا نیاز به دخالت فراهم‌کننده سرویس به سرعت فراهم شده یا آزاد (رها) گردند.

به طور خلاصه به وسیله‌ی رایانش ابری شرکت‌ها، کاربران سرویس‌های فناوری اطلاعات، می‌توانند سرویس‌های مرتبط با فناوری اطلاعات خود به عنوان سرویس بخرند؛ به جای خرید سرورها برای سرویس‌های درونی یا برونی، یا خرید مجوز نرم‌افزارها شرکت‌ها می‌توانند آن‌ها را به عنوان سرویس بخرند. رایانش ابری راهی برای افزایش ظرفیت ذخیره‌سازی یا امکانات، بدون هزینه کردن برای زیرساخت جدید، آموزش پرسنل جدید، یا خرید مجوز نرم‌افزار جدید می‌باشد؛ در واقع شرکت‌ها یا افراد تنها برای آنچه مصرف می‌کنند پول خواهند داد. بنابراین راهی موثر برای استفاده از منابع، مدیریت سرمایه و هزینه‌های پشتیبانی فناوری است.

ساختار کاملاً باز و توزیع شده در رایانش ابری و سرویس‌های آن موجب می‌شود تا هدفی جذاب برای مهاجمان باشد. این ساختار شامل پارادایم‌های سرویس‌گرا و توزیع شده mesh چندگانه، اجاره چندگانه، دامنه‌های چندگانه و ساختارهای مدیریتی خودمختار چند کاربره می‌باشد که مستعد تهدیدات امنیتی و آسیب‌پذیری بیشتری هستند. معماری سرویس در رایانش ابری از ترکیب سه لایه وابسته به هم به نام‌های زیرساخت، سکو یا بستر و برنامه تشکیل شده است که با خطاهای پیکربندی متفاوتی که توسط کاربر یا فراهم کننده سرویس ایجاد می‌شود، معرفی می‌گردد. یک سیستم رایانش ابری می‌تواند با چندین تهدید متفاوت رو به رو شود که شامل تهدیدات یکپارچگی (صحت)، محرمانگی و

4 – Odell,L.A.
5- Wagner,R.
6-Weir,T.J.

دسترس‌پذیری منابع، داده و زیرساخت‌های مجازی سازی شده که به عنوان بستری برای حملات جدید می‌باشد. یکی از روش‌های شناسایی حملات استفاده از سیستم‌های تشخیص نفوذ می‌باشد و هدف از این تحقیق بررسی راهکارهای مختلف ارائه شده در مورد کنترل امنیت رایانش ابری در ذخیره سازی داده ها میباشد. امتیازات بارز ابرها توجه بسیاری از سازمانها را به خود جلب کرده است، اما جنبه‌ای که هنوز باعث عقب نشینی بسیاری از سازمانها در برابر این فناوری می‌گردد، نحوه امن سازی داده‌ها در ابر و اطمینان از امنیت محیط است.

## تعاریف متغیرها

### رایانش ابری چیست؟

رایانش ابری یا cloud computing، یکی از روش‌های ارائه سرویس‌های محاسباتی است که شامل سرورها، فضای ذخیره‌سازی، پایگاه‌های اطلاعاتی، شبکه‌ها، نرم‌افزارها، تجزیه‌وتحلیل‌ها و اطلاعات ازطریق اینترنت می‌شود و به کاربران اجازه می‌دهد تا به سادگی و با کمترین هزینه، به منابع محاسباتی مورد نیاز خود دسترسی پیدا کنند و نیاز به تهیه و نگهداری سخت‌افزار و نرم‌افزار خود را نداشته باشند.

درحقیقت، ذخیره‌سازی مبتنی بر ابر به جای ذخیره و نگه‌داری فایل‌ها روی هارد دیسک اختصاصی یا دستگاه ذخیره‌سازی لوکال، امکان ذخیره‌سازی آن‌ها را در پایگاه داده از راه دور فراهم می‌کند. با استفاده از رایانش ابری، می‌توانید در زمان و مکان دلخواه فقط با استفاده از اتصال به اینترنت به داده‌ها و برنامه‌ها نرم‌افزاری دسترسی داشته باشید. (Zhou et al,2010)

دلیل نام‌گذاری رایانش ابری این است که دسترسی به اطلاعات را ازطریق فضای ابری یا فضای مجازی امکان‌پذیر می‌کند. شرکت‌هایی که سرویس‌های ابری ارائه می‌کنند، به کاربران امکان می‌دهند تا فایل‌ها و برنامه‌های کاربردی خود را روی سرورهای راه دور ذخیره کنند و سپس با استفاده از اینترنت در زمان و مکان مدنظرشان به اطلاعاتشان دسترسی داشته باشند. این یعنی کاربر به حضور در مکانی خاص برای دسترسی نیازی ندارد و از راه دور می‌تواند داده‌های ذخیره‌شده‌اش را به‌راحتی کنترل و مدیریت کند. رایانش ابری تمام کارهای سنگین مربوط به پردازش داده‌ها را انجام می‌دهد و تمام این کارها را به کامپیوترهای بسیار دور در فضای مجازی منتقل می‌کند؛ درنتیجه، اینترنت به فضایی ابری تبدیل می‌شود و شما می‌توانید در هر نقطه‌ای از جهان با هر دستگاهی، به داده‌ها و فایل‌هایتان دسترسی داشته باشید. (Wu et al,2014)

### نکات مهم درباره رایانش ابری:

- رایانش ابری سرویس‌های مختلفی را ازطریق اینترنت ارائه می‌دهد؛ ازجمله ذخیره‌سازی داده‌ها، سرورها، پایگاه‌های داده، شبکه و نرم‌افزارهای کاربردی.
- ذخیره‌سازی مبتنی‌بر ابر امکان ذخیره فایل‌ها را در پایگاه‌داده راه دور و بازیابی آن‌ها را فراهم می‌کند.
- سرویس‌های رایانش ابری هم عمومی و هم خصوصی هستند. خدمات عمومی به‌صورت آنلاین همراه با هزینه ارائه می‌شوند؛ اما خدمات خصوصی در شبکه برای مشتریان خاصی میزبانی می‌شوند.

### رایانش ابری شامل سه بخش اساسی است:

- شرکت‌های ارائه‌دهنده سرویس‌های ابری داده‌ها و برنامه‌های کاربردی را در ماشین‌های فیزیکی ذخیره می‌کنند؛ یعنی مکان‌هایی که به‌عنوان مراکز داده شناخته می‌شوند.

- کاربران به این داده‌ها و برنامه‌های کاربردی دسترسی دارند.
- اینترنت شرکت‌های ارائه‌دهندگان و کاربران را به‌سرعت حتی در فواصل طولانی به‌هم متصل می‌کند.

این بخش‌ها ساده هستند؛ اما فناوری‌ای که آن‌ها را درکنارهم قرار می‌دهد، پیچیده است.

رایانش ابری به‌طرز چشمگیری رویکرد کسب‌وکارها به منابع IT را تغییر می‌دهد و ساده می‌کند. به‌عنوان مثال، بسیاری از ارائه‌دهندگان فضای ابر خدمات مبتنی بر اشتراک را ارائه می‌دهند و مشتریان در ازای پرداخت هزینه ماهانه، می‌توانند به تمام منابع محاسباتی موردنیاز خود دسترسی داشته باشند. این یعنی آنان مجبور نیستند مجوزهای نرم‌افزاری را تهیه کنند، سرورهای قدیمی را ارتقا دهند، ماشین‌های بیشتری را درصورت تمام‌شدن فضای ذخیره‌سازی بخرند یا به‌روزرسانی‌های نرم‌افزاری را نصب کنند تا همگام با تهدیدات امنیتی در حال تکامل و ارتقا باشند. (ولوی و موحدی، ۱۳۹۹)

بدین‌ترتیب، رایانش ابری مانند اجاره ماشین است. کاربر می‌تواند از وسیله نقلیه استفاده کند؛ اما انجام تعمیرات، جایگزینی خودروهای جدید با خودروهای قدیمی و... برعهده مالک خودروست. اگر کاربر به ماشینی با امکانات بیشتری نیاز داشت، کافی است قراردادی جدید را امضا کند و کلیدها را تحویل بگیرد.

## مدل‌های مختلف رایانش ابری:

ابرها انواع مختلفی دارند که هرکدام با دیگری متفاوت‌اند. درمجموع، رایانش ابری به سه دسته «عمومی» و «خصوصی» و «ترکیبی» و «چند ابری» تقسیم می‌شود که درادامه، هرکدام از آن‌ها را بررسی می‌کنیم.

### ۱. ابر عمومی

ابرهای عمومی سرویس‌های خود را روی سرورها و فضای ذخیره‌سازی در اینترنت ارائه می‌دهند. این ابرها را شرکت‌های شخص ثالثی اداره می‌کنند که وظیفه مدیریت و کنترل تمام سخت‌افزار و نرم‌افزار و زیرساخت‌های کلی را برعهده دارند. کاربران با استفاده از حساب‌هایی که تقریباً برای هرکسی دردسترس است، می‌توانند به این سرویس‌ها دسترسی پیدا کنند.

### ۲. ابرهای خصوصی

ابرهای خصوصی برای مشتریان خاص (معمولاً کسب‌وکارها یا سازمان‌ها) تهیه می‌شوند. مرکز خدمات داده شرکت ممکن است هاست سرویس رایانش ابری باشد. بسیاری از خدمات رایانش ابری خصوصی روی شبکه خصوصی ارائه می‌شوند. از شرکت‌ها گرفته تا دانشگاه‌ها و سازمان‌ها می‌توانند ابرهای خصوصی را برای استفاده انحصاری خود میزبانی کنند. هنگامی که آن‌ها این کار را انجام می‌دهند، مالک زیرساخت‌های زیرین ابر هستند و آن را در محلی از راه دور میزبانی می‌کنند.

### ۳. ابرهای ترکیبی

ابرهای ترکیبی همان‌طورکه از نامشان پیداست، ترکیبی از خدمات عمومی و خصوصی هستند. این نوع مدل به کاربر انعطاف‌پذیری بیشتری می‌دهد و به بهینه‌سازی زیرساخت و امنیت او نیز کمک می‌کند. به‌طورکلی، سازمان‌ها از ابرهای خصوصی برای عملکردهای حساس و از ابرهای عمومی برای تطبیق با افزایش تقاضای محاسباتی استفاده می‌کنند. داده‌ها و برنامه‌ها اغلب به‌طورخودکار بین آن‌ها ردوبدل می‌شود. این کار به سازمان‌ها انعطاف‌پذیری بیشتری می‌دهد، بدون اینکه آن‌ها را به کنارگذاشتن زیرساخت‌های موجود و امنیت ملزم کند.

### ٤. چندابری (Multicloud)

چندابری زمانی اتفاق می‌افتد که سازمان‌ها از ابرهای متعددِ چندین شرکت ارائه‌دهنده استفاده کنند. این کار مزایای بسیار زیادی به‌همراه دارد. درحقیقت، استفاده از چندین شرکت مختلف ارائه‌دهنده رایانش ابری بدین‌معنی است که می‌توانید ویژگی‌ها و عملکردهای آن‌ها را باهم ترکیب کنید.

### معرفی انواع مدل‌های Cloud Computing

سه سرویس مهم رایانش ابری که کاربرد و طرفداران زیادی دارند، رایانش ابری فناوری واحدی مانند ریزتراشه یا تلفن‌همراه نیست؛ بلکه سیستمی است که درمجموع، از سه سرویس تشکیل شده است: ۱. نرم‌افزار به‌عنوان سرویس (SaaS)؛ ۲. زیرساخت به‌عنوان سرویس (IaaS)؛ ۳. پلتفرم[7]به‌عنوان سرویس (PaaS). (Holtz et al,2017).

### ۱. نرم‌افزار به‌عنوان سرویس (SaaS)

نرم‌افزار به‌عنوان سرویس (SaaS) رایج‌ترین نوع رایانش ابری است. درواقع، SaaS برنامه‌های کاربردی را به‌صورت کامل و آماده ازطریق اینترنت دراختیار کاربران قرار می‌دهد و دیگر نیازی نیست که کاربران نرم‌افزار را دانلود و روی کامپیوترشان نصب کنند. استفاده از این سرویس به کاربران کمک می‌کند در مدت‌زمان کوتاهی به نرم‌افزار مدنظرشان دسترسی پیدا کنند. شایان ذکر است که تعمیر و نگه‌داری و عیب‌یابی این سرویس کاملاً برعهده شرکت ارائه‌دهنده رایانش ابری است. همچنین، نرم‌افزار به‌عنوان سرویس (SaaS) صدور مجوز برنامه نرم‌افزاری به کاربران را شامل می‌شود. مجوزها معمولاً ازطریق مدل پرداختی یا برحسب تقاضا ارائه می‌شوند. این نوع سیستم را می‌توان در Microsoft Office 365 یافت.

### ۲. زیرساخت به‌عنوان سرویس (IaaS)

زیرساخت به‌عنوان سرویس (IaaS) رویکرد انتخاب را برای محاسبات ارائه می‌دهد. فرض بر این است که درحال‌حاضر زیرساخت‌های اساسی فناوری اطلاعات را دراختیار دارید و درصورت نیاز، می‌توانید آن را با بلوک‌های ساختمانی مختلف تقویت کنید. این رویکرد برای سازمان‌هایی بهترین کار را انجام می‌دهد که سیستم‌عامل خاص خود را دارند؛ اما در طول زمان، به ابزارهایی برای پشتیبانی از آن سیستم‌ها احتیاج دارند. اتصال به سرورها، فایروال‌ها، سخت‌افزار و سایر زیرساخت‌ها به شرکت‌ها آزادی طراحی در مقیاس را با استفاده از اجزای ازپیش‌ساخته‌شده می‌دهد. IaaS می‌تواند به‌عنوان داربستی عمل کند که روی آن پروژه‌های خاص با الزامات منحصربه‌فرد فناوری اطلاعات اجرا می‌شود. برای مثال، کسب‌وکاری که در حال توسعه نرم‌افزار جدید است، احتمال دارد از IaaS برای ایجاد محیطی آزمایشی قبل از راه‌اندازی آن استفاده کند. افزون‌براین، شرکت تجارت الکترونیک ممکن است از IaaS برای میزبانی وب‌سایتش بهره ببرد. این سرویس روشی برای ارائه همه‌چیز را شامل می‌شود؛ از سیستم‌عامل گرفته تا سرورها و فضای ذخیره‌سازی ازطریق اتصال مبتنی بر IP به‌عنوان بخشی از سرویس درخواستی. با استفاده از سرویس IaaS، کاربران دیگر به خرید نرم‌افزار یا سرور نیازی ندارند و این منابع را در سرویس برون‌سپاری و براساس تقاضا می‌توانند تهیه کنند. از نمونه‌های معروف سیستم IaaS می‌توان به IBM Cloud و Microsoft Azure اشاره کرد.

7- Platform

### ۳. پلتفرم به‌عنوان سرویس (PaaS)

پلتفرم به عنوان سرویس (PaaS) ابزارهای مهم برای طراحی و توسعه نرم‌افزار را فراهم می‌کند. این سرویس شامل ابزارهای توسعه، کتابخانه‌های کد، سرورها، محیط‌های برنامه‌نویسی و اجزای برنامه ازپیش‌پیکربندی‌شده است.

با PaaS، شرکت‌های ارائه‌دهنده رایانش ابری نگرانی‌های مربوط به پشتیبان مانند امنیت و زیرساخت و ادغام داده‌ها را مدیریت می‌کنند؛ درنتیجه، کاربران می‌توانند روی ساخت و هاست و آزمایش برنامه‌ها تمرکز کنند و سریع‌تر و ارزان‌تر آن را انجام دهند. این سرویس پیچیده‌ترین لایه از سه‌لایه محاسبات مبتنی‌بر ابر شناخته می‌شود.

نکته مهم اینکه PaaS شباهت‌هایی با SaaS دارد؛ ولی تفاوت اصلی‌شان در این است که به‌جای ارائه نرم‌افزار به‌صورت آنلاین، درواقع پلتفرمی برای توسعه نرم‌افزار است که ازطریق اینترنت ارائه می‌شود. این مدل شامل پلتفرم‌هایی مانند Salesforce.com و Heroku است.

**جدول تفاوت‌های SaaS و PaaS و IaaS**

| انواع پلتفرم | تحویل | مزایا | ویژگی‌ها | کاربرد | محدودیت‌ها |
|---|---|---|---|---|---|
| **SaaS** | وب‌سایت | کاهش زمان و هزینه برای انجام کارهایی مانند نصب و مدیریت و ارتقای نرم‌افزار | از یک مکان مرکزی مدیریت می‌شود. – روی سرور راه دور میزبانی می‌شود. – ازطریق اینترنت دردسترس است. – کاربران مسئول به‌روزرسانی سخت‌افزار یا نرم‌افزار نیستند. | استارت‌آپ‌ها یا شرکت‌های کوچک – پروژه‌های کوتاه‌مدت – برنامه‌هایی که هم به وب و هم به موبایل نیاز دارند. | قابلیت همکاری – قفل فروشنده – نداشتن پشتیبانی یکپارچه – امنیت داده‌ها – سفارشی‌سازی – فقدان کنترل – محدودیت‌های ویژگی – عملکرد و خرابی |
| **PaaS** | وب‌سایت | نصب و توسعه مقرون‌به‌صرفه برنامه‌ها – مقیاس‌پذیر – دسترسی آسان – سفارشی‌سازی آسان برنامه‌ها – کاهش درخورتوجه کدگذاری – انتقال | مبتنی‌بر فناوری مجازی‌سازی است. – خدمات مختلفی را برای کمک به توسعه و آزمایش و استقرار برنامه‌ها ارائه می‌دهد. – برای کاربران زیادی ازطریق همان برنامه توسعه | ایجاد برنامه‌های کاربردی سفارشی – ساده‌سازی جریان‌های کاری زمانی که چندین توسعه‌دهنده روی یک پروژه توسعه کار می‌کنند. | امنیت داده‌ها – یکپارچگی‌ها – قفل فروشنده – سفارشی‌سازی سیستم‌های قدیمی – مشکلات زمان اجرا – محدودیت‌های عملیاتی |

| | | | | | |
|---|---|---|---|---|---|
| | | دردسترس است. – خدمات وب و پایگاه‌داده را ترکیب می‌کند. | آسان به مدل هیبریدی | | |
| امنیت – سیستم‌های قدیمی که در فضای ابری کار می‌کنند. – منابع داخلی و آموزش | استارت‌آپ‌ها و شرکت‌های کوچک – شرکت‌های بزرگ – شرکت‌هایی که رشد سریعی را تجربه می‌کنند. | منابع به‌عنوان سرویس دردسترس هستند. – هزینه بسته به مصرف متفاوت است. – خدمات بسیار مقیاس‌پذیر هستند. – سازمان کنترل کامل زیرساخت را حفظ می‌کند. – پویا و انعطاف‌پذیر است. | منعطف‌ترین مدل رایانش ابری – خودکارسازی آسان استقرار ذخیره‌سازی، شبکه، سرورها و قدرت پردازش – امکان خرید منابع درصورت نیاز – مقیاس‌پذیری چشمگیر | داشبورد یا API | **IaaS** |

**مزایای رایانش ابری:**

**۱. استفاده آسان و راحت**

استفاده از رایانش ابری ذخیره و بازیابی و به‌اشتراک‌گذاری اطلاعات را سریع و آسان می‌کند. همچنین، می‌توان به توانایی استفاده از نرم‌افزار ازطریق دستگاه‌های مختلف برنامه‌ای بومی یا یک مرورگر اشاره کرد. درنتیجه، کاربران می‌توانند فایل‌ها و تنظیمات خود را به روشی کاملاً یکپارچه به دستگاه‌های دیگر منتقل کنند.

**۲. انعطاف‌پذیری**

ازآن‌جاکه اطلاعات در مکان‌ها و دستگاه‌ها جریان دارد، کارمندان می‌توانند با خیال راحت و به‌طورایمن در هر جایی کار کنند. این باعث می‌شود که آنان در انجام کارشان موفق‌تر و راضی‌تر باشند.

**۳. هزینه**

در هسته رایانش ابری، ایده «چندتداومی» وجود دارد؛ یعنی ارائه‌دهنده سرویس ابری مشتریان زیادی دارد که از منابع محاسباتی مشابهی استفاده می‌کنند. این درست مانند ساختمان آپارتمانی است. اگرچه ساکنان امکانات و زیرساخت‌های مشترک دارند، همه آزادند آپارتمانشان را به‌دلخواه خود تزیین کنند.

همچنین، رایانش ابری در کاهش هزینه بسیار زیاد کسب‌وکارها نقش مؤثری ایفا می‌کند. پیش از فناوری رایانش ابری، شرکت‌ها به خرید و ساخت و نگه‌داری فناوری و زیرساخت مدیریت اطلاعات پرهزینه ملزم بودند. درحالی‌که امروزه

شرکت‌ها می‌توانند مراکز پرهزینه سرور و بخش‌های فناوری اطلاعات را با اتصالات اینترنتی سریع تعویض کنند و کارمندان نیز برای انجام وظایفشان می‌توانند به‌صورت آنلاین با همدیگر درارتباط باشند.

### ٤. قابلیت اطمینان

ارائه‌دهندگان سرویس‌های ابری به‌طورمستمر معماری خود را اصلاح می‌کنند تا بهترین استانداردهای عملکرد و دردسترس‌بودن را ارائه دهند. در همین حال، اشخاص ثالثی که خدمات آن‌ها را میزبانی می‌کنند، به‌طورمداوم آن‌ها را نگه‌داری و به‌روز و دسترسی آسان به پشتیبانی مشتری را فراهم می‌کنند. این تعهد به بهبود مستمر آن‌ها را در استانداردهای برتر قابل‌اعتماد می‌کند.

### ٥. مقیاس‌پذیری[٦]

فروشندگان ابری معمولاً به مشتریان اجازه می‌دهند منابع محاسباتی را درصورت نیاز افزایش یا کاهش دهند. این بدان‌معناست که میزان رایانش ابری می‌تواند باتوجه‌به کسب‌وکارتان افزایش یا کاهش یابد؛ یعنی پهنای باند و کاربرها و سرویس‌ها را می‌توانید کم و زیاد و حتی ارائه‌دهندگان خدمات بیشتری را اضافه کنید. علاوه‌براین، بسیاری از ارائه‌دهندگان خدمات ابری این مقیاس‌بندی را ازطرف شما خودکار می‌کنند تا تیم‌ها بتوانند زمان بیشتری را برای تجربه مشتری و زمان کمتری را برای برنامه‌ریزی ظرفیت صرف کنند.

### ٦. بک‌آپ‌گیری

رایانش ابری بسیار فراتر از دسترسی به فایل‌ها در دستگاه‌های مختلف است. به‌لطف خدمات رایانش ابری، کاربران می‌توانند ایمیل خود را در هر کامپیوتری بررسی و حتی فایل‌ها را با استفاده از سرویس‌هایی مانند Dropbox و Google Drive ذخیره کنند. سرویس‌های رایانش ابری امکان بک‌آپ‌گیری از فایل‌های موسیقی و عکس و ویدئو را نیز برای کاربران فراهم می‌کنند؛ درنتیجه درصورت خراب‌شدن هارد دیسک، آنان می‌توانند به‌راحتی به تمامی اطلاعاتشان دسترسی پیدا کنند. (تیلور و فرانسیس، ۲۰۱۸)

### ۷. سرعت زیاد

ساختار ابری به افراد اجازه می‌دهد تا فضای ذخیره‌سازی را روی دسکتاپ یا لپ‌تاپ خود ذخیره کنند و نرم‌افزار را سریع‌تر ارتقا دهند؛ زیرا شرکت‌های نرم‌افزاری می‌توانند محصولاتشان را به‌جای روش‌های سنتی‌تر و ملموس‌تر شامل هارد دیسک‌ها یا درایوهای فلش، ازطریق وب ارائه دهند. به‌عنوان مثال، کاربران Adobe می‌توانند ازطریق اشتراک مبتنی‌بر اینترنت به برنامه‌های کاربردی موجود در Creative Cloud خود دسترسی داشته باشند. این امر به کاربران امکان می‌دهد نسخه‌های جدید برنامه‌هایشان را به‌راحتی دانلود و نصب کنند.

8- Scaleable


## نقاط ضعف رایانش ابری:

- **امنیت:** امنیت همیشه ازجمله نگرانی‌های مهم درباره فضای ابری بوده و خواهد بود؛ به‌خصوص زمانی که از سوابق پزشکی و اطلاعات مالی حساس صحبت می‌شود. مقررات سرویس‌های رایانش ابری را مجبور می‌کند تا اقدامات امنیتی و انطباق خود را تقویت کند. رمزگذاری از اطلاعات حیاتی محافظت می‌کند؛ اما اگر آن کلید رمزگذاری گم شود، داده‌ها ناپدید می‌شوند.
- **اختلالات سروری:** سرورهایی که شرکت‌های رایانش ابری نگه‌داری می‌کنند، ممکن است قربانی بلایای طبیعی و اشکالات داخلی و قطع برق شوند؛ درنتیجه، گستره جغرافیایی محاسبات ابری هر دو طرف را کاهش می‌دهد.
- **انتقال اشتباهات:** مانند هر فناوری دیگری، منحنی یادگیری هم برای کارکنان و هم برای مدیران وجود دارد؛ اما ازآن‌جاکه بسیاری از افراد ازطریق یک پورتال به اطلاعات دسترسی پیدا و آن‌ها را دست‌کاری می‌کنند، اشتباهات غیرعمدی ممکن است به کل سیستم منتقل شوند.

## یافته های تحقیق

## کنترل امنیت در رایانش ابری:

از موارد مهم در این زمینه از دست رفتن داده ها است. نکته ی دیگر تأخیر در مباحث رایانش ابری است؛ که از مهم ترین چالش ها امینت است. خطرات گوناگونی، هم کاربران استفاده کننده از خدمات رایانش ابری و هم شرکت های سرویس دهنده رایانش ابری را تهدید می کند. این خطرات می تواند شامل موارد خیلی گسترده ای باشد، چون رایانش ابری بر بستر اینترنت است و همچنین اینترنت دروازه ای به یک شبکه ی بسیار گسترده که می تواند انواع تهدید ها و خطرات گوناگون را به رایانش ابری تحمیل می کند. دسترس پذیر بودن خود می تواند ترغیبی برای هکرها برای هجوم به این سیستم ها باشد و می توانند از آسیب پذیری های آن سوء استفاده کنند. تهدیداتی که این سیستم ها را تحت شعاع خود قرار می دهد، شامل انواع حملات جهت نفوذ، تخریب، بدافزارها (که شامل انواع ویروس ها، کرم ها، اسب های تراوا یا تروجان و موارد دیگر است)، دسترسی های غیر مجاز، دزدی اطلاعات، تغییر اطلاعات، افشاءکردن اطلاعات و غیره باشد. در رایانش ابری کاربران و مشتریان با مهاجرت به ابر به طور اساسی از برآوردن هزینه های نگهداری زیرساخت رها می شوند، اما با این وجود هزینه های ارتباطات افزایش می یابد به عنوان نمونه هزینه ارسال و دریافت داده ها مسئله ی جدیدی است که پیش روی مشتریان ابر است. یکی از چالش های دیگر حالت جعبه سیاه بودن سرویس های ابری است به طوری که کاربران سرویس گیرنده اطمینان خود را نسبت به خدمات دهنده ابر از دست می

دهند. در واقع هیچ معیاری بر امنیت این سیستم ها وجود ندارد و کاربران توانایی برای سنجیدن امنیت ابر را ندارند. هم چنین کاربران از محل ذخیره سازی اطلاعات خود آگاهی ندارند و کاربران نمی دانند که اطلاعاتی که در ابر ذخیره می کنند در کجا است. اطلاعات کاربران در دیتاسنترهای بزرگی ذخیره می شود و شرکت های خدمات دهنده از امن بودن اطلاعات ذخیره شده به کاربران اطمینان می دهند اما احتمال تغییر و از دست رفتن اطلاعات به دلیل نفوذ کردن و یا حتی اشتباهات انسانی وجود دارد؛ اما با پشتیبان گیری از اطلاعات و تنظیمات دوره ای می توان تا حد بالایی در حفظ و نگهداری اطلاعات کمک کنند تا در صورت بروز هر گونه رخدادی که باعث از بین رفتن اطلاعات شد، اطلاعات و تنظیمات از بین نروند، در این حالت در صورت از بین رفتن اطلاعات، اطلاعات می توانند بازگردانی شوند. پشتیبان گیری از اطلاعات می تواند خودکار و یا به صورت دستی باشد که می تواند در یک سیستم ویا چند سیستم ذخیره شوند. از مشکلات دیگر می تواند به حریم خصوصی کاربران اشاره کرد. معماری امنیتی ابر تنها در صورتی موثر است که پیاده سازی های دفاعی صحیح در محل باشد. معماری امنیت ابر کارآمد باید مسائلی که مدیریت امنیت را بوجود می آیند را تشخیص دهد. مدیریت امنیت، این مسائل را با کنترل های امنیتی نشان می دهد. این کنترل ها برای حفاظت از نقاط ضعف در سیستم و کاهش اثر یک حمله در محل قرار داده می شود. در حالی که بسیاری از انواع کنترل پشت یک معماری امنیتی ابر وجود دارد، آنها معمولا در یکی از دسته های زیر می توان یافت:

### ۱. کنترل بازدارنده[۷]

این کنترل ها برای کاهش حملات بر روی یک سیستم ابر در نظر گرفته شده است. بسیار شبیه به یک علامت هشدار دهنده در یک حصار و یا یک ملک است. کنترل بازدارنده به طور معمول سطح تهدید با اطلاع رسانی به مهاجمان احتمالی است که در صورت تداوم عواقب نامطلوب برای آنها وجود خواهد داشت.

### ۲. کنترل پیشگیرانه[۸]

کنترل پیشگیرانه تقویت سیستم در برابر حوادث است. به طور کلی اگر در واقع حذف آسیب پذیری نباشد با کاهش همراه است. به عنوان مثال، تأیید هویت قوی از کاربران ابر، که احتمال دسترسی کاربران غیر مجاز به سیستم های ابری را کمتر می کند. بیشتر احتمال شناسایی کاربران ابر را دارد.

### ۳. کنترل تشخیصی[۹]

کنترل تشخیصی برای شناسایی و واکنش های مناسب به هر حادثه ای که رخ می دهد، در نظر گرفته شده است. در صورت حمله، کنترل تشخیصی، به کنترل پیشگیرانه و یا اصلاحی سیگنالی جهت رسیدگی به این مسئله ارسال می کند. سیستم و نظارت بر امنیت شبکه، شامل تشخیص نفوذ و ترتیبات پیشگیرانه، معمولا برای تشخیص حملات در سیستم های ابر و زیرساخت های ارتباطی را پشتیبانی می کنند.

### ۱- کنترل اصلاحی[۱۰]

9-Deterrent controls
10- Preventive controls

11- Detective controls
12- Corrective controls

کنترل اصلاحی، به طور معمول با محدود کردن آسیب، عواقب ناشی از یک حادثه را کاهش می دهد. آنها در طول یا پس از وقوع حادثه اجرا می شوند. بازگرداندن پشتیبان گیری یک سیستم سازشی به منظور بازسازی یک مثال از یک کنترل اصلاحی است.

**فواید استفاده از رایانش ابری**

| **بهره وری** | |
|---|---|
| **استفاده از فناوری رایانش ابری** | **وضعیت فعلی** |
| • استفاده حداکثری (بیش از 70 درصدی) از دارایی ها و منابع تجمیع منابع و دارایی ها<br>• افزایش بهره وری در سرعت توسعه برنامه ها، شبکه، مدیریت برنامه ها و کاربران | • استفاده محدود (حداکثر 30 درصدی) از دارایی ها<br>• مستقل بودن سیستم ها از یکدیگر<br>• مدیریت سخت و پیچیده سازمان |
| چابکی | |
| **استفاده از فناوری رایانش ابری** | **وضعیت فعلی** |
| • خرید خدمات از ارائه دهندگان خدمات افزایش و<br>• کاهش سریع یرفیت ها پاسخگویی سریع به درخواست ها | • صرف زمان چندساله برای ساخت مراکز<br>• صرف زمان زیاد برای راه اندازی یک خدمت |
| **نوآوری** | |
| **استفاده از فناوری رایانش ابری** | **وضعیت فعلی** |
| • تغییر از مالکیت خدمت به ارائه خدمت تشویق<br>• فرهنگ کارآفرینی | • مالکیت دارایی ها |

### انواع تهدیدات امنیتی در رایانش ابری:

بزرگترین چالش در اجرای موفق فن آوری های محاسبات ابری، مدیریت امنیت است. به محض اینکه برنامه های کاربردی حساس و داده ها به مراکز داده ابر نقل مکان کرد، اجرا بر روی منابع محاسباتی مجازی در قالب ماشین مجازی ممکن است باعث بسیاری از نگرانی های امنیتی شود. شش تهدید امنیتی مهم مربوط به محاسبات ابری که توسط " اتحاد امنیت ابر "(CSA) کشف شده است عبارت است از:

**الف) استفاده نابجا از محاسبات ابری:** این تهدید برتر شناسایی شده توسط CSA است. در این روش مهاجمان می توانند به یک ابر عمومی نفوذ و با استفاده از قدرت زیرساخت های ابر و با آپلود نرم افزارهای مخرب به هزاران کامپیوتر برای حمله به ماشین های دیگر استفاده کنند.

**ب)API ناامن رابط برنامه نویسی کاربردی نا امن:** APIها مجموعه ای از رابط های برنامه کاربردی است که توسط مشتریان برای تعامل با خدمات ابر استفاده می شود. هنگامی که third party شروع به ایجاد آن برنامه می کند، کاربر را با خطرات تهیه، محرمانه بودن و یکپارچگی داده ها مواجه می کند.

**ج) آسیب پذیری فناوری به اشتراک گذاشته شده:** به عنوان ارائه دهنده پلتفرم ابر که توسط کاربران مختلف به اشتراک گذاشته می شود، این احتمال وجود دارد که این اطلاعات متعلق به مشتریان مختلف که در مرکز داده مشابه قرار دارند، باشد؛ بنابراین نشت اطلاعات غلط توسط یک مشتری ممکن است به دیگران انتقال داده شود.

**د) از دست دادن داده / نشتی:** از دست دادن داده یک مشکل شایع در محاسبات ابری است. اگر ابر ارائه دهنده خدمات رایانش ابری خدمات خود را به دلیل برخی از مشکلات مالی و حقوقی ببندد، پس از آن از دست رفتن اطلاعات برای کاربرانش وجود خواهد داشت.

**ه) ترافیک ربایی:** ترافیک مشکل دیگری است که کاربران ابر باید از آن آگاه باشند. این تهدیدات شامل حملات man in the middle، اسپم ها، حملات dos می باشد.

**و) Insider های مخرب:** این گونه تهدیدها شامل تقلب، آسیب و سرقت یا از دست دادن اطلاعات محرمانه ناشی از خودی مورد اعتماد است. خودی های مخرب می توانند بوسیله توانایی خود برای نفوذ به سازمان و دارایی ها باعث ایجاد: زیان بهره وری، آسیب نام تجاری و تاثیرات مالی و... شوند.

**ابعاد امنیت ابری:**

کنترل های امنیتی درستی باید برای دارایی ها، تهدیدها و ریسک آسیب پذیری ماتریس های ارزیابی پیاده سازی شوند. ابعاد امنیت به ۲ دسته کلی تقسیم شده اند: مسائل امنیتی و خصوصی سازی، مسائل پذیرش و مسائل حقوقی و قراردادی و...؛ که در زیر آمده است:

۱- **مسائل امنیتی و حریم خصوصی:** شامل چهار بخش مهم می باشد؛ که شامل موارد زیر است:

الف – مدیریت هویت

ب– امنیت فیزیکی

ج– امنیت پرسنل

د– حریم خصوصی



**مسائل حقوقی و قراردادها:** ارائه دهندگان محاسبات ابری و مشتریان آنها درباره مسئولیت هایی مذاکره خواهند کرد از قبیل مشخصه های معنوی و زمان پایان خدمات، زمانیکه داده و برنامه های کاربردی در نهایت به مشتری بازگردانده می شود، مسائل حقوقی نیز ممکن است شامل نیازهایی برای نگهداری سوابق در بخش دولتی که در آن بسیاری از سازمان ها توسط قانون برای حفظ و ایجاد پرونده های الکترونیکی موجود در یک روش خاص است، می باشد. این امر توسط قانونگذاری ممکن است به منظور نیاز سازمان به مطابقت با قوانین و شیوه های تعیین شده توسط آژانس های حفظ سوابق، مشخص شود. سازمان های دولتی با استفاده از محاسبات ابری و ذخیره سازی باید این نگرانی ها را مورد توجه قرار دهند.

**تهدیدها و حملات ابر:**

مشکلات امنیتی به عنوان یک مانع بزرگ در مقابل استفاده کاربران از سیستم های رایانش ابری قلمداد می شود. هر یک از انواع مختلف خدمات رایانش ابری- مانند SaaS، PaaS، IaaS- چالش های امنیتی خودش را دارد. ولی IaaS همه انواع چالش مانند: حملات شبکه، حمله مبتنی بر رفتار، حمله مبتنی بر درخواست، کنترل درخواست ها از کاربران نامطمین، XSS و DDoS و بسیاری دیگر را در بر می گیرد. این حملات مستقل از یکدیگرند و در نتیجه کیفیت خدمات ارائه شده توسط ابر را به خطر می اندازند. (Aljarah and Ludwing, 2015)

**حمله DoS**: یا از کار اندازی سرویس، نوعی حمله است که هدف آن از کاراندازی سیستم با استفاده از هدر دادن منابع آن است. بطوریکه سرویس دهنده توانایی سرویس دهی عادی به کاربران مجاز را از دست بدهد. محرومیت از سرویس یا DoS در دنیای کامپیوتر همانند هکر ها خیلی مشهور هستند و در طی سالیان به صورت های مختلف برای رد کاربران در استفاده از سرویس ها استفاده شده اند. هدف از حملات رد سرویس، غیر قابل دسترس کردن منابع کامپیوتر از کاربرانی که قصد دستیابی به آن را دارند، می باشد.

**DoS توزیع شده**[۱۳]

حملات DDoS نیز مشابه DoS هستند با این تفاوت که حمله از طریق چندین سیستم و بصورت توزیع شده است. DoS توزیع شده حمله ای است که اغلب هزاران یا حتی میلیون ها کامپیوتر به یک هدف حمله می کنند. معمولا مهاجم از تعدادی کامپیوتر بدون اجازه مالکشان که botnet نامیده می شود، استفاده می کند. این botnet ها توسط یک مدیر کنترل می شوند قدرتشان برای حمله به یک هدف به کار برده می شود.

**حمله سیل آسا Flooding Attack**

یکی از اقداماتی که مهاجم برای دسترسی به سرور انجام می دهد محرومیت کاربران مجاز از سرویس های درخواستی می باشد. حملات سیل آسا نه تنها در محیط ابری بلکه در رایانش های خوشه ای و توری نیز رخ می دهد. در سیستم های ابری سرورهایی که از طریق ارتباطات داخلی با هم در ارتباطند به انجام کار خاصی می پردازند و هنگامی که درخواست های سمت یک سرور زیاد می شود و سرور پربار می شود قسمتی از کارهای خود را به سرور خاص شبیه به خود از لحاظ کاری می دهد و اینگونه بارگذاری جانبی صورت می گیرد. هنگامی که مهاجم با مجوز و داده های ساختگی درخواست های خود را به سمت سرور گسیل می کند، مهاجم درخواست ساختگی خود را به سمت سرور می فرستد در سمت سرور درخواست های ارسالی کنترل شده، مجوز آن ها بررسی می شود و مشخص می گردد که درخواست فعلی نامعتبر بوده است. در طی این فرآیند کنترل کردن درخواست های فوق به مصرف پردازشگر و حافظه زیادی نیاز دارد که این امر باعث بالا رفتن بار روی سرور شده سرور مجبور به بارگذاری جانبی به سرور دیگر می شود. در نتیجه مهاجم با ایجاد اختلال در فرآیندهای معمول و عادی سرور موفق به انجام حمله خود شده است.

**XSS**[۱۴] **:** حملات کراس سایت اسکریپت روش نفوذ و گرفتن دسترسی غیرمجاز از یک وب گاه توسط هکرها می باشد.

**حملات ماسک:** در این حملات تهدیدها نقش کاربران مجاز را بازی می کنند.

13-Distributed DOS
14-Cross Site Scripting

**حملات مبتنی بر میزبان:** این حملات نتیجه حملات ماسک و عموما در ناهنجاری رفتاری کاربران قابل مشاهده است.

**پیشنهادات تحقیق**

**راهکارهای امنیت ابر**:

شکست در امنیت رایانش ابری به چند دلیل رخ می دهد که یکی از دلایل آن، سخت افزاری است که در لایه زیرساخت به عنوان سرویس ابر بکار می رود. در این جدول خلاصه ای از تهدیدها و راه حل های ارائه شده (۲۰۱۲ . Arora et al,)

**تهدیدها و راه حل های امنیت زیرساخت ابر**

| مؤلفه های IaaS | تهدیدها / چالش ها | راه حل ها |
|---|---|---|
| SLA (موافقت نامه سطح خدمات) | نظارت و اجرای SLA<br>نظارت ویژگیهای کیفیت خدمات | چارچوب (WSLA) موافقت نامه سطح خدمات وب<br>نظارت SLA و اجرا در SOA |
| محاسبات سودمند | اندازه گیری و صورتحساب ارائه دهندگان<br>دسترس پذیری سیستم صورتحساب بنابه تقاضا | سیستم پرداخت آمازون |
| نرم افزار ابر | حملات به XML<br>حملات به خدمات وب | رمزگذاری XML و امضای آن |
| اتصالات اینترنت و شبکه ها | کلاهبرداری IP<br>اسکن پورت<br>امنیت DNS | دیوار آتش و بخش بندی شبکه منطقی<br>رمزگذاری ترافیک<br>نظارت بر شبکه<br>سیستم تشخیص نفوذ و ممانعت از نفوذ |
| مجازی سازی | تهدیدهای امنیتی از منبع میزبان:<br>☐ نظارت ماشین های مجازی از میزبان<br>تهدیدهای امنیتی از منبع ماشین مجازی:<br>☐ نظارت ماشین مجازی از ماشین مجازی دیگر<br>☐ ارتباطات بین ماشین | تهدیدهای امنیتی از منبع میزبان:<br>☐ پلتفرم رایانش ابری مطمئن<br>☐ مراکز داده<br>تهدیدهای امنیتی از منبع ماشین مجازی:<br>☐ رمزگذاری<br>☐ VPN<br>☐ امنیت Xen با جداسازی |

| | | | | |
|---|---|---|---|---|
| | ارتباطات بین ماشین های مجازی و میزبان<br>تغییرات ماشین های مجازی | های مجازی<br>ماشین های مجازی سیار<br>منابع انکار خدمات (DOS)<br>مهاجرت ماشین های مجازی | مجازی مطمئن (TVDc)<br>کنترل دسترسی الزامی (MAC) | معماری LoBot برای تأمین امنیت و مهاجرت ماشین مجازی |
| سخت افزار کامپیوتر | حمله فیزیکی به سخت افزار کامپیوتر<br>امنیت داده در دستگاههای ذخیره سازی از رده خارج شده یا جایگزین شده | | اتاق های قفل شده با امنیت بالا با دستگاههای نظارت<br>دسترسی چندگانه به مخازن رمزگذاری سیستم فایل های مخفی شفاف | |

## نتیجه گیری

رایانش ابری اصطلاحی جدید است که سرویس‌ها و منابع فناوری اطلاعات را از طریق اینترنت فراهم می‌آورد. علاوه بر مزایای بسیار آن، نگرانی‌های امنیتی ناشی از کمبود کنترل در سطوح مختلف معماری ابری وجود دارد. محیط ابری هدفی جذاب برای مهاجمان است و تهدیدات جدیدی را به دلیل مدل‌های سرویس‌دهی، تکنولوژی‌های زیرساخت و طبیعت توزیع شده آن، برای سازمان ایجاد می‌کند. مشتریان ابر برای حفاظت از برنامه‌های خود در مقابل حملات سایبری مختلف نیاز به استفاده از سیستم‌های تشخیص نفوذ دارند زیرا فایروال‌ها به تنهایی قادر به ارائه راهکار مناسب امنیتی در ابر نیستند. با این وجود پیاده‌سازی‌های امنیتی موجود در فراهم آورندگان ابری کنترل کامل بر مولفه‌های مختلف سرویس تشخیص نفوذ ابری را تدارک نمی‌بینند. در نهایت توجه به وجود تعامل میان سطح امنیت سیستم و عملکرد آن بر اساس رابطه متوازن میان آنها ارزشمند است. یک سیستم تشخیص نفوذ که سرویس‌های معتمد با امنیت بالا فراهم می‌کند الگوها و قوانین بیشتری را به کار می‌گیرد. بنابراین منابع محاسباتی بیشتری برای تامین امنیت بهتر لازم است. با توسعه این راهکار در رایانش ابری، منابع اختصاصی مشتریان ابر کاهش خواهد یافت. بنابراین بهترین راه لزوماً سیستمی پیچیده با منابع و قوانین بسیار، نمی‌باشد بلکه طراحی بهینه و استفاده از تکنیک‌های هوشمند که توسط خودگردانی و خودیادگیری موجب استقلال سیستم می‌شود، می‌باشد.

سیستم های ابری در دسترس هستند پس می توانند مورد مناسبی جهت حملات باشند. استفاده از تجهیـزات نرم افزاری و

سخت افزاری امنیتی می تواند جهت بالا بردن امنیت این شبکه ها استفاده شود، استفاده از فایروال ها IDS و IPS می تواند بسیار به تأمین امنیت کمک کند. با توجه به این که رایانش ابری سرویس های خوبی ارائه می دهد اما باید در استفاده از آن ها محتاط بود. اطلاعاتی که در سرورهای شرکت های خدمات دهنده رایانش ابری ذخیره می شوند می توانند مورد تعرض قرار گیرند و یا امکان از دست رفتن اطلاعات نیز وجود دارد، با توجه به این مهم باید از ذخیره کردن اطلاعات مهم و با ارزش و حساس پرهیز کرد؛ اما آگاهی از خطرات استفاده از این امکان می تواند کاربران را در استفاده بهتر از خدمات رایانش ابری یاری کند و تصمیم گیری را برای آن ها راحت تر نماید. اما استفاده بهتر به این معنا نیست که از استفاده از خدمات آن ها بی بهره بود اما لازم است که برخی انجام ملاحظات شود. به عنوان نمونه اطلاعات مهم یک سازمان که بسیار با ارزش است نباید در جایی ذخیره شود که کنترلی روی آن نمی توان انجام داد. انتخاب یک رمز عبور مناسب و قوی و هم چنین استفاده از ارتباطات رمز گذاری شده از مواردی است که رعایت آن ها در بهبود امنیت تأثیر زیادی دارد. البته متخصصان امنیتی در برقراری امنیت در حد بالا تأکید دارند و نه امنیت صد درصد. امنیت به طور صد در صد قابل دستیابی نیست اما می توان تا حد بالایی آن را تأمین کرد. ایجاد امنیت در رایانش ابری یک همکاری مشترک بین ارائه‌دهنده خدمات ابری و مشتری است که انجام دقیق آن توسط هر دو طرف، به بالابردن بیشتر ایمنی کمک می‌کند. به‌عنوان‌مثال توسعه Backend در برابر آسیب‌های امنیتی تا حد زیادی در دست ارائه دهندگان خدمات ابری است که این خود اهمیت انتخاب یک ارائه‌دهنده خدمات ابری حرفه‌ای از طرف مشتری را نشان می‌دهد. از طرف دیگر خود مشتری نیز باید در ایجاد دسترسی برای کاربران و پرسنل دقت کند و به آنها آموزش‌های لازم را بدهد تا امنیت اطلاعات صدمه نبیند.

با اینکه در فضای ابری می‌توان از اطلاعات موجود به طرق مختلف محافظت کرد، اما در صورت دزدیده شدن اعتبارنامه‌ها و لورفتن نام کاربری و رمز عبور کاربران سیستم‌های ابری ممکن است با چالش‌های امنیتی بسیاری روبرو شوند.

**۱- برای ایجاد امنیت بیشتر در رایانش ابری لازم است در قرارداد مشخص شود که مسئولیت انجام کدام‌یک از موارد زیر با ارائه‌دهنده خدمات و کدام‌یک با مشتری است:**

- **تجهیزات فیزیکی شبکه**: شامل روترها، برق، کابل و...
- **تجهیزات دیتاسنتر:** شامل کنترل تهویه مطبوع فضا و...
- **منابع ذخیره‌سازی داده**: شامل ذخیره‌سازها، هاردها و...
- **سرورهای فیزیکی میزبان**: شامل سخت‌افزار به کار برده شده، میان‌افزارها و درایورها
- **زیرساخت مجازی‌سازی**: شامل برنامه مجازی ساز
- **سیستم‌های عامل و نرم‌افزارهای آن**
- **Middlewareبرای مدیریت رابط برنامه نویسیAPI**
- **داده‌ها**: شامل تمامی اطلاعات ذخیره شده، اصلاح شده و در دسترس قرار گرفته
- **اپلیکیشن‌ها**: شامل سرویس‌های نرم‌افزاری مثل ایمیل و...
- **دستگاه‌هایEnd-user** : مثل کامپیوترها، موبایل‌ها، اینترنت اشیا و...

## ۲- مدلها و راه حلهایی برای امنیت داده ها در رایانش ابری:

**الف - مدل دیاگرام حالت:** راه حل امنیت مراکز داده با مدل دیاگرام حالت برای نشان دادن یکپارچگی و محرمانگی امنیت داده ها به هفت چهارچوب در گروه های متعدد تقسیم بندی می شود:

الف-یکپارچگی و محرمانه بودن اطلاعات، اگر شرکت متکی بر ارائه دهنده خدمات تجاری برای خدمات انتقال داده ها به عنوان یک آیتم کالا و نه به عنوان یک سرویس مدیریت شده کامل.

ب- داده های ورودی - مدیریت چرخه اطلاعات، فرایندهایی مانند طبقه بندی داده، ذخیره سازی، استفاده و در اختیار گذاشتن حقوق مبتنی بر الزامات قانونی و کسب و کار را فراهم می کند

ج- نظارت بر ایمنی - شرکت کنترل های امنیتی در سیستم اطلاعات را به طور مداوم پایش می کند.

د- ماژول مدیریتی - اشاره به کاربر نهایی و مدیریتی دارد که برای ایجاد کنترل های مناسب برای همه مشتریان که اطلاعات را پردازش و واسطه دسترسی به سیستم های اطلاعاتی دیگر است، بکار می رود.

ه- مدیریت حساب – شرکت، حساب های سیستم اطلاعات را مدیریت می کند، از جمله تشکیل، فعال سازی، تغییر، تجدید نظر و از بین بردن و خاموش کردن حسابها را انجام می دهد.

ر- خطرات امنیتی - شرکت توسعه، انتشار، اقدامات احتیاطی منظم برای حفظ از خطرات امنیتی انجام می دهد.

ز- اطلاعات حساس - شرکت دسترسی به اطلاعات حساس بر اساس نقش کاربران که براساس حسابهای مدیریت تعیین شده، اختصاص می دهد.

### ب- لایه بندی امنیت در مراکز داده رایانش ابری

آزمایشگاه SANS مقاله تحلیلی با حمایت شرکت سیمانتک ارائه داد که در آن امنیت دیجیتال با داشتن پنج لایه، حفاظت، تشخیص، درمان و اصلاح حوادث، تامین می شود. این لایه ها همیشه به یک سیستم فیزیکی نگاشت نمی شود. برخی از این لایه ها به خدمات مربوط می شود. برخی از این سیستم های امنیتی حول لایه های متعدد می چرخد که می تواند دلیل خوبی برای وجود بیشتر تقسیم این لایه ها باشد، اما این پنج لایه همانند نقطه شروع صداست. سازمان هایی که این پنج لایه را بخوبی اجرا کردند، وضعیت بسیار بهتری به دفع و کشف حملات خواهند داشت.

### ج - امنیت به عنوان سرویس در محاسبات ابری

امنیت به عنوان یک سرویس (SECaaS) یک مدل کسب و کار که در آن یک ارائه دهنده خدمات بزرگ، سرویس های امنیتی خود را به شرکت های زیرساخت بزرگ بر اساس هزینه اشتراک، ادغام می کند. در این سناریو، امنیت به عنوان یک سرویس ابری، بدون نیاز به سخت افزار در محل، از هزینه های قابل توجهی جلوگیری می کند. این سرویس های امنیتی اغلب شامل احراز هویت، آنتی ویروس، ضد تروجان / نرم افزارهای جاسوسی، تشخیص نفوذ و مدیریت رویداد امنیتی و ... می باشد. صدور مجوز امنیتی از خارج از سازمان هزینه های بسیاری را تحمیل می کند. SECaaS برای کاربران اینترنت سرویس های امنیتی حفاظت از تهدیدات آنلاین مانند: حملات DDoS را مانند که به طور مداوم برای نقاط دسترسی جستجو می کند، ارائه می کند. همانطور که تقاضا و استفاده از محاسبات ابری به شدت افزایش می یابد، کاربران با توجه به دسترسی به اینترنت از نقاط دسترسی جدید بیشتر به حملات آسیب پذیر هستند. SECaaS به عنوان یک سپر در برابر تهدیدات آنلاین مقاومت می کند.

## نیازمندی ها و تهدیدات امنیتی لایه های سرویس دهی ابر

| سطح | سطح سرویس | نیازمندی های امنیتی | حملات |
|---|---|---|---|
| سطح برنامه کاربردی | نرم افزار به عنوان سرویس (SaaS) | حریم خصوصی<br>محافظت از داده ها کنترل دسترسی حفاظت از ارتباطات<br>امنیت نرم افزار<br>در دسترس بودن سرویس | استراق سمع تغییر و حذف داده ها<br>نقض حریم خصوصی جریان ترافیک ربودن نشست جعل هویت |
| سطح | سطح سرویس | نیازمندی های امنیتی | حملات |
| سطح مجازی | بستر به عنوان سرویس (PaaS)<br>زیرساخت به عنوان سرویس (IaaS) | کنترل دسترسی<br>امنیت برنامه کاربردی و داده ها<br>امنیت کنترل مدیریت ابر تصاویر ایمن<br>حفاظت از ابر مجازی امنیت ارتباطات | نقص برنامه نویسی تغییر نرم افزار<br>وقفه در نرم افزار ربودن نشست<br>اختلال در ارتباطات سیل اتصالات |
| سطح فیزیکی | دیتاسنتر فیزیکی | امنیت سخت افزار<br>قابلیت اطمینان سخت افزار<br>حفاظت از شبکه حفاظت از منابع شبکه | حملات شبکه ای حملات DDOS<br>ازکارافتادن و تغییر سخت افزارسوءاستفاده از زیرساخت<br>سرقت سخت افزار بلایای طبیعی |

در عمل به طور معمول پنج گام تا امنیت مرکز داده برای انجام چک لیست برای امنیت مراکز داده در محل ابر مراحل زیر را طی میکنند.

۱- فراهم کردن امنیت فیزیکی - کنترل دسترسی فیزیکی به مرکز داده ها
۲- ایجاد مناطق امن در شبکه
۳- قفل کردن سرور و میزبانها
۴- اسکن برای آسیب پذیری نرم افزارها
۵- هماهنگ کردن ارتباط بین دستگاه های امنیتی برای دیدشان به جریان داده

## نتیجه گیری آخر

الف) ایجاد محیط رایانش ابری با ویژگی هایی نظیر بومی، امن و اختصاصی بودن با در نظر گرفتن محیط های تعاملی که در ابرهای عمومی وجود دارد؛

ب) یکپارچه سازی در حوزه های زیرساخت و شبکه سازمان های نظامی، مراکز داده، اطلاعات و برنامه های کاربردی موجود از الزامات مهم در مهاجرت سازمان های دفاعی است؛

ج) ایجاد زیرساخت های مجاز ی‌سازی در سطح خدمات از مهم ترین الزامات مهاجرت می باشد و باید توجه ویژه ای در این حوزه به عمل آید؛

د) ایجاد کارگزاری های رایانش ابری در سطح سازمان های دفاعی برای ارتباط دهی فراهم کنندگان خدمات و مصرف کنندگان خدمات باید مورد توجه قرار گیرد؛

ه ) مهاجرت گام به گام به محیط رایانش ابری حوزه با در نظر گرفتن اولویت ها مد نظر قرار گیرد؛

ر ) تغییر فرهنگ سازمانی در جهت مهاجرت به محیط رایانش ابری و تجدیدنظر در رویکردها و سیاست هایی که در محیط ابری وجود دارد، به منظور چالاکی و کم شدن هزینه های سازمان های دفاعی صورت پذیرد؛

ز ) مدل به اشتراک گذاری ایمن داده ها و خدمات در محیط رایانش ابری دفاعی بر اساس کارکردهای سازمان های دفاعی به عنوان یک اولویت مهم و اساسی تدوین گردد.

## منابع


۱- رزمجو، محمدرضا (۱۳۸۶). مدیریت اطلاعات و تأثیر آن بر بنیهٔ دفاعی. فصلنامه مدیریت نظامی،۸()۵۲، ۴۸-۲۷.

۲- ولوی، محمدرضا و موحدی صفت محمدرضا (۱۳۹۵). ارائه الگوی امن استقرار زیرساخت های دفاعی کشوردر محیط رایانش ابری. فصلنامه مطالعات بین رشته ای راهبردی، ۷(۲۲)، ۲۹-۴۴.

۳- رادمنش، نگین (۱۳۹۵). مروری بر امنتیت محیط های رایانش ابری و انواع سیستم های تشخیص نفوذ ابری،

۴- روستایی، رسول. عباسی، امین (۱۳۹۸)، امنیت در رایانش ابری.

۵- تیز کار سعد آبادی، زینب (۱۳۹۹)، امنیت رایانش ابری.

۶- شفیع پور مطلق، زهرا (۱۳۹۵)، بررسی امنیت در رایانش ابری بر اساس فناوری IoT

۷- روشن ضمیر، اکبر. زنگویی، سارا (۱۳۹۵)، عوامل موثر بر شکل گیری کسب و کارهای کوچک به کمک فناوری رایانش ابری

8- Wilson, J. R. (2013). *The challenge of a secure military cloud. military and aerospace*. http://www.militaryaerospace.com/articles/print/volume-24/issue-11/technology-focus/the-challenge-of-a-secure-military-cloud.html

9- Takai, M. (2012). *DoD Cloud Computing Strategy*. Department of Defense Chief Information Officer.

10- *Bhadauria, R. and Chaki R. and Chaki N. and Sanyal S., A Survey on Security Issues in Cloud Computing, 2014. [2]*

11- mona marzenaki et al "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing ".

12- Holtz, M. D., David, B. M., Timoteo, R. And Junior, S. (0). Building Scalable Distributed Intrusion Detection Systems Based on the MapReduce Framework.

13- Stergiou, Christos, Kostas E. Psannis, Brij B.Gupta, and Yutaka Ishibashi. "Security, privacy &efficiency of sustainable cloud computing for big data & IoT." Sustainable Computing: Informatics and Systems 19 (2018): 174-184.

14- Zhang, PeiYun, Yang Kong, and MengChu Zhou. "A domain partition-based trust model for unreliable clouds." IEEE Transactions on Information Forensics and Security 13, no. 9 (2018): 2167-2178.
15- Kashif, Ubaidullah Alias, Zulfiqar Ali Memon, Shafaq Siddiqui, Abdul Rasheed Balouch, and Rakhi Batra. "Architectural design of trusted platform for IaaS cloud computing." In Cloud Security: Concepts, Methodologies, Tools, and Applications, pp. 393-411. IGI Global, 2019.
16- Krautheim FJ, Phatak DS, Sherman AT. Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing. Trust and Trustworthy Computing: Springer; 2010. p. 211-27.