

شناسایی نیازمندی‌های تعامل‌پذیری ابری



عنوان گزارش: شناسایی نیازمندی‌های تعامل‌پذیری ابری
کلمات کلیدی: خدمات ابری، تعامل‌پذیری، قابلیت حمل ابری، اتصال متقابل مراکز داده، مهاجرت به خدمات ابری
تهیه کنندگان: علی شریفی، معصومه صادقی، سوگل بابازاده، حمیرا مقدمی، کلثوم عباسی شاهکوه
ناظر علمی: پژمان گودرزی، مریم محمودی، محمود خراط
گروه پژوهشی: خدمات و محتوای الکترونیکی
تاریخ نشر: آذر ماه ۱۴۰۳

حقوق معنوی این اثر متعلق به پژوهشگاه ارتباطات و فناوری اطلاعات است و استفاده از آن با ذکر ماخذ بلامانع است.

خلاصه مدیریتی

قابلیت‌همکاری چندابری و قابلیت‌حمل کاربردها و داده‌ها به‌عنوان اولویت اصلی در پذیرش راه‌حل‌های مبتنی بر ابر و تحول دیجیتال کسب‌وکارها به‌شمار می‌رود. تعامل‌پذیری و قابلیت‌حمل نیازمندی‌های اصلی برای پذیرش سطح بالاتر ابر است و درک قابلیت همکاری (تعامل‌پذیری) و قابلیت‌حمل ابری یک گام اساسی در فرآیند برنامه‌ریزی و طراحی خدمات و برنامه‌های کاربردی جدید ابری است و کسب و کارها براساس آن می‌توانند مسیر ایده‌آل برای برنامه‌ریزی راه‌حل‌های ابری خود را شناسایی کنند. همچنین، دغدغه‌های خاص در مورد قابلیت‌همکاری و قابلیت‌حمل می‌تواند به شناسایی ویژگی‌هایی که بهترین تناسب را برای راه‌حل‌های جدید مبتنی بر ابر ارائه می‌کنند، کمک کند.

توسعه شبکه ملی اطلاعات و اقتصاد رقومی (دیجیتال) و نیز اصلاح نظام اداری مبتنی بر هوشمندسازی دولت از جمله اهداف اصلی در برنامه هفتم توسعه کشور تا سال ۱۴۰۷ می‌باشند و در این راستا، وزارت ارتباطات و فناوری اطلاعات موظف است با مشارکت و سرمایه‌گذاری بخش غیردولتی از طریق سازمان توسعه‌ای زیرمجموعه خود نسبت به تأمین زیرساخت‌های لازم اعم از ارتباطی و اطلاعاتی (ابری) و ذخیره‌سازی و پردازش سریع به‌منظور حضور و رقابت در بازارهای داخلی و بین‌المللی، اقدام نماید.

به‌کارگیری راه‌حل‌های نرم‌افزاری نوآورانه و پیشرو باعث تغییر رویکرد و نقش کسب و کارها می‌شود. در این راستا، انتقال زیرساخت‌های سازمانی به فضای ابری، تحولی فناوری-محور و مبتنی بر ساختار کسب و کار است که در آن فناوری در مرکز نیازهای کاربران و متمرکز بر ارزش‌های کسب و کاری سازمان است. در فصل ۲۳ برنامه هفتم در بخش هوشمندسازی و دولت الکترونیک، دستگاه‌های اجرائی موظف شده‌اند تا با رعایت قانون مدیریت داده‌ها و اطلاعات ملی، مراکز داده اصلی و پشتیبان خود را به زیرساخت یکپارچه ابری دولت‌هوشمند متصل نمایند. مدیریت داده‌ها و اطلاعات ملی اشاره به نقش تبادل داده‌ها و اطلاعات بین دستگاه‌ها و نهادها و همچنین ایجاد پایگاه‌های ملی (پایه) داده و دسترسی و به‌روز رسانی آنها براساس الزامات تعامل‌پذیری دولت الکترونیک دارد.

اتصال مراکز داده و ابری به یکدیگر نقشی کلیدی در رشد و چابکی مقیاس‌پذیر زیرساخت‌های اطلاعاتی در سازمان‌ها دارد و به‌عنوان مولفه مرکزی مدل‌های کسب و کاری جدید در نظر گرفته می‌شود. با توجه به گستردگی حوزه‌های عملکردی و خدمات دولت الکترونیک، ابتکارات بهینه‌سازی مرکز داده و اتصال آنها به یکدیگر یک جزء سازنده کلیدی در ایجاد زیرساخت یکپارچه خدمات، اتصال مشتریان و ارتباطات شرکای زیست بوم می‌باشد.

در این گزارش، نیازمندی‌های تعامل‌پذیری و قابلیت‌حمل سامانه‌ها، خدمات و داده‌ها در یک محیط چند ابری مرتبط با اهداف برنامه هفتم توسعه شامل توسعه زیرساخت‌های ارتباطی و اطلاعاتی (ابری) شبکه ملی اطلاعات، توسعه زیرساخت‌های ابری دولت‌هوشمند، اتصال مراکز داده سازمان‌ها به زیرساخت یکپارچه ابر دولت و مهاجرت سازمان‌های دولتی به فضای ابری بررسی می‌شود.

تعامل‌پذیری و قابلیت‌حمل نشان‌دهنده توانایی بالقوه اجزای و مولفه‌های ابر عمومی و خصوصی در زیست‌بوم ابری برای درک یکدیگر است. تمرکز قابلیت‌حمل برنامه‌های ابری بر انتقال برنامه‌ها یا اجزای برنامه در میان محیط‌های چندگانه و مختلف ابری بدون نیاز به ایجاد تغییرات در منطق برنامه است. اجزای برنامه می‌تواند بخشی از برنامه‌های توزیع شده یا یک برنامه یکپارچه باشد.



شکل ۱: مولفه‌های قابلیت همکاری و قابلیت حمل ابری

قابلیت همکاری مدیریت یکی از جنبه‌های مهم در تعامل‌پذیری ابری است و به همکاری خدمات ابری و نرم‌افزارهایی اشاره دارد که مولفه‌های خودخدمت براساس تقاضا را در یک محیط ابری مدیریت و کنترل می‌نمایند. هدف اصلی مولفه انتشار و اکتساب، سازگاری و همکاری میان خدمات، پلتفرم‌ها و داده‌های ابری است. به‌طور کلی، ارائه‌دهندگان خدمات ابری از بازارها برای انتشار خدمات ابری و اجزای مرتبط خود استفاده می‌کنند. قابلیت همکاری با فراهم‌آوری رابط‌های استاندارد برای انتشار و اکتساب خدمات و داده‌ها ابری می‌تواند هزینه‌های کمتر رایانش را تضمین کند.

تقاضای روزافزون برای رایانش ابری و مجازی‌سازی منابع شبکه پیامدهای خود را بر اتصال مرکز داده دارد. این امر بر معماری شبکه ارائه دهنده‌گان ابری تاثیر گذاشته و تمرکز آن بر اشتراک بار و بارهای کاری توزیع شده را ضروری می‌نماید. اتصال متقابل مرکز داده همچنین، راهی برای اتصال مراکز داده مختلف در فضای ابری با استفاده از SDN^۱ به‌منظور تخصیص خودکار منابع براساس نیاز می‌باشد و مزیت‌های مختلفی از جمله الف) خودکارسازی بازبازی شکست و دسترسی‌پذیری بالاتر از ۹۹٫۹۹٪، ب) اتصال انعطاف‌پذیر، مقیاس‌پذیر و یکپارچه، پ) خدمات بهتر تبادل اینترنت و مراکز همتایی محتوا و پروتکل اینترنت، ت) مراکز داده بزرگ مقیاس و بی طرفی حامل و ث) پهن‌بند شبکه شهری و گسترده را به‌همراه می‌آورد.

مهاجرت از زیرساخت‌های قدیمی مراکز داده به خدمات ابری مزیت‌های زیادی همچون صرفه‌جویی در هزینه‌ها، یکپارچگی بهتر خدمات، افزایش کیفیت و سرعت ارائه خدمات، فراهم‌سازی ابزارهای پیشرفته تحلیل و ویژگی‌های امنیت سایبری را برای سازمان‌ها فراهم می‌آورد. استفاده از ابرعمومی برای موقعیت‌هایی که تقاضاها غیرقابل پیش‌بینی بوده و یا ویژگی‌های پیشرفته مانند رایانش با هوش مصنوعی یا افزایش امنیت سایبری نیاز باشد، مناسب‌تر است. ابر خصوصی، برای سازمان‌هایی که چارچوب حاکمیتی/ نظارتی بسته‌تری دارند و یا داده‌های حساس را مدیریت می‌کنند، گزینه مناسب‌تری است.

^۱ Software Defined Networking

جدول ۱: مشخصه‌ها و چالش‌های راه‌حل‌های ابری

چالش‌ها	مشخصه‌ها	راه‌حل
• هزینه بالای عملیات و نگهداری (سامانه‌ها و کارکنان)، • تسهیلات اغلب قدیمی، با بهره‌وری پایین و بدون قابلیت گسترش • عدم انعطاف برای پاسخگویی به تقاضای در حال نوسان. • قابلیت‌های امنیتی محدود و گران‌تر	• نیاز به مهارت و تخصص کمتر تیم‌های فناوری اطلاعات • کنترل سخت داده‌ها که الزامات محلی‌سازی داده‌ها را برآورده می‌کند	حفظ سامانه‌های قدیمی فناوری اطلاعات (مرکز داده محلی)
• انعطاف‌پذیری محدود برای پاسخگویی به تقاضای در حال نوسان • امنیت سایبری محدود و نیاز به سرمایه‌گذاری برای تضمین برخی امنیت‌ها • مشکل ساخت مراکز داده سبز در مقیاس کوچک • نیاز به منابع انسانی داخلی با تخصص فنی بالا	• سفرهای ساخت‌افزار، ذخیره‌سازی داده‌ها و اتصال بر اساس نیازها (مانند امنیت) • قابلیت اشتراک منابع در سراسر دولت و صرفه‌جویی در هزینه‌ها • تیم‌های داخلی فناوری اطلاعات • عدم انطباق با مقررات برای داده‌های "فوق سری"	مهاجرت به ابر خصوصی (رایانش ابری در محل)
• قابلیت مشاهده و کنترل به دلیل کمبود ابزار برای نظارت موثر • استقرار ممکن است کاهش یابد • هزینه نگهداری و به‌روز رسانی سامانه‌ها • وابستگی به ارائه‌دهنده خدمات ابری • درجه بالایی از تخصص فنی مورد نیاز	• مقیاس‌پذیری بیشتر ابر خصوصی • هزینه‌های پایین‌تر عملیات، نگهداری و آموزش • افزایش بهره‌وری عملکرد، کارایی و هزینه • گزینه‌های امنیت سایبر بیشتر و بهتر • انطباق با الزامات محلی‌سازی داده‌ها	مهاجرت به ابر خصوصی (میزبانی ارائه دهنده خدمت ابری)
• قابلیت مشاهده و مدیریت خدمات و داده‌ها • تضمین الزامات انطباق حفاظت از داده‌ها برای هر صنعت • قراردادهای سطح خدمات برای تدارکات • تسهیم تهدیدات امنیت در محیط مشترک ابری • وابستگی به یک فروشنده و کاهش نیاز به راه‌حل چند ابری	• مقرون به صرفه بودن و هزینه‌های سرمایه‌ای صفر • بالاترین سطح عملکرد و امنیت سایبری • مقیاس‌پذیری نامحدود • ویژگی‌های پیشرفته مانند امنیت توانمند شده با هوش مصنوعی	مهاجرت به ابر عمومی (ارائه دهنده ابر بزرگ مقیاس)
• مشکلات قابلیت همکاری به دلیل دشواری مدیریت همزمان چندین سامانه ناهمگون • افزایش پیچیدگی به دلیل زیرساخت‌های اضافی • تحمیل هزینه‌ها برای آموزش کارکنان، عملیات و نگهداری • قراردادهای سطح خدمات برای تدارکات	• مزیت‌های ابر عمومی و ابر خصوصی مانند پشتیبانی • دارایی‌های حساس و بارهای کاری با تأخیر کم • مهاجرت تدریجی و زمان‌بندی شده به ابر متناسب با بارهای کاری • انطباق با الزامات محلی‌سازی داده‌ها	به کارگیری ابر ترکیبی (یکپارچگی داده‌ها در ابر خصوصی و ابر عمومی)

مدل ابر ترکیبی با ایجاد توازن میان گزینه‌های ابر عمومی و ابر خصوصی از جمله هزینه‌ها و مزایا و مخاطرات، گزینه بهتری برای بیشتر کاربردها و الزامات در سازمان‌های بخش دولتی می‌باشد. رویکرد ابر عمومی به نهادهای دولتی کمک می‌کند تا پایگاه داده‌های خود را ایمن کرده و سازوکارهای پیشرفته امنیت سایبری را مستقر کنند. رایانش ابر عمومی کارآمد، انعطاف‌پذیر و قابل اعتماد و تقریباً به‌طور نامحدود مقیاس‌پذیر است و همچنین، پتانسیل کاهش قابل توجه انرژی و انتشار کربن را در مقایسه با سایر گزینه‌های ابری دارد.

رویکرد بومی ابر برای ساخت و اجرای کاربردهایی است که به‌طور کامل از مزیت‌های مدل رایانش ابری برای ایجاد و استقرار مولفه‌های برنامه کاربردی بهره می‌برند. کاربردهای بومی ابری با استفاده از ریزخدمات و معماری مبتنی بر کانتینر و مبتنی بر یکپارچه‌سازی فرآیندهای توسعه نرم‌افزار و عملیات فناوری اطلاعات به‌منظور بهبود چابکی و مدیریت‌پذیری توسعه داده می‌شوند.

یکی از الزامات مهم در قابلیت همکاری ابری، استانداردسازی رابط‌ها است که امکان تعویض آسان‌تر میان چندین ارائه‌دهنده خدمات ابری

را برای مشتری فراهم می‌کند. همچنین، قابلیت حمل داده‌ها و توانایی بازیابی داده‌های مشتری از پلتفرم‌های ابری منبع یکی از نکات مهم مرتبط در انتخاب محیط ابری می‌باشد. همچنین، باید توجه داشت که قابلیت همکاری پلتفرم یک نیاز ضروری برای تسهیل قابلیت همکاری برنامه‌ها است و قابلیت همکاری چند ابری باید مدیریت داده‌ها (در حال انتقال و نیز ذخیره شده) را تسهیل کند.

هر چند استانداردهای مختلف برای قابلیت حمل خدمات ابری IaaS وجود دارند، با این وجود سازمان‌ها باید زمان، آموزش و سرمایه‌گذاری مالی قابل‌توجهی را برای جابجایی بارهای کاری خود در میان محیط‌های ابری در نظر بگیرند. چالش‌های تعامل‌پذیری رایانش ابری در خدمات ابر پلتفرم (PaaS) و پلتفرم‌های SaaS به دلیل فقدان استانداردهای رابط بیشتر است. قابلیت حمل داده برای محیط‌های SaaS اهمیت بیشتری دارد و استخراج و پشتیبانی داده‌ها در قالب استاندارد ضروری است.

قابلیت همکاری نیاز به یکپارچگی فنی و اشتراک داده‌ها و درک عمیق‌تری از مالکیت فکری میان ارائه‌دهندگان ابری دارد که در حال حاضر در برابر آن مقاومت می‌شود. راه‌حل‌های چند ابری خطر اختلال در خدمت و از دست دادن داده‌ها را کاهش می‌دهد، با این وجود احتمال قرار گرفتن سامانه‌ها در معرض آسیب‌پذیری‌های امنیتی منفرد را افزایش می‌دهد و تلاش‌ها برای درک، مدل‌سازی و کنترل نمایه‌های ریسک را پیچیده‌تر می‌کند.

فهرست مطالب

۱	۱ مقدمه
۴	۲ همکاری و قابلیت حمل ابری
۶	۱-۲ ملاحظات مرتبط با همکاری ابری
۷	۳ اتصال متقابل مراکز داده
۹	۴ مهاجرت به زیرساخت‌های ابری
۱۱	۱-۴ مزایا و مخاطرات مهاجرت به ابر عمومی
۱۴	۲-۴ رویکرد مهاجرت به ابر
۱۷	۳-۴ چارچوب تصمیم‌گیری مهاجرت به ابر
۱۹	۵ قابلیت همکاری کاربردها در محیط ابر
۲۳	۱-۵ ملاحظات و توصیه‌های کلیدی مرتبط با قابلیت حمل و قابلیت همکاری در محیط ابری
۲۶	۶ چارچوب و نیازمندی‌های بلوغ رایانش ابری
۲۹	۷ رویکرد بومی ابر
۳۰	۱-۷ معماری بومی ابر
۳۱	۲-۷ الزامات بومی ابر
۳۲	۳-۷ اصول معماری برنامه کاربردی بومی ابر
۳۴	۸ نتیجه‌گیری
۳۷	۹ مراجع

۱ مقدمه

کسب و کارها در سرتاسر جهان در تلاش برای بررسی پذیرش راه‌حل‌های مبتنی بر ابر به منظور تحول دیجیتالی خود هستند در نتیجه قابلیت همکاری^۱ چندابری در کنار قابلیت حمل^۲ به عنوان اولویت اصلی کسب و کارهای جهانی ظاهر شده است. تعامل‌پذیری و قابلیت حمل نیازمندی‌های اصلی برای پذیرش سطح بالاتر ابر است و کاربرانی که با ارائه‌دهنده مختلف خدمات ابری سروکار دارند می‌توانند بر پایه این قابلیت‌ها، مدیریت و کنترل بهتری بر خدمات و داده‌های خود داشته باشند.

تعامل‌پذیری ابری، توانایی چند ارائه‌دهنده خدمات رایانش ابری برای تعامل با یکدیگر برای تسهیل تبادل اطلاعات و پیام‌ها است. از سوی دیگر، قابلیت حمل به معنای توانایی جابجایی داده‌ها و برنامه‌ها است. قابلیت حمل داده‌ها در رایانش ابری به توانایی انتقال داده‌ها مانند اسناد، جداول پایگاه داده و فایل‌ها بین سامانه‌های ابری و در عین حال اطمینان از قابلیت استفاده داده‌ها اشاره دارد. قابلیت حمل کاربردها اشاره به توانایی انتقال نرم‌افزارها یا برنامه‌های اجرایی بین سامانه‌های ابری در عین حصول اطمینان از قابلیت استفاده در سامانه‌های مقصد دارد.

درک قابلیت همکاری (تعامل‌پذیری) و قابلیت حمل ابری یک گام اساسی در فرآیند برنامه‌ریزی و طراحی خدمات و برنامه‌های کاربردی جدید ابری است و کسب و کارها براساس آن می‌توانند مسیر ایده‌آل برای برنامه‌ریزی راه‌حل‌های ابری خود را شناسایی کنند. همچنین، دغدغه‌های خاص در مورد قابلیت همکاری و قابلیت حمل می‌تواند به شناسایی ویژگی‌هایی که بهترین تناسب را برای راه‌حل‌های جدید مبتنی بر ابر ارائه می‌کنند، کمک کند.

برای قابل حمل بودن، مشتریان بالقوه علاقه‌مند هستند که بدانند آیا می‌توانند داده‌ها یا برنامه‌های کاربردی خود را در چندین محیط ابری با هزینه کم و حداقل اختلال منتقل کنند. از منظر تعامل‌پذیری، کاربران نگران توانایی برقراری ارتباط با چند ابر یا ارتباط در میان چند ابر هستند.

افزایش سهم و نقش شبکه ملی اطلاعات و اقتصاد رقومی (دیجیتال) و اصلاح نظام اداری مبتنی بر هوشمندسازی دولت دو هدف اصلی تعیین شده در برنامه هفتم توسعه کشور در بازه زمانی سال ۱۴۰۳ تا سال ۱۴۰۷ می‌باشند. در فصل ۱۳ برنامه با عنوان توسعه شبکه ملی اطلاعات و اقتصاد رقومی (دیجیتال) و در ذیل ماده ۶۶ به منظور افزایش سهم اقتصاد رقومی (دیجیتال) از تولید ناخالص ملی به اقدامات زیر اشاره گردیده است.

در بند ب ماده ۶۶، وزارت ارتباطات و فناوری اطلاعات موظف است با مشارکت و سرمایه‌گذاری بخش غیردولتی از طریق سازمان توسعه‌ای زیرمجموعه خود نسبت به تأمین زیرساخت‌های لازم برای توسعه اقتصاد رقومی (دیجیتال)، اعم از ارتباطی و اطلاعاتی (ابری) و ذخیره‌سازی و پردازش سریع برای حضور و رقابت در بازارهای داخلی و بین‌المللی، اقدام نماید.

در بند ج این ماده، وزارت ارتباطات و فناوری اطلاعات مکلف است با رعایت قانون مدیریت داده‌ها و اطلاعات ملی به منظور فراهم کردن و تسهیل نوآوری‌های مبتنی بر داده‌ها در خدمات و محصولات، دسترسی کسب و کارهای رقومی (دیجیتال) به داده‌ها و اطلاعات مورد نیاز را از طریق مرکز ملی تبادل اطلاعات با حفظ امنیت داده‌های شخصی فراهم نماید. در تبصره این بند وزارت ارتباطات و فناوری اطلاعات مکلف است ظرف سه ماه از لازم‌الاجرا شدن این قانون اقدامات قانونی لازم را برای تدوین «سند

^۱ Interoperability

^۲ Portability

سیاست‌ها و الزامات حفاظت و حمایت از داده‌های شخصی» انجام دهد.

انتقال زیرساخت‌های سازمانی به فضای ابری نه تنها یک تحول فناوری محور است، بلکه تحولی در ساختار کسب و کار است. دسترسی به راه‌حل‌های نرم‌افزاری نوآورانه و پیشرفته در کنار کاهش نیازها برای سرمایه‌گذاری در مدیریت و نگهداری زیرساخت‌ها، رویکرد و نقش کسب و کارها را تغییر می‌دهد. فناوری در مرکز نیازهای کاربران و متمرکز بر ارزش کسب و کار برای سازمان است.

در فصل ۲۳ برنامه با عنوان اصلاح نظام اداری در بخش هوشمندسازی و دولت الکترونیک و ذیل ماده ۱۰۷، دستگاه‌های اجرائی موظف شده‌اند تا با رعایت مواد (۷) و (۱۰) قانون مدیریت داده‌ها و اطلاعات ملی و قانون تسهیل صدور مجوزهای کسب و کار اقدامات زیر را به منظور هوشمندسازی و تحقق دولت الکترونیک انجام دهند.

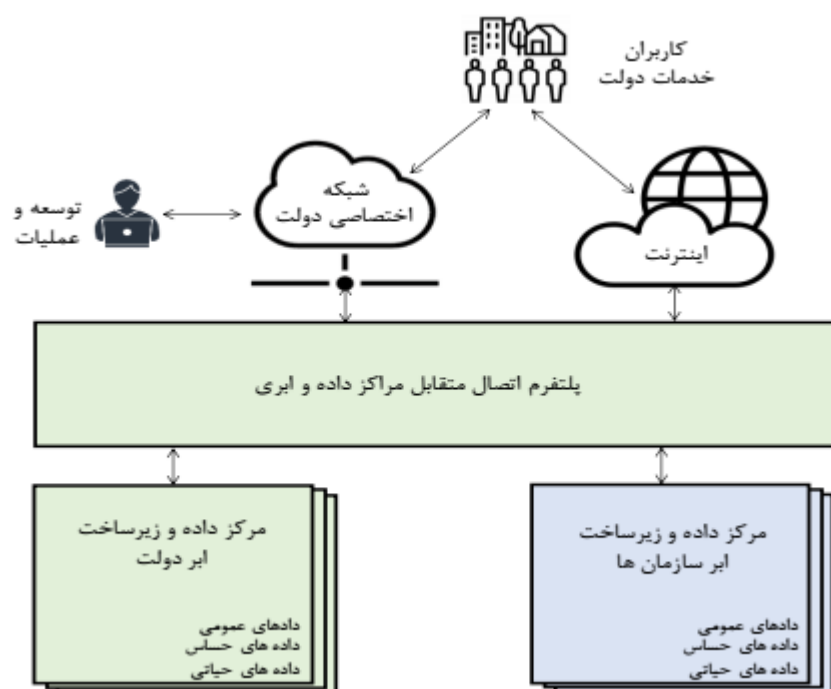
در بند الف ماده ۱۰۷، دستگاه‌های اجرائی موظف شده‌اند تا مراکز داده اصلی و پشتیبان خود را به زیرساخت یکپارچه ابری دولت‌هوشمند متصل نمایند. آیین‌نامه اجرائی این بند مشتمل بر اتصال دستگاه‌های مذکور و انتقال داده دستگاه‌های زیرمجموعه قوه مجریه و نیز انتقال داده سایر دستگاه‌ها در صورت موافقت آنها و زمان‌بندی و شیوه انجام آن توسط وزارت ارتباطات و فناوری اطلاعات با همکاری وزارت اطلاعات تهیه می‌شود و به تصویب هیأت وزیران می‌رسد. در این بند وزارت ارتباطات و فناوری اطلاعات موظف است تا پایان سال اول برنامه با اولویت استفاده از الگوی مشارکت عمومی- خصوصی نسبت به ایجاد، تقویت و استقرار زیرساخت یکپارچه ابری دولت‌هوشمند اقدام نماید.

ماده ۷ قانون مدیریت داده‌ها و اطلاعات ملی اشاره به نقش مرکز ملی تبادل اطلاعات در تبادل داده‌ها و اطلاعات بین دستگاه‌ها و نهادها دارد. ماده ۱۰ قانون مدیریت داده‌ها و اطلاعات، ۲۷ پایگاه داده و اطلاعات ملی (پایه) و متولیان اداره و به‌روز رسانی آنها بر اساس مصوبات کارگروه تعامل‌پذیری دولت الکترونیک را مشخص می‌کند.

در بند ث ماده ۱۰۷، دستگاه‌های اجرائی موظف شده‌اند تا اقدامات لازم را برای توسعه دولت‌هوشمند به‌منظور ارتقای شاخص‌های ملی و بین‌المللی از جمله شاخص بین‌المللی توسعه دولت الکترونیک با رعایت قانون مدیریت داده‌ها و اطلاعات ملی اجرا نمایند. وزارت ارتباطات و فناوری اطلاعات با همکاری سازمان اداری و استخدامی کشور مکلف است، دستورالعمل و ضوابط مربوطه را تهیه و ابلاغ نماید.

اتصال داخلی مرکز داده (DCI)^۱، سازوکاری برای اتصال مراکز داده یا ابری به یکدیگر است و به‌عنوان مولفه مرکزی مدل‌های کسب و کاری جدید در نظر گرفته می‌شود. ایجاد اتصال مناسب میان مراکز داده یکی از الزامات کلیدی در رشد و چابکی مقیاس‌پذیر زیرساخت‌های اطلاعاتی سازمان‌های دولتی است. با توجه به گستردگی حوزه‌های عملکردی و خدمات دولت الکترونیک، اتصال مرکز داده به یکدیگر یک جزء سازنده کلیدی در ایجاد زیرساخت یکپارچه خدمات دولت و اتصال مشتریان و شرکای زیست بوم می‌باشد. در این راستا، به‌کارگیری فناوری‌های نوین از جمله اتصال تعریف‌شده نرم‌افزاری می‌تواند مراکز داده موجود را به یک دارایی راهبردی در توسعه خدمات ابری دولت تبدیل نماید.

۱ Data Center Interconnect (DCI)



شکل ۲: اتصال مراکز داده سازمان‌ها به زیرساخت یکپارچه ابر دولت

بطور کلی سازمان‌های دولتی توجه کمتری به نقش و کارکردهای مرکز داده در کسب و کار داشته و تمامی تلاش‌های خود را بر توسعه و ارائه خدمت به مشتریان منعطف می‌نمایند. ابتکارات بهینه‌سازی مرکز داده و ملزومات دیجیتال می‌تواند سازمان‌های دولتی را به سوی مدرن‌سازی زیرساخت‌های دولت هوشمند سوق دهد. با این وجود زیرساخت‌های یکپارچه فناوری اطلاعات در سازمان‌ها مانع از این امر می‌شود. یک پلتفرم ارتباط متقابل مرکز داده می‌تواند به عنوان عامل تسهیل‌گر برای بهینه‌سازی دارایی‌های فناوری اطلاعات موجود و همچنین پاسخگویی نیازمندی‌های روزافزون کیفیت و امنیت خدمات و داده‌ها در آینده باشد. اتصال مراکز داده سازمان‌ها به زیرساخت‌های یکپارچه ابری مزیت‌های کاهش انرژی مصرفی مراکز داده، کاهش هزینه سخت‌افزار، نرم‌افزار و عملیات، افزایش امنیت فناوری اطلاعات، به‌کارگیری فناوری‌ها و پلتفرم‌های رایانشی کارآمدتر، دستیابی درجه بالاتری از مقیاس و انعطاف‌پذیری، کنترل دقیق‌تر داده‌ها و برنامه‌ها و تمرکز بیشتر فعالیت‌های سازمان بر توسعه خدمات و کسب و کار را به همراه خواهد داشت.

توسعه زیرساخت‌های ارتباطی و اطلاعاتی (ابری) شبکه ملی اطلاعات، توسعه زیرساخت‌های ابری دولت هوشمند، اتصال مراکز داده سازمان‌ها به زیرساخت یکپارچه ابر دولت و مهاجرت سازمان‌های دولتی به فضای ابری از جمله موضوعاتی است که در برنامه هفتم توسعه به آنها اشاره شده است. تحقق هریک از این اهداف مستلزم شناسایی نیازمندی‌های تعامل‌پذیری ابری و پذیرش ابر می‌باشد. در این گزارش به‌منظور شناسایی نیازمندی‌های همکاری سامانه‌ها و خدمات در محیط چند ابری در ابتدا مفاهیم و ملاحظات مرتبط با همکاری و قابلیت حمل در یک زیست‌بوم ابری و همچنین الزامات در سطح اتصال متقابل مراکز داده بررسی می‌شود. در ادامه با مرور رویکرد و چارچوب‌های مهاجرت به زیرساخت‌های ابر عمومی و نیازمندی‌های بلوغ و تکامل خدمات رایانش ابری، چالش‌های مرتبط با دسترسی‌پذیری و قابلیت استفاده خدمات و داده‌ها در محیط ابر شناسایی می‌شود. در انتها، مفهوم بومی ابر بررسی گردیده و نیازمندی‌های مرتبط با معماری برنامه‌های کاربردی در محیط ابری معرفی می‌شود.

۲ همکاری و قابلیت حمل ابری

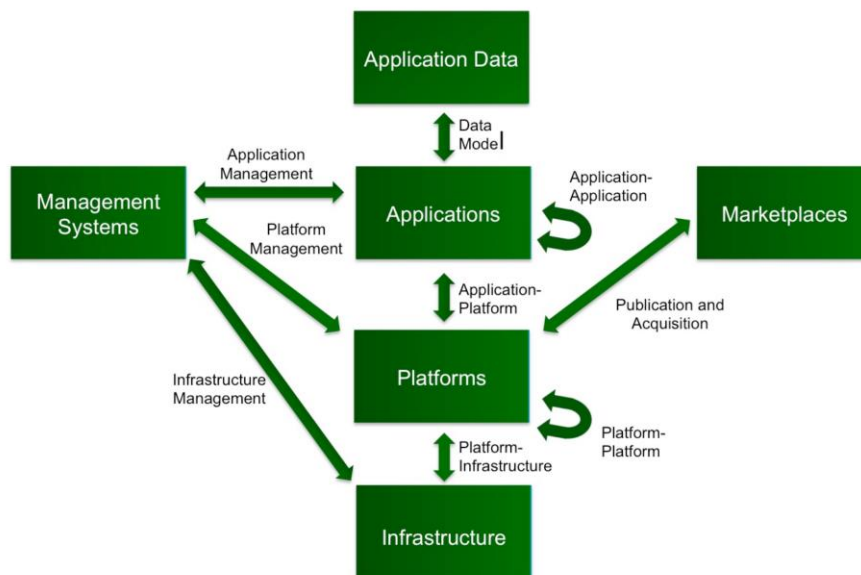
قابلیت همکاری به مفهوم توسعه‌ای است که در آن سامانه‌ها و اجزای مختلف یک زیست‌بوم ابری می‌توانند در هماهنگی با یکدیگر کار کنند. براساس تعریف IEEE و ISO، قابلیت همکاری توانایی تسهیل تبادل اطلاعات یکپارچه بین دو یا چند سامانه و برنامه‌های مبتنی بر ابر است [۱]. تعامل‌پذیری ابری بر اساس استاندارد ISO/IEC ۱۹۹۴۱، توانایی سامانه مشتری برای تعامل با یک خدمت ابری یا توانایی یک خدمت ابری برای تعامل با سایر خدمات ابری از طریق تبادل اطلاعات براساس یک روش تجویز شده است.

قابلیت همکاری نشان‌دهنده توانایی بالقوه خدمات ابر عمومی و خصوصی در کنار سایر سامانه‌ها در زیست‌بوم ابری برای درک یکدیگر است. قابلیت همکاری می‌تواند درک رابط‌های برنامه و خدمات، روش‌های احراز هویت، رویکردهای مجوز و تنظیمات را تسهیل کند. در بیشتر موارد اجزای تعامل‌کننده متعلق به مشتریان خدمات ابری هستند و مشتریان از قابلیت همکاری برای تعامل با زیرساخت و خدمات ارائه‌دهندگان خدمات ابری استفاده می‌کنند. یکی از جنبه‌های اصلی قابلیت همکاری به استانداردسازی رابط‌ها اشاره دارد که امکان تعویض آسان‌تر میان چندین ارائه‌دهنده خدمات ابری را فراهم می‌کند.

تعیین کاربردهای حمل رایانش ابری در کسب و کار مستلزم درک تعریف قابل حمل بودن است. قابلیت حمل رایانش ابری به توانایی مشتریان خدمات ابری برای جابجایی و تطبیق داده‌ها و برنامه‌های کاربردی خود در میان پلتفرم‌های مختلف خدمات ابری اشاره دارد. علاوه بر این قابلیت حمل می‌تواند تبادل داده‌ها و برنامه‌های کاربردی را در بین مدل‌های مختلف استقرار ابری امکان‌پذیر نماید.

قابلیت حمل داده‌ها: بر اساس استاندارد ISO/IEC ۱۹۹۴۱، قابلیت جابجایی داده‌های ابری به معنای توانایی انتقال آسان داده‌ها از یک خدمت ابری به خدمت ابری دیگر یا بین سامانه مشتری خدمت ابری و خدمت ابری، در یک قالب الکترونیکی رایج است. قابلیت حمل داده‌های ابری بر توانایی انتقال یکپارچه داده‌ها از یک پلتفرم ابری به پلتفرم دیگر تاکید دارد. علاوه بر این، ابزارهای رایج قابل حمل می‌توانند تبدیل ساده و آسان بین فرمت‌های داده ناسازگار را تسهیل کنند. یکی از نکات مهم مرتبط با قابلیت حمل داده‌های رایانش ابری، توانایی بازیابی داده‌های مشتری از پلتفرم‌های ابری منبع می‌باشد، در عین حال، قابلیت حمل بر توانایی وارد کردن داده‌های مشتری به پلتفرم ابری مورد نظر نیز متکی است.

قابلیت حمل برنامه: هدف اصلی قابلیت حمل برنامه‌های ابری بر انتقال آسان‌تر برنامه‌ها یا اجزای برنامه بین خدمات ابری و فراهم‌آوردندگان چندگانه ابری است. با استفاده از این قابلیت، می‌توان برنامه‌ها را باز کامپایل کرده یا با خدمات ابری مورد نظر پیوند مجدد داد بدون آنکه نیازی به ایجاد تغییرات گسترده در منطق برنامه باشد.



شکل ۳: قابلیت همکاری و قابلیت حمل ابری [۱]

قابلیت همکاری برنامه: امکان همکاری بین اجزای برنامه را فراهم می‌کند. اجرای برنامه می‌تواند بخشی از برنامه‌های غیرمتمرکز یا یک برنامه یکپارچه باشد. در رویکرد طراحی اولیه قابلیت همکاری برنامه‌ها، هدف اصلی بهبود دیده شدن و شفافیت داده‌ها است. علاوه بر این، قابلیت همکاری چند ابری باید مدیریت داده‌های در حال انتقال و داده‌های ذخیره شده را تسهیل کند. قابلیت همکاری برنامه‌ها همچنین باید بر شناسایی الزامات مدیریت منابع «سامانه ثبت» تمرکز کند.

قابلیت همکاری پلتفرم: به قابلیت همکاری بین اجزای پلتفرم اشاره دارد و به پروتکل‌های استاندارد برای تسهیل کشف خدمت و تبادل اطلاعات نیاز دارد. همچنین باید توجه داشت که قابلیت همکاری پلتفرم یک نیاز ضروری برای تسهیل قابلیت همکاری برنامه‌ها است. در حال حاضر تعداد کمی از برنامه‌ها از شناسایی خدمت استفاده می‌کنند و تمرکز بر اطمینان از حداکثر بلوغ یکپارچه‌سازی خدمت ضروری است. پروتکل‌های شناسایی خدمت باید با پلتفرم‌هایی که توسط ثبت خدمات و برنامه‌های مختلف استفاده می‌شوند، سازگار باشند. از سوی دیگر، پروتکل‌های تبادل اطلاعات باید انتقال اطلاعات جلسه، انتقال اطلاعات و توسعه نشست^۱ را امکان‌پذیر کنند.

قابلیت همکاری مدیریت: یکی از جنبه‌های مهم در قابلیت همکاری محیط‌های ابری است و به قابلیت همکاری در میان خدمات ابری و نرم‌افزارهایی اشاره دارد که اجزای برنامه‌های کاربردی خودخدمت بر اساس تقاضا را کنترل می‌نمایند. قابلیت همکاری انتشار و اکتساب^۲: به قابلیت همکاری بین پلتفرم‌ها اشاره دارد. به‌طور کلی، ارائه‌دهندگان خدمات ابری از بازارها برای انتشار خدمات ابری و اجزای مرتبط خود استفاده می‌کنند. با در دسترس بودن رابط‌های استاندارد برای این بازارها، قابلیت همکاری می‌تواند هزینه‌های رایانش ابری کمتر را تضمین کند.

^۱ session

^۲ acquisition

۲-۱ ملاحظات مرتبط با همکاری ابری

شناسایی چالش‌های مربوط به قابلیت همکاری و قابلیت حمل در زیست‌بوم ابری ضروری است. اکثر رابط‌های برنامه‌نویسی کاربردی خدمات ابری فاقد استانداردسازی هستند و ارائه‌دهندگان مختلف از رابط‌های منحصر به فرد استفاده می‌کنند. بالاترین قابلیت همکاری رایانش ابری در خدمات ابری IaaS^۱ وجود دارد جایی که چندین رابط استاندارد وجود دارد. از سوی دیگر، مورد‌های استفاده تعامل‌پذیری رایانش ابری در خدمات ابری PaaS^۲ به دلیل فقدان استانداردهای رابط، کمتر است. همچنین چالش‌های قابلیت همکاری در پلتفرم‌های SaaS^۳ به دلیل عدم وجود رابط‌های استاندارد بیشتر است. حمل برنامه‌های کاربردی همچنین به چالش‌های قابل توجهی برای برنامه‌های مبتنی بر PaaS اشاره دارد. خدمات ابری IaaS می‌توانند از استانداردهای مختلفی مانند OVF^۴ برای قابلیت حمل استفاده کنند [۲].

استانداردها و ابزارهای پذیرش ناقص: استانداردها و ابزارهای موجود پذیرش قابلیت حمل و قابلیت همکاری (به عنوان مثال، مبدل‌های پروتکل، مترجم‌ها و شبیه‌سازهای محیط نرم‌افزار) برای توانمند کردن انعطاف‌پذیری مورد نیاز مشتریان سازمانی و جبران کامل خطر اختلال در خدمات کافی نیستند. این امر مانع ایجاد رویکردهای کافی برای فعال کردن تبادل و مهاجرت داده‌ها و/یا برنامه‌های میزبانی شده در فضای ابری می‌شود. علاوه بر این، قبل از اینکه استانداردهای کافی و ابزارهای پذیرش حضور قابل توجهی در بازار پیدا کنند، یک دوره انتقال طولانی‌تر رخ خواهد داد و تلاش‌ها برای کاهش چالش‌های اختلال در خدمات را بیشتر به تأخیر می‌اندازد [۳].

دشوار بودن عملیاتی کردن قابلیت حمل: حتی اگر ارائه‌دهندگان ابر قابلیت حمل را فعال و پشتیبانی کنند، مشتریان باید زمان، آموزش و سرمایه‌گذاری مالی قابل توجهی (به عنوان مثال، خرید مجوزهای تکراری نرم‌افزار) را در نظر بگیرند تا با موفقیت بار کاری را بین محیط‌های ابری جابجا کنند. علاوه بر این، حتی اگر بتوانند این سرمایه‌گذاری‌ها را انجام دهند، ممکن است نیاز داشته باشند که داده‌ها را به قالب‌های دیگر (برای سازگاری با محیط جدید) تبدیل کنند و اطمینان حاصل کنند که همان سیاست‌های مدیریت هویت، امنیت و حریم خصوصی در این محیط جدید اعمال می‌شود. این عوامل مانع سازمان‌ها برای انتقال سریع داده‌ها در پاسخ به یک حادثه می‌شود.

موانع قابلیت همکاری: قابلیت همکاری نیاز به یکپارچگی فنی و اشتراک داده‌ها و درک عمیق‌تری از مالکیت فکری میان ارائه‌دهندگان ابری دارد که ممکن است در برابر آن مقاومت شود. علاوه بر این، ممکن است تقاضای مشتری نسبتاً کمتری برای قابلیت همکاری وجود داشته باشد، زیرا به نظر می‌رسد قابلیت حمل انعطاف‌پذیری و چابکی مورد نظر مشتریان را فراهم می‌کند. در معرض خطرات امنیتی قرار گرفتن مشتریان با قابلیت همکاری: اگرچه به نظر می‌رسد اتکاء به چندین ارائه‌دهنده ابری، خطر اختلال در خدمت و از دست دادن داده‌ها را کاهش دهد، با این وجود این امر همچنین سطح تماس سامانه مشتری و احتمال قرار گرفتن در معرض آسیب‌پذیری‌های امنیتی منفرد را افزایش می‌دهد. علاوه بر این وابستگی به ارائه‌دهندگان ابری و سایر طرف‌های

^۱ Infrastructure as a Service

^۲ Platform as a Service

^۳ Software as a Service

^۴ Open Virtualization Format

سوم، تلاش‌ها برای درک، مدل‌سازی و کنترل نمایه‌های ریسک آن‌ها را پیچیده می‌کند، زیرا مشتریان نگران امنیت سرتاسری خواهند بود، در حالی که هر ارائه‌دهنده ممکن است فقط به دنبال ایمن کردن پیشنهاد خود باشد.

ظهور ارائه‌دهندگان تخصصی: تعامل‌پذیری و قابلیت حمل بیشتر ممکن است درآمد یک ارائه‌دهنده را کاهش دهد. در نتیجه، حداقل برخی از ارائه‌دهندگان ممکن است از تلاش‌ها برای افزایش و گسترش این قابلیت‌ها پشتیبانی نکنند. با این حال، با افزایش تقاضای مشتری برای قابلیت حمل و قابلیت همکاری، طیفی از ارائه‌دهندگان تخصصی در حال ظهور هستند تا این شکاف را پر کنند و رشد را در بازار کلی خدمات ابری افزایش دهند.

مسئولیت‌های مشترک هنگام انتقال داده‌ها: طرف‌های چندگانه در انتقال داده‌ها دخیل هستند و در نتیجه مسئولیت‌های زیادی برای حفظ امنیت و حفظ حریم خصوصی داده‌ها را هنگام انتقال داده‌ها از محیطی به محیط دیگر به اشتراک می‌گذارند. طرف‌های ذی‌نفع به ویژه مشتریان، ممکن است همیشه از مسئولیت‌های خود آگاه نباشند یا آن را درک نکنند.

مدل‌های مختلف خدمات ابری ممکن است الزامات مختلف در ارتباط با قابلیت حمل و تعامل‌پذیری داشته باشند. به عنوان مثال، IaaS به توانایی انتقال داده‌ها و اجرای برنامه‌های کاربردی در یک ابر جدید نیاز دارد. بنابراین، گرفتن تصاویر ماشین مجازی و مهاجرت به فراهم‌کنندگان ابری جدید که ممکن است از فناوری‌های مجازی‌سازی مختلف استفاده کنند، ضروری است. هر گونه افزودنی خاص فراهم‌کننده^۱ برای تصاویر ماشین‌های مجازی^۲ باید پس از انتقال، حذف یا ضبط شود. در حالی که برای محیط‌های SaaS، قابلیت حمل داده اهمیت بیشتری داشته و بنابراین انجام استخراج و پشتیبانی داده‌ها در قالب استاندارد ضروری است [۴].

۳ اتصال متقابل مراکز داده

اصطلاح فرامقیاس^۳ مترادف با مکان‌های عظیمی است که سرورهای بی‌شماری را در تسهیلات به‌ظاهر بی‌پایان خود جای می‌دهند. مفهوم فرامقیاس به‌طور فزاینده‌ای نه تنها برای تعریف بزرگی و اندازه این مراکز داده، بلکه همچنین برای توصیف معماری خاص آنها استفاده می‌شود. فراتر از ردپا و تعداد سرورها، معماری این مراکز برای سیدکاری کاربردهای سبز در مقیاس همگن طراحی می‌شود که به‌طور فزاینده‌ای از زیرساخت‌های تفکیک‌شده، با چگالی بالا و انرژی بهینه‌شده بهره می‌برد.

یک فرامقیاس باید خدمات تقریباً بی‌عیب و نقصی را به میلیون‌ها مشتری ارائه دهد. با وجود مزایای رایانش سفارشی شده، شبکه‌های پرسرعت و نرم‌افزارهای پیشرفته مجازی‌سازی، که املاک و مستغلات بیشتری را در مقایسه با یک فضای شهری اشغال می‌کند، هیچ مرکز داده مستقلی نمی‌تواند این خواسته‌های مشتری را برآورده کند. در الگوواره^۴ جدید فرامقیاس، راه‌حل‌های اتصال مرکز داده، عنصر اتصال بین همه‌ی مکان‌ها را فراهم می‌کند و یک مجموعه بزرگ را قادر می‌سازد تا به عنوان یک موجودیت رفتار کند [۵].

تقاضای روزافزون برای مرکز داده و مجازی‌سازی شبکه پیامدهای خود را بر اتصال مرکز داده دارد. این امر بر معماری شبکه ارائه

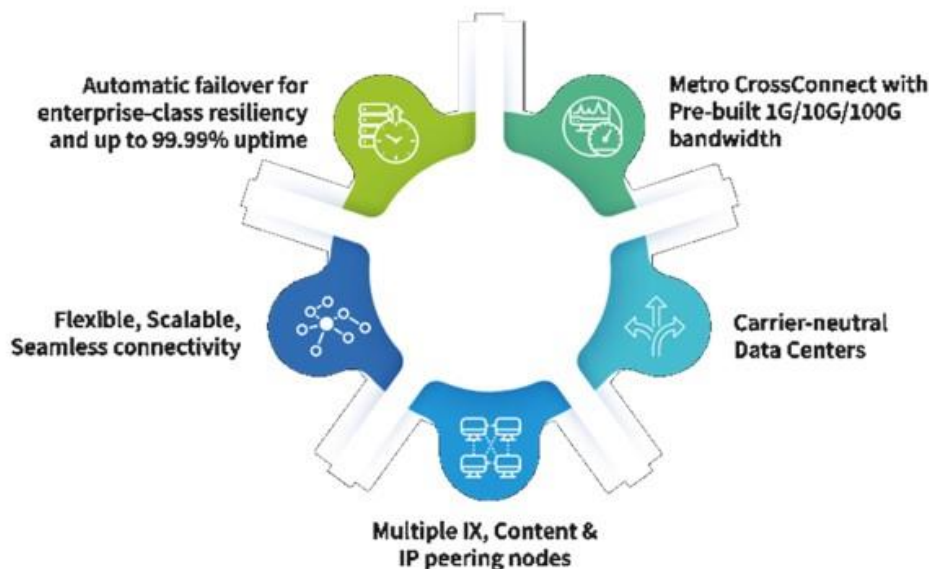
^۱ provider-specific extensions

^۲ virtual machines Images

^۳ Hyperscale

^۴ Paradigm

دهندگان ابری تاثیر گذاشته و تمرکز آن بر اشتراک بار و بارهای کاری توزیع شده را ضروری می‌نماید. اتصال متقابل مرکز داده همچنین راهی برای اتصال مراکز داده مختلف در فضای ابری با استفاده از SDN^۱ به منظور تخصیص خودکار منابع بر اساس نیاز می‌باشد [۶].



شکل ۴: مزیت‌های اتصال متقابل مراکز داده [۷]

فناوری اتصال مرکز داده (DCI) دو یا چند مرکز داده را برای تبادل یکپارچه داده‌ها به هم متصل می‌کند و همچنین پشتیبانی برای افزونگی فراهم می‌کند. اتصال مرکز داده شرکت‌ها را قادر می‌سازد تا به صورت پویا از منابع فیزیکی و مجازی در چندین سایت استفاده کنند و در صورت لزوم بار زیرساخت شبکه خود را متعادل نمایند. مفهوم اتصال مرکز داده، به فناوری مورد استفاده برای پیوند دو یا چند مرکز داده منفرد به منظور تجميع منابع، متعادل کردن بار کاری، نسخه‌برداری داده‌ها یا اجرای طرح‌های بازیابی فاجعه و فراهم‌آوری داده‌های تجاری نزدیک‌تر به لبه اشاره دارد. هر چند اتصال مرکز داده در گذشته امری ساده بود، اما به دلیل پیشرفت‌های فراوان فناوری و در دسترس بودن گزینه‌های مختلف، سردرگمی زیادی در بازار وجود دارد [۷].

استقرار سریع و استفاده از راه‌حل‌های اتصال، روشی کارآمد برای حفظ مقیاس‌پذیری و تطبیق‌پذیری بدون افزودن ظرفیت سرور یا زیرساخت‌های فیزیکی است. اتکاء به فناوری حیاتی اتصال مراکز داده برای اتصال‌های شهری و مسافت‌های طولانی، آسیب‌پذیری را در برابر نفوذهای خارجی، شکستگی‌های تصادفی یا قطع ارتباط افزایش می‌دهد که می‌تواند منجر به قطعی‌های پرهزینه شود. به همین دلیل، راه‌حل‌های نظارت بر فیبر و راه‌حل‌های نظارت بر عملکرد، ابزارهای ضروری برای محافظت از اتصال مراکز داده به روشی فعال و جهت به حداقل رساندن میانگین زمان تعمیر (MTTR)^۲ هستند.

اگرچه اتصال مراکز داده یک جزء جدایی ناپذیر از معماری مرکز داده است، اما یک موجودیت مستقل با ملاحظات آزمون و قابلیت اطمینان منحصر به فرد خود است و بنابراین نیاز به راه‌حل‌های خاص خود دارد. چالش‌های زیادی برای اتصال متقابل مراکز داده وجود دارد که باید بر آنها غلبه کرد.

^۱ Software Defined Networking

^۲ Mean Time To Repair

فاصله: کاربردهای اتصال مراکز داده از نظر اندازه و دامنه برای مراکز داده‌ای که ممکن است در سراسر جهان یا منطقه شهری یا در سراسر یک کشور پراکنده باشند، بسیار متفاوت است. بنابراین، حمل بیشتر بیت‌ها در دورترین فاصله بسیار مهم است، اما وقتی فاصله افزایش می‌یابد تأخیر نیز افزایش می‌یابد. در حالی که انتخاب کوتاه‌ترین مسیر ممکن است تأخیر را به حداقل برساند، تجهیزات نامناسب نیز ممکن است منجر به تأخیر شود.

ظرفیت اتصال: مراکز داده کاربردها را ذخیره و تحویل می‌دهند. مجموعه داده‌هایی که به یک مرکز وارد یا از آن خارج می‌شوند ممکن است بسیار بزرگ باشند. محدوده ممکن است از چند صد گیگابایت تا ترابایت متفاوت باشد. برای مدیریت چنین داده‌های بزرگ، تجهیزات باید اتصالات قابل اعتماد و با ظرفیت بالا را عرضه نمایند. معماری مرکز داده همچنین باید مقیاس مورد نیاز برای رسیدگی به جهش‌های نیازمندی‌ها را تضمین کند.

امنیت داده‌ها: مراکز داده حجم زیادی از اطلاعات حیاتی را ذخیره می‌کنند. این امر نیازمند اتصالات مرکز داده قابل اعتماد، ایمن و رمزگذاری شده است تا از رخنه‌های پرهزینه و همچنین از دست دادن داده‌ها جلوگیری شود. در حالی که امنیت داده‌های ذخیره شده بسیار مهم است، توجه به امنیت داده‌های در حال انتقال از اهمیت بیشتری برخوردار است.

عملیات خودکار: عملیات دستی نیازمند کار دستی فشرده، پیچیده، کند و همچنین مستعد خطا است. بنابراین بسیار ضروری است که پیچیدگی و سرعت کمتر اتصال ناشی از عملیات دستی با حرکت به سمت خودکارسازی به حداقل برسد. ایجاد ارتباط میان مراکز داده نباید زمان زیادی را صرف کرده و نیازی به عملیات دستی مداوم داشته باشد.

افزایش هزینه‌ها: جریان‌سازی داده‌های حجیم در میان مراکز داده باید به روشی مقرون به صرفه انجام شود. برای اینکه مراکز داده قابل دوام باقی بماند، هزینه‌ها نباید مانند پهنای باند افزایش یابد. برای رسیدگی به این مسائل، راه‌حل‌های شبکه‌سازی پرسرعت باید رویکردهایی را معرفی نمایند که مراکز داده را با کمترین هزینه برای هر بیت به هم متصل کند.

۴ مهاجرت به زیرساخت‌های ابری

مهاجرت از زیرساخت‌های قدیمی فناوری اطلاعات و ذخیره‌سازی داده‌ها به خدمات ابری می‌تواند برای دولت‌ها مزایای زیادی همچون صرفه‌جویی در پول دولت‌ها؛ افزایش یکپارچگی، کیفیت و سرعت ارائه خدمات و فراهم‌سازی دسترسی به پیشرفته‌ترین ابزارهای تحلیلی و ویژگی‌های امنیت سایبری موجود داشته باشد. این مزایا باعث شده تا دولت‌ها در سراسر جهان از سامانه‌های قدیمی فناوری اطلاعات (IT) دور شوند و به سمت راه‌حل‌های ابری، از جمله خدمات ابر عمومی، حرکت کنند [۸].

گسترده‌ترین تعریف معماری ابری دربرگیرنده نرم‌افزارها، خدمات و برنامه‌هایی (از جمله ذخیره‌سازی) است که به صورت محلی میزبانی نمی‌شوند و برای تسهیل رایانش به اتصال به اینترنت نیاز دارند. ارائه‌دهندگان ابر شامل ارائه‌دهندگان ابر خصوصی، ارائه‌دهندگان ابر عمومی ملی یا منطقه‌ای و ارائه‌دهندگان خدمات ابر مقیاس بزرگ هستند. در حال حاضر تعداد روزافزونی از نرم‌افزارهای پیچیده نرم‌افزار به عنوان خدمت (SaaS) و برنامه‌های کاربردی تجاری پلتفرم به عنوان خدمت (PaaS) برای حل چالش‌های خاص بخش عمومی از طریق این راه‌حل‌های ابر عمومی و خصوصی مانند پلتفرم‌های ثبت نام، صورت حساب و همکاری

تیم مجازی، یا برنامه‌های پیچیده‌تر مانند مدیریت ارتباط با مشتری، ابزارهای انرژی و داشبوردهای پایداری^۱ برای پشتیبانی از اهداف تاب‌آوری و انتقال سبز (مدیریت مصرف انرژی، ردپای کربن و ...) در دسترس هستند.

گزینه ابر عمومی زمانی مناسب‌تر است که یک نهاد بخش عمومی به دنبال افزایش کارایی هزینه بدون متحمل شدن هزینه‌های سرمایه اولیه باشد، زمانی که اوج تقاضا غیرقابل پیش‌بینی است، یا زمانی که نیاز به ویژگی‌های پیشرفته مانند رایانش با هوش مصنوعی یا افزایش امنیت سایبری وجود دارد. ابر خصوصی ممکن است برای نهادهای مناسب‌تر باشد که توسط یک چارچوب نظارتی محدودتر اداره می‌شود، داده‌های حساس را مدیریت می‌کند یا می‌تواند به‌طور مداوم روی فناوری با عملکرد بالا و پرسنل فناوری اطلاعات واجد شرایط سرمایه‌گذاری کند.

اکثر نهادهای بخش دولتی یک مدل ابر ترکیبی را انتخاب می‌کنند که شامل خدمات ابر عمومی و خصوصی برای کاربردها و الزامات مختلف می‌شود، که منعکس‌کننده مبادله بهینه بین هزینه‌ها، مزایا و مخاطرات است. عوامل خاص، تصمیم‌گیری را در خصوص تعادل بین گزینه‌های ابر عمومی و خصوصی بیشتر می‌کند.

جدول ۲: مزیت‌ها و چالش‌های مراکز داده محلی و گزینه‌های مختلف ابری

راه‌حل	مشخصه‌ها	چالش‌ها
مرکز داده	کنترل سخت داده‌ها که الزامات محلی‌سازی داده‌ها را برآورده می‌کند	• هزینه نگهداری و به‌روزرسانی سامانه‌ها • کارایی و ظرفیت محدود برای ادغام سریع برنامه‌های کاربردی پیشرفته و نوآوری • امنیت سایبری محدود و سامانه‌های ایمن گران‌تر • مشکل ساختن مراکز داده سبز در مقیاس کوچک • درجه بالایی از تخصص فنی داخلی مورد نیاز، از جمله هزینه‌های آموزش منظم
ابر خصوصی ON-PREM	• صرفه جویی در هزینه اگر در سراسر دولت به اشتراک گذاشته شود • کنترل سخت داده‌ها که الزامات محلی‌سازی داده‌ها را برآورده می‌کند	• هزینه نگهداری و به‌روزرسانی سامانه‌ها • امنیت سایبری محدود و سامانه‌های ایمن گران‌تر • مشکل ساختن مراکز داده سبز در مقیاس کوچک • درجه بالایی از تخصص فنی داخلی مورد نیاز، از جمله هزینه‌های آموزش منظم
ابر خصوصی OFF-PREM (میزبانی با ارائه دهنده خدمت ابری)	• افزایش بهره‌وری هزینه • مزایای بالقوه امنیت سایبری و عملکرد و کارایی هزینه • در صورت ارائه توسط ارائه دهنده خدمات ابری • انطباق با الزامات محلی‌سازی داده‌ها	• هزینه نگهداری و به‌روزرسانی سامانه‌ها • پایداری به ارائه‌دهنده خدمات ابری بستگی دارد • درجه بالایی از تخصص فنی مورد نیاز
ابر عمومی (ارائه دهنده ابر عمومی ملی / منطقه‌ای)	• بهبود عملکرد و مقیاس‌پذیری • افزایش بهره‌وری هزینه • ویژگی‌های امنیت سایبری پیشرفته • انطباق با الزامات محلی‌سازی داده‌ها	• تعهدات اغلب نامشخص یا کمتر مربوط به پایداری • کنترل کمتر بر روی داده‌ها • تدارکات مستلزم توجه دقیق به قراردادهای سطح خدمات است • وابستگی به یک فروشنده (Vendor lock-in)

^۱ sustainability dashboard

• تدارکات مستلزم توجه دقیق به قراردادهای سطح خدمات است • مشکلات بالقوه قفل فروشنده (اگرچه می‌توان از طریق راه‌حل‌های چند ابری آن را کاهش داد) • مسائل محلی‌سازی داده‌ها و حاکمیت ممکن است این گزینه را محدود کند	• بالاترین سطح عملکرد و مقیاس پذیری • بالاترین سطح مقرون به صرفه بودن • بالاترین سطح امنیت سایبری • امکان نوآوری سریع به دلیل دسترسی به پیشرفته‌ترین ابزارها که می‌توانند به‌طور منظم به روز شوند • تعهد قوی به پایداری از طریق مراکز داده سبز، استفاده از انرژی‌های تجدیدپذیر و مدیریت کارآمدتر داده‌ها	ابر عمومی (ارائه دهنده ابر بزرگ مقیاس)
--	--	---

دولت‌ها در سراسر جهان به‌طور فزاینده‌ای راه‌حل‌های ابر عمومی را به‌ویژه به دلایل مختلفی که در این گزارش ذکر شده است، اتخاذ می‌کنند. ابر عمومی روشی مقرون به‌صرفه برای استفاده، نگهداری و ارتقاء از زیرساخت قدیمی فناوری اطلاعات داخلی (on-prem) است. این رویکرد به نهادهای دولتی کمک می‌کند تا پایگاه داده‌های خود را ایمن کنند و سازوکارهای پیشرفته امنیت سایبری را مستقر کنند که کارآمد، انعطاف‌پذیر و قابل اعتماد است و تقریباً به‌طور نامحدود مقیاس‌پذیر است، رایانش ابر عمومی همچنین پتانسیل کاهش قابل توجه انرژی و انتشار کربن را در مقایسه با سایر گزینه‌های ابری دارد.

۴-۱ مزایا و مخاطرات مهاجرت به ابر عمومی

مهاجرت به ابر و به‌ویژه خدمات ابر عمومی مزایای متعددی از جمله بهبود کارایی هزینه، امنیت داده‌ها، کیفیت خدمات، بهبود عملکرد، مقیاس‌پذیری و نوآوری و پایداری محیط زیست را برای دولت و سازمان‌ها به همراه دارد. تأخیر در انتقال به خدمات ابری، باعث از دست رفتن مزایای چند جانبه‌ای می‌شود که رایانش ابری می‌تواند فراهم کند. دولت‌ها اگر راه‌حل‌های ابری را با توجه به منابع موجود، نیازهای برنامه‌ها و زمینه‌های محلی اتخاذ نکنند، شکاف دیجیتالی بیشتری را تجربه خواهند کرد. با این وجود راه‌حل‌های ابری همچنین مستلزم خطراتی هستند که دولت‌ها و وزارتخانه‌ها باید قبل از شروع انتقال آن‌ها را ارزیابی کنند. تجربیات حاصل از انتقال به خدمات ابری در کشورهای مختلف، ملاحظات مهمی را برای تصمیم‌گیرندگان دولت در مورد هزینه‌ها، امنیت، حفاظت از داده‌ها، عملکرد و قابلیت اطمینان و در نهایت، پایداری زیست محیطی بیان می‌کند.

امنیت: ابر عمومی و به ویژه ارائه‌دهندگان خدمات ابر عمومی فرامقیاس می‌توانند به نهادهای دولتی کمک کنند تا امنیت سایبری را با استقرار سازوکارهای دفاعی پیشرفته افزایش دهند. انجام این کار بسیار مهم است زیرا پیشرفت سریع ابزارهایی با اهداف مخرب، آسیب به زیرساخت دیجیتال دولت را آسان‌تر از همیشه کرده است. حملات رمزنگاری (که معمولاً به عنوان باج‌افزار شناخته می‌شود) به‌طور فزاینده‌ای رایج شده‌اند. افزایش تهدیدهای امنیتی، سازمان‌ها را مجبور کرده است که به‌طور مداوم فناوری و استانداردهای امنیتی فناوری اطلاعات خود را بهبود و ارتقاء دهند تا با چشم‌انداز تهدید در حال تغییر همگام شوند. زیرساخت‌های دولتی دیجیتال به‌ویژه اهداف رایجی برای حمله هستند و کشورهای در حال توسعه به دلیل ظرفیت و پرسنل پایین امنیت سایبری در معرض خطر هستند.

استفاده از ابر عمومی اجازه می‌دهد دولت‌ها فناوری‌های پیچیده مانند مدیریت دسترسی هویت دقیق و رمزنگاری احراز هویت چند عاملی که دستیابی به آن به تنهایی بسیار پرهزینه خواهد بود را به‌کارگیرند. انجام وظایفی مانند حسابرسی جامع و اجرای اصل کمترین امتیاز (اعطای کمترین سطح ممکن از امتیازات لازم به کاربر برای انجام یک کار خاص) بسیار دشوار است مگر اینکه

ظرفیت‌های امنیتی قوی وجود داشته باشد، و این قابلیت‌ها باید به‌طور مداوم به‌روز شوند تا بتوانند به تهدیدات امنیتی جدید پاسخ دهند. ارائه‌دهندگان ابر سرمایه‌گذاری هنگفت برای به‌روز نگه داشتن ویژگی‌های امنیتی برای مواجهه با قابلیت‌های مهاجمان انجام می‌دهند و دائماً ویژگی‌های امنیتی جدید، مانند تشخیص تهدید مبتنی بر یادگیری ماشین را توسعه می‌دهند. استفاده از ارائه‌دهندگان ابر عمومی همچنین به نهادهای دولتی این امکان را می‌دهد که از چارچوب امنیتی توسعه یافته توسط مهندسان بسیار آموزش دیده بدون نیاز به سرمایه‌گذاری هنگفت استفاده کنند.

تقریباً تمام موارد نقض امنیت ناشی از سوء مدیریت کاربران در طراحی کنترل‌های محافظت از داده‌ها می‌باشد، نه شکست ارائه‌دهنده ابر برای استقرار در مکان مناسب. در نتیجه برای دولت‌ها و وزارتخانه‌ها اهمیت دارد که قبل از انتقال داده‌ها، راهبردها و سیاست‌های ابری مناسب را توسعه دهند و یک تیم مدیریتی را برای نظارت بر اجرای آنها تعیین کنند. علاوه بر این، امنیت یک «مسئولیت مشترک» بین مشتریان و فروشندگان ابری است، و استفاده از ابر عمومی سازمان‌ها را به طور کامل از نیاز حیاتی به ظرفیت امنیت سایبری داخلی خلاص نمی‌کند.

حفاظت از داده‌ها: خدمات ابری می‌توانند با جلوگیری از شناسایی غیرمجاز داده‌های ذخیره‌شده در ابر، سطح بالایی از حفاظت را برای داده‌های حساس فراهم کنند. برای محافظت و ایمن سازی داده‌های خود در محیط‌های ابری، دولت‌ها باید بدانند چه داده‌هایی دارند و آن داده‌ها در کجا قرار دارند و مخاطرات مرتبط با هر نوع از داده‌ها چه هستند. با این حال، بیشتر متخصصان فناوری اطلاعات نمی‌دانند داده‌های حساس یا محرمانه در کجا قرار دارند. ندانستن محل ذخیره داده‌ها، دانستن اینکه چه کسی می‌تواند به آنها دسترسی داشته باشد را دشوار می‌کند. عموماً ارائه‌دهندگان ابر عمومی اقدامات زیر را برای محافظت از داده‌های کاربر اعمال می‌کنند و برخی از مسئولیت‌ها را با کاربران به اشتراک می‌گذارند:

- کاربران داده‌ها را کنترل می‌کنند. ارائه‌دهنده ابر داده‌ها را بر اساس توافق‌نامه سطح خدمات پردازش می‌کند، خدمات را مشخص می‌کند و تضمین می‌کند که عرضه خواهد کرد. بسیاری از شرکت‌ها انعطاف‌پذیری را در طراحی این خدمات برای مطابقت با نیازهای مشتری امکان‌پذیر می‌کنند که برای هر نهاد دولتی متفاوت خواهد بود.
- جمع‌آوری و استفاده از داده‌ها شفاف است و با مقرراتی مانند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR)، مطابقت دارد.

الزامات حفاظت از داده‌ها خاص کشورها است و به قوانین ملی و محلی بستگی دارد. الزامات محلی‌سازی داده‌ها می‌تواند امنیت داده‌ها را کاهش دهند و در نتیجه همیشه نمی‌توانند نیازها برای مؤثرترین اقدامات امنیتی را برآورده سازند. دولت‌ها باید قبل از انجام اقداماتی برای انتقال داده‌های خود به فضای ابری، از این قوانین آگاه باشند.

سازمان‌هایی که به چندین ارائه‌دهنده خدمات ابری متکی هستند ممکن است کنترل کمی بر حرکت داده‌های خود از طریق مراکز داده مختلف در سراسر جهان داشته باشند. علاوه بر این، همیشه مشخص نیست که متولی داده یا ارائه‌دهنده خدمات طرف سوم مسئول حفاظت از داده‌ها است یا مجموعه‌ای از قوانین حفاظت از داده اعمال می‌شود. ارائه‌دهندگان خدمات ابری همچنین ممکن است تمایلی به افشای کامل اقدامات امنیتی که برای محافظت از اطلاعات یا نحوه پردازش داده‌ها استفاده می‌کنند، نداشته باشند. در نتیجه دولت‌ها باید اطمینان حاصل کنند که ارائه‌دهندگان خدمات ابری نیازهای حفاظت از داده‌های محلی و الزامات قانونی را در طول بررسی توافق‌نامه‌های سطح خدمت برآورده کنند.

عملکرد و قابلیت اطمینان: شاخص اولیه قابلیت اطمینان برای خدمات ابری، زمان برپایی^۱ است. به نظر می‌رسد زمان کار سامانه‌های در محل^۲ به تقریب ۱۰۰ درصد باشد. اما اجرای یک برنامه کاربردی ۲۴/۷ در محل، کارایی کمتری نسبت به راه‌حل‌های ابر عمومی دارد، که گزینه‌های بهینه‌سازی بهتری دارند، می‌توانند در صورت تقاضای واقعی تغییر مقیاس دهند و در صورت بروز فاجعه یا قطع سامانه، اقدامات بازگشتی گسترده‌ای را انجام دهند. نرخ بهره‌برداری بهبودیافته ارائه‌دهندگان خدمات ابر عمومی، مزیت افزوده‌ای را به همراه دارد که باعث صرفه‌جویی کلی در مصرف انرژی می‌شود. اکثر ارائه‌دهندگان ابر عمومی و ارائه‌دهندگان ابر مقیاس‌بزرگ، روش‌های بازیابی فاجعه گسترده‌ای دارند که دائماً آنها را بهبود می‌بخشند تا در برابر خطرات فیزیکی و سایبری انعطاف‌پذیر باشند.

فراهم‌آوردندگان ابر عمومی معیارهای عملکرد ابری منابع را رصد می‌کنند تا اطمینان حاصل شود که همه اجزاء به‌طور یکپارچه با هم ارتباط برقرار می‌کنند. این معیارها عملیات ورودی/خروجی در ثانیه، عملکرد سیستم فایل، قابلیت دسترسی و مقیاس خودکار را اندازه‌گیری می‌کنند. یک مرکز داده با میزبانی دولت می‌تواند این ویژگی‌ها را فراهم کند و این نوع نظارت را انجام دهد، اما انجام این کار بسیار گران تمام می‌شود و کارایی هزینه را در مقیاسی که ارائه‌دهندگان خدمات ابری مقیاس بزرگ از آن سود می‌برند، از دست می‌دهد.

مقیاس‌پذیری: مقیاس‌پذیری اشاره به آن دارد که چگونه یک سامانه می‌تواند به خوبی به تقاضاهای در حال تغییر، واکنش نشان داده و خود را آن تطبیق دهد. ابر عمومی، مقیاس‌پذیری تقریباً نامحدودی را فراهم می‌کند و به کاربران اجازه می‌دهد ۱- خدمات را در صورت تقاضا اضافه و رها کند. این مشخصه «ابری با قابلیت ارتجاعی» می‌تواند خودکار و یکپارچه^۳ باشد، ۲- یک سامانه با اجزای اضافی بسازند (مثلاً با پیوند دادن یک سرور به سایرین برای افزودن قدرت پردازش یا حافظه). این «مقیاس‌بندی افقی» می‌تواند افزونگی را افزایش دهد و تضمین کند که خدمات در دسترس و قابل اعتماد باقی می‌مانند، ۳- انواع مختلف مقیاس‌بندی را به‌طور خودکار مدیریت کنند (مقیاس‌سازی خودکار). این توانایی مقیاس یکپارچه برای مدیریت بارهای اوج معمولی (مانند ثبت نام در مدرسه) و واکنش به شرایط اضطراری (مانند بلایای طبیعی یا بیماری‌های همه‌گیر) بسیار مفید است.

پایداری زیست محیطی: رایانش ابری همچنین می‌تواند مصرف انرژی و انتشار کربن دولت را تا ۳۰ درصد یا بیشتر در مقایسه با اجرای برنامه‌های مشابه در زیرساخت‌های خود کاهش دهد [۸]، زیرا ارائه‌دهندگان ابر از صرفه‌جویی در مقیاس، به‌ویژه ارائه‌دهندگان ابر مقیاس بزرگ عمومی سود می‌برند. مزایا به‌ویژه برای مؤسسات کوچک که می‌توانند از صرفه‌جویی خالص انرژی و کاهش ردپای کربن بیش از ۹۰ درصد بهره‌مند شوند، بسیار زیاد است. چهار عامل به مراکز داده اجازه داده است تا با وجود افزایش بار کاری مرکز داده و ترافیک اینترنت، مصرف انرژی خود را ثابت نگه دارند: ۱- بهره‌وری عملیاتی فناوری اطلاعات، ۲- بهره‌وری تجهیزات فناوری اطلاعات؛ ۳- بهره‌وری داده‌های زیرساخت مرکز و ۴- برق تولید شده از منابع تجدیدپذیر. بهره‌وری عملیاتی ارائه‌دهندگان ابر بزرگ به دلیل سه عامل تدارک پویا، چند اجاره‌ای و بهره‌وری سرور^۴ بالا است.

^۱ uptime

^۲ On-premises

^۳ seamless

^۴ Server utilization

مراکز داده بزرگ از فناوری‌های پیشرفته‌ای استفاده می‌کنند که الکتریسیته مورد نیاز را برای کارهای سربار مانند روشنایی، سرمایش و مصرف برق کاهش می‌دهد. مراکز داده ابر فرامقیاس اثربخشی مصرف برق (PUE^۱) بسیار بیشتری دارند و از طریق نوآوری و بهبود مستمر، در طراحی، ساخت و راه اندازی مراکز داده با اثربخشی مصرف برق بیشتر پیشرو هستند.

صرف نظر از اینکه کدام استاندارد یا گواهی اعمال می‌شود، پذیرش یا مهاجرت به خدمات ابر عمومی، چشم‌انداز ریسک فناوری اطلاعات را تغییر می‌دهد. دولت‌ها باید پنج نوع ریسک شامل امنیت داده‌ها و نظارتی، فناوری، عملیاتی، فروشنده، و مالی را قبل از شروع فرآیند مهاجرت به ابر در نظر بگیرند.

جدول ۳: مخاطرات ابر عمومی و اقدامات دولت برای کاهش آنها

مخاطره	اقدامات دولت‌ها برای کاهش ریسک
امنیت داده‌ها و مقررات	- ایجاد یک راهبرد ابری دولتی - تهیه یک نقشه راه برای مهاجرت ابری
فناوری	بازنگری سیاست‌ها برای به‌روزرسانی حاکمیت داده‌ها برای کاهش دسته‌های ریسک کلیدی.
عملیاتی	مشارکت در حاکمیت ابری برای کاهش ریسک‌های فروشنده، داده، فناوری و عملیات، متخصصان امنیت و ریسک
فروشنده	- ساده سازی فرآیندهای مدیریت ابر تا امکان نظارت بر ریسک‌های فروشنده، داده‌ها، فناوری و عملیاتی فراهم شود. - اطمینان از الزامات حفاظت از داده‌ها و میزبانی مطابق با قانون امنیت داده‌ها به منظور کاهش فروشندگان و خطرات داده
مالی	استفاده از ابزارهای خودکارسازی پیشرفته برای بهره‌مندی از ابر و کاهش خطرات در همه دسته‌ها

۴-۲ رویکرد مهاجرت به ابر

دولت‌هایی که مهاجرت به خدمات ابری را انتخاب می‌کنند، چهار گزینه اساسی ۱- مهاجرت به ابر خصوصی، ۲- مهاجرت به مرکز داده هم‌مکانی، ۳- مهاجرت به سمت یک ابر ترکیبی و ۴- مهاجرت به ابر عمومی را دارند که می‌توانند از میان آنها انتخاب کنند.

مهاجرت به ابر خصوصی (با داده‌های ذخیره شده در محل): ابرهای خصوصی اغلب توسط سازمان‌های دولتی، مؤسسات مالی و سایر سازمان‌های با اندازه متوسط تا بزرگ با عملیات کسب و کاری حیاتی که به دنبال کنترل بیشتر بر محیط خود هستند، استفاده می‌شوند. برای برخی از سازمان‌ها، ابر خصوصی ممکن است تنها گزینه واقعی برای اطمینان از انطباق با مقررات باشد. بسیاری از مشتریان ابری خصوصی، داده‌ها را در مرکز داده خودشان یا با کمک یک خدمت ابری شخص ثالث میزبانی می‌کنند. در هر صورت، خدمات و زیرساخت‌ها در یک شبکه خصوصی نگهداری می‌شوند و سخت‌افزار و نرم‌افزار به تنهایی در دسترس آن مشتری است. یک ابر خصوصی می‌تواند با حفظ همه چیز در داخل، استفاده از سرمایه‌گذاری قدیمی را به حداکثر برساند اما یک ساختار سرمایه‌بر و پرهزینه را در جای خود ایفا می‌کند.

مهاجرت به مرکز داده هم‌مکانی (با داده‌هایی که در خارج ذخیره می‌شوند): این گزینه اجرای سریع‌تر را امکان‌پذیر

^۱ Power usage effectiveness

می‌کند، زیرا می‌تواند نیاز به ساخت یک مرکز داده جدید را برطرف کند و در عین حال برخی از مزایای ابر عمومی مانند کاهش نیاز به کارکنان فنی داخلی را فراهم کند. اساساً، این گزینه‌ای است برای هم‌مکانی تجهیزات سرور داده با اجاره یک مرکز داده مشترک، که به‌عنوان مرکز داده طرف سوم نیز شناخته می‌شود. در عین حال، این گزینه معایب خاصی مانند هزینه‌های بالا و توانایی محدود برای پاسخگویی به افزایش تقاضا را حفظ می‌کند.

مهاجرت به سمت یک ابر ترکیبی (با داده‌های ذخیره‌شده در محل یا در یک ابر خصوصی به همراه داده‌های ذخیره‌شده یا پردازش‌شده توسط ارائه‌دهنده ابر عمومی): این گزینه راه‌حل‌های ابر عمومی و خصوصی را ترکیب می‌کند و به داده‌ها و برنامه‌ها اجازه می‌دهد بین دو مکان (که ممکن است به ویژگی‌های قابلیت همکاری نیاز داشته باشند یا نباشند) جریان داشته باشند. ابر ترکیبی به ارتباط متقابل ذخیره‌سازی ابری در محل یا خصوصی با ابر عمومی اشاره دارد. بسیاری از سازمان‌ها و دولت‌ها یک گزینه ترکیبی را انتخاب می‌کنند تا بتوانند چالش‌های خاصی مانند انطباق با مقررات، سرعت و کیفیت پایین اینترنت، یا امنیت بیشتر و در عین حال انعطاف‌پذیری بیشتر را برطرف کنند. راه‌حل ترکیبی برخی از مزایای ابر عمومی بویژه مقرون به صرفه بودن کشسانی ظرفیت اوج بار را ارائه می‌دهد. ترکیب به عنوان حالت نهایی^۱ زمانی استفاده می‌شود که برخی از بخش‌های بار کاری عمومی هرگز نمی‌توانند به ابر عمومی منتقل شوند. تحت رویکرد «ترکیب به عنوان شبکه جدید»^۲، پروژه‌های جدید به ابر عمومی منتقل می‌شوند. با این رویکرد، تمام حجم کاری در نهایت در زمانی که سامانه‌های قدیمی جایگزین می‌شوند در فضای ابری خواهد بود، اما این فرآیند در یک دوره زمانی طولانی رخ خواهد داد. روندهای فناوری چشم‌انداز این راه‌حل‌ها را تغییر خواهد داد، زیرا رایانش لبه، دسترسی به راه‌حل‌های ابر عمومی را از طریق سناریوهای کم‌اتصال بیشتر می‌کند. برخی از حوزه‌ها مانند دفاعی، همیشه محدودیت‌های شدیدی در استفاده از ابر عمومی خواهند داشت. با این وجود امکان استفاده از یک راه‌حل ابر ترکیبی برای هم پیوستگی بارهای کاری، بدون اجبار به خروجی داده‌ها به ابر عمومی وجود دارد.

مهاجرت به یک ابر عمومی (با داده‌های ذخیره شده خارجی): رایج‌ترین گزینه رایانش ابری، بطور معمول توسط یک شرکت طرف سوم ارائه می‌شود، که ممکن است یک ارائه‌دهنده ابر فرامقیاس باشد یا نباشد. این گزینه یک محیط توانمند برای راه‌حل‌های ابر عمومی که در قبل به آنها اشاره شد را فراهم می‌آورد. برخی از دولت‌ها (به عنوان مثال، سنگاپور) ابر عمومی خود را راه اندازی کرده‌اند که نشان دهنده رویکردهای جایگزینی است که دولت‌ها می‌توانند در پیش گیرند. در این مدل، ارائه‌دهنده خدمات ابری تمام مسئولیت مراکز داده، سخت‌افزار و زیرساخت‌هایی را بر عهده می‌گیرد که بار کاری مشتری را اجرا می‌کنند. برای بهره‌مندی کامل از ساختار کم‌هزینه و افزایش سریع ظرفیت ارائه شده توسط ابر عمومی، مهاجرت باید بعد از ارزیابی محیط قدیمی انجام شود. در مهاجرت به ابر عمومی، دولت می‌تواند از دو یا چند خدمت ابری و از دو یا چند ارائه دهنده خدمات ابری استفاده کند. مشتریان ممکن است این گزینه را برای جلوگیری از وابستگی به فروشنده، انتخاب از میان خدمات بیشتر، یا اطمینان از دسترسی به آخرین نوآوری‌ها دنبال نمایند. این رویکرد موانع ورود بالاتری را داراست زیرا به مهارت‌های فنی بیشتری برای مدیریت زیرساخت‌های ابری مختلف و اقدامات سختگیرانه احتمالی امنیتی نیاز است. هر چند این اقدامات ممکن است نسبت به مولفه‌های کمتر ایمن رویکرد ترکیبی بیشتر نباشد.

^۱ Hybrid-as-an-end-state

^۲ hybrid-as-net-new

جدول ۴، مزیت‌ها و معایب این چهار گزینه را در کنار رویکرد قدیمی ذخیره‌سازی داده‌های فناوری اطلاعات خلاصه می‌نماید:

جدول ۴: مزیت‌ها و معایب رویکردهای مهاجرت به ابر

گزینه	مزیت‌ها	معایب
حفظ سامانه‌های قدیمی فناوری اطلاعات (ذخیره داده‌ها در محل)	منابع معمول کسب و کار با دیگران به اشتراک گذاشته نمی‌شود، پیکربندی توسط تیم داخلی فناوری اطلاعات نگهداری می‌شود.	- هزینه‌های سرمایه‌ای برای سرمایه‌گذاری اولیه و آموزش کارکنان، عملیات و نگهداری می‌تواند بالا باشد. - تسهیلات اغلب قدیمی و با بهره‌وری پایین هستند. - سامانه قدیمی بدون سرمایه‌گذاری اولیه ذاتاً قادر به گسترش فراتر از نیازمندی‌های اولیه تعریف شده نیست. - حضور مستمر سامانه‌های قدیمی متحمل هزینه‌های فزاینده‌ای برای ادغام‌های لازم، کاهش مخاطرات و ... خواهد شد. - عدم انعطاف برای پاسخگویی به تقاضای در حال نوسان. - غیرقابل اعتماد بودن به دلیل عدم وجود گسترده سامانه‌های پشتیبان مورد نیاز برای ارائه قابلیت‌های بازیابی بلایا - قابلیت‌های امنیتی محدود
مهاجرت به ابر خصوصی اطلاعات (ذخیره داده‌ها در محل)	- سخت‌افزار، ذخیره‌سازی داده‌ها و اتصال می‌تواند بطور دقیق برای وظایف مورد نظر به منظور تضمین برخی امنیت‌ها با سرمایه‌گذاری‌های عظیم سفارشی شود - انطباق با مقررات ممکن است برای داده‌ها طبقه بندی شده به عنوان "فوق سری" دشوار باشد.	- انعطاف‌پذیری برای پاسخگویی به تقاضای در حال نوسان محدود است. - عدم وجود سامانه‌های پشتیبان گسترده برای فراهم‌آوری بازیابی فاجعه ممکن است منجر به عدم قابلیت اعتماد شود. - قابلیت‌های امنیتی محدود است. راه‌حل‌های ابر خصوصی برای ماندن در سطح ویژگی‌های امنیتی مبتنی بر ابر تلاش خواهند کرد
مهاجرت به مرکز داده هم‌مکانی (ذخیره داده‌ها در خارج)	- ابره‌ای خصوصی خارجی اغلب مقیاس‌پذیری بیشتری نسبت به زیرساخت‌های در محل ارائه می‌کنند. - هزینه‌های آموزش کارکنان، عملیات و نگهداری پایین‌تر هستند	- قابلیت همکاری به دلیل دشواری مدیریت همزمان چندین سامانه ناهمگون می‌تواند چالش برانگیز باشد، - زیرساخت‌های اضافی، پیچیدگی را افزایش می‌دهد - هزینه‌ها برای آموزش کارکنان، عملیات و نگهداری باید متحمل شود
به کارگیری ابر ترکیبی (به هم پیوستگی داده‌های در محل، ذخیره شده در ابر خصوصی یا ابر عمومی)	- سازمان می‌تواند زیرساخت‌های خصوصی را برای دارایی‌های حساس یا بارهای کاری که نیاز به تاخیر کم دارند، حفظ کند. - منابع اضافی در ابر عمومی در صورت نیاز می‌تواند قابل دسترسی باشد - انتقال به ابر لازم نیست طاق‌ت فرسا باشد، زیرا مهاجرت می‌تواند با مرحله‌بندی زمانی بارهای کاری به تدریج انجام شود.	قابلیت کنترل و قابلیت مشاهده را با توجه به نحوه و مکان ذخیره و مدیریت داده‌ها از دست می‌دهد.
مهاجرت به ابر عمومی (از جمله ارائه دهندگان خدمات فرامقیاس)	- هزینه‌های سرمایه‌ای صفر است زیرا نیازی به خرید سخت‌افزار یا نرم‌افزار نیست - راه‌حل‌های جدید را می‌توان تقریباً بلافاصله آزمایش کرد - ارائه‌دهنده خدمات همه تعمیر و نگهداری را فراهم می‌کند - مقیاس‌پذیری به صورت مجازی نامحدود است؛ منابع بر حسب تقاضا برای برآورد نیازهای در حال تغییر در دسترس	- الزامات انطباق حفاظت از داده‌ها برای هر صنعت باید تضمین شود. - در کشورهایی با پیچیدگی مقرراتی بالا، الزامات اسکان داده ممکن است نگهداری محلی انواع خاصی از داده‌ها را اجبار نماید در حالی که سایر بارهای کاری می‌توانند بر روی ابر عمومی قرار گیرند

مزیت‌ها	معایب	گزینه
• هستند • قابلیت اطمینان بالا است زیرا شبکه گسترده‌ای از سرورها • مقابله با شکست را تضمین می‌کند • ویژگی‌های پیشرفته، مانند امنیت توانمند شده با هوش مصنوعی ارائه می‌شوند.	• امنیت مشترک به این معنی است که تهدیدات برای امنیت نیز تسهیم می‌شود • کاربر ممکن است در یک فروشنده قفل شده باشد. این مشکل را می‌توان از طریق یک راه‌حل چند ابری کاهش داد. با این حال، راه‌حل چند ابری چالش‌های قابلیت همکاری را افزایش می‌دهد	

انتخاب بین ابر عمومی، خصوصی یا ترکیبی به عوامل متنوعی وابسته می‌باشد. کشورها گزینه‌های مختلفی را انتخاب کرده‌اند. سنگاپور برای راه‌اندازی یک ابر عمومی، سیاست "نخست ابر تجاری" را در سال ۲۰۱۸ انتخاب کرد. هدف اصلی مهاجرت سامانه‌های فناوری اطلاعات دولت به ابر عمومی و میزبانی حداقل ۷۰ درصد از سامانه‌های با حساسیت کمتر دولت (مانند منابع انسانی) بر روی ابر عمومی تا سال ۲۰۲۳ بود. دلایل کلیدی برای انتقال به ابر عمومی شامل در دسترس بودن بیشتر و کیفیت بهبود یافته خدمات عمومی، کاهش هزینه‌های میزبانی و کاهش زمان خاموشی سامانه‌ها است.

۳-۴ چارچوب تصمیم‌گیری مهاجرت به ابر

مدل تصمیم‌گیری شامل ملاحظات در سطوح سیاست، راهبرد و عملیات است. ساختار این مدل سه لایه‌ای، بر اساس نهاد سازمان دولتی و میزان انعطاف‌پذیری آنها در هنگام در نظر گرفتن مهاجرت ابری می‌باشد و نشان می‌دهد که چگونه آنها می‌توانند به بهترین شکل از منابع محدود برای ایجاد بیشترین منفعت برای عموم استفاده کنند.

در سطح سیاست، اهداف مهاجرت (به عنوان مثال، بهبود خدمات برای شهروندان با استفاده از ابر عمومی) بیان می‌شوند. تصمیم‌گیری در این سطح شامل ارزیابی عوامل و روندهای موثر بر تصمیم مهاجرت و ارزیابی سرعت نوآوری در بخش خدمات ابری است. سطح راهبرد، زمینه محلی را در نظر می‌گیرد و راحت‌ترین حوزه‌های سازگار با راه‌حل‌های ابر عمومی را شناسایی می‌کند. این سطح برخی از محدودیت‌هایی را پوشش می‌دهد که دولت‌ها در قالب مقررات، تحمل ریسک و عمده سرمایه‌گذاری‌های اجتماعی با آن مواجه هستند و بر انتخاب پروژه‌هایی که می‌توانند به ابر منتقل شوند تأثیر بگذارد. سطح عملیاتی بر جزئیات عملی شروع پروژه‌های ابر عمومی متمرکز است و آنچه را که باید قبل از شروع در نظر گرفته شود برجسته می‌کند.



شکل ۵: چارچوب سه مرحله‌ای هدایت گزینه‌های مهاجرت به ابر [۸]

فهرستی از سؤالات کلیدی در سطح سیاست‌ها می‌تواند به ارزیابی دولت از "وضعیت بالغ" کمک کند که شامل موارد زیر است:

- داده‌ها قرار است در کجا ذخیره شوند؟
- چه کسی داده‌ها را مدیریت خواهد کرد؟
- آیا آموزش اضافی مورد نیاز است؟
- مزایا، هزینه‌ها و خطرات غیرمستقیم هر گزینه چیست؟
- آیا ابر یا سامانه‌های ذخیره‌سازی داده با سایر سازمان‌های دولتی که ممکن است از دسترسی به داده‌ها منتفع شوند قابلیت همکاری خواهد داشت؟
- آیا الزامات محلی‌سازی یا حفاظت از داده‌ها که ممکن است مانع استفاده از ابر شوند وجود دارد؟
- آیا دستورالعملی برای کمک به دولت در تهیه راه‌حل‌های ابری وجود دارد؟
- کدام بخش‌های عمومی در اولویت هستند؟
- کدام خدمات دولتی باید در اولویت قرار گیرند؟
- مولفه‌های اساسی معماری فناوری اطلاعات مورد نیاز چیست (به عنوان مثال، شناسه دیجیتال، پرداخت دیجیتال)؟
- آیا رویکرد می‌تواند به راحتی ارتقاء سطح داده شود؟
- آیا مسائل حقوقی خاص کشور وجود دارد؟

دلیل اینکه محلی‌سازی داده‌ها در خط مقدم بحث سیاست ابری قرار دارد آن است که این الزامات به‌طور قانونی نحوه پردازش و ذخیره‌سازی انواع خاصی از داده‌ها را در یک کشور مشخص می‌کند. قبل از مهاجرت به ابر، دولت و سازمان‌ها از شناسایی داده‌هایی که قرار است در ابر قرار گیرند، سود می‌برند، زیرا قوانین در بیشتر موارد بین انواع داده‌ها تمایز قائل می‌شود. به عنوان مثال، داده‌های در دسترس عموم در ثبت‌های رسمی احتمالاً سخت‌گیری کمتری در الزامات محلی‌سازی نسبت به داده‌های شخصی در مورد سلامت یا امور مالی دارند.

چارچوب طبقه‌بندی داده‌ها، می‌تواند به دولت و سازمان‌ها برای تعیین داده‌هایی که می‌توانند در راه‌حل‌های ابر عمومی

واقع شوند و یا در خارج از کشور پردازش یا نگهداری شوند کمک نماید.

جدول ۵ راه‌حل‌های ممکن ابری را براساس سطح حساسیت داده‌ها نشان می‌دهد. این چارچوب طبقه‌بندی داده‌ها به سازمان‌ها کمک می‌کند تا تصمیم بگیرند که کدام راه‌حل ابری به بهترین وجه با نیازهای آن مطابقت دارد.

جدول ۵: راه‌حل‌های ابری بر اساس سطح حساسیت داده‌ها

سطح حساسیت داده‌ها	راه‌حل ابری
اطلاعات امنیت ملی	سامانه‌های سفارشی، سخت، پیش‌فرض
داده‌های حساس کسب‌وکار دولتی یا شهروندان	راه‌حل‌های ابری خصوصی و/یا ترکیبی با کنترل‌های امنیتی افزوده
کسب و کار معمول دولت، اطلاعات عمومی یا غیر محرمانه	راه‌حل‌های ابر عمومی با استاندارد امنیت صنعت

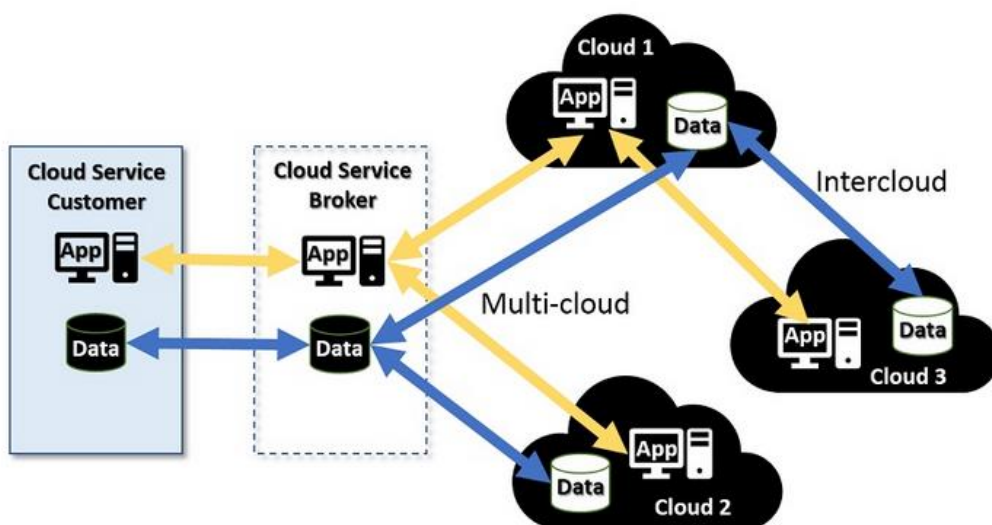
۵ قابلیت همکاری کاربردها در محیط ابر

استفاده از طیف گسترده‌ای از خدمات ابری و انتقال داده‌ها و برنامه‌های کاربردی به محیط‌های رایانش ابری، برای بسیاری از سازمان‌ها مهم است. موضوعاتی چون قابلیت همکاری و قابلیت حمل، ملاحظات قابل توجهی در رابطه با استفاده از خدمات ابری هستند که همچنان سردرگمی و پیچیدگی‌های فراوانی در ارتباط با آن وجود دارد. زیست‌بوم ابری گسترده و بزرگ است و بسیاری از فراهم‌کنندگان خدمات ابری متنوعی را ارائه می‌دهند. درک قابلیت همکاری و قابلیت حمل، اولین گام ضروری در برنامه‌ریزی و طراحی برای استفاده از هر خدمت ابری است. مشخص کردن و رفع نگرانی‌های قابلیت همکاری و حمل‌پذیری خاص، شناسایی گزینه‌های مناسب و توسعه راه‌حل‌های بالقوه را تسریع می‌کند.

توصیف قابلیت همکاری و قابلیت حمل براساس مجموعه‌ای از سناریوهای رایانش ابری رایج، نشان می‌دهد که قابلیت همکاری و قابلیت حمل جنبه‌های متعددی دارند و به تعدادی از مؤلفه‌های مختلف در معماری رایانش ابری مربوط می‌شوند و لازم است که هر کدام به تنهایی در نظر گرفته شوند. این سناریوها، فراهم‌کنندگان و مشتریان را در ارائه و انتخاب خدمات ابری راهنمایی کرده و نشان می‌دهد چگونه این دو قابلیت بر هزینه، امنیت و ریسک مربوطه تأثیر می‌گذارند [۹]. سناریوهای مطرح مرتبط با قابلیت همکاری و قابلیت حمل ابری شامل پنج مورد اصلی به شرح ذیل می‌باشد:

- سناریو ۱: تغییر فراهم‌کنندگان خدمات ابری: مشتری می‌خواهد یک برنامه کاربردی و داده را از ابر ۱ به ابر ۲ منتقل کند.
 - سناریو ۲: استفاده از چندین فراهم‌کننده خدمات ابری: مشتری به عنوان مشترک خدمات مشابه یا متفاوتی از دو یا چند ابر است (ابره‌ای ۱ و ۲ در شکل ۶).
 - سناریو ۳: خدمات ابری با پیوند مستقیم: مشتری برای استفاده از خدمات، نیاز دارد که ابر ۱ به ابر ۳ مرتبط شود.
 - سناریو ۴: پیکربندی ابر ترکیبی: مشتری سامانه‌های قدیمی را به یک ابر خصوصی داخلی (به عنوان مثال، ابر ۱) که به یک خدمت ابری عمومی (به عنوان مثال ابر ۳) مرتبط است، متصل می‌کند.
 - سناریو ۵: مهاجرت ابری: مشتری یک یا چند برنامه in-house و/یا داده را به ابر ۱ منتقل می‌کند.
- در هریک از سناریوهای ابری ارائه شده، ملاحظات اصلی شامل قابلیت همکاری، قابلیت حمل، رابط مدیریتی^۱، رابط کسب و کاری و امنیت بررسی می‌شوند.

^۱ Admin interface



شکل ۶: سناریوهای مطرح برای تعامل‌پذیری و قابلیت حمل ابری [۹]

معماری ابری برنامه کاربردی موبایل بر پایه مطالعه آی‌بی‌ام که در شکل ۷ نشان داده شده است، شامل چهار بخش دستگاه همراه، شبکه عمومی، فراهم‌آورنده ابر و شبکه سازمانی اجزای اصلی معماری ابری برنامه کاربردی سازمانی است [۱۰].

شبکه عمومی: شامل خدمات لبه (خدمات مورد نیاز برای اتصال دستگاه تلفن همراه و برنامه‌های آن به دروازه تلفن همراه مناسب، از طریق اینترنت با استفاده از Wi-Fi یا شبکه تلفن همراه (شامل شبکه ارائه‌دهنده خدمات تلفن همراه و ارتباطات بی‌سیم که تمام عناصر لازم به‌منظور فروش و ارائه خدمات برای استفاده نهایی را کنترل کرده یا مالکیت آنها را بر عهده دارد).

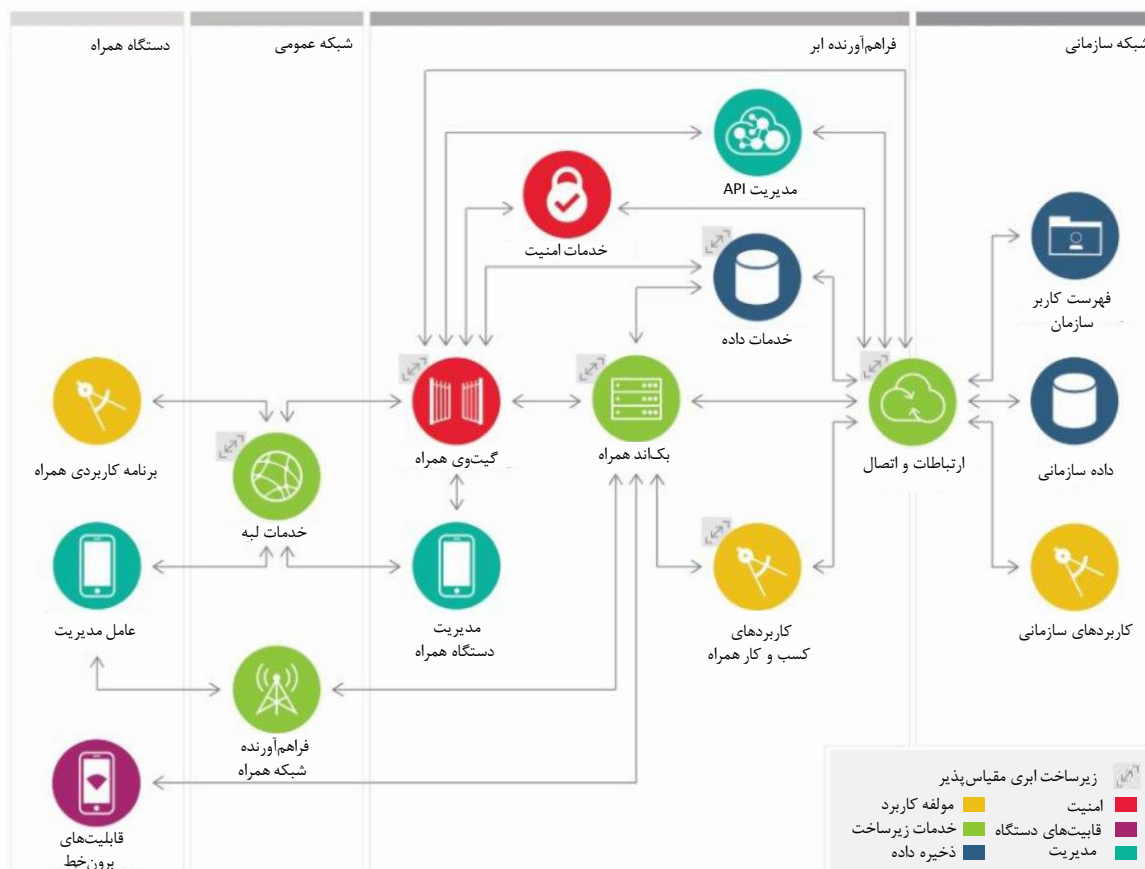
فراهم‌آورنده ابر: شامل بخش‌های ذیل است:

دروازه موبایل: نقطه ورود را از یک برنامه کاربردی موبایل به خدمات خاص تلفن همراه مشخص می‌کند که به‌طور معمول، مجموعه‌ای از API^۱ها را ارائه می‌دهد. همچنین، دروازه موبایل ممکن است از خدمات داده و یا دایرکتوری کاربر سازمان استفاده کند. یک دروازه موبایل می‌تواند توسط یک دروازه معمولی در تمام کانال‌ها به شکل یک زیست‌بوم API بکاربرده شود.

بک اند موبایل: خدمات زمان اجرا را برای برنامه‌های کاربردی تلفن همراه فراهم می‌کند که منطق سمت سرور^۲، حفظ داده‌ها و استفاده از خدمات تلفن همراه را اجرا می‌کنند. بک‌اند موبایل، محیطی را برای اجرای منطق کاربردی و اجرای APIها فراهم می‌کند.

^۱ Application Programming Interface

^۲ Server-side logic



شکل ۷: مؤلفه‌های معماری ابری برنامه کاربردی سازمانی

مدیریت تجهیزات موبایل: بر مدیریت دستگاه‌ها، عمدتاً در سناریوهای کسب و کار به کارمند تمرکز دارد. ^۱MDM، خدماتی را برای پیگیری دستگاه‌های متعلق به شرکت و همچنین مدیریت دستگاه‌هایی که با استفاده از عوامل مدیریتی روی دستگاه‌ها به شبکه‌های شرکتی متصل می‌شوند، ارائه می‌کند.

برنامه‌های کاربردی کسب و کار موبایل: این برنامه‌ها، قابلیت‌های خاص شرکت یا صنعتی را نشان می‌دهند که باید برای دستگاه‌هایی که خدمات تلفن همراه و یا ارتباطات با کاربران را استفاده می‌کنند، در دسترس بوده و شامل مؤلفه‌های تحلیلی برای رصد میزان استفاده باشند.

مدیریت رابط برنامه‌نویسی کاربردی: قابلیت‌های مدیریت API برای نقاط پایانی خدمات موجود، که دروازه موبایل به آنها دسترسی دارد، را انتشار^۲ می‌دهد.

خدمات امنیتی: مدیریت دسترسی را امکان‌پذیر می‌کند تا فقط کاربران مجاز بتوانند به‌طور ایمن به خدمات ابری موبایل دسترسی داشته باشند. این مؤلفه همچنین از داده‌ها در دستگاه‌های تلفن همراه و خدمات ابری محافظت می‌کند.

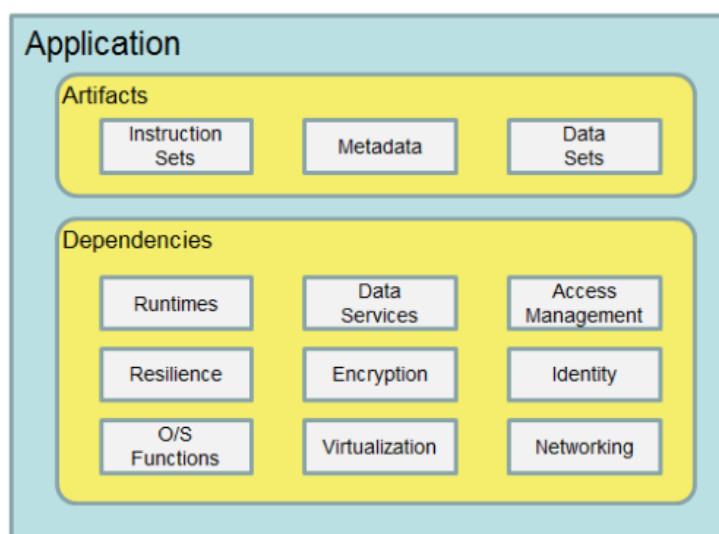
اجزای شبکه سازمانی عبارتند از: ۱- فهرست کاربری سازمانی: ذخیره‌سازی و دسترسی به اطلاعات کاربر را برای پشتیبانی از

^۱ Mobile Device Management (MDM)

^۲ Advertise

احراز هویت، اعطای مجوز، یا داده‌های نمایه^۱ فراهم می‌کند، ۲- داده‌های سازمانی: یک یا چند سامانه ثبت داده‌های تراکنش یا انبارهای داده که نشان‌دهنده داده‌های موجود در شرکت هستند و ۳- برنامه‌های کاربردی سازمانی: برنامه‌هایی که فرآیندهای تجاری و منطق سازمانی را در سامانه‌های سازمانی موجود اجرا می‌کنند.

داشتن یک مدل از برنامه کاربردی، به‌ویژه هنگامی که قابلیت حمل برنامه مدنظر است، ضرورت دارد. همانطور که در شکل ۸ نشان داده شده، برنامه کاربردی دربرگیرنده مجموعه‌ای از آرتیفکتهای شامل مجموعه‌ای از دستورالعمل‌ها، متادیتا (فرا داده) و مجموعه داده‌ها است که بطور مستقیم با برنامه کاربردی در ارتباط هستند.



شکل ۸: مدل برنامه کاربردی [۱۰]

آرتیفکتهای و وابستگی‌ها نشان دهنده اجزای اصلی برنامه کاربردی هستند. برنامه کاربردی دارای مجموعه‌ای از وابستگی‌ها است که عبارتند از: زمان اجرا، خدمات داده‌ای (مانند پایگاه‌های داده)، مدیریت دسترسی؛ هویت، رمزگذاری، قابلیت تاب‌آوری، عملکردهای سیستم عامل، قابلیت‌های مجازی‌سازی و شبکه.

رابط: سه رابط مهم بین سیستم‌های مشتری و خدمت ابری وجود دارد که عبارتند از رابط‌های عملکردی، رابط‌های ادمن و رابط‌های کسب و کاری

قابلیت همکاری خدمت ابری: به سه رابط میان مشتری، سیستم و خدمت ابری مرتبط است. لازم بذکر است، قابلیت همکاری این سه رابط ممکن است مستقل از یکدیگر بوده و قابلیت همکاری یک رابط تضمین کننده همکاری سایر رابط‌ها نمی‌باشد.

قابلیت حمل برنامه کاربردی: به قابلیت انتقال کد برنامه به یا از خدمت ابری مربوط می‌شود. معمولاً فقط برای خدمات IaaS و PaaS اعمال می‌شود، زیرا در مورد خدمت SaaS، کد برنامه کاربردی متعلق به فراهم‌کننده خدمات ابری است و مشتری نمی‌تواند آن را به جای دیگری منتقل کند. یکی از مهمترین عوامل برای قابل حمل بودن برنامه کاربردی این است که محیط

^۱ Profile

^۲ Runtime

هدف باید از آرتیفکت‌های برنامه کاربردی و وابستگی‌های برنامه کاربردی پشتیبانی کنند.

قابلیت حمل داده: به قابلیت انتقال داده به داخل و خارج از محیط خدمت ابری مربوط می‌شود. برای داده‌های مشتریان خدمت ابری، حمل داده معمولاً بیشترین نگرانی را برای خدمات ابری SaaS دارد زیرا برای این خدمات، محتوا، طرح‌واره‌های^۱ داده و فرمت ذخیره‌سازی تحت کنترل فراهم‌کننده خدمات ابری قرار دارد و مشتری باید بداند که داده‌ها چگونه می‌توانند وارد و خارج از خدمت شوند.

کانتینر و زیرساخت کانتینر: برای قابلیت حمل برنامه کاربردی، کانتینر و زیرساخت کانتینر فناوری‌های کلیدی هستند. برای کانتینرها، پلتفرم Docker و Open Containers Initiative یک رویکرد استاندارد برای توسعه کد برنامه کاربردی و پشته‌های نرم‌افزاری مرتبط ارائه می‌دهد. فراهم‌کنندگان خدمات ابری از نرم‌افزارهایی که در کانتینرهای Docker مستقر شده‌اند، پشتیبانی می‌کنند و فرآیند انتقال برنامه‌های کاربردی بین محیط‌ها را ساده‌تر و سراسرتر می‌کنند. این اصولاً برای خدمات ابری IaaS و PaaS اعمال می‌شود. همچنین، فرآیند استقرار و مدیریت مجموعه کانتینرهای مورد نیاز برای هر برنامه کاربردی از طریق فرایند استاندارد شده‌ای است که از طریق پذیرش مشترک ابزار منبع باز ارکستراسیون کانتینر Kubernetes حاصل می‌شود. با این حال، مهم است که بدانیم کانتینرها و مجموعه ابزارهای مرتبط با آنها نوشدارو نبوده و مشکلات خاص خود را در رابطه با قابلیت حمل و قابلیت همکاری دارند. استقرار کانتینرهای موجود در محیط‌های فراهم‌کنندگان خدمات ابری مختلف ممکن است مشکلات قابلیت همکاری به همراه داشته باشد که ناشی از تفاوت در رابط‌های موجود است. قابلیت حمل نیز ممکن است یک چالش باشد، هم از نظر سطوح نرم‌افزاری که توسط فراهم‌کنندگان خدمات ابری مختلف استفاده می‌شود، و هم به دلیل روش‌های متفاوتی که در آن فراهم‌کننده خدماتی را برای نتیجه بخش بودن وابستگی‌های مختلف برنامه کاربردی در دسترس قرار می‌دهد. در حقیقت امکان انتقال یک برنامه کانتینری بدون ایجاد تغییراتی در آن وجود ندارد.

خودکارسازی: فناوری‌هایی که قابلیت حمل برنامه‌ها و داده‌ها را آسان‌تر می‌کنند، ابزارهای خودکارسازی هستند که معمولاً برای رسیدگی به عملیات سمت مشتری مربوط به استفاده از خدمات ابری استفاده می‌شود. خودکارسازی یک عنصر کلیدی از رایانش ابری است. عنصر کلیدی ابزار خودکارسازی این است که ابزارها معمولاً یا تطبیق دهنده‌هایی دارند که آنها را قادر به کار با طیف وسیعی از خدمات ابری فراهم‌کنندگان مختلف می‌کند. به عبارت دیگر، ابزار خودکارسازی، قابلیت همکاری با خدمات ابری هدف را ممکن کرده و همچنین می‌تواند با مسائل مربوط به قابلیت حمل داده‌ها و برنامه‌های کاربردی که در آن محیط در خدمت ابری هدف متفاوت است را مدیریت نماید. بدین ترتیب، مشتریان خدمات ابری می‌توانند نگرانی‌های مربوط به قابلیت همکاری را با استفاده از ابزارهای خودکارسازی کاهش دهند و قادر به ارتباط با طیف وسیعی از خدمات ابری و فراهم‌کنندگان خدمات ابری باشند.

۵-۱ ملاحظات و توصیه‌های کلیدی مرتبط با قابلیت حمل و قابلیت همکاری در محیط ابری

سناریوهای مختلفی برای قابلیت حمل و قابلیت همکاری در محیط ابری مطرح است. برای هر یک از این سناریوها، ملاحظات

^۱ schemas

وجود دارد که در جدول ۶ به آنها پرداخته شده است [۱۱].

جدول ۶: ملاحظات و توصیه‌های کلیدی قابلیت حمل و قابلیت همکاری

ملاحظات و توصیه‌های کلیدی	الزامات
بکارگیری اصول طراحی SOA در برنامه‌های کاربردی on-premise و استفاده از API‌ها برای قابلیت همکاری در خدمات ابری مجازی‌سازی برنامه‌های کاربردی و وابستگی‌های آنها با استفاده از کانتینرها که بیشتر از VM‌ها پشتیبانی می‌شوند. پیاده‌سازی Enterprise Service Bus (ESB) برای انجام رابط، پروتکل و تبدیل داده‌ها به منظور نشان دادن تفاوت میان برنامه‌های کاربردی on-premise و خدمات ابری به موازات نشان دادن تفاوت‌های میان خدمات ابری فراهم‌کنندگان مختلف استفاده از یک واسطه (ارائه‌دهنده بین ابری) برای رسیدگی و حل مسائل یکپارچه‌سازی، قابلیت همکاری، و قابلیت حمل چندین سرویس ابری استفاده از پلتفرم مدیریت ابری (CMP)^۱ برای مدیریت خدمات ابری تاکید بر اینکه فراهم‌کننده خدمات ابری از فناوری‌های کلیدی باز (استانداردهای باز یا منبع باز) برای واسطه‌های کسب و کاری و مدیریتی استفاده می‌کند. استفاده از یک واسطه، «ارائه‌دهنده بین ابری»، برای کمک به رسیدگی و حل مسایل یکپارچه‌سازی، قابلیت همکاری و قابل حمل بودن چندین خدمت ابری. (استفاده از ابزارهایی مانند CMP که می‌توانند با چندین خدمت ابری ادغام شوند).	موضوعات کلی
تعریف دقیق و استانداردسازی API‌ها، پروتکل‌ها، قالب‌های داده و زمینه داده (وسعت و معنایی)^۲ در صورت امکان. (در جایی که ابزار استاندارد وجود ندارد، ممکن است بتوان یک ابزار سفارشی ساخت.) در نظر گرفتن سازگاری برنامه‌های کاربردی on-premise و خدمات ابری در نظر گرفتن سازگاری خدمات ابری ارائه‌شده توسط فراهم‌کنندگان مختلف خدمات ابری تعامل‌پذیر بودن API‌ها برای خدمت SaaS در نظر گرفتن سازگاری برنامه‌های کاربردی داخلی و خدمت ابری مهاجرت کرده اطمینان از اینکه که رابط‌های کاربر، API‌ها، پروتکل‌ها و قالب‌های داده برای خدمات ابری مهاجرت یافته به خوبی تعریف شده‌اند. در صورت امکان، اصرار بر استاندارد بودن API‌ها، پروتکل‌ها و فرمت‌های داده	نرم افزار به عنوان خدمت (SaaS) قابلیت حمل تعامل پذیری
اطمینان از سازگاری محیط برنامه کاربردی (سرور وب، سرور پایگاه داده و غیره) که توسط فراهم‌کننده خدمات ابری پشتیبانی می‌شود، با محیط برنامه کاربردی on-premise مشتری در مهاجرت برنامه‌های کاربردی تضمین اینکه رابط‌ها، پروتکل‌ها و قالب‌های داده‌ای کاربر (وب سرور، سرور پایگاه داده و ...) که توسط فراهم‌کنندگان مختلف ابری پشتیبانی می‌شوند، سازگار هستند.	پلتفرم به عنوان خدمت (Paas) تعامل پذیری

^۱ Cloud Management Platform

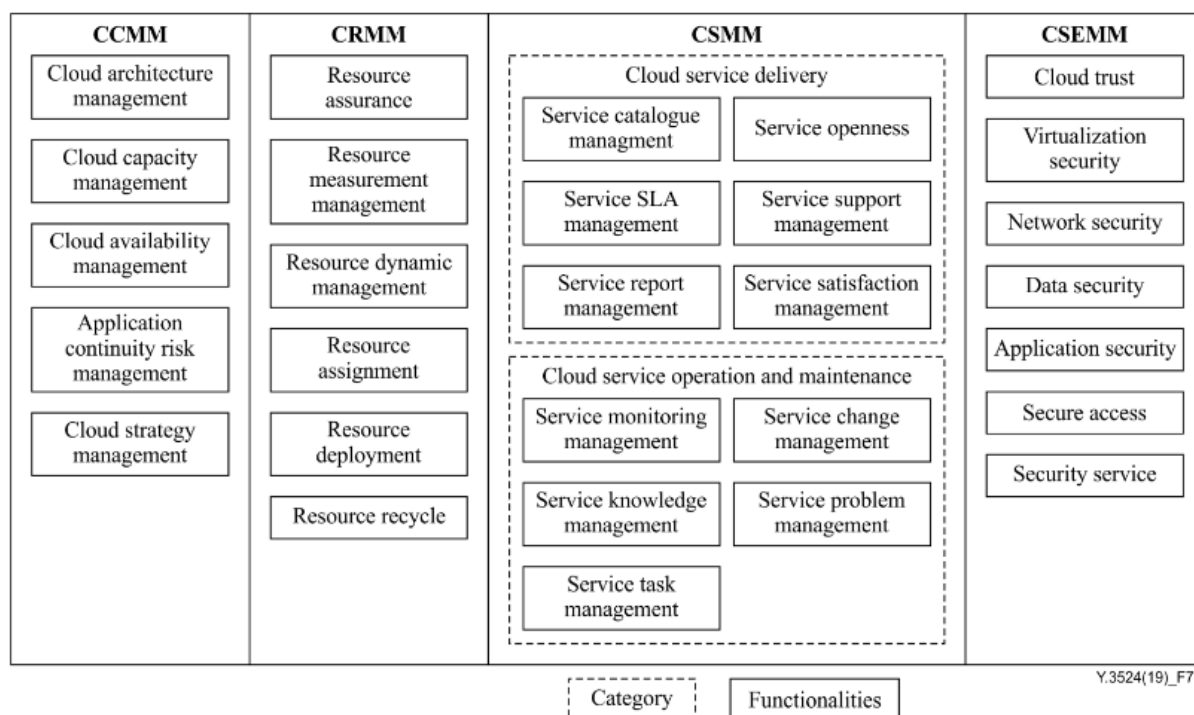
^۲ Extent and Semantics

ملاحظات و توصیه‌های کلیدی	الزامات
برای قابلیت حمل بین خدمات ابری، محیط برنامه کاربردی مبتنی بر فناوری‌های باز باشد بطوریکه تعداد فراهم‌کنندگان خدمات ابری جایگزین که ماندنی هستند افزایش یافته و تسهیل در فرایند مهاجرت در صورت تغییر فراهم‌کننده رخ دهد. برای داده‌های مشتری، خدمت PaaS نمونه‌هایی از پایگاه‌های داده آماده را ارائه دهد که در آن به تعامل‌پذیری معنایی داده‌های مشتری حساس باشند. پشتیبانی فرمت‌های عمومی مانند CSV، XML، و غیره از طرف پایگاه‌های داده در خدمات PaaS اطمینان از اینکه وابستگی‌های برنامه کاربردی براساس فناوری‌های باز است به منظور افزایش تعداد فراهم‌کنندگان خدمات ابری جایگزین پایدار که می‌تواند مهاجرت را تسهیل کنند در زمانیکه تغییر در فراهم‌کننده تضمین شده باشد.	قابلیت حمل
اطمینان از اینکه که خدمت ابری قالب‌های بسته‌بندی استاندارد یا به‌طور گسترده‌ای پذیرفته‌شده مانند Docker یا OVF را پذیرفته و هر یک از رابط‌ها و API‌ها باز و/یا استاندارد هستند.	زیرساخت به عنوان خدمت (IaaS)
پشتیبانی از شناسه شخص ثالث و عملکرد مدیریت دسترسی برای احراز هویت و مجوز دسترسی به خدمات ابری (در حالت ایده‌آل سامانه‌ای که تحت مالکیت و یا اداره مشتری است یا قابلیت معادل ارائه شده توسط یک تامین‌کننده، خود می‌تواند یک خدمت ابری باشد). دسترسی به API‌ها یا داده‌های on-premise از محیط ابری برای خدمات ابری که نیاز به دسترسی به این قابلیت‌ها دارند. (بطور مثال، برای جلوگیری از دسترسی غیرمجاز، قابلیت‌های مدیریت API مناسب جایگزین شوند تا مشکلات امنیتی ایجاد شده برطرف شوند). در هنگام استفاده از چندین فراهم‌کننده خدمات ابری، اطمینان حاصل شود که فناوری‌های امنیتی پشتیبانی‌شده توسط خدمت ابری دوم، زمانی که خدمت ابری از قابلیت‌های خدمت ابری دوم استفاده می‌کند، قابل استفاده هستند.	امنیت
ضرورت بررسی اینکه آیا سامانه‌های داخلی موجود برای مواجهه با جنبه‌های کسب و کاری استفاده از خدمات ابری در دسترس هستند یا خیر. اگر در دسترس نیستند، نصب سامانه‌های جدید برای پوشش این جنبه‌ها در نظر گرفته شود. در صورت در دسترس بودن، نحوه اتصال آن سامانه‌ها به قابلیت‌های کسب و کاری خدمت(های ابری) در نظر گرفته شود. بررسی اینکه آیا رابط‌های خدمات فراهم‌کننده ابری برای قابلیت‌های کسب و کاری و مدیریتی در نظر گرفته شده‌اند یا خیر. – اصرار بر اینکه فراهم‌کننده خدمات ابری از فناوری‌های کلیدی باز (استانداردهای باز و/یا منبع باز) برای رابط‌های مدیریتی و کسب و کاری پشتیبانی می‌کند. – رابط‌های معمول و باز پشتیبانی از چندین فراهم‌کننده را بطور همزمان آسان‌تر می‌کنند و نیز جابجایی از یک فراهم‌کننده به یک فراهم‌کننده متفاوت را آسان‌تر می‌کنند. تست واسط‌های فراهم‌کننده خدمات ابری برای قابلیت‌های مدیریتی و تجاری و اطمینان از اینکه می‌توان آنها را بطور مستقیم یا ادغام با سیستم‌های in-house موجود یا جدید استفاده کرد.	کسب و کاری و مدیریتی
اطمینان از اینکه الزامات کلیدی تعامل‌پذیری و قابلیت حمل در قرارداد خدمات ابری مشتری گنجانده شده است.	توافق سطح خدمت (SLA)

۶ چارچوب و نیازمندی‌های بلوغ رایانش ابری

هدف مدیریت رایانش ابری، استفاده کارآمد از منابع ابری، اطمینان از ثبات خدمات ابری و انعطاف‌پذیری کاربر خدمت ابری است. اتحادیه جهانی مخابرات (ITU) یک چارچوب بلوغ رایانش ابری بر اساس طراحی چهار ماژول و سه بعد توصیف کرده که از فرآیندهای مدیریتی مستقل از فناوری مورد استفاده پشتیبانی می‌کند [۱۲].

براساس این چارچوب، نیازمندی‌های بلوغ حاصل از سه بعد فناوری، مدیریت و بهره‌وری می‌باشد. اجزای این چارچوب در شکل ۹ نمایش داده شده است. چهار ماژول مدیریت عبارتند از: مدیریت مشتری ابری (CCMM)^۱، مدیریت خدمات ابری (CSMM)^۲، مدیریت منابع ابری (CRMM)^۳ و مدیریت امنیت ابری (CSEMM)^۴. هر یک از این پیمانه‌ها در این سه بعد باید در نظر گرفته شوند. هریک از پیمانه‌ها، نیازمندی‌های بلوغ خود را داراست و با سایر پیمانه‌ها ارتباط دارد.



شکل ۹: چارچوب عملکردی بلوغ رایانش ابری [۱۲]

- مدیریت مشتری ابری (CCMM): مدیریت معماری ابری، مدیریت ظرفیت ابری، مدیریت دسترسی ابری، مدیریت ریسک

^۱ Cloud Customer Management Module (CCMM)

^۲ Cloud Service Management Module (CSMM)

^۳ Cloud Resource Management Module (CRMM)

^۴ Cloud Security Management Module (CSEMM)

تداوم برنامه کاربردی و مدیریت استراتژی ابری

- مدیریت خدمات ابری (CSMM): شامل دو دسته است.

- توزیع خدمات ابری: مدیریت کاتالوگ خدمات، مدیریت SLA، مدیریت گزارش‌دهی خدمات، باز بودن خدمت، مدیریت پشتیبانی از خدمات، مدیریت رضایت از خدمات
- بهره‌برداری و نگهداری از خدمات: مدیریت نظارت بر خدمات، مدیریت دانش خدمات، مدیریت وظیفه خدمات، مدیریت تغییر خدمات، مدیریت مشکلات خدمات

- مدیریت منابع ابری (CRMM): تضمین منابع، مدیریت اندازه‌گیری منابع، مدیریت پویای منابع، تخصیص منابع، استقرار منابع و بازیافت منابع

- مدیریت امنیت ابری (CSEMM): اعتماد ابری، امنیت مجازی‌سازی، امنیت شبکه، امنیت داده، امنیت برنامه کاربردی، دسترسی امن، امنیت خدمت

در جدول ۷، الزامات بلوغ رایانش ابری که حاصل از بررسی موردها می‌باشد، آورده شده است.

جدول ۷: توصیه‌های بلوغ رایانش ابری

توصیه‌ها	حوزه مدیریت
مدیریت معماری ابری: توصیه می‌شود که فراهم کننده خدمات ابری ^۱ ، معماری باز و پیمانانه‌ای برای پشتیبانی از مدیریت منابع ناهمگن و مدیریت اعتماد میان ابری فراهم نماید.	مدیریت مشتری ابری
مدیریت ظرفیت ابری: توصیه می‌شود که فراهم کننده داده‌های اندازه‌گیری ظرفیت را فراهم نموده و در سطح بالای بلوغ، پیش‌بینی ظرفیت را اجرا نماید.	
بکارگیری هزینه منابع ابری: توصیه می‌شود که فراهم کننده از بهینه‌سازی استفاده از منابع برای بهبود هزینه استفاده از منابع ابری پشتیبانی نماید.	
مدیریت دسترسی ابری: توصیه می‌شود که فراهم کننده، یک خدمت بک‌آپ داده و بازیابی اطلاعات در ارتباط با تداوم کسب و کار و بازیابی در هنگام بلایا ^۲ فراهم نماید.	
مدیریت تداوم برنامه کاربردی: توصیه می‌شود که فراهم کننده، از تمرین تداوم برنامه کاربردی در چندابری ^۳ یا بین‌ابری ^۴ برای اطمینان از ثبات و اطمینان خدمات پشتیبانی کند.	
مدیریت استراتژی ابری: توصیه می‌شود که فراهم کننده برنامه‌ریزی راهبرد ابری را متناسب با تقاضاهای CSC تنظیم کند. برنامه‌ریزی راهبرد ابری شامل چندابری، بین‌ابری می‌باشد اما محدود به آنها نمی‌شود.	
مدیریت اندازه‌گیری منابع: توصیه می‌شود که فراهم کننده از بروزرسانی مداوم پیکربندی و اندازه‌گیری داده‌ها پشتیبانی کند. توصیه می‌شود که فراهم کننده از باز بودن و در دسترس بودن منابع ابری و داده‌های استفاده شده آنها توسط API ها یا اشکال دیگر پشتیبانی کند.	مدیریت منابع ابری
مدیریت پویای منابع: توصیه می‌شود که فراهم کننده، برنامه‌ریزی منابع خودکار را انجام دهد.	

^۱ Cloud Service Provider (CSP)

^۲ business continuity and disaster recovery (BC/D)

^۳ Multi-cloud

^۴ Inter-cloud

توصیه‌ها	حوزه مدیریت
تخصیص منابع: توصیه می‌شود که فراهم‌کننده خودکارسازی را برای تخصیص منابع ابری فراهم کند.	مدیریت خدمات ابری
استقرار منابع: توصیه می‌شود که فراهم‌کننده خودکارسازی را برای استقرار منابع ابری فراهم کند.	
باز یافت منابع: توصیه می‌شود که فراهم‌کننده خودکارسازی را برای باز یافت منابع ابری فراهم کند.	
مدیریت کاتالوگ خدمات: توصیه می‌شود که فراهم‌کننده از مدیریت کاتالوگ خدمات ابری پشتیبانی نماید.	
باز بودن خدمت: توصیه می‌شود که فراهم‌کننده، API های خدمات ابری را فراهم نماید.	
مدیریت پشتیبانی خدمات: توصیه می‌شود که فراهم‌کننده، پشتیبانی خدمات ابری را انجام دهد. توصیه می‌شود که فراهم‌کننده از چارچوب نگهداری یکپارچه به صورت کپسوله شده پشتیبانی نماید.	
مدیریت گزارش‌های خدمات: توصیه می‌شود که فراهم‌کننده، گزارش ارزیابی و شارژ شامل توزیع بهره‌برداری، میانگین بهره‌برداری و اوج بهره‌برداری را ارائه دهد.	
مدیریت رضایت از خدمات: توصیه می‌شود که فراهم‌کننده از یک نظرسنجی رضایت برای غنی سازی و بهبود فضای خدمات ابری خود پشتیبانی کند.	
مدیریت تغییر خدمات: توصیه می‌شود که فراهم‌کننده، یکپارچه‌سازی و استقرار مستمر را برای پشتیبانی از فرایند مدیریت تغییر فراهم کند.	
مدیریت مشکلات خدمات: توصیه می‌شود که فراهم‌کننده از ثبت مشکلات خدمات، حفظ لیست مشکلات خدمات و طبقه‌بندی مشکلات براساس فوریت و اولویت پشتیبانی نماید.	
مدیریت دانش خدمات: توصیه می‌شود که فراهم‌کننده، پایگاه داده مدیریت دانش برای ارائه سوالات پرسیده شده مکرر (FAQ) ایجاد کند. توصیه می‌شود که فراهم‌کننده، پایگاه داده دانش راهبرد برای افزایش قابلیت نگهداری ایجاد کند.	مدیریت امنیت ابری
مدیریت وظایف خدمات: توصیه می‌شود که فراهم‌کننده، سوالات یا مشکلات CSC را به وظایف و سوابق اختصاص داده و به صورت فابل رهگیری سازماندهی کرده و آنها را در یک فرایند مدیریت وظیفه اجرا کند.	
مدیریت اعتماد ابری: توصیه می‌شود که فراهم‌کننده، از مدیریت اعتماد بین ابری برای ترغیب مهاجرت به سمت چند ابری پشتیبانی کند.	
امنیت مجازی سازی: توصیه می‌شود که فراهم‌کننده، از کنترل ترافیک شرق به غرب ^۱ بین ماشین‌های مجازی پشتیبانی کند. توصیه می‌شود که فراهم‌کننده، از جداسازی خطا بین ماشین‌های مجازی پشتیبانی کند.	
امنیت شبکه: توصیه می‌شود که فراهم‌کننده، از جداسازی ترافیک شبکه در بین برنامه‌های کاربردی CSC ها پشتیبانی کند.	
امنیت داده: توصیه می‌شود که فراهم‌کننده، کنترل داده‌ها را در حالت استراحت و در حال انتقال اعمال کند. توصیه می‌شود که فراهم‌کننده، از رمزگذاری داده، احراز هویت یکپارچه‌گی داده، نرم‌افزار و امضای داده پشتیبانی نماید.	
دسترسی امن: توصیه می‌شود که فراهم‌کننده، از یک خدمت IAM ^۲ پشتیبانی کند که دسترسی ایمن به لایه کاربر از پشته مجازی سازی، پلتفرم و برنامه کاربردی را فراهم می‌کند.	
خدمت امنیت: اختیاری است که فراهم‌کننده، خط پایه امنیتی پیکربندی را برای سیستم‌عامل و پلتفرم فراهم کند.	

^۱ East-west traffic (جریان بسته‌های داده بین سرورها در یک مرکز داده)

^۲ Identity and Access Management (IAM)

توصیه‌ها	حوزه مدیریت
توصیه می‌شود که فراهم‌کننده، از خدمات امنیتی مختلف پشتیبانی کند.	

۷ رویکرد بومی ابر

به طور کلی، بومی‌ابر^۱ رویکردی برای ساخت و اجرای برنامه‌های کاربردی است که از مزایای مدل محاسبات ابری بهره‌برداری می‌کند. رویکرد بومی‌ابر به نحوه ایجاد و استقرار برنامه‌های کاربردی اشاره می‌کند، نه جایی که آنها اجرا می‌شوند. این شامل مواردی مانند معماری‌های خدمات، زیرساخت به‌عنوان یک کد، خودکارسازی، خطوط لوله یکپارچه/تحویلی^۲ پیوسته، ابزارهای قابلیت مشاهده/ نظارتی و غیره است.

یکی از ویژگی‌های کلیدی بومی‌ابر این است که چگونه یک سامانه برنامه‌های کاربردی را ایجاد و مستقر می‌کند. طبق تعریف CNCF^۳، بومی‌ابر به این معناست که برنامه‌های کاربردی کانتینری^۴ شده است و از پشته نرم‌افزار منبع باز استفاده می‌کند. یک برنامه کاربردی بومی ابر (CNA^۵) به عنوان ریزخدماتی با اتصال آزاد^۶ برای بهبود چابکی و مدیریت‌پذیری توسعه داده شده است. هر ریزخدمت در یک کانتینر بسته‌بندی می‌شود و یک هماهنگی و همزمان کننده پویای مرکزی کانتینرها را برای مدیریت کارآمد منابع سرور و کاهش هزینه‌های عملیاتی، برنامه‌ریزی می‌کند [۱۳].

برنامه‌های کاربردی بومی ابر همچنین به یک محیط DevOps نیاز دارند. DevOps به یک نوعی از توسعه یا متدولوژی عملیاتی اشاره دارد که توسعه نرم‌افزار و عملیات فناوری اطلاعات را ادغام می‌کند. بطور سنتی، تیم توسعه سعی می‌کرد خدمات را با افزودن ویژگی‌های جدید بهبود بخشد در حالیکه تیم عملیاتی تمایلی به تغییر برای حفظ عملیات خدمات قابل اعتماد نداشت.

^۱ Cloud Native

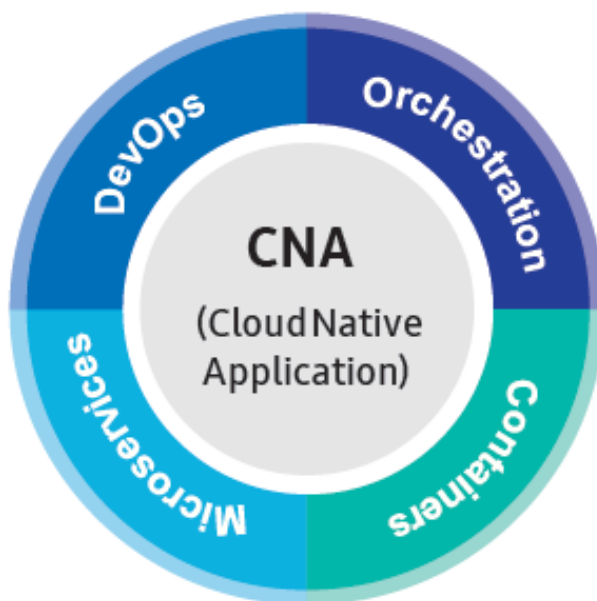
^۲ integration/delivery pipelines

^۳ Cloud Native Computing Foundation

^۴ containerized

^۵ cloud native application

^۶ loosely-coupled



شکل ۱۰: الزامات برنامه کاربردی بومی ابر [۱۳]

در محیط فناوری اطلاعات محور امروزی، خدمات باید به سرعت و به راحتی منتشر شوند، از این رو خدمات بطور مداوم در حال به‌روزرسانی و بهبود هستند بطوریکه منعکس کننده تقاضاهای بازار می‌باشند. در یک محیط DevOps، هم تیم توسعه و هم تیم عملیاتی تحت اهداف کسب و کاری مشترک که شامل کاهش زمان توسعه و ارائه خدمات بهبود یافته است، با یکدیگر و نزدیک به هم کار می‌کنند. توسعه‌دهندگان ویژگی‌های جدید را برنامه‌ریزی کرده و می‌سازند، آنها را در سامانه مستقر کرده، سپس خدمت را اجرا می‌کنند و آن را برای بهبود نظارت می‌کنند. برای توسعه و بهبود سریع، DevOps بطور مداوم خدمات را با خودکار کردن فرآیندهای دستی موجود، یکپارچه و مستقر می‌کند. همچنین، از جمله ویژگی‌های cloud native می‌توان به موارد ذیل اشاره نمود [۱۴]:

- سرعت: معرفی سریع و کم‌هزینه خدمات جدید در مقیاس کوچک
- مقیاس: مقیاس کردن سریع با هزینه پایین از هزاران کاربر به میلیون‌ها کاربر
- عملیات‌های کارا و موثر: خودکارسازی، عملیات‌های بدون تماس، میراث و خدمات جدید، استقلال چرخه حیات (خدمات/زیرساخت)
- کارایی و ظرفیت: ظرفیت بهینه شده توان عملیاتی و بهره‌برداری از منابع

۷-۱ معماری بومی ابر

یک معماری بومی ابر، معماری است که در آن یک برنامه کاربردی به‌طور خاص برای استقرار ابر طراحی شده است. معماری‌های بومی ابر، آن‌هایی هستند که از مواردی که پلتفرم‌های ابری به خوبی انجام می‌دهند، بهره می‌برند. به عنوان مثال، کوچک کردن یک برنامه مبتنی بر ابر به سادگی با افزودن گره‌های سرور بیشتر، و همچنین کاهش مقیاس اگر افزایش مقیاس به دلیل افزایش موقت تقاضا باشد، انجام می‌شود (به عنوان مثال، وبسایت یک خرده‌فروش در جمعه سیاه یا دوشنبه سایبری). بنابراین برنامه‌های

کاربرد ابری باید قابلیت مقیاس‌بندی افقی را ارائه دهند و برنامه‌های کاربردی یکپارچه^۱ نباشند که روی یک سرور منفرد مستقر شوند. این تا حدی با اتخاذ یک معماری ریزخدمت انجام می‌شود، جایی که برنامه به قطعات عملکردی کوچکی تجزیه می‌شود که می‌توانند به طور مستقل مستقر شوند و از طریق API‌های باثبات و با وضوح تعریف شده به هم متصل شوند.

به‌طور مشابه، هنگامی که یک برنامه کاربردی کوچک شده و در چندین گره مستقر می‌شود، مطلوب است که سامانه در برابر خرابی‌هایی که بر یک یا تعداد کمی از گره‌ها تأثیر می‌گذارد، مقاوم باشد. بنابراین، یک برنامه کاربردی بومی ابر باید طوری طراحی شود که در صورت قطع گره به کار خود ادامه دهد و به خوبی از خرابی‌ها بازیابی کند.

توسعه قابلیت‌هایی مانند مقیاس‌پذیری افقی و تحمل خطا از ابتدا دشوار است، اما این ویژگی‌ها جزء کلیدی پلتفرم‌های کانتینری‌سازی^۲ مانند Docker هستند. به همین دلیل است که بسیاری از شرکت‌ها به عنوان بخشی از هرگونه مهاجرت به فضای ابری، به یک پلتفرم کانتینری منتقل می‌شوند و به همین دلیل است که پذیرش معماری مبتنی بر کانتینر مترادف با Cloud Native بودن در نظر گرفته می‌شود. یک چارچوب اركستراسیون کانتینر مانند Kubernetes (که اساس پشته‌های بسته‌بندی شده مانند Red Hat OpenShift است) برای مدیریت استقرار کانتینرها لازم است.

یک معماری مبتنی بر کانتینر، برنامه‌ای را که قرار است اجرا شود، را در بر می‌گیرد و آن را با تمام وابستگی‌هایش در یک تصویر جمع می‌کند که شامل همه چیزهایی است که برای اجرای یک برنامه لازم است بطوریکه شامل زمان‌های اجرا^۳ زبان، کتابخانه‌های نرم‌افزار، و کد برنامه کاربردی می‌باشد. سپس این تصویر در یک مخزن متمرکز (عمومی یا خصوصی) ذخیره می‌شود و پس از آن استقرار برنامه از طریق ابزارهای ساده‌ای انجام می‌شود که تصویر را در سامانه هدف کپی می‌کند، ظرفی را برای اجرا ایجاد می‌کند (بطوریکه جداسازی از سایر برنامه‌های کانتینری‌شده را فراهم می‌کند که ممکن است بر روی همان سرور فیزیکی اجرا شود)، و در صورت لزوم با منابعی مانند پورتهای شبکه ارتباط برقرار می‌کند.

در حالی که مجموعه‌ای از معیارهای مورد توافق جهانی برای تعریف یک برنامه کاربردی بومی ابر وجود ندارد، اکثر منابع موافق هستند که یک برنامه کاربردی که به مجموعه‌ای از ریزخدمات تجزیه شده است، با این ریزخدمات‌ها که از طریق کانتینرها مستقر شده‌اند، واجد شرایط به عنوان C بومی ابر هستند. داشتن یک چارچوب پیوسته ادغام/استقرار مستمر که به تصاویر کانتینر اجازه می‌دهد تا به‌طور منظم مطابق با شیوه‌های توسعه نرم‌افزار چابک به روز شده و مستقر شوند، ویژگی دیگری است که معمولاً با معماری بومی ابر مرتبط است [۱۵].

۷-۲ الزامات بومی ابر

در سال‌های اخیر، معماری برنامه‌های کاربردی به‌گونه‌ای تحول یافته‌اند که با برنامه‌های کاربردی بومی ابر و ریزخدمات‌ها، خدمات

^۱ monolithic apps

^۲ containerization platforms

^۳ runtimes

بدون سرور و خدمات مبتنی بر رویداد^۱ که بر روی زیرساخت‌های تغییرناپذیر در پلتفرم‌های ترکیبی^۲ و چند ابری اجرا می‌شوند، جا بیفتند [۱۶].

به گفته بنیاد رایانش بومی ابر (CNCF)، فناوری‌های بومی ابر سازمان‌ها را قادر می‌سازد تا برنامه‌های مقیاس‌پذیر را در محیط‌های مدرن و پویا مانند ابرهای عمومی، خصوصی و ترکیبی بسازند و اجرا کنند. کانتینرها، مش‌های خدماتی، ریزخدمات‌ها، زیرساخت‌های تغییرناپذیر و API های اعلامی^۳ نمونه‌ای از این رویکرد هستند. این راهکارها سامانه‌های loosely coupled را قادر می‌سازند که انعطاف‌پذیر، قابل مدیریت و قابل مشاهده باشند. همراه با خودکارسازی قوی، به مهندسان اجازه می‌دهند تا تغییراتی با تاثیر زیاد و به طور مکرر و قابل پیش‌بینی با حداقل زحمت ایجاد کنند.

در حالیکه راه‌های زیادی برای ساخت و معماری برنامه‌های کاربردی بومی ابر وجود دارد، موارد زیر باید به عنوان الزامات در این نوع معماری در نظر گرفته شود:

- زمان اجرا: این برنامه‌ها به احتمال زیاد به زبان کانتینر یا/و بومی کوبرنیتیز^۴ و با استفاده از ابزارهایی مانند Node.js، Java، Go، Python و Ruby نوشته می‌شوند
- امنیت: هنگام استقرار و نگهداری برنامه‌های کاربردی در یک محیط برنامه کاربردی چند ابری یا ابر ترکیبی، امنیت از اهمیت بالایی برخوردار است و باید بخشی از محیط باشد.
- قابلیت مشاهده: استفاده از ابزارهایی مانند Prometheus، Grafana و Kiali که می‌توانند با ارائه معیارهای در زمان واقعی و اطلاعات بیشتر در مورد نحوه استفاده و رفتار برنامه‌های کاربردی در فضای ابری، قابلیت مشاهده را افزایش دهند.
- کارایی: تمرکز بر استفاده حافظه‌های کوچک، اندازه کوچک آرتیفکت‌ها و زمان راه‌اندازی سریع به منظور پشتیبانی قابل حمل برنامه‌ها در پلتفرم‌های ترکیبی/چند ابری است.
- قابلیت همکاری: یکپارچه نمودن برنامه‌های کاربردی cloud-native با فناوری‌های منبع باز به‌طوری که امکان مواجهه با الزامات ذکر شده در بالا، از جمله Infinispan، MicroProfile، Kafka، Jaeger، Prometheus و غیره را برای ساخت معماری‌های استاندارد زمان اجرا برآورده نماید.
- DevOps/DevSecOps: این متدولوژی‌ها برای استقرار مداوم در تولید، در راستای حداقل محصول قابل دوام^۵ (MVP) و با امنیت به عنوان بخشی از ابزار طراحی شده‌اند.

۷-۳ اصول معماری برنامه کاربردی بومی ابر

ویژگی‌های معماری‌های بومی ابر ممکن است متفاوت باشند، اما اکثر طراحی‌ها مفاهیم زیر را در بر می‌گیرند:

^۱ event-driven

^۲ hybrid

^۳ declarative

^۴ Kubernetes

^۵ minimum viable product

پردازش بدون حالت^۱: پردازش بدون حالت یک مفهوم اصلی در برنامه‌های کاربردی cloud native است که مقیاس‌پذیری بالا با تحمل خطای ذاتی را ممکن می‌سازد. این شامل یک سامانه پردازش تراکنشی است که به دو لایه تقسیم می‌شود. یک لایه شامل تعداد متغیر عناصر تراکنش است که اطلاعات حالت طولانی مدت را حفظ نمی‌کنند، در حالیکه لایه دیگر شامل یک سامانه ذخیره‌سازی مقیاس‌پذیر است. سامانه ذخیره‌سازی از عناصر مختلفی برای ذخیره داده‌های حالت به صورت ایمن و اضافی استفاده می‌کند. مولفه پردازش تراکنش، داده‌های حالت را از سامانه ذخیره‌سازی حالت پردازش می‌کند تا تراکنش‌ها را انجام دهد، و داده‌های حالت جدید (در حین تراکنش‌ها به‌روز می‌شوند) را در سامانه ذخیره‌سازی می‌نویسد.

ریزخدمات‌ها: ریزخدمات‌ها یک رویکرد معماری هستند که برنامه‌های پیچیده را به بخش‌های کوچکتر و قابل مدیریت‌تر تقسیم می‌کند. یک ریزخدمت یک فرآیند مستقل است که از طریق یک API زبان آگنوستیک^۲ با دیگران ارتباط برقرار می‌کند. هر خدمت کاملاً ایزوله است و برای تکمیل یک کار خاص اختصاص داده شده است. معماری‌های ریزخدمت، رویکرد ساخت کاربردهای پیمانه‌ای را امکان‌پذیر می‌کنند و استفاده مجدد و طراحی مجدد عناصر منفرد را آسان‌تر می‌کنند. این قابلیت پیمانه‌ای^۳ همچنین از تنوع فناوری پشتیبانی می‌کند و توسعه، استقرار و مقیاس‌بندی آسان‌تر را امکان‌پذیر می‌نماید.

کانتینر سازی^۴: کانتینرها به روشی فراگیر برای ساخت برنامه‌های کاربردی cloud native تبدیل شده‌اند. کانتینرها از فضاهای نام لینوکس^۵ (پارتیشن‌های طولانی مدت) برای حفظ ایزوله بین سامانه‌های فایل، پشته‌های شبکه و فرآیندها استفاده می‌کنند. کانتینرها پارتیشن‌های امنی براساس روش فضای نام هستند که هر کدام یک یا چندین فرآیند لینوکس را اجرا می‌کنند. یک هسته^۶ لینوکس بر روی یک میزبان از این فرآیندها پشتیبانی می‌کند.

کانتینرها مشابه ماشین‌های مجازی (VM) کار می‌کنند، اگرچه کانتینرها بسیار انعطاف‌پذیرتر هستند. در حالیکه نصب VMها فقط از طریق پشتیبانی یک سیستم عامل کامل امکان‌پذیر است، کانتینرها می‌توانند از برنامه‌های کاربردی با بسته‌بندی نرم‌افزاری پشتیبانی کنند. این رویکرد بسته‌بندی به توسعه‌دهندگان اجازه می‌دهد تا برنامه‌های کاربردی را به راحتی اضافه کنند. تفاوت مهم دیگر این است که کانتینرها وزن کمتری نسبت به ماشین‌های مجازی دارند و به منابع و نگهداری کمتری نیاز دارند. آنها می‌توانند سریعتر شروع کنند، به راحتی مستقر شوند و قابلیت حمل بالاتری را ارائه می‌دهند.

همکاری و ارتباطات: خدمات بومی ابر باید توانایی برقراری ارتباط و تعامل با یکدیگر و با خدمات خارجی را داشته باشند. APIها (معمولاً، APIهای RESTful) ارتباط بین برنامه‌های کاربردی بومی ابر و برنامه‌های قدیمی یا شخص ثالث را امکان‌پذیر می‌کنند. ریزخدمات‌ها می‌توانند مدیریت و ارتباطات داخلی را با ایجاد یک لایه زیرساخت اختصاصی، به نام مش خدمات، که این ارتباطات را مدیریت می‌کند، تسهیل کنند. نقش اصلی یک خدمت مش، ایمن‌سازی، اتصال و نظارت بر خدمات در برنامه‌های کاربردی بومی ابر است. اگرچه Istio پرکاربردترین خدمت مش است، چندین پیاده‌سازی منبع باز نیز در دسترس می‌باشند.

^۱ Stateless processing

^۲ language-agnostic

^۳ modularity

^۴ Containerization

^۵ Linux namespaces

^۶ Kernel

خودکارسازی: معماری‌های بومی ابر خودکارسازی زیرساخت را تسهیل کرده و به توسعه‌دهندگان اجازه می‌دهند خطوط لوله یکپارچه‌سازی و تحویل مستمر (CI/CD)^۱ را پیاده‌سازی کنند و وظایفی مانند استقرار، مقیاس‌بندی و بازیابی را تسریع می‌بخشند. خط لوله CI/CD مراحل ساخت، آزمایش و استقرار چرخه عمر توسعه را خودکار می‌کند. سیستم‌های بومی ابر همچنین از فرآیندهای خودکار مانند بازگشت، بازیابی، استقرار canary و نظارت پشتیبانی می‌کنند.

دفاع در عمق^۲: معماری‌های کاربردی سنتی عمدتاً به یک محیط امنیتی برای جلوگیری از نفوذ متکی هستند. با این حال، صرف نظر از اینکه یک سازمان چقدر شبکه خود را سخت می‌کند، اتکاء به یک خط دفاعی برای جلوگیری از حملات داخلی و خارجی کافی نیست. چالش دیگر برای رویکرد محیطی شبکه سنتی، باز کردن شبکه برای دسترسی از راه دور و دستگاه‌های موبایل برای پاسخگویی به خواسته‌های کاربر است. معماری‌های بومی ابر طبق تعریف از خدمات اینترنتی استفاده می‌کنند، بنابراین باید از محافظت‌های داخلی برای کاهش حملات خارجی برخوردار باشند. دفاع در عمق یک رویکرد امنیتی است که بر امنیت داخلی سامانه تأکید دارد و بر اساس راهبرد نظامی کاهش سرعت حمله با دفاع‌های چند لایه است. در محیط‌های محاسباتی، این کار با اجرای چالش‌های احراز هویت بین تمام اجزای داخل شبکه، با از بین بردن اعتماد ضمنی بین اجزا انجام می‌شود. معماری‌های cloud native می‌توانند علاوه بر احراز هویت، اصل دفاع را در عمق با script injection و محدود کردن نرخ گسترش دهند. هر جزء طراحی باید از خود در برابر سایر اجزا محافظت کند، حتی اگر بخشی از همان معماری باشد. این رویکرد معماری بومی ابر را انعطاف‌پذیرتر کرده و سازمان‌ها را قادر می‌سازد تا خدمات را در محیط‌های ابری بدون شبکه قابل اعتماد بین کاربران و خدمت مستقر کنند.

۸ نتیجه‌گیری

در این گزارش، به‌منظور شناسایی الزامات قابلیت همکاری خدمات ابری و اتصال مراکز داده به ابر، مشخصه‌ها و ویژگی مرتبط با هر یک از جنبه‌های مهاجرت به پلتفرم ابری، قابلیت همکاری مراکز داده و ابری در سطوح کسب و کاری، پلتفرم فنی، زیرساخت مراکز داده، شبکه ارتباطی، داده‌های سازمانی و امنیت مراکز داده و ابر بررسی گردید.

توسعه شبکه ملی اطلاعات و نیز هوشمندسازی دولت از جمله اهداف اصلی در برنامه هفتم توسعه کشور هستند که وزارت ارتباطات و فناوری اطلاعات موظف است با مشارکت و سرمایه‌گذاری بخش غیردولتی از طریق سازمان توسعه‌ای زیرمجموعه خود نسبت به تأمین زیرساخت‌های لازم اعم از ارتباطی و اطلاعاتی (ابری) و ذخیره‌سازی و پردازش سریع در این رابطه اقدام نماید. انتقال زیرساخت‌های سازمانی به فضای ابری، تحولی فناوری-محور و مبتنی بر ساختار کسب و کار است که در این رابطه در برنامه هفتم در بخش هوشمندسازی و دولت الکترونیک، دستگاه‌های اجرایی موظف شده‌اند تا با رعایت قانون مدیریت داده‌ها و اطلاعات ملی، مراکز داده اصلی و پشتیبان خود را به زیرساخت یکپارچه ابری دولت‌هوشمند متصل نمایند.

در این رابطه، طرح بلند مدت ابر دولت در راستای تحقق اهداف توسعه‌ای شبکه ملی اطلاعات و به‌منظور طراحی و توسعه زیرساخت‌های رایانش ابری دولت الکترونیک در حال انجام است. اهداف اصلی در این طرح عبارتند از: طراحی کلان ابر دولت،

^۱ Continuous Integration and Continuous Delivery (CI/CD)

^۲ Defense in Depth

تعیین معماری زیرساخت یکپارچه مراکز داده و ابری سازمان‌های دولتی، طراحی بستر ارائه خدمات ابری شامل زیرساخت، پلتفرم و نرم‌افزار به‌منظور توسعه دولت هوشمند و ارائه نقشه راه توسعه خدمات ابر دولت.

چالش‌های زیادی در ارتباط با قابلیت همکاری رایانش ابری وجود دارد. بطور کلی، رابط‌ها و رابط‌های برنامه‌نویسی کاربردی خدمات ابری استاندارد نیستند و ارائه‌دهندگان برای خدمات ابری مشابه از رابط‌های متفاوتی استفاده می‌کنند. قابلیت حمل به جابجایی داده‌ها برنامه‌های ابری اشاره دارد. اولین جنبه قابل حمل بودن داده‌ها بین خدمات ابری این است که باید قابلیت بازیابی داده‌های مشتری از خدمت ابری منبع و همچنین، قابلیت وارد کردن داده‌های مشتری به خدمت ابری مورد نظر وجود داشته باشد. توجه به این نکته ضروری است که API مورد استفاده برای خدمت منبع ممکن است با API مورد استفاده برای خدمت هدف یکسان نباشد و ممکن است در هر مورد به ابزارهای متفاوتی نیاز باشد.

بیشترین سطح قابلیت همکاری به احتمال در خدمات ابری IaaS وجود دارد، جایی که عملکرد غالباً به‌طور گسترده معادل و مشابه است و تعدادی رابط استاندارد وجود دارد (برخی بطور رسمی مانند رابط مدیریت داده‌های ابری^۱ استاندارد شده‌اند و برخی دیگر به‌عنوان استانداردهای غیررسمی^۲ در بازار وجود دارند). خدمات ابری PaaS سطوح پایین‌تری از تعامل‌پذیری را دارند. استانداردهای رابط کمی برای عملکرد PaaS وجود دارد.

برنامه‌های SaaS بیشترین چالش را در قابلیت همکاری ابری دارند. رابط‌های استاندارد بسیار کمی برای برنامه‌نویسی کاربردهای SaaS وجود دارد و حتی جابجایی از یک برنامه SaaS به برنامه SaaS دیگر با عملکردهای مشابه معمولاً شامل تغییر در رابط است. بدین جهت، تأثیر متقابلی هم بر روی کاربران نهایی خدمت ابری برای هر رابط کاربری و هم بر هر برنامه کاربردی یا سامانه متعلق به مشتری خدمت ابری که از API های ارائه شده توسط برنامه SaaS استفاده می‌کند، وجود دارد. برخی از رویکردهای عملی برای مدیریت چنین چالش‌های قابلیت همکاری وجود دارد. یک امکان به‌کارگیری یک لایه جداسازی^۳ یا لایه انطباق بین برنامه‌های کاربردی و سامانه‌های مشتری و رابط‌های خدمت ابری فراهم‌آورنده است بطوریکه خدمات ابری مستقیماً توسط برنامه‌های کاربردی مشتری فراخوانی نشوند. فناوری‌هایی مانند گذرگاه خدمات سازمانی^۴ (ESB) می‌توانند برای ساخت این لایه‌های جداسازی استفاده شوند. امکان دیگر استفاده از خدمات ارائه شده توسط یک فراهم‌کننده بین ابری^۵ (که گاهی اوقات کارگزار خدمات ابری نیز نامیده می‌شود) است، که نقش یک تطبیق‌دهنده رابط «استاندارد» ارائه شده به مشتری با مجموعه متفاوتی از رابط‌های ارائه‌شده توسط فراهم‌کنندگان خدمات ابری مختلف را بر عهده می‌گیرد.

در خصوص قابلیت حمل برنامه کاربردی، بزرگترین چالش‌ها برای برنامه‌های کاربردی ساخته شده برای پلتفرم‌های PaaS است. برای خدمات ابری IaaS، در عمل تعدادی استاندارد مانند OVF^۶ وجود دارد که قابلیت جابجایی برنامه‌های کاربردی را فراهم نموده و ارائه سیستم‌عامل‌های رایج مانند لینوکس را امکان‌پذیر می‌سازد. پلتفرم‌های PaaS می‌توانند به‌طور گسترده‌ای بین

^۱ Cloud Data Management Interface (CDMI)

^۲ De-facto

^۳ isolation

^۴ Enterprise Service Bus

^۵ inter-cloud provider

^۶ Open Virtualization Format

فراهم‌کنندگان مختلف متفاوت باشند. به عنوان مثال، برای اینکه یک PaaS مقیاس‌پذیر و کشسان باشد، ممکن است روش خاصی را برای تداوم و مدیریت داده‌ها اعمال کند که ممکن است توسط سایر پلتفرم‌های PaaS پشتیبانی نشوند. تفاوت‌های بین پلتفرم‌های جایگزین PaaS، بویژه در هنگام جابه‌جایی کدها، نیازمند مهندسی مجدد گسترده کد مشتری است. به نظر می‌رسد دو روند در بازار، نویدبخشی برای تسهیل شرایط باشند. اول، پذیرش فزاینده پلتفرم‌های منبع باز PaaS مشترک و دوم ظهور فناوری‌های کانتینرسازی که امکان تقسیم و استقرار مستقل بخش‌هایی از یک برنامه کاربردی را فراهم می‌کند.

فراتر از ردپا و تعداد سرورها، معماری مراکز داده ابری فرامقیاس برای سبک‌کاری کاربردهای سبز در مقیاس همگن طراحی می‌شود که به طور فزاینده‌ای از زیرساخت‌های تفکیک‌شده، با چگالی بالا و انرژی بهینه‌شده بهره می‌برد. یک فرامقیاس باید خدمات رایانش سفارشی شده، شبکه‌های پرسرعت و نرم‌افزارهای پیشرفته را برای میلیون‌ها مشتری فراهم آورد. راه‌حل‌های اتصال مرکز داده برای پاسخگویی به این نیازها با اتکاء به شبکه‌های تعریف شده نرم‌افزاری و خودکار منابع براساس نیاز، اتصال بین همه‌ی مکان‌ها را فراهم می‌کند و یک مجموعه بزرگ را قادر می‌سازد تا به عنوان یک موجودیت رفتار کند.

کاربردهای اتصال مراکز داده از نظر ظرفیت و دامنه جغرافیایی بسیار متفاوت است. بنابراین، حمل بیشتر بیت‌ها در فاصله‌های دور بسیار مهم است. انتخاب کوتاه‌ترین مسیر تأخیر را به حداقل می‌رساند و تجهیزات نامناسب ممکن است منجر به تأخیر شود. برای مدیریت داده‌های بزرگ در حد ترابیت تجهیزات باید اتصالات قابل اعتماد و با ظرفیت بالا را عرضه نمایند. ایجاد ارتباط میان مراکز داده باید در کمترین زمان ممکن و بر پایه خودکارسازی فرآیندها و کاهش عملیات دستی باشد. جریان‌سازی داده‌های حجیم در میان مراکز داده باید به روشی مقرون به صرفه و مبتنی بر راه‌حل‌های شبکه‌سازی پرسرعت انجام شود.

مهاجرت از زیرساخت‌های قدیمی مراکز داده به خدمات ابری از جمله خدمات ابر عمومی برای سازمان‌ها مزایای زیادی از جمله صرفه‌جویی اقتصادی، بهبود کیفیت خدمات و دسترسی به ابزارها و فناوری‌های پیشرفته را به همراه دارد. راه‌حل‌های ابر عمومی و ابر ترکیبی روش‌های مقرون به صرفه برای استفاده، نگهداری و ارتقاء زیرساخت قدیمی فناوری اطلاعات داخلی سازمان‌ها را معرفی می‌نمایند. با این وجود راه‌حل‌های ابری همچنین دربرگیرنده مخاطراتی هستند که دولت و سازمان‌ها باید قبل از مهاجرت به محیط ابری آن‌ها را ارزیابی نمایند.

استفاده از ابر عمومی به نهادهای دولتی این امکان را می‌دهد که تا از چارچوب‌های امنیتی توسعه یافته و پیشرفته بدون نیاز به سرمایه‌گذاری و منابع انسانی قابل توجه استفاده کنند. بیشتر موارد نقض امنیت ناشی از سوء مدیریت کاربران در طراحی کنترل‌های محافظت از داده‌ها می‌باشد. امنیت یک «مسئولیت مشترک» بین مشتریان و فروشندگان ابری است و سازمان‌ها باید قبل از انتقال داده‌ها به محیط ابر، راهبردها و سیاست‌های ابری مناسب را توسعه داده و تیم مدیریتی را برای نظارت بر اجرای آنها تعیین کنند. سازمان‌ها باید از داده‌هایی که دارند، مکان قرارگیری آنها و مخاطرات مرتبط با هر نوع از داده‌ها آگاه باشند. پیچیدگی‌های مرتبط با ذخیره‌سازی داده‌ها در راه‌حل‌های ابری، آگاهی از اینکه چه کسی به آنها دسترسی دارد را دشوار می‌کند. ارائه‌دهندگان ابر عمومی باید اقدامات الف) تضمین کنترل کاربران بر داده‌ها بر اساس توافق‌نامه سطح خدمات برای پردازش داده‌ها، ب) شفاف‌سازی جمع‌آوری و استفاده از داده‌ها مطابق با مقررات عمومی و دولتی را برای محافظت از داده‌ها اعمال نموده و مسئولیت‌های مرتبط را با کاربران به اشتراک گذارند.

پذیرش یا مهاجرت به خدمات ابر عمومی، چشم‌انداز مخاطرات فناوری اطلاعات را تغییر می‌دهد و اقدامات دولت برای کاهش

مخاطرات می‌تواند شامل ۱- ایجاد یک راهبرد ابری و تهیه یک نقشه راه برای مهاجرت ابری شامل سامانه‌ها، خدمات و داده‌ها ۲- بازنگری سیاست‌ها برای به‌روزرسانی حاکمیت داده‌ها به منظور کاهش ریسک‌های فناوری، ۳- مشارکت با فراهم‌آوردندگان در حاکمیت ابری به منظور کاهش مخاطرات فروشنده، فناوری و عملیات، داده، پرسنل و امنیت، ۴- ساده‌سازی فرآیندهای مدیریت ابر و اطمینان از الزامات حفاظت از داده‌ها و میزبانی مطابق با قانون امنیت داده‌ها و ۵- استفاده از ابزارهای خودکارسازی پیشرفته برای بهره‌مندی از ابر و کاهش مخاطرات باشد.

سناریوهای مختلفی برای قابلیت‌حمل و قابلیت‌همکاری در محیط ابری مطرح است. برای هر یک از این سناریوها، ملاحظات عملیاتی را می‌توان در سطوح مختلف ۱- سیاست‌های کلی پیاده‌سازی ابر مانند استفاده از فناوری‌های باز، ۲- تعامل‌پذیری و قابلیت‌حمل خدمات مختلف ابری شامل نرم‌افزار به‌عنوان خدمت (SaaS)، پلتفرم به‌عنوان خدمت (Paas) و زیرساخت به‌عنوان خدمت (IaaS)، ۳- کسب و کاری و مدیریتی و ۴- توافق‌های سطح خدمت دسته‌بندی نمود.

رویکرد بومی‌ابر به این معناست که برنامه‌های کاربردی کانتینری شده است و از پشته نرم‌افزار منبع باز استفاده می‌کند. این رویکرد چگونگی ایجاد و استقرار برنامه‌های کاربردی را براساس موضوعاتی مانند معماری‌های ریزخدمات، زیرساخت به‌عنوان کد، خودکارسازی، خطوط لوله یکپارچه/تحویل و ابزارهای قابلیت مشاهده/نظارتی توصیف می‌کند. برنامه‌های کاربردی بومی ابر همچنین به یک محیط یکپارچه توسعه نرم‌افزار و عملیات فناوری اطلاعات نیاز دارند. از جمله ویژگی‌های بومی ابر عبارتند از: ۱- معرفی سریع و کم‌هزینه ریزخدمات، ۲- مقیاس کردن سریع با هزینه پایین از هزاران کاربر به میلیون‌ها کاربر، ۳- خودکارسازی، عملیات‌های بدون تماس و استقلال چرخه حیات (خدمات/زیرساخت) و ۴- ظرفیت بهینه‌شده توان عملیاتی و بهره‌برداری از منابع. فناوری‌های بومی ابر سازمان‌ها را قادر می‌سازد تا برنامه‌های مقیاس‌پذیر، انعطاف‌پذیر، قابل مدیریت و قابل مشاهده را در محیط‌های پویای ابرهای عمومی، خصوصی و ترکیبی با استفاده از ابزارهایی مانند کانتینرها، مش‌های خدماتی، ریزخدمات‌ها، زیرساخت‌های تغییرناپذیر و APIهای اعلامی ایجاد و اجرا کنند. راه‌های زیادی برای ساخت و معماری برنامه‌های کاربردی بومی ابر وجود دارد. موارد زمان اجرا، امنیت، قابلیت مشاهده، کارایی، قابلیت همکاری و تیم‌های توسعه و عملیات (امنیت) به عنوان الزامات این معماری در نظر گرفته می‌شوند.

۹ مراجع

- [۱] A Guide to Cloud Interoperability and Portability, ۱۰۱ Blockchains, ۲۰۲۳, <https://۱۰۱blockchains.com/cloud-interoperability-and-portability/>
- [۲] Open Virtualization Format White Paper, Version ۲,۰,۰, DMTF Informational, ۲۰۱۴, https://www.dmtf.org/sites/default/files/standards/documents/DSP۲۰۱۷_۲,۰,۰.pdf
- [۳] Portability and Interoperability, Cloud Governance, ۲۰۲۱, <https://cloud.carnegieendowment.org/cloud-governance-issues/portability-and-interoperability/#skeletabsPanel۱۹>
- [۴] NIST Cloud Computing Reference Architecture, Information Technology Laboratory, National Institute of Standards and Technology, September ۲۰۱۱
- [۵] What is Data Center Interconnect, VIAVI Solutions, <https://www.viavisolutions.com/en-us/what-data->

center-interconnect

- [۶] Data Center Interconnect: Details, Challenges & Solution, Sify Technologies, ۲۰۱۸, <https://www.sifytechnologies.com/us/blog/data-center-interconnect-details-challenges-solution/>
- [۷] Ensure dynamic and instant access to critical data, Sify Technologies, <https://www.sifytechnologies.com/data-center/datacenter-interconnect/>
- [۸] Government Migration to Cloud Ecosystem: Multiple Options ,Significant Benefits ,Manageable Risks, International Development Association for The World Bank, ۲۰۲۲, International Bank for Reconstruction and Development
- [۹] Interoperability and Portability for Cloud Computing: A Guide, Version ۲٫۰, Cloud Standards Customer Council, December, ۲۰۱۷
- [۱۰] بررسی ذی‌نفعان خدمات بستر توسعه نرم‌افزارهای کاربردی در شبکه ملی اطلاعات، پروژه امکان‌سنجی بومی‌سازی خدمات بستر توسعه نرم-افزارهای کاربردی شبکه ملی اطلاعات، ۱۴۰۱
- [۱۱] Cloud Standards Customer Council, Interoperability and Portability for Cloud Computing A Guide, Version ۲٫۰, December ۲۰۱۷, <https://www.omg.org/cloud/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf>
- [۱۲] ITU, Recommendation ITU-T Y.۳۵۲, Cloud computing maturity requirements and framework, ITU-T, ۱۲/۲۰۱۹
- [۱۳] Naresh Ramamurthy Avva & Sai Kiran Reddy Padooru, "Future of Cloud Computing Architecture", ۲۰۲۰
- [۱۴] Samsung, Technical Report: Cloud Native ۵G Core, Vol.۲, ۲۰۲۰
- [۱۵] Balaji Ethirajulu, "Cloud Native Introduction", Ericsson, ۲۰۱۹
- [۱۶] ۵G-PPP Software Network Working Group, Cloud Native and ۵G Verticals' services, February ۲۰۲۰



نشانی: تهران، انتهای کارگر شمالی، پژوهشگاه
ارتباطات و فناوری اطلاعات، معاونت پژوهش و
توسعه ارتباطات علمی

تلفن: ۰۲۱-۸۸۶۳۰۳۵۵

نمابر: ۰۲۱-۸۸۶۳۰۳۵۶