ارائه یک مدل معماری بومی رایانش ابری در بخش دفاعی

محمدرضا ولوی[1]

محمدرضا موحدی صفت[2]

تاریخ دریافت: ۱۳۹۴/۱۰/۰۵ تاریخ پذیرش: ۱۳۹۴/۱۲/۲۵

چکیده

فناوری رایانش ابری بر اساس استفاده بهینه از سرویس‌های موجود در شبکه‌های رایانه‌ای به عنوان یک رویکرد نوین در حوزه فناوری اطلاعات در حال توسعه است. مزایای این فناوری باعث شده که بسیاری از کشورهای دنیا، سرویس‌ها، پلتفرم‌ها و زیرساخت‌های خود را در این ساختار پیاده‌سازی نمایند. وجود اسناد راهبردی در این حوزه نشان می‌دهد که استقرار امن رایانش ابری با توجه به تهدیدات نوظهور پیش رو به عنوان یک الزام در همه زیرساخت‌ها به ویژه حوزه نظامی مورد تأکید است. در این خصوص موسسه ملی استاندارد و فناوری آمریکا توانسته استاندارد رایانش ابری برای این کشور را تدوین نماید. این استاندارد مورد قبول وزارت دفاع، موسسه تحقیقات پیشرفته دفاعی، موسسه بین‌المللی ارتباطات و سایر سازمان‌های نظامی آمریکا است. بدیهی است سیاست‌های خاص دفاعی و امنیتی جمهوری اسلامی ایران، پذیرش معماری‌های موجود را تأیید نمی‌نماید و در نتیجه استانداردها و روال‌های مورد پذیرش جهانی به طور کامل و امن مورد استفاده قرار نمی‌گیرند و لازم است که اصول، سیاست‌ها و چارچوب‌های معماری امن برای استقرار رایانش ابری به صورت بومی طراحی شود. هدف از این مقاله ارائه یک مدل معماری بومی برای رایانش ابری دفاعی با توجه به مقتضیات خاص نیروهای مسلح است.

در این مقاله ضمن بررسی معماری‌های رایانش ابری، چارچوب معماری امن رایانش ابری حوزه دفاعی کشور پیشنهاد شده و بر اساس نظرات خبرگان مورد راستی آزمایی قرار گرفته است. نتیجه این تحقیق اضافه کردن لایه امنیت به عنوان سرویس در معماری رایانش ابری است به گونه ای که همه بخش‌های معماری و ارتباطات بین لایه‌ها را در برگیرد.

واژه‌های کلیدی: محیط امنیتی ، منافع ملی ،منافع امنیت ملی ، سیاست خارجی

---

[1] عضو هیات علمی دانشگاه صنعتی مالک اشتر

[2] نویسنده مسئول و عضو هیات علمی دانشگاه عالی دفاع ملی

مقدمه

در عصر حاضر وجود سامانه‌های مبتنی بر فناوری اطلاعات و ارتباطات باعث شده فضای سایبر در تمامی عرصه‌های زندگی انسان گسترش پیدا نماید. بسیاری از ارتباطات میان و درون سازمانی نیز در حال حاضر بر روی این بستر قرار دارند و اختلال در ارائه سرویس‌های موجود می‌تواند زمینه ساز نارضایتی کاربران گردد.

در این فضا، مجموعه‌ای متشکل از زیرساخت‌ها، شبکه‌ها، نرم‌افزارها، تجهیزات و سخت‌افزارها، پروتکل‌ها، محیط‌های نرم افزاری، سرویس‌ها و سیاست‌های حاکم بر حوزه سایبر وجود دارد. (قنبری، ۱۳۹۳: ۲) همچنین فضای سایبر با توجه به ویژگی منحصر به فرد خود، دربرگیرنده مجموعه‌ای از مفاهیم فرهنگی، سیاسی، حقوقی و معنوی است. این ویژگی‌ها باعث می‌شود تا توجه ویژه‌ای از سمت کاربران و استفاده‌کنندگان در خصوص کارکردهای آن به وجود آید.

امروزه رشد مجازی‌سازی و گسترش شبکه‌های کامپیوتری، حوزه جدیدی به نام رایانش ابری[1] را به دنیای فناوری اطلاعات و ارتباطات اضافه کرده که ایده اصلی آن پردازش و نگهداری اطلاعات سامانه‌های موجود بر روی یک فضای انتزاعی است (متیو، ۲۰۱۳، ۲۶). این ایده با استفاده از سرورهای درون شبکه در مناطق مختلف می‌تواند به خواسته‌های کاربران پاسخ داده و نیازهای ایشان را مرتفع سازد. باید توجه داشت که وجود یک سرویس دهنده در این فضا و ارائه سرویس‌های مورد نظر کاربران از خارج از سازمان، باعث ایجاد نگرانی در حوزه‌های امنیتی شده که توجه به آن یک امر حیاتی است.

حرکت به سمت استفاده از سرویس‌های ابری علی الخصوص در بخش دفاعی، دارای مزایای بسیاری است ولی چالش‌هایی را نیز به همراه دارد. با پیاده‌سازی سرویس‌های ابری در محیط دفاعی، دو قابلیت ایجاد اطمینان و شفافیت به عنوان دو مزیت مورد توجه قرار می‌گیرد. همچنین عدم وجود یک گلوگاه باعث می‌شود تا سرویس‌های لازم همواره در دسترس بوده و درصورت بروز هرگونه حمله حتی به صورت فیزیکی، با انتقال پردازش و داده‌ها به نقطه امن دیگر، قابلیت اطمینان سامانه تا حد زیادی افزایش یابد. همچنین عدم اطلاع کاربران از محل انباشت داده‌ها و پردازش اطلاعات از دیگر مزایای پیاده‌سازی سرورهای ابری است که ضریب محرمانگی سامانه را

1.Cloud Computing

افزایش می‌دهد (مککی، ۲۰۱۲: ٦٧٩). این ویژگی‌ها در صحنه‌های نبرد و در شرایط بحرانی باعث حفظ محرمانگی اطلاعات و در دسترس ماندن سرویس‌ها می‌شود.

یک مشکل مهم در این زمینه مطلوب نبودن امنیت سرویس‌های رایانش ابری است. راهکارهای سنتی امنیتی هم در این حوزه پاسخ گو نمی‌باشند. (یانچان، ۲۰۱٤: ۱) در این خصوص قوانین جدیدی در حوزه حملات و دفاع سایبری با استفاده از خدمات رایانش ابری در سطح جهان مورد تصویب دولت‌ها قرار گرفته است. اهمیت این مفهوم زمانی تشدید خواهد شد که بدانیم فناوری رایانش ابری باید در کنار نظام امنیتی سنتی فعلی به کار گرفته شود.

در این تحقیق، ابتدا تعاریف مرتبط با رایانش ابری، مزیت‌ها و چالش‌های استقرار آن بیان شده و سپس دو مدل مرجع مورد بررسی قرار می‌گیرند. پس از شناسایی نقاط ضعف و قوت این مدل‌ها، مؤلفه ها و گام‌های مورد نیاز برای ارائه چارچوب معماری رایانش ابری بومی در حوزه دفاع ارائه می‌شود.

بیان مسئله:

در پیاده سازی و استقرار کامل رایانش ابری بخش دفاعی، درنظر گرفتن مؤلفه امنیت حائز اهمیت است و لازم است که جنبه‌های مختلف امنیت به طور کامل مورد بررسی قرار گیرند. چالش‌های بسیاری در این حوزه وجود دارد که مهم‌ترین آن در دسترس نبود اطلاعات کافی از زیرساخت های استقرار این فناوری است. به عنوان مثال نداشتن اطلاعات در خصوص متن برنامه‌های منابع رایانشی در دنیا می‌تواند یک چالش و تهدید برای استقرار آن در بخش دفاعی محسوب گردد. لذا تجزیه و تحلیل، طراحی و استقرار معماری امن رایانش ابری بومی با در نظر گرفتن مقتضیات خاص جغرافیایی و فرهنگی در این تحقیق مورد بررسی قرار گرفته است.

در این تحقیق توجه به مؤلفه‌هایی نظیر تعیین ویژگی‌های همه بازیگران در محیط ابر حوزه دفاعی و نحوه تعامل آن‌ها با یکدیگر در محیط‌های توزیع پذیر[1]، مقیاس‌پذیر[2] و تحرک‌پذیری[3] و در نظر گرفتن اصل یکپارچگی در ایجاد پایگاه‌های داده دفاعی پرداخته شده است. همچنین به عواملی

[1] Distributed Environment
[2] Scalability
[3] Mobility

مانند یکپارچه‌سازی پورتال‌های سازمان‌های دفاعی و در نظرگرفتن مولفه‌های خاص بومی (مؤلفه فرهنگی، جغرافیایی) توجه کامل شده است.

مسئله اصلی عدم امنیت معماری‌های موجود رایانش ابری برای مهاجرت بخش دفاعی کشور به این حوزه است و لازم است که یک معماری بومی امن با توجه به شرایط خاص دفاعی کشور ایجاد شود و تاکنون این معماری بومی بخش دفاعی ارائه نشده است.

اهمیت و ضرورت تحقیق:

بر اساس گزارشات موسسه اکونومیست، در حال حاضر عرصه سایبری پنجمین عرصه نبرد پس از زمین، دریا، هوا و فضا است. (Economist، ۲۰۱۰:۲) واژه نبرد سایبری[1] محصول ورود عرصه سایبر به عرصه‌های نبرد است. در نبرد سایبری در واقع نوع نبرد به صورت محتوایی نیست بلکه رویکرد، از دسترس خارج کردن سرویس‌ها و از کار انداختن ارائه‌دهندگان خدمات زیرساخت‌هاست (Teotari، ۲۰۱۵: ۲). به عنوان نمونه امروزه شاهد هستیم که اقدام‌های بسیاری از سوی دشمن برای جلوگیری از ارائه سرویس سایت‌های جمهوری اسلامی ایران صورت می‌گیرد. این نبرد هم مانند سایر نبردها لوازم و ابزار ویژه خود را دارد؛ نیروی انسانی، سخت افزار، نرم‌افزار و جنگ‌افزارهای خاص منظوره، برای این نوع نبرد مورد نیاز است. به عنوان نمونه‌ای دیگر از تلاش‌های صورت گرفته در این حوزه می‌توان به تشکیل فرماندهی سایبری ارتش آمریکا[2] با مأموریت مشخص تحت عنوان حمله و دفاع در عرصه سایبری در سال ۲۰۱۱ اشاره کرد (Harington،۲۰۱۵:۵).

وجود مزیت‌های بسیاری که برای رایانش ابری متصور است از جمله چابکی، کاهش هزینه‌ها، عدم وابستگی به زمان و مکان، به اشتراک‌گذاری منابع بین گروهی از کاربران، افزایش کارایی، استفاده حداکثری از منابع موجود در شبکه، افزایش قابلیت اطمینان با استفاده از سایت‌های مطمئن، تدارک منابع در زمان تقاضا و به صورت پویا، افزایش امنیت و عدم نیاز به نصب برنامه‌های کاربردی برای هر کاربر باعث شده که هر روز بر محبوبیت رایانش ابری اضافه شود (بهشتی،

[1] Cyber Attack
[2] Headquarters Company, Army Cyber Command

۱۳۹۱: ۱). همچنین افزایش قابلیت‌ها در حوزه‌های دفاعی، استفاده از رایانش ابری را امری اجتناب ناپذیر تبدیل کرده است.

متقضیات خاص دفاعی کشور و لزوم بهره‌برداری حداکثری از رایانش ابری با در نظرگرفتن شاخص‌های امنیتی، ضرورت استفاده از معماری بومی رایانش ابری حوزه دفاعی را مشخص می‌سازد. در مدل‌های استاندارد موجود در دنیا کمتر به حوزه کنترل، رصد و پایش پرداخته شده و بیشتر به استفاده از فضای اشتراکی سرویس‌ها در محیط‌های تجاری تأکید شده است درحالی که در مدل مورد نظر این تحقیق، اهمیت امنیت سرویس‌ها، حفاظت از داده‌ها، کنترل دسترسی‌ها و در نظر گرفتن سیاست‌های دفاعی به عنوان مهم‌ترین شاخص‌های الگوی بومی مورد نظر واقع شده است.

روش شناسی تحقیق و ابزارهای جمع آوری داده‌ها

روش پژوهش از نوع توصیفی و تحلیل محتوا است. هدف تحقیق کاربردی، آزمون در موقعیت‌های واقعی و حل مشکلات ملموس است و نتایج آن قابلیت به کارگیری در سازمان‌های دفاعی را دارد.

به‌منظور جمع‌آوری داده‌ها در این پژوهش، از دو روش کتابخانه‌ای و میدانی استفاده شده است. بدین ترتیب که به منظور جمع‌آوری پیشینه و مبانی نظری پژوهش از روش کتابخانه‌ای با مراجعه به کتاب‌ها، پایان‌نامه‌ها، نشریات و کتابخانه‌های دانشگاه‌ها و مراکز اطلاع رسانی و جستجو در پایگاه‌های اطلاع رسانی علمی و موتورهای جستجوگر جهت دستیابی به آخرین دستاوردهای مطالعات و پژوهش‌های انجام شده و تکمیل ادبیات تحقیق و بررسی مباحث نظری مرتبط با موضوع استفاده شده و در نهایت طراحی معماری نهایی رایانش ابری پیشنهادی با مطالعات میدانی و مصاحبه با افراد خبره انجام شده است.

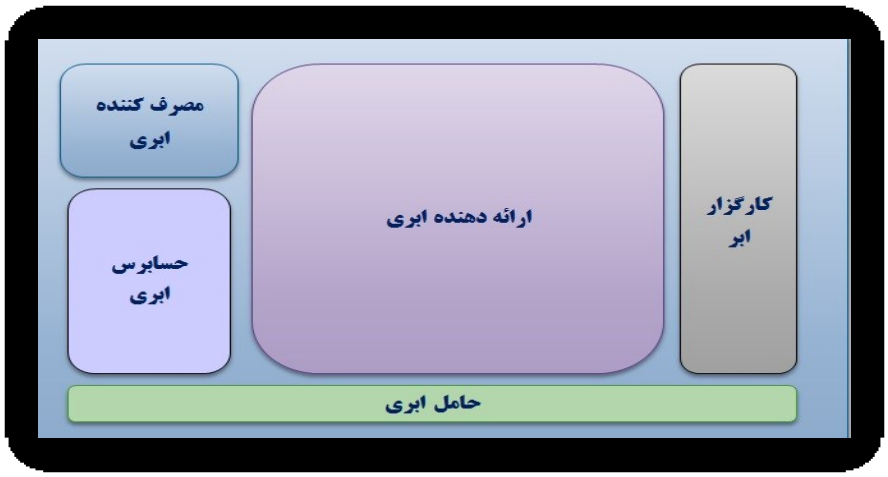
جامعه نمونه این پژوهش محققان، کارشناسان، خبرگان حوزه‌ی امور نظامی و دفاعی، سیاست دفاعی، علوم و فناوری‌های دفاعی هستند که سابقه و تجربه‌ی مدیریت و فرماندهی در سطوح بالای نیروهای مسلح را دارند و به صورت هدفمند انتخاب شده‌اند. تحقیق حاضر به دنبال پاسخ به این پرسش است که معماری بومی رایانش ابری در حوزه دفاعی کشور با در نظرگفتن شاخص‌های امنیتی، دارای چه مؤلفه‌هایی است و ارتباط این مولفه‌ها با یکدیگر چگونه است؟

مبانی نظری تحقیق:

پیشینه تحقیق:

در خصوص معماری‌های رایانش ابری مطالعات و پژوهش‌هایی صورت گرفته که اهم آن عبارت‌اند از:

۱- مدل مرجع موسسه ملی استاندارد و فناوری[1] به بیان پنج ویژگی اصلی خدمات خود تقاضا، دسترسی به شبکه گسترده، توزیع منابع، انعطاف سریع، کنترل منابع و بهینه‌سازی برای رایانش ابری پرداخته است. در مدل مرجع موسسه ملی استاندارد و فناوری، پنج بازیگر مصرف کننده ابر[2]، ارائه دهنده ابر[3]، رصد و پایش ابر[4]، کارگزارابر[5] و حامل ابر[6] قرار دارند. (شکل ۳) (بادجر، ۲۰۱۱، ۲۰).

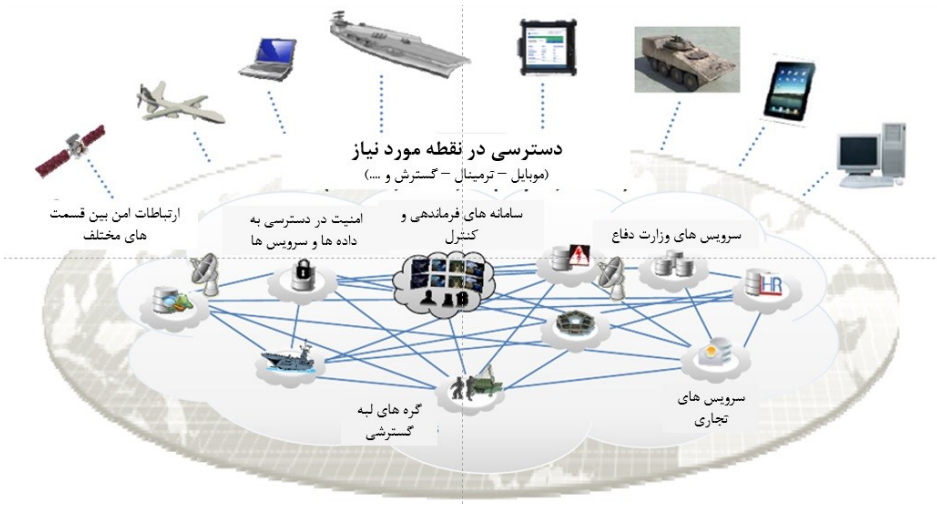


شکل ۳ – بازیگران اصلی در مدل مرجع NIST

۲- مرکز فناوری اطلاعات وزارت دفاع[7] به منظور شناسایی فرصت‌ها و مزیت‌هایی که در قبال استفاده از رایانش ابری در وزارت دفاع آمریکا فراهم می‌شود تصمیم دارد تا وزارت دفاع را از یک

[1] NIST (National Institute of Standard and Technology)
[2] Customer
[3] Provider
[4] Auditor
[5] Broker
[6] Carrier
[7] CIO (Chief Information Officer)

حالت تکراری، پر زحمت، طاقت فرسا و پر هزینه به یک مجموعه چالاک، امن و کم هزینه تبدیل کند. در این خصوص ایجاد یک ابر خصوصی برای وزارت دفاع آمریکا با قابلیت‌های گفته شده به عنوان یک پروژه تعریف شده در حال اجرا است. هدف اصلی از رایانش ابری در وزارت دفاع آمریکا پشتیبانی از ماموریت سازمانی در هر جا و در هر زمان و بر روی هر وسیله دارای هویت در وزارت دفاع است. (شکل ٤) نقشه جامعی از استقرار رایانش ابری در وزارت دفاع آمریکا را نمایش می‌دهد. منظور از سرویس‌های تجاری در این شکل، نحوه تعامل با سایر سازمان و امور برون‌سپاری فناوری دفاعی وزارت دفاع است. (تاکایی، ۲۰۱۲، ۱۰).



شکل ٤ – نقشه استقرار رایانش ابری در DoD

۳– ارائه معماری مرجع امنیتی محیط رایانش ابر خصوصی سازمان، در یک مقاله علمی – پژوهشی توسط مهدی نقیان فشارکی مورد بررسی قرار گرفته و در آن به گام‌های شناخت سازمان و مهندسی نیازمندی‌ها، ترسیم معماری سطح بالای محیط ابری سازمان، نگاشت مولفه‌های امنیتی با بازیگران ابری، تدوین الگوی رسمی معماری مرجع امنیتی و ارزیابی معماری پرداخته شده است (نقیان فشارکی، ۱۳۹۳: ۱).

٤– شرکت IBM در معماری رایانش ابری سازمانی خود، امنیت محیطی را به عنوان یکی از شاخص‌های اصلی در نظر گرفته و بر این اساس معماری مجزایی برای محیط رایانش ابری ارائه کرده است (Viliam،۲۰۱۱:۲).

۵- ناسا سالیانه ۱.۵ میلیارد دلار در بخش فناوری اطلاعات خود هزینه می‌کند تا بتواند زیرساخت امن و بهینه برای ذخیره‌سازی و پردازش داده‌های علمی در محیط رایانش ابری فراهم کند. پروژه اپن استاک[1] به عنوان بزرگ‌ترین محصول رایانش ابری این شرکت است (مارتین، ۲۰۱۳، ۳).

متغیرهای تحقیق:

در این تحقیق، رایانش ابری به عنوان متغیر مستقل و معماری بومی مدنظر محقق به عنوان متغیر وابسته است.

تعریف رایانش ابری

رایانش ابری یک الگو برای دسترسی فراگیر، راحت و به محض درخواست به منابع رایانشی به اشتراک گذاشته است که می‌تواند به سرعت و با کمترین تلاش مدیریتی یا تعامل با ارائه دهنده سرویس، تأمین شده و در دسترس قرار گیرد (Mell،۲۰۱۱:۲).

رایانش ابری مبتنی بر یک معماری توزیع شده است که از طریق پروتکل‌های رایج اینترنت و استانداردهای شبکه قابل دسترسی است. این فناوری جدید، نیازهای کاربران برای دریافت منابعی همچون منابع محاسباتی، شبکه‌ها، محیط‌های ذخیره‌سازی، سرورها، سرویس‌ها و کاربردها را بدون دستیابی فیزیکی کاربران و بدون صرف هزینه گزاف و تنها با پرداخت هزینه بر اساس میزان استفاده فراهم می‌سازد (سارین۵۳۳: ۲۰۱۳،Sarin).

خدمات رایانش ابری:

خدمات رایانش ابری به سه شکل مختلف ارائه می‌گردد. سازمان‌ها و شرکت‌ها با توجه به نیازشان می‌توانند یک یا چند خدمات از خدمات رایانش ابری را انتخاب و استفاده نمایند (صدرالساداتی، ۱۳۹۲: ۳و٤).

۱. نرم‌افزار به عنوان سرویس[2]
۲. پلتفرم به عنوان سرویس[3]
۳. زیرساخت به عنوان سرویس[1]

---

[1] Open Stack
2 SaaS(Software as a Service)
3 PaaS(Platform as a Service)

نرم‌افزار به عنوان سرویس: یعنی نرم‌افزارها و سامانه‌های مورد نیاز کاربران بر روی اینترنت تحویل شده و نیاز به نصب نرم افزار بر روی رایانه‌های مشتریان از بین رود. خدمات ارائه شده در این حوزه می‌تواند شامل نرم‌افزارهای کاربردی از قبیل مدیریت ارتباط مشتری[۲] و برنامه‌ریزی منابع سازمانی[۳] باشد.

پلتفرم به عنوان سرویس: این سرویس یک لایه نرم‌افزاری را به عنوان بسته ارائه می‌دهد که می‌توان از آن برای تولید سرویس‌های سطح بالاتر استفاده نمود. یک مثال خوب موتور تولید برنامه نرم‌افزاری گوگل است که امکان اجرای برنامه‌های کاربردی توسط پلتفرم گوگل را فراهم می‌آورد.

زیرساخت به عنوان سرویس: زیرساخت رایانه‌ای که یک بستر مجازی است را به صورت سرویس ارائه می‌دهد. کاربران به جای خرید سخت‌افزار و نرم‌افزار و فضای مرکز داده و یا تجهیزات شبکه، همه این زیرساخت‌ها را به صورت یک سرویس کاملاً برون‌سپاری شده سفارش می‌دهند. صورتحساب سرویس معمولاً بر اساس مدل محاسبات همگانی و میزان منابع مصرف شده صادر می‌شود. در حال حاضر سایت آمازون بسیاری از این سرویس‌ها را ارائه می‌دهد.

شبکه به عنوان سرویس: یک زیرساخت شبکه مجازی شده را برای ارائه سرویس‌های شبکه به مشتری ایجاد می‌نماید.

ویژگی‌های مهم رایانش ابری:

در رایانش ابری سرویس‌ها مبتنی بر تقاضا هستند و مشتری می‌تواند به صورت یک طرفه امکانات و خدمات محاسباتی همچون سرور و فضای ذخیره‌سازی در شبکه را به هنگام نیاز از هر فراهم کننده‌ای به صورت خودکار و بدون نیاز به دخالت انسان به دست آورد. دسترسی‌ها به شبکه سریع است و استخری از منابع به صورت فیزیکی یا مجازی و به شکلی پویا و بنابر درخواست مشتری در دسترس است. در رایانش ابری می‌توان امکانات را به سرعت، با قابلیت انعطاف بالا و یا به صورت خودکار به دست و میزان استفاده از منابع می‌تواند به شکلی شفاف هم برای مشتری و هم برای فراهم کننده سرویس، کنترل شده و گزارش داده شود (Brunet,۲۰۱۵).

1 IaaS(Infrastructure as a Service)
2 CRM
3 ERP

مدل‌های پیاده‌سازی رایانش ابری:

ابرهای خصوصی[1]، ابرهای عمومی[2] و ابرهای ترکیبی[3] روش‌های مختلف پیاده‌سازی رایانش ابری در یک سازمان هستند. (شکل ۱) (صادق زاده، ۱۳۹۲: ۲و۳).

شکل ۱ – انواع پیاده سازی های ابرها

ابر خصوصی یک زیرساخت محاسبات ابری است که توسط یک سازمان برای استفاده داخلی آن سازمان به وجود آمده و امکان کنترل بیشتر بر روی تمام سطوح پیاده‌سازی ابر مانند سخت‌افزار، شبکه، سیستم‌عامل و نرم افزار را فراهم می‌سازد. مزیت ابرهای خصوصی امنیت بیشتری است که ناشی از قرارگیری تجهیزات در درون مرزهای سازمان و عدم ارتباط با دنیای خارج است. ابرعمومی توصیف کننده محاسبات ابری در معنای اصلی و سنتی آن است. سرویس‌ها به صورت پویا و از طریق اینترنت و در واحدهای کوچک از یک عرضه کننده شخص ثالث تدارک داده می‌شوند و عرضه‌کننده منابع را به صورت اشتراکی به کاربران اجاره می‌دهند و براساس مدل محاسبات همگانی و مشابه صنعت برق و تلفن برای کاربران صورتحساب می‌فرستد. یک ابر ترکیبی متشکل از چندین ارائه دهنده داخلی و یا خارجی است و گزینه مناسبی برای بیشتر مؤسسات تجاری است.

مزایای و معایب رایانش ابری:

از مزایای رایانش ابری می‌توان به چابک شدن سازمان، کاهش هزینه‌ها و تبدیل هزینه‌های سرمایه‌ای به هزینه‌های عملیاتی، کاهش هزینه توسعه نرم‌افزاری، عدم وابستگی کاربران به

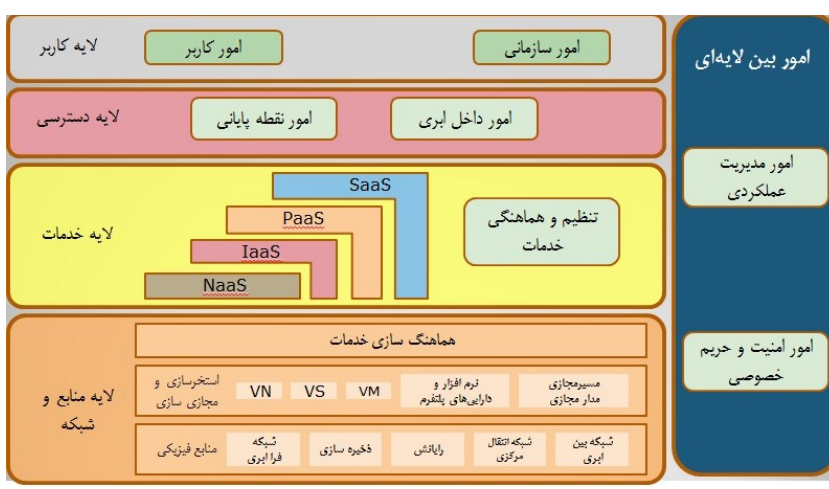
[1] Private Clouds.
[2] Public Clouds.
[3] Hybrid Clouds.

زیرساخت‌های پیچیده، امکان به اشتراک‌گذاری منابع و هزینه‌ها بین گروهی از کاربران، متمرکز سازی زیرساخت‌ها با هزینه کمتر، افزایش کارایی سامانه‌ها، استفاده بر اساس تقاضا از منابع و افزایش امنیت به دلیل تمرکز داده‌ها و افزایش دسترسی‌ها اشاره کرد. همچنین به دلیل عدم نیاز به نصب برنامه‌های کاربردی برای هر کاربر نگهداری‌ها آسان‌تر و با هزینه کمتر انجام می‌شوند. (Pritzker,۲۹۷: ۲۰۱٤).

از چالش‌های پیش روی رایانش ابری می‌توان به مقاومت مدیران در پذیرش آن، امکان ورود به حریم‌های خصوصی کاربران، نیاز به توسعه پروتکل‌های امنیتی در ابرهای عمومی، وجود ساختارهای امنیتی آسیب پذیر در دسترسی به ابر، نیاز به نیروی انسانی خبره و نبود معماری امن حوزه دفاعی اشاره کرد. همچنین مخاطراتی نظیر از دست رفتن حاکمیت، مسائل مربوط به تصدیق اصالت، نحوه و میزان دسترسی‌ها، مشکلات موجود در ارتباط از راه دور، تأثیر مشتریان بر هم در استفاده از منابع اشتراکی و حفظ محرمانگی در این حوزه وجود دارد (توراب، ۲۰۱۳، ۲۱۲).

لایه‌های اصلی معماری رایانش ابری:

معماری رایانش ابری شامل چهار لایه اصلی کاربر، دسترسی، خدمات و منابع است(شکل ۲) خدمات امنیت و حریم خصوصی و همچنین مدیریت و امور عملکرد نیز به عنوان امور بین لایه‌ای است .(Badger،۱۹ :۲۰۱۱)



شکل ۲ – چهار لایه اصلی موجود در معماری رایانش ابری

لایه کاربر در بالاترین سطح وجود دارد و شامل برنامه‌های کاربردی ابر است. لایه دسترسی شامل امور داخل ابر و ارتباطات نقطه پایانی (ارتباط از خارج ابر به داخل) است. لایه منابع و شبکه، زیر ساخت فیزیکی را تشکیل می‌دهد که بر روی آن لایه مدیریت عمل می‌نماید. در این لایه شبکه‌های مجازی[1]، سرویس‌های مجازی[2] و ماشین‌های مجازی[3] قرار می‌گیرند. لایه خدمات، دربرگیرنده سرویس‌هایی است که در رایانش ابری ارائه می‌شوند که مه‌ترین آن‌ها نرم افزارها، پلتفرم‌ها و زیرساخت‌ها است.

تجزیه و تحلیل مدل استاندارد مرجع رایانش ابری

موسسه ملی استاندارد و فناوری، استانداردی را در جهت استقرار رایانش ابری با هدف پیشبرد علوم سنجشی و فناوری تدوین نموده که امروزه به عنوان مرجع معماری رایانش ابری برای اکثر دولت‌ها و سازمان‌ها در نظر گرفته می‌شود. ویژگی‌های اصلی رایانش ابری عبارت‌اند از: (Hogon،۱۱: ۲۰۱۱)

۱) خدمات خود تقاضا: مصرف‌کننده می‌تواند پارامترهای محاسباتی مانند زمان سرور یا ذخیره‌سازی شبکه را به صورت خودکار تغییر دهد.

۲) دسترسی به شبکه گسترده: امکانات بسیاری بر روی تجهیزات (تلفن همراه، فبلت[4]، تبلت، لپ تاپ و ایستگاه‌های کاری) قابل دسترسی است.

۳) توزیع منابع: منابع رایانشی(حافظه، پهنای باند و ...) می‌توانند به تعدادی از مصرف‌کنندگان به صورت پویا و بر اساس نیاز ارائه شود.

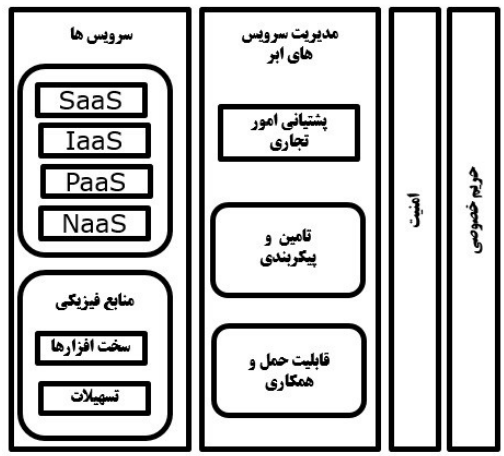
٤) انعطاف سریع: بسیاری از منابع می‌توانند با انعطاف بالا و متناسب با تقاضا داده و یا گرفته شوند.

۵) کنترل منابع و بهینه سازی: متناسب با نوع خدمت(ذخیره‌سازی، پردازش، پهنای باند و حساب‌های کاربران) منابع کنترل و بهینه می‌شوند.

---

[1] VN (Virtual Network)
[2] VS (Virtual Service)
[3] VM(Virtual Machines)
[4] phablet

لایه ارائه دهنده در معماری رایانش ابری در موسسه ملی استاندارد و فناوری از چهار زیر لایه اصلی شامل سرویس و منابع فیزیکی، مدیریت سرویس‌های ابری، امنیت و محرمانگی تشکیل شده است (شکل ۵).



شکل ۵- اجزاء تشکیل لایه ارائه دهنده

لایه رصد و پایش در معماری رایانش ابری مرجع، کلیه امور مربوط به ارزیابی از خدمات ابر، عملیات، عملکرد و نحوه استقرار امنیت را مورد حسابرسی و رصد قرار می‌دهد. این لایه دارای سه سطح کنترل امنیتی به صورت مدیریتی، عملیاتی و تکنیکی است و به کنترل محرمانگی، یکپارچگی و در دسترس بودن به عنوان عوامل مهم رصد امنیت توجه دارد. همچنین کنترل قوانین مصوب موجود در زمینه حریم خصوصی بر عهده این لایه است (شکل ٦ الف).

شکل ٦ الف – لایه رصد و پایش

شکل ٦ ب – لایه کارگزار

لایه کارگزار در معماری مرجع رایانش ابری، مدیریت عملکرد و ارتباط بین مشتریان و مصرف کنندگان را بر عهده دارد و مهم‌ترین وظایف آن بهبود مدیریت دسترسی به خدمات ابر و بهبود کارایی، ترکیب و ادغام خدمات مختلف را به یک یا چند سرویس جدید، یکپارچه‌سازی داده‌ها و اطمینان از حرکت داده‌های امن بین مصرف کنندگان ابر و ارائه‌دهندگان ابر، انعطاف‌پذیری در انتخاب خدمات از سازمان‌های متعدد و انتخاب بهترین سرویس مورد نیاز است (شکل ٦ ب).

تجزیه و تحلیل مدل رایانش ابری وزارت دفاع آمریکا (DoD)

وزارت دفاع آمریکا نیز با اهداف کاهش هزینه‌ها، افزایش توان عملیاتی، افزایش توان ماموریت سازمانی و امنیت در فضای سایبر، چهار گام همزمان را برای پیاده‌سازی محیط ابری تعیین و بر مبنای آن عمل می‌کند. این چهار گام عبارت‌اند از: (Takai،٦: ۲۰۱۲)

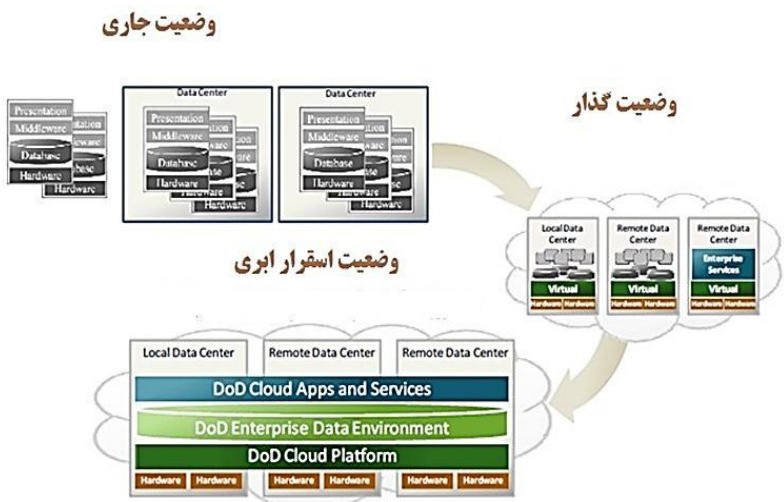
۱) پذیرش قطعی رایانش ابری شامل ایجاد یک ساختار به هم پیوسته برای گذار از روش سنتی به استفاده از محیط ابری و قبول تعهدهای مبتنی بر قرار گرفتن در این فضا است و ایجاد فرهنگ سازمانی قرارگرفتن در محیط ابری، تجدید نظر در برخی رویکردها و سیاست‌هایی که در محیط ابری وجود دارد و همچنین رسیدن به چالاکی و کم شدن هزینه‌ها و ایجاد یک رایانش ابری به صورت خصوصی با در نظر گرفتن محیط‌های تعاملی که در ابر زیرساخت دولتی وجود دارد، از اهم اهداف است.

۲) بهینه کردن یکپارچگی مراکز داده شامل یکپارچه کردن داده‌ها و برنامه‌های کاربردی موجود و سنتی و حرکت به سمت مجازی سازی به عنوان یک گام مهم تلقی می‌شود.

۳) ایجاد زیرساخت ابری موسسه وزارت دفاع شامل تأسیس هسته مرکزی زیرساخت در مرکز داده یکپارچه وزارت دفاع و بهینه کردن سرویس‌هایی است که از تعدادی از ارائه کنندگان سرویس‌ها و از طریق کارگزاری‌های مرتبط برای وزارت دفاع فراهم می‌شود. همچنین طراحی و ایجاد یک مدل برای ارائه سرویس‌ها با در نظر گرفتن اصل چالاکی و طراحی مدل به اشتراک گذاری ایمن داده‌ها در محیط ابر با در نظر گرفتن نوآوری‌های مربوطه از اهداف اصلی است.

٤) تحویل سرویس‌های ابری شامل سرویس‌های قبلی است بدون آنکه اختلالی در آن‌ها به وجود آید و قدرت سرویس‌ها نیز باید افزایش یابد. این افزایش بر اساس قابلیت‌هایی است که فضای رایانش ابری فراهم می‌آورد.

در نقشه گذار از وضع فعلی به استقرار رایانش ابری که در شکل ۷ آورده شده است سرویس‌های قبلی تداوم اجرا دارند (همان: ۲۰۱۲، ۲۶).



شکل ۷ – نحوه استقرار رایانش ابری در DoD

ارائه مدل پیشنهادی

با توجه به موارد بیان شده لزوم حرکت به سمت استقرار رایانش ابری برای حوزه دفاعی کشور مشخص گردید در حال حاضر یک الگوی معماری در رایانش ابری در حوزه دفاعی وجود ندارد و متولی ایجاد حوزه رایانش ابری در حوزه دفاعی نیز مشخص نیست. دلایلی که باید به سمت بومی‌سازی در این حوزه حرکت کرد به شرح ذیل است:

۱. بسیاری از زیرساخت‌های رایانش ابری در دسترس نمی‌باشند. به همین دلیل استفاده از زیرساخت‌های موجود در دنیا دارای ریسک بالایی بوده و می‌تواند مخاطرات جدی را در حوزه دفاعی به وجود آورد.

۲. در معماری ابری حوزه دفاعی کشور رایانش گرید[1] پذیرفته می‌شود. به این دلیل که با توجه به مقتضیات خاص دفاعی کشور تقریباً هیچ یک از سرویس‌های موجود در رایانش ابری را نمی‌توان

[1] Grid Computing

به صورت کاملاً باز تعریف نمود و محل داده‌ها، نوع سرویس‌ها و نحوه ارتباطات باید کاملاً مشخص باشد.

۱- معماری امن بومی بر اساس یک ابر چند لایه صورت می‌گیرد که هر ابر مقتضیات خاص دفاعی کشور را شامل می‌شود. و در نهایت ابر بومی حوزه دفاعی باید تحت کنترل است.

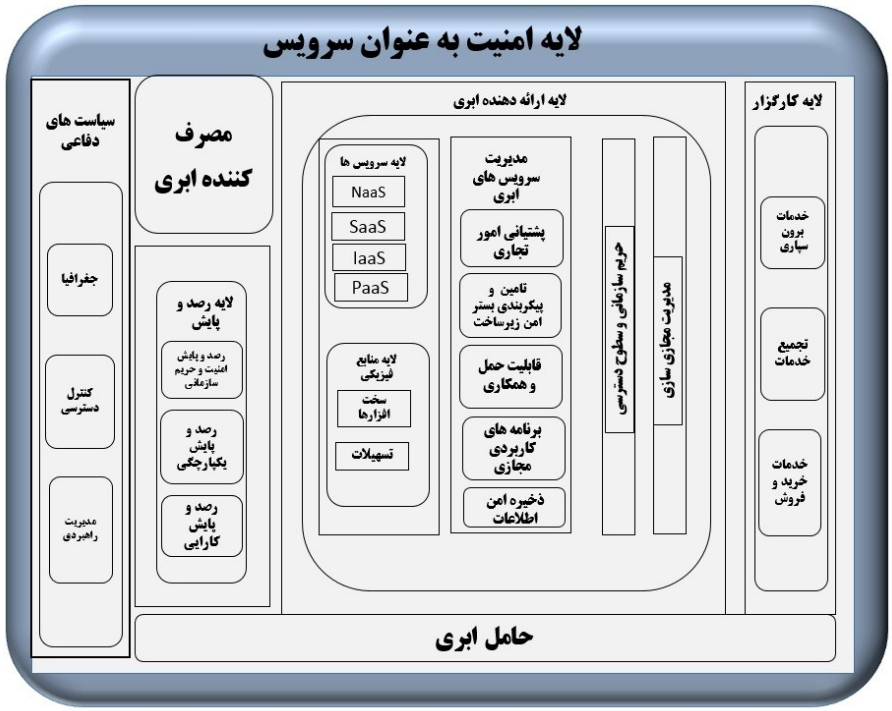
مولفه‌های مدل پیشنهادی:

نظر به اهمیت مولفه‌های امنیتی حوزه دفاعی، لایه امنیت به عنوان سرویس به عنوان لایه زیرساخت در کل معماری بومی رایانش ابری طراحی گردیده است. به گونه‌ای که کلیه لایه‌های موجود در رایانش ابری و ارتباطات بین آن‌ها بر روی لایه امنیت قرار می‌گیرد. بر اساس نظرسنجی که از خبرگان حوزه رایانش ابری و فناوری اطلاعات انجام پذیرفته، همگی بر حضور امنیت در همه ابعاد مدل پیشنهادی تأکید داشته و آن را جزء لاینفک رایانش ابری حوزه دفاعی دانسته‌اند.

مولفه‌های مدل پیشنهادی در دو بخش سیاست‌های دفاعی و رصد و پایش فعالانه دفاعی قرار می‌گیرند. که هر بخش بر اساس نیازهای دفاعی کشور طراحی و با توجه به وضعیت فعلی کشور بومی‌سازی و طراحی شده است.

مؤلفه سیاست‌های دفاعی

سیاست‌های خاص دفاعی کشور باعث ایجاد تغییراتی در لایه‌های موجود در معماری‌های رایانش ابری خواهد شد. یکی از این سیاست‌ها، ایجاد مدیریت لایه ای و سلسله مراتبی بر روی ابر است. همچنین باید کنترل دسترسی‌ها به صورت ساختارمند و در قالب مدیریت سلسله مراتبی تعریف شود. اگرچه مؤلفه های سیاست دفاعی تأثیرگذار در این معماری زیاد می‌باشند اما سه عامل جغرافیا، کنترل دسترسی و مدیریت و نظارت قانونی چندجانبه از اهمیت بالاتری برخوردار هستند. همان‌گونه که در شکل ۱۲ نشان داده شده است، در مدل معماری بومی ارائه شده سیاست‌های دفاعی کشور به عنوان یک لایه جدید در نظرگرفته شده است.



شکل ۱۲ – اضافه کردن لایه سیاست‌های دفاعی به معماری

در طراحی این لایه به موارد زیر پرداخته شده است:

۱. جغرافیا به عنوان یک عامل مهم: در نظر گرفتن محل جغرافیایی افراد و سامانه‌هایی که به رایانش ابری دسترسی دارند، از اهمیت ویژه‌ای برخوردار است. با در نظر گرفتن این عامل کنترل زیادی بر روی محل تراکنش‌های رایانش ابری به وجود می‌آید و در عمل شناسایی تهدیدات به نحو مناسب تری انجام می‌شود.

۲. کنترل دسترسی‌ها: به دلیل افزایش ضریب محرمانگی در دسترسی به اطلاعات و سامانه‌های موجود، کنترل دسترسی‌ها در مدل پیشنهادی به صورت متمرکز انجام می‌گیرد.

۳. مدیریت قانونی چندجانبه بر روی ابر: به منظور افزایش ضریب امنیت در کل محیط رایانش ابری حوزه دفاعی، سیاست‌گذاری‌ها به صورت یکپارچه است. همچنین به منظور افزایش بهره‌وری، مراکز مستقل دفاعی در کل محیط رایانش ابری به وجود خواهند آمد که مدیریت و نظارت آن‌ها از نوع قانونی و به صورت چندجانبه است.

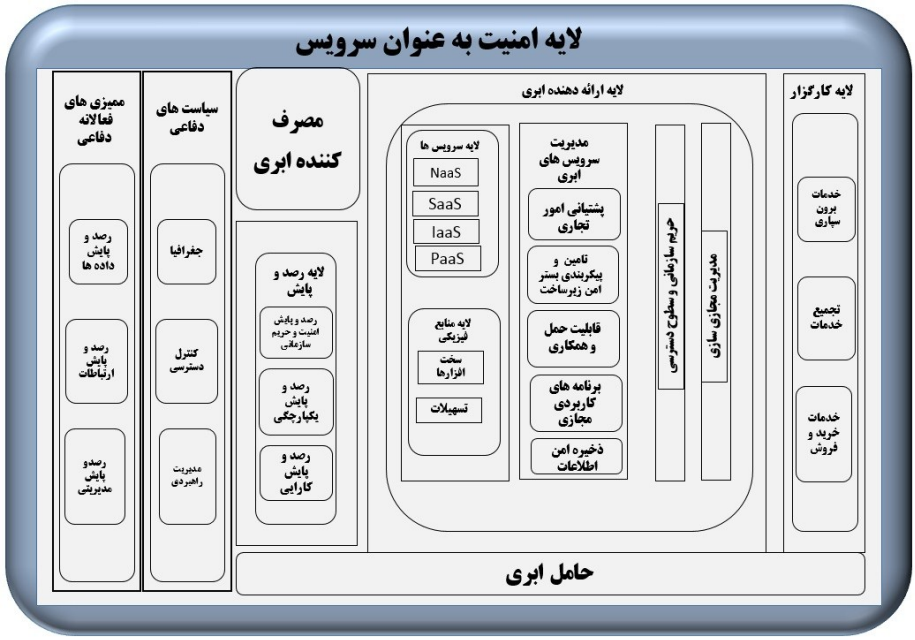
در طراحی این لایه به سه اصل زیر توجه شده است:

۱. اصل یکپارچگی در پایگاه‌های داده دفاعی: اگرچه در مدل رایانش ابری حوزه دفاعی با تعدد و انواع پایگاه‌ها و بانک‌های اطلاعاتی و دانشی مواجه هستیم، اما اصل یکپارچگی به منظور افزایش بهره‌وری و ایجاد مدیریت بر روی بانک از اهمیت ویژه‌ای برخوردار است.
۲. توجه به اصل افزونگی داده‌ها و ارائه راه‌حل بهینه: محیط‌های رایانش ابری با بانک‌های داده بزرگ[1] و حجم بسیار زیاد اطلاعات تولید شده مواجه هستند. بدیهی است در این نوع بانک‌های اطلاعاتی عدم توجه به اصل افزونگی می‌تواند آسیب‌های جدی به کل مجموعه وارد نماید.
۳. توجه به اصل جنگ‌های نامتقارن: با توجه به آنکه راهبرد اصلی حوزه دفاعی کشور، استفاده از جنگ‌های نامتقارن است، باید این مهم به عنوان یکی از سیاست‌های در نظر گرفته شده در طراحی رایانش ابری بومی مد نظر قرار گیرد.

رصد و پایش فعالانه دفاعی

علاوه بر لایه رصد و بازرسی که جزء پنج لایه اصلی در هر رایانش ابری است، لایه رصد و پایش فعالانه دفاعی به گونه ای طراحی شده که ضمن جلوگیری از افزونگی، استفاده از مسیرهای جانشین همواره مد نظر قرار گرفته و همچنین گردش داده‌ها نیز به صورت دائمی مورد ارزیابی قرار می‌گیرد. رصد در این لایه در سه بخش داده‌ها، ارتباطات و رصد و پایش‌های مدیریتی انجام می‌گیرد. (شکل ۱۳)

[1] Big DataBase



شکل ۱۳ – اضافه کردن لایه رصد و پایش دفاعی به معماری

در طراحی این لایه باید توجه داشت که سرویس‌های مورد استفاده در رایانش ابری حوزه دفاعی از اهمیت بالایی برخوردار هستند و گردش داده‌ها در این سرویس‌ها باید در یک محیط امن و تحت کنترل به صورت دائم مورد رصد و پایش قرار گیرد. ضمن آنکه پایگاه‌های داده نیز باید با سیاست‌های خاص بومی و امن طراحی و بکار گرفته شوند. همچنین ارتباطات بین بخش‌های مختلف و لایه‌های مختلف رایانش ابری حوزه دفاعی از اهمیت ویژه ای برخوردار است و در صورت وجود نقص در این بخش آسیب پذیری و تهدیدات افزایش خواهد یافت. لذا رصد در حوزه ارتباطات از اهمیت ویژه‌ای برخوردار است.

بررسی مدل پیشنهادی: برای بررسی مدل پیشنهادی، پرسشنامه ای با ۲۸ سؤال بین خبرگان حوزه‌های فناوری اطلاعات توزیع گردید و از ایشان خواسته شد تا نظر خود را در خصوص دو مؤلفه پیشنهادی سیاست‌های دفاعی و رصد و پایش فعالانه دفاعی در استقرار رایانش ابری در حوزه دفاعی بیان کنند.

نتایج این بررسی نشان داد که ۹۲/۸٪ پاسخ دهندگان وجود لایه سیاست دفاعی و ۹۶/٤٪ وجود لایه رصد و پایش فعالانه دفاعی را برای استقرار رایانش ابری در حد زیاد و خیلی زیاد تشخیص داده‌اند.

نتیجه گیری:

زیرساخت‌های خاص دفاعی جمهوری اسلامی ایران باعث شده که نتوان از معماری‌های رایانش ابری موجود در دنیا علیرغم استاندارد بودن، به دلیل ریسک موجود در عدم تأمین امنیت لازم در آن‌ها استفاده کرد و لذا لازم است که یک چارچوب معماری امن بومی برای استقرار رایانش ابری طراحی شود. در طراحی این مدل توجه به دو اصل سیاست‌های دفاعی (با مؤلفه هایی نظیر توجه به جغرافیا، اصل یکپارچگی، توجه به اصل جنگ‌های نامتقارن، توجه به کنترل دسترسی‌ها و اصل افزونگی) و رصد و پایش فعالانه دفاعی (با مؤلفه‌هایی نظیر توجه به داده‌ها، در نظر گرفتن شیوه ارتباطات و رصد و پایش‌های مدیریتی) حائز اهمیت است.

در این مقاله ضمن بررسی معماری‌های موجود در دنیا (علی‌الخصوص معماری‌های رایانش ابری حوزه دفاعی) و بر اساس استفاده از نظرات خبرگان این حوزه، چارچوب معماری امن رایانش ابری طراحی و بر اساس استفاده از تجربیات نخبگان این حوزه‌ها مورد بررسی قرار گرفت.

در پاسخ به سؤال تحقیق که معماری بومی رایانش ابری در حوزه دفاعی کشور با در نظرگفتن شاخص‌های امنیتی، دارای چه مؤلفه‌هایی باید باشد، وجود لایه زیرساخت به عنوان سرویس به عنوان مهم‌ترین لایه در کل معماری اضافه و مورد تأکید قرار گرفت. همچنین ایجاد مولفه‌های سیاست دفاعی و ممیزی‌های فعالانه دفاعی در مدل پیشنهادی گنجانده شد.

نظر اکثریت قریب به اتفاق خبرگانی که در این پژوهش شرکت کرده‌اند این است که باید در ارائه یک مدل معماری بومی رایانش ابری در بخش دفاعی به اصول زیر توجه داشت:

۱- لایه‌های استاندارد موجود در رایانش ابری در دنیا به عنوان اصل طراحی بومی در نظر گرفته شود و لایه‌های پیشنهادی در این تحقیق به جهت بومی سازی رایانش ابری حوزه دفاعی در کشور به آن‌ها اضافه گردد.

۲- در طراحی معماری رایانش ابری بومی حوزه دفاعی توجه به این اصل مهم است که بخش‌های زیرساختی رایانش ابری باید به روش گرید و شبکه محور مورد استفاده قرار گیرند تا کنترل بر روی ساختار توسط مدیریت قانونی چندجانبه به وجود آید.

۳- ارتباطات بین لایه‌های مختلف موجود در معماری رایانش ابری کاملاً تحت کنترل و قابل رصد و پایش باشند. یعنی فضای کلی حاکم بر رایانش ابری حوزه دفاعی کاملاً تحت کنترل و ارزیابی سلسله مراتب مدیریتی قرار گیرد.

٤- امنیت به عنوان یک سرویس در معماری رایانش ابری مورد توجه قرار گیرد. به گونه ای که همه بخش‌های معماری و همه ارتباطات بین بخش‌ها و لایه‌ها تحت کنترل این سرویس امنیتی قرار گیرد.

۵- استقرار رایانش ابری امن حوزه دفاعی در کشور به صورت گام به گام و برنامه ریزی شده قرارمی گیرد. در گام نخست توجه به امن سازی زیرساخت‌های مورد استفاده در رایانش ابری مورد نظر است و در گام‌های بعدی ایجاد سرویس‌ها، هماهنگی بین بخش‌ها، تعریف کنترل دسترسی‌ها، یکپارچه سازی پایگاه‌های داده و غیره مورد توجه قرار واقع شود.

مراجع

- بهشتی، محمدتقی، (۱۳۹۱)،" *رایانش ابر: ساختار، مزایا و چالش‌ها*"، اولین کارگاه ملی رایانش ابری ایران - دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر،ایران.
- صادق زاده، پیام،(۱۳۹۲)،" *تحلیل و بررسی چالش‌های امنیتی موجود در محاسبات ابری*" هشتمین *سمپوزیوم پیشرفت‌های علوم و تکنولوژی*"، ریاست جمهوری،ایران.
- صدرالساداتی، سید محسن، (۱۳۹۲)،" *چالش‌های امنیتی در رایانش ابری و ارائه راهکاری جهت بهبود امنیت آن در راستای توسعه خدمات عمومی دولت الکترونیک*"، هشتمین سمپوزیوم پیشرفت‌های علوم و تکنولوژی"، ریاست جمهوری،ایران.
- قنبری، عباس، (۱۳۹۳)،"*رایانش ابری و نقش مجازی سازی در آن*"، دانشکده آموزش‌های الکترونیکی دانشگاه شیراز،ایران.
- نقیان فشارکی، مهدی،(۴۷:۱۳۹۳)، " ارائه معماری مرجع امنیتی محیط رایانش ابر خصوصی سازمان"، *فصلنامه علمی - پژوهشی امنیت پژوهی*

منابع لاتین:

- (Badger Lee, Bohn Robert ,2011),US Government Cloud Computing Technology Roadmap Volume II", NIST press.
- (Brunet Jean and Claudon Nicolas ,107-2015:81),Chapter 7 - Military and Big Data Revolution, In Application of Big Data for National Security, edited, Butterworth-Heinemann.
- Economist Report, "CyberWar: War in the fifth domain", on www.economist.com/node/16478792
- (Theothary Harrington ,2015)" Cyber Operations in DOD Policy and Plans: Issues for Congress", Congressional Research Service.
- (Hogan Michael ,2011),NIST Cloud Computing Standards Roadmap " NIST.
- ,(Mackay, T. Baker, A. Al-Yasiri,686-2012:679) Security-oriented cloud computing platform for critical infrastructures, Computer Law & Security Review, Volume 28, Issue 6.
- (Martin Paul ,2013) "NASA'S PROGRESS IN ADOPTING CLOUD-COMPUTING TECHNOLOGIES", OFFICE OF INSPECTOR GENERAL.

- Matthew Metheny, Chapter 1 - Introduction to the Federal Cloud Computing Strategy, In Federal Cloud Computing, edited by Matthew Metheny, Syngress, Boston, 2013, Pages 1-3۰
- Mell, Peter, “ The NIST Definition of Cloud Computing” , NIST Special Publication 800-145, 2011
- Pritzker, Penny,” NIST Cloud Computing Forensic Science Challenges” , NIST press, 2014
- Sareen Pankaj, Cloud Computing: Types, Architecture, Applications, Concerns, Virtualization and Role of IT Governance in Cloud, 2013
- Takai, M.Teresa, “DoD Cloud Computing Strategy”, Department of Defense Chief Information Officer, 2012
- Theothary , Catherine , " Cyberwarfare and Cyberterrorism: In Brief", Congressional Research Service, 2015
- Turab Nidal,” CLOUD COMPUTING CHALLENGES AND SOLUTIONS”, International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.5, September 2013
- Williams Stuart, “IBM Cloud Services Balancing compute options: How IBM Smart Cloud can be a catalyst for IT transformation” , 2011
- Yunchuan Sun, "Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903.