دریافت مقاله: ۱۳۹۵/۰۳/۰۵
پذیرش مقاله: ۱۳۹۵/۱۲/۱۶

فصلنامهٔ مدیریت نظامی
سال هفدهم، شمارهٔ ۱، بهار ۱۳۹۶
ص‌ص ۱۰۶-۱۳۰

ارائه الگوی راهبردی مهاجرت سازمان‌های دفاعی به محیط رایانش ابری

دکتر محمدرضا ولوی[۱]، محمدرضا موحدی‌صفت[۲]، ایمان باقری کوشالشاه[۳]

چکیده

فناوری اطلاعات و ارتباطات دارای تأثیر مستقیم در همه بخش‌های یک سازمان است. رایانش ابری به‌عنوان یک فناوری نوظهور توانسته با به اشتراک‌گذاری منابع و برنامه‌های کاربردی میان کاربران، محیط انعطاف‌پذیر و قدرتمندی را در سازمان‌ها ایجاد نماید. امروزه اغلب سازمان‌های دنیا ازجمله سازمان‌های دفاعی در حال برنامه‌ریزی برای مهاجرت به محیط رایانش ابری می‌باشند. با وجود همه مزایای استفاده از رایانش ابری در سازمان‌های دفاعی، باید به مسئله امنیت به عنوان مهم‌ترین چالش توجه ویژه شود. تحقیق حاضر که به شیوه توصیفی ° پیمایشی است، به ارائه الگوی راهبردی برای نحوه مهاجرت سازمان‌های دفاعی به محیط رایانش ابری پرداخته است. جامعه آماری این تحقیق فرماندهان، مدیران و کارشناسان ارشد سازمان‌های فناوری اطلاعات نیروهای مسلح و دانشجویان دوره‌های دکتری مدیریت راهبردی فضای سایبر می‌باشند که به‌عنوان خبرگان تحقیق در نظر گرفته شده‌اند. نتایج تحقیق نشان می‌دهد که شناسایی زیرساخت‌های جاری سازمان‌های دفاعی در حوزه‌های مختلف و ایجاد الگو برای مهاجرت به محیط رایانش ابری به‌عنوان مهم‌ترین راهبردها باید مد نظر قرار گیرند. همچنین اقدامات مرتبط با هر راهبرد نیز به‌عنوان نتایج تحقیق آورده شده است.

واژه‌های کلیدی: رایانش ابری، سازمان‌های دفاعی، امنیت فناوری اطلاعات و ارتباطات

---

۱. دانشیار برق، دانشگاه صنعتی مالک اشتر
۲. استادیار مهندسی فناوری اطلاعات، دانشگاه عالی دفاع ملی (نویسندهٔ مسئول)، ✉ movahedi@sndu.ac.ir
۳. کارشناسی ارشد مهندسی نرم‌افزار، دانشگاه آزاد اسلامی واحد تهران جنوب

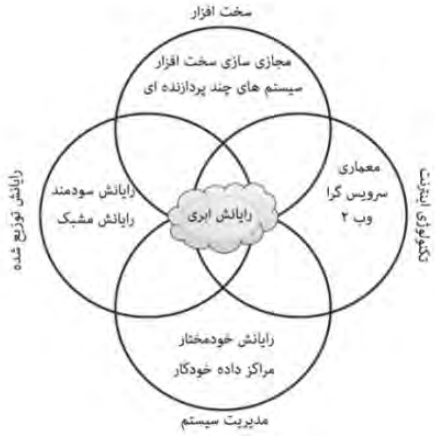
مقدمه

ماهیت نبردها در عصر فناوری اطلاعات و ارتباطات تغییر کرده و به شکل جنگ اطلاعات درآمده و در این خصوص استفاده از سامانه‌های فناوری به منظور برتری اطلاعاتی نقش حیاتی را ایفا می‌نماید (عبدی، ۱۳۹۰). سازمان‌های دفاعی در دنیا نیز در حال مهاجرت به سوی فناوری نوظهور رایانش ابری هستند تا از این طریق به مزیت‌های فراوانی ازجمله چابکی، کارایی و نوآوری دست یابند (تاکایی[1]، ۲۰۱۲). کسب اطلاعات دقیق‌تر از وضعیت دشمن در صحنه نبرد از دیگر مزایایی است که از اهمیت ویژه‌ای برخوردار است (رزمجو، ۱۳۸۶).

محیط رایانش ابری دارای ویژگی‌های مهمی نظیر ارائه سرویس بر مبنای تقاضا، دسترسی به شبکه گسترده و ادغام منابع است. هدف از مهاجرت سازمان‌های دفاعی به این محیط نیز استفاده از سامانه‌های قدرتمند در محیط شبکه با در نظر گرفتن کاهش هزینه‌ها و افزایش بهره‌وری و عملکرد می‌باشد. لذا رایانش ابری بر اساس خصوصیات خود و همچنین حساسیت نهادهای دفاعی می‌تواند برای توسعه هر چه بیشتر مورد استفاده قرار گرفته و علاوه بر کاهش هزینه‌های مراکز داده و افزایش بهره‌وری، محیطی یکپارچه را برای این سازمان‌ها ایجاد نماید (تاکایی، ۲۰۱۲).

پیدایش رایانش ابری مرتبط با توسعه فناوری در حوزه‌های سخت‌افزاری (نظیر مجازی‌سازی و پردازنده‌های چندهسته‌ای)، فناوری اینترنت (نظیر وب‌سرویس‌ها، معماری سرویس‌گرا و وب ۲) و رایانش توزیع شده (نظیر رایانش خوشه‌ای[2] و مشبک[3]) است. می‌توان رایانش ابری را حاصل همگرایی و پیشرفت در حوزه‌های اصلی فناوری دانست. این فناوری‌های که در تعامل با یکدیگر به ظهور فناوری رایانش ابری کمک کرده‌اند، در شکل ۱ نشان داده شده‌اند.

1. Takai, M.
2. cluster computing
3. grid computing



شکل ۱: فناوری‌های مرتبط با رایانش ابری

رایانش ابری فرصت جدیدی را برای سازمان‌های دفاعی در محیط شبکه‌محور فراهم می‌کند. دسترسی به منابع اشتراکی بر اساس تقاضا و به‌صورت بی‌درنگ یکی از این منافع می‌باشد. این فناوری دارای سه مدل اصلی نرم‌افزار به‌عنوان خدمت[۱]، بستر به‌عنوان خدمت[۲] و زیرساخت به‌عنوان خدمت[۳] است که در بخش بعدی تعریف شده‌اند (ادل[۴]، وانگر[۵] و ویر[۶]، ۲۰۱۵).

مهاجرت سازمان‌های دفاعی به محیط رایانش ابری باعث می‌شود تا زیرساخت‌های فناوری اطلاعات این سازمان‌ها در جهت بهره‌برداری حداکثری از اطلاعات و خدمات تغییر کرده و مدل‌های جدیدی برای عرضه خدمات فراهم گردد. استفاده از این فناوری در حوزه دفاعی کمک می‌نماید تا خدمات و کارکردهای دفاعی در یک بستر یکپارچه و با حداکثر بهره‌وری بکار گرفته شود. البته باید به مسئله امنیت و ایجاد ملاحظات و تمهیدات امنیتی به عنوان مهم‌ترین چالش‌های پیش رو توجه ویژه‌ای داشت. بدیهی است انجام این مهاجرت در صورتی که به چالش‌های امنیتی آن توجه نشود، می‌تواند یک تهدید جدی به حساب آید.

1. SaaS-Software as a Service
2. PaaS-Platform as a Service
3. IaaS-Infrastructure as a Service
4. Odell, L. A.
5. Wagner, R.
6. Weir, T. J.

در حال حاضر بسیاری از سازمان‌های دفاعی دنیا نظیر وزارت دفاع آمریکا برنامه‌ریزی‌های گسترده‌ای را برای مهاجرت به محیط رایانش ابری در دست اقدام داشته و در این خصوص اسناد راهبردی خود را تنظیم کرده‌اند.

بیان مسئله و ضرورت انجام تحقیق

بیان مسئله

ایجاد هماهنگی در بخش‌های مختلف نهادهای دفاعی کشور و ارتقای بهره‌وری این سازمان‌ها مبتنی بر استفاده از فناوری‌های نوظهور، از اهمیت بالایی برخوردار است و با استفاده از روش‌های سنتی و فناوری‌های قدیمی قطعاً نمی‌توان به این مهم دست یافت. رایانش ابری به‌عنوان یک ظرفیت جدید بر اساس قابلیت‌هایی که دارد، می‌تواند به افزایش کارایی و چابکی سازمان‌های دفاعی کمک نماید.

در حال حاضر اغلب خدمات موجود در سازمان‌های دفاعی مبتنی بر سامانه‌هایی است که عموماً به‌صورت جزیره‌ای تولید و مورد استفاده قرار می‌گیرند و این مسئله باعث شده تا ارتباطات درون و بین سازمانی با صرف هزینه و زمان نسبتاً زیادی انجام پذیرد و مسئله یکپارچگی این سامانه‌ها با معضلات فراوانی مواجه شود. مهاجرت سازمان‌های دفاعی به محیط رایانش ابری برای استفاده از سامانه‌های یکپارچه می‌تواند باعث افزایش قابلیت دسترسی‌پذیری، کارایی، توسعه‌پذیری و کاهش هزینه‌ها شود. از الزامات مهاجرت سازمان‌های دفاعی به این محیط‌ها می‌توان به بلادرنگ شدن و کاهش هزینه خدمات، امکان دسترسی بیشتر به اطلاعات و خدمات، اشتراک‌پذیری در خدمات و عدم نیاز به دخالت‌پذیری سرویس‌دهندگان اشاره داشت. لازم به ذکر است که در همه این موارد باید ملاحظات و تمهیدات امنیتی در نظر گرفته شوند. زیرا با توجه به حساس بودن مراکز دفاعی کشور، تهدیدات امنیتی می‌تواند تمام منافع مهاجرت به رایانش ابری را از بین برده و نتایج جبران‌ناپذیری را برای این مراکز به وجود آورد. اتحادیه امنیت پردازش ابری[1] دستورالعمل‌هایی را برای بهبود امنیت رایانش ابری ارائه نموده است که اگر این دستورالعمل‌های بین‌المللی با سیاست‌های امنیتی کشور ادغام شوند، می‌توانند به یک راهکار امنیتی مناسب برای ایجاد زیرساخت رایانش ابری حوزه دفاعی تبدیل گردند. لذا ارائه الگوی

1. Cloud Security Alliance (CSA)

امنیت پایه برای مهاجرت سازمان‌های دفاعی به محیط رایانش ابری بسیار حائز اهمیت است.

ضرورت و اهمیت تحقیق

تحقیقات انجام شده نشان می‌دهد که تاکنون روشی برای مهاجرت سازمان‌های دفاعی به محیط شبکه‌محور رایانش ابری انجام نشده است. همچنین در مدل‌های ارائه شده که بیشتر برای سازمان‌های تجاری می‌باشد، کمتر به ملاحظات و تهدیدات امنیتی که جزء مهم‌ترین عوامل هستند، توجه شده است.

برای مهاجرت سازمان‌های دفاعی به محیط‌های رایانش ابری به‌منظور بهره‌برداری حداکثری از منابع باید الگوهای راهبردی مهاجرت تدوین شوند که تحقیق حاضر درصدد است تا این الگوها را با در نظر گرفتن شاخص‌های امنیتی ارائه نماید. برای انجام این مهاجرت باید به طراحی معماری امنیتی نیز توجه ویژه‌ای صورت پذیرد.

سؤال تحقیق

الگوی راهبردی مهاجرت سازمان‌های دفاعی به محیط رایانش ابری با در نظر گرفتن مؤلفه‌های امنیتی چیست؟

پیشینه تحقیق

امنیت همواره به‌عنوان مهم‌ترین دغدغه در محیط رایانش ابری مطرح و این موضوع به یک چالش اساسی تبدیل شده است. از طرفی مزیت‌های زیادی که در حوزه رایانش ابری وجود دارد، دولت‌ها و سازمان‌های بزرگ دنیا ازجمله سازمان‌های دفاعی را به این سمت استفاده از آن هدایت نموده است. در ادامه به برخی از تحقیقات انجام شده اشاره می‌شود:

- محمدرضا ولوی در مقاله خود الگویی امن جهت استقرار زیرساخت‌های دفاعی کشور در محیط رایانش ابری ارائه نموده است (ولوی و موحدی، ۱۳۹۵). در مدل ارائه شده امنیت به عنوان مهم‌ترین خدمت[1] در یک لایه مجزا در نظر گرفته شده؛ به گونه‌ای که بر روی همه خدمات دیگر تأثیرگذار می‌باشد؛

1. SECaaS-Security as a Service

- مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، طرح فراسازمانی فاوای نیروهای مسلح را ارائه نموده است. در این طرح معماری مفهومی رایانش ابری اپراتور امید ارائه شده و به مسئله امنیت به‌عنوان مهم‌ترین چالش استقرار رایانش ابری پرداخته شده است (سند زیرساخت فاوای فرماندهی و کنترل، ۱۳۹۲)؛
- مهدی نقیان فشارکی معماری مرجع امنیتی برای سازمان‌هایی را که درصدد پیوستن به محیط رایانش ابری هستند، مورد بررسی قرار داده است. در این مقاله به شناخت سازمان و مهندسی نیازمندی‌های امنیتی سازمان، ترسیم معماری سطح بالای محیط ابری سازمان، نحوه نگاشت مؤلفه‌های امنیتی با بازیگرهای محیط ابری و الگوهای پیاده‌سازی آن، تدوین الگوی رسمی معماری مرجع امنیتی و در نهایت به ارزیابی معماری مرجع امنیتی اشاره شده است (نقیان فشارکی: ۱۳۹۳)؛
- مرکز فناوری اطلاعات وزارت دفاع[1] آمریکا به‌منظور شناسایی فرصت‌ها و مزیت‌هایی که بر اثر استفاده از رایانش ابری فراهم می‌شود، برنامه‌ریزی‌های لازم برای تبدیل این وزارتخانه از یک حالت تکراری، پرزحمت، طاقت‌فرسا و پرهزینه به یک مجموعه چالاک، امن و کم‌هزینه را انجام داده و پروژه مهاجرت را در دست اقدام دارد. هدف اصلی از رایانش ابری در وزارت دفاع آمریکا پشتیبانی از مأموریت سازمانی در همه مکان‌ها و همه زمان‌ها و بر روی همه تجهیزات دارای هویت در وزارت دفاع است (تاکایی، ۲۰۱۲)؛
- شرکت IBM در معماری رایانش ابری سازمانی امنیت محیطی را به عنوان مهم‌ترین شاخص در نظر گرفته و بر این اساس معماری را ارائه کرده است (ویلسون[2]، ۲۰۱۳).

1. CIO (Chief Information Officer)
2. Wilson, J. R.

وضعیت جاری این سازمان نشان می‌دهد که زیرساخت‌های مهم آن بر روی محیط رایانش ابری استقرار یافته است؛

- ناسا سالیانه ۱,۵ میلیارد دلار در بخش فناوری اطلاعات خود هزینه می‌کند تا بتواند یک 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 می‌باشد (پائول[2]، ۲۰۱۳).

روش تحقیق و جامعهٔ آماری

روش استفاده شده در این پژوهش از نوع توصیفی- پیمایشی است و نتایج آن قابلیت به‌کارگیری در سازمان‌های دفاعی را دارد. این تحقیق از لحاظ نوع هدف، کاربردی است و به منظور جمع‌آوری داده‌ها در این پژوهش، از دو روش کتابخانه‌ای و میدانی برای دستیابی به آخرین دستاوردهای مطالعات و پژوهش‌های انجام شده است. همچنین برای تکمیل ادبیات تحقیق از روش مطالعات میدانی و مصاحبه با افراد خبره استفاده شده است.

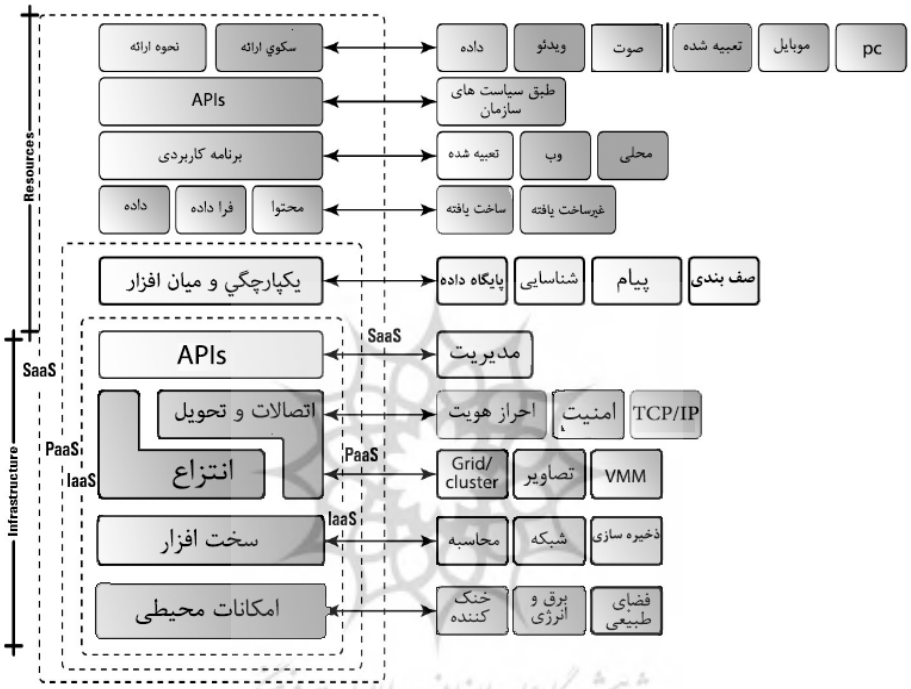
جامعه آماری این تحقیق شامل مدیران و کارشناسان ارشد سازمان‌های فناوری اطلاعات نیروهای مسلح و همچنین دانشجویان دوره‌های دکتری مدیریت راهبردی فضای سایبر می‌باشد. برای تحقیق حاضر حجم نمونه ۴۷ نفر به روش تمام شماری و با بهره‌گیری از خبرگی تعیین گردیده است. برای این منظور پرسشنامه‌ای توزیع و نظرات اخذ شده است. با استفاده از داده‌های به‌دست آمده و به کمک نرم‌افزار SPSS میزان ضریب اعتماد با روش آلفای کرونباخ بیش از ۰/۷ به دست آمد. لذا پرسشنامه مورد استفاده دارای قابلیت اعتماد لازم می‌باشد.

مبانی نظری تحقیق

مؤسسه ملی استاندارد و فناوری[3] رایانش ابری را این‌گونه تعریف کرده است: «رایانش ابری مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه به

1. Open Stack
2. Paul, M.
3. NIST-National Institute of Standard and Technology

مجموعه‌ای از منابع رایانشی قابل تغییر و پیکربندی که این دسترسی بتواند با کمترین نیـاز بـه مدیریت منابع و یا نیاز به دخالت مستقیم فراهم‌کننده سرویس به‌سرعت فراهم شـود». (مـل[1] و گرنس[2] ۲۰۱۱) شکل ۲ معماری خدمات رایانش ابری را نشان می‌دهد. (سوسینکی[3]، ۲۰۱۰)



شکل ۲: معماری خدمات رایانش

مدل‌های مهم در رایانش ابری عبارت‌اند از:

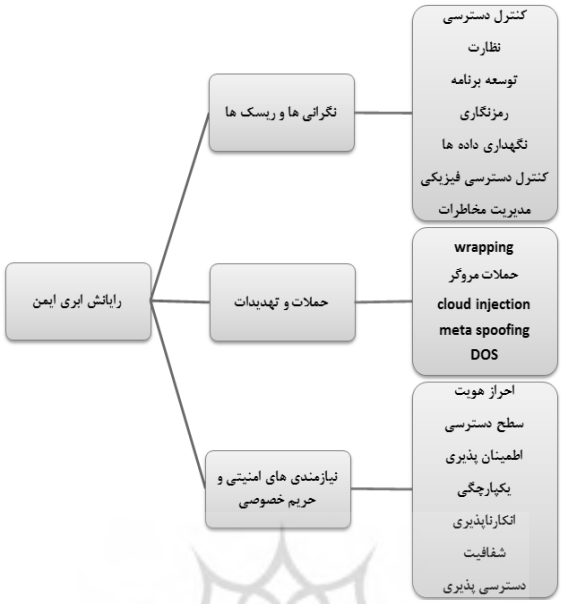
- مدل نرم‌افزار به عنوان خدمت: هنگامی‌که کاربر از یک نرم‌افزار مانند برنامه‌های کاربردی به عنوان خدمت استفاده می‌کند؛

1. Mell, P.
2. Grance, T.
3. Sosinsky, B.

- بستر به عنوان خدمت: به کاربر اجازه می‌دهد تا برنامه‌های کاربردی مورد نظرشان را با استفاده از ابزارهایی که از سوی ارائه دهنده عرضه شده‌اند، به وجود آورند؛
- زیرساخت به عنوان خدمت: دسترسی کاربران به زیرساخت‌های اصلی مثل سرورها، ماشین‌های مجازی، فضاهای ذخیره‌سازی و غیره را فراهم می‌کند.

با وجود همه مزایای رایانش ابری باید به چالش‌های آن نیز توجه داشت. در محیط‌های رایانش ابری به دلیل عدم دسترسی فیزیکی به سیستم و وجود ساختارهای پیچیده، پیگیری و بررسی تهدیدات امنیتی دشوار است (امنیت رایانش ابری، ۲۰۱۳). از سوی دیگر مجازی‌سازی می‌تواند باعث به وجود آمدن تهدیدات امنیتی جدیدی در محیط ابری شود (لو[1]، لین[2]، چن[3]، یانگ[4] و چن[5]، ۲۰۱۱). لذا در حوزه امنیت رایانش ابری لازم است تا نیازمندی‌های امنیتی برای کاربران و ارائه‌دهندگان ابری تعیین شود. در شکل ۳ تهدیدات و حملات امنیتی موجود در محیط رایانش ابری نشان داده شده است (یوسف[6] و الجیل[7]، ۲۰۱۲).

1. Luo, S.
2. Lin, Z.
3. Chen, X.
4. Yang, Z.
5. Chen, J.
6. Youssef, A.
7. Alageel, M.



شکل ۳: تهدیدات و حملات امنیتی درون ابر

همچنین لازم است تهدیدات و چالش‌های امنیتی موجود در رایانش ابری برای هر یک از سرویس‌های ارائه شده شناسایی شود. حوزه‌های تعامل، تمرکززدایی و توزیع‌شدگی و تنوع از مهم‌ترین خصوصیات رایانش ابری دفاعی می‌باشند. جدول ۱ نیازمندی‌ها و تهدیدات امنیتی هر یک از سطوح سرویس‌های ابری را نشان می‌دهد.

جدول ۱: نیازمندی‌ها و تهدیدات امنیتی لایه‌های سرویس‌دهی ابر

سطح	سطح سرویس	نیازمندی‌های امنیتی	حملات
سطح برنامه کاربردی	نرم‌افزار به عنوان سرویس (SaaS)	حریم خصوصی محافظت از داده‌ها کنترل دسترسی حفاظت از ارتباطات امنیت نرم‌افزار در دسترس بودن سرویس	استراق سمع تغییر و حذف داده‌ها نقض حریم خصوصی جریان ترافیک ربودن نشست جعل هویت

سطح	سطح سرویس	نیازمندی‌های امنیتی	حملات
سطح مجازی	بستر به‌عنوان سرویس (PaaS) زیرساخت به‌عنوان سرویس (IaaS)	کنترل دسترسی امنیت برنامه کاربردی و داده‌ها امنیت کنترل مدیریت ابر تصاویر ایمن حفاظت از ابر مجازی امنیت ارتباطات	نقص برنامه‌نویسی تغییر نرم‌افزار وقفه در نرم‌افزار ربودن نشست اختلال در ارتباطات سیل اتصالات
سطح فیزیکی	دیتاسنتر فیزیکی	امنیت سخت‌افزار قابلیت اطمینان سخت‌افزار حفاظت از شبکه حفاظت از منابع شبکه	حملات شبکه‌ای حملات DDOS ازکارافتادن و تغییر سخت‌افزار سوءاستفاده از زیرساخت سرقت سخت‌افزار بلایای طبیعی

رایانش ابری دفاعی

همان‌گونه که اشاره گردید بسیاری از سازمان‌ها رایانش ابری را به عنوان یک فناوری نوین پذیرفته و مهاجرت به آن را به‌عنوان یک اولویت در نظر گرفته‌اند. بسیاری از کشورها در حال برنامه‌ریزی برای استقرار زیرساخت‌های حساس و مهم خود بر روی این محیط هستند. دفاع نیز یکی از زیرساخت‌های مهم و حیاتی است که در حال استقرار بر روی محیط رایانش ابری است که البته در این خصوص ملاحظات امنیتی با دقت بیشتری باید مورد توجه قرار گیرد.

رایانش ابری دفاعی زیرساخت یکپارچه و توزیع‌شده‌ای است که قادر است تمامی مراکز دفاعی کشور را با یکدیگر هماهنگ نماید. استفاده از رایانش ابری و تطبیق آن با حوزه دفاعی می‌تواند باعث کاهش هزینه‌ها و افزایش بهره‌وری شده و تهدیدات امنیتی را کاهش دهد. فواید استفاده از رایانش ابری در حوزه دفاعی می‌تواند در سه ویژگی چابکی، نوآوری و بهره‌وری تقسیم‌بندی گردد. این فواید در جدول ۲ نشان داده شده است.

جدول ۲: فواید استفاده از رایانش ابری

بهره‌وری	
استفاده از فناوری رایانش ابری	وضعیت فعلی
• استفاده حداکثری (بیش از ۷۰ درصدی) از دارایی‌ها و منابع • تجمیع منابع و دارایی‌ها • افزایش بهره‌وری در سرعت توسعه برنامه‌ها، شبکه، مدیریت برنامه‌ها و کاربران	• استفاده محدود (حداکثر ۳۰ درصدی) از دارایی‌ها • مستقل بودن سیستم‌ها از یکدیگر • مدیریت سخت و پیچیده سازمان
چابکی	
استفاده از فناوری رایانش ابری	وضعیت فعلی
• خرید خدمات از ارائه دهندگان خدمات • افزایش و کاهش سریع ظرفیت‌ها • پاسخگویی سریع به درخواست‌ها	• صرف زمان چندساله برای ساخت مراکز داده • صرف زمان زیاد برای راه‌اندازی یک خدمت
نوآوری	
استفاده از فناوری رایانش ابری	وضعیت فعلی
• تغییر از مالکیت خدمت به ارائه خدمت • تشویق فرهنگ کارآفرینی	• مالکیت دارایی‌ها

با توجه به جدول ۲ مشاهده می‌شود که مهاجرت سازمان‌های دفاعی به محیط رایانش ابری می‌تواند به افزایش انعطاف‌پذیری، چابکی و صرفه‌جویی بینجامد. با وجود این، مهاجرت از سامانه‌های سنتی به‌سوی ارائه خدمات مبتنی بر رایانش ابری، باعث بروز چالش‌های جدیدی

در حوزه‌های امنیتی خواهد شد که این مسئله برای سازمان‌های دفاعی حائز اهمیت است و لازم است تا مؤلفه‌ها و زیرساخت‌های لازم شناسایی شوند... شکل ۴ تصویری منطقی از ابر دفاعی را نشان می‌دهد. همان‌طور که مشاهده می‌شود این ابر قادر است تا با یکپارچه کردن سامانه‌ها، بسترها و زیرساخت‌ها، سازمان‌های دفاعی و حوزه‌های تابعه را با یکدیگر هماهنگ نماید. به این محیط یکپارچه «ابر یکپارچه دفاعی» اطلاق می‌گردد.

شکل ۴: تصویری منطقی از ابر یکپارچه دفاعی

بازیگران موجود در رایانش ابری دفاعی

چالش‌های امنیتی در قرن حاضر در حال تغییر است و در این میان امنیت به عنوان مهم‌ترین شاخص باید در همه حوزه‌های دفاعی مورد توجه واقع گردد. همچنین فناوری‌های نظامی نیز در حال تغییر و تحول هستند و هر روز نیاز به فناوری‌های جدید احساس می‌شود. فرض کنید قرار است یک عملیات نظامی در سطح ملی و یا بین‌المللی انجام شود، آنگاه چگونه می‌توان عملیات، نیروها، افراد و تجهیزات را با یکدیگر هماهنگ نمود؟

ساختار رایانش ابری حوزه دفاعی که در مقاله نویسندگان این مقاله به آن اشاره شده است (ولوی و موحدی، ۱۳۹۵)، به طور کامل منطبق بر مدل استاندارد مرجع رایانش ابری است. فراهم‌کنندگان سرویس‌ها، مصرف‌کنندگان سرویس‌ها، کارگزاری‌ها، کنترل‌ها و حامل‌ها به عنوان مهم‌ترین این بخش‌ها هستند.

زیرساخت ارتباطی

وجود ارتباطات میان موجودیت‌ها یکی از ملزومات اصلی در ایجاد محیط رایانش ابری دفاعی است که باید طراحی و ایجاد شود. با توجه به اهمیت امنیت در محیط رایانش ابری دفاعی، طراحی و ایجاد زیرساخت‌های ارتباطی نیز چالش‌برانگیز هستند. زیرساخت‌های ارتباطی باید ایمن، چابک، دارای قدرت تحمل‌پذیری بالا، پهنای باند بالا و پویا باشند تا بتوان خدمات مورد نیاز به سازمان‌های دفاعی ارائه شود.

با وجود هزاران پایگاه اطلاعاتی و عملیاتی هوایی، دریایی و زمینی ثابت و سیّار در سطح کشور، این زیرساخت ارتباطی باید بسیار انعطاف‌پذیر، در دسترس و قابل مدیریت باشد. در شکل ۵ جایگاه پروتکل‌های ارتباطی در یک محیط رایانش ابر دفاعی نشان داده شده است.

شکل ۵: جایگاه ارتباطات در محیط رایانش ابری دفاعی

زیرساخت ارتباطی باید در نقاط حساس مانند صحنه نبرد دارای ویژگی‌هایی زیر باشد:

- انتقال داده‌های فراوان در کسری از زمان؛

- قابلیت دسترسی سراسری و گستردگی پویا؛
- تحویل مطمئن اطلاعات؛
- ایجاد ارتباطات سیار.

جلوگیری از انواع حملات فیزیکی، سایبری یا الکترونیکی، چند مسیری بودن ارتباطات، توانایی تخصیص مجدد مسیر، سیاست‌ها و اولویت‌بندی‌های فرماندهان و مسیریابی خودکار ازجمله مهم‌ترین ملاحظات مطرح در ایجاد زیرساخت ارتباطی است که باعث ایجاد دسترسی‌پذیری بالا می‌شود.

ملاحظات مطرح در رایانش ابری دفاعی

محیط‌های اشتراکی منشأ بروز بسیاری از چالش‌ها و تهدیدات هستند. در یک محیط اشتراکی کاربران از سامانه‌ها و منابع به‌صورت اشتراکی استفاده می‌کنند و مسائل مربوط به تخصیص و مدیریت منابع در چنین محیطی حائز اهمیت می‌باشد. به علاوه، ارتباط‌های موجود میان این نوع سامانه‌ها با یکدیگر می‌تواند مستلزم ایجاد تهدیدات امنیتی و یا کاهش قابلیت دسترسی گردد. اگرچه مسائل مربوط به جداسازی کارکردها همیشه در محیط‌های دفاعی مطرح است، اما این چالش به طور کامل برطرف نگردیده است (آرداگنا[1]، ۲۰۱۵: ۱).

همچنین مجازی‌سازی به‌عنوان اصلی‌ترین محور در ایجاد و استقرار رایانش ابری مطرح می‌گردد. مجازی‌سازی می‌تواند قابلیت استفاده از منابع سامانه‌ها را به میزان زیادی افزایش دهد. در واقع تمامی مسائل مطرح در ایجاد عمومی می‌تواند به طور جدی‌تر در ابر دفاعی مطرح شود. تفکیک رایانش ابری خصوصی ویژه سازمان‌های دفاعی از رایانش ابری عمومی الزامی است و به منظور اشتراک‌پذیری اطلاعات باید به الگوریتم‌های رمزنگاری به طور کامل توجه شود. در شکل ۶ ملاحظات مهم امنیتی در ابر حوزه دفاعی نشان داده شده است.

1. Ardagna, D.

شکل ۶: ملاحظات امنیتی رایانش ابری حوزه دفاعی

- **کارکرد:** محیط رایانش ابری دفاعی مانند محیط‌های فرماندهی و کنترل یک محیط اشتراکی برای استفاده از منابع موجود در سازمان‌های دفاعی است و باید به گونه‌ای ایجاد شود تا بر اثر استفاده بیش از حد از منابع موجود، عملکرد آن کاهش نیافته و باعث اختلال در عملکردها نگردد. اگر در صحنه نبرد داده‌ها به سرعت منتقل نشوند، باعث بروز مشکلات فروانی خواهند شد و این مسئله در ابر دفاعی می‌تواند به یک بحران تبدیل شود.
- **امنیت اطلاعات:** امنیت اطلاعات مهم‌ترین مسئله در رایانش ابری حوزه دفاعی است. امنیت اطلاعات شامل مواردی همچون احراز هویت کاربران، محرمانگی، یکپارچگی و کنترل دسترسی می‌باشد.
- **حریم خصوصی داده‌ها:** با وجود داده‌های محرمانه و طبقه‌بندی‌شده، داده‌های موجود در محیط رایانش ابر دفاعی باید از دید دیگران مخفی بماند. اطمینان از مخفی ماندن داده‌ها با توجه به اهمیت حوزه‌های دفاعی بسیار حائز اهمیت است.

- **نظارت:** یکی از محوری‌ترین مؤلفه‌هایی که لازم است در محیط رایانش ابر حوزه دفاعی در نظر گرفته شود، نظارت بر مکان قرارگیری داده‌ها، عملکرد سیستم و کیفیت سرویس‌ها است.
- **دسترسی‌پذیری:** با توجه به وجود مراکز و زیرساخت‌های بحرانی در ابر حوزه دفاعی لازم است تمامی این قسمت‌ها بتوانند به تمامی امکانات موجود در ابر به سرعت و به سهولت دسترسی داشته باشند.
- **قابلیت حمل:** به منظور همسویی و یکپارچگی در اطلاعات و خدمات حوزه دفاعی باید قابلیت حمل را برای سامانه‌ها به وجود آورد. این امر باعث کاهش هزینه‌ها و کاهش زمان شده و از دوباره‌کاری در تولید برنامه‌های جدید جلوگیری می‌کند.
- **یکپارچگی:** داده‌های موجود در شرایط بحرانی و حساس باید به سرعت یکپارچه شده و اطلاعات و داده‌ها در تمامی مراکز مهم به‌صورت یکسان قابل دسترسی باشند.

معماری‌های امنیتی رایانش ابری

در حوزه رایانش ابری، تاکنون چارچوب‌های معماری امنیتی متنوعی به وسیلهٔ محققان و سازمان‌های دولتی و خصوصی مانند سازمان ملی استاندارد و فناوری، وزارت دفاع، دارپا، آژانس امنیت اطلاعات و شبکهٔ اروپا[1] و اتحادیه امنیت ابری ارائه شده است. در حال حاضر دو معماری مهم DoDAF و C_4ISR که مختص سازمان‌های نظامی هستند، در حال بازتعریف شدن در محیط رایانش ابری هستند. مؤسسه ملی استاندارد و فناوری نیز مدل مرجع معماری امنیتی را در یک سند مجزا انتشار داده است. (سند مؤسسه ملی استاندارد و فناوری، ۲۰۱۳)

چالش‌ها و الزامات امنیتی در ابر حوزه دفاعی

اگرچه رایانش ابری دارای مزایای بسیاری است که مهم‌ترین آن‌ها استفاده از منابع اشتراکی و

1. European Network and Information Security Agency

استفاده از منابع بر اساس میزان تقاضا می‌باشد، اما چالش‌هایی نیز در خصوص استفاده از آن وجود دارد که به کارگیری کامل آن را برای مدیران سازمان‌های دفاعی با مشکل مواجه می‌کند. توسعه‌پذیری رایانش ابری ممکن است بر اساس محدودیت‌هایی که سرویس‌دهنده‌ها دارند، سطحی از عدم اطمینان را به وجود آورد و سازمان در مواردی با محدودیت منابع روبرو شود (کویورا[1]، ایبی‌کانل[2] و اوودل[3]، ۲۰۱۱). به طور کلی چالش‌های موجود در محیط رایانش ابری به بخش‌های زیر تقسیم می‌شوند.

- **امنیت و حریم شخصی**

امنیت[4] و حریم شخصی[5]، بزرگ‌ترین چالش رایانش ابری هستند. در سال‌های اخیر تحقیقات فراوانی در این خصوص انجام شده، اما همچنان این چالش به طور کامل برطرف نشده است. با وجود این، مسائل مرتبط به حریم شخصی و امنیت می‌تواند با استفاده از ساختارهایی نظیر رمزنگاری، استفاده از سخت‌افزارها و نرم‌افزارهای امنیتی تا حدودی برطرف شود (جلمن[6]، ۲۰۰۹ و کومار[7]، ۲۰۱۵).

- **دسترس‌پذیری[8]**

قابلیت دسترسی یکی از مهم‌ترین مؤلفه‌هایی است که باید در ابر حوزه دفاعی به آن توجه ویژه شود. از آنجا که فعالیت‌های موجود در ابر دفاعی می‌تواند بحرانی بوده و دارای نقطه پایان زودهنگام باشد، لازم است سیستم‌ها به طور یکنواخت فعال بوده و قابلیت پاسخگویی به نیازهای کاربران را داشته باشد (مظهر[9]، سماعی[10]، اتناسیس[11]، واسیلاکس[12]، ۲۰۱۵).

---

1. Kuyoro, S. O.
2. Ibikunle, F.
3. Awodele, O.
4. security
5. privacy
6. Gellman, R.
7. Kumar, N.
8. availability
9. Mazhar, A.
10. Samaee, U.
11. Athansios, V.
12. Vasilakos, M.

- **قابلیت همکاری**

سامانه‌های مستقر بر روی ساختار رایانش ابری باید قادر باشند تا خدمات مربوطه را با یکدیگر ترکیب نمایند. این عمل از طریق خدمات مبتنی بر وب امکان‌پذیر می‌باشد. تولید این‌گونه خدمات وب، پیچیده است و نیاز به متخصصان این حوزه دارد (متر[1]، کوماراسوامی[2] و لطیف[3]، ۲۰۰۹).

- **قابلیت حمل**

با توجه به آنکه لازم است برنامه‌های تولید شده در محیط رایانش ابری از یک ارائه‌دهنده به ارائه دهنده دیگری منتقل شود، لازم است در این خصوص سیاست‌های مناسبی برای بهبود این امر اتخاذ گردد. سامانه‌های کاربردی باید بتوانند به راحتی منتقل شوند. این مشکل تاکنون به طور کامل حل نشده است؛ زیرا ارائه‌دهندگان خدمات رایانش ابری از یک زبان استاندارد برای زیرساخت‌ها استفاده نمی‌کنند (مظهر، سماعی، اتناسیس، واسیلاکس، ۲۰۱۵).

تجزیه وتحلیل یافته‌های تحقیق

پس از بررسی‌های صورت گرفته و دریافت نظرات خبرگانی که در این طرح مشارکت داشته‌اند، مهاجرت سازمان‌های دفاعی به محیط رایانش ابری مزایای فراوانی را به وجود خواهد آورد. در ادامه به برخی از این موارد اشاره شده است.

رایانش ابری حوزه دفاعی یک الزام برای کشور می‌باشد و در این خصوص ملاحظات و تمهیدات امنیتی به‌عنوان مهم‌ترین چالش می‌باشد. همچنین در مهاجرت سازمان‌های دفاعی به محیط‌های رایانش ابری، توجه به زیرساخت‌ها در نهادها و سازمان‌های دفاعی یک مسئله حیاتی است. از نکات دیگر در مهاجرت سازمان‌های دفاعی به محیط‌های رایانش ابری باید به گام به گام بودن و مرحله‌ای بودن مهاجرت توجه ویژه شود. از نکات دیگر می‌توان به آموزش و فرهنگ‌سازی سازمانی مخصوصاً در رده مدیران و فرماندهان نظامی توجه داشت.

از آنجا که رایانش ابری حوزه دفاعی یک محیط یکپارچه اما توزیع شده است لازم است

1. Mather, T.
2. Kumaraswamy, S.
3. Latif, S.

تمامی مؤلفه‌ها، بازیگران و نقش‌ها بر اساس استانداردهای این حوزه تعریف شوند. همچنین با توجه به آنکه برای استقرار رایانش ابری مدل‌های مختلفی وجود دارد، برای سازمان‌های دفاعی بهتر است از مدل استقرار ابر خصوصی استفاده شود. در طراحی زیرساخت‌ها، شبکه‌ها و حامل‌ها می‌توان از توان کارکنان سازمان‌های دفاعی نیز استفاده کرد.

از آنجا که امنیت مهم‌ترین و شاخص‌ترین مؤلفه رایانش ابری حوزه دفاعی است، لازم است سرویس امنیت بر روی همه مؤلفه‌ها تأثیرگذار باشد. ایجاد لایه امنیت به عنوان سرویس به‌عنوان یک راهکار مؤثر پیشنهاد می‌شود. سرویس امنیت می‌تواند در بخش‌های مختلفی همچون ذخیره‌سازی داده‌ها، دسترسی به داده‌ها و سامانه‌ها و همچنین پایگاه‌های داده‌ای شکل گیرد و با ارائه الگوریتم‌های رمزنگاری امنیت دسترسی به این داده‌های طبقه‌بندی شده افزایش یابد. یکی از اهداف مهم برای مهاجرت سازمان‌های دفاعی، ایجاد قابلیت دسترس‌پذیری از طریق ایجاد پایگاه‌های داده یکپارچه است که با ایجاد یکپارچگی در این حوزه بسیاری از امور تکراری که در حال حاضر در سازمان‌های دفاعی وجود دارد، از بین خواهد رفت.

معماری امنیتی رایانش ابری دفاعی

شکل ۷ معماری امنیت پایه رایانش ابری حوزه دفاعی را نشان می‌دهد که در مؤسسه آموزشی و تحقیقاتی دفاعی تحت عنوان معماری مفهومی رایانش ابری اپراتور امید طراحی شده است.

شکل ۷: الگوی امنیت برای معماری رایانش ابری حوزه دفاعی امید

در معماری رایانش ابری حوزه دفاع باید سرویسی تحت عنوان امنیت به مجموعه اضافه شود تا اشراف امنیتی بر روی سایر سرویس‌ها و خدمات به وجود آید. همچنین تأمین یکپارچگی، محرمانگی و دسترس‌پذیری به سرویس‌ها علی‌الخصوص در شرایط بحرانی در این بخش انجام خواهد شد. نظارت بر امنیت خدمات برون‌سپاری شده دفاعی که حائز اهمیت می‌باشد نیز بر عهده این بخش است و سرویس‌هایی به سازمان‌های خارج از سازمان دفاعی سپرده می‌شوند که از امنیت آن سازمان‌ها اطمینان حاصل شده باشد.

تأمین و پیکربندی زیرساخت‌های مورد استفاده در معماری رایانش ابری دفاعی که غالباً در لایه حامل و فیزیکی وجود دارند نیز در این قسمت تعبیه شده است. نحوه پیکربندی زیرساخت شبکه‌ای که در رایانش ابری حوزه دفاعی مورد استفاده قرار می‌گیرد، دارای طبقه‌بندی‌های لازم می‌باشد و لازم است که امنیت پیکربندی تأمین گردد. همچنین مدیریت پیکربندی

کارگزاری شبکه ارتباطی دفاعی که بستر اصلی برای زیرساخت ارتباطی کلیه شبکه‌های نیروهای مسلح می‌باشد نیز در این قسمت انجام می‌شود. لازم به ذکر است وجود شبکه امن ارتباطی باعث شده تا دغدغه‌های ارتباطات بین کلیه بخش‌های شرکت‌کننده در محیط رایانش ابری از بین برود و لازم نباشد در این تحقیق به آن پرداخته شود.

دریافت‌کننده خدمات ابری: همان مصرف‌کنندگان خدمات هستند که سرویس‌های دفاعی مورد نیاز را از فراهم‌کنندگان سرویس‌ها دریافت می‌کنند. با توجه به آنکه امنیت سرویس‌ها و امنیت ارتباطات در بخش‌های دیگر تأمین شده این اطمینان خاطر وجود دارد که سرویس‌هایی که به دست مصرف‌کنندگان می‌رسند امن خواهند بود.

رصد و پایش دفاعی: در معماری رایانش ابری حوزه دفاعی لازم است که تمامی حوزه‌های دفاعی مورد رصد و پایش قرار گیرند. در این بخش کلیه رخدادها و تهدیدات مورد بررسی قرار می‌گیرند. خدمات برون‌سپاری نیز باید مورد بررسی دقیق امنیتی قرار گیرند که این حوزه نیز در این بخش انجام می‌شود. همچنین پایداری خدمات و سرویس‌ها که از ملزومات سامانه‌های دفاعی است باید به طور دقیق مورد رصد و پایش قرار گیرد و تضمین پایداری در ارتباطات برقرار شده به وسیلهٔ زیرساخت ارتباطی نیروهای مسلح نیز باید در این قسمت مورد بررسی قرار گیرد.

واسط‌های کاربری و کارگزاری: در معماری رایانش ابری، خدمات و سرویس‌هایی که از طرف فراهم‌کنندگان به مصرف‌کنندگان ارائه می‌شود، از طریق واسط‌ها و کارگزارها صورت می‌گیرد. این خدمات شامل مدیریت سرویس‌ها، مدیریت پایگاه‌های داده و بانک‌های اطلاعاتی، مدیریت شبکه زیرساخت ارتباطی خاص نیروهای مسلح و برون‌سپاری خدمات دفاعی است.

نتیجه‌گیری و پیشنهادها

رایانش ابری یکی از حوزه‌های نوظهور فناوری اطلاعات است. بسیاری از دولت‌های مهاجرت به این فناوری را در برنامه خود قرار داده‌اند. یکی از دلایلی که باعث ترغیب دولت‌ها به استفاده از رایانش ابری شده است، استفاده حداکثری از منابع سیستم‌ها، کاهش هزینه‌ها و یکپارچگی زیرساخت فناوری اطلاعات در کشورها می‌باشد. حوزه نظامی نیز بی‌بهره از این فناوری نیست و کشورهای صاحب فناوری، استفاده حداکثری از رایانش ابری در حوزه‌های نظامی را جزء اهداف اصلی خود تعریف کرده‌اند.

در کشور ما نیز لازم است تا مهاجرت سازمان‌های نظامی با در نظر گرفتن شاخص‌های امنیتی نظیر احراز هویت، دسترس‌پذیری، سطوح دسترسی به خدمات، محرمانگی و حریم خصوصی در دستور کار قرار گیرد و بدون در نظر گرفتن مؤلفه‌های امنیتی مهاجرت به حوزه رایانش ابری به مصلحت نمی‌باشد.

در پاسخ به سؤال تحقیق، دو راهبرد اصلی مهاجرت سازمان‌های دفاعی به محیط رایانش ابری به همراه اقدامات آنها به شرح زیر می‌باشد:

۱- شناسایی وضعیت جاری سازمان‌های دفاعی در حوزه‌های شبکه و زیرساخت، محتوا، کاربران و سامانه‌ها صورت پذیرد؛

۲- الگوی مهاجرت سازمان‌های دفاعی بر اساس در نظر گرفتن شاخص‌های سازمانی و امنیتی تدوین شود. اقدامات این بخش عبارت‌اند از:

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

ب) یکپارچه‌سازی در حوزه‌های زیرساخت و شبکه سازمان‌های نظامی، مراکز داده، اطلاعات و برنامه‌های کاربردی موجود از الزامات مهم در مهاجرت سازمان‌های دفاعی است؛

ج) ایجاد زیرساخت‌های مجازی‌سازی در سطح خدمات از مهم‌ترین الزامات مهاجرت می‌باشد و باید توجه ویژه‌ای در این حوزه به عمل آید؛

د) ایجاد کارگزاری‌های رایانش ابری در سطح سازمان‌های دفاعی برای ارتباط‌دهی فراهم‌کنندگان خدمات و مصرف‌کنندگان خدمات باید مورد توجه قرار گیرد؛

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

و) تغییر فرهنگ سازمانی در جهت مهاجرت به محیط رایانش ابری و تجدیدنظر در رویکردها و سیاست‌هایی که در محیط ابری وجود دارد، به منظور چالاکی و کم شدن هزینه‌های سازمان‌های دفاعی صورت پذیرد؛

ز) مدل به اشتراک‌گذاری ایمن داده‌ها و خدمات در محیط رایانش ابری دفاعی بر اساس کارکردهای سازمان‌های دفاعی به عنوان یک اولویت مهم و اساسی تدوین گردد.

برای ادامه تحقیق و برای کارهای آتی پیشنهاد می‌شود معماری‌های امنیتی ابر دفاعی و نحوه عملکرد و ارتباط میان موجودیت‌های موجود در ابر دفاعی مورد بررسی قرار گیرند.

فهرست منابع

رزمجو، محمدرضا (۱۳۸۶). مدیریت اطلاعات و تأثیر آن بر بنیهٔ دفاعی. *فصلنامه مدیریت نظامی*، ۸(۲۵)، ۲۷-۴۸.

عبدی، فریدون (۱۳۹۰). سامانهٔ فرماندهی و کنترل C5I2 و بررسی نقش رایانه‌ها در آن. *فصلنامه مدیریت نظامی*، ۱۱(۴۲)، ۴۳-۷۰.

مؤسسه آموزشی و تحقیقاتی صنایع دفاعی (۱۳۹۲). *سند زیرساخت فاوای فرماندهی و کنترل*.

نقیان فشارکی، مهدی (۱۳۹۳). ارائه معماری مرجع امنیتی محیط رایانش ابر خصوصی سازمان. *فصلنامه امنیت‌پژوهی*، ۱۳(۴۷)، ۹۱-۱۱۲.

ولوی، محمدرضا و موحدی‌صفت، محمدرضا (۱۳۹۵). ارائه الگوی امن استقرار زیرساخت‌های دفاعی کشور در محیط رایانش ابری. *فصلنامه مطالعات بین‌رشته‌ای راهبردی*، ۷(۲۲)، ۲۹-۴۴.

Ardagna, D. (2015). *Cloud and Multi-cloud Computing: Current Challenges and Future Applications*, IEEE/ACM 7th International Workshop on Principles of Engineering Service-Oriented and Cloud Systems, 1-2.

Cloud Security Alliance (2013). *Cloud Security Alliance, Warns Providers of 'The Notorious Nine' Cloud Computing Top Threats in 2013*, available at: https://cloudsecurityalliance.org/media/news/ca-warns-providers-of-the-notoriousnine-cloud-computing-top-threats-in-2013.

Gellman, R. (2009). *Privacy in the clouds: Risks to privacy and confidentiality*

from cloud computing, The World Privacy Forum. http://www.worldprivacyforum.org/pdf/WPF_Cloud_P rivacy_Report.pdf.

Kumar, N. (2015). Cryptography during Data Sharing and Accessing Over Cloud. *International Transaction of Electrical and Computer Engineers System, 3*(1), 12-18.

Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud computing security issues and challenges. *International Journal of Computer Networks*, *3*, 247-255.

Luo, S., Lin, Z., Chen, X., Yang, Z., & Chen, J. (2011). *Virtualization security for cloud computing services*. In Cloud and Service Computing (CSC), 2011 International Conference on (pp. 174-179). IEEE.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)*, O Reilly Media.

Mazhar, A., Samee, U., Athanasios, V., & Vasilakos, M. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305*, 357-383.

Mell, P., & Grance, T. (2011) *The NIST Definition of Cloud Computing, Recommendation of NIST, Special Publication 800-145*. http://csrc.nist.gov/publications/nistpubs/800-145/SP800- 145.pdf

National Institute of Standards and Technology (2013). NIST *Cloud Computing Security Reference Architecture* (draft), NIST Special Publication 500-299.

Odell, L. A., Wagner, R., & Weir, T. J. (2015). *Department of Defense Use of Commercial Cloud Computing Capabilities and Services*, Institute for Defense Analyses (IDA).

Paul, M. (2013). *NASA'S Progress in Adopting Cloud Computing Technologies*. Office of Inspector General.

Sosinsky, B. (2010). *Cloud computing bible*. John Wiley & Sons.

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

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

Youssef, A., & Alageel, M. (2012). A Framework for A Framework for Secure Cloud ure Cloud ure Cloud Computing Computing Computing, IJCSI *International Journal of Computer Science Issues, 9*(4), 487-500.