فصلنامه مطالعات دفاعی استراتژیک
سال شانزدهم، شماره ۷۳، پاییز ۱۳۹۷
مقاله دوم، از صفحه ۴۶-۲۷

ارائه یک چارچوب معماری امن برای شبکه دفاعی کشور

محمدرضا ولوی[۱]، محمدرضا موحدی صفت[۲]

دریافت مقاله: ۹۶/۰۹/۰۶ پذیرش مقاله: ۹۶/۱۰/۱۵

چکیده

فناوری اطلاعات و ارتباطات در همه ارکان سازمان‌ها دارای تأثیر مستقیم می‌باشد. شبکه‌های حوزه دفاعی در محیط‌های امن شبکه محور، یکی از نوظهورترین حوزه‌های فناوری می‌باشند که باعث شده تا اکثر سازمان‌های دفاعی دنیا این شبکه‌ها را پذیرفته یا در حال برنامه‌ریزی برای ایجاد و استقرار سامانه‌های خود در محیط آن باشند. حوزه دفاعی کشور یکی از زیرساخت‌های حساس و حیاتی کشور است که با استقرار آن در چنین محیطی می‌توان از قابلیت‌هایی نظیر افزایش کارایی، نوآوری و چابکی استفاده کرد. باوجود همه مزایای این شبکه، باید به مسئله امنیت به‌عنوان مهم‌ترین چالش در این محیط توجه ویژه شود. در این تحقیق الگو معماری شبکه دفاعی امن موردنیاز سازمان‌های دفاعی بیان گردیده است. جامعه آماری استفاده‌شده در تحقیق حاضر، استادان و دانشجویان دوره‌های دکتری مدیریت راهبردی فضای سایبر و برخی از مدیران و کارشناسان ارشد حوزه فناوری در نیروهای مسلح می‌باشند. نتایج تحقیق نشان می‌دهد که برای ارتقاء حوزه فناوری در سازمان‌های دفاعی باید یک الگوی معماری امنیتی به‌منظور پذیرش شبکه‌های دفاعی تدوین و مورد بهره‌برداری قرار گیرد. همچنین در نظر گرفتن امنیت در معماری یادشده یک الزام مهم و حیاتی است. در الگوی ارائه‌شده، مؤلفه‌های مختلف امنیت شبکه‌های دفاعی موردبررسی قرار گرفته است.

واژگان کلیدی: فناوری اطلاعات و ارتباطات، امنیت فناوری اطلاعات و ارتباطات، شبکه‌های دفاعی، زیرساخت‌های دفاعی، رایانش ابری.

۱- دانشیار فناوری و اطلاعات دانشگاه صنعتی مالک اشتر valavi@mut.ac.ir
۲- دکتری فناوری و اطلاعات دانشگاه صنعتی مالک اشتر، (نویسنده مسئول) movahedi@sndu.ac.ir

مقدمه

حوزه دفاع همانند بهداشت، ارتباطات، نیرو و اقتصاد، یکی از زیرساخت‌های حیاتی و حساس کشور است و استقرار سامانه‌های دفاعی در یک ساختار شبکه‌محور امن و بومی دفاعی می‌تواند مزیت‌های زیادی مانند چابکی[1] و نوآوری[2] را به ارمغان آورد. استفاده از شبکه دفاعی امن و اختصاصی برای نهادهای دفاعی ضمن آنکه استفاده از سامانه‌های مشترک در محیط شبکه را بین بخش‌های مختلف دفاعی امکان‌پذیر می‌سازد، هزینه‌ها را کاهش داده و افزایش بهره‌وری را به دنبال خواهد داشت. امروزه بسیاری از کشورها، ساختارهای دفاعی خود را بر روی شبکه‌های دفاعی که عمدتاً بر روی محیط رایانش ابری هستند مستقر کرده‌اند (تاکایی، ۲۰۱۲: ۴۳–۱) . با توجه به اهمیت بسیار ویژه شبکه‌های دفاعی و سامانه‌های امنی که بر روی این شبکه‌ها مستقر هستند، لازم است که اصول امنیتی با بالاترین اولویت در آن‌ها لحاظ گردد؛ زیرا قرارگرفتن سامانه‌های دفاعی در محیط‌های شبکه‌محور درصورتی‌که امنیت آن‌ها تأمین نشده باشد، می‌تواند حتی باعث بروز مخاطرات در امنیت ملی یک کشور گردد.

استفاده از شبکه‌های دفاعی امن، فرصت جدیدی را برای ارائه‌دهندگان و کاربران خدمات در محیط شبکه فراهم می‌سازد تا بتوانند به‌صورت بلادرنگ و بر اساس تقاضا به منابع اشتراکی دسترسی داشته باشند. سازمان‌های دفاعی و همچنین سازمان‌های غیردفاعی می‌توانند به‌عنوان بهره‌برداران این نوع شبکه‌ها باشند و باقابلیت بهتری به منابع دسترسی خواهند داشت. (رایان، ۲۰۱۵). بنابراین حرکت به سمت استقرار زیرساخت‌ها و سامانه‌های دفاعی بر روی محیط‌های شبکه‌محور بومی و امن دفاعی، ضمن آنکه باعث کاهش هزینه‌ها می‌شود، به مدیریت منسجم، یکپارچگی در اطلاعات و چابک‌سازی سازمان‌های دفاعی می‌انجامد.

یک شبکه امن و اختصاصی حوزه دفاعی به ترکیبی از زیرساخت‌ها نظیر مراکز داده[3]، تجهیزات و سخت‌افزارها، سامانه‌ها و نرم‌افزارهای مورداستفاده سازمان‌های دفاعی اطلاق می‌گردد (چونگ و همکاران، ۲۰۱۵: ۱۱–۴)

تحقیق حاضر به بررسی ویژگی‌ها و مؤلفه‌های امنیتی تأثیرگذار در معماری شبکه دفاعی پرداخته و درنهایت یک چارچوب معماری امن بر اساس استانداردهای موجود برای این نوع شبکه‌ها ارائه

1- Agility
2- Innovation
3- Data Center

کرده است. همچنین هر یک از مؤلفه‌های تأثیرگذار در معماری موردبررسی قرارگرفته‌اند. استفاده از نظرات خبرگان حوزه سایبری که در قالب پرسشنامه و مصاحبه صورت گرفته، این امکان را برای مؤلفان به وجود آورده که جایگاه هر یک از مؤلفه‌ها را در معماری به‌صورت دقیق مشخص نمایند. همه خبرگان بر مؤلفه امنیت تأکید نموده و ایجاد یک لایه به نام امنیت در معماری را مورد تائید قرار داده‌اند که این مسئله در معماری به‌طور کامل لحاظ شده است.

مبانی نظری

الف ـ پیشینه تحقیق:

در حال حاضر معماری‌های زیادی برای شبکه‌های سازمان‌های دفاعی مبتنی بر امنیت و کارایی طراحی و مورداستفاده قرار گرفته است. اما باید توجه داشت که سازمان‌های دفاعی هر کشوری دارای مقتضیات خاص و بومی هستند که بر اساس آن مؤلفه‌های تأثیرگذار بر معماری متفاوت خواهند شد. لذا لازم است که برای نهادهای دفاعی کشور یک چارچوب معماری خاص طراحی شود. در حال حاضر اگرچه برای شبکه‌های دفاعی معماری‌هایی نظیر C_4ISR ۱ ارائه‌شده اما متأسفانه این معماری تاکنون نتوانسته به‌صورت دقیق در کشور پیاده‌سازی گردد. در تحقیق حاضر سعی شده بر اساس معماری‌های امنیتی استانداردی که در دنیا تعریف شده، چارچوب معماری بومی امن ارائه گردد. ایجاد شرایطی که این معماری بتواند در محیط‌های رایانش ابری واقع گردد نیز از اهداف این تحقیق است. یکی از این استانداردها توسط موسسه ملی استاندارد و فناوری۲ در آمریکا ارائه شده که مورداستفاده محققین نیز قرار گرفته است. در این تحقیق توجه به مؤلفه‌هایی نظیر تعیین ویژگی‌های بازیگران در محیط شبکه دفاعی و نحوه تعامل آن‌ها با یکدیگر در محیط‌های توزیع‌پذیر۳، مقیاس‌پذیر۴ و تحریک‌پذیر و در نظر گرفتن اصل یکپارچگی در ایجاد پایگاه‌های داده دفاعی پرداخته شده است.

ایجاد هماهنگی بین همه زیرساخت‌های دفاعی که در سازمان‌های مختلف دفاعی کشور مستقر هستند، از اهمیت بالایی برخوردار است و نباید از روش‌های سنتی برای این منظور استفاده شود. وجود شبکه‌های دفاعی امن و اختصاصی در حوزه‌های دفاعی در بسیاری از کشورها توانسته به

1- Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
2- NIST – National Institute of Standard and Technology
3- Distributed Environment
4 - Scalable

یکپارچه‌سازی خدمات و سرویس‌ها کمک نماید و بهره‌وری زیرساخت‌های دفاعی را تا حد ممکن افزایش دهد. متأسفانه در حال حاضر اکثر سامانه‌های موجود در سازمان‌های دفاعی در کشور به‌صورت جزیره‌ای تولید و مورداستفاده قرار می‌گیرند که این مسئله به افزونگی و تکرار سامانه‌ها نیز می‌انجامد. ایجاد شبکه دفاعی می‌تواند با ایجاد هم‌افزایی بین سامانه‌های تولیدشده در نهادهای مختلف، ارتباط مناسب و امنی را نیز برای به‌کارگیری این سامانه‌ها به وجود آورد. لذا وجود یک سامانه یکپارچه که بتواند باعث افزایش قابلیت دسترسی‌پذیری۱، کارایی۲، توسعه‌پذیری۳ و کاهش هزینه شود برای حوزه دفاعی کشور لازم و حیاتی است. ایجاد این شبکه دفاعی اگر مبتنی بر حوزه رایانش ابری نیز باشد، می‌تواند جایگزین مناسبی برای محیط‌های قدیمی گردد. اما باید در نظر داشت که با پیشرفت همه‌جانبه‌ی این نوع شبکه‌ها، مشکلات امنیتی جدیدی نیز به وجود می‌آید. گسترش شبکه‌های دفاعی باعث می‌شود نهادهای دفاعی بیش‌ازپیش تحت تأثیر عوامل خارجی و تهدیدات قرار گیرند (تائویو و همکاران، ۲۰۱۳: ۱۴۲۰–۱۴۱۷).

ایجاد چارچوب معماری بومی اختصاصی و امن برای شبکه دفاعی کشور بر اساس مقتضیات خاص دفاعی و لزوم بهره‌برداری حداکثری از ظرفیت سامانه‌ها در محیط شبکه محور و با در نظر گرفتن شاخص‌های امنیتی انجام می‌گیرد. در مدل‌های استاندارد موجود کمتر به حوزه کنترل، رصد و پایش پرداخته شده و بیشتر به استفاده از فضای اشتراکی سرویس‌ها در محیط‌های شبکه‌محور تأکید شده است؛ اما در مدل ارائه‌شده در این تحقیق، اهمیت امنیت سرویس‌ها، حفاظت از داده‌ها، کنترل دسترسی‌ها۴ و در نظر گرفتن سیاست‌های دفاعی به‌عنوان مهم‌ترین شاخص‌های الگوی بومی در نظر گرفته شده است. طراحی لایه امنیت در معماری شبکه دفاعی بر اساس‌های شاخص‌های ارائه‌شده، از دیگر دلایل اهمیت موضوع و ضرورت انجام این پژوهش است.

تحقیقات انجام‌شده بیانگر آن است که تاکنون روشی جهت استقرار زیرساخت‌های دفاعی کشور در یک محیط شبکه‌محور مبتنی بر رایانش ابری که متضمن ایجاد امنیت لازم نیز باشد انجام‌نشده است و معماری‌های موجود اگرچه برای سازمان‌های تجاری کافی به نظر می‌رسند اما پاسخگوی مهاجرت سازمان‌های دفاعی به این شبکه‌های امن نیستند و لازم است یک معماری امنیتی برای

1- Accessibility
2- Performance
3 - Extensibility
4 - Access Control

این منظور طراحی و ارائه گردد. همچنین معماری C_4ISR به دلیل عدم‌حمایت نهادهای دفاعی و ضعف در پیاده‌سازی نتوانسته مطالبات موردنظر نهادهای دفاعی کشور را برآورده نماید.

با توجه به حساس بودن مراکز دفاعی کشور، تهدیدات امنیتی می‌تواند تمام منافع ورود به شبکه‌های دفاعی را از بین برده و نتایج جبران‌ناپذیری را برای این مراکز به وجود آورد. اتحادیه امنیت پردازش ابری[1] دستورالعمل‌هایی را برای بهبود امنیت در شبکه‌ها ارائه نموده است که اگر این دستورالعمل‌های بین‌المللی با سیاست‌های امنیتی حوزه دفاعی کشور ادغام شوند، می‌توانند تبدیل به یک راهکار امنیتی مناسب برای ایجاد زیرساخت شبکه حوزه دفاعی گردند (آرفین و همکاران، ۲۰۱۵: ۳۰۶-۲۹۹).

چارچوب معماری امن بومی برای شبکه دفاعی کشور دارای چه شاخص‌ها و چه ویژگی‌هایی است؟

هدف از این تحقیق، ارائه یک چارچوب معماری امنیتی برای استقرار سامانه‌های دفاعی در محیط شبکه محور (شبکه دفاعی) است.

ایجاد معماری شبکه دفاعی امن، بومی و اختصاصی برای نهادهای دفاعی یک الزام می‌باشد.

امنیت همواره به‌عنوان مهم‌ترین دغدغه در محیط شبکه‌های دفاعی است و امروزه این موضوع به یک چالش اساسی تبدیل شده است. مزیت‌های زیادی ایجاد شبکه دفاعی امن و اختصاصی برای نهادهای دفاعی، این سازمان‌ها را به سمت ایجاد و استفاده از آن‌ها هدایت کرده است. مهم‌ترین پژوهش‌های انجام‌شده در ارتباط با موضوع این تحقیق عبارت‌اند از:

مهدی نقیان فشارکی در تحقیقی معماری مرجع امنیتی برای سازمان‌هایی که خواستار پیوستن به محیط‌های شبکه محور هستند را موردبررسی قرار داده است. در این مقاله به شناخت سازمان و مهندسی نیازمندی‌های امنیتی سازمان، ترسیم معماری سطح بالای سازمان، نحوه نگاشت مؤلفه‌های امنیتی با بازیگران محیط شبکه و الگوهای پیاده‌سازی آن، تدوین الگوی رسمی معماری مرجع امنیتی و درنهایت به ارزیابی معماری مرجع امنیتی اشاره شده است (نقیان فشارکی، ۱، ۱۳۹۳).

مرکز فناوری اطلاعات وزارت دفاع[2] در جهت شناسایی فرصت‌ها و مزیت‌هایی که در قبال استفاده از شبکه‌های دفاعی مبتنی بر رایانش ابری هستند، برنامه‌ریزی‌هایی را انجام داده تا بتواند وزارت

1- Cloud Security Alliance (CSA)
2- CIO (Chief Information Officer)

دفاع آمریکا را از یک حالت تکراری، پرزحمت، طاقت‌فرسا و پرهزینه به یک مجموعه چابک، امن و کم‌هزینه تبدیل کند. در این خصوص پروژه‌ای برای ایجاد یک شبکه خصوصی برای وزارت دفاع آمریکا با قابلیت‌های گفته‌شده در حال اجرا می‌باشد. هدف اصلی از محیط شبکه محور در وزارت دفاع آمریکا پشتیبانی از مأموریت سازمانی در هر جا و در هر زمان و بر روی هر وسیله دارای هویت در وزارت دفاع است. (تاکایی، ۲۰۱۲: ۴۳-۱)

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 شبکه محور فراهم کند. پروژه اپن استاک۱ به‌عنوان بزرگ‌ترین محصول این شرکت می‌باشد (استوارت،۲۰۱۱).

ولوی و موحدی صفت در مقاله‌ای یک معماری امن برای استقرار زیرساخت‌های دفاعی ارائه کرده‌اند. در این معماری امنیت به‌عنوان شاخص اصلی موردبررسی قرار گرفته است (ولوی و همکاران، ۱۳۹۴).

امروزه در پیشبرد بسیاری از امور دفاعی و نظارتی از شبکه‌های حسگر بی‌سیم استفاده می‌شود. امنیت در چنین شبکه‌ای نیز می‌بایست تأمین گردد. در همین راستا در مقاله (جون وو و همکاران، ۲۰۱۶: ۴۲۴-۴۱۶) نویسنده به بررسی شبکه‌های حسگر بی‌سیم در محیط‌های هوشمند مانند شهر هوشمند پرداخته است. علاوه بر آن، یک چارچوب سلسله‌مراتبی به‌منظور افزایش امنیت در شبکه‌های حسگر نیز در این مقاله پیشنهاد شده است. چارچوب امنیتی پیشنهادی در کنار افزایش امنیت در شبکه‌های حسگر بی‌سیم توانسته از پیچیدگی پیاده‌سازی آن بکاهد.

ب ــ مفهوم شناسی :

اگرچه ایجاد یک شبکه دفاعی دارای مزایای بسیاری برای سازمان‌های دفاعی هست که مهم‌ترین آن استفاده از منابع اشتراکی در یک محیط شبکه محور است، اما چالش‌ها و تهدیداتی نیز در این خصوص وجود دارد که به‌کارگیری کامل آن را برای سازمان‌های دفاعی با مشکلات جدی مواجه می‌کند. توسعه این نوع شبکه‌ها ممکن است بر اساس محدودیت‌هایی که سازمان‌های ارائه‌دهنده دارند، سطحی از عدم اطمینان را به وجود آورد و سازمان در مواردی با محدودیت منابع روبرو شود (کویورا۲ و همکاران، ۲۰۱۱: ۲۴۷). به‌طورکلی چالش‌هایی که در اثر ایجاد شبکه‌های دفاعی به وجود می‌آیند به حوزه‌های زیر تقسیم می‌شوند:

1- Open Stack
2- Kuyoro

امنیت و حریم خصوصی : امنیت[1] و حریم خصوصی[2]، به‌عنوان دو تهدید اصلی در ایجاد شبکه‌های دفاعی هستند. برای رفع این تهدیدات لازم است تا از روش‌هایی نظیر رمزنگاری و یا استفاده از تجهیزات و سامانه‌های امنیتی استفاده شود. (ویدیالکشمی، ۲۰۱۴: ۴۶۳-۴۵۶).

قابلیت اعتماد[3] : شبکه دفاعی باید دارای قابلیت اعتماد باشد تا بتواند برای استقرار تجهیزات و سامانه‌ها در شرایط خاص و بحرانی مورداستفاده سازمان‌های دفاعی واقع گردد. ازآنجاکه سرویس‌های ارائه‌شده در سازمان‌های دفاعی دارای طبقه‌بندی اطلاعاتی می‌باشند، لازم است که زیرساخت ارتباطی نیز دارای این قابلیت باشد که اطلاعات در آن نشت پیدا نکند. (سان، ۲۰۱۱: ۵۲-۲۸)

دسترس‌پذیری[4] : یکی از مهم‌ترین مؤلفه‌های شبکه دفاعی، قابلیت دسترسی بالا است. از آنجایی فعالیت‌های موجود در شبکه دفاعی می‌تواند بسیار بحرانی و دارای نقطه پایان زودهنگام باشد، لازم است سیستم‌ها به‌طور یکنواخت فعال بوده و قابلیت پاسخگویی به نیازهای کاربران را داشته باشند (مظهر، ۲۰۱۵: ۳۵۷).

قابلیت همکاری : سامانه‌های دفاعی مستقر بر روی یک شبکه دفاعی باید قادر باشند تا خدمات مربوطه را با یکدیگر ترکیب نمایند. این عمل از طریق خدمات مبتنی بر وب امکان‌پذیر می‌باشد اما تولید این‌گونه خدمات وب، پیچیده و نیاز به متخصصان این حوزه دارد (ماجک، ۲۰۱۵: ۶-۱)

قابلیت حمل[5] : با توجه به آنکه لازم است برنامه‌های تولیدشده در محیط شبکه دفاعی از یک سرویس‌دهنده خاص خدمات به سرویس‌دهنده دیگری منتقل شوند، لازم است در این خصوص سیاست‌های مناسبی برای بهبود این امر اتخاذ گردد. در این صورت سامانه‌های کاربردی می‌تواند به‌راحتی از یک سرویس‌دهنده به سرویس‌دهنده دیگری منتقل شوند. این مشکل تاکنون به‌طور کامل حل نشده است زیرا هریک از سرویس‌دهندگان خدمات شبکه‌های دفاعی، از روش‌های متفاوتی برای زیرساخت‌هایشان استفاده می‌کنند (هاردمن، ۲۰۱۳: ۱۱۸-۱۱۷).

1- security
2- privacy
3- reliability
4- availability
5- Portability

روش‌شناسی

شبکه دفاعی: بسیاری از سازمان‌های دفاعی در دنیا اصل ایجاد یک شبکه امن و اختصاصی حوزه دفاعی را پذیرفته‌اند و بسیاری از امور دفاعی مخصوصاً زیرساخت‌های دفاعی و حساس خود را بر روی این شبکه‌ها مستقر کرده‌اند. ویژگی‌های مهم شبکه‌های دفاعی در بخش قبل موردبررسی قرار گرفت. در این تحقیق به‌منظور ایجاد ساختار جامع و یکپارچه برای کلیه سرویس‌ها و تجهیزات موجود در سازمان‌های دفاعی، یک معماری امن برای شبکه دفاعی پیشنهاد شده است. در این معماری بر اساس ملاحظات خاص دفاعی، مؤلفه‌های امنیتی ویژه‌ای نیز در نظر گرفته شده است.

شبکه دفاعی متشکل از یک زیرساخت یکپارچه و توزیع شده[1] است که این امکان را برای ارتباط امن تمامی مراکز نظامی و دفاعی کشور با یکدیگر مهیا می‌سازد. این شبکه با توجه به قابلیت‌هایی نظیر استفاده اشتراکی از منابع، در دسترس‌پذیر بودن خدمات در شرایط بحرانی، قابلیت اعتماد و چابکی و همچنین به دلیل استقرار در یک جغرافیای گسترده در کشور و داشتن اطلاعات طبقه‌بندی‌شده، باید در زیرساخت‌های رایانشی نظیر رایانش ابری مستقر گردد و کلیه ویژگی‌های معماری C_4ISR را نیز دارا باشد. جدول ۱ فواید استفاده از شبکه‌های امن و اختصاصی حوزه دفاعی را در سه ویژگی چابکی، نوآوری و بهره‌وری نمایش می‌دهد.

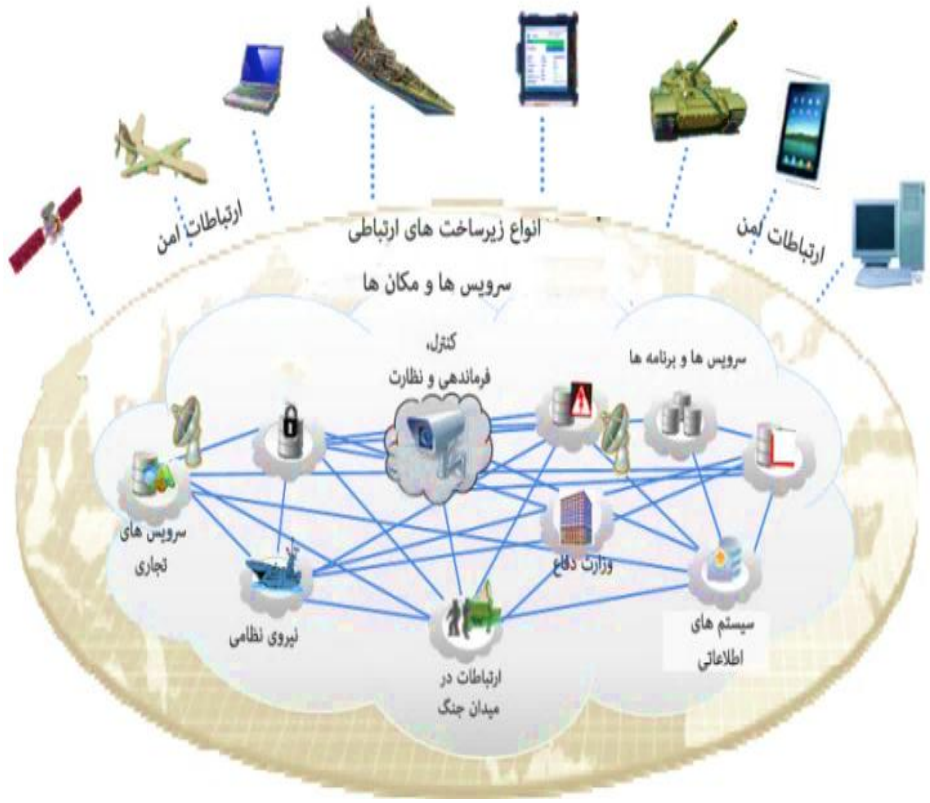
با توجه به جدول ۱ مشاهده می‌شود که ایجاد شبکه‌های امن و یکپارچه دفاعی می‌تواند سازمان‌ها را به‌سوی افزایش انعطاف‌پذیری پیش برده و انجام کارها را آسان نماید. بااین‌وجود استقرار سامانه‌های دفاعی بر روی شبکه دفاعی و حرکت از سمت سیستم‌های سنتی قدیمی به‌سوی خدمات شبکه محور، چالش‌های جدیدی را به وجود آورده است. سازمان‌های دفاعی باید در ابتدا مؤلفه‌ها و زیرساخت‌های لازم برای استقرار به محیط شبکه محور را شناسایی و سپس اقدام به مهاجرت بر روی این‌گونه شبکه‌ها کنند.

1- Distributed

جدول ۱: فواید استفاده از شبکه دفاعی امن و اختصاصی برای سازمان‌های دفاعی

بهره‌وری	
استفاده از شبکه دفاعی امن و اختصاصی	شرایط فعلی (عدم وجود شبکه دفاعی)
استفاده حداکثری از دارایی‌ها و منابع تجمیع منابع و ایجاد یکپارچگی افزایش سرعت توسعه برنامه‌ها و زیرساخت‌ها	استفاده محدود و کم از دارایی‌ها مستقل بودن سیستم‌ها از یکدیگر دشواری مدیریت سیستم‌ها
چابکی	
استفاده از شبکه دفاعی امن و اختصاصی	شرایط فعلی (عدم وجود شبکه دفاعی)
پاسخگویی سریع به درخواست‌ها عدم افزونگی و جلوگیری از امور تکراری افزایش و کاهش سریع ظرفیت‌ها در بخش‌های دفاعی	زمان زیاد برای ایجاد مراکز داده پیچیدگی در افزایش ظرفیت‌ها انجام درخواست‌های تکراری
نوآوری	
استفاده از شبکه دفاعی امن و اختصاصی	شرایط فعلی (عدم وجود شبکه دفاعی)
تغییر از مالکیت سرویس‌ها به مدیریت سرویس‌ها پذیرش آسان فناوری‌های نوظهور	مالکیت دارایی‌ها و سرویس‌ها انجام امور تکراری

در یک محیط مبتنی بر شبکه امن دفاعی، به سازمان‌های دفاعی و غیر دفاعی اجازه داده می‌شود تا در یک محیط یکپارچه با یکدیگر در ارتباط بوده و منابع موجود را به‌صورت اشتراکی استفاده نمایند. شکل ۱ تصویری منطقی از یک ساختار دفاعی شبکه محور مبتنی بر رایانش ابری را نمایش می‌دهد. این محیط شبکه محور قادر است تا با یکپارچه کردن بسترها و زیرساخت‌ها، سازمان‌های دفاعی و حوزه‌های تابعه را با یکدیگر هماهنگ نماید.



شکل ۱: تصویری از یک شبکه دفاعی یکپارچه بین سازمان‌های دفاعی مختلف

چالش‌های امنیتی برای ورود سازمان‌های دفاعی به محیط شبکه دفاعی: سازمان‌های دفاعی در هنگام ورود به محیط رایانش ابری با چالش‌ها و تهدیداتی مواجه است که مهم‌ترین این چالش‌ها عبارت‌اند از: (ساندرز، ۲۰۱۳)

–دسترسی‌های غیرمجاز (از طریق احراز هویت نامناسب و یا بدون مجوز و آسیب‌رسانی به نرم‌افزارها، اطلاعات و منابع در حال استفاده)

–عدم تضمین محرمانگی اطلاعات که باید از طرف ارائه‌کنندگان خدمات شبکه انجام پذیرد

–افزایش سطح حملات مبتنی بر شبکه مانند حملات انکار سرویس

–مشکلات موجود در رمز کردن داده‌ها در یک محیط چند اجاره‌ای[1]

–محدودیت‌های حمل ناشی از رابط‌های برنامه‌نویسی نرم‌افزاری غیراستاندارد

1- Multi tenancy

–وجود حملات مبتنی بر استفاده از ماشین‌های مجازی[1]
–نبود حفاظت از مرورگرهای اینترنت از حملات برای کاهش آسیب‌پذیری‌های امنیتی کاربر نهایی
–عدم اعتماد در حفاظت از داده‌های سازمان‌ها از دسترسی‌های غیرمجاز
–افشا، اصلاح و یا نظارت و همچنین عدم جلوگیری از دسترسی غیرمجاز به منابع زیرساخت شبکه‌ای

برای ورود سازمان‌های دفاعی به محیط شبکه دفاعی امن و اختصاصی دفاعی باید به فن‌آوری‌های کنترل دسترسی و تشخیص نفوذ در ارائه‌دهندگان سرویس‌های ابری نیز توجه شود.

زیرساخت ارتباطی: از دیگر ملزومات موجود در ایجاد، توسعه و استفاده از محیط شبکه دفاعی، وجود ارتباطات میان تولیدکنندگان و مصرف‌کنندگان خدمات است. درواقع یک زیرساخت ارتباطی امن و اختصاصی میان موجودیت‌های موجود در شبکه دفاعی باید طراحی و ایجاد شود. بدیهی است با توجه به اهمیت امنیت در ایجاد شبکه دفاعی، طراحی و ایجاد زیرساخت‌های ارتباطی چالش‌برانگیز است و استفاده از ارتباطات موجود در شرکت مخابرات به دلیل لحاظ نکردن بسیاری از تمهیدات امنیتی نمی‌تواند به‌عنوان یک راه‌حل مناسب مورداستفاده قرار گیرد. زیرساخت ارتباطی باید ایمن، چابک، دارای قدرت تحمل‌پذیری خطای بالا و دارای پهنای باند مناسب و پویا باشد تا بتواند پهنای باند لازم را در اختیار کاربران و سرویس‌ها قرار دهد(کاراباکاک، ۲۰۱۶: ۵۳۹–۵۲۶).

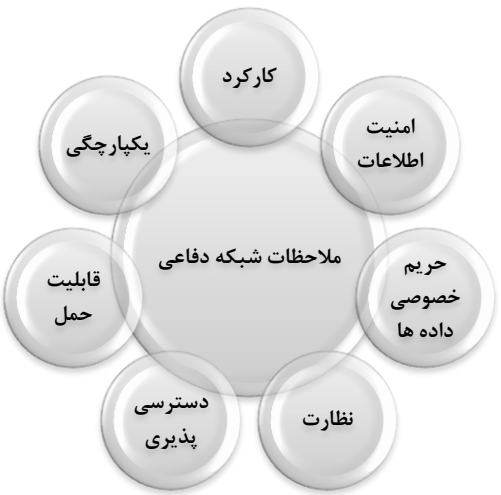
با توجه به وجود هزاران پایگاه اطلاعاتی و عملیاتی هوایی، دریایی و زمینی ثابت و سیّار در سطح کشور، زیرساخت ارتباطی شبکه دفاعی باید بسیار انعطاف‌پذیر، در دسترس و قابل مدیریت باشد. زیرساخت ارتباطی شبکه دفاعی باید در نقاط حساس مانند صحنه نبرد دارای ویژگی‌های خاصی نظیر انتقال حجم بسیار زیاد داده‌ها در کسری از زمان، قابلیت دسترسی سراسری، تحویل مطمئن اطلاعات، ایجاد ارتباطات سیار و توانایی گسترده شدن پویا را داشته باشد. 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 به ایجاد دسترسی‌پذیری بالا می‌انجامد (جوشی، ۲۰۱۶: ۱۴–۶).

1- Virtual Machines

ملاحظات مطرح در شبکه دفاعی: محیط‌های اشتراکی که در اثر استفاده از شبکه‌های دفاعی به وجود می‌آید، منشأ ایجاد بسیاری از چالش‌ها و تهدیدات هستند. در یک محیط اشتراکی چندین کاربر از یک سامانه مشترک استفاده می‌کنند. این سامانه‌ها دارای منابع اشتراکی بوده و مسائل مربوط به تخصیص و مدیریت منابع در چنین محیطی حائز اهمیت خواهد بود. به‌علاوه، ارتباط‌های موجود میان این نوع سامانه‌ها با یکدیگر و یا با مصرف‌کنندگان خدمات دفاعی می‌تواند مستلزم ایجاد تهدیدات امنیتی و یا کاهش قابلیت دسترسی گردد. اگرچه مسائل مربوط به جداسازی کارکردها همیشه در یک شبکه دفاعی مطرح است، اما این چالش به‌طور کامل برطرف نگردیده است (مارکن، ۲۰۱۳: ۹-۱).

همچنین مجازی‌سازی به‌عنوان اصلی‌ترین محور در ایجاد و استقرار شبکه دفاعی مطرح می‌گردد. اگرچه مجازی‌سازی توانسته قابلیت استفاده از منابع سامانه‌ها را از طریق ارائه یک سامانه به چندین کاربر افزایش دهد، اما باعث بروز مشکلات جدیدی نیز گردیده است.

در این خصوص ایجاد یک شبکه دفاعی امن و یکپارچه دارای ملاحظاتی وجود دارد که مستلزم به‌کارگیری متخصصان این حوزه است و برای ایجاد چنین شبکه‌ای لازم است متخصصان این حوزه توجه کافی را نسبت به جنبه‌های مختلف ایجاد این شبکه داشته باشند. همان‌طور که در شکل ۲ نشان داده شده است، مسائل حائز اهمیت در شبکه دفاعی در هفت حوزه مطرح می‌شوند (واکا، ۲۰۱۳):



شکل ۲: ویژگی‌های مهم شبکه‌های دفاعی

ازآنجاکه محیط شبکه دفاعی اشتراکی است بنابراین باید به مسئله رقابت میان کاربران برای استفاده از منابع توجه داشت. چه‌بسا براثر استفاده بیش‌ازحد از منابع موجود در یک بخش از شبکه، عملکرد آن منبع کاهش یافته و باعث اختلال در عملکرد شبکه دفاعی شود. فرض کنید در هنگام انجام یک عملیات گسترده که لازم است داده‌های بسیار زیادی به‌یک‌باره تبادل شوند، از منابع بسیاری استفاده شود که به انفجار داده‌ها منجر گردد. بااین‌وجود، اگر داده‌ها به‌سرعت نتوانند منتقل شوند باعث بروز مشکلات فراوانی خواهند شد. این مسئله در شبکه دفاعی می‌تواند به یک بحران تبدیل شود درحالی‌که در شبکه‌های معمولی شاید به‌مراتب کم‌هزینه‌تر بوده و تنها ارائه‌دهنده‌ی خدمات لازم است تا جریمه‌ای را بر اساس قرارداد سطح سرویس به کاربر بپردازد.

یکی دیگر از محوری‌ترین مؤلفه‌هایی که لازم است در محیط شبکه دفاعی در نظر گرفته شود، نظارت بر مکان قرارگیری داده‌ها، عملکرد سیستم و کیفیت سرویس‌ها است.

تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق

تحقیق حاضر به دنبال ارائه یک الگو برای معماری امنیتی به‌منظور استقرار سامانه‌های دفاعی در محیط شبکه محور است. در این خصوص پس از دریافت نظرات خبرگان شرکت‌کننده در این تحقیق و انجام مصاحبه‌های متعدد، مهم‌ترین اقداماتی که باید در این راستا انجام پذیرد به شرح زیر عنوان می‌گردد:

۱. لایه امنیت به‌عنوان لایه اصلی در زیرساخت معماری شبکه دفاعی به‌گونه‌ای طراحی شود که همه لایه‌های موجود شبکه و ارتباطات بین آن‌ها بر روی این لایه خاص و مهم قرار گیرد. این لایه باید بر روی همه لایه‌ها و سرویس‌های موجود اشراف داشته باشد.

۲. سازمان‌های دفاعی برای استفاده شبکه دفاعی باید از یک شبکه خصوصی دفاعی امن و یکپارچه استفاده کنند و معماری لازم بر اساس استانداردها و نیازهای بومی طراحی و بکار گرفته شود. توجه به امنیت در ساختار این شبکه‌ها دفاعی حائز اهمیت است و باید کلیه سرویس‌ها و خدمات حوزه دفاعی بین نهادهای دفاعی در این شبکه تعریف گردند.

۳. ساختار شبکه حوزه دفاعی باید همه ارکان اصلی نهادهای دفاعی را شامل شود تا بتواند از ظرفیت‌های تعاملی و فضاهای اشتراکی برای انجام عملیات مشترک دفاعی استفاده کند. بازیگران اصلی در این شبکه شامل ارائه‌دهندگان سرویس‌های دفاعی، کاربران خدمات و ناظران شبکه می‌باشند.

۴. تعیین روش‌های احراز هویت، اطمینان از نگهداری امن کلان داده‌ها و تعیین سیاست‌های استفاده از رمزنگارها، دیواره‌های آتش و سامانه‌های تشخیص نفوذ در محیط شبکه دفاعی از اهمیت بسیار بالایی برخوردار است و لازم است که سیاست‌های لازم در این خصوص تدوین و ابلاغ گردد.

۵. تعامل‌پذیری بین سازمان‌های دفاعی در حوزه‌های اطلاعات، سامانه‌ها و خدمات توسط شبکه دفاعی به وجود می‌آید و سازمان‌های دفاعی کشور می‌توانند به‌صورت دائم و پویا با یکدیگر هماهنگ و در ارتباط باشند. در نظر بگیرید نیروهای هوایی و دریایی هرکدام دارای یک شبکه دفاعی اختصاصی بوده و هر دونیرو به شبکه دفاعی کشور که در سطح بالاتر قرار دارد، متصل باشند. در این حالت می‌توان هماهنگی‌های لازم و اجرای دستورات به نیروی هوایی را در زمان مانور نیروی دریایی صادر نمود. وجود تعاملات بین نهادهای دفاعی در شبکه دفاعی کشور این فرصت را به فرماندهان رده‌بالا و تصمیم گیر سازمان‌ها می‌دهد تا بتوانند بر سایر بخش‌های سازمان خود اشراف اطلاعاتی داشته باشند.

۶. یکی از قابلیت‌های سازمان‌های دفاعی که در محیط شبکه‌محور به وجود می‌آید، چابکی است که بخشی از این مسئله در اثر کوچک‌سازی سازمانی ایجاد می‌شود که از مزیت‌های ایجاد شبکه است.

۷. تعامل بانک‌های اطلاعاتی و پایگاه‌های داده مربوط به سازمان‌های دفاعی و ایجاد یک بانک اطلاعاتی جامع یکپارچه دفاعی می‌تواند به مسئله هماهنگی بین نیروهای دفاعی بیانجامد. این مسئله در خصوص اطلاعات راهبردی از اهمیت بیشتری برخوردار است.

۸. وجود شبکه اختصاصی امن دفاعی با محدودیت‌ها و سطوح خاص دسترسی که بر روی‌داده‌ها و سامانه‌های آن تعریف می‌شود، به افزایش قابلیت محرمانگی در اطلاعات منجر می‌شود. برای افزایش محرمانگی در اطلاعات حوزه دفاع، علاوه بر آنکه باید از روش‌های فنی محرمانگی مانند رمزنگاری استفاده شود باید نحوه تعامل نهادهای دفاعی، ممیزی‌ها، رصد و پایش اطلاعات در شبکه دفاعی به‌گونه‌ای تعریف شود تا به حداکثر امنیت در دسترسی به اطلاعات منجر شود.

معماری امنیت در شبکه حوزه دفاعی : در استقرار شبکه دفاعی در کشور ضمن توجه به مدل‌های مرجع و استاندارد، باید به مؤلفه‌هایی نظیر نحوه تعامل بازیگران در محیط رایانش ابری

حوزه دفاعی، اصل مقیاس‌پذیری[1]، اصل یکپارچگی، تداوم سرویس‌ها در زمان رفتن از وضعیت فعلی به وضعیت کامل استقرار شبکه دفاعی، در نظر گرفتن مؤلفه‌های خاص بومی (مانند مؤلفه فرهنگی و جغرافیایی) و در نظر گرفتن سطوح دسترسی و محرمانگی توجه کامل شود. وجود موانع فنی و امنیتی همانند درخواست یک نیازمندی سخت و پیچیده امنیتی از یک زیرساخت، ممکن است استفاده از شبکه دفاعی را در زمان‌های بحرانی با چالش‌های جدی مواجه کند(لی، ۲۰۱۵: ۱۵۰-۱۳۲). مشکل مهم در این زمینه، مطلوب نبودن امنیت سرویس‌های شبکه دفاعی است. ضمن آنکه راهکارهای سنتی امنیتی هم در این حوزه پاسخ‌گو نمی‌باشند. بنابراین قوانین جدیدی در حوزه حملات و دفاع سایبری با استفاده از سرویس‌های شبکه محور به تصویب سازمان‌های دفاعی رسیده است.

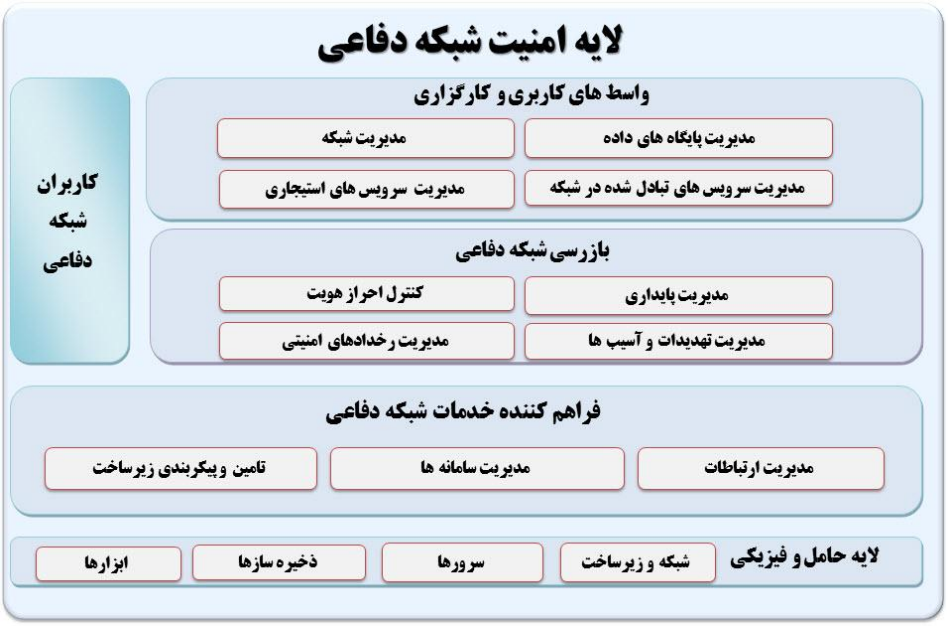
بر اساس موارد بیان‌شده و دریافت نظرات خبرگان حوزه دفاعی که در این تحقیق شرکت کرده‌اند، الگوی امنیت برای معماری شبکه به‌صورت شکل ۳ نمایش داده شده است. اجزاء این شکل به‌صورت زیر تعریف شده‌اند:

لایه تجهیزات: در این قسمت تجهیزات و زیرساخت‌های به‌کاررفته در شبکه دفاعی مستقر هستند. بدیهی است امنیت این تجهیزات قبل از به‌کارگیری باید احرازشده باشد و حتی‌الامکان از تجهیزات ساخت داخل کشور استفاده شود.

منابع مجازی شده: مجازی‌سازی یکی از ارکان اصلی محیط‌های شبکه محور می‌باشد که باعث بهره‌وری حداکثری از منابع و صرفه‌جویی در به‌کارگیری از تجهیزات می‌گردد. مجازی‌سازی در سطح سرورها و ذخیره‌سازها به افزایش توان مدیریت فنی می‌انجامد.

فراهم‌کننده خدمات ابری دفاعی: بر اساس مدل‌های استاندارد، فراهم‌کنندگان خدمات وظایفی نظیر ارائه سرویس‌های اصلی (نرم‌افزار، پلتفرم‌ها و زیرساخت) را بر عهده دارند. از دیگر خدمات این بخش تأمین امنیت و محرمانگی در ارائه سرویس‌ها می‌باشد و باید این تضمین را به وجود آورد که سرویس‌ها در یک محیط امن به دست کاربران خواهند رسید.

1- Scalability



شکل ۳ . الگوی امنیت برای معماری شبکه حوزه دفاعی

در معماری شبکه حوزه دفاع باید سرویسی تحت عنوان امنیت به مجموعه اضافه شود تا اشراف امنیتی بر روی سایر سرویس‌ها و خدمات به وجود آورد. همچنین تأمین یکپارچگی، محرمانگی و دسترس‌پذیری به سرویس‌ها علی‌الخصوص در شرایط بحرانی در این بخش انجام می‌گیرد. نظارت بر امنیت خدمات برون‌سپاری شده دفاعی که حائز اهمیت می‌باشد نیز بر عهده این بخش است و سرویس‌هایی به عوامل خارج از سازمان دفاعی سپرده می‌شوند که از امنیت آن‌ها اطمینان حاصل شده باشد. تأمین و پیکربندی زیرساخت‌های مورداستفاده 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 شبکه دفاعی مورداستفاده 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 این شبکه امن 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.

کاربران شبکه دفاعی: همان مصرف‌کنندگان خدمات هستند که سرویس‌های دفاعی موردنیاز را از فراهم‌کنندگان سرویس‌ها دریافت می‌کنند. با توجه به آنکه امنیت سرویس‌ها و امنیت ارتباطات در بخش‌های دیگر تأمین‌شده این اطمینان خاطر وجود دارد که سرویس‌هایی که به دست کاربران می‌رسند امن می‌باشند.

بازرسی شبکه دفاعی: امنیت مهم‌ترین بخش معماری شبکه دفاعی است و در معماری ارائه‌شده لازم است که تمامی حوزه‌های دفاعی مورد رصد و پایش قرار گیرند. در این بخش کلیه رخدادها و تهدیدات از طریق روش‌های لازم موردبررسی قرار می‌گیرند. خدمات برون‌سپاری نیز باید موردبررسی دقیق امنیتی قرار گیرد که این حوزه نیز در این بخش انجام می‌شود. همچنین پایداری خدمات و سرویس‌ها که از ملزومات سامانه‌های دفاعی است باید به‌طور دقیق مورد رصد و پایش قرار گیرد و تضمین پایداری در ارتباطات برقرارشده توسط زیرساخت ارتباطی نیروهای مسلح نیز باید در این قسمت موردبررسی قرار گیرد.

واسطهای کاربری و کارگزاری: در معماری رایانش ابری، خدمات و سرویس‌هایی که از طرف فراهم‌کنندگان به کاربران ارائه می‌شود از طریق واسطها و کارگزارها[1] صورت می‌گیرد. در معماری شبکه دفاعی، بخش‌هایی اضافه شده است که عمده آن‌ها نقش مدیریت سرویس‌ها، مدیریت پایگاه‌های داده و بانک‌های اطلاعاتی، مدیریت شبکه زیرساخت ارتباطی خاص نیروهای مسلح و برون‌سپاری خدمات دفاعی را بر عهده دارند.

نتیجه‌گیری و پیشنهاد

الف ـ نتیجه‌گیری:

امروزه فناوری اطلاعات در تمامی عرصه‌های زندگی حضور دارد و یکی از نوظهورترین حوزه‌های فناوری اطلاعات در عصر حاضر، شبکه‌های دفاعی برای نهادهای دفاعی است. بسیاری از سازمان‌های دفاعی این فناوری را قبول کرده‌اند که دلایل آن استفاده حداکثری از منابع سیستم‌ها، کاهش هزینه‌ها، چابکی و نوآوری در سازمان‌های دفاعی است. با توجه به حائز اهمیت بودن امنیت در زیرساخت‌های حوزه دفاعی و به‌منظور کاهش تهدیدات، در معماری شبکه دفاعی پیشنهادی لایه امنیت به‌عنوان یک لایه دربرگیرنده کل معماری در نظر گرفته شده است. در این خصوص نحوه جانمایی امنیت در بخش‌های اصلی شبکه دفاعی مانند ارائه‌دهندگان سرویس‌های

1- Brokers

دفاعی، کاربران خدمات دفاعی، بازرسی‌ها و کارگزاری‌های امنیت و همچنین در بخش‌های حامل و زیرساخت‌های فیزیکی و منابع مجازی شده مشخص شده است. همچنین در معماری ارائه شده، امنیت در بخش‌هایی نظیر مدیریت خدمات برون‌سپاری، مدیریت رخدادها و وقایع، مدیریت کارگزاری شبکه نیروهای مسلح، تأمین و پیگیری زیرساخت، مدیریت تهدیدات و همچنین کنترل ورود به شبکه دفاعی موردتوجه قرار گرفته و عامل‌های رصد و پایش تهدیدات و مخاطرات رایانش ابری حوزه دفاعی مشخص گردیده‌اند.

ب ـ پیشنهادها

در راستای مباحث مطرح شده در این مقاله پیشنهادات زیر ارائه می‌گردد:

۱- از الگوی ارائه شده در این مقاله در طراحی و اجرای معماری‌های امنیت پایه برای سازمان‌های دفاعی کشور استفاده گردد.

۲- تحقیقات در خصوص معماری‌های امنیت پایه برای سازمان‌های دفاعی کشور که مبتنی بر فناوری‌های نوظهور علی‌الخصوص سه فناوری رایانش ابری، اینترنت اشیاء و کلان داده‌ها باشد ادامه یابد.

فهرست منابع

الف – منابع فارسی:

- نقیان فشارکی، مهدی، "*ارائه معماری مرجع امنیتی محیط رایانش ابر خصوصی سازمان*"، فصلنامه علمی -پژوهشی امنیت پژوهی، (۱۳۹۳).
- ولوی، محمدرضا، (۱۳۹۴)، "*ارائه الگوی امن استقرار زیرساخت‌های دفاعی کشور در محیط رایانش ابری*"، فصلنامه علمی پژوهشی مطالعات بین‌رشته‌ای راهبردی، دانشگاه عالی دفاع ملی، تهران.

ب – منابع انگلیسی:

- Arifeen, F. U., Siddiqui, R. A., Ashraf, S., & Waheed, S. (2015). "Inter-Cloud Authentication through X. 509 for defense organization". Paper presented at the 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST).

- B., Wong, R. K., Ghanavati, M., & Chi, C. H. (2014). "Privacy as a service in social network communications". Paper presented at the Services Computing (SCC), 2014 IEEE International Conference on.

- Chung, C.-J., Xing, T., Huang, D., Medhi, D., & Trivedi, K. (2015). "SeReNe: on establishing secure and resilient networking services for an SDN-based multi-tenant datacenter environment". Paper presented at the 2015 IEEE International Conference on Dependable Systems and Networks Workshops.

- D. Sun, G. Chang, L. Sun, X. Wang, (2011), "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", Procedia Engineering, vol. 15, 2852-2856.

- Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). "Regulatory approaches for cyber security of critical infrastructures: The case of Turkey". Computer Law & Security Review, 32(3), 526-539.

- Hardman, O., Groat, S., Marchany, R., & Tront, J. (2013). "Optimizing a network layer moving target defense for specific system architectures". Paper presented at the Proceedings of the ninth ACM/IEEE Symposium on Architectures for Networking and Communications Systems.

- Joshi, B. K., Shrivastava, M. K., & Joshi, B. (2016). "Security Threats and Their Mitigation in Infrastructure as a Service". Perspectives in Science.

- Li, J., Feng, Z., Feng, Z., & Zhang, P. (2015). "A survey of security issues in cognitive radio networks". China Communications, 12(3), 132-150

- Májek, V., & Gazárková, O. (2015). "Networked interoperable real-time information services as a partial solution of command and control systems interoperable connection". Paper presented at the Military Technologies (ICMT), 2015 International Conference on.

- Marcon, D. S., Oliveira, R. R., Neves, M. C., Buriol, L. S., Gaspary, L. P., & Barcellos, M. P. (2013). "Trust-based grouping for cloud datacenters: improving security in shared infrastructures". Paper presented at the IFIP Networking Conference, 2013.

- Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos,(2015), "Security in cloud computing: Opportunities and challenges",Information Sciences, Volume 305, 357-383

- Ryan R. Wagner,Tristan J. Weir, (2015), "Department of Defense Use of Commercial Cloud Computing Capabilities and Services", Institute for Defense Analyses (IDA).
- Sanders, C., & Smith, J. (2013). "Applied network security monitoring: collection, detection, and analysis": Elsevier.

- S.O. Kuyoro, F. Ibikunle, O. Awodele, (2011), "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks 3, pp. 247-255.

- Takai and M.Teresa, "DoD Cloud Computing Strategy," *Department of Defense Chief Information Officer*, 2012.
- Vacca, J. R. (2013). "Network and system security": Elsevier.

- W. Stuart, "IBM Cloud Services Balancing compute options: How IBM Smart Cloud can be a catalyst for IT transformation," TECHNOLOGY BUSINESS RESEARCH, 2011.

- Wu, J., Ota, K., Dong, M., & Li, C. (2016). "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities". IEEE Access, 4, 416-424.

- Yu, T., Cao, X., Chen, Z., & Zhang, C. (2013). "Research on Network Attack and Defense of SCADA System Model Based on FNN". Paper presented at the Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on.