Dor: 20.1001.1.28212673.1404.9.2.8.3

فصلنامهٔ محیط‌شناسی راهبردی ج.ا.ایران، سال نهم، شمارهٔ ۲(۳۱)، تابستان ۱٤۰٤

شناسایی و اولویت‌بندی مسائل راهبردی خدمات ابری در سازمان‌های دفاعی با رویکرد جهانی

محمدحسین معینی[۱]، محمدرضا موحدی صفت[۲]، منصوره علیقلی[۳]، سینا کیهانیان[٤]

تاریخ دریافت: ۱٤۰٤/۰۳/۱۸ پذیرش مقاله: ۱٤۰٤/۰۵/۲٤

چکیده

خدمات ابری به‌عنوان یک فناوری نوظهور و تحول‌آفرین، با ورود به عرصه دفاعی، قابلیت دگرگونی کلی خدمات دفاعی را دارد. سازمان‌های دفاعی جمهوری اسلامی ایران نیز از این تحول مستثنی نیستند. این فناوری، فرصت‌ها و تهدیدهایی به همراه دارد و نیازمند شناخت و اقدامات مناسب است. این پژوهش به شناسایی و اولویت‌بندی مسائل راهبردی خدمات ابری در سازمان‌های دفاعی با رویکرد جهانی می‌پردازد. مسائلی مانند «امنیت اطلاعات»، «مدیریت هویت»، «زیرساخت‌ها» و «استانداردسازی» از جمله چالش‌های کلیدی هستند. هدف اصلی پژوهش، ایجاد هماهنگی و همگرایی بین بازیگران این حوزه در سطح دفاعی و ملی است. روش تحقیق به‌صورت آمیخته (کمی و کیفی) و با رویکرد توصیفی-تحلیلی انجام شده است. بر اساس نتایج پژوهش، توسعه خدمات ابری در سازمان‌های دفاعی نیازمند فرهنگ‌سازی، امنیت‌سازی و وضع قوانین مناسب است. پیشنهاداتی برای توسعه این خدمات با رویکرد جهانی ارائه شده است.

واژگان کلیدی: امنیت اطلاعات، حملات سایبری، خدمات ابری، سازمان‌های دفاعی، فناوری اطلاعات.

۱. گروه مدیریت فناوری اطلاعات، واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول).
رایانامه: *moeini@sndu.ac.ir*

۲. دانشیار، رئیس گروه سایبر، هیئت علمی دانشگاه عالی دفاع ملی، تهران، ایران. رایانامه: *mvahedi@sndu.ac.ir*

۳. دانشیار، گروه مدیریت بازرگانی، هیئت علمی واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران.
رایانامه: *man.aligholi@iauctb.ac.ir*

٤. استادیار دانشگاه عالی دفاع ملی، تهران، ایران. رایانامه: *s.keyhanian@sndu.ac.ir*

۱. مقدمه

در عصر فناوری‌های پیشرفته کنونی، سازمان‌های دفاعی به شدت تحت تأثیر تحولات سریع در حوزه اطلاعات و ارتباطات قرار دارند. «رایانش ابری»، راهکاری نوین برای مدیریت انعطاف‌پذیر و مقیاس‌پذیر منابع محاسباتی و کاهش هزینه‌ها است (ولوی و همکاران، ۱۳۹۶: ۱۱۱). پذیرش رایانش ابری در سازمان‌های دفاعی با چالش‌های امنیتی خاصی همراه است. این چالش‌ها شامل نگرانی‌های مربوط به حریم خصوصی، امنیت داده‌ها و تهدیدات سایبری هستند که می‌توانند بر عملکرد و اعتبار سازمان‌های دفاعی تأثیر بگذارند (ال‌کافحالی[1] و همکاران، ۲۰۲۲: ۷). به‌عنوان مثال، داده‌های حساس نظامی و اطلاعات راهبردی که در محیط‌های ابری ذخیره می‌شوند، در معرض خطرات متعددی قرار دارند، از جمله نقض داده‌ها، حملات سایبری و دسترسی غیرمجاز (ریشیکا[2]، ۲۰۲٤: ۳).

چالش‌های امنیتی در رایانش ابری به دلیل ماهیت «چند مستاجری»[3] این فناوری پیچیده‌تر می‌شود. در این مدل، منابع محاسباتی بین چندین کاربر یا سازمان به اشتراک گذاشته می‌شود که ممکن است به نشت اطلاعات حساس بین کاربران مختلف منجر گردد (جاستی[4] و همکاران، ۲۰۱۰: ٤). همچنین، پیکربندی نادرست تنظیمات امنیتی (گوفی[5] و لی[6]، ۲۰۲۳: ۲) و عدم آگاهی کاربران از بهترین شیوه‌های امنیت سایبری می‌تواند خطرات بیشتری را به همراه داشته باشد. بنابراین، شناسایی و اولویت‌بندی مسائل راهبردی مرتبط با خدمات ابری در سازمان‌های دفاعی از اهمیت بالایی برخوردار است.

ظهور فناوری‌های برهم‌زن مانند رایانش ابری در حوزه دفاعی نشان‌دهنده یک تغییر پارادایم در مدیریت اطلاعات و منابع است. این فناوری نه‌تنها توانسته هزینه‌ها و زمان دسترسی به داده‌ها را کاهش دهد بلکه امکان ایجاد زیرساخت‌های انعطاف‌پذیر و پویا برای پاسخگویی به نیازهای پیچیده سازمان‌های دفاعی را فراهم کرده است. اهمیت این موضوع

1. El Kafhali
2. Rishika
3. Multitenancy
4. Jasti
5. Guffey
6. Li

در این واقعیت نهفته است که سازمان‌های دفاعی برای حفظ برتری اطلاعاتی و عملیاتی خود نیازمند سامانه‌هایی هستند که بتوانند به سرعت با تغییرات محیطی و تهدیدات نوظهور سازگار شوند. رایانش ابری این توانایی را دارد که با تسهیل پردازش و اشتراک داده‌ها در مقیاس بزرگ، به این نیاز پاسخ دهد.

با وجود مزایای بی‌بدیل رایانش ابری، چالش‌های امنیتی و پیچیدگی‌های فنی آن نیازمند بررسی عمیق و تدوین راهبردهای خاص در سازمان‌های دفاعی است. در جهانی که تهدیدات سایبری در حال گسترش است و بازیگران متخاصم از ابزارهای پیچیده برای حمله به زیرساخت‌های حیاتی استفاده می‌کنند، یکپارچه‌سازی رایانش ابری بدون داشتن رویکردی هدفمند می‌تواند سازمان‌ها را در معرض آسیب‌های جدی قرار دهد. ازاین‌رو، ضرورت دارد تا با شناسایی فرصت‌ها و تهدیدات این فناوری، راهکارهایی برای پیاده‌سازی ایمن و مؤثر آن تدوین شود.

مقاله حاضر به بررسی چالش‌ها و فرصت‌های موجود در زمینه رایانش ابری برای سازمان‌های دفاعی می‌پردازد و سعی دارد تا با ارائه یک الگوی راهبردی، راهکارهایی برای پیاده‌سازی موفق خدمات ابری معرفی کند.

۲. مبانی نظری و پیشینه‌شناسی تحقیق

۲-۱. پیشینه تحقیق

در بخش پیشینه پژوهش در ارتباط با مسائل راهبردی خدمات ابری در سازمان‌های دفاعی، تعداد ۱۹ سند راهبردی و گزارش تحقیقاتی راهبردی، ۱۵ رساله دکتری و پایان‌نامه‌های کارشناسی ارشد و نخبگان، ۵۸ مقاله علمی–پژوهشی داخلی و خارجی و ۳۳ کتاب داخلی و خارجی مورد بررسی و واکاوی قرار گرفت. در قسمت زیر به مهم‌ترین آن‌ها به‌خصوص در بازه زمانی چهار سال اخیر اشاره می‌شود.

«دفتر افسر ارشد اطلاعات وزارتخانه دفاع ایالات متحده آمریکا»، سند راهبردی ابری وزارت دفاع (۲۰۲۱) تدوین کرده است؛ این سند یک نقشه راه برای پیاده‌سازی زیست‌بومی مبتنی بر فناوری ابری ارائه می‌دهد. این سند راهبردی به دلایلی مانند ظهور مجدد رقابت‌های راهبردی، پیشرفت سریع فناوری‌ها، و تغییر مفاهیم جنگ و رقابت تهیه شده است. این راهبرد بر دو محور

اصلی تأکید دارد: آماده‌سازی سکو[1]های ابری برای پذیرش داده‌ها و برنامه‌ها؛ و انتقال و توسعه مداوم برنامه‌های کاربردی در فضای ابری. در نسخه ۲۰۲۱م. بر اجرای فناوری ابری در جنگنده‌های آمریکایی و بازنگری در فعالیت‌های اجرایی وزارت دفاع با هدف بهره‌گیری از نوآوری و انعطاف‌پذیری ابری تأکید شده است. این سند اجرای مؤثر فناوری ابری را یک ضرورت برای حفظ مزیت فنی و برتری اطلاعاتی وزارت دفاع می‌داند (راهبرد ابری وزارت دفاع آمریکا[2]، ۲۰۲۱: ۵).

«مکنزی» و «کامپنی» در گزارش «ابر در چین: چشم‌انداز سال ۲۰۲۵» (۲۰۲۲) نشان می‌دهند که رشد مبتنی بر مصرف‌کننده همچنان محرک اصلی پذیرش رایانش ابری در چین است؛ اما پیش‌بینی می‌شود موج بعدی این تحول، توسط بخش‌های صنعتی و تولیدی هدایت شود. براساس این گزارش حجم بازار ابر عمومی چین تا سال ۲۰۲۵م. به بیش از دو برابر افزایش خواهد یافت و از ۳۲ میلیارد دلار در سال ۲۰۲۱م. به ۹۰ میلیارد دلار خواهد رسید. تحول سریع چین در این حوزه، نه‌تنها اهمیت اقتصادی رایانش ابری را تأکید می‌کند بلکه نقشی کلیدی در توسعه زیرساخت‌های رقمی[3] این کشور ایفا خواهد کرد (مکنزی و کامپنی[4]، ۲۰۲۲: ٦).

«دولت فدراسیون روسیه» نیز «سند راهبردی توسعه صنعت ارتباطات» (۲۰۲۳) تدوین کرده است. روسیه تلاش دارد تا به جایگاهی رقابتی و امیدوارکننده در این حوزه دست یابد. این سند به‌عنوان یک برنامه‌ریزی راهبردی، اهداف کلیدی از جمله ایجاد زیرساخت‌های ارتباطی مدرن و ایمن مانند رایانش ابری، توسعه فناوری‌های نوین، تقویت ظرفیت علمی و نیروی انسانی، و بهبود چارچوب‌های نظارتی را در بر می‌گیرد. اجرای این سند نه‌تنها زمینه ارائه خدمات با کیفیت بالا به شهروندان، کسب‌وکارها و دولت را فراهم می‌کند بلکه به تحقق اهداف امنیت ملی و تقویت زیرساخت‌های رقمی این کشور نیز کمک شایانی خواهد کرد (پراوی‌تیل‌ست‌وو[5]، ۲۰۲۳: ٤).

1. Platform
2. DOD Cloud Strategy
3. Digital
4. McKinsey & Company
5. Правительство (Pravitel'stvo)

«غضنفرپور» و «موسوی» در راستای بررسی اهمیت و کاربرد رایانش ابری در سازمان‌های دفاعی، مقاله‌ای با عنوان «معماری به‌کارگیری رایانش ابری در سازمان‌ها» (۱٤۰۰) در همایش تخصصی مهندسی دفاعی منتشر کرده، و به تحلیل معماری استفاده از این فناوری پرداخته‌اند. این مقاله تأکید می‌کند که بسیاری از کشورها زیرساخت‌های حیاتی خود، از جمله دفاع را بر پایه محیط‌های ابری طراحی و اجرا می‌کنند. با این حال، نویسندگان به اهمیت ملاحظات امنیتی در استقرار این زیرساخت‌ها در حوزه‌های نظامی اشاره دارند. این مقاله به‌طور خاص بر نیاز به دقت و برنامه‌ریزی در استفاده از رایانش ابری برای حفظ امنیت و عملکرد بهینه زیرساخت‌های دفاعی تأکید می‌کند (غضنفرپور و موسوی، ۱٤۰۰: ۷).

«بالاشووا»[1] و «موسین»[2] در مقاله‌ای مشترک تحت عنوان «رایانش ابری: روندها و چالش‌های جهانی برای روسیه در زمان تحریم‌ها» (۲۰۲۲) وضعیت خدمات ابری در روسیه و چالش‌های ناشی از تحریم‌های سال ۲۰۲۲ را بررسی کرده‌اند. نتایج تحقیق نشان می‌دهد که عوامل زیرساختی، اقتصادی، اجتماعی و قانونی از محرک‌های اصلی پذیرش رایانش ابری در این کشور هستند، اگرچه سطح پذیرش کلی این خدمات همچنان پایین است. بازار ابری روسیه بیشتر توسط بازیگران محلی اداره می‌شود اما عدم تمایل شرکت‌های کوچک و متوسط برای مهاجرت به فضای ابری یکی از موانع اصلی است. تحریم‌ها تأثیر قابل‌توجهی بر زیرساخت‌های فناوری اطلاعات روسیه داشته‌اند اما پژوهشگران معتقدند که با موفقیت برنامه‌های جایگزینی واردات، حمایت‌های قانونی و تغییر نگرش کسب‌وکارها، ارائه‌دهندگان محلی قادر به جایگزینی ارائه‌دهندگان جهانی خواهند بود (بالاشووا و موسین، ۲۰۲۲: ۸).

«علوی‌زاده»[3] و همکاران در مقاله‌ای مشترک تحت عنوان «ارزیابی اثرات امنیتی و اقتصادی تکنیک‌های دفاع از هدف متحرک در فضای ابری»[4] (۲۰۲۲) را منتشر کرده‌اند. نتایج این پژوهش نشان می‌دهد که روش‌های دفاع هدف متحرک به‌عنوان یک سازوکار امنیتی فعال، با تغییر سطح حمله، مهاجمان را گیج کرده و امنیت ابری را بهبود می‌بخشند؛ ولی تاکنون ارزیابی جامعی از

1. Balashova
2. Musin
3. Alavizadeh
4. Moving Target Defense (MTD)

اثربخشی این روش‌ها بر اساس معیارهای امنیتی و اقتصادی انجام نشده است. در این مقاله، ترکیبی از سه روش دفاع هدف متحرک تعریف شده و اثربخشی آن‌ها با استفاده از چهار معیار امنیتی شامل مخاطره[1] سامانه، هزینه حمله، بازگشت در حمله و قابلیت اطمینان در مدل‌های ابری در مقیاس بزرگ ارزیابی شده است. علاوه‌بر این، هزینه‌های مرتبط با استقرار این روش‌ها بررسی شده و یک مدل برنامه‌ریزی خطی باینری برای بهینه‌سازی تخصیص تنوع و حداکثرسازی سود خالص ارائه گردید (علوی‌زاده[2] و همکاران، ۲۰۲۲: ٤).

«عَلوفی»[3] و همکاران، در مقاله‌ای مشترک تحت عنوان «مروری سیستماتیک بر ادبیات امنیت محاسبات ابری: تهدیدات و استراتژی‌های کاهش آنها» (۲۰۲۱) با استفاده از یک مرور نظام‌مند ادبیات[4]، مطالعات مرتبط با امنیت، تهدیدات و چالش‌های رایانش ابری را بین سال‌های ۲۰۱۰ الی ۲۰۲۰.م بررسی کرده‌اند. این پژوهش پس از غربالگری دقیق، ۸۰ مقاله را انتخاب و هفت تهدید امنیتی عمده برای خدمات رایانش ابری شناسایی کرده است؛ از جمله این تهدیدات می‌توان به دستکاری داده‌ها، نشت اطلاعات، نفوذ داده‌ها و چالش‌های مربوط به ذخیره‌سازی داده‌ها در محیط ابری اشاره کرد. علاوه‌بر این، برون‌سپاری داده‌های مصرف‌کنندگان نیز به‌عنوان یک چالش مداوم برای ارائه‌دهندگان خدمات ابری[5] و کاربران ابری گزارش شده است. این تحقیق با ارائه دیدگاه جامعی از تهدیدات امنیتی، به شناسایی راهبردهای کاهش این چالش‌ها کمک می‌کند (عَلوفی و همکاران: ۲۰۲۱: ۹).

طبق بررسی به‌عمل‌آمده در تحقیقات ذکرشده، هر یک از پژوهش‌ها به جنبه‌ای از رویکردهای مرتبط با موضوع پژوهش (خدمات ابری امن، راهبردهای ابری، توسعه خدمات، سازمان‌های دفاعی) از قبیل کارکردها، تهدیدها و فرصت‌های مترتب بر به‌کارگیری، نقاط ضعف و چالش‌های امنیتی و... را مطرح نموده که از نظر موضوعی قابلیت لازم برای استفاده در ادبیات این تحقیق را دارد. مهم‌ترین نتیجه حاصل از

1. Risk
2. Alavizadeh
3. Alouffi
4. Systematic Literature Review (SLR)
5. Cloud Service Providers (CSP)

جمع‌بندی پیشینه‌ها مبین این نکته است که هرچند بهره‌گیری از خدمات ابری امن مزایایی همچون صرفه‌جویی در مصرف انرژی و کاهش هزینه‌ها، در اختیار قرارگرفتن حجم بالایی از داده‌های بخش‌های مختلف، اشراف بیشتر بر حوزه کاری و تسریع در تصمیم‌گیری می‌گردد لیکن سازمان‌های دفاعی را با چالش‌هایی از قبیل حفظ استقلال سازمانی (حریم خصوصی) سازمان‌ها، تهدیدات امنیتی، مواجهه با داده‌های حجیم، نیاز به پهنای باند وسیع و... روبرو می‌سازد؛ این چالش‌ها به‌عنوان موانع تحقیق قلمداد شده و نیازمند چاره‌اندیشی است. اغلب کشورها در این حوزه دغدغه دارند و همواره اسناد خود را با توجه به پیشرفت فناوری‌های نوین بازنگری می‌کنند.

۲-۲. مبانی نظری

۱-۲-۲. فناوری خدمات ابری

رایانش ابری، یکی از فناوری‌های کلیدی در عصر رقمی است که به سازمان‌ها این امکان را می‌دهد تا منابع محاسباتی و ذخیره‌سازی خود را به‌صورت مقیاس‌پذیر و انعطاف‌پذیر مدیریت کنند. این فناوری شامل سه معماری اصلی است:

- نرم‌افزار به‌عنوان خدمت[1]؛
- سکو به‌عنوان خدمت[2]؛
- زیرساخت به‌عنوان خدمت[3].

هرکدام از این معماری‌ها، با توجه به نیاز سازمان‌ها، خدمات متفاوتی ارائه می‌دهند. نرم‌افزار به‌عنوان خدمت، امکان استفاده از نرم‌افزارها بدون نیاز به نصب محلی را فراهم می‌کند. سکو به‌عنوان خدمت بستر توسعه و تست نرم‌افزار را ارائه می‌دهد. زیرساخت به‌عنوان خدمت با ارائه منابع پایه‌ای مانند توان پردازشی و فضای ذخیره‌سازی، نیاز به خرید تجهیزات سخت‌افزاری را کاهش می‌دهد.

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

۲-۲-۲. راهکارهای افزایش امنیت خدمات ابری

امنیت فضای ابری، یکی از مهم‌ترین چالش‌های این فناوری است؛ زیرا شامل حفاظت از داده‌ها، برنامه‌ها، و زیرساخت‌ها در برابر تهدیدات سایبری می‌شود. این موضوع اهمیت ویژه‌ای دارد چون بسیاری از سازمان‌ها داده‌های حساس خود را به فضای ابری منتقل کرده‌اند. برای مقابله با این چالش‌ها، راهکارهای متعددی ارائه شده است؛ مهم‌ترین آن‌ها عبارت‌اند از:

- اجرای احراز هویت چندعاملی[1]؛
- مدیریت دسترسی کارمندان؛
- نظارت بر فعالیت کاربران نهایی؛
- پشتیبان‌گیری و بازیابی اطلاعات.

این راهکارها، همراه با استفاده از فناوری‌هایی مانند دیواره‌های آتش[2] پیشرفته و نظارت بر رویدادنگار[3]های سامانه، می‌توانند به بهبود امنیت خدمات ابری کمک کنند.

۳-۲-۲. معماری خدمات ابری

معماری خدمات ابری سه بخش اصلی دارد:

۱. فرانت‌اند: نمایانگر تعاملات کاربران با ساختار ابری است؛
۲. بک‌اند: شامل زیرساخت‌های فنی و منابع پردازشی است که توسط ارائه‌دهندگان خدمات مدیریت می‌شود؛
۳. شبکه: ارتباط بین این دو بخش را فراهم می‌کند و امکان انتقال داده‌ها و خدمات را به کاربران ارائه می‌دهد.

1. Multi-Factor Authentication (MFA)
2. Firewall
3. Log

٤-۲-۲. مفهوم‌شناسی خدمات ابری امن

امنیت فضای ابری از اهمیت فراوانی برخوردار است؛ زیرا تقریباً همه سازمان‌ها برای کارهای اساسی و ضروری‌شان به خدمات ابری متکی هستند. بااین‌حال، با افزایش حمله‌های سایبری و نقض امنیت در سکوهای ابری و حفاظت از برنامه‌ها و داده‌های ابری، افزایش امنیت رایانش ابری برایشان ضروری شده است (آبیجیت[1]، ۲۰۲۲: ۵).

امنیت فضای ابری[2] یا امنیت رایانش ابری، عملی برای تأمین امنیت شبکه‌های کامپیوتری و داده‌های کاربر در محیط‌های محاسبات ابری است که برای محافظت از برنامه‌ها و دستگاه‌های مبتنی بر ابر برنامه‌ریزی شده‌اند. امنیت فضای ذخیره‌سازی ابری شامل ترکیبی از سیاست‌ها، کنترل‌ها، راهبُردها و فناوری‌ها خواهد بود (سردبیری کانسنشوس[3]، ۲۰۲۲: ۷).

۱-٤-۲-۲. اجرای احراز هویت چندعاملی

«رخنه‌گرها»[4]، راه‌های متعددی برای دسترسی به داده‌ها و برنامه‌های کسب‌وکار برخط شما دارند؛ اما یکی از روش‌های اصلی آن‌ها، دزدیدن اعتبارنامه‌هاست. برای افزایش امنیت ذخیره‌سازی ابری، به کمک احراز هویت چندعاملی می‌توان از اطلاعات همه کاربران خود محافظت کنید و مطمئن شوید که فقط کارکنان مجاز می‌توانند به برنامه‌های ابری شما وارد شوند و به داده‌های حساس دسترسی داشته باشند (عبدی‌پور، ۱٤۰۲: ۸).

۲-٤-۲-۲. مدیریت دسترسی کارمندان[5]

اکثر کارمندان نیازی ندارند به هر برنامه یا فایلی در زیرساخت ابری شما دسترسی داشته باشند. کنترل دسترسی کارمندان نه‌تنها از ویرایش تصادفی اطلاعاتی جلوگیری می‌کند (برخی کارمندان مجاز به دسترسی به آن‌ها نیستند) بلکه از شما در برابر رخنه‌گرهایی محافظت می‌کند که اطلاعات کارمندان را دزدیده‌اند. بنابراین، مدیریت دسترسی کارمندان

1. Abhijeet
2. Cloud Security
3. Consensus editorial
4. hackers
5. IAM

به برنامه‌ها و فایل‌های سازمان شما در امنیت فضای ذخیره‌سازی ابری بسیار مؤثر خواهد بود (عبدی‌پور، ۱٤۰۲: ۸).

۳-٤-۲-۲. نظارت بر فعالیت‌های کاربران نهایی[1]

نظارت و تجزیه‌وتحلیل فعالیت‌های کاربران نهایی برای تشخیص هرگونه ناهنجاری یا بدافزارهای نشان‌دهنده نقض احتمالی سامانه شما و به‌منظور افزایش امنیت فضای ابری ضروری است. برای نمونه، اگر شخصی از طریق دستگاهی با شناسه اینترنتی[2] ناشناخته وارد سامانه شود، باید به‌راحتی بتوانید آن را تشخیص دهید. تشخیص این فعالیت‌های غیرطبیعی به جلوگیری از فعالیت رخنه‌گرها کمک می‌کند و به شما امکان می‌دهد تا بدافزارها را شناسایی و سریعاً مشکلات امنیتی را برطرف کنید. یکی از راه‌حل‌های موجود، استفاده مرکز عملیات امنیتی به‌عنوان خدمتی است که در افزایش امنیت ذخیره‌سازی ابری می‌تواند به شما کمک شایانی کند. علاوه‌بر این، خدمت یادشده می‌تواند آسیب‌پذیری‌های سامانه را پویش[3] کرده و آن‌ها را اصلاح کند (سیلوا[4]، ۲۰۲۳: ۱۱).

یک روش دیگر، روش مبتنی بر ابر برای برون‌سپاری امنیت سایبری است. امنیت برون‌سپاری می‌تواند حفاظت از داده‌ها، امنیت صدا روی شناسه اینترنت[5]، امنیت پایگاه‌داده و امنیت عمومی شبکه را پوشش دهد. این موارد می‌تواند به سازمان‌ها کمک کند تا با تهدیدات شبکه مانند بدافزارها و شبکه‌های رباتی[6] مقابله کنند. امنیت به‌عنوان خدمت یک راه‌حل فزاینده محبوب امنیت داده برای سازمان‌ها است (سنگفور تکنولوژیز[7]، ۲۰۲۳: ۹).

1. End-User
2. Internet Protocol (IP)
3. Scan
4. Silva
5. Voice over Internet Protocol (VoIP)
6. Botnets
7. Sangfor Technologies

جدول شماره ۱. راهکارهای افزایش امنیت خدمات ابری

راهکارهای افزایش امنیت خدمات ابری		
اجرای احراز هویت چندعاملی	مدیریت دسترسی کارمندان	نظارت بر فعالیت‌های کاربران نهایی[1]
کنترل دسترسی کارمندان	آموزش کارمندان برای مبارزه با فیشینگ	استفاده از پشتیبان‌گیری ابر به ابر[2]
استفاده از ابر خصوصی	رویدادنگاری و نظارت ابری[3]	استفاده از فایروال‌های پیشرفته
پشتیبان‌گیری منظم		اجرای تست نفوذ

۵-۲-۲. معماری مفهومی فناوری خدمات ابری

«معماری ابری» به شیوه‌ای گفته می‌شود که اجزای فناوری ابری با یکدیگر ترکیب می‌شوند. این معماری نشان می‌دهد که منابع چگونه از طریق اینترنت و فضای ابری در اختیار کاربران قرار می‌گیرد. برای اینکه به شکل دقیق‌تری بدانیم معماری ابری چیست باید ابتدا اجزای آن را بشناسیم. معماری رایانش ابری از اجزای زیر تشکیل شده است (آقایی، ۱٤۰۱: ٤):

۱. سمت خدمت‌دهنده[4]؛ بک‌اند

بک‌اند، به قسمتی از معماری ابری گفته می‌شود که فقط شرکت ارائه‌کننده معماری ابری با آن سروکار دارد. این قسمت شامل تمام منابع موردنیاز مشتری‌های خدمت‌های ابری از جمله ماشین‌های مجازی، فضای ذخیره‌سازی، مکانیزم‌های کنترل ترافیک و اپلیکیشن‌های مجازی می‌شود.

۲. سمت کاربر[5]؛ فرانت‌اند

منظور از فرانت‌اند، اتفاقاتی است که در سمت مشتری رایانش ابری می‌افتد. به‌عبارت دیگر، اپلیکیشن‌ها و برنامه‌هایی است که مشتری برای اتصال به خدمت ابری و استفاده از خدمات آن به‌کار می‌گیرد. برای مثال مرورگری که باید برای اتصال به این خدمت‌ها استفاده کنید جزء فرانت‌اند به حساب می‌آید.

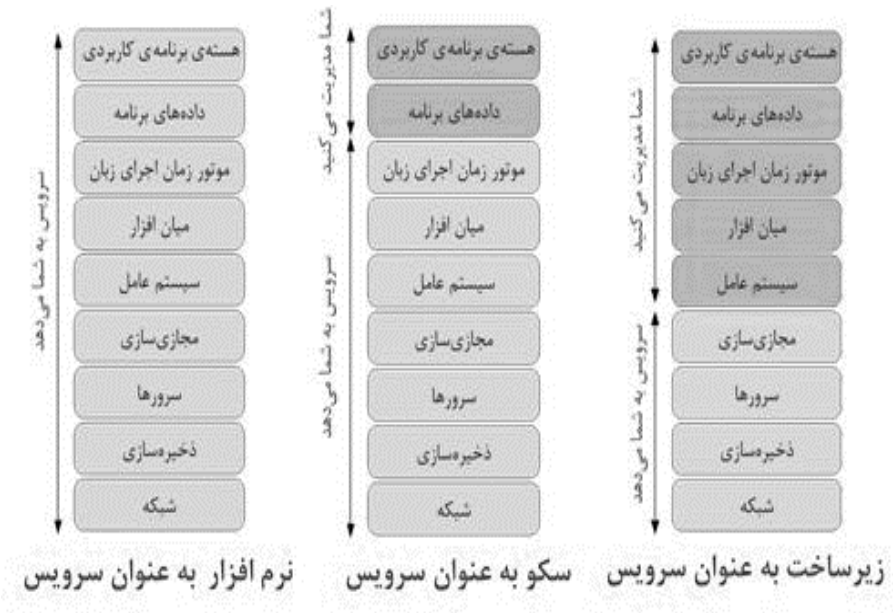
1. End-User
2. Cloud-to-Cloud
3. Cloud Monitoring & Logging
4. Back-End (Server-Side)
5. Front-End (Client-Side)

۳. شبکه[1]

عبارت است از شبکه‌ای که بین اپلیکیشن و خدمت‌های ابری ارتباط برقرار می‌کند. این شبکه به کاربران بیرونی و اپلیکیشن‌هایی که می‌خواهند از زیرساخت‌های ابری استفاده کنند، اجازه می‌دهد تا به یکدیگر وصل شوند.

۱-۵-۲-۲. انواع معماری ابری

سه معماری اصلی برای خدمت‌های ابری داریم که هر سازمان یا فردی با توجه به نیازهایی که دارد می‌تواند یک مورد یا چند مورد از این خدمات را استفاده کند. در این قسمت از پژوهش هر یک از این خدمت‌ها را نام برده و توضیح می‌دهیم. انواع معماری ابری مطابق شکل (۱) شامل موارد زیر می‌شود (اشتهاردی، ۱۳۹۳: ۹).



شکل شماره ۱. انواع معماری ابری

1. Network

خدماتی که رایانش ابری ارائه می‌دهد عبارت‌اند از: نرم‌افزار به‌عنوان خدمت، بستر به‌عنوان خدمت و زیرساخت به‌عنوان خدمت:

۱. نرم‌افزار به‌عنوان خدمت

این خدمت بنا به درخواست کاربر به‌صورتی ارائه می‌شود که پردازشی منفرد از یک نرم‌افزار در محیط ابر اجرا می‌شود و می‌تواند هم‌زمان به چندین کاربر نهایی خدمت‌دهی کند. به کمک این خدمت دیگر نیازی به نصب نرم‌افزار روی رایانهٔ کاربران نیست و باعث تسهیل در پشتیبانی می‌شود؛ زیرا نرم‌افزار تنها روی یک خدمت‌دهندهٔ مرکزی نصب شده و توسط آن اداره می‌شود. جهت بروزرسانی نرم‌افزار نیز تنها نرم‌افزار خدمت‌دهنده نیاز به ارتقا دارد. بزرگ‌ترین مزیت این خدمت دسترسی دائمی کاربر به نرم‌افزار در هر نقطه به وسیلهٔ بستر اینترنت است (اشتهاردی، ۱۳۹۳: ۹).

٦-۲-۲. مفهوم‌شناسی سازمان‌های دفاعی ابری

سازمان‌های دفاعی در طول زمان با تغییرات اساسی در پاسخ به ماهیت تهدیدات و محیط پیرامونی تحول یافته‌اند. این سازمان‌ها ابتدا با تأثیر از تحولات انقلاب صنعتی، به سمت ساختارهای ماشینی حرکت کردند که شامل استانداردسازی قوانین، تجهیزات و فرایندها بود (چَن[1] و همکاران، ۲۰۰۵: ۳). با پایان جنگ سرد و ظهور تهدیدات نوین، سازمان‌های دفاعی به ساختارهای زیستی‌تر برای انطباق با چالش‌های جدید تغییر مسیر دادند. در عصر کنونی، این سازمان‌ها باید با بهره‌گیری از دانش و شبکه‌سازی به برتری اطلاعاتی و شناختی دست یابند و بر پردازش و انتشار مستمر اطلاعات و استفاده از فناوری‌های نوین برای تصمیم‌گیری سریع و مؤثر تمرکز کنند. این تحولات، زمینه‌ساز مفهوم سازمان‌های دفاعی ابری و اهمیت آن‌ها در مدیریت دانش و اطلاعات دفاعی شده است.

ماهیت نبردها در عصر فناوری اطلاعات و ارتباطات تغییر کرده و به شکل جنگ اطلاعات درآمده است؛ در این خصوص استفاده از سامانه‌های فناوری به‌منظور برتری اطلاعاتی نقش حیاتی در سازمان‌های دفاعی ایفا می‌کنند (عبدی، ۱۳۹۰: ۳). ایجاد

1. Chan

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 نمی‌توان به این مهم دست یافت.

امروزه اغلب سازمان‌های دنیا از جمله سازمان‌های دفاعی در حال برنامه‌ریزی برای مهاجرت به محیط رایانش ابری هستند. 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؛ لذا رایانش ابری بر اساس خصوصیات خود و حساسیت نهادهای دفاعی می‌تواند برای توسعه هرچه بیشتر مورد استفاده قرار گیرد و علاوه‌بر کاهش هزینه‌های مراکز داده و افزایش بهره‌وری، محیطی یکپارچه را برای این سازمان‌ها ایجاد نماید (مایکروسافت آژور[1]، ۲۰۲۱: ۹).

تدوین برنامه مبتنی بر خدمات ابری در سازمان‌های دفاعی یک اولویت اساسی در کشور خواهد بود. این جنبه‌ها را می‌توان به‌صورت خلاصه به شرح زیر ارائه داد:

- ❖ طراحی برنامه دقیق و سنجیده برای توسعه خدمات ابری امن در سازمان‌های دفاعی (ولوی و موحدی‌صفت، ۱۳۹۵: ٤)؛
- ❖ داشتن نگاه کلان و راهبردی برای توسعه خدمات ابری امن در سازمان‌های دفاعی (ولوی و همکاران، ۱۳۹٦: ۸)؛
- ❖ توسعه مفهوم خدمات ابری امن در سازمان‌های دفاعی (ولوی و موحدی‌صفت، ۱۳۹۵: ٤)؛
- ❖ بررسی تهدیدات سایبری در حوزه ابر دفاعی کشور (رحمتی لارهنگ و همکاران، ۱٤۰۱: ۹)؛
- ❖ بررسی اثر زیرساخت‌ها و سامانه‌ها در مواجهه با توسعه خدمات ابری امن (گوپتا[2] و واشیست[3]، ۲۰۲۳: ٦)؛

1. Microsoft Azure
2. Gupta
3. Vashisth

❖ کمک به سازمان‌های دفاعی کشور برای کاربردی کردن ابر دفاعی امن (رِدی[1] و مونیکا[2]، ۲۰۱۲: ۸).

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 است. به‌علاوه، 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 به‌طور کامل برطرف نگردیده است (آرداگنا[3]، ۲۰۱۵: ۱۲).

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. همه‌ی مسائل مطرح در ایجاد عمومی می‌تواند به‌طور جدی‌تر در خدمات ابری امن سازمان‌های دفاعی مطرح شود (ولوی، ۱۳۹۷: ۸).

شکل ۲. ملاحظات مهم امنیتی در خدمات ابری امن

1. Reddy
2. Monika
3. Ardagna

تفکیک رایانش ابری خصوصی ویژه سازمان‌های دفـاعی از رایـانش ابـری عمـومی الزامـی است (پاچکو[1]، ۲۰۲۳: ۱۱). به‌منظور اشتراک‌پذیری اطلاعات باید به الگوریتم‌های رمزنگاری به‌طور کامل توجه شود. در شکل (۲) ملاحظات مهم امنیتی در خدمات ابری امن سازمان‌های دفاعی برگرفته از مقاله (ولوی، ۱۳۹۷: ۸) نشان داده شده است.

در حوزه رایانش ابری، تاکنون چارچوب‌های معمـاری امنیتـی متنـوعی بـه وسـیلهٔ پژوهشگران و سازمان‌های دولتی و خصوصی مانند «سازمان ملی استاندارد و فناوری»، «وزارت دفاع آمریکا»، «دارپا»[2]، «آژانـس امنیت اطلاعات و شبکهٔ اروپا»[3] و «اتحادیه امنیت ابری»[4] ارائه شده است. در حال حاضر دو معماری مهم «دودَف»[5] و «فرماندهی و کنترل»[6] که مختص سازمان‌های نظـامی هستند، در حـال بازتعریف‌شدن در محیط رایانش ابری می‌باشد. مؤسسه ملی استاندارد و فناوری نیز مدل مرجع معماری امنیتی را در یک سند مجزا هر چند سال منتشر می‌نماید (اتحاد امنیت ابری[7]، ۲۰۲۱: ۹).

۷-۲-۲. مطالعه تطبیقی حوزه خدمات ابری

تغییر دیدگاه غالب افراد جامعه بر قابل اتکا کردن شبکه‌های مقیاس وسیع و «اینترنت جهانی» از نظر در دسترس بودن، پایداری، سرعت و تداوم ارتباطات شبکه‌ای، زمینه لازم برای پذیرش خدمات ابری را در بسیاری از کشورهای دنیا به وجود آورده است. اغلب کشورهایی که در سطح کلان به خدمات ابری روی آورده‌اند، در سطحی از توسعه زیرساخت‌های فناوری اطلاعات و ارتباطات قرار دارند که در پی بهره‌گیری مدیریت‌شده از رایانش ابری برای تحقق اهداف توسعه‌ای خود هستند.

1. Pacheco
2. Darpa
3. European Network and Information Security Agency
4. CSA
5. Department of Defense Architecture Framework (DoDAF)
6. C4ISR: Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR)
7. Cloud Security Alliance

نکته مهم در مورد این بخش، مطالعه سیاست‌ها و اقدامات سیاسی کشورهای منتخب در زمینه خدمات ابری است. بنابراین هدف از مطالعه خدمات ابری در این کشورها، دستیابی به دید جامع در چگونگی پرداختن به خدمات ابری است. تعیین روش‌های اتخاذشده در سایر کشورها و بهره‌گیری از نتایج تحقیقات آن‌ها جهت ارائه راهبردها ضروری است؛ چراکه نتایج این مطالعات نشان می‌دهد که کشورها در سطح جهانی از چه جهت‌گیری‌ها، راهبردها، برنامه‌ها، ساختارها و سازوکارهایی به‌منظور بهره‌گیری از خدمات ابری در راستای دستیابی به راهبردها و سیاست‌های خود استفاده می‌کنند.

مؤلفه‌های ارزیابی برای انتخاب اسناد و کشورهای موردمطالعه در این تحقیق عبارت‌اند از: نقشه راه در توسعه خدمات ابری، وضعیت خدمات ابری، وضعیت بازیگران و کاربران؛ برای کشورهایی همچون ایالات متحده آمریکا، روسیه، چین، انگلستان، اتحادیه اروپا، استرالیا، کره جنوبی، ترکیه و قطر است. برخی یافته‌های مهم برآمده از این مطالعات که در تبیین و تدوین راهبردها و سیاست‌های توسعه خدمات ابری امن نقش کلیدی و تأثیر بسزایی می‌تواند داشته باشد، در جدول (۲) آمده است.

جدول شماره ۲. گزاره‌های اهداف، راهبردها و اقدامات اساسی کشورها در زمینه توسعه خدمات ابری(محقق)

ردیف	اهداف، راهبردها و اقدامات اساسی کشورها در زمینه توسعه خدمات ابری
۱	تمرکز دولت‌ها در ترویج توسعه خدمات ابری
۲	دولت‌ها نقش تسهیل‌کننده داشته، اعمال چارچوب سیاستی در تشویق رشد و نوآوری خدمات ابری و کمک به گسترش آن با کاهش موانع
۳	تمرکز بر موضوعاتی نظیر امنیت سایبری، حفظ حریم خصوصی، نوآوری و مالکیت معنوی، حاکمیت داده‌ها، توسعه استانداردها، مشارکت عمومی و خصوصی در سطوح مختلف محلی، ملی و بین‌المللی.
٤	ایجاد مراکز و برنامه‌های تخصصی در حوزه خدمات ابری
٥	برنامه‌های آموزشی به‌منظور تربیت نیروی متخصص و توسعه مهارت‌ها در کنار تقویت نوآوری
٦	بهبود چارچوب قانون‌گذاری و استانداردهای توسعه خدمات ابری
۷	افزایش سرمایه‌گذاری کشورها در هدایت، شکل‌دهی و جهت‌دهی خدمات ابری
۸	ارتقای تحقیق و توسعه در زمینه‌های مختلف خدمات ابری
۹	برنامه‌های مشترک تحقیقاتی با کشورهای پیشرو به‌منظور انتقال فناوری همانند اتحادیه اروپا
۱۰	تدوین قوانین و مقررات استفاده از داده در سایه رعایت حریم خصوصی و حفظ امنیت
۱۱	اعطای امتیازهای مالیاتی برای شرکت‌های خدمات ابری
۱۲	سرمایه‌گذاری عظیم ارتش‌های بعضی از کشورها برای توسعه خدمات ابری امن

۳. روش‌شناسی تحقیق

این تحقیق با رویکرد جهانی به شناسایی و اولویت‌بندی مسائل راهبردی خدمات ابری در سازمان‌های دفاعی پرداخته است. در این پژوهش از دو روش تحلیل مضمون (برای کشف الگوهای مفهومی) و تحلیل محتوای کیفی (برای طبقه‌بندی داده‌ها) استفاده شده است. مراحل تحلیل مضمون شامل کدگذاری باز، محوری و انتخابی است. تحلیل محتوا با استفاده از نرم‌افزار MAXQDA و محاسبه فراوانی مقوله‌ها انجام شده است. در این مقاله با استفاده از روش توصیفی-تحلیلی، تحلیل مضامین، مصاحبه و پرسش‌نامه، داده‌های کمی و کیفی را بررسی شده است.

برای تدوین راهبرد در این تحقیق، در سطح کلان از چرخه تدوین راهبرد (دِیوید[1]، ۲۰۱۱: ۳۸)، شامل کنکاش مفهومی، کنکاش محیطی، تدوین راهبرد، پیاده‌سازی، کنترل و ارزیابی استفاده شده است (الخفاجی[2] و نِلسون[3]، ۲۰۱۳: ۳۱). در گام‌های اجرایی نیز از روش سند «آی‌تی‌یو» به نام راهنمای تدوین راهبردی ملی امنیت سایبری و بهره‌گیری از هیئت[4] خبرگان استفاده شده است. در واقع از راهنمای تدوین راهبرد ملی امنیت سایبری ارائه‌شده توسط اتحادیه بین‌المللی مخابرات به‌عنوان یک چارچوب معتبر برای شناسایی و اولویت‌بندی مسائل راهبردی خدمات ابری در سازمان‌های دفاعی استفاده شده است (الداجه[5] و الرباعی[6]، ۲۰۲٤: ۱۱). این راهنما به‌عنوان یک مرجع جهانی، به سازمان‌ها کمک کمک می‌کند تا راهبردهای امنیتی و فناوری خود را بر اساس استانداردهای بین‌المللی تدوین کنند.

به منظور احصاء مسائل اساسی از پرسش‌نامه محقق‌ساخته با ۸۱ گویه (از ادبیات تحقیق نقاط قوت، ضعف، و فرصت و بررسی محیطی به معنای پایش و پویش اطلاعات مربوط

1. David
2. Alkhafaji
3. Nelson
4. Panel
5. AlDaajeh
6. Alrabaee

به تهدیدات استخراج شده است) استفاده شد. برای سنجش روایی پرسش‌نامه از روایی محتوایی استفاده شده است.

جامعه آماری پژوهش شامل تعدادی از خبرگان صاحب‌نظر و متولیان حوزه راهبردی فناوری اطلاعات کشور هستند که با روش «نمونه‌گیری هدفمند» و «گلوله برفی» انتخاب شدند. برای رسیدن به اشباع نظری طی پرسش‌نامه‌ای از حدود تعداد ۳۰ نفر نظرخواهی به عمل آمد. پس از جمع‌آوری داده‌ها از طریق پرسش‌نامه، فرایند اولویت‌بندی مسائل در چهار مرحله انجام شد:

۱. محاسبه میانگین نمرات اهمیت

برای هر یک از ۸۱ گویه، میانگین نمرات اهمیت (در مقیاس ۱ تا ۱۰) از نظرات خبرگان محاسبه شد.

۲. تحلیل آماری با اِس‌پی‌اِس‌اِس[1]

داده‌ها با استفاده از آزمون‌های توصیفی (میانگین، انحراف معیار) و تحلیلی (همبستگی پیرسون) بررسی شدند تا اطمینان حاصل شود که تفاوت معناداری بین نظرات خبرگان وجود دارد.

۳. تأیید نهایی توسط هیئت خبرگان

نتایج اولویت‌بندی در جلسه‌ای با حضور ۱۰ نفر از خبرگان ارشد مورد بحث قرار گرفت و اصلاحات نهایی اعمال شد. این مرحله تضمین کرد که اولویت‌ها نه‌تنها بر اساس داده‌های کمی بلکه با در نظر گرفتن ملاحظات کیفی و راهبردی سازمان‌های دفاعی تعیین شده‌اند.

٤. تحلیل استخراج نقاط قوت، ضعف، فرصت و تهدید[2]

مسائل شناسایی‌شده در چارچوب نقاط قوت، ضعف، فرصت‌ها و تهدیدها قرار گرفتند تا اولویت‌ها در تعامل با عوامل داخلی و خارجی سازمان‌ها سنجیده شوند.

1. IBM SPSS
2. SWOT Analysis (Strenghts, Weaknesses, Oppurtunities, Threats).

۱-۳. روایی و پایایی پرسش‌نامه

۱-۱-۳. روایی محتوایی

برای اطمینان از روایی محتوایی پرسش‌نامه، از روش اعتبارسنجی توسط خبرگان استفاده شد. بدین منظور، پرسش‌نامه طراحی‌شده در اختیار تعدادی از متخصصان و صاحب‌نظران حوزه فناوری اطلاعات و امنیت سایبری قرار گرفت. این متخصصان شامل اساتید دانشگاهی، مدیران ارشد فناوری اطلاعات در سازمان‌های دفاعی و کارشناسان با سابقه در حوزه رایانش ابری بودند. پس از جمع‌آوری نظرات و پیشنهادات، اصلاحات لازم در پرسش‌نامه اعمال گردید تا اطمینان حاصل شود که سؤالات به‌طور کامل ابعاد مختلف موضوع تحقیق را پوشش می‌دهند و از نظر محتوایی معتبر هستند.

۲-۱-۳. پایایی پرسش‌نامه

برای سنجش پایایی پرسش‌نامه، از روش «آلفای کرونباخ»[1] استفاده شد. این روش، یکی از متداول‌ترین روش‌ها برای اندازه‌گیری پایایی ابزارهای تحقیق است. مقدار آلفای کرونباخ برای پرسش‌نامه حاضر برابر با ۰/۸۹ محاسبه شد؛ این امر نشان‌دهنده پایایی بالای پرسش‌نامه است. مقادیر آلفای کرونباخ بالای ۰/۷ به‌عنوان حداقل مقدار قابل‌قبول برای پایایی در نظر گرفته می‌شود؛ مقدار به‌دست‌آمده نشان می‌دهد که پرسش‌نامه از قابلیت اعتماد بالایی برخوردار است.

٤. یافته‌های تحقیق و تجزیه‌وتحلیل داده‌ها

۱-٤. یافته‌های تحقیق

۱-۱-٤. کنکاش مفهومی

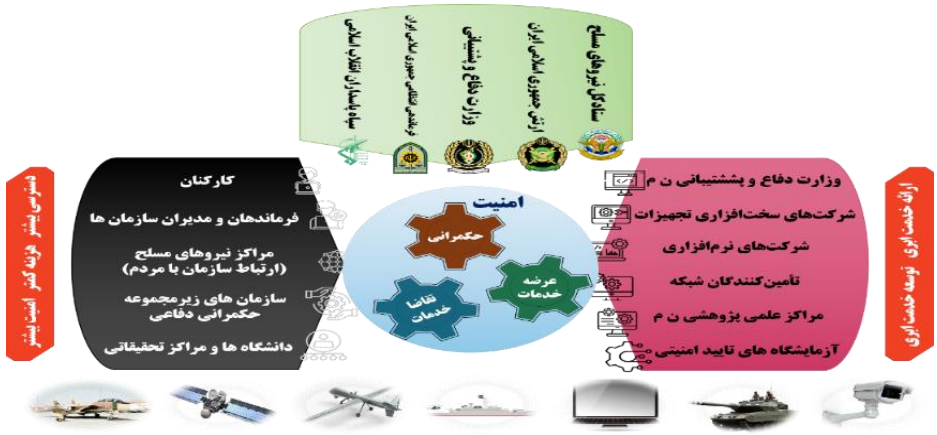
در کنکاش مفهومی به بررسی اسناد بالادستی و مرتبط، مبانی نظری خدمات ابری، سازمان‌های دفاعی، مرور ادبیات سازمان‌های دفاعی ابری، مطالعه تطبیقی توسعه خدمات ابری در کشورهای پیشتاز، اسناد راهبردی کشورهای پیشرفته و همسایه جمهوری اسلامی ایران، بررسی سیاست‌ها و تدابیر ج.ا.ایران در حوزه فناوری اطلاعات و خدمات ابری،

1. Cronbach alpha

مفهوم‌شناسی امنیت از منظر خدمات ابری، مفهوم‌شناسی طرح راهبردی و ارکان آن و... پرداخته شد.

نظر به اینکه شکستن و تبیین یک ساختار از منظرهای مختلف سبب کاهش پیچیدگی نسبت به زمانی است که ساختار تنها از یک بعد نگریسته شود، شفاف‌سازی و تبیین بیشتر مدل مفهومی ارائه‌شده از منظرهای مختلف می‌تواند کمک شایانی به درک و تبیین ابعاد پیچیده و گسترده آن نماید. از طرف دیگر، وجود یک مدل مفهومی جامع و کامل می‌تواند در تدوین، شناسایی، اعتبارسنجی راهبردها و ایجاد هماهنگی و انسجام در میان گروه‌های کانونی و خبرگان پژوهش نقش مهمی ایفا کند. ازاین‌رو، در این مقاله درصدد ارائه مدلی هستیم که فرایند توسعه خدمات ابری امن را به شکلی نظام‌مند و پویا هدایت کرده و روابط مؤثری میان بازیگران اصلی، ذی‌نفعان، سرمایه‌گذاران و سازمان‌های سیاست‌گذار برقرار سازد. در این مدل، بر مشارکت پایدار و تعامل سازنده میان اجزای مختلف آن تأکید می‌شود، به‌گونه‌ای که علاوه‌بر ارتقای نوآوری و توسعه خدمات ابری امن، دسترسی گسترده‌تر و کاهش هزینه‌ها را نیز فراهم کند. بر همین اساس، پس از مطالعه اسناد بالادستی ایران و جهان و انجام مصاحبه‌های تخصصی با صاحب‌نظران حوزه علم و فناوری، به یک مدل مفهومی جامع دست یافته‌ایم.

در این مدل، روابط در سطح سازمان‌های دفاعی به‌گونه‌ای طراحی شده است که با ایجاد زیرساخت‌ها، سیاست‌گذاری مناسب و تنظیم دقیق چارچوب‌ها، به محض اعلام نیاز در حوزه تقاضای خدمات، بخش عرضه بتواند با ارائه خدمات جدید به این نیاز پاسخ دهد. این فرایند به‌صورت یک چرخه تکرارشونده و بهبودیابنده عمل می‌کند، به‌گونه‌ای که تقاضای مداوم برای خدمات موجب توسعه و نوآوری مداوم در بخش عرضه خدمات می‌شود. در شکل (۳) اجزاء اصلی مدل مفهومی توسعه خدمات ابری امن در سازمان‌های دفاعی (حکمرانی، عرضه خدمات، تقاضا خدمات و امنیت) نشان داده شده است.



شکل شماره ۳. مدل مفهومی نهایی توسعه خدمات ابری امن در سازمان‌های دفاعی

مدل مفهومی تحقیق بر اساس مرور نظام‌مند ادبیات علمی و تحلیل اسناد راهبردی ملی و بین‌المللی طراحی شده است. از جمله منابع کلیدی می‌توان به گزارش‌های اتحادیه بین‌المللی مخابرات، اسناد راهبردی وزارت دفاع ایالات متحده و پژوهش‌های منتشرشده در مجلات معتبر (موجود در بخش منابع) اشاره کرد.

برای سنجش اعتبار مدل مفهومی، از پرسش‌نامه‌ها بهره‌گیری شد. جامعه خبرگان از متخصصان حوزه فناوری اطلاعات و راهبردهای دفاعی تشکیل یافته بود. پرسش‌نامه‌ها حاوی پرسش‌های اصلی برای ارزیابی جامعیت، قابلیت اجرایی و سازگاری مدل بودند. علاوه‌بر این، نظرات خبرگان در چند مرحله بازبینی و اصلاح مدل لحاظ گردید.

مدل مفهومی تحقیق به‌طور خاص برای خدمات ابری در سازمان‌های دفاعی طراحی شده و در آن ویژگی‌ها و الزامات منحصربه‌فرد این حوزه لحاظ شده است. ازجمله این ویژگی‌ها می‌توان به ملاحظات امنیتی پیشرفته نظیر مدیریت هویت و دسترسی، حاکمیت داده‌ها و حفاظت از زیرساخت‌های حساس اشاره کرد که به‌طور ویژه در محیط‌های دفاعی مطرح هستند. علاوه‌بر این، مسائل مربوط به اشتراک‌گذاری منابع در محیط‌های چندکاربره و تطبیق با استانداردهای بین‌المللی در زمینه امنیت سایبری از مواردی است که مدل به‌طور اختصاصی برای خدمات ابری در نظر گرفته است. همچنین، ورودی‌های مدل از طریق

تحلیل محیطی و استخراج مسائل خاص سازمان‌های دفاعی با تمرکز بر نیازهای خدمات ابری طراحی شده که آن را از سایر خدمات متمایز می‌کند.

۲-۱-٤. کنکاش محیطی

بررسی محیطی عبارت است از پایش و پویش اطلاعات مربوط به محیط‌های داخلی و خارجی سازمان. محیط داخلی در این تحقیق بخش‌های مختلف حوزه فناوری اطلاعات در محدوده داخلی کشور را دربرمی‌گیرد. یکی از بهترین منابع موجود برای شناخت عوامل محیطی اثرگذار بر توسعه فناوری بهره‌گیری از دیدگاه‌های خبرگان و مدیران باتجربه است.

در گام اول، واکاوی داخلی وضع موجود کشور در دو حوزه فناوری اطلاعات و سازمان‌های دفاعی از طریق مصاحبه با متخصصان، سیاست‌گذاران و ذی‌نفعان این دو حوزه انجام پذیرفت (حدود ۱۰ نفر). سپس به منظور جمع‌بندی و ترکیب عوامل مؤثر محیط داخلی شامل نقاط ضعف شایستگی‌ها و نقاط قوت، کارگروهی متشکل از خبرگان و کارشناسان این دو حوزه تشکیل و بر اساس مدل تحقیق عناوین و مطالب استخراج‌شده در حضور خبرگان مورد بررسی، اصلاح و تدوین قرار گرفت. خروجی این جلسات به استخراج نقاط ضعف (۹ مورد) و نقاط قوت (۷ مورد) منتج شد.

در تحلیل محیطی ابتدا با استفاده از روش‌های هدفمند شناسایی و تحلیل روندها، مواردی از مهم‌ترین پیشران‌ها و روندهای مؤثر و تأثیرگذار در کشور در حوزه‌های مطرح شده، احصاء گردید. این تحلیل با هدف دستیابی به تجربیات و دانش جهانی و داخلی، یکی از مهم‌ترین اقدامات برای تدوین چشم‌انداز و مدل توسعه خدمات ابری امن در سازمان‌های دفاعی محسوب می‌شود. بدین منظور، آخرین ویرایش طرح‌های راهبردی و اقدامات اساسی کشورها در توسعه خدمات ابری در کشورهای امریکا، چین، روسیه، استرالیا، اتحادیه اروپا، کره جنوبی، انگلیس، ترکیه و قطر مورد مطالعه و تحلیل قرار گرفتند. محورهای محتوایی اسناد راهبردی و مطالعات تطبیقی کشورهای فوق در ۷ حوزه تحقیق‌وتوسعه، نوآوری، زیرساخت رقمی، زیست‌بوم داده، حاکمیت و قانون‌گذاری، انتقال فناوری و آموزش و تقویت نیروی انسانی دسته‌بندی گردید. سپس با رویکرد تحلیل محتوا، و بررسی اسناد راهبردی، گزاره‌های راهبردی و عملیاتی استخراج گردید. برخی یافته‌های

مهم برآمده از این مطالعات که در تبیین و تدوین راهبردها و سیاست‌های توسعه خدمات ابری امن نقش کلیدی و تأثیر بسزایی می‌تواند داشته باشد، با تشکیل یک هیئت خبرگی و ارائه کردن خروجی‌های تحلیل محیطی فرصت‌ها (۱۰ مورد) و تهدیدات (۷ مورد) استخراج شد.

مسائل در این تحقیق به مسئله‌یابی مشکلات، ضعف، تهدیدها و مسائل عمومی در موضوع تحقیق اشاره دارد. مسائل از تعامل نقاط قوت و ضعف و فرصت و تهدید که ناشی از شناخت محیط داخلی و بیرونی است، به‌دست می‌آید.

در این پژوهش مسائل اساسی توسعه خدمات ابری امن در ۸۱ گویه، استخراج شد. سپس گویه‌ها در چهار حوزه عرضه خدمات، تقاضا خدمات، حکمرانی و امنیت دسته‌بندی و برای تعیین میزان اهمیت و تأثیرگذاری هر یک از مسائل از طریق پرسش‌نامه به جامعه نمونه (۳۰) نفر از خبرگان صاحب‌نظران و متولیان حوزه راهبردی فناوری اطلاعات ارائه شد.

جدول شماره ۳. توزیع فراوانی پاسخگویان برحسب حوزه تخصصی

حوزه تخصصی	فراوانی	درصد فراوانی
فناوری	۷	۲۳.۳
خدمات	۸	۲٦.۷
امنیت سایبری	۱۲	٤۰
هوش مصنوعی	۳	۱۰
جمع کل	۳۰	۱۰۰

داده‌های پرسش‌نامه‌های جمع‌آوری‌شده برای تجزیه‌وتحلیل وارد نرم‌افزار «اکسل»[1] و «اِس‌پی‌اِس‌اِس» گردید. به‌عنوان نمونه توزیع فراوانی پاسخگویان بر حسب حوزه تخصصی در چهار سطح فناوری، خدمات، امنیت سایبری و هوش مصنوعی در جدول (۳) آمده است. همان‌طور که ملاحظه می‌گردد دو نمونه جامعه آماری در دو حوزه تخصصی تبحر داشته و توزیع تخصصی بین نمونه‌ها تقریباً مناسب است.

1. Microsoft Excel

۱-۲-۱-٤. شناسایی نقاط قوت و ضعف فرصت‌ها و تهدیدها

برای اعتباربخشی به روش استخراج نقاط قوت، ضعف، فرصت و تهدید، نشست‌های خبرگی با حضور ۳۰ نفر از خبرگان حوزه فناوری اطلاعات و سازمان‌های دفاعی برگزار شد. این افراد بر اساس معیارهایی مانند سابقه کاری، تخصص در زمینه راهبردهای فناوری، و مشارکت در پروژه‌های مشابه انتخاب شدند. در این نشست‌ها از ابزارهایی همچون پرسش‌نامه‌های محقق‌ساخته و دستورالعمل‌های استاندارد بهره‌گیری شد.

داده‌های به‌دست‌آمده با تحلیل محتوای کیفی تحقیقات پیشین ترکیب گردید. در این مرحله، از روش تحلیل مضمون برای شناسایی و طبقه‌بندی مضامین کلیدی استفاده شد. داده‌های مستخرج از منابع بررسی گردید. علاوه‌بر این، از چارچوب راهبردی «راهنمای تدوین راهبردی ملی امنیت سایبری» که توسط اتحادیه بین‌المللی مخابرات تدوین شده، برای طراحی و اجرای فرایند استخراج نقاط قوت و ضعف و فرصت‌ها و تهدیدها استفاده شد. این رویکرد ترکیبی، امکان انطباق مسائل شناسایی‌شده با یافته‌های تحقیقات پیشین و نیز تأیید اعتبار آن‌ها را فراهم کرد. در نهایت، نتایج حاصل از تحلیل‌ها در جلسه‌ای با حضور خبرگان بازبینی و تأیید شد.

یکی از بهترین منابع موجود برای شناخت عوامل محیطی اثرگذار بر توسعه فناوری، بهره‌گیری از دیدگاه‌های خبرگان و مدیران باتجربه است. به همین دلیل و به‌منظور جمع‌بندی و ترکیب عوامل مؤثر محیط داخل (شامل نقاط ضعف، شایستگی‌ها و نقاط قوت) با مشورتی که از خبرگان و کارشناسان این حوزه انجام گرفت و بر اساس مدل تحقیق، عناوین و مطالب استخراج‌شده، مورد بررسی، تدوین و تأیید قرار گرفت. خروجی این هیئت‌های خبرگی، استخراج نقاط قوت و ضعف‌ها بود؛ در شکل (٤) نمایش داده شده است.

به‌منظور بهینه‌کاوی موضوعات، مهم‌ترین اهداف، راهبردها و اقدامات اساسی کشورهای مورد مطالعه ارائه شدند، و ۱۲ مفهوم مهم که برای حوزه حکمرانی کشور مفید است، جهت بهینه‌کاوی در معرض اعضاء هیئت قرار داده شد. خروجی نهایی این هیئت، تدوین و تأیید فرصت‌ها و تهدیدات بود؛ در شکل(٤) آمده است:

شکل شماره ٤. تحلیل نقاط قوت، ضعف، فرصت‌ها و تهدیدها

باتوجه‌به میزان اهمیت مسائل بر اساس بالاترین نمرات اخذ شده و طبق دسته‌بندی حوزه‌های چهارگانه مرتب و جمع‌بندی شد. مهم‌ترین مسائل احصاءشده بر اساس بالاترین نمرات اخذشده در جدول (۵) قابل مشاهده است.

جدول شماره ٤. مهم‌ترین مسائل توسعه خدمات ابری امن در سازمان‌های دفاعی

حوزه	مصادیق مسئله	میزان اهمیت
عرضه خدمات	نیروی انسانی متعهد و متخصص کارآزموده در حوزه خدمات ابری امن در توسعه خدمات ابری امن	۸.٦۷
	اهمیت جامعیت در ارائه خدمات در توسعه خدمات ابری امن در سازمان‌های دفاعی	۷.۸۳
	وجود یک سکو یا سکوی ارزیابی‌شده و قابل‌اعتماد در جهت توسعه خدمات ابری امن	۷.٦۸
	وجود شرکت‌های ارائه خدمات نرم‌افزاری در حوزه خدمات ابری در سازمان‌های دفاعی	۷.۳۳
	نقش سازمان‌ها (وزارت دفاع و...) در حوزه عرضه خدمات در راستای توسعه خدمات ابری امن	۷.۳۳
	استانداردها و الگوهای توسعه خدمات ابری مورد قبول در سازمان‌های دفاعی	۷.۲۳
	میزان مشارکت مراکز علمی-پژوهشی ن م جهت توسعه خدمات ابری امن	۷.۱۷
تقاضا خدمات	مقاومت و نگرانی بعضی سازمان‌های دفاعی در برابر تغییر در توسعه خدمات ابری امن	۸.۵۰
	فرهنگ‌سازی و آگاهی‌بخشی از فرصت‌ها و مزیت‌های خدمات ابری امن	۷.۸۳
	هزینه‌های بالای تجهیزات، زیرساخت‌های توسعه و عملیاتی‌کردن خدمات ابری امن	۷.٦۷

	وجود دستگاه‌های جزیره‌ای شبکه‌ای و عدم تبادل داده‌ها در سازمان‌های دفاعی	۷.۵۰
	عدم وجود شرکت‌های تأمین‌کننده تجهیزات زیرساخت و سخت‌افزاری سازمان‌های دفاعی در حوزه خدمات ابری امن	۷.۳۳
	عدم دسترسی مناسب بعضی سازمان‌های دفاعی به خدمات ابری در توسعه خدمات ابری امن	۷.۳۳
	عدم پاسخگویی ظرفیت‌های موجود شبکه‌های دفاعی برای توسعه خدمات ابری امن	۷.۱٦
حکمرانی	حکمرانی، مالکیت داده و اشتراک‌گذاری داده‌ها در توسعه خدمات ابری امن	۸.۸۷
حکمرانی	وجود مسائل ناشی از تحریم‌های بین‌المللی و عدم تعامل سازمان‌های دفاعی با سازمان‌های کشورهای صاحب فناوری	۸.۸۳
حکمرانی	نیاز به وجود یک راهبرد جامع در حوزه حکمرانی خدمات ابری	۸.٦۷
حکمرانی	وجود یک سازمان مرجع استاندارد در کشور جهت استانداردسازی خدمات ابری امن	۸.٦۷
حکمرانی	تعامل ضعیف بین دستگاه‌های ذی‌ربط سازمان‌های دفاعی	۸.۵۷
حکمرانی	نظارت و پایش از سوی حکمران‌ها در توسعه خدمات ابری امن	۸.۳۳
حکمرانی	عملکرد جزیره‌ای و مجزا از یکدیگر که در نهادهای تصمیم‌گیر، مقررات گذار و بهره‌بردار مرتبط	۸.۳۳
امنیت	وجود ملاحظات امنیتی و حفاظتی برای نگهداری اطلاعات سازمان‌های دفاعی در توسعه خدمات ابری	۸.۹۳
امنیت	امنیت کافی در تجهیزات خدمات ابری (زیرساخت، سخت‌افزار، نرم‌افزار) در توسعه خدمات ابری امن	۸.٦۷
امنیت	ارتباطات و مختل نمودن دسترسی به اطلاعات سامانه‌های خدمات ابری مثل حملات DDoS و... در توسعه خدمات ابری امن	۸.۵۰
امنیت	حیطه‌بندی و استقلال سازمانی (حریم خصوصی) در توسعه خدمات ابری امن	۸.۳۳
امنیت	فقدان زیرساخت لازم جهت شناسایی حفره‌ها و مشکلات امنیتی در ریزتراشه‌های تجهیزات جهت توسعه خدمات ابری امن	۸.۳۳
امنیت	وجود اطمینان در فرایند جمع‌آوری، پردازش، انتقال و ذخیره‌سازی داده‌ها در توسعه خدمات ابری امن	۷.۸۳
امنیت	وجود تهدیدات سایبری متصور در توسعه خدمات ابری امن	۷.٦۷

۲-٤. خروجی یافته‌ها

در این بخش، یافته‌های تحقیق به تفکیک موضوعات اصلی و با جزئیات بیشتر بر اساس اولویت‌بندی موجود ارائه می‌شوند. این یافته‌ها از تجزیه‌وتحلیل داده‌های جمع‌آوری‌شده از پرسش‌نامه‌ها و مصاحبه‌ها با خبرگان حوزه رایانش ابری در سازمان‌های دفاعی به‌دست آمده‌اند.

۱-۲-٤. زیرساخت‌های موجود

۱-۱-۲-٤. وابستگی به زیرساخت‌های قدیمی

- ❖ بسیاری از سازمان‌های دفاعی هنوز به زیرساخت‌های فناوری اطلاعات قدیمی وابسته‌اند. این زیرساخت‌ها شامل سرورهای محلی، سامانه‌های ذخیره‌سازی سنتی و نرم‌افزارهای قدیمی هستند که قابلیت یکپارچگی با خدمات ابری را ندارند.
- ❖ این وابستگی می‌تواند مانع از انتقال موفق به محیط رایانش ابری شود و نیاز به هزینه‌های بالای ارتقا و نگهداری را افزایش دهد.

۲-۱-۲-٤. کمبود منابع فنی

- ❖ برخی از سازمان‌ها فاقد منابع انسانی و فنی لازم برای مدیریت و پیاده‌سازی خدمات ابری هستند. این کمبود می‌تواند شامل عدم متخصصان فناوری اطلاعات باتجربه در زمینه رایانش ابری، فقدان تیم‌های امنیت سایبری قوی و کمبود دانش فنی در کارکنان باشد.
- ❖ این امر نیاز به آموزش و ارتقا مهارت‌های فنی را ایجاب می‌کند تا کارکنان بتوانند به‌طور مؤثر از خدمات ابری استفاده کنند.

در جدول(۵) وضعیت زیرساخت موجود نشان داده شده است.

جدول شماره ۵. وضعیت زیرساخت‌ها و سهم هرکدام

وضعیت زیرساخت	درصد
قدیمی	٪۶۰
نیمه‌مدرن	٪۳۰
مدرن	٪۱۰

۲-۲-٤. چالش‌های امنیتی

۱-۲-۲-٤. نگرانی‌های امنیتی

- ❖ امنیت اطلاعات به‌عنوان یکی از بزرگ‌ترین چالش‌ها در پیاده‌سازی خدمات ابری در سازمان‌های دفاعی مطرح است. نگرانی‌هایی درباره نقض داده‌ها، دسترسی غیرمجاز و حملات سایبری وجود دارد.

۲-۲-۲-٤. نقض داده‌ها

- ❖ احتمال دسترسی غیرمجاز به داده‌های حساس نظامی و اطلاعات راهبردی که ممکن است به افشای اطلاعات حیاتی منجر شود. این موضوع می‌تواند عواقب جدی برای امنیت ملی داشته باشد.

۳-۲-۲-٤. حملات سایبری

- ❖ تهدیدات ناشی از حملات سایبری می‌تواند به سامانه‌های ابری آسیب برساند و موجب اختلال در عملکرد سازمان‌ها گردد. این حملات ممکن است شامل موارد زیر باشد:

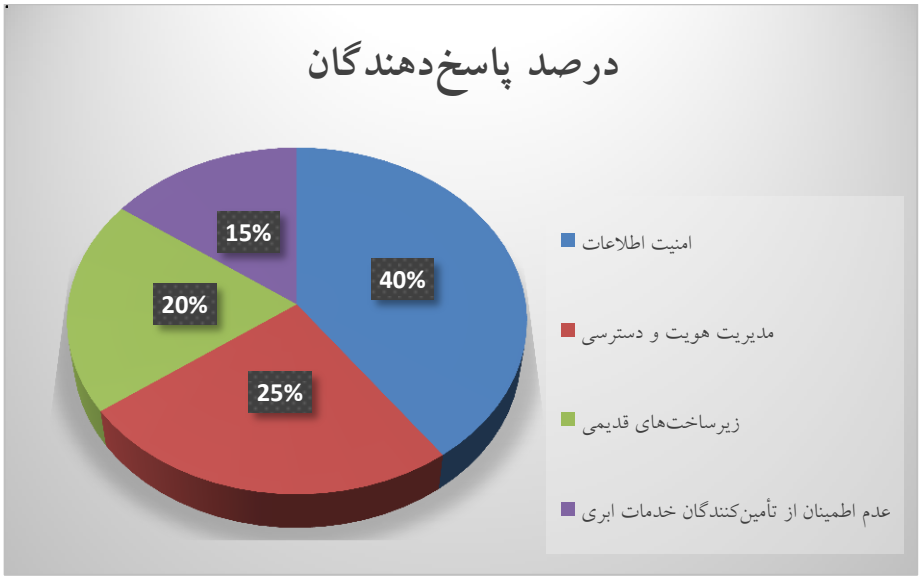
(۱) حملات محروم‌سازی توزیع‌شده از خدمت[1]،

(۲) کلاهبرداری اینترنتی[2]،

(۳) بدافزارها.

٤-۲-۲-٤. عدم اطمینان از تأمین‌کنندگان خدمات ابری

- ❖ برخی از سازمان‌ها نسبت به واگذاری امنیت و حریم خصوصی داده‌ها به تأمین‌کنندگان خدمات ابری نگران هستند.



شکل شماره ۵. وضعیت چالش‌های امنیتی بر حسب درصد پاسخ‌دهندگان

1. Distributed Denial-of-Service (DDoS)
2. Phishing

این نگرانی‌ها معمولاً ناشی از عدم شفافیت در سیاست‌های امنیتی تأمین‌کنندگان و سابقه آن‌ها در مدیریت داده‌ها است. در شکل (۵) وضعیت چالش‌های امنیتی نشان داده شده است.

۳-۲-٤. مدیریت هویت و دسترسی

۱-۳-۲-٤. کمبود سامانه‌های مدیریت هویت

- بسیاری از سازمان‌ها فاقد سامانه‌های مؤثر برای مدیریت هویت کاربران هستند؛ این موضوع می‌تواند به دسترسی غیرمجاز و نشت اطلاعات منجر شود.

۲-۳-۲-٤. نیاز به آموزش کاربران

- عدم آگاهی کاربران درباره بهترین شیوه‌های امنیت سایبری ممکن است خطرات بیشتری را ایجاد کند. کاربران باید با روش‌های شناسایی تهدیدات سایبری و نحوه حفاظت از اطلاعات خود آشنا شوند.

۳-۳-۲-٤. استفاده از فناوری‌های جدید

- پیشنهاد می‌شود که سازمان‌ها از فناوری‌هایی مانند احراز هویت چندعاملی استفاده کنند تا لایه‌ای اضافی از امنیت را برای دسترسی به سامانه‌ها فراهم کنند.

٤-۲-٤. الگوهای مهاجرت به محیط ابری

۱-٤-۲-٤. ایجاد یک الگوی راهبردی

- نتایج نشان می‌دهند که ایجاد یک الگوی راهبردی برای مهاجرت به خدمات ابری ضروری است. این الگو باید شامل مراحل مشخصی مانند موارد زیر باشد:

(۱) ارزیابی زیرساخت‌های فعلی،

(۲) شناسایی نیازها،

(۳) طراحی نقشه راه برای انتقال.

۲-٤-۲-٤. اقدامات مرتبط با هر مرحله

- ❖ پیشنهاد می‌گردد اقدامات مرتبط با هر مرحله از مهاجرت شامل ارزیابی مخاطره، انتخاب تأمین‌کنندگان خدمات ابری، تست امنیت سامانه‌ها و نظارت بر عملکرد پس از انتقال مشخص گردد.

۳-٤-۲-٤. توسعه برنامه آزمایشی

- ❖ قبل از مهاجرت کامل، پیشنهاد می‌شود که یک برنامه آزمایشی[1] اجرا شود تا مشکلات احتمالی شناسایی شده و اصلاحات لازم انجام گیرد.

این یافته‌ها نشان‌دهنده چالش‌ها و فرصت‌هایی هستند که سازمان‌های دفاعی در پیاده‌سازی خدمات ابری با آن مواجه‌اند. توجه به این مسائل و اتخاذ تصمیمات آگاهانه می‌تواند به موفقیت در فرایند انتقال به رایانش ابری کمک کند. همچنین، همکاری بین بخش خصوصی و دولتی در راستای توسعه فناوری اطلاعات در سازمان‌های دفاعی ضروری است تا بتوانند با چالش‌های روزافزون دنیای رقمی مقابله کنند.

۳-٤. تجزیه‌وتحلیل یافته‌ها

۱-۳-٤. تجزیه‌وتحلیل کمی

تجزیه‌وتحلیل کمی داده‌های این مقاله شامل بررسی و تفسیر داده‌های جمع‌آوری‌شده از پرسش‌نامه‌ها و نظرسنجی‌ها است؛ که به شناسایی مسائل و فرصت‌های موجود در پیاده‌سازی خدمات ابری در سازمان‌های دفاعی پرداخته است. مراحل تجزیه‌وتحلیل کمی در شکل (٦) قابل مشاهده است.

1. Pilot Program

۱. طراحی پرسشنامه

پرسشنامه‌ای محقق‌ساخته با استفاده از مبانی نظری و پیشینه تحقیق تهیه شد. این پرسشنامه شامل سؤالات بسته برای ارزیابی چالش‌ها و فرصت‌های خدمات ابری در سازمان‌های دفاعی بود.

۲. جمع‌آوری داده‌ها

پرسشنامه‌ها بین 30 نفر از خبرگان حوزه فناوری اطلاعات و دفاعی توزیع شد. خبرگان بر اساس معیارهایی نظیر تجربه کاری، تخصص در خدمات ابری، و آشنایی با چالش‌های امنیتی انتخاب شدند.

۳. کدگذاری داده‌ها

پاسخ‌های کمی در نرم‌افزار SPSS وارد و کدگذاری شدند.

۴. تحلیل داده‌ها

داده‌های جمع‌آوری‌شده با استفاده از آمار توصیفی مورد تجزیه و تحلیل قرار گرفتند. فراوانی پاسخ‌ها در دسته‌بندی‌های مختلف محاسبه و درصدهای مرتبط استخراج شد.

۵. تفسیر نتایج

نتایج حاصل از تحلیل به شناسایی چالش‌های اصلی، نظیر امنیت اطلاعات (40%)، مدیریت هویت و دسترسی (25%)، زیرساخت‌های قدیمی (20%) و عدم اطمینان از تأمین‌کنندگان خدمات ابری (15%) منجر شد. این چالش‌ها مبنای ارائه راهکارها قرار گرفتند.

شکل شماره ٦. مراحل تجزیه‌وتحلیل کمی این پژوهش

بر اساس این مراحل، نتایج حاصل از تجزیه‌وتحلیل کمی نشان‌دهنده چالش‌های اصلی در پیاده‌سازی خدمات ابری در سازمان‌های دفاعی است:

- **چالش امنیت اطلاعات**: (٤٠٪) از پاسخ‌دهندگان (بالاترین درصد) این چالش را بزرگ‌ترین مشکل ذکر کردند؛
- **مدیریت هویت و دسترسی**: ۲۵٪ از پاسخ‌دهندگان نگرانی‌هایی درباره مدیریت هویت داشتند؛
- **زیرساخت‌های قدیمی**: ۲۰٪ از پاسخ‌دهندگان اشاره کردند که زیرساخت‌های موجود مانع از انتقال به خدمات ابری می‌شود؛
- **عدم اطمینان از تأمین‌کنندگان خدمات ابری**: ۱۵٪ از پاسخ‌دهندگان نگران امنیت داده‌ها در دست تأمین‌کنندگان بودند.

تجزیه‌وتحلیل کمی داده‌های این مقاله نشان‌دهنده اهمیت شناسایی چالش‌ها و فرصت‌های موجود در پیاده‌سازی خدمات ابری در سازمان‌های دفاعی است. بر اساس

تفسیر این تجزیه‌وتحلیل سازمان‌های دفاعی باید موارد زیر را انجام دهند تا بتوانند از مزایای رایانش ابری بهره‌مند شوند:

- ❖ باید بر روی توسعه سیاست‌های امنیتی قوی تمرکز کنند تا از اطلاعات حساس خود محافظت کنند؛
- ❖ آموزش کارکنان در زمینه امنیت سایبری ضروری است تا آگاهی آن‌ها نسبت به تهدیدات افزایش یابد؛
- ❖ ارتقا زیرساخت‌های فناوری اطلاعات برای همخوانی با خدمات ابری باید مورد توجه قرار گیرد.

٤-۳-۲. تجزیه‌وتحلیل کیفی

تجزیه‌وتحلیل کیفی در این مقاله به بررسی عمیق‌تر نظرات و تجربیات جمع‌آوری‌شده از پاسخ‌دهندگان و خبرگان در زمینه خدمات ابری در سازمان‌های دفاعی پرداخته است. این نوع تحلیل به شناسایی مضامین کلیدی، الگوها و روابط موجود در داده‌ها کمک می‌کند. مضامین کلیدی همچون «چالش‌های امنیتی»، «مدیریت هویت»، «زیرساخت‌های فناوری اطلاعات» و «آموزش کارکنان» شناسایی شدند.

٤-۳-۲-۱. مراحل تجزیه‌وتحلیل کیفی

تجزیه‌وتحلیل کیفی این پژوهش در چند مرحله انجام شده است:

٤-۳-۲-۱-۱. گردآوری داده‌ها

داده‌های کیفی از طریق مصاحبه‌های نیمه‌ساختاریافته با ۱۰ نفر از خبرگان حوزه خدمات ابری و امنیت سایبری گردآوری شد. این افراد بر اساس معیارهایی مانند تخصص در فناوری اطلاعات و تجربه عملی در پروژه‌های مرتبط با خدمات ابری انتخاب شدند.

٤-۳-۲-۱-۲. کدگذاری اولیه

متن مصاحبه‌ها به‌طور دقیق پیاده‌سازی و در نرم‌افزار MAXQDA وارد شد. سپس کدهای اولیه از داده‌ها استخراج شدند.

۳-۱-۲-۳-٤. شناسایی مضامین

با استفاده از روش تحلیل مضمون، کدهای مشابه ترکیب و مضامین کلیدی مانند «چالش‌های امنیتی»، «مدیریت هویت»، «زیرساخت‌های فناوری اطلاعات» و «آموزش کارکنان» شناسایی شدند.

٤-۱-۲-۳-٤. اعتبارسنجی مضامین

نتایج استخراج‌شده با بازبینی توسط سه نفر از خبرگان تأیید و اصلاح شدند تا دقت و صحت مضامین تضمین شود.

۵-۱-۲-۳-٤. تفسیر نتایج

بر اساس یافته‌های نهایی، چالش‌های امنیتی و نیاز به مدیریت هویت از مهم‌ترین موانع پذیرش خدمات ابری در سازمان‌های دفاعی هستند. همچنین، آموزش کارکنان و بروزرسانی زیرساخت‌ها به‌عنوان راهکارهای پیشنهادی جهت غلبه بر این چالش‌ها شناسایی شدند.

نتایج تجزیه‌وتحلیل کیفی نشان‌دهنده چالش‌های اصلی در پیاده‌سازی خدمات ابری در سازمان‌های دفاعی است:

- ❖ چالش امنیت اطلاعات: بسیاری از پاسخ‌دهندگان بر اهمیت امنیت اطلاعات تأکید کردند و آن را بزرگ‌ترین مانع برای پذیرش خدمات ابری دانستند؛
- ❖ مدیریت هویت و دسترسی: نگرانی‌هایی درباره مدیریت هویت کاربران و دسترسی غیرمجاز مطرح شد که نیاز به سامانه‌های قوی برای مدیریت هویت را نشان می‌دهد؛
- ❖ زیرساخت‌های قدیمی: برخی پاسخ‌دهندگان اشاره کردند که زیرساخت‌های موجود مانع از انتقال به خدمات ابری می‌شود؛
- ❖ آموزش کارکنان: نیاز به آموزش کارکنان در زمینه امنیت سایبری و استفاده مؤثر از خدمات ابری مورد تأکید قرار گرفت.

تفسیر تجزیه‌وتحلیل کیفی نشان می‌دهد که:

- ❖ سازمان‌های دفاعی باید بر روی توسعه سیاست‌های امنیتی قوی تمرکز کنند تا از اطلاعات حساس خود محافظت کنند؛
- ❖ آموزش کارکنان در زمینه امنیت سایبری ضروری است تا آگاهی آن‌ها نسبت به تهدیدات افزایش یابد؛
- ❖ ارتقا زیرساخت‌های فناوری اطلاعات برای هم‌خوانی با خدمات ابری باید مورد توجه قرار گیرد.

۳-۳-٤. تجزیه‌وتحلیل امنیتی

تحلیل امنیتی این مقاله به بررسی چالش‌ها و فرصت‌های امنیتی مرتبط با پیاده‌سازی خدمات ابری در سازمان‌های دفاعی می‌پردازد. این تحلیل شامل شناسایی تهدیدات امنیتی، ارزیابی مخاطره‌ها و ارائه راهکارهای مناسب برای کاهش این تهدیدات است.

۱-۳-۳-٤. شناسایی تهدیدات امنیتی

مقاله به شناسایی چندین تهدید امنیتی کلیدی در زمینه خدمات ابری در سازمان‌های دفاعی می‌پردازد:

۱-۱-۳-۳-٤. نقض داده‌ها

احتمال دسترسی غیرمجاز به اطلاعات حساس نظامی و راهبردی که می‌تواند منجر به افشای اطلاعات حیاتی شود.

۲-۱-۳-۳-٤. حملات سایبری

تهدیدات ناشی از حملات محروم‌سازی توزیع‌شده از خدمت، بدافزارها و حملات هدفمند که می‌تواند به زیرساخت‌های ابری آسیب برساند.

۳-۱-۳-۳-٤. مدیریت هویت و دسترسی

خطرات ناشی از عدم سامانه‌های مؤثر برای مدیریت هویت کاربران، می‌تواند به دسترسی غیرمجاز منجر شود.

۲-۳-۳-٤. ارزیابی مخاطره‌ها

برای هر یک از تهدیدات شناسایی‌شده، ارزیابی مخاطره انجام شده است:

۱-۲-۳-۳-٤. نقض داده‌ها

مخاطره بالا به دلیل حساسیت اطلاعات و احتمال بالای افشا.

٤-۳-۳-۲-۲. حملات سایبری

مخاطره متوسط تا بالا، بسته به نوع حمله و آمادگی سازمان برای مقابله.

٤-۳-۳-۲-۳. مدیریت هویت و دسترسی

مخاطره متوسط به‌ویژه در سازمان‌هایی که سامانه‌های مدیریت هویت ضعیفی دارند.

٤-۳-۳-۳. تحلیل نقاط ضعف

تحلیل نقاط ضعف موجود در زیرساخت‌های فناوری اطلاعات سازمان‌های دفاعی نیز در این مقاله مورد توجه قرار گرفته است:

٤-۳-۳-۳-۱. زیرساخت‌های قدیمی

بسیاری از سازمان‌ها هنوز به زیرساخت‌های فناوری اطلاعات قدیمی وابسته‌اند که قابلیت یکپارچگی با خدمات ابری را ندارند.

٤-۳-۳-۳-۲. کمبود منابع انسانی

فقدان متخصصان کافی در زمینه امنیت سایبری و فناوری اطلاعات.

علاوه‌بر این، استفاده از راهنمای تدوین راهبردی ملی امنیت سایبری ارائه‌شده توسط اتحادیه بین‌المللی مخابرات، به‌عنوان یک چارچوب ساختاریافته، به شناسایی و اولویت‌بندی مسائل راهبردی خدمات ابری در سازمان‌های دفاعی کمک کرده است. این راهنما به نویسندگان مقاله این امکان را داد تا مسائل کلیدی مانند امنیت اطلاعات، مدیریت هویت و دسترسی، و زیرساخت‌ها را به‌طور نظام‌مند بررسی و اولویت‌بندی کنند. این چارچوب به‌عنوان یک ابزار راهبردی، به سازمان‌ها کمک می‌کند تا با رویکردی جامع و مبتنی بر استانداردهای جهانی، به توسعه خدمات ابری امن بپردازند.

٤-۳-٤. تجزیه‌وتحلیل هزینه‌ای

تحلیل هزینه‌ای، یک ابزار کلیدی در مدیریت مالی و برنامه‌ریزی است که به سازمان‌ها کمک می‌کند تا هزینه‌های مرتبط با پروژه‌ها و خدمات را شناسایی، ارزیابی و مدیریت کنند. در این بخش، تحلیل هزینه‌ای مقاله موردنظر به تفصیل بررسی می‌شود.

٤-۳-٤-۱. شناسایی هزینه‌ها

در ابتدا شناسایی هزینه‌های مرتبط با پیاده‌سازی خدمات ابری در سازمان‌های دفاعی ضروری است. این هزینه‌ها می‌توانند به دسته‌های زیر تقسیم شوند:

۱-۱-٤-۳-٤. هزینه‌های مستقیم

- ❖ هزینه نرم‌افزار و سخت‌افزار: خرید یا اجاره زیرساخت‌های ابری، نرم‌افزارهای امنیتی و ابزارهای مدیریت.
- ❖ هزینه نیروی انسانی: استخدام متخصصان فناوری اطلاعات و امنیت سایبری برای پیاده‌سازی و نگهداری سامانه‌ها.

۲-۱-٤-۳-٤. هزینه‌های غیرمستقیم

- ❖ آموزش کارکنان: هزینه‌های مرتبط با آموزش کارکنان برای استفاده از خدمات ابری و آشنایی با پروتکل‌های امنیتی.
- ❖ هزینه‌های پشتیبانی: هزینه‌های مرتبط با پشتیبانی فنی و نگهداری سامانه‌ها.

۲-٤-۳-٤. تحلیل هزینه-فایده

تحلیل هزینه-فایده به مقایسه هزینه‌ها و منافع حاصل از پیاده‌سازی خدمات ابری کمک می‌کند. این تحلیل شامل مراحل زیر است:

۱-۲-٤-۳-٤. شناسایی منافع

- ❖ کاهش هزینه‌های عملیاتی: با استفاده از خدمات ابری، سازمان‌ها می‌توانند هزینه‌های مربوط به نگهداری زیرساخت‌های فیزیکی را کاهش دهند.
- ❖ افزایش کارایی: بهبود در دسترسی به اطلاعات و منابع، که می‌تواند به افزایش بهره‌وری کارکنان منجر شود.

۲-۲-٤-۳-٤. محاسبه نسبت هزینه به فایده

- ❖ محاسبه نسبت کل هزینه‌ها به کل منافع برای تعیین اینکه آیا مزایای حاصل از پیاده‌سازی خدمات ابری بیشتر از هزینه‌ها است یا خیر.

بر اساس تحلیل انجام‌شده، پیاده‌سازی خدمات ابری در سازمان‌های دفاعی می‌تواند به کاهش قابل‌توجهی در هزینه‌ها و افزایش کارایی منجر شود. نسبت هزینه به فایده کمتر از یک نشان‌دهنده این است که مزایای حاصل از این پروژه بیشتر از هزینه‌ها است. تحلیل

هزینه‌ای این پژوهش نشان‌دهنده اهمیت شناسایی دقیق هزینه‌ها و ارزیابی منافع حاصل از پیاده‌سازی خدمات ابری است. با استفاده از این تحلیل، مدیران می‌توانند تصمیمات مؤثرتری اتخاذ کنند که به بهبود عملکرد سازمان کمک کند.

۵. نتیجه‌گیری و پیشنهادات

۵-۱. نتیجه‌گیری

خدمات ابری به‌عنوان یک فناوری برهم‌زن انقلابی، می‌تواند در حوزه‌های مختلف دفاعی مورد استفاده قرار گیرد. بررسی مطالعات اکتشافی صورت‌گرفته در این پژوهش نشان داد که سیاست‌گذاری دولت‌ها در توسعه خدمات ابری نقش قابل‌توجهی دارند؛ سازمان‌های دفاعی جمهوری اسلامی ایران می‌توانند با اتخاذ سیاست‌های مناسب فرایند توسعه این فناوری در صنعت دفاعی کشور را سرعت ببخشند.

مشارکت ذی‌نفعان و بازیگران مختلف، یکی از اشتراکات سیاست‌گذاری کشورهای منتخب در توسعه خدمات ابری من است که در نتایج مطالعات حاصل شد؛ و با یافته‌های مطالعه حاضر در الگوی مفهومی خدمات ابری من در سازمان‌های دفاعی همسو است. به همین منظور برای مواجهه فعالانه و هوشمندانه با این فناوری و استفاده از فرصت‌های فراوان پیش‌رو ضروری است که سازمان‌های دفاعی در توسعه خدمات ابری امن مطابق با مدل مفهومی تدوین‌شده در این پژوهش (شکل ۲) با به‌رسمیت‌شناختن ذی‌نفعان و بازیگران و برقراری تعاملات پایدار میان عرضه خدمات و تقاضا خدمات به شکل‌گیری جریان توسعه این فناوری کمک کنند.

این تحقیق به شناسایی و اولویت‌بندی مسائل راهبردی خدمات ابری در سازمان‌های دفاعی با رویکرد جهانی پرداخته است. بر اساس یافته‌های پژوهش، مهم‌ترین چالش‌های شناسایی‌شده عبارت‌اند از: امنیت اطلاعات، مدیریت هویت و دسترسی، زیرساخت‌های قدیمی، و عدم اطمینان به تأمین‌کنندگان خدمات ابری. این مسائل به‌عنوان اولویت‌های اصلی در پیاده‌سازی و توسعه خدمات ابری در سازمان‌های دفاعی شناسایی شده و پیشنهاداتی برای مقابله با آن‌ها ارائه گردید. از جمله این پیشنهادات می‌توان به ارتقای

سیاست‌های امنیتی، آموزش کارکنان، بروزرسانی زیرساخت‌ها، و ایجاد سامانه‌های مدیریت هویت اشاره کرد.

مدل مفهومی طراحی‌شده در این پژوهش به‌عنوان ابزاری برای سازماندهی و تحلیل مسائل راهبردی مورد استفاده قرار گرفت و ساختاری منسجم برای درک و تحلیل چالش‌ها و فرصت‌ها ارائه داد. با این‌وجود، تمرکز اصلی تحقیق بر شناسایی و اولویت‌بندی مسائل بود تا راهکارهایی عملی و مبتنی بر نیازهای سازمان‌های دفاعی برای توسعه خدمات ابری ارائه گردد.

در بخش‌های انتهایی پژوهش تجزیه‌وتحلیل یافته‌ها در خصوص شناسایی مسائل راهبردی خدمات ابری در سازمان‌های دفاعی انجام شد. بر این اساس باید نیروی انسانی همانند سرمایه انسانی در نظر گرفته شود که می‌تواند به‌عنوان نیروی محرکه دانشگاه‌ها، مراکز تحقیقاتی و صنعتی ایفای نقش کند. مسائل خدمات ابری امن در سازمان‌های دفاعی می‌تواند موانع غیرضروری و غیرعمدی را حذف کند، همگرایی و هم‌افزایی در سطح دفاعی ایجاد کند و نیازهای سازمان‌های دفاعی را برآورده سازد.

سازمان‌های دفاعی ج.ا.ایران با درس‌آموزی از راهبردهای سایر کشورها باید درصدد ایفای نقشی فعال در استانداردگذاری جهانی و منطقه‌ای خدمات ابری به‌عنوان مؤلفه‌ای مهم در قدرت رهبری با به رسمیت شناختن ذی‌نفعان و بازیگران و مدیریت این فناوری باشد (شکل ۳). سازمان‌های دفاعی می‌توانند با سیاست‌گذاری و حمایت‌های مالی و غیرمالی و استفاده از ظرفیت شرکت‌های دانش‌بنیان نیروهای مسلح شرایط این سازمان‌ها را برای توسعه این فناوری آماده سازند و با تدابیر خود رقابت را در سمت عرضه و پذیرش و استفاده را در جانب تقاضا ایجاد کنند. متولیان حوزه دفاعی کشور بر اساس مسائل ارائه‌شده در این پژوهش قادر خواهند بود جهت عملیاتی‌کردن خدمات ابری امن در سازمان‌های دفاعی در کشور برنامه‌ریزی کنند.

۲-۵. پیشنهادات

پیشنهادهای این پژوهش به دو بخش تقسیم می‌شود:

الف. پیشنهادهای پژوهشی (علمی و ابتکاری)؛

ب. پیشنهادها و راهکارهای اجرایی.

لازم به ذکر است که پژوهش حاضر با بررسی اسناد بالادستی و برنامه‌های نظام ج.ا.ایران همانند برنامه هفتم توسعه، تدوین شده است؛ بنابراین امید است علاوه‌بر سازمان‌های دفاعی، دولت و مجلس شورای اسلامی نیز در تدوین برنامه‌های بعدی توسعه کشور که از جنس هویت رقمی بوده، از پیشنهادهای ذیل استفاده کنند:

۱-۲-۵. پیشنهادهای اجرایی

- وزارت دفاع و پشتیبانی نیروهای مسلح با همکاری سازمان‌های دفاعی نسبت به راه‌اندازی آزمایشگاه‌های مرجع تخصصی جهت تست امنیتی تجهیزات ابری اقدام نماید.
- سازمان مرجع نیروهای مسلح (ستاد کل ن م) نسبت به تدوین دستورالعمل استانداردسازی نرم‌افزارها، پروتکل‌ها و فرایندهای ارتباطات خدمات ابری اقدام نماید.
- سازمان مرجع نیروهای مسلح (ستاد کل ن م) نسبت به تکمیل شبکه نیروهای مسلح برای توسعه این شبکه به کلیه سازمان‌های دفاعی، با تضمین شبکه‌ای پرسرعت، امن و مطمئن در کل کشور اقدام نماید.
- سازمان مرجع نیروهای مسلح (ستاد کل ن م) اولویت‌بندی توسعه خدمات و فناوری‌های ابری در حوزه‌های دفاعی را در دستورکار قرار دهد.
- سازمان مرجع نیروهای مسلح (ستاد کل ن م) نسبت به اعمال ملاحظات امنیتی در تولید و خرید تجهیزات ارتباطی، حسگرها و سکوهای توسعه خدمات ابری به‌صورت بومی و با بهره‌گیری از فناوری‌های نوین جهت مقابله با تهدیدات سایبری اقدام کند.

- ❖ سازمان مرجع نیروهای مسلح (ستاد کل ن م) و وزارت دفاع و پشتیبانی نیروهای مسلح تربیت نیروی انسانی متخصص نیازمند خدمات ابری امن بر اساس نیازمندی‌های اولویت‌دار دفاعی کشور را اجرایی نمایند.
- ❖ سازمان مرجع نیروهای مسلح (ستاد کل ن م) با ایجاد شبکه دفترکل توزیع شده[1] اختصاصی دفاعی امکان ورود اطلاعات دفاعی از طریق ابر در این شبکه را فراهم نماید.

همان‌طور که در بخش یافته‌های تحقیق اشاره شد، چالش‌های اصلی در حوزه خدمات ابری امن شامل امنیت اطلاعات، مدیریت هویت و دسترسی، زیرساخت‌های قدیمی و نیاز به آموزش کارکنان بوده است. پیشنهادهای پژوهشی زیر به‌طور مستقیم از این چالش‌ها و نیازها نشئت گرفته‌اند و هدف آنها ارائه راهکارهایی برای رفع این مسائل و بهبود وضعیت خدمات ابری در سازمان‌های دفاعی است؛ به‌عنوان مثال، پیشنهادهای مربوط به امن‌سازی شبکه و تدوین سند محرمانگی داده‌ها، از نگرانی‌های امنیتی شناسایی‌شده در تحقیق و پیشنهادهای مربوط به بومی‌سازی معماری خدمات ابری و استفاده از هوش مصنوعی از نیاز به تطبیق فناوری‌های نوین با الزامات خاص حوزه دفاعی نشئت گرفته‌اند.

۲-۲-۵. پیشنهادهای پژوهشی

۱-۲-۲-۵. تدوین پژوهشی در راستای تبیین زیست‌بوم خدمات ابری امن در سازمان‌های دفاعی

بر اساس یافته‌های تحقیق که نشان‌دهنده نیاز به هماهنگی بین بازیگران مختلف در حوزه خدمات ابری است، پیشنهاد می‌گردد پژوهشی برای شناسایی و تحلیل روابط و تعامل بین ذی‌نفعان اصلی (ارائه‌دهندگان خدمات، سازمان‌های دفاعی و نهادهای نظارتی) انجام شود.

۲-۲-۲-۵. تدوین پژوهشی در راستای ارائه الگوی نظارت، ارزیابی و کنترل توسعه خدمات ابری امن

با توجه به چالش‌های امنیتی و نیاز به نظارت مستمر بر خدمات ابری، پیشنهاد می‌گردد الگویی برای نظارت و ارزیابی عملکرد خدمات ابری در سازمان‌های دفاعی طراحی شود.

1. Blockchain

۵-۲-۲-۳. تدوین پژوهشی در خصوص معماری خدمات ابری امن و بومی‌سازی آن

نیاز به تطبیق معماری خدمات ابری با الزامات امنیتی و سازمانی خاص حوزه دفاعی، تدوین پژوهشی برای طراحی و بومی‌سازی معماری امن خدمات ابری را ضروری می‌سازد.

۵-۲-۲-٤. تدوین پژوهشی به‌منظور تدوین سند نظام محرمانگی، حق دسترسی و استقلال سازمانی داده‌های دفاعی

بر اساس یافته‌های تحقیق که نشان‌دهنده نگرانی‌های مربوط به حریم خصوصی و امنیت داده‌ها است، پیشنهاد می‌گردد سندی برای تعیین چارچوب‌های محرمانگی و دسترسی به داده‌های دفاعی تدوین شود.

۵-۲-۲-۵. تدوین پژوهش الگوی مدیریت راهبردی هوش مصنوعی در داده‌کاوی داده‌های دفاعی

با درنظر گرفتن نیاز به تحلیل داده‌های حجیم و پیچیده در سازمان‌های دفاعی، پیشنهاد می‌گردد الگویی برای استفاده از هوش مصنوعی در داده‌کاوی داده‌های دفاعی طراحی شود.

۵-۲-۲-٦. تدوین پژوهش مدیریت راهبردی فناوری‌های نوین و همگرا با خدمات ابر

با توجه به نیاز به همگرایی فناوری‌های نوین (مانند اینترنت اشیاء، هوش مصنوعی و بلاکچین) با خدمات ابری، پیشنهاد می‌گردد پژوهشی برای مدیریت راهبردی این فناوری‌ها انجام شود.

۵-۲-۲-۷. تدوین پژوهشی در خصوص راهبردهای هوشمندسازی سازمان‌های دفاعی

با توجه به نیاز به استفاده از فناوری‌های نوین برای بهبود کارایی و امنیت سازمان‌های دفاعی، پیشنهاد می‌گردد راهبردهایی برای هوشمندسازی این سازمان‌ها تدوین شود.

منابع

الف- فارسی

- اشتهاردی شاه‌بیک، محمدامین (۱۳۹۳). ***سند تحلیل روند و نقشه مفهومی فناوری‌های پایگاه‌داده و رایانش ابری***، پروژه نخبگان، تهران: دانشگاه صنعتی مالک اشتر.
- آقایی، محمد (۱٤۰۱). «آشنایی با معماری رایانش ابری و معمار ابری»، ***سایت سپیدار سیستم***.
- رحمتی لارهنگ، مهدی؛ مهدی‌نژاد نوری، محمد؛ طالبی، مرتضی؛ و اسکندری، حسین (۱٤۰۱). «ارائه الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی جمهوری اسلامی ایران»، ***فصلنامه مطالعات راهبردی فضای سایبر***، ۲(۳)، ۸۹-۱۲.
- عبدی، فریدون (۱۳۹۰). «سامانهٔ فرماندهی و کنترل I٤C و بررسی نقش رایانه‌ها در آن»، ***فصلنامه مدیریت نظامی***، ۱۱(٤۲)، ۷۰-٤۳.
- عبدی‌پور، سانیا (۱٤۰۲). «آشنایی با معماری رایانش ابری و معمار ابری»، ***سایت سپیدار سیستم***.
- غضنفرپور، مجید؛ موسوی، سید مجید (۱٤۰۰). «معماری به‌کارگیری رایانش ابری در سازمان‌ها»، ***همایش تخصصی مهندسی دفاعی با عنوان «تهدیدات سایبرالکترونیک»***.
- مهدی‌نژاد نوری، محمدرضا؛ سعادتی، مجتبی؛ خسروجردی، علی؛ فخری، مجید (۱۳۹٦). «طراحی الگوی سازمان‌های دفاعی دانش‌بنیان»، ***فصلنامه علمی-پژوهشی مطالعات دفاعی راهبردی***، ۱۵(٦۸)، ۹۲-۷۱.
- ولوی، محمدرضا؛ موحدی صفت، محمدرضا (۱۳۹۵). «ارائه یک مدل معماری بومی رایانش ابری در بخش دفاعی»، ***فصلنامه امنیت ملی***، ٦(۱۹)، ۱٦۹-۱٤۷.
- ولوی، محمدرضا؛ موحدی صفت، محمدرضا (۱۳۹۷). «ارائه یک چارچوب معماری امن برای شبکه دفاعی کشور»، ***فصلنامه علمی-پژوهشی مطالعات دفاعی استراتژیک***، ۱٦(۷۳)، ٤٦-۲۷.
- ولوی، محمدرضا؛ موحدی صفت، محمدرضا؛ باقری کوشالشاه، ایمان (۱۳۹٦). «ارائه الگوی راهبردی مهاجرت سازمان‌های دفاعی به محیط رایانش ابری»، ***فصلنامه مدیریت نظامی***، ۱۷(٦۵)، ۱۰٦-۱۳۰.

ب- انگلیسی

- Alavizadeh, H., Aref, S., Kim, D. S., & Jang-Jaccard, J. (2022). Evaluating the security and economic effects of moving target defense techniques on the cloud. ***IEEE Transactions on Emerging Topics in Computing***, *10*(4), pp. 1772-1788.
- AlDaajeh, S.; Alrabaee, S. (2024). Strategic cybersecurity. ***Computers & Security***, *141*, 103845.
- Alkhafaji, A.; & Nelson, R. A. (2013). ***Strategic management: formulation, implementation, and control in a dynamic environment***, Routledge.
- Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies, ***Ieee Access***, *9*, pp. 57792-57807.
- Ardagna, D. (2015). ***Cloud and multi-cloud computing: current challenges and future applications***, In *2015 IEEE/ACM 7th International Workshop on Principles of Engineering Service-Oriented and Cloud Systems* (pp. 1-2). IEEE.
- Balashova, S. A., & Musin, T. I. (2022). Cloud computing: global trends and challenges for Russia in the time of sanctions. ***R-Economy***. *2022. Vol. 8. Iss. 3*, *8*(3), pp. 268-280.
- Chan, K., Singh, S., Ramaya, R., & Lim, K. H. (2005). ***Spirit & System: Leadership Development for a Third Generation SAF*** [4th Pointer Monograph].
- Chinchole, A. (2022). ***Why is cloud security important?***, Cloudlytics. Available at: https://cloudlytics.com/why-is-cloud-security-important.
- Cloud Security Alliance (2021). ***CSA enterprise architecture reference guide,*** **Cloud Security Alliance**, Available at: https://cloudsecurityalliance.org/artifacts/enterprise-architecture-reference-guide-v2
- Consensus Editorial (2022). ***Cloud security definition*****. Consensus**, Available at: https://www.consensus.com/cloud/security/
- David, F. R. (2011). ***Strategic management concepts and cases***, Prentice hall.
- Department of Defense (2021). ***Department of Defense outside the Continental United States (OCONUS) cloud strategy***, Office of the DOD Chief Information Officer.

- D'Silva, F. (2023). **How to improve cloud security: 9 expert strategies.** ***Ntiva***, Available at https://www.ntiva.com/blog/9-tips-for-improving-cloud-computing-security.
- El Kafhali, S., El Mir, I., & Hanini, M. (2022). ***Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering***, *29*(1), pp.223-246.
- Gompert, D. C., Lachow, I., Perkins, J., Smith, R. C., & Wells, L. (2006). ***Battle-Wise: Seeking Time-Information Superiority in Networked Warfare***, Center for Technology and National Security Policy.
- Guffey, J.; Li, Y. (2023). ***Cloud Service Misconfigurations: Emerging Threats, Enterprise Data Breaches and Solutions***. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0806-0812). IEEE.
- Gupta, Y; Vashisth, R. (2023). ***Cyber Threats in Cloud Computing Environment***. In *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 548-555). IEEE.
- Jasti, A., Shah, P., Nagaraj, R., & Pendse, R. (2010). ***Security in multi-tenancy cloud***, In *44th Annual 2010 IEEE International Carnahan Conference on Security Technology* (pp. 35-41). IEEE.
- McKinsey & Company (2022). **Cloud in China: The outlook for 2025.** ***McKinsey***, Available at https://www.mckinsey.com/ capabilities /mckinsey-digital/our-insights/cloud-in-china-the-outlook-for-2025
- Microsoft Azure (2021). ***What is cloud computing? A beginner's guide, Microsoft***, Available at: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#benefits.
- Pacheco, M (2023). **Private cloud architecture: A complete overview.** ***TierPoint***, Available at: https://www.tierpoint.com/blog/ private-cloud-architecture/
- Reddy, J. M.; Monika, J. M. (2012). ***Integrate military with distributed cloud computing and secure virtualization***. In *2012 SC Companion: High Performance Computing, Networking Storage and Analysis* (pp. 1200-1206). IEEE.
- Rishika, S. (2024). ***Cloud storage of military data: Risks and opportunities in active war zones***,NASSCOM.
- Sangfor Technologies. (2023). ***What is Security as a Service (SECaaS)?*** Sangfor, Available at: https://www.sangfor.com/ glossary/ cybersecurity/ what-is-security-service-secaas

- Правительство Российской Федерации. (2023). ***Правительство утвердило Стратегию развития отрасли связи до 2035 года***. Government.ru, Available at http://government.ru/news/50304/.