فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره ۲، بهار ۱۴۰۱
مقاله سوم، از صفحات ۸۰-۶۳

بررسی الزامات بهره‌برداری از فناوری اینترنت اشیاء در سامانه فرماندهی و کنترل

محمدرضا موحدی‌صفت[۱]، رسول رمضانی دهقی[۲]

تاریخ دریافت: ۱۳۹۹/۱۲/۱۰ تاریخ پذیرش: ۱۴۰۰/۰۷/۱۶

چکیده

فناوری نوظهور اینترنت اشیاء قابلیت ارسال و دریافت داده بین اشیاء مختلف از طریق شبکه‌های ارتباطی را فراهم کرده و می‌تواند منشأ ایجاد تغییراتی شگرف در تجهیزات نظامی شده و همچنین موجب ارتقاء کارایی بخش‌های دفاعی گردد. سامانه فرماندهی و کنترل یکی از مهم‌ترین بخش‌های حوزه دفاع است که می‌تواند با ورود فناوری اینترنت اشیاء متحول گردد. فرماندهی و کنترل عبارت است از برنامه‌ریزی، هدایت، هماهنگی و کنترل عملیات مبتنی بر اجرای مؤثر سناریوی عملیاتی، بنابراین جهت دستیابی به بهترین نتیجه، داشتن اطلاعات کامل، دقیق و درزمان امری حیاتی است. از طرفی بهره‌گیری از فناوری اینترنت اشیاء این امکان را به فرماندهان می‌دهد تا در کمترین زمان ممکن به بیشترین و دقیق‌ترین اطلاعات مربوط به صحنه نبرد دست یابند. این پژوهش با هدف بررسی الزامات موردنیاز جهت بهره‌برداری از فناوری اینترنت اشیاء در سامانه فرماندهی و کنترل انجام‌شده است.

پژوهش حاضر به لحاظ هدف از نوع کاربردی و به لحاظ روش از نوع توصیفی (موردی) و با رویکرد آمیخته (کمی و کیفی)، کمی به‌صورت آمار توصیفی و کیفی به روش تحلیل محتوا می‌باشد. جامعه آماری پژوهش افراد آگاه و خبره در خصوص موضوعات فضای سایبر و همچنین فرماندهی و کنترل بودند که تعداد ۳۰ نفر از آن‌ها به‌صورت هدفمند انتخاب و پرسشنامه در مورد آن‌ها اجرا گردید.

نتایج بدست آمده نشان می‌دهد جهت به‌کارگیری اینترنت اشیاء در سامانه فرماندهی و کنترل، بایستی در سه لایه برنامه، دریافت، شبکه و زیرساخت نسبت به ارتقاء و بومی‌سازی نرم‌افزارها، بهره‌گیری از وصله‌های امنیتی پویا، اطمینان از سلامت ریزپردازنده‌ها، تأمین امنیت حسگرهای کشف و شناسایی، بهره‌گیری از رمزنگاری، تأمین دسترس‌پذیری شبکه، تطبیق پروتکل‌ها، مقیاس‌پذیری شبکه، ایجاد ابر اختصاصی، تأمین حفاظت فیزیکی و تأمین انرژی حسگرها اقدام نمود.

کلیدواژه‌ها: اینترنت اشیاء، دسترس‌پذیری، تطبیق پروتکل‌ها، فرماندهی و کنترل.

۱- دانشیار دانشگاه عالی دفاع ملی.

۲ - دانشجوی مقطع دکتری دانشگاه عالی دفاع ملی (نویسنده مسئول) r.ramezany@sndu.ac.ir

۱. مقدمه

اینترنت اشیاء[1] یک ایده جهانی برای اتصال همه اشیاء به یکدیگر است. حوزه‌های انرژی، سلامت، حمل‌ونقل، تولید، صنایع هوایی و نیز صنایع نظامی و دفاعی حوزه‌های کاربردی این ایده جهانی خواهند بود. در این میان حوزه‌های نظامی و دفاعی به دلیل وجود تعاملات گسترده با بخش غیرنظامی و نیز بهره‌گیری از فناوری‌های پیشرفته مختلف از اهمیت ویژه‌ای برخوردارند. از طرفی استفاده از اینترنت اشیا حجم بی‌سابقه‌ای از اطلاعات را در اختیار واحدهای نظامی قرار می‌دهد که تأثیر زیادی بر نحوه عمل نیروهای نظامی در حین عملیات و جنگ خواهد داشت (وب‌سایت انجمن اینترنت اشیاء ایران، ۱۳۹٦).

فرماندهی و کنترل شامل برنامه‌ریزی، هدایت، هماهنگی و کنترل عملیات و مبتنی بر اجرای مؤثر سناریوی عملیاتی می‌باشد؛ اما باید توجه داشت که وظیفه اصلی آن تصمیم‌سازی است. فرماندهی و کنترل مؤثرترین اقدام به‌ویژه درزمانی است که برتری تصمیم‌گیری مدنظر است. برتری تصمیم‌گیری از برتری اطلاعاتی ناشی می‌شود که درواقع مبتنی بر تجربه، دانش، آموزش و قضاوت فرماندهان است. یک فرمانده باید آخرین تحولات صحنه نبرد را مدنظر داشته باشد و دستورات لازم را برای مقابله با متغیرهای پیش‌بینی‌نشده صادر کرده و برای نیروهای عملیاتی ارسال و بر فرآیند عملیات اشراف کامل داشته باشد.

تکامل فناوری اطلاعات به نحو فزاینده‌ای به نیروهای نظامی اجازه خواهد داد که اشکال سنتی عملیات اطلاعاتی را با منابع پیچیده اطلاعاتی، نظارت و تجسس در قالب یک حرکت اطلاعاتی، هماهنگ نمایند. توسعه یک مفهوم با عنوان شبکه اطلاعات جهانی، محیط شبکه‌ای لازم برای دستیابی به این هدف را فراهم می‌سازد. این شبکه در سراسر جهان گسترده شده، پایانه‌های اطلاعاتی و افراد را به یکدیگر مرتبط ساخته، پردازش‌ها را یکپارچه نموده و اطلاعات موردنیاز جنگجویان، تصمیم سازان و پرسنل پشتیبانی‌کننده را فراهم نموده و قدرت رزم را افزایش می‌دهد و به موفقیت عملیات نظامی کمک می‌کند (مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، ۱۳۹۲: ۷).

این پژوهش با هدف بررسی الزامات به‌کارگیری فناوری اینترنت اشیاء **در** سامانه فرماندهی و کنترل، با استفاده از روش توصیفی (موردی) و با رویکرد آمیخته (کمی و کیفی)، کیفی به روش تحلیل محتوا و کمی به‌صورت آمار توصیفی و با استفاده از نرم‌افزار spss انجام گرفت. جامعه آماری پژوهش تعداد ۸۰ نفر افراد آگاه و خبره در خصوص موضوعات فرماندهی و کنترل و همچنین فضای سایبر هستند و حجم نمونه با استفاده از فرمول کوکران در سطح خطای ۵ درصد برابر با ۳۰ نفر به دست می‌آید.

در ادامه مقاله به‌صورت ذیل سازماندهی می‌شود. در بخش ۲ به‌صورت مختصر در مورد مباحث اینترنت اشیاء مطالبی بیان‌شده است. در بخش ۳ مباحث رایانش ابری ارائه‌شده است. بخش ٤ به مبحث فرماندهی و کنترل و اتوماسیون سامانه فرماندهی و کنترل می‌پردازد. در بخش ۵ بهره‌گیری از اینترنت اشیاء در سامانه فرماندهی و کنترل ارائه‌شده است. و در بخش ٦ چالش‌های به‌کارگیری اینترنت اشیاء در سامانه فرماندهی و کنترل تشریح گردیده است. در

[1] **I.O.T (Internet Of Thongs)**

بخش ۷ مدل مفهومی تحقیق ارائه‌شده و در بخش ۸ روش تحقیق بیان گردیده است. در بخش ۹ به تجزیه‌وتحلیل و ارزیابی داده‌ها می‌پردازیم و درنهایت در بخش ۱۰ نتیجه‌گیری و پیشنهادات ارائه می‌گردد.

۲. اینترنت اشیاء فناوری جدید در فضای سایبر

گزارش‌های آینده‌پژوهی در حوزه سایبری موید این مطلب است که روندهای اصلی سایبر در آینده شامل رایانش ابری، داده‌های حجیم، اینترنت اشیاء، اینترنت همراه، رابط مغز و کامپیوتر، پرداخت ارتباطات میدان نزدیک، ربات‌های متحرک، محاسبات کوانتومی و تسلیحات اینترنتی است (محمدی، ۱۳۹۵: ۲). در این میان اینترنت اشیا با ترکیب دو عرصه دیجیتالی و فیزیکی، دسترسی به فناوری اطلاعات را گسترده‌تر خواهد ساخت. امکانات بی‌شمار فراهم‌شده به کمک توانمندی نظارت و کنترلِ الکترونیکی اشیای جهان فیزیکی، الهام‌بخش موج جدیدی از نوآوری خواهد بود (دبیرخانه برنامه ملی آینده‌نگاری علم و فناوری در حوزه فاوا، ۱۳۹۵: ۳).

عبارت اینترنت اشیا نخستین بار در سال ۱۹۹۹ توسط کوین اشتون بکار رفت و در آن جهانی توصیف شد که در آن هر چیزی ازجمله اشیاء بی‌جان برای خود هویت دیجیتال دارند و کامپیوترها این قابلیت را دارند که این اشیا را مدیریت نمایند. درواقع اینترنت اشیا فناوری مدرنی در دنیای مجازی است که هر موجودی اعم از جامدات، گیاهان، حیوانات و انسان‌ها قابلیت ارسال اطلاعات از طریق شبکه‌های ارتباطی اعم از اینترنت و یا اینترانت را داشته باشند (Zheng,& Carter, ۲۰۱۵: ۳).

اینترنت اشیا می‌تواند تغییرات وسیعی در چگونگی نظارت و مدیریت از راه دور بر فعالیت‌های مختلف، ردیابی کالاها، مدیریت دارایی‌های فیزیکی سازمان‌ها و ... ایجاد نماید و منجر به شکل‌گیری چشم‌اندازهای مختلفی برای آینده گردد. توانمندی ایجاد پیوند میان جهان فیزیکی و اینترنت و نیز سایر شبکه‌های داده، پیامدهای عمیقی برای جامعه در زمینه‌های نظامی، اقتصادی، اجتماعی و فرهنگی خواهد داشت. و بیش از تکامل بعدی فناوری اطلاعات، اینترنت اشیا به بازتعریف چگونگی تعامل ما با جهان فیزیکی خواهد پرداخت و شیوه‌های رایانه محوری برای مدیریت زیرساخت‌های عمومی و سازماندهی امور مختلف ایجاد می‌کند (دبیرخانه برنامه ملی آینده‌نگاری علم و فناوری در حوزه فاوا، ۱۳۹۵: ٤).

۲،۱. لایه‌های کلیدی معماری اینترنت اشیاء

لایه‌های کلیدی معماری اینترنت اشیاء عبارت‌اند از (الامپالایام کومار، تایلر، هارشیت، ۱۳۹۵: ۲٤):

لایه برنامه: این لایه از برنامه‌ها و سرویس‌های مختلفی که اینترنت اشیاء ارائه می‌دهد، تشکیل‌شده است. برنامه‌ها و کاربردها شامل شهرهای هوشمند، خانه‌های هوشمند، حمل‌ونقل، مراقبت‌های بهداشتی و ... می‌شوند.

لایه دریافت: این لایه از انواع مختلف فناوری‌های حسی ازجمله حسگرهای دما، حسگرهای ارتعاش، حسگرهای فشار، حسگرهای حرکت و ... تشکیل‌شده است که به دستگاه اجازه می‌دهند سایر اشیاء موجود در محیط پیرامونی را حس کند.

لایه شبکه: این لایه از نرم‌افزار ارتباطات شبکه و همچنین اجزای فیزیکی مانند توپولوژی، سرورها، گره‌های

شبکه و اجزای شبکه که امکان ارتباط شبکه را فراهم می‌آورند، تشکیل‌شده است. هدف اصلی آن انتقال داده‌ها میان دستگاه‌ها و از دستگاه‌ها به گیرنده‌ها می‌باشد.

لایه فیزیکی: لایه فیزیکی شامل سخت‌افزار پایه مانند اجزای فیزیکی، لوازم هوشمند و تجهیزات برقی که به‌عنوان پایه و اساس شبکه‌بندی اشیاء هوشمند عمل می‌کنند، تشکیل‌شده است (الامپالایام کومار، ساتیش، ویلی، تایلر، استاوا، هارشیت، ۱۳۹۵: ٢٤).

۲،۲.اینترنت اشیاء مبتنی بر رایانش ابری[1]

یکی از خروجی‌های اینترنت اشیاء تولید حجم بی‌سابقه‌ای از داده‌ها می‌باشد که ذخیره‌سازی و پردازش این حجم از داده توسط بسیاری از اشیاء متصل به اینترنت امکان‌پذیر نمی‌باشد. ذخیره‌سازی، مالکیت و انقضای داده‌ها به مسائل بااهمیتی در این حوزه تبدیل‌شده است. امروزه اینترنت، ۵ درصد از کل انرژی تولیدشده دنیا را مصرف می‌کند و با گسترش اینترنت اشیاء این مقدار رشد قابل‌توجهی خواهد داشت. بنابراین ایجاد مراکز داده متمرکز نظیر ابرهای اطلاعاتی، تضمینی برای بهره‌وری انرژی و ارتقاء قابلیت اطمینان خواهد بود. داده‌ها باید ذخیره و به‌طور مناسبی برای نظارت هوشمند استفاده شوند (قیصری و دیگران، ۱۳۹۲: ۳۱).

یک چارچوب مفهومی از اینترنت اشیاء مبتنی بر رایانش ابری که به مدل اینترنت اشیاء اینترنت محور معروف است در شکل (۱) آورده شده است این چارچوب نه‌تنها باعث انعطاف‌پذیری در تقسیم هزینه‌های مربوطه به منطقی‌ترین شیوه می‌شود، بلکه بسیار مقیاس‌پذیر نیز می‌باشد. ارائه‌دهندگان خدمات سنجشی می‌توانند به شبکه متصل شده و داده‌های خود را برای استفاده در ابر ذخیره‌سازی ارائه دهند، توسعه‌دهندگان ابزار تحلیلی می‌توانند ابزار نرم‌افزاری خود را ارائه دهند، متخصصان هوش مصنوعی ابزارهای داده‌کاوی و یادگیری ماشینی مفید خود را جهت تبدیل اطلاعات به دانش فراهم می‌آورند و درنهایت طراحان گرافیک کامپیوتر طیف متنوعی از ابزارهای تجسمی را ارائه می‌دهند. رایانش ابری این خدمات را به‌عنوان زیرساخت‌ها، سیستم‌عامل و یا نرم‌افزار در اختیار کاربران قرار می‌دهد و اطلاعات تولیدشده، ابزار مورداستفاده و تجسم ایجادشده با بهره‌برداری از پتانسیل کامل اینترنت اشیاء در حوزه‌های مختلف کارکردی، در پس‌زمینه ناپدید می‌شوند (قیصری و دیگران، ۱۳۹۲: ۳۵).

۱-Cloud Computing

شکل ۱. مدل مفهومی اینترنت اشیاء مبتنی بر رایانش ابری (قیصری و دیگران، ۱۳۹۲: ۳۶).

رایانش ابری یکی از رویکردهای جدید محاسباتی است که در چند سال اخیر موردتوجه بسیار قرارگرفته است و به‌طور فزاینده‌ای در حال گسترش است. دنیای محاسبات به‌سرعت به سمت توسعه نرم‌افزارهایی پیش می‌رود که به‌جای اجرا بر روی رایانه‌های منفرد، به‌عنوان یک سرویس در دسترس میلیون‌ها کاربر قرار داده می‌شوند. از این نقطه‌نظر، رایانش ابری از دید کاربران نهایی ساختاری شبیه به یک توده ابر دارد که به‌واسطه آن می‌توان به برنامه‌های کاربردی از هرجایی از دنیا دسترسی یافت (اکبری، سرگلزایی جوان، ۱۳۹۳: ٤).

رایانش ابری از دید زیرساخت، به‌گونه‌ای از سیستم‌های توزیع‌شده و موازی اطلاق می‌گردد که مجموعه‌ای از رایانه‌های مجازی را که به یکدیگر متصل هستند شامل می‌شود. این رایانه‌ها به‌طور پویا عرضه‌شده و به‌عنوان یک یا چند منبع محاسباتی یکپارچه بر اساس توافقات سطح سرویس ارائه می‌شوند. رایانش ابری بر آن است تا نسل جدیدی از مراکز داده را، با ارائه سرویس‌ها و خدمات در ماشین‌های مجازی شبکه شده به‌صورت پویا، به‌گونه‌ای ممکن سازد که ارائه‌دهندگان خدمات کاربردی بتوانند سرویس‌ها و برنامه‌های کاربردی را با انعطاف‌پذیری و سهولت بیشتری ارائه کنند و کاربران نیز بتوانند از هرجایی از دنیا به برنامه‌های کاربردی دسترسی داشته باشند (اکبری، سرگلزایی جوان، ۱۳۹۳: ۷).

انواع مختلف ابرها عبارت‌اند از: ابر عمومی، ابر خصوصی، ابر گروهی و ابر هیبریدی. با عنایت به اینکه این تحقیق در پی آن است که داده‌های حاصل از اشیاء نظامی را از طریق ابر خصوصی مورد بهره‌برداری قرار دهد، لذا در اینجا فقط ابر اختصاصی توضیح داده می‌شود (شرح کامل مطلب در: اکبری، سرگلزایی جوان، ۱۳۹۳: ۲۵).

ابرهای خصوصی برای استفاده انحصاری یک مشتری ایجاد می‌شوند به‌طوری‌که بتواند بیشترین حد کنترل روی داده، امنیت و کیفیت سرویس را داشته باشد. شرکت صاحب زیرساخت است و روی چگونگی ارائه برنامه‌های کاربردی کنترل دارد. ابرهای خصوصی ممکن است در مرکز داده یک سازمان قرار داشته باشد یا اینکه در مکانی اشتراکی واقع‌شده باشد. ابرهای خصوصی می‌توانند توسط بخش فناوری اطلاعات خود سازمان یا اینکه توسط یک سرویس‌دهنده ابری ایجادشده و مدیریت شوند. در این مدل یک شرکت می‌تواند زیرساخت موردنیاز برای ابر خصوصی را در داخل مرکز داده یک شرکت دیگر نصب، پیکربندی و اجرا کند. این مدل به شرکت‌ها، سطح بالایی از

کنترل را بر روی استفاده منابع ابری آن‌ها می‌دهد (اکبری، محمدکاظم، سرگلزایی جوان، مرتضی، ۱۳۹۳: ۳۰).

۲،۳.اینترنت اشیاء و کاربردهای حوزه نظامی

وزارت دفاع آمریکا در تعریف اینترنت اشیاء بیان می‌دارد که: اینترنت اشیاء شامل دو جنبه پایه است: ۱) خود اینترنت ۲) دستگاه‌های نیمه اتوماتیک (اشیاء)، باقابلیت استفاده از محاسبات ساده، شبکه، مشاهده و احساس و به‌کارگیری این قابلیت‌ها برای حس کردن و اقدام در دنیای فیزیکی (DoD, ۲۰۱۶: ۲). به‌کارگیری فناوری‌های مرتبط با اینترنت اشیاء توسط نیروهای نظامی در درجه اول متمرکز بر برنامه‌های جنگی است. فرماندهی، کنترل، ارتباطات، رایانه، اطلاعات، نظارت و سامانه‌های شناسایی، میلیون‌ها حسگر را برای آگاهی‌بخشی به فرماندهان ارشد و سربازان حاضر در زمین و دریا و هوا در اختیار قرار می‌دهد (Zheng,& Carter, ۲۰۱۵: ۳).

بخش‌های بالقوه یگان‌های نظامی جهت استفاده از فناوری IoT عبارت‌اند از (RTO Task Group, ۲۰۱۵: ۱٤۷):

- لجستیک (فرماندهی و کنترل پشتیبانی و تدارکات عملیات ترکیبی)
- آگاهی وضعیتی (در سطح تاکتیکی یک میدان جنگ ازجمله نظارت، سنجش، شناسایی تهدید، موقعیت هدف، علامت‌گذاری وسایل نقلیه و سربازان، نظارت بر وضعیت و نظارت بر محیط‌زیست)
- مراقبت‌های پزشکی (نظارت بر سلامت میدان جنگ، نظارت بر بیماران و غیره).

بااین‌حال فاصله زیادی بین سامانه‌های موجود با آنچه که برای سامانه‌های نظامی اینترنت اشیاء برنامه‌ریزی‌شده است، وجود دارد. بسیاری از اطلاعات جمع‌آوری‌شده توسط حسگرها مورد تجزیه‌وتحلیل قرار نمی‌گیرند. درحالی‌که ارزش اینترنت اشیاء که اطلاعات آن از طریق اتوماسیون جمع‌آوری‌شده به این است که می‌توان آن‌ها را به‌سرعت به کار گرفت.

در حال حاضر مسائل امنیتی و امکان آسیب‌پذیری آن‌ها در جنگ الکترونیک، مهم‌ترین دلیل عدم به‌کارگیری اینترنت اشیاء در نیروهای نظامی است. باوجود این چالش‌ها، پتانسیل بالایی برای روزآمدسازی جنگ‌افزارها، استفاده از داده‌ها و اتوماسیون جهت حفظ جان سربازان و از طرف دیگر کاهش هزینه‌ها و افزایش کارایی وجود دارد. ازجمله (Zheng,& Carter, ۲۰۱۵: ۳):

- ارتقاء نرم‌افزارهای اینترنت اشیاء باهدف کاهش هزینه.
- مدیریت پایه و بهره‌وری انرژی
- ایجاد و گسترش فناوری‌های مرتبط با اینترنت اشیاء در حوزه‌های مختلف.
- گسترش قابلیت اتصال.
- اتخاذ پوشش امنیتی مشترک برای نرم‌افزارها و دستگاه‌های تجاری.
- تولید پروتکل و استانداردهای مشترک با بخش تجاری.
- یافتن راه‌های ابتکاری برای دسترسی به نوآوری.

- اتخاذ سیاست توسعه نرم‌افزارهای سریع.
- بهره‌گیری از خدمات مبتنی بر وب با حفظ زیرساخت‌های آن.

توانایی اینترنت اشیاء در ساده‌سازی تصمیم‌گیری است و آن را به پایه حلقه ارزش در یک چرخه تشخیص و همچنین در مرحله نظارت بر تصمیم‌گیری تبدیل می‌نماید. حلقه ارزش قادر است که نظم و ترتیب را به محرک فناوری‌های اینترنت اشیاء بسپارد و نشان دهد که چگونه هرکدام از فرآیندهای تصمیم‌گیری را پشتیبانی می‌کند. حلقه ارزش نشان می‌دهد، جمع‌آوری انواع مختلف داده‌ها، مجموعه‌ای از استانداردهای داده را ضروری می‌سازد. با سازماندهی چندگانه، فرماندهی و خدمات نظامی که در تولید، انتقال و مصرف تمام انواع این داده‌ها دخیل هستند، ایجاد مجموعه‌ای از استانداردهای مشترک، به‌احتمال‌زیاد به یک دستورالعمل کلان جهت راهبری نیاز دارد تا در مورد استانداردها تصمیم‌گیری نماید (Mariani, Williams & Loubert, ۲۰۱۵: ۷).

تجهیزات نظامی مدرن به‌طور فزاینده‌ای باقابلیت پردازش و ارتباطات مجهز شده و برای بررسی و تغییر وضعیت تجهیزات مورداستفاده قرار خواهند گرفت. تا حدودی، این تجهیزات می‌تواند به‌عنوان سنسورها و یا محرک‌ها در نظر گرفته شود و در بقیه زیرساخت‌های اطلاعاتی ارتقا یابد. اشیاء نظامی فیزیکی و مجازی دارای هویت، ویژگی‌های جسمی، شخصیت‌های مجازی و رابط‌های هوشمند خواهند بود و باید به‌صورت یکپارچه در شبکه اطلاعات نظامی ادغام شوند. برای انجام یکپارچگی کامل باید سازوکارهای امنیتی مربوط، تطبیق پروتکل‌ها و خواص مقیاس‌پذیری ارائه شود. نتیجه احتمالی این ادغام مجموعه گسترده‌ای از سنسورها و اطلاعات برای استفاده در برنامه‌های آگاهی‌رسانی وضعیت، برنامه‌های اطلاعات پزشکی، برنامه‌های حمل‌ونقل و تدارکات و غیره است (IEEE WF IoT, ۲۰۱۵).

۳.فرماندهی و کنترل خودکار

نحوه تجهیز، راهبردها و معماری کلان فرماندهی و کنترل به یک سامانه یکپارچه فرماندهی و کنترل خودکار که بتواند کلیه سطوح فرماندهی شامل فرماندهی عملیاتی و تاکتیکی (از ستاد نیرو گرفته تا سربازان در میدان نبرد) را پوشش دهد، یکی از مباحث روز است. نکته کلیدی در فرایند توسعه و بهینه‌سازی سامانه‌های فرماندهی و کنترل، اتوماسیون کامل کارکردهای فرماندهی و کنترل به کمک فناوری‌های نوین، رایانه، نرم‌افزارهای پیشرفته و مدل‌سازی‌های پیشرفته است. دستیابی به این هدف مستلزم رعایت نکات ذیل است (دیوسالار، ۱۳۹۵: ۲۲۰-۲۴۵):

- افزایش اطمینان و اثربخشی سامانه‌ها
- بهینه‌سازی نرم‌افزارها
- بهبود ورودی‌های اطلاعاتی و فرایند فرآوری اطلاعات
- استانداردسازی و ساده‌سازی نحوه گردش مستندات در سامانه یکپارچه فرماندهی و کنترل اتوماتیک
- بهره‌گیری از فناوری هوش مصنوعی
- مقابله با تهاجمات نرم‌افزاری
- آموزش منسجم علمی و فنی کاربران سامانه‌های یکپارچه فرماندهی و کنترل.

بر این اساس بهترین راه‌حل یکپارچه‌سازی سامانه‌های فرماندهی کنترل، استانداردسازی سخت‌افزارها و نرم‌افزارها در عین اعطای استقلال کارکردی به زیرسامانه‌های مختلف است. به نظر می‌رسد بدین منظور ابتدا باید چالش‌های ذیل را از پیش رو برداشت (دیوسالار، ۱۳۹۵: ۲۲۰-۲٤٥):

- فائق آمدن بر معضلات طراحی یک سامانه کنترل بر اساس عناصر یک معماری استاندارد
- غلبه بر دشواری‌های خلق «محیط اطلاعاتی واحد»
- رفع مشکلات ایجاد شبکه اطلاعاتی رایانه‌ای یکپارچه
- استفاده از آخرین فناوری‌های نوظهور
- استانداردسازی نرم‌افزارها و سخت‌افزارها در پردازش داده‌های شبکه
- ایجاد پایانه‌های خودکار چندمنظوره برای کاربران عمده
- سازماندهی مجدد سازوکارهای حاکم بر تولید و توسعه سخت‌افزارها و نرم‌افزارها.

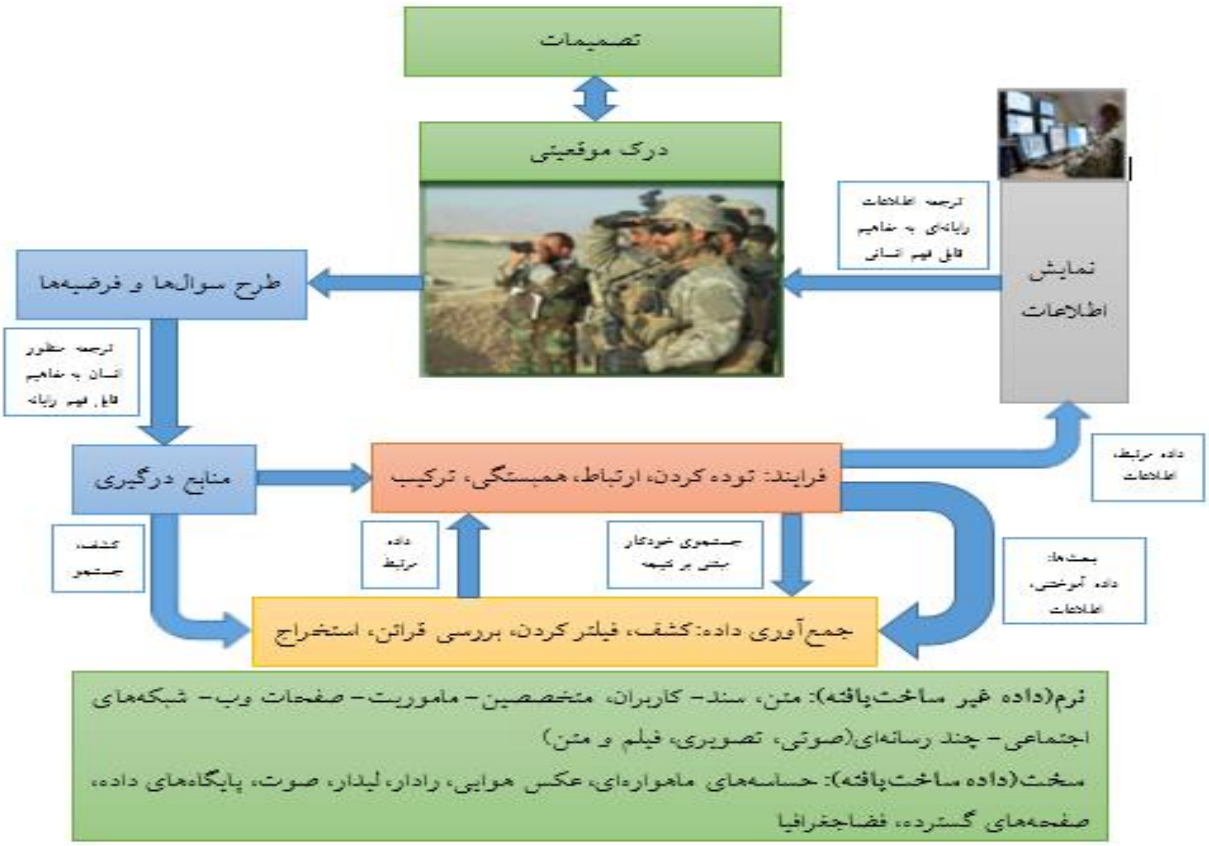
٤.بهره‌گیری از اینترنت اشیاء در سامانه فرماندهی و کنترل

فناوری اینترنت اشیاء امکان جمع‌آوری داده‌ها، و همچنین تولید و انتشار اطلاعات ساختاریافته را برای کاربردهای نظامی و به‌خصوص سامانه‌های فرماندهی و کنترل فراهم می‌نماید. با استفاده از این فناوری توانایی‌های نیروهای نظامی (از قبیل فرماندهان، تحلیلگران و ...) در شناخت محیط نبرد و انجام تصمیم‌گیری در زمان مناسب افزایش خواهد یافت و عملکرد بهتر اجزای سیستم و همچنین کاهش ریسک، نیروی انسانی و هزینه را در پی خواهد داشت (Michaelis, ۲۰۱٦: ۲).

همان‌گونه که در شکل (۲) نشان داده‌شده است، تلفیق اینترنت اشیاء با سامانه فرماندهی و کنترل، اطلاعات بسیار زیادی را جهت تجزیه‌وتحلیل وضعیت خودی و دشمن، در اختیار فرماندهان صحنه نبرد قرار می‌دهد. این اطلاعات از صدها سنسور، رادار و ماهواره به دست می‌آید و این داده‌ها را با یک زبان مشترک برای سیستم‌های دفاع موشکی جهت تعامل و تهدید در نظر می‌گیرد (FEARN, ۲۰۱۷).

اهداف موردنظر در اتصال سامانه فرماندهی و کنترل به اینترنت اشیاء عبارت‌اند از (Michaelis, ۲۰۱٦: ٥):

- تسهیل انتشار و اتصال داده‌های قابل تفسیر از طریق وب‌سایت.
- پشتیبانی از تفسیر داده‌ها به اطلاعات عملی، از طریق رمزگذاری داده‌ها مبتنی بر منطق.
- استفاده از ابزارهای اینترنت اشیاء جهت کشف پویا و محاسبات فراگیر.



شکل ۲: اینترنت اشیاء می‌تواند ابزار جدیدی برای ایجاد درک موقعیتی فرماندهی و کنترل باشد (Michaelis, ۲۰۱۶: ٦).

۵.چالش‌های به‌کارگیری اینترنت اشیاء در سامانه فرماندهی و کنترل

همان‌گونه که گفته شد اینترنت اشیاء امکانات زیادی را برای عملیات فرماندهی و کنترل ارائه می‌دهد بااین‌وجود، قابلیت اطمینان داده‌ها و اطلاعات مشتق شده از این فناوری ممکن است توسط چندین عامل تهدید شود، این عوامل عبارت‌اند از (Michaelis, ۲۰۱٦: ۷):

- محدودیت‌های اتصال و ظرفیت پردازش.
- نیاز به پهنای باند قابل‌توجهی جهت ارسال داده به/ از مراکز.
- امنیت / اعتماد برای دارایی‌های حوزه نظامی IoT .
- نیاز به دسترسی به محتوای توزیع‌شده.

علاوه بر موارد یادشده فوق چالش‌های دیگری در به‌کارگیری اینترنت اشیاء در حوزه نظامی وجود دارد که بایستی در مورد آن‌ها چاره‌اندیشی شود، این موارد عبارت‌اند از (FEARN, ۲۰۱۷):

- تأمین الزامات IoT در مناطق کاربردی نظامی.
- معماری خدمات برای IoT نظامی و ادغام در معماری ارتباطات نظامی.

- ادغام سنسورها و شبکه‌های ارتباطی.
- و درنهایت هک شدن بزرگ‌ترین این مخاطرات است که نتیجه آن سرقت اطلاعات و یا ایجاد اختلال در جریان داده‌ها خواهد بود.

۵,۱. ریزپردازنده‌ها در دستگاه‌های کاربری

در مبحث اینترنت اشیاء، مهم‌ترین بخشی که هر شیء را قادر به دریافت، پردازش و انتقال داده‌ها می‌نماید، بخش ریزپردازنده‌ها می‌باشد، که عملاً وظیفه کنترل تمام بخش‌های دیگر را بر عهده دارد. در حال حاضر ریزپردازنده‌های وارداتی در تمامی زیرساخت‌های فنی به‌صورت گسترده مورداستفاده قرار می‌گیرند. صاحب‌نظران بر این باورند که تهدیدات سخت‌افزاری و نرم‌افزاری از قبیل کلیدهای ازکارانداز و حفره‌های امنیتی که درواقع غیرقابل‌شناسایی هستند، قابلیت جاسازی شدن در هر نوع ریزپردازنده الکترونیکی‌ای را دارند. ازآنجاکه این ریزپردازنده‌ها در سامانه‌های بسیار حساس نظامی و اطلاعاتی نیز به کار می‌روند، لزوم توجه به شناسایی دقیق خرابکاری در آن‌ها بیش‌ازپیش هویدا شده است. با توجه به این‌که سامانه‌های نظامی به شکل معمول از دو گونه ریزتراشه الکترونیکی استفاده می‌کنند، با دو گونه تهدید نیز روبه‌رو خواهد بود. گونه نخست به تراشه‌های ساخته‌شده برای مأموریت‌های ویژه مربوط است. در اینجا خطر اصلی در کارخانه و زمان تولید این تراشه‌ها نهفته است؛ هرچند گام‌های طراحی نیز آسیب‌پذیر هستند. گونه دوم تهدید به اف‌پی‌جی‌ای‌ها مربوط می‌شود. این دسته ادوات الکترونیکی، مدارهای مجتمع آماده برای برنامه‌نویسی هستند و امکان تغییر کد برنامه در آن‌ها، هم یک مزیت است و هم یک عیب. کاملاً روشن است که این عیب برای نیروهای مسلح بسیار مشهودتر و در حقیقت یک تهدید خواهد بود، چراکه ممکن است تراشه‌ای که در شرایطی مطمئن برنامه‌نویسی شده است، در آینده از سوی یک خرابکار دست‌کاری شود و اطلاعات موردنظر را ارسال نکرده و یا اطلاعات غیرواقعی ارسال نماید (کاشی‌پور، ۱۳۸۸: ۳۲ –۳۳).

۵,۲. تطبیق پروتکل‌ها در لایه شبکه

یکی از چالش‌های اتصال اشیاء در اینترنت، یکسان نبودن پروتکل‌های مورداستفاده در طراحی شیء موردنظر با پروتکل بکار رفته در ارتباط‌دهی و مسیریابی محیط کاری می‌باشد. زمانی که دو ماشین به یک شبکه سوئیچینگ بسته‌ای یکسان مرتبط باشند یک فضای آدرس و رویه مسیریابی استفاده می‌گردد به‌عبارت‌دیگر جریان انتقال داده با استفاده از یک پروتکل انجام می‌شود. اما هنگامی‌که دو ماشین به شبکه‌های مختلفی مرتبط می‌شوند، انتقال داده بایستی از دو یا چند شبکه که احتمالاً ازنقطه‌نظر مسیریابی و آدرس‌دهی با هم متفاوت هستند، انجام شود. درنتیجه برای برقراری ارتباط در شبکه‌های میانی به پروتکل‌های بین شبکه‌ای نیاز است تا بتوانند دروازه‌ها/ مسیریاب‌ها را به هم مرتبط سازد. پروتکل‌های بین شبکه‌ای همچنین می‌بایست تفاوت‌های آدرس‌دهی و سایز بسته‌ها را نیز مدیریت کنند (طرقی‌حقیقت، ۱۳۹٤: ۲۱).

۵,۳. مقیاس‌پذیری شبکه

یکی از مشخصه‌های محیط نظامی، احتمال تغییر سطح امنیتی منطقه عملیات و لزوم به‌کارگیری تجهیزات گوناگون

در تعداد و انواع مختلف می‌باشد. به‌عبارت‌دیگر تعداد و نوع تجهیزات مورداستفاده در منطقه عملیاتی با تغییر سطح امنیتی منطقه تغییر خواهد کرد. لذا شبکه‌ای که قرار است ارتباط داخل و خارج منطقه عملیاتی را برقرار نماید بایستی به نحوی در نظر گرفته شود که با افزایش تعداد تجهیزات با مشکل مواجه نگردد.

در علم ارتباطات راه دور و مهندسی نرم‌افزار، مقیاس‌پذیری، ویژگی مطلوبی از یک سامانه (سیستم)، شبکه یا فرایند است که به توانایی آن برای پاسخگویی به افزایش میزان بار کاری به سهولت دلالت می‌کند یا میزان آمادگی سیستم را برای افزایش بار کاری نشان می‌دهد. به‌عنوان نمونه، مقیاس‌پذیری می‌تواند به توانایی یک سامانه برای افزایش عملکرد کلی در هنگام افزودن منابع (مثل سخت‌افزار) اشاره کند. هنگامی‌که این واژه در موضوعات مرتبط با کسب‌وکار، به کار می‌رود نیز مفهوم مشابهی از آن برداشت می‌شود. مدل‌های کسب‌وکار

مقیاس‌پذیر مدل‌هایی هستند که پتانسیل ایجاد رشد اقتصادی سازمان را دارند.

تعریف مقیاس‌پذیری به‌عنوان یک خصوصیت از سامانه به‌سادگی امکان‌پذیر نیست و در هر مورد خاصی با توجه به ابعاد مورد اهمیت باید نیازمندی‌های جدیدی را برای مقیاس‌پذیری تعریف کرد. نقش مقیاس‌پذیری در طراحی و انجام سامانه‌های پیچیده و بزرگ همچون پایگاه‌های داده‌ها، پایگاه‌های دانش، محاسبات گسترده، اینترنت، کاوش‌های ماشینی در داده‌ها، بینایی رایانه‌ای و مخابرات، بسیار حیاتی است. سامانه‌ای که با افزایش ظرفیت، کارایی آن افزایش می‌یابد یک سامانه مقیاس‌پذیر خوانده می‌شود (دانشنامه آزاد ویکی‌پدیا، ۱۳۹۷).

۵،٤. تأمین امنیت در اینترنت اشیاء

تهدیدات متوجه اینترنت اشیا را می‌توان به سه دسته تقسیم کرد: محرمانگی، امنیت و ایمنی. تهدیدات اینترنت اشیا وسیع بوده و به‌صورت بالقوه می‌توانند سیستم را از کار بیندازند. اینترنت اشیا می‌تواند به دلیل دارا بودن زیرساخت‌های حیاتی، هدف خوبی برای جاسوسی ملی و صنعتی و نیز از کار انداختن خدمات و دیگر انواع حملات باشد. موضوع نگران‌کننده دیگر می‌تواند محرمانگی اطلاعات شخصی ذخیره‌شده در شبکه باشد که خود آن برای مجرمان سایبری جذاب است.

علی‌رغم وجود همه این تهدیدات می‌توان محیط اینترنت اشیا را با ابزارهای امنیتی نظیر **رمزنگاری** داده، تصدیق قوی‌تر کاربر، کد نویسی بهتر و رابط نرم‌افزاری برنامه‌های کاربردی[1] تست‌شده و استاندارد که به حالات قابل پیش‌بینی می‌توانند واکنش نشان دهند، ایمن‌تر کرد. و برخی از ابزارهای امنیتی را می‌توان مستقیماً به تجهیزات متصل اعمال کرد. رندی مارچانی، مدیر ارشد اجرایی در دانشگاه ویرجینا تک و مدیر آزمایشگاه امنیت فناوری اطلاعات این دانشگاه، معتقد است تجهیزات اینترنت اشیا توانایی محافظت از خود را ندارند و باید از سیستم‌های دیواره آتش یا شناسایی ورود غیرمجاز استفاده کنند و یا از یک بخش شبکه ایزوله شده استفاده نمایند. به اعتقاد مارچانی امنیت فیزیکی مسئله‌ای است که اهمیت بیشتری دارد، زیرا معمولاً تجهیزات در محیط‌های دور از دسترس قرار دارند و هرکسی می‌تواند به آن‌ها

۱- Application Programming Interface(API)

دسترسی پیدا کند. در صورت دسترسی فیزیکی فردی به یک دستگاه، مشکلات امنیتی به‌طور فزاینده‌ای بیشتر خواهد شد.

نیازهای امنیتی باید به‌عنوان بنیان سیستم‌های اینترنت اشیا قرار داده شود و کنترل‌های سخت‌گیرانه تصدیقی، اعتماد، تأیید داده و رمزنگاری تمامی داده‌ها باید گنجانده شود. در سطح اپلیکیشن، سازمان‌های توسعه نرم‌افزار باید کدهای باثبات‌تر و قابل‌اعتمادتری بنویسند. با تعامل سیستم‌ها با یکدیگر، ضرورت وجود استانداردهای سازگاری که امن و مورد اعتماد هستند، بیش‌ازپیش بااهمیت به نظر می‌رسد. بدون ساختار مستحکم از پایین به بالا ما تهدیدات بیشتری را با افزودن هر دستگاه به اینترنت اشیا، ایجاد خواهیم کرد. دستیابی به اینترنت اشیایی امن و ایمن کاری دشوار ولی شدنی خواهد بود (IEEE WF IoT, ۲۰۱۵).

۵,۵. حسگرهای شناسایی:

در مبحث اینترنت اشیاء هر شیء به‌عنوان یک گره در نظر گرفته می‌شود. ازآنجایی‌که گره‌ها از حسگرها (سنسور (تشکیل‌شده‌اند، اهداف اصلی هکرهایی می‌باشند که می‌خواهند از آن‌ها برای جابه‌جایی نرم‌افزار دستگاه با نرم‌افزار دستگاه خود استفاده کنند. در لایه دریافت، بیشتر تهدیدها از جانب اشخاص خارجی و عمدتاً با توجه به حسگرها و سایر تجهیزات جمع‌آوری داده‌ها می‌باشند. ازآنجایی‌که نوع ارتباط میان این دستگاه‌ها بی‌سیم و از طریق اینترنت می‌باشد، اگر از آن‌ها محافظت نشود، نسبت به حملات استراق سمع آسیب‌پذیر خواهند بود. در این حمله، حسگرهای موجود در خانه هوشمند که در معرض خطر قرار می‌گیرند، می‌توانند برای کاربران پیام ارسال کرده و از کاربران اطلاعات خصوصی دریافت نمایند. هکرها می‌توانند حسگرها یا دستگاه‌های مخرب را نزدیک به حسگرهای نرمال دستگاه‌های اینترنت اشیاء قرار دهند و به اطلاعات دستگاه دست یابند. فراوانی دستگاه‌های اینترنت اشیاء محیط هوشمند به این معنی است که انسان‌ها می‌توانند از طریق محیط فیزیکی و بدون رضایت خود آن‌ها تا حد زیادی شناسایی و ردیابی شوند و مشخصات آن‌ها نشان داده شود (الامپالایام کومار، تایلر، هارشیت، ۱۳۹۵: ٢٤).

۵,٦. حفاظت فیزیکی:

اشیایی که قرار است از طریق احساس تغییرات محیط پیرامون، داده‌های باارزشی را جمع‌آوری و به مراکز کنترل و فرماندهی ارسال نمایند، بایستی در برابر حملات فیزیکی هم ازنظر عوامل طبیعی (مانند باران، برف، باد و ...) و هم ازنظر افراد غیرمجاز محافظت شوند. حسگرهای در معرض خطرات محیطی، عملکرد و قابلیت مورد انتظار خود را ازدست‌داده و در برابر خطرات دیگر نیز آسیب‌پذیر می‌شود. همچنین در راستای پیشگیری از اتفاقات ناخواسته و حملات هدفمند، سیستم‌های اینترنت اشیاء بایستی به‌گونه‌ای طراحی شوند که امکان نفوذ و دست‌کاری تجهیزات مرتبط با اینترنت اشیاء توسط افراد غیرمجاز به حداقل برسد (الامپالایام کومار، تایلر، هارشیت، ۱۳۹۵: ۲۵).

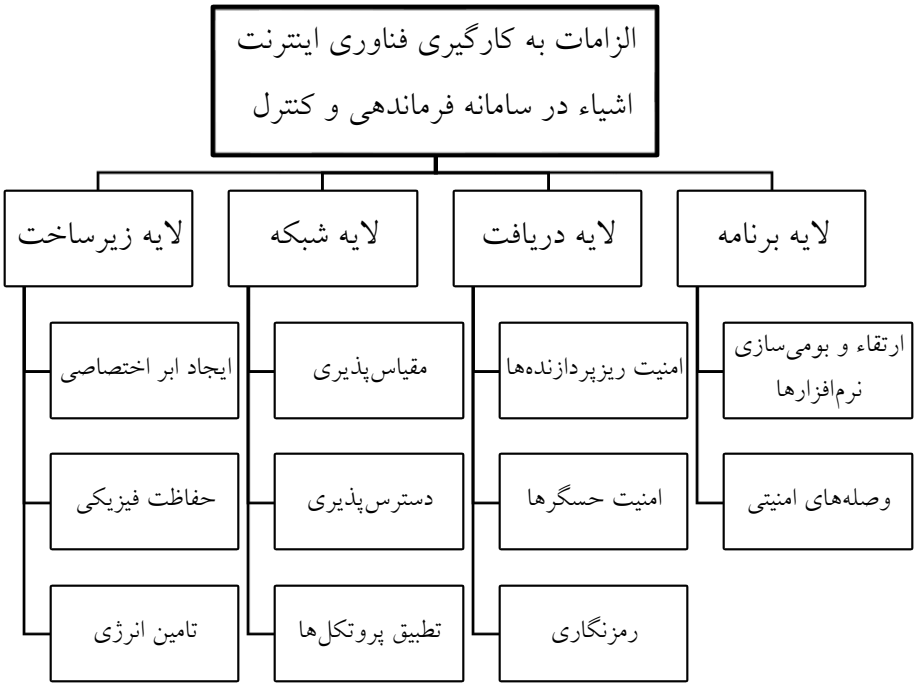
۵,۷. تأمین انرژی:

حساسه‌های اینترنت اشیاء که به‌صورت مجزا و تکی مورداستفاده قرار می‌گیرند باید ازنظر تأمین انرژی، اثربخشی لازم را داشته باشند و بتوانند با استفاده از نیروی باتری مدت‌زمان زیادی فعال باقی بمانند. باتری‌ها باید به مدت

مشخص شارژ خود را نگه‌دارند و برای استفاده مداوم از دستگاه به‌سرعت شارژ شوند (الامپالایام کومار، تایلر، هارشیت، ۱۳۹۵: ۲۶).

۶. مدل مفهومی پژوهش

مدل مفهومی تحقیق در نمودار ۱ آورده شده است. در این مدل الزامات به‌کارگیری فناوری اینترنت اشیاء در سامانه فرماندهی و کنترل در چهار لایه برنامه، دریافت، شبکه و زیرساخت موردبررسی قرارگرفته و با اخذ نظر خبرگان و صاحب‌نظران حوزه‌های سایبر و فرماندهی و کنترل، الزامات هر لایه به‌نحوی‌که محرمانگی، جامعیت و دسترس‌پذیری داده‌ها تأمین شود، استخراج گردیده است.



نمودار ۱: مدل مفهومی تحقیق

۷.روش تحقیق

این تحقیق به لحاظ هدف از نوع کاربردی و به لحاظ روش از نوع توصیفی (موردی) و با رویکرد آمیخته (کمی و کیفی)، کمی به‌صورت آمار توصیفی و کیفی به روش تحلیل محتوا می‌باشد. جامعه آماری این تحقیق تعداد ۸۰ نفر از خبرگان و صاحب‌نظران در خصوص موضوعات فضای سایبر و همچنین فرماندهی و کنترل بودند که با استفاده از روش آلفای کرونباخ و در سطح خطای پنج درصد، حجم جامعه نمونه برابر با ۳۰ نفر خواهد بود که به‌صورت هدفمند انتخاب و پرسشنامه در مورد آن‌ها اجرا گردید. نمره‌گذاری پرسشنامه‌ها به‌صورت طیف لیکرت ۵ تایی از کاملاً مخالفم (۱) تا کاملاً موافقم (۵) می‌باشد.

۸.یافته‌های تحقیق

پس از مطالعه منابع و با اخذ نظر خبرگان، الزامات به‌کارگیری اینترنت اشیاء در سامانه فرماندهی و کنترل، در چهار

لایه برنامه، دریافت، شبکه و زیرساخت به شرح ذیل استخراج گردید:

الف- در لایه برنامه: ارتقاء و بومی‌سازی نرم‌افزارها و همچنین بهره‌گیری از وصله‌های امنیتی پویا.

ب- در لایه دریافت: اطمینان از سلامت ریزپردازنده‌ها، تأمین امنیت حسگرهای کشف و شناسایی و بهره‌گیری از رمزنگاری.

ج- در لایه شبکه: تأمین ارتباطات موردنیاز در همه‌جا (دسترس‌پذیری)، تطبیق پروتکل‌ها و مقیاس‌پذیری شبکه.

د- در لایه زیرساخت: ایجاد ابر اختصاصی، تأمین حفاظت فیزیکی و تأمین انرژی حسگرها.

متغیرهای فوق طی پرسشنامه‌ای توسط تعداد ۳۰ نفر از صاحب‌نظران حوزه‌های سایبری و فرماندهی و کنترل مورد نظرسنجی قرارگرفته و پاسخ‌های حاصله، با استفاده از نرم‌افزار spss ارزیابی گردید. و برای هر شاخص معیارهای میانگین (به‌عنوان شاخص گرایش مرکزی)، فراوانی، فراوانی تجمعی، واریانس و انحراف استاندارد (به‌عنوان شاخص پراکندگی) محاسبه شد. نتایج حاصله به شرح جدول ذیل می‌باشد:

متغیرها	میانگین	انحراف استاندارد	واریانس	فراوانی تجمعی (٤ و ٥)
ارتقاء و بومی‌سازی نرم‌افزارها	٤/٤٠٠	۰/٦٧٤٧	۰/٤٥٥	۹۰/۰
وصله‌های امنیتی	٤/٤٦٧	۰/۷۳۰۳	۰/٥۳۳	۹۰/۰
سلامت ریزپردازنده‌ها	٤/٢٦٧	۰/۷۸٤۹	۰/٦١٦	۸۳/٤
امنیت حسگرها	٤/١٦٧	۰/٦٤٧٧	۰/٤٢۰	۸٦/۷
رمزنگاری	٤/٢۳۳	۰/۷٢۷۹	۰/٥۳۰	۸٦/۷
دسترس‌پذیری	٤/۳۳۳	۰/٦۰٦٥	۰/۳٦۸	۹۳/۳
مقیاس‌پذیری	٤/٤۳۳	۰/۷٢۷۹	۰/٥۳۰	۹۰/۰
تطبیق پروتکل‌ها	٤/۳۰۰	۰/٦٥۱۳	۰/٤٢٤	۹۰/۰
ایجاد ابر اختصاصی	٤/١٦٧	۰/٥۹٢۱	۰/۳٥۱	۹۰/۰
تأمین حفاظت فیزیکی	٤/٢٦٧	۰/٦۳۹۷	۰/٤۰۹	۹۰/۰
تأمین انرژی حسگرها	٤/٢٦٧	۰/٥۸۳۳	۰/۳٤۰	۹۳/۳

جدول ۱: نتایج آمار توصیفی به‌دست‌آمده با استفاده از نرم‌افزار spss.

طبق جدول ۱ در بین متغیرها بیشترین میانگین متعلق استفاده از وصله‌های امنیتی پویا است و میانگین نمرات اخذشده جهت کلیه متغیرها بیش از ٤ می‌باشد. بنابراین می‌توان چنین پنداشت که ازنظر صاحب‌نظران کلیه متغیرهای سؤال شده جهت بهره‌گیری از اینترنت اشیاء در سامانه فرماندهی و کنترل ضروری می‌باشند.

بیشترین میزان انحراف استاندارد مربوط به اطمینان از سلامت ریزپردازنده‌ها است و بیانگر این مطلب است که نمرات افراد در این متغیر دارای پراکندگی زیادی بوده و نظر افراد در این متغیر با یکدیگر تفاوت زیادی دارد. همچنین

کمترین میزان انحراف استاندارد مربوط به تأمین انرژی حسگرها است و درواقع میزان نمرات افراد در این متغیر به یکدیگر نزدیک است.

بیشترین میزان فراوانی تجمعی (گزینه‌های موافقم و کاملاً موافقم) مربوط به متغیرهای تأمین انرژی حسگرها و دسترس‌پذیری شبکه می‌باشد، و تغییرات این شاخص بین ۸۳/٤ تا ۹۳/۳ درصد می‌باشد، بنابراین می‌توان چنین پنداشت که اکثریت مطلق صاحب‌نظران با لزوم توجه به کلیه متغیرهای سؤال شده جهت بهره‌گیری از اینترنت اشیاء در سامانه فرماندهی و کنترل موافق می‌باشند.

از طرفی با توجه به اینکه خبرگان و متخصصین جامعه نمونه ازلحاظ معیارهای میزان تحصیلات، سابقه کاری، اشتغال در مشاغل راهبردی و همچنین میزان آشنایی با مباحث سایبری و فرماندهی و کنترل، همگی در حد بالایی قرار دارند بنابراین می‌توان نتیجه گرفت پاسخ‌های دریافت شده از اعتبار بالایی برخوردار می‌باشد.

۹. نتیجه‌گیری و پیشنهادات

الف- نتیجه‌گیری:

فناوری نوظهور اینترنت اشیاء قابلیت ارسال و دریافت داده بین اشیاء مختلف از طریق شبکه‌های ارتباطی را فراهم کرده و می‌تواند منشأ ایجاد تغییراتی شگرف در تجهیزات نظامی شده و همچنین موجب ارتقاء کارایی بخش‌های دفاعی گردد. سامانه فرماندهی و کنترل یکی از مهم‌ترین بخش‌های حوزه دفاع است که می‌تواند با ورود فناوری اینترنت اشیاء متحول گردد. فرماندهی و کنترل عبارت است از برنامه‌ریزی، هدایت، هماهنگی و کنترل عملیات مبتنی بر اجرای مؤثر سناریوی عملیاتی، بنابراین جهت دستیابی به بهترین نتیجه، داشتن اطلاعات کامل، دقیق و درزمان امری حیاتی است. از طرفی بهره‌گیری از فناوری اینترنت اشیاء این امکان را به فرماندهان می‌دهد تا در کمترین زمان ممکن به بیشترین و دقیق‌ترین اطلاعات مربوط به صحنه نبرد دست یابند.

این مقاله به بررسی الزامات بهره‌برداری از اینترنت اشیاء در سامانه فرماندهی و کنترل، می‌پردازد. بدین منظور مباحث مرتبط با فناوری اینترنت اشیاء، رایانش ابری، سامانه فرماندهی و کنترل و چالش‌های مرتبط با بهره‌گیری از فناوری اینترنت اشیاء در سامانه فرماندهی و کنترل موردبررسی قرار گرفت و الزامات به‌کارگیری فناوری اینترنت اشیاء در سامانه فرماندهی و کنترل در چهار لایه برنامه، دریافت، شبکه و زیرساخت پس از مراجعه به نظر خبرگان به‌نحوی‌که محرمانگی، جامعیت و دسترس‌پذیری داده‌ها تأمین شود، استخراج گردیده و پس از نظرسنجی از صاحب‌نظران حوزه‌های سایبری و فرماندهی و کنترل نتایج زیر به دست آمد:

- ❖ در لایه برنامه: ارتقاء و بومی‌سازی نرم‌افزارها و همچنین بهره‌گیری از وصله‌های امنیتی پویا ضروری خواهد بود.
- ❖ در لایه دریافت: اطمینان از سلامت ریزپردازنده‌ها، تأمین امنیت حسگرهای کشف و شناسایی و بهره‌گیری از رمزنگاری ضروری است.
- ❖ در لایه شبکه: تأمین ارتباطات موردنیاز در همه‌جا (دسترس‌پذیری)، تطبیق پروتکل‌ها و مقیاس‌پذیری شبکه ضروری است.

❖ در لایه زیرساخت: ایجاد ابر اختصاصی، تأمین حفاظت فیزیکی و تأمین انرژی حسگرها ضروری است.

ب- پیشنهادات:

با توجه به این‌که گزارش‌های آینده‌پژوهی در حوزه سایبری موید این نکته است که در آینده کلیه اشیاء به بستر اینترنت متصل خواهند شد، و با عنایت به امکانات و فرصت‌های زیادی که این فناوری در اختیار کاربران قرار می‌دهد، پیشنهاد می‌گردد حوزه نظامی ضمن در نظر گرفتن چالش‌ها و تهدیدات پیش رو پیش‌بینی‌های لازم در راستای بهره‌گیری از اینترنت اشیاء در بخش‌های مختلف را به عمل‌آورند.

منابع:

۱. اکبری، محمدکاظم، سرگلزایی جوان، مرتضی، (۱۳۹۳)، مقدمه‌ای بر رایانش ابری، آزمایشگاه و تحقیقات رایانش ابری دانشگاه صنعتی امیرکبیر.

۲. الامپالایام کومار، ساتیش، تایلر، ویلی، هارشیت، استاوا، پدافند سایبری در اینترنت اشیاء: چالش‌ها، راه حل‌ها و اهداف آینده، نشریه آموزشی، پژوهشی و ترویجی پدافند سایبری، سال اول شماره ٤، اسفند (۱۳۹۵).

۳. دانشنامه‌آزادویکی‌پدیا، "مقیاس‌پذیری‌شبکه"،(۱۳۹۷)، برگرفته از HTTPS://FA.WIKIPEDIA.ORG/WIKI.

٤. دبیرخانه برنامه ملی آینده‌نگاری علم و فناوری در حوزه فناوری اطلاعات و ارتباطات، "گزارش شماره ۱ از سلسله مطالعات برنامه ملی آینده‌نگاری در حوزه فناوری اطلاعات و ارتباطات اینترنت اشیا و چگونگی ارزش‌آفرینی آن از نگاه موسسه جهانی مکنزی"، (۱۳۹۵)،۳-٤.

۵. دیوسالار، عبدالرسول، "راهبردها و معماری کلان فرماندهی و کنترل در روسیه"، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، (۱۳۹۵).

٦. طرقی‌حقیقت، ابوالفضل، "شبکه‌های کامپیوتری"، انتشارات نشر، (۱۳۹٤).

۷. قیصری، محمد؛ تاج فر، امیرهوشنگ؛ وحدت، داود؛ حسینی، ساره، مدیریت زنجیره تأمین با به‌کارگیری فناوری نوین اینترنتی از اشیاء مبتنی بر ابر اطلاعات، فصلنامه علمی ترویجی مدیریت زنجیره تأمین، زمستان ۱۳۹۲، شماره ٤۲، ۲٦-٤۱.

۸. کاشی‌پور، میثم، (۱۳۸۸)، دیده‌بانی و رصد تهدیدها و فرصت‌های موجود در شکاف‌های عملکردی ریزتراشه‌ها، مرکز آینده‌پژوهی علوم و فناوری دفاعی، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

۹. محمدی، علی، " نسل بعدی اقدامات امنیتی فضای سایبر با تأکید بر فناوری‌های برهم زن"، دانشگاه صنعتی

امیر کبیر، (۱۳۹۵).

۱۰.مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، "نگاهی به آینده سامانه‌های فرماندهی و کنترل"،(۱۳۹۲).

۱۱.وب‌سایت انجمن اینترنت اشیاء ایران، (۱۳۹۶)، دسترسی از طریق آدرس اینترنتی.WWW.IOTIRAN.COM

۱۲. FEARN, N., "US ARMY IS USING IOT TECH AND DATA TO TRANSFORM WARFARE", JANUARY ۲۰, ۲۰۱۷, RETRIEVED FROM https://internetofbusiness.com/us-army-iot-warfare.

۱۳. IEEE WORLD FORUM ON INTERNET OF THINGS, FEBRUARY ۲۰۱۸, "MILITARY APPLICATIONS OF IOT", RETRIEVED FROM http://wfiot۲۰۱۸.iot.ieee.org/sps۲-military-applications-iot/

۱٤. MARIANI, J., WILLIAMS, B.,& LOUBERT, B., "THE PAST, PRESENT, AND FUTURE OF THE IOT IN THE MILITARY", AUGUST ۰٦, ۲۰۱٥,

۱٥. MICHAELIS, J. R., "MILITARY INTERNET OF THINGS (IOT), AUTONOMY, AND THINGS TO COME," ۲۱ST INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM (ICCRTS), PP. ۲-۷, ۲۰۱٦.

۱٦. RTO TASK GROUP, "MILITARY APPLICATIONS OF INTERNET OF THINGS (IST-۱٤۷)" CONTACT STO/CSO PANEL OFFICE, P ۲, ۲۰۱٥. RETRIEVED FROM HTTPS://WWW.CSO.NATO.INT/ACTIVITY_META.ASP

۱۷. U.S. DEPARTMENT OF DEFENSE, DECEMBER ۲۰۱٦, "POLICY RECOMMENDATIONS FOR THE INTERNET OF THINGS (IOT)", CHIEF INFORMATION OFFICER.

۱۸. ZHENG, D. E., CARTER, W. A. (۲۰۱٥), "LEVERAGING THE INTERNET OF THINGS FOR A MORE EFFICIENT AND EFFECTIVE MILITARY", A REPORT OF THE CSIS STRATEGIC TECHNOLOGIES PROGRAM, P. ۳.