فصلنامه پژوهش‌های حفاظتی ـ امنیتی
دانشگاه جامع امام حسین(علیه‌السلام)

سال نهم، شمارهٔ ۳۳ (بهار ۱۳۹۹)صص۸۸-۶۵

مدل معماری امنیت‌پایه برای صحنهٔ نبرد مبتنی بر فنّاوری اینترنت اشیاء

■ **منصور فرزین‌فرد** ■
دانشجوی دکتری امنیت سایبری دانشگاه عالی دفاع ملّی (نویسنده مسئول)، m.farzinfard@sndu.ac.ir
■ **محمدرضا موحدی‌صفت** ■
استادیار دانشگاه عالی دفاع ملّی، movahedi@sndu.ac.ir

تاریخ دریافت: ۱۳۹۹/۰۱/۲۸ تاریخ پذیرش: ۱۳۹۹/۰۲/۲۰

چکیده

اینترنت اشیاء به‌عنوان یک فنّاوری نوظهور می‌تواند قابلیت شناسایی و انتقال داده‌ها را برای همه اشیاء فراهم نماید. کنترل بر عملکرد تجهیزات، شناسایی کاربران و کنترل اطلاعات از مزیت‌های اصلی این فنّاوری است. ویژگی‌های خاص صحنهٔ نبرد و تعدد و تنوع تجهیزات به‌کاررفته در این محیط باعث شده تا سازمان‌های دفاعی در دنیا برای کنترل صحنه نبرد از این فنّاوری استفاده نمایند. از الزامات به‌کارگیری فنّاوری اینترنت اشیاء در صحنهٔ نبرد، توجه به مقولهٔ امنیت و ایجاد یک معماری امنیت‌پایه است که بر اساس آن همه اجزاء و روابط بین اجزاء در قالب مؤلفه‌های امنیت تعریف گردد. تحقیق حاضر از نوع کاربردی بوده و روش آن توصیفی - تحلیلی با رویکرد اکتشافی است و داده‌های کیفی این تحقیق از مطالعهٔ منابع و پژوهش‌های علمی و با استفاده از روش پژوهش کیفی فراترکیب جمع‌آوری گردیده است و جهت اعتبارسنجی معماری پیشنهادی از نظرات جامعهٔ نمونه که کارشناسان حوزهٔ دفاعی هستند و با فنّاوری اینترنت اشیاء آشنایی کامل دارند و همچنین متخصصان حوزهٔ اینترنت اشیاء بر اساس مصاحبه استفاده شده است. نتایج تحقیق نشان می‌دهد که فنّاوری اینترنت اشیاء در محیط رایانش ابری و مبتنی بر کلان داده‌ها بهترین عملکرد در صحنه نبرد را خواهد داشت. همچنین، مشخص گردید که با توجه به ویژگی‌های صحنهٔ نبرد، لایهٔ امنیت باید تمامی لایه‌های معماری را پوشش دهد.

کلید واژگان: *امنیت، اینترنت اشیاء، حسگرها، صحنه نبرد.*

مقدمه

«رشد بسیار سریع دستگاه‌های با قابلیت اتصال به اینترنت، از حسگرهای ساده تا سرورهای ابری پیچیده منجر به شکل‌گیری اینترنت اشیاء[1] شده است» (Ammar, Russello & Crispoa, 2018: 9). این فنّاوری نوظهور و برهم‌زن[2] شبکه‌ای از اجزاء فیزیکی (از قبیل ابزارهای پوشیدنی، لوازم برقی خانگی، سامانه‌های امنیتی، نانوتکنولوژی، ابزارهای ساخت و تولید و...) است که به اجزاء هوشمندی (از قبیل ریزپردازنده‌ها، حافظه‌های ذخیره‌سازی، حسگرها و...) مجهز شده‌اند و در بستر اینترنت با سایر ابزارها ارتباط برقرار می‌کنند (Gupta & Quamara, 2018: 38).

این فنّاوری باعث تغییر در روندهای توسعه در سازمان‌های دفاعی دنیا شده و این سازمان‌ها استفادهٔ حداکثری از این فنّاوری را در رأس برنامه‌های خود قرار داده‌اند. این فنّاوری مزیت‌های فراوانی را برای این سازمان‌ها به همراه آورده است که مهم‌ترین آنها کنترل کامل تجهیزات، بهبود عملکردهای سازمانی، افزایش احساس امنیت، ایجاد جریان عظیم اطلاعات درون‌سازمانی، تسهیل ارتباطات و بهبود سامانه‌های مدیریتی است (DoD[3], 2017).

فنّاوری اینترنت اشیاء همانند تمام فنّاوری‌های دیگر دارای چالش‌هایی در حوزهٔ کاربرد و استفاده، به‌ویژه در سازمان‌های نظامی است که تولید حجم عظیمی از اطلاعات (کلان داده)[4] ، چالش‌های حوزهٔ ارتباطات بی‌سیم، پیچیدگی در معماری، گستردگی مقیاس عملکرد، نیاز به پهنای باند بالا، امنیت و حریم خصوصی از مهم‌ترین این چالش‌ها است. البته مزیت‌های حاصل از این فنّاوری که به چابک‌سازی[5] سازمانی خواهد انجامید، باعث شده تا سازمان‌های دفاعی نظیر وزارت دفاع آمریکا، اسناد راهبردی برای توسعهٔ این فنّاوری را تهیه و نسبت به به‌روزرسانی سالیانهٔ آن اقدام نمایند (همان).

از قابلیت‌های اصلی فنّاوری اینترنت اشیاء می‌توان به هدایت و مدیریت تجهیزات، تدارکات و فعّالیت‌های نظامی در میدان‌های جنگ، مأموریت‌ها، آموزش‌ها و همچنین اطلاع فرماندهان از وضعیت سلامت جسمانی نیروها در هر زمان و تسهیل در تصمیم‌گیری در لحظات دشوار اشاره نمود.

[1]Internet of things
[2]Disruptive
[3]U.S. Department of Defense
[4]Big Data
[5]Agility

استفاده حداکثری از قابلیت‌های فنّاوری اینترنت اشیاء در سازمان‌های دفاعی نیازمند یک معماری است تا بر اساس آن بتوان ضمن تعیین جایگاه اجزاء و مؤلفه‌ها، ارتباطات آنها را با یکدیگر مشخص نمود. محققان در این مقاله ضمن بررسی کارهای علمی انجام‌شده در سطح ملّی و بین‌المللی، یک مدل معماری امن مبتنی بر اینترنت اشیاء را بر اساس مدل‌ها و معماری‌های مرجع در دنیا و همچنین نظرات خبرگان و مدیران سازمان‌های دفاعی کشور ارائه کرده‌اند.

بیان مسئله

امروزه در روابط بین‌الملل ماهیت جنگ‌ها تغییر کرده است، ناهمگونی، کوتاه بودن زمان درگیری، وسعت منطقهٔ نبرد، سرعت در چرخش اطلاعات، دقت و هوشمندی تسلیحات، داده‌ها و ارتباطات هوشمند، ائتلافی بودن و غیرخطی بودن از ویژگی‌های نبردهای آینده است. بهره‌گیری از سرمایه‌های دانشی و تحولات فنّاورانه در بستر فنّاوری اطلاعات و استفاده از فنّاوری‌های برهم‌زن همچون اینترنت اشیاء در صحنه‌های نبرد، امری ضروری است. از طرف دیگر، ویژگی‌های فضای سایبر و اینترنت اشیاء موجب شده است تا تمام قدرت‌های منطقه‌ای و جهانی سرمایه‌گذاری‌های فراوانی را در حوزه‌های تحقیقاتی و عملیاتی انجام دهند. در صحنهٔ نبرد، اینترنت اشیاء کاربرد جدی دارد. معماری‌های متفاوتی از کاربرد اینترنت اشیاء در صحنهٔ نبرد وجود دارد، اما یا ازلحاظ امنیتی ضعیف هستند و یا امنیت در آنها به‌طور کامل نادیده گرفته شده است.

این مقاله ازآن‌جهت اهمیت دارد که می‌تواند زمینه‌ساز توجه بیشتر سازمان‌های نظامی به استفاده از اینترنت اشیاء در صحنهٔ نبرد، افزایش بهره‌وری و اثربخشی و ایجاد یک نگاه جدید کلنگرانه برای فرماندهی صحنه‌های نبرد شود. از سوی دیگر، پرداختن به حوزهٔ معماری امنیت‌پایه می‌تواند بستر امن لازم برای فرماندهی و مدیریت صحنهٔ نبرد با در نظر گرفتن مخاطرات و چالش‌های ناشی از به‌کارگیری اینترنت اشیاء را مهیا نماید. عدم پژوهش در این عرصه می‌تواند باعث افزایش شکاف فنّاورانه، غافلگیری راهبردی، بروز بحران در جنگ احتمالی آینده و عدم استفاده سازمان‌های نظامی از قابلیت‌ها و فرصت‌های فراوان پیشِ رو گردد. همچنین، بی‌توجهی به مقولهٔ امنیت در سامانه‌های نظامی مبتنی بر اینترنت اشیاء می‌تواند به افزایش مخاطرات تهدیدکنندهٔ بازیگران صحنهٔ نبرد بیانجامد. بنابراین، هدف از این تحقیق ارائهٔ یک معماری امنیت‌پایه برای صحنهٔ نبرد

مبتنی بر فنّاوری اینترنت اشیاء است. نیروهای مسلح با بهره‌گیری از این معماری می‌توانند اقدامات موردنیاز برای حضور مؤثر در صحنهٔ نبرد و حفاظت از زیرساخت‌ها را اولویت‌بندی و طرح‌ریزی نمایند. درواقع، این تحقیق به دنبال پاسخ به این سؤال است که «معماری امنیت‌پایه برای صحنهٔ نبرد مبتنی بر فنّاوری اینترنت اشیاء چگونه است؟ این معماری از چه اجزاء و مؤلفه‌هایی تشکیل شده و نقش امنیت در هر یک از اجزای آن چگونه می‌باشد؟»

روش‌شناسی تحقیق

پژوهش حاضر از نوع کاربردی بوده و روش آن توصیفی – تحلیلی با رویکرد اکتشافی است و در زمرهٔ تحقیقات کیفی دسته‌بندی می‌گردد. داده‌های کیفی این تحقیق از مطالعهٔ منابع و پژوهشهای علمی و با استفاده از روش پژوهشی کیفی فراترکیب[1] جمع‌آوری گردید. رویکرد فرا ترکیب نوعی مطالعهٔ کیفی است که اطلاعات و یافته‌های استخراج‌شده از مطالعات کیفی دیگر با موضوع مشابه و مرتبط را بررسی می‌کند. درنتیجه، نمونهٔ موردنظر برای فراترکیب از مطالعات کیفی منتخب و بر اساس ارتباط آنها با سؤال پژوهش ساخته می‌شود. فراترکیب با فراهم کردن نگرشی سامانمند برای محققان، ازطریق ترکیب مطالعات کیفی گوناگون، به کشف موضوعات و استعاره‌های جدید و اساسی می‌پردازد و با این روش، دانش جاری را ارتقا می‌دهد و دید جامع و گستردهای نسبت به مسائل ایجاد می‌کند (کشتکار، ۱۳۹۵: ۱۶۵). «سه فاز اصلی برای فراترکیب، انتخاب مطالعات بر اساس جستجوی سیستماتیک و گزینش نهایی، ترکیب یافته‌ها بر اساس شباهتها و اختلافات و ارائهٔ تلفیقی یافته‌ها در دسته‌بندی گروهی است» (Sandelowski & Barros: 2007).

در این پژوهش محققان با مطالعه و واکاوی بیش از ۶۰ مقالهٔ علمی و اسناد رسمی و گزارش‌های تحقیقاتی قابل‌دسترس در زمینه‌های معماری امنیت‌پایه، معماری اینترنت اشیاء، امنیت و کاربردهای اینترنت اشیاء در صحنهٔ نبرد، اطلاعات اصلی موردنیاز را از بین ۲۵ مقالهٔ علمی – پژوهشی یا سند معتبر مرتبط با حوزهٔ موضوع، استخراج نمودند. در ادامه با روشهای خبرگی و منطقی به تحلیل و تلفیق یافته‌های حاصل از مطالعات کیفی پرداخته و یافته‌های جدید را ارائه نمودند. نتایج به‌دست‌آمده به تعدادی از خبرگان این حوزه که عمدتاً از محققان، کارشناسان و مدیران حوزهٔ دفاعی بوده و با فنّاوری اینترنت اشیاء آشنایی کامل داشته‌اند، ارائه گردید و سپس نظرات تکمیلی اصلاحی و یا انتقادی آنها دریافت و در ارزیابی نتایج اعمال گردید.

[1] Meta-Synthesis

پیشینهٔ تحقیق

برخی از تحقیقات و معماری‌های ارائه‌شدهٔ مرتبط با معماری اینترنت اشیاء و مناسب با موضوع و اهداف این تحقیق مورد بررسی و تحلیل قرار گرفته است که مهم‌ترین آنها عبارت‌اند از:

۱. خانم ترکمن و همکارش در مقاله‌ای با عنوان «تحلیل مدل‌های معماری مرجع اینترنت اشیاء» پس از بررسی معماری مرجع اینترنت اشیاء ارائه‌شده توسط اتحادیهٔ ارتباطات بین‌المللی[1] ، چهار پروژهٔ مرجع در حوزهٔ معماری اینترنت اشیاء توسط کشورهای چین و کره جنوبی را بررسی کرده و آنها را ازلحاظ مدیریت، قابلیت اطمینان، امنیت و نیازمندی‌های کارکردی با یکدیگر مقایسه نموده‌اند (Torkaman & Seyyedi, 2016).

۲. «بازنگری در اینترنت اشیاء برای دفاع و ایمنی عمومی» عنوان مقاله‌ای است که پائولا فراگا[2] و همکاران در آن به موضوعات اصلی مربوط به کاربرد مفاهیم اینترنت اشیاء در ارتش و حوزهٔ امنیت عمومی پرداخته‌اند. آنها نقاط ضعف اصلی و چالش‌های فنی اینترنت اشیاء را تشریح و یک مدل معماری را ارائه نموده‌اند. در این معماری لایه حس و دریافت، دسترسی، شبکه، خدمات، برنامه‌های کاربردی و کسب‌وکار لحاظ شده و پروتکل‌های مربوطه توضیح داده شده است (Paula, et.al., 2016).

۳. یک مدل سه‌لایه‌ای برای اینترنت اشیاء توسط آشیش مهتا[3] و همکاران در مقاله‌ای به نام «نقشهٔ معماری بیمارستان هوشمند مبتنی بر اینترنت اشیاء» پیشنهاد شده است. این معماری که در یکی از بیمارستان‌های دانشگاهی چین پیاده‌سازی شده، به علت ترکیب با چارچوب‌ها و برنامه‌های موجود بیمارستان، به‌خصوص سامانهٔ اطلاعاتی بیمارستانی[4] ، نتایج رضایت‌بخشی را به همراه داشته است. لایه‌های اصلی و زیرلایه‌های این معماری شامل لایهٔ ادراک (لایهٔ گردآوری داده و لایهٔ دسترسی)، لایهٔ شبکه (سکوی ارسال شبکه‌ای و سکوی برنامه‌های کاربردی) و لایهٔ برنامه‌های کاربردی (برنامه‌های مفید بیمارستانی و برنامه‌های کاربردی و مدیریت تصمیم‌گیری) است (Mehta & Dhariwal, 2017).

۴. در پژوهشی که توسط لی و همکاران تحت عنوان «بررسی و تحقیق بر روی اینترنت اشیاء» صورت گرفت، مدل معماری خدمت‌گرا در چهار لایه با اجزا، ارتباطات و لایه‌های معماری شامل لایهٔ

---

[1] International Telecommunication Union (ITU)
[2] Paula Fraga
[3] Ashish Mehta
[4] Hospital Information System (HIS)

حسگر، شبکه، خدمت و برنامه‌های کاربردی به‌طور کامل تشریح شده و سپس به فنّاوری‌های وابسته و استانداردهای مربوطه اشاره شده است. این تحقیق به چالش‌ها و مشکلات این حوزه مانند امنیت و حفظ حریم خصوصی نیز می‌پردازد (Li, et.al., 2015).

۵. دکتر شهریار محمدی و همکاران در مقاله‌ای تحت عنوان «معماری پیشنهادی مبتنی بر اینترنت اشیاء و سیستم‌های توصیه‌گر برای هوشمندسازی شهر تهران»، ضمن بررسی ۲۰ شهر هوشمند مطرح در سطح جهان و مشخص کردن کاربردهای اینترنت اشیاء در آنها یک مدل معماری را پیشنهاد داده‌اند. در این معماری، پنج لایهٔ زیرساخت، جمع‌آوری داده‌ها، مدیریت و پردازش داده‌ها، خدمات و برنامه‌های کاربردی لحاظ شده و اجزاء هر لایه به‌طور مشروح توضیح داده شده است (محمدی و همکاران، ۱۳۹۵).

۶. تحلیل تهدیدات و مخاطرات موجود در حوزهٔ امنیت و حریم خصوصی اینترنت اشیاء توسط ارکیان، پورخلیلی و خوش‌اخلاق در مقاله‌ای با عنوان «امنیت و حریم خصوصی در اینترنت اشیاء» با رویکردی نظام‌مند و مبتنی بر یک روش استاندارد صورت گرفته و راه‌حل‌ها و پیشنهادهای مختلفی مبتنی بر بخش‌های مختلف امنیت اینترنت اشیاء در آن ارائه شده است (ارکیان، پورخلیلی و خوش‌اخلاق، ۱۳۹۴).

مبانی و مفاهیم نظری

معماری امنیت پایه

«در معماری امنیت‌پایه، ارتباط همهٔ لایه‌ها و اجزایی که در لایه‌ها وجود دارد، به‌صورت امن تعریف می‌شود و مؤلفه‌های محرمانگی، دسترس‌پذیری و یکپارچگی به‌طور کامل در ارتباط بین اجزا و لایه‌ها رعایت می‌شود» (Truyen & frank, 2018: 1). یک معماری امنیتی دارای ساختاری از مؤلفه‌های سازمانی، مفهومی، منطقی و فیزیکی است که به روشی منسجم به‌منظور دستیابی و حفظ وضعیت ریسک، تعامل دارند. درواقع، معماری امنیتی محرک و فراهم‌کنندهٔ رفتار امن، ایمن و قابل‌اعتماد است و به تمامی ریسک‌های سازمان رسیدگی می‌نماید. هدف معماری امنیتی فراسازمانی، ارائهٔ یک رویکرد جامع برای امنیت در سطح فراسازمانی و ارائهٔ راهنمایی‌های مؤثر و کارآمد برای تمامی اهداف امنیتی در داخل سازمان است (شورای اجرایی (عالی) فنّاوری اطلاعات کشور، ۱۳۹۶).

مفهوم اینترنت اشیاء

اصطلاح اینترنت اشیاء، نخستین بار در سال ۱۹۹۹ میلادی توسط کوین اشتون مورد استفاده قرار

گرفت. اتحادیهٔ ارتباطات بین‌المللی، این فنّاوری را این‌گونه تعریف می‌کند: «ارتباط هر چیز، در هر مکان و در هر زمان، مفهومی به نام اینترنت اشیاء را پدید می‌آورد» (ITU, 2005). مؤسسه مکنزی در تحقیقی بیان می‌دارد: «اقتصاد جهانی فنّاوری اینترنت اشیاء در سال ۲۰۲۵ بین ۳,۹ تا ۱۱,۱ تریلیون دلار در هر سال خواهد بود» (مکنزی، ۲۰۱۶).

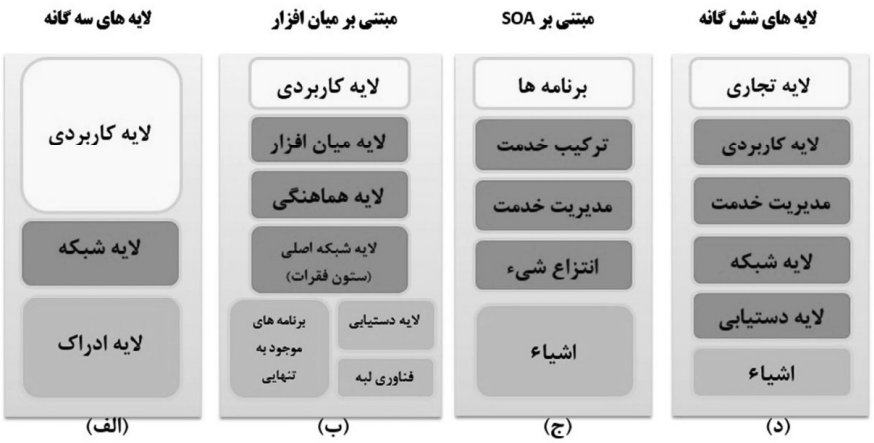
فنّاوری اینترنت اشیاء در صحنهٔ نبرد کاربرد مؤثری دارد و به‌گونه‌ای منسجم و یکپارچه به جمع‌آوری داده‌های محیطی دفاعی و رزمی در زمان و مکان مناسب پرداخته و پس از پردازش داده‌ها (شامل دسته‌بندی، ادغام و تجزیه‌وتحلیل) و تولید و انتقال اطلاعات به فرماندهان و تصمیم‌گیرندگان در درک مؤثر صحنهٔ نبرد کمک شایانی می‌نماید، به‌گونه‌ای که اطلاعات «هرزمان، هر جا و برای هر فرد» در دسترس خواهد بود (NATO, 2017).

معماری‌های اینترنت اشیاء

توسعه اینترنت اشیاء مبتنی بر توسعهٔ زیرساخت، ارتباطات، واسط‌ها، پروتکل‌ها و استانداردهایی است که همگی از موضوعات تحقیقاتی جدید و به‌روز محسوب می‌شوند. توسعه‌پذیری[1]، مقیاس‌پذیری[2]، قابلیت همکاری[3] میان دستگاه‌های ناهمگن[4] و مدل‌های کسب‌وکار (با توجه به ماهیت متحرک بودن اشیاء و غیرمتمرکز بودن فرایندها)، ازجمله مؤلفه‌های مهمی هستند که در طراحی معماری اینترنت اشیاء باید در نظر گرفت (Li, et.al., 2013: 2235). اینترنت اشیاء باید قادر به اتصال میلیاردها اشیاء ناهمگن ازطریق اینترنت باشد، ازآنجایی‌که اینترنت اشیاء در زمینه‌های مختلف کاربردی نظیر مراقبت‌های بهداشتی، سیستم‌های حمل‌ونقل هوشمند، مدیریت صنعتی و دیگر موارد، کاربرد دارد، تحقق مسائل امنیتی به‌منظور ایجاد سیستم‌های قابل‌اعتماد و برنامه‌های کاربردی، مورد نیاز است. وجود یک معماری لایه‌ای انعطاف‌پذیر، ضروری است (Gupta & Quamara, 2018: 305). «معماری اینترنت اشیاء باید به‌اندازهٔ کافی انعطاف‌پذیر باشد تا بتواند، پاسخگوی عوامل مختلفی از قبیل کیفیت سرویس، مدولار بودن[5]، قابلیت اطمینان، مدیریت حریم خصوصی، تعامل معنایی[6]

[1] Extensibility
[2] Scalability
[3] Interoperability
[4] Heterogeneous
[5] Modularity
[6] Semantic Interoperability

، پشتیبانی دستگاه‌های مختلف و دیگر موارد باشد» .(Ray, 2018: 14) بسیاری از سازمان‌های بین‌المللی شناخته‌شده و گروه‌های کاری از قبیل اتحادیه بین‌المللی مخابرات، انجمن مهندسان برق و الکترونیک[1] ، سازمان سیسکو، موسسهٔ استانداردسازی ارتباطات اروپا[2]و اتحادیه اروپا بر اساس نیازمندی‌های برنامه، توپولوژی شبکه، پروتکل‌ها، مدل‌های کسب‌وکار، خدمات و دیگر موارد، چارچوب‌هایی را ارائه کرده‌اند. بااین‌حال، هیچ‌یک از آنها تا به این تاریخ استاندارد نشده است(Gupta & Quamara, 2018: 307; Ray, 2018: 18). در شکل شمارهٔ ۱، متداول‌ترین معماری‌های اینترنت اشیاء نشان داده شده است.



شکل شمارهٔ ۱: معماری اینترنت اشیاء؛(الف) معماری سه‌لایه‌ای، (ب) معماری مبتنی بر میان‌افزار، (ج) معماری مبتنی بر خدمت (SOA)، (د) معماری شش‌لایه‌های

«معماری سه‌لایه‌ای، معماری اصلی و پایهٔ اینترنت اشیاء است که از لایه‌های ادراک، شبکه و کاربرد تشکیل شده است» (Sarkar, et.al., 2014: 510)، اما سایر مدل‌ها از سطح انتزاع بیشتری برخوردار هستند. بااین‌حال، «معماری پنج‌لایه برای برنامه‌های کاربردی مبتنی بر اینترنت اشیاء کارآمدی بیشتری دارد»(Al-Fuqaha ,et.al., 2015: 2349).

در معماری اینترنت اشیاء اتحادیهٔ ارتباطات بین‌المللی چهار لایهٔ اصلی، دو لایهٔ پشتیبان و همچنین هفت صنعت هوشمند مورد توجه قرار گرفته است. لایه‌های دستگاه‌ها، گذرگاه‌ها و وسایل، لایهٔ شبکه، لایهٔ پشتیبانی کاربرد و خدمات و لایهٔ برنامه‌های کاربردی به‌عنوان

[1] Institute of Electrical and Electronics Engineers (IEEE)
[2] European Telecommunications Standards Institute (ETSI)

لایه‌های اصلی و دو لایهٔ مدیریت و امنیت به‌عنوان لایه‌های فرعی در نظر گرفته شده‌اند. در این معماری از زندگی هوشمند، سلامت هوشمند، انرژی هوشمند، خانه‌های هوشمند، حمل‌ونقل هوشمند و شهر هوشمند به‌عنوان صنعت‌های هوشمند نام برده شده است. از نقاط قوت این معماری در نظر گرفتن صنایع هوشمند استفاده‌کننده از اینترنت اشیاء و در نظر گرفتن دو مقولهٔ امنیت و مدیریت در مدل ارائه شده است (Vermesan & fries, 2014: 14).

«در جدول شمارهٔ (۱)، مقایسه‌ای بر روی چهار معماری اصلی در حوزهٔ اینترنت اشیاء، قابل مشاهده است» (پاکروان و عسکریان‌ابیانه، ۱۳۹۷: ۴).

	ITU	CISCO	IOT-A	SOA
مدل لایه‌بندی	۴ لایهٔ افقی ۲ لایهٔ عمودی	۳ لایهٔ افقی	۷ لایهٔ افقی ۲ لایهٔ عمودی	۴ لایهٔ افقی ۱ لایهٔ عمودی
کنترل‌پذیری	لایهٔ عمودی مدیریت	توزیع‌شده	لایهٔ عمودی مدیریت	توزیع‌شده
امنیت و محرمانگی	لایهٔ عمودی امنیت	توزیع‌شده	لایهٔ عمودی امنیت	لایهٔ عمودی امنیت
تحرک پذیری	دارد	دارد	دارد	دارد
مدیریت انرژی	دارد	دارد	دارد	دارد
سرویس‌دهی	دارد	دارد	دارد	دارد

جدول شمارهٔ ۱: مقایسه‌ای بر روی چهار معماری اصلی در حوزهٔ اینترنت

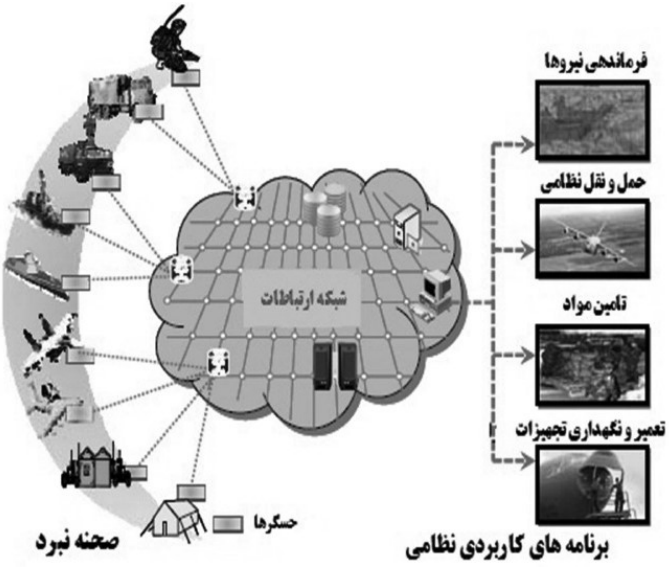
از مقایسهٔ این معماری‌ها می‌توان تشابه‌ها و تفاوت‌های ذیل را مشاهده نمود: تمامی معماری‌های ارائه‌شده دارای ساختار لایه‌بندی بوده و در دو لایهٔ دستگاه و شبکه ازلحاظ کارکردی مشترک هستند. لایهٔ امنیت در سه مدل ارائه‌شده، غیر از مدل سیسکو به‌صورت عمودی دیده شده است تا بتوان سیاست‌های امنیتی را به تمام لایه‌های افقی اعمال نمود. در دو مدل «ITU» و «IOT-A» لایهٔ مدیریت نیز به‌صورت عمودی دیده شده است. می‌توان گفت با توجه به اهداف «IOT-A»، مدل مرجع «ITU» را به یک مدل عملیاتی تبدیل نموده است. البته در هر دو مدل «SOA» و سیسکو نیز سرویس‌گرایی بیشتری وجود دارد و با توجه به ماهیت این مدل‌ها، بُعد مدیریت یکپارچهٔ آن، کم‌رنگ‌تر است.

اینترنت اشیاء در صحنهٔ نبرد

گسترش و توسعهٔ کاربردهای اینترنت اشیاء در حوزه‌های دفاع و امنیت کشورها، به‌ویژه در زیرساخت‌های عمومی، خدمات اضطراری و ردیابی تجهیزات باعث شده تا سازمان‌های دفاعی و نظامی درصدد استفاده از فنّاوری اینترنت اشیاء برای هدایت و مدیریت تجهیزات جنگی، تدارکات، رصد فعّالیت‌های نظامی سربازان در میدان‌های جنگ، آموزش و همکاری نیروها، فرماندهی و کنترل[1] ، نظارت و مدیریت سامانه‌های کنترل آتش و دیگر موارد، بوده تا از مزایای آن در کاهش هزینه‌ها، افزایش اشرافیت اطلاعاتی و حتی از اثرات مثبت حاکمیتی اینترنت اشیاء و محیط ابری استفاده نمایند.

استفادهٔ روزافزون از فنّاوری‌هایی همچون شبکه‌های بی‌سیم و دستگاه‌های هوشمند که مجهز به حسگرهای مختلف، برچسب‌های ردفاشگر[2] و ارتباطات میدان نزدیک می‌باشند، منجر به توسعهٔ به‌کارگیری فنّاوری نوین اینترنت اشیاء در پوشیدنی‌های هوشمند و تجهیزات مختلف دفاعی، نظارتی، امنیتی و خدمات اضطراری شده است. امروزه مأموریت‌های نظامی مستلزم تعاملات مداوم و بدون وقفه بین نیروهای زمینی، دریایی، هوایی، مراکز فرماندهی و تجهیزات نظامی است. یکپارچگی سنسورها، همکاری داده‌ها و محاسبات امن، گام بعدی در راستای تحقق قابلیت‌های میدان جنگ‌های آینده است. در این دهه، اینترنت اشیاء نظامی با مزایا و ویژگی‌های خاص خود برای کاربران، روند جدیدی در فنّاوری ایجاد کرده است. این پتانسیل با ترکیب فنّاوری‌های مبتنی بر اینترنت اشیاء، تجزیه‌وتحلیل کلان داده‌ها، امنیت در چند لایهٔ مستقل[3] ، شبکه‌های تعریف‌شدهٔ نرم‌افزاری، زیرساخت شبکه‌های هوشمند و مجازی‌سازی، امکان دستیابی به یک صحنه نبرد را فراهم می‌نماید. در شکل شمارهٔ ۲، این مفهوم نشان داده شده است (Yushi, et.al., 2011: 632).

[1] Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)
[2] RFID
[3] Multiple Independent Levels of Security (MILS)



شکل شمارهٔ ۲: مفهوم اینترنت اشیاء در صحنهٔ نبرد

یکی از برنامه‌های کاربردی مورد استفاده در صحنهٔ نبرد، سامانه‌های کنترل آتش پیشرفتهٔ خودکار بوده که با بهره‌گیری از اینترنت اشیاء می‌توان شناسایی و ردیابی یک بار مهمات هدایت‌شده به ۱۰۰ هدف مستقل را در یک زمان کاملاً کنترل نمود. مهمات می‌تواند به شبکه متصل شده و به سلاح‌های هوشمند اجازه داده شود تا اهداف را دنبال کنند. همچنین ازطریق کنترل ماهواره‌ای می‌توان موشک شلیک‌شده را به سمت یک هدف جدید هدایت نمود (Jacobson, 2015: 5).

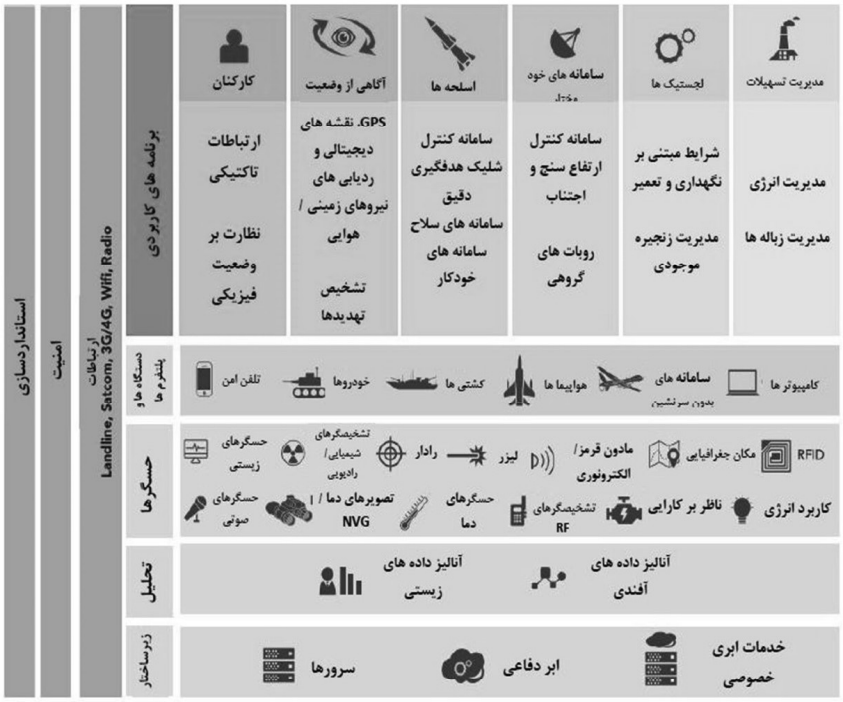
سربازان در میدان نبرد ازطریق گوشی‌های هوشمند امن به این شبکه متصل می‌شوند و طیف وسیعی از برنامه‌های کاربردی، نقشه‌های سه‌بعدی، ردیابی نیروی آبی، ترجمه زبان و پروفایل‌های باارزش برای آنها فراهم می‌گردد.

اجزاء و زیرساخت‌های فنّاوری اینترنت اشیاء در سازمان‌های دفاعی

اطلاعات صحنهٔ نبرد ازطریق میلیون‌ها حسگر تعبیه‌شده در تجهیزات و وسایلی مانند رادارها، سونار، دوربین‌های تصویری، حسگرهای مادون‌قرمز، فرکانس رادیویی، حسگرهای سامانه‌های هوابرد، ماهواره‌های نظارتی، وسایل نقلیهٔ بدون سرنشین[1]، کشتی و ناوهای جنگی، ایستگاه‌های زمینی، سربازان و دیگر موارد، در فضا، دریا و زمین جمع‌آوری و ازطریق زیرساخت‌های تعبیه‌شده به سرورهای مربوطه

[1] Unmanned Aerial Vehicles (UAVs)

ارسال و برای تجزیه‌وتحلیل به مرکز اصلی سامانهٔ فرماندهی و کنترل؛ یعنی سامانهٔ زمین مشترک توزیع‌شده[1] فرستاده می‌شود. در شکل شمارهٔ ۳، اجزا و زیرساخت‌های فنّاوری اینترنت اشیاء نظامی آمریکا نمایش داده شده است (Zheng & Carter, 2015: 14).



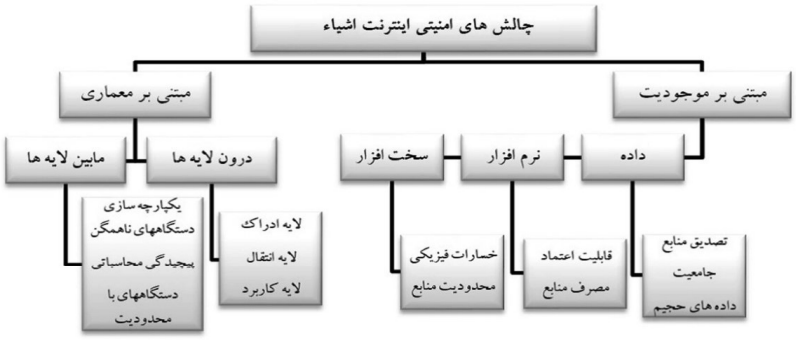
شکل شمارهٔ ۳: اجزا و زیرساخت‌های فنّاوری اینترنت اشیاء نظامی آمریکا

چالش‌ها و الزامات امنیتی اینترنت اشیاء در صحنهٔ نبرد

اینترنت اشیاء در حال تبدیل شدن به یک عنصر کلیدی از اینترنت آینده و یک زیرساخت حیاتی ملّی و بین‌المللی است. با این شرایط، تأمین امنیت کافی برای زیرساخت‌های اینترنت اشیاء در صحنه‌های نبرد، اهمیت روزافزونی پیدا می‌کند. در صحنهٔ نبرد، برنامه‌های کنترل و فرماندهی و خدمات عملیاتی مبتنی بر اینترنت اشیاء به‌طور فزاینده‌ای در برابر هرگونه اختلال، حملات و یا سرقت اطلاعات، آسیب‌پذیر هستند. شناخت این چالش‌ها، تهدیدات و ریسک‌های امنیتی در طراحی معماری امن بسیار ضروری است. از منظرهای گوناگونی مانند اجزا و لایه‌های معماری، امنیت و حریم خصوصی، زیرساخت، پروتکل‌های مربوطه

[1] Distributed Common Ground System (DCGS)

و آسیب‌پذیری تجهیزات اینترنت اشیاء می‌توان این چالش‌ها را بررسی، دسته‌بندی و ارزیابی نمود. مهم‌ترین چالش‌های توسعهٔ اینترنت اشیاء و به‌کارگیری آن در صحنهٔ نبرد عبارت‌اند از دسترس‌پذیری [۱]، قابلیت اطمینان [۲]، متحرک بودن [۳]، عملکرد [۴]، مدیریت [۵]، مقیاس‌پذیری، قابلیت همکاری، امنیت و حریم خصوصی [۶]، محدودیت و مصرف منابع. این چالش‌ها عمدتاً از حوزه‌های ادبیات و مصاحبه‌ها به دست آمده است.



شکل شمارهٔ ۳: چالش‌های مهم امنیتی در اینترنت اشیاء در صحنهٔ نبرد

شکل شمارهٔ ۴، چالش‌های امنیتی اینترنت اشیاء را از منظر معماری و موجودیت نشان می‌دهد. چالش‌های مبتنی بر معماری، مسائل خاص مربوط به هر لایه و نیز مسائل مربوط به یکپارچه‌سازی لایه‌ها در یک چارچوب واحد را پوشش می‌دهند. چالش‌های امنیتی مبتنی بر موجودیت بر مسائل مرتبط با امنیت اجزای سه نهاد اساسی هر سامانهٔ محاسباتی؛ یعنی سخت‌افزار، نرم‌افزار و داده‌ها تمرکز دارد (Gupta & Quamara, 2019: 38).

مؤلفه‌ها و سیاست‌های امنیتی در اینترنت اشیاء در صحنهٔ نبرد

مهم‌ترین مؤلفه‌های امنیتی در اینترنت اشیاء در صحنهٔ نبرد که عمدتاً از حوزه‌های ادبیات به دست آمده، در جدول شمارهٔ ۲ نشان داده شده است.

---

[1] Availability
[2] Reliability
[3] Mobility
[4] Performance
[5] Management
[6] Security and Privacy

مؤلفه‌ها	شرح مؤلفه
احراز هویت	روشی برای شناسایی کاربران مجاز برای ورود به سامانه‌ها است. در محیط‌های رزمی از روش‌های احراز هویت چندمرحله‌ای مانند کلمه و رمز عبور، بیومتریک، موبایل و... استفاده می‌شود.
کنترل دسترسی	باید مشخص شود که هر کاربر یا دستگاه به کدام بخش از سرویس‌های اینترنت اشیاء و یا داده‌ها حق دسترسی و استفاده دارد. در محیط‌های نظامی باید مکانیسم خاصی برای دسترسی به خدمات برای کاربران تعریف شود.
محرمانگی	اطلاعات و سرویس‌های موجود در صحنهٔ نبرد باید فقط در اختیار افراد مجاز قرار بگیرد. این محرمانگی باید بر اساس اطلاعات (سری، خیلی محرمانه، محرمانه و عادی) صورت گیرد.
یکپارچگی	باید خدمات و داده‌های موجود در محیط نظامی به‌صورت یکپارچه و در کل صحنه نبرد اعم از زمینی، دریایی و هوایی با یکدیگر در تعامل باشند تا از وجود داده‌های تکراری و یا فقدان داده جلوگیری شود.
دسترس‌پذیری	خدمات موجود در صحنه نبرد باید دارای این قابلیت باشد که در هر شرایط بحرانی و عملیاتی به دست بهره‌برداران مجاز برسد.
حریم خصوصی	اطلاعات هر کاربر فقط در اختیار وی باشد و دیگران حق دسترسی به این اطلاعات را نداشته باشند.
اعتماد	شامل اعتماد کاربران به فراهم‌کنندگان خدمات اینترنت اشیاء و اعتماد فراهم‌کنندگان خدمات به کاربران و بهره‌برداران خود است.
عدم انکار	بهره‌برداران از خدمات اینترنت اشیاء نباید بتوانند استفاده از خدمات را منکر شوند.
ارتباطات امن	یکی از الزامات مهم امنیتی، وجود زیرساخت ارتباطی امن بین بخش‌های مختلف موجود در صحنهٔ نبرد و همچنین ارتباطات بین لایه‌های معماری اینترنت اشیاء است.

جدول شمارهٔ ۲: مؤلفه‌های مهم امنیتی در اینترنت اشیاء در صحنهٔ نبرد

برای ایجاد یک معماری امنیت‌پایه لازم است که اینترنت اشیاء گره‌های فیزیکی امنیتی، اکتساب اطلاعاتی امن، انتقال اطلاعاتی امن و پردازش اطاعاتی امن داشته باشد تا به صحت، محرمانه بودن و انسجام اطلاعاتی برسد. به همین منظور، نیازمند داشتن سیاست‌های امنیتی در حوزه‌های سخت‌افزار فیزیکی، شبکهٔ حسگر، پایانه‌های حسگر، کسب اطلاعات، پردازش اطلاعات، انتقال اطلاعات و امنیت اطلاعات برنامه‌های کاربردی است.

تجزیه‌وتحلیل یافته‌های تحقیق

ازآنجاکه امنیت و حریم خصوصی، مهم‌ترین و شاخص‌ترین مؤلفه اینترنت اشیاء در حوزهٔ نظامی است، بایستی خدمت امنیت بر روی همهٔ اجزا و مؤلفه‌های آن تأثیرگذار باشد. به‌عبارتی‌دیگر، باید یک معماری امنیت‌پایه مدنظر قرار بگیرد. تأمین یکپارچگی، محرمانگی و دسترس‌پذیری به خدمات، به‌ویژه در شرایط بحرانی و میدان نبرد بسیار ضروری است. همچنین، در نظر گرفتن شاخص‌های امنیتی نظیر احراز هویت، دسترس‌پذیری، سطوح دسترسی به خدمات، محرمانگی، حریم خصوصی و رمزنگاری در همهٔ سطوح انتقال داده الزامی است.

بر اساس مدل‌های معماری بررسی‌شده در پژوهش، مدل معماری ارائه شده توسط اتحادیهٔ ارتباطات بین‌المللی که با مدل شش‌لایهٔ فضای سایبری کشور ارائه شده توسط شورای عالی فضای مجازی، نزدیکی بیشتری داشت، مدنظر قرار گرفت. در ادامه با توجه به نیازمندی‌های صحنهٔ نبرد و امنیت‌پایه بودن آن و همچنین مؤلفه‌ها و سیاست‌های امنیتی احصاءشده، معماری تدوین گردید.

به‌منظور به‌کارگیری مفید و مؤثر اینترنت اشیاء در نیروهای مسلح و به‌ویژه در صحنهٔ نبرد، باید از یک معماری چندلایه‌ای خدمت‌گرا و چارچوب مبتنی بر رایانش ابری استفاده کرد تا علاوه بر کاهش هزینه‌ها، قابلیت مقیاس‌پذیری نیز مهیا شود. این چارچوب امکان انجام محاسبات، تجزیه‌وتحلیل و ذخیره‌سازی را به‌صورت جداگانه برای بهره‌برداران فراهم می‌کند. بنابراین، امکان توسعه و گسترش هر بخش به‌صورت جداگانه و درنهایت تکامل یکدیگر از طریق خدمات موجود در یک محیط اشتراکی فراهم می‌گردد. با توجه به اینکه این معماری برای میدان نبرد طراحی می‌گردد، ازاین‌رو، مؤلفه‌های تحرک‌پذیری تجهیزات و سیار بودن ارتباطات، انتقال داده‌های فراوان به‌صورت بلادرنگ، تحویل مطمئن اطلاعات و عدم وابستگی به تجهیزات خاص در لایه‌های معماری مورد توجه قرار گرفته است. با به‌کارگیری رایانش مه [1] برای پردازش داده‌ها بین ابر و دستگاه‌های اینترنت اشیاء در این معماری، ضمن استفاده از مزایای آن مانند افزایش امنیت، کاهش پهنای باند و کاهش تأخیر در شبکه، می‌تواند تا حدودی این نواقص را پوشش دهد.

معماری پیشنهادی دارای چهار لایهٔ افقی اشیاء، زیرساخت و شبکه، خدمات و برنامه‌های کاربردی و دو لایه عمودی مدیریت و مقررات (حکمرانی) و امنیت بوده که در شکل شمارهٔ ۵، قابل‌مشاهده است. این معماری پیشنهادی برای ارزیابی و اعتباربخشی به رؤیت خبرگان این تحقیق که عموماً از مدیران، فرماندهان حوزه‌های دفاعی آشنا با فنّاوری اینترنت اشیاء، دانشجویان دکتری مدیریت راهبردی فضای سایبر و متخصصان این فنّاوری هستند، رسیده است. در ادامه، نظرات تکمیلی اصلاحی و یا انتقادی آنها از طریق مصاحبه دریافت و در ارزیابی نتایج اعمال گردید. درنهایت مدل پیشنهادی به‌طور مجدد به رؤیت و تأیید جامعهٔ مذکور رسیده است.

معماری امنیت‌پایه پیشنهادی اینترنت اشیاء برای صحنهٔ نبرد

معماری پیشنهادی (معماری امنیت‌پایه برای صحنهٔ نبرد مبتنی بر فنّاوری اینترنت اشیاء) در شش لایه تعبیه شده است که در شکل شمارهٔ، قابل‌مشاهده است. اکنون به تشریح اجزاء، لایه‌ها، ارتباطات مؤلفه‌ها و سیاست‌های امنیتیِ معماری پیشنهادی می‌پردازیم.

[1] Fog Computing

۱. امنیت در لایهٔ اشیاء [1]

این لایه، پایین‌ترین لایهٔ معماری بوده و از شبکهٔ حسگرهای بی‌سیم، دوربین‌ها، فعّال‌کننده‌ها، سیستم‌های توکار و دستگاه‌های مختلف تشکیل شده است که با یکدیگر ارتباط برقرار کرده و برای شناسایی و جمع‌آوری اطلاعات صحنهٔ نبرد استفاده می‌شوند. در این لایه انواع حسگرهای موردنیاز صحنهٔ نبرد مانند حسگرهای رادار، سونار، شیمیایی، زیستی، حرارتی، مادون‌قرمز، رادیویی، تشخیصی، لیزری، صوتی و دیگر موارد، دیده شده است. ارتباطات فرد با فرد، فرد با ماشین و ماشین با ماشین و ازطریق فنّاوری‌هایی مانند «GSM»، «WSN»، «Zigbee»، «6LoWPLAN»، «5G»، «4G»، «Wi-Fi»، «UMTS»، «بلوتوث» و دیگر موارد، میسر است. با توجه به اینکه در این لایه با دستگاه‌هایی با منابع محدود، توان محاسباتی پایین و مستعد آسیب و حملات سروکار داریم، رویکرد رمزنگاری سبک‌وزن در هر دو بخش رمزهای قالبی و رمزهای جریانی بیشتر مورد توجه است. سیاست‌های امنیتی این لایه عبارت‌اند از ایمنی کسب داده‌ها و امنیت سخت‌افزارها مثل حسگرها و گره‌های برچسب‌های ردفاشگر [2] و پیکربندی امن تجهیزات، داده، حسگرهای محافظت‌شده و وضع قوانین امنیتی، می‌توانند مفید باشند. مؤلفه‌های امنیتی یکپارچگی، صحت داده و حریم خصوصی حائز اهمیت می‌باشند.

۲. امنیت در لایهٔ زیرساخت و شبکه

لایهٔ شبکه و زیرساخت، امکانات شبکه‌ای موردنیاز را فراهم می‌کند و فنّاوری‌ها و پروتکل‌های متعددی را به خدمت می‌گیرد و قابلیت شبکه‌سازی و انتقال اطلاعات را دارد. در این لایه با توجه به ماهیت صحنهٔ نبرد می‌بایست از شبکه‌ها و ارتباطات مختلفی نظیر شبکهٔ ارتباطی موبایل [3]، شبکه حسگر بی‌سیم [4]، شبکه سیار [5]، ارتباطات ماهواره‌ای [6] و سایر شبکه‌ها استفاده نمود. این شبکه‌ها می‌توانند به‌صورت خصوصی، عمومی و یا ترکیبی باشند که برای پشتیبانی از ارتباطات موردنیاز در صحنهٔ نبرد با امنیت لازم ساخته شده‌اند. در این لایه، برای داشتن چارچوبی ایمن برای شبکه‌ها باید از ادغام سیاست‌های مختلف امنیتی مانند الگوریتم‌های رمزنگاری متقارن، سیاست‌های توزیع کلید، مکانیسم‌های تشخیص نفوذ، سیاست‌های احراز هویت، کنترل جریان داده،

[1] Objects
[2] RFID
[3] LET
[4] Wireless Sensor Networks (WSN)
[5] VAnet
[6] Satellite

سیاست‌های مسیریابی امن و دیگر موارد، استفاده گردد. حفظ صحت، محرمانگی، یکپارچگی و در دسترس بودن داده‌ها در حین انتقال در شبکه، ضروری است.

۳. امنیت در لایهٔ مدیریت خدمات‌دهی

لایهٔ سوم معماری پیشنهادی، مدیریت خدمات‌دهی است که در این لایه، امکانات متعددی به‌منظور مدیریت، رصد و پایش، هماهنگی خدمات، خدمات امنیتی و پردازش اطلاعات، ارائه شده است. توجه به امکانات این لایه، به‌ویژه از منظر معماری خدمات‌محور، بسیار حائز اهمیت است، چراکه بسیاری از برنامه‌های کاربردی مورد استفاده در لایهٔ بعدی، به‌طور مستقیم تحت تأثیر معماری این لایه قرار خواهند گرفت. درحقیقت، از این لایه می‌توان در این معماری به‌عنوان لایهٔ مدیریت فرماندهی و کنترل نام برد. ابر دفاعی، پایگاه‌های دادهٔ دفاعی، تحلیل داده‌های صحنهٔ نبرد و دیگر موارد، همه در این لایه پیش‌بینی شده است. مدیریت خدمات امکان پردازش اطلاعات را ازطریق تجزیه‌وتحلیل اطلاعات، کنترل امنیت، مدل‌های فرایندی و ابزارهای مدیریتی فراهم می‌کند. محاسبات چندبخشی امن، محاسبات ابری امن، امنیت ماشین‌های مجازی و ارتباطات، دسترس‌پذیری، کنترل دسترسی و تضمین امنیت و محرمانگی (حریم خصوصی) داده‌ها بین خدمات، توسط خدمات امنیتی در نظر گرفته شده در این معماری انجام می‌پذیرد.

۴. امنیت در لایهٔ برنامه‌های کاربردی

در بالاترین لایهٔ معماری، لایهٔ برنامه‌های کاربردی قرار دارد که وظیفهٔ محاسبات و پردازش داده‌هایی که توسط لایهٔ ادراک و اشیاء جمع‌آوری‌شده را بر عهده دارد. مسئولیت این لایه، ساختن یک مدل گرافیکی مبتنی بر داده‌ها است که از لایهٔ خدمات دریافت میکند. این لایه ارتباط مستقیمی با مرکز فرماندهی و کنترل صحنهٔ نبرد دارد و فرماندهان با استفاده از سامانه‌هایی نظیر امداد و نجات، نظارت و شناسایی، کنترل تسلیحات، پشتیبانی نظامی، تحرکات نیروها، وضعیت سلامت نیروها، فرماندهی و کنترل و دیگر موارد، به هدایت و فرماندهی صحنهٔ نبرد می‌پردازند. اطلاعات این سامانه می‌تواند به‌طور هم‌زمان در اختیار نیروهای زمینی، دریایی و هوایی نیز قرار بگیرد.

برنامه‌های کاربردی با مسائل امنیتی مختلفی در حوزهٔ نرم‌افزار و داده روبه‌رو هستند. حفاظت از داده‌ها، پشتیبان‌گیری از داده‌ها و مکانیسم‌های بازیابی اطلاعات برای رسیدن به امنیت استفاده می‌شود. برای اطمینان از امنیت داده‌ها در برنامه‌های کاربردی، باید مدیریت امنیتی و الگوریتم‌های رمزگذاری و رمزگشایی بر پایگاه داده اعمال گردد. مؤلفه‌های مدیریت دسترسی، برای جلوگیری از دسترسی غیرمجاز به پایگاه داده‌ای و همچنین

مدیریت پایگاه داده‌ای، اعمال گردد. احراز هویت به‌صورت چندعامله، مجازشناسی و حسابرسی[1] محافظت از حریم خصوصی، تعیین سطوح دسترسی، ضدهرزنامه، آنتی‌ویروس و دیگر موارد، ضروری است.

۵. لایهٔ مدیریت و مقررات

در کنار تمام این لایه‌هایی که توضیح داده شد، لایهٔ مدیریت و مقررات (حکمرانی)، نقش یکپارچه‌کنندهٔ شبکهٔ اصلی، تدوین استانداردهای ملّی و بین‌المللی، تدوین سیاست‌های دفاعی امنیتی و رصد و پایش را در تمام این معماری ایفا می‌کند. همان‌طور که در شکل شمارهٔ (۵) می‌بینیم، این لایه، همهٔ لایه‌های معماری؛ یعنی لایهٔ اول تا چهارم را پوشش می‌دهد. در یک صحنهٔ نبرد، چون اجزاء به‌صورت توزیع‌شده هستند، نیاز به سطح مدیریتی داریم که فعّالیت این اجزاء را در کل شبکه‌ای که منطقه عملیاتی را فرا گرفته، از حسگرها تا محیط‌های ابری، محیط‌های زیرساخت و خدمات‌دهی را مدیریت کند و هماهنگی بین اهداف هر یک از اجزاء برای رسیدن به یکپارچگی کلی را فراهم نماید. بنابراین، مدیریت به‌عنوان جزء جدایی‌ناپذیر در معماری صحنهٔ نبرد مبتنی بر اینترنت اشیاء به‌حساب می‌آید.

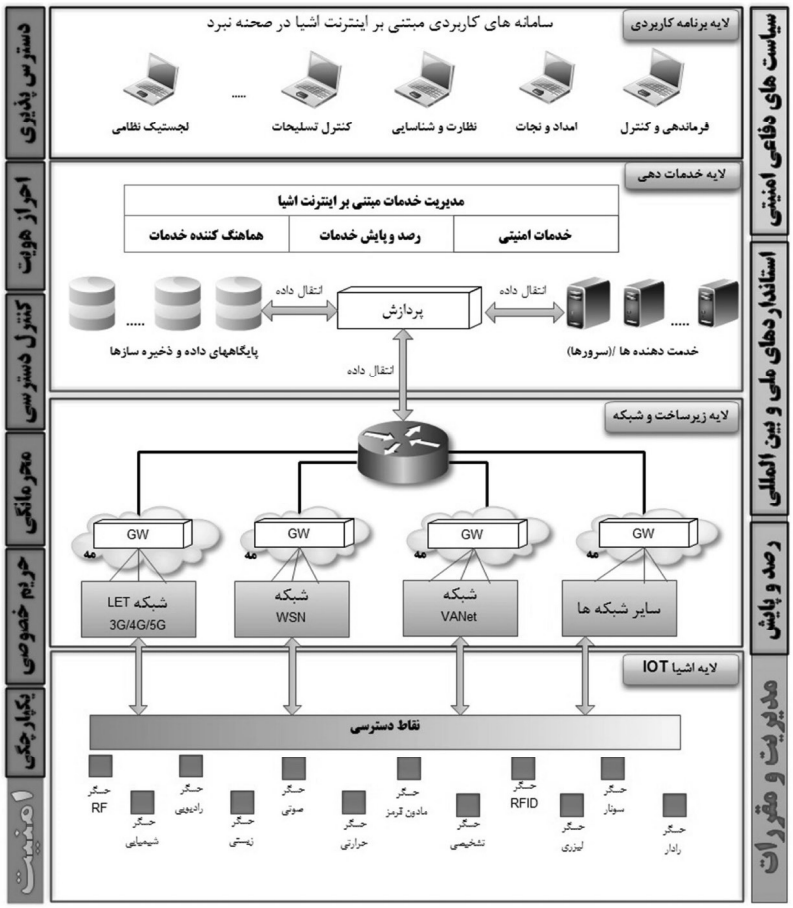
۶. لایهٔ امنیت

اولین و مهم‌ترین لایهٔ این معماری، لایهٔ امنیت است که با در نظر گرفتن امنیت‌پایه بودن معماری پیشنهادی و حساسیت صحنه نبرد، از اهمیت بسیار بالایی برخوردار است. این لایه همچون لایهٔ مدیریت، از لایهٔ پایینی اشیاء هوشمند تا لایهٔ بالایی برنامه‌های کاربردی باید به اجرا درآید و کلیهٔ ارتباطات و اجزاء را دربرگیرد، چراکه مقولهٔ امنیت یک فرایند است، فرایندی که می‌بایست در تک‌تک لایه‌ها، اجزاء معماری و ارتباطات آنها پیش‌بینی گردد.

کلیهٔ سیاست‌های امنیتی و کنترل‌های دفاعی باید در این لایه پیش‌بینی، تعریف، اجرا، رصد و پایش گردد. مؤلفه‌های امنیتی همچون یکپارچگی، محرمانگی، دسترس‌پذیری، کنترل دسترسی، شناسایی و احراز هویت، اعتماد و حریم خصوصی باید در همهٔ اجزای معماری شامل کاربران، حسگرها، نرم‌افزارها، سخت‌افزارها، شبکه‌ها، پروتکل‌ها، سامانه‌ها و دیگر موارد، لحاظ گردد. مدیریت و به‌کارگیری سیاست‌های رمزنگاری داده‌ها، زیرساخت کلید عمومی[2]، سازوکارهای اعتباردهی و اعتبارسنجی خدمت‌دهنده‌ها و خدمت‌گیرندگان از دیگر وظایف این لایه است.

---

[1] Authentication, Authorization, Acounting (AAA)
[2] Public Key Infrastructure (PKI)



شکل شمارهٔ ۵: معماری امنیت‌پایهٔ پیشنهادی برای صحنهٔ نبرد مبتنی بر فنّاوری اینترنت اشیاء

مزیت‌های اصلی معماری پیشنهادی در مقایسه با سایر معماری‌ها عبارت‌اند از:

۱. قرار دادن لایهٔ امنیت در معماری و تأثیر آن در همهٔ لایه‌های دیگر به‌منظور افزایش ضریب امنیت در همهٔ بخش‌های معماری.

۲. قرار دادن لایهٔ مقررات و قوانین به‌صورت عرضی در کنار همهٔ لایه‌های موجود در معماری.

۳. با توجه به ممزوج شدن فنّاوری اینترنت اشیاء با فنّاوری رایانش ابری، در این معماری، خدمات اینترنت اشیاء در صحنهٔ نبرد مبتنی بر محیط‌های ابری (ابر دفاعی) در نظر گرفته شده است.

نتیجه‌گیری و پیشنهادها

اینترنت اشیاء به‌وسیلهٔ قابلیت‌های خود توانسته است تا در بسیاری از حوزه‌ها نظیر حمل‌ونقل، انرژی و صنعت وارد شده و به افزایش دقت و کارایی سازمان‌های مرتبط بیانجامد. حوزهٔ دفاعی نیز بی‌تأثیر از این فنّاوری نمانده و امروزه سازمان‌های نظامی، اسناد راهبردی خود در حوزهٔ به‌کارگیری این فنّاوری نوظهور را تدوین کرده و مورد استفاده قرار می‌دهند.

ویژگی‌های خاص سازمان‌های دفاعی و نحوهٔ عملکرد آنها در صحنهٔ نبرد باعث شده تا کارشناسان حوزه فنّاوری بر استفاده از اینترنت اشیاء در این محیط تأکید نمایند و همهٔ تجهیزات، کاربران، سامانه‌ها و دیگر موارد را در محیط صحنهٔ نبرد بر اساس ویژگی‌های خاص اینترنت اشیاء به‌کار ببرند.

با این فنّاوری، مزیت‌های زیادی در این حوزه برای سازمان‌های دفاعی به وجود می‌آید که مهم‌ترین آنها شناسایی اجزای محیط عملیاتی، انجام پردازش‌های مرتبط در حداقل زمان و بالا بردن کارایی تجهیزات است. ایجاد قابلیت مانیتورینگ صحنهٔ نبرد از دیگر ویژگی‌های خاص استفاده از این فنّاوری نوظهور است.

در این تحقیق، معماری امنیت‌پایهٔ مرتبط با اینترنت اشیاء بر اساس مدل‌های موجود در سازمان‌های دفاعی و مؤسسات استاندارد دفاعی و همچنین نظرات خبرگان طراحی شده است.

با توجه به اینکه امنیت به‌عنوان مهم‌ترین چالش به‌کارگیری فنّاوری اینترنت اشیاء در صحنهٔ نبرد است، در معماری ارائه‌شده در این تحقیق به مؤلفه‌های امنیتی در همهٔ لایه‌ها توجه شده است. پس‌ازآنکه اجزاء و ارتباطات بین اجزای معماری بر اساس یافته‌های پژوهش در حوزه‌های دفاعی کسب شد، درنهایت مدل ارائه‌شده نیز به تأیید این گروه خبرگان رسیده است. نظر به اینکه فنّاوری اینترنت اشیاء با سایر فنّاوری‌های نوظهور مانند رایانش ابری و کلان داده‌ها در ارتباط تنگاتنگ است، پیشنهاد می‌شود تا در کارهای آینده به طراحی صحنهٔ نبرد مبتنی بر ترکیب این فنّاوری‌های نوین پرداخته شود.

منابع و مآخذ

الف) کتب فارسی

۱. ارکیان، علیرضا؛ پورخلیلی، عاطفه؛ خوش‌اخلاق، حمیدرضا؛ (۱۳۹۴)، «***امنیت و حریم خصوصی در اینترنت اشیاء***»، دوفصلنامهٔ علمی- ترویجی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)، دورهٔ ۸، شمارهٔ ۲.

۲. پاکروان، پدرام؛ عسکریان‌ابیانه، حسین (۱۳۹۷)، «***نظارت، کنترل و مانیتورینگ سیستم‌های قدرت مبتنی بر اینترنت اشیاء و عملیاتی نمودن آن در شبکهٔ وای‌فای***»، سیزدهمین کنفرانس ملّی کیفیت و بهره‌وری؛ دو بال توسعه پایدار.

۳. شورای اجرایی (عالی) فنّاوری اطلاعات کشور (۱۳۹۶)، «***چارچوب معماری سازمانی ایران و مدل مرجع امنیت***»، کمیسیون توسعهٔ دولت الکترونیک.

۴. کشتکارهرانکی، مهران (۱۳۹۵)، «***طراحی الگوی راهبردی نوآوری اجتماعی در جمهوری اسلامی ایران***»، رسالهٔ دکتری دانشگاه عالی دفاع ملّی.

۵. محمدی، شهریار (۱۳۹۵)، «***معماری پیشنهادی مبتنی بر اینترنت اشیاء و سیستم‌های توصیه‌گر برای هوشمندسازی شهر تهران***»، فصلنامهٔ علمی پژوهشی پژوهشگاه علوم و فنّاوری اطلاعات ایران، دوره ۳۲، شماره ۱.

۶. مکنزی (۱۳۹۵)، «***اینترنت اشیاء و چگونگی ارزش‌آفرینی آن***»، تهران: دبیرخانه برنامه ملّی آینده‌نگاری علم و فنّاوری در حوزه فنّاوری اطلاعات و ارتباطات.

ب) کتب لاتین

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M, & Ayyash, M.,(2015), ***"Internet of Things: A Survey on Enabling Technologies, Protocols and Applications"***, IEEE Communications Surveys & Tutorials, vol. 17. pp. 2347 - 2376. Cisco's white paper.

2. Ammar, Mahmoud, Russello, Giovanni & Crispoa, Bruno, .,(2018). ***"Internet of Things: A survey on the security of IoT frameworks"***.

Journal of Information Security and Applications, vol. 38, pp. 8 – 27.

3. DoD CIO., (2017). ***"Policy Recommendations for the Internet of Things"***. Chief Information Officer U.S. Department of Defense, white paper.

4. Gubbi, Jayavardhana, Buyya, Rajkumar, Marusic, Slaven & Palaniswami, Marimuthu (2013). ***"Internet of Things (IoT): A vision, architectural elements, and future directions"***, Elsevier. Future Generation Computer Systems, volume 29, number 7. P 1645 - 1660.

5. Gupta, B., & Quamara, M., (2018) ***"An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols"***, Concurrency and Computation: Practice and Experience, pp. 291 – 319.

6. ITU (2005), ***"ITU Internet Reports 2005: The Internet of Things. Executive Summary"***, International Telecommunication Union (ITU), Geneva, available online at http://www.itu.int/osg/spu/publications/internetofthings/,last retrieved April 18, 2012.

7. Jacobson, Michael, (2015). ***"The Internet of Things***", the Department of Defense and the Dangers of Networked Warfare. COMP-116: Computer Systems Security December 15, 2015 M.

8. Li, Shancang, Li, Da Xu & Shanshan, Zhao (2015). ***"The internet of things: a survey"***, Information Systems Frontiers. Springer Science + Business Media: 243 - 259.

9. Li, X., R.X., Lu, X.H., Liang & X.M. Shen. (2011). ***"Smart community: an internet of things application"***, IEEE Commun Mag 68 - 75.

10. Mehta, Ashish & Dhariwal, Kunal, (2017). ***"Architecture and***

Plan of Smart hospital based on Internet of Things (IOT)", International Research Journal of Engineering and Technology (IRJET). Volume: 04 Issue: 04.

11. NATO Parliamentary Assembly, Science and Technology Commitee, (2017). ***"The Internet of Things: Promises and Perils of a Disruptive Technology"***, www.nato-pa.int.

12. Paul, A., and Jeyaraj, R., (2019) ***"Internet of Things: A primer"*** Human Behaviour and Emerging Technology, vol. 1, no. 1, pp. 37- 47.

13. Paula, F-L., Tiago, M., Manuel, F-C., Luis, S-A., & Miguel, G.L., (2016). ***"A Review on Internet of Things for Defense and Public Safety"***, Sensors. 16. 1644; doi: 10.3390/s16101644, www.mdpi.com/journal/sensors.

14. Ray, P.P., (2018) ***"A survey on Internet of Things architectures"*** Journal of King Saud University - Computer and Information Sciences, vol. 30, no. 3, pp. 291 – 319.

15. Sandelowski, M., Barros, J., (2007). ***"Handbook for synthesizing qualitative research"***, Springer publishing company Inc. Available at: https://epdf.tips/handbook-for-synthesizing-qualitative-research.html.

16. Sarkar, C., Nambi, S.N.A.U., Prasad, R.V., Rahim, A., (2014). ***"A scalable distributed architecture towards unifying IoT applications"***. In Proceedings of the IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6 – 8 March 2014; pp. 508 – 513.

17. Torkaman, A., Seyyedi, M.A., (2016). ***"Analyzing IoT Reference Architecture Models"***. International Journal of Computer Science and Software Engineering (IJCSSE), Volume 5, Issue 8, August 2016.

18. Truyen, frank, (2018). ***"Modeling a SABSA® Based Enterprise Security Architecture using Enterprise Architect"***, Cephas Consulting Corp. All rights reserved.

19. Vermesan, O., & fries, P., (2014) ***"Internet of Things - from Research and Innovation to Market Deployment"***, River Publishers.

20. Yushi, L., Fei, J., Hui, Y., (2012). ***"Study on application modes of military Internet of Things (MIOT)"***. In Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE), hangjiajie China; Voloum 3, pp. 630 – 634.

21. Zheng, Denise, & Carter, William, (2015). ***"Leveraging the Internet of Things for a More Efficient and Effective Military"***, S.l. Rowman & Littlefield, Center for Strategic and International Studies.