ارزیابی چالش‌های پدافندغیرعامل با بکارگیری اینترنت اشیا

امیر هوشنگ تاجفر[1]
محمد قیصری[2]
سیدمصطفی موسوی‌نیا[3]

تاریخ دریافت: ۱۳۹۶/۰۵/۱۸ تاریخ پذیرش: ۱۳۹۶/۰۷/۲۶

چکیده

اینترنت اشیا به عنوان مرحله‌ای اصلی در سیر تکاملی فضای سایبر، در کنار خلق فرصت‌هایی بیشمار، چالش‌های قابل توجهی به خصوص در حوزه پدافندغیرعامل ایجاد می‌کند، که می‌تواند مانع تحقق درک مزایای آن شود. هدف از پژوهش حاضر ارزیابی چالش‌های پدافندغیرعامل با بکارگیری اینترنت اشیا است. این تحقیق از نوع توصیفی-پیمایشی و کاربردی بوده و جامعه آماری آن شامل، مدیران، مسئولان و کارشناسان فناوری اطلاعات و پدافندغیرعامل است.

در این پژوهش عوامل افزایش سطح نظارت و کنترل زیرساخت‌های حیاتی و اتصال دائمی به اشیا و محیط در مقابله با بحران‌ها به عنوان مهم‌ترین کاربردهای اینترنت اشیا و عوامل سطح پایین حفاظت فیزیکی دستگاه‌های اینترنت اشیا، پایش فراگیر بر سازمانهای اطلاعاتی حریف و سطح دسترسی بالا به حریم خصوصی افراد چالش‌های اصلی پدافندغیرعامل شناسایی شده است. همچنین عوامل نهادینه‌سازی الزامات پدافندغیرعامل و تهیه دستورالعمل‌های امنیتی برای فناوری اینترنت اشیا به عنوان راهبردها و سیاست‌های موثر پدافندغیرعامل و عوامل استفاده از رمزنگاری قوی، سیستم‌های احراز هویت پیشرفته و ایجاد یک سیستم مدیریت امنیت جهت کنترل دستگاه‌های اینترنت اشیا به عنوان راهکارهای فنی موثر پدافندغیرعامل در برابر چالش‌های بکارگیری فناوری اینترنت اشیا شناسایی شده‌اند.

از نتایج مهم تحقیق می‌توان امکان استفاده از کاربردهای این فناوری و کاهش چالش‌های پیشروی آن، با نهادینه سازی الزامات پدافندغیرعامل و عدم اعمال مقررات سختگیرانه اشاره کرد.

کلید واژگان: *اینترنت اشیا، پدافندغیرعامل، چالش‌ها، راهبردها، راهکارها، کاربردها*

---

۱. استادیار گروه مهندسی کامپیوتر و فن‌آوری اطلاعات دانشگاه پیام نور تهران، ، ایران(A.Tajfar@yahoo.com)
۲.کارشناسی ارشد مدیریت فناوری اطلاعات، دانشگاه پیام نور تهران، ایران(Mohammad_Gheysari@yahoo.com)
۳.کارشناسی ارشد مدیریت فناوری اطلاعات(نویسنده مسئول)، دانشگاه پیام نور تهران، ایران(mostafa_jam@yahoo.com

۱. مقدمه

اینترنت اشیاء[۱]، مفهومی جدید در دنیای فناوری و ارتباطات است که به عنوان فناوری مدرن قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت، را برای هر چیزی (انسان، حیوان یا اشیا) فراهم می‌کند.(چیوئی و همکاران، ۲۰۱۲: ۲۲)

واژه اینترنت اشیا اولین بار در سال ۱۹۹۹ توسط کوین اشتون[۲] پیشگام فناوری بریتانیایی، به منظور توصیف سامانه‌ای استفاده شد که در آن اشیاء، موجود در دنیای فیزیکی بتوانند توسط حسگرها به اینترنت متصل شوند. امروزه، اینترنت اشیاء به اصلاح متداولی تبدیل شده که توصیف کننده راه‌حل‌هایی کاربردی جهت اتصال اینترنت و قابلیت محاسبات، به انواع اشیاء، تجهیزات، حسگرها و مواد روزمره است. (قیصری و همکاران، ۱۳۹۶ :۱۷)

کشورهای مختلف از جمله ایالات متحده آمریکا (پروژه چالش آمریکای هوشمند[۳]، ۲۰۱۵)، چین (اینترنت اشیای چین[۴]، ۲۰۱۵)، اتحادیه اروپا (خوشه پژوهشی اروپایی اینترنت اشیاء[۵]، ۲۰۱۵) و هند (دیتی، ۲۰۱۵) با انگیزه‌های متفاوت از گسترش فناوری اینترنت اشیاء حمایت می‌کنند. (قاسمی و همکاران، ۱۳۹۵ : ۲۶)

همچنین گارتنر[۶] بیان می‌کند تا سال ۲۰۱۸ بیش از ۱۸ میلیارد وسیله به اینترنت متصل خواهند شدکه ۹ میلیارد از این اتصالات به شبکه، ناشی از اتصال اشیا می باشد. خانه های هوشمند نیز در این حوزه بسیار جذاب است بطوریکه تا سال ۲۰۱۷ سهم خانه‌های هوشمند از این میان، برابر با ۷۲ میلیارد دلار می‌باشد. در برآورد دیگری، شرکت گارتنر اعلام کرده‌است که تا ۲۰۲۰ حدود ۲۶ میلیارد وسیله مبتنی بر اینترنت اشیا وجود خواهد داشت.(عاملی، مرکز ملی فضای مجازی، ۱۳۹۵)

۲. طرح مساله

در کنار مزیت‌های حاصل از این فناوری، چالش‌هایی مانند، سطح پایین حفاظت فیزیکی دستگاه‌های اینترنت اشیا، پایش فراگیر سازمانهای اطلاعاتی حریف و سطح دسترسی بالا به حریم خصوصی و ... وجود دارد که پدافند غیر عامل با توجه به ماموریت خود بر آن است تا با

۱. Internet of Things
۲. Kevin Ashton
۳. The Smart America Challenge
۴. China Internet of Things
۵. IOT European Research Cluster (IERC)
۶. Gartner

کاهش آسیب پذیری‌ها و ایمن سازی زیر ساخت های سایبری کشور تداوم فعالیت‌های ضروری را تضمین کند. در واقع پدافندغیرعامل شامل کلیه اقدامات به منظور حفظ امنیت، ایمنی و پایداری شبکه و تجهیزات وابسته به شبکه می‌باشد. اهداف کلان پدافند غیرعامل در حوزه فضای سایبر شامل موارد زیر است:

- تامین امنیت و حصول اطمینان از عدم دسترسی‌های غیرمجاز به اسرار و اطلاعات کشور.
- ایمن‌سازی و حصول اطمینان از پایداری و خلل‌ناپذیری در فعالیت شبکه‌های الکترونیکی مدیریت و کنترل کشور.
- حفظ و تامین آرامش اجتماعی و عمومی از طریق توسعه اطمینان و اعتماد آحاد جامعه.
- اطمینان نسبت به صحت و تداوم کارکرد سامانه‌های الکترونیکی خدمات عمومی.
- توسعه ظزفیت دفع الکترونیکی در برابر تهاجم فرهنگی و نرم از طریق شبکه‌های ملی و بین-المللی اینترنت.
- تقویت ضریب امنیت و پایداری در زیرساخت‌های ملی و حیاتی کشور.

۳. اهداف، سؤالات تحقیق و فرضیه

۳-۱. پرسش‌های اصلی و فرعی

۳-۱-۱. پرسش اصلی

چالش‌های پدافندغیرعامل با بکارگیری فناوری اینترنت اشیا کدام است؟

۳-۱-۲.پرسش فرعی

سیاست‌ها، راهبردها و راهکارهای فنی پدافندغیرعامل در برابر چالش‌های بکارگیری فناوری اینترنت اشیا کدام است؟

۳-۲. فرضیه‌های پیشنهادی

- اینترنت اشیا کارکردهای موثری در حوزه پدافندغیرعامل دارد؟
- بکارگیری فناوری اینترنت اشیا باعث ایجاد چالش‌هایی در فضای سایبر می‌شود.
- سیاست‌ها و راهبردهای مبتنی بر پدافندغیرعامل در راستای کاهش تهدیدات و آسیب‌پذیری فناوری اینترنت اشیا موثر است.
- راهکارهای فنی مبتنی بر پدافندغیرعامل در راستای کاهش تهدیدات و آسیب‌پذیری فناوری اینترنت اشیا موثر است.

٤. پیشینه تحقیق

با توجه به اینکه فناوری اینترنت اشیا پدیده نوظهوری است، چالش‌های پیشروی پدافندغیرعامل با بکارگیری آن نیز پژوهشی جدید است که کمتر به آن پرداخته شده است و

تحقیقاتی که در این زمینه انجام شده است هر کدام تنها به یکی از ابعاد این فناوری پرداخته‌اند.

برخی اقدامات پدافندغیرعامل در حوزه تسهیل کننده مدیریت بحران است و به ۳ دسته کلی تقسیم می شود. اقدامات زیر ساختی، اقدامات مدیریتی و اقدامات ساختاری. در حوزه اقدامات مدیریتی، مطالعه و پیش بینی بحران‌ها، حوادث و بلایا موضوع بحث است. دانشگاه استنفورد مجموعه‌ای از سیستم‌های نظارت ساختمانی بر اساس شبکه حسگرهای بی‌سیم[۱] را برای اتفاقات ریسکی و آزمون‌های دوره‌ای و طولانی مدت مستقرکرده است. اطلاعات جمع‌آوری شده توسط این شبکه توسط یک واسط نرم افزار[۲] به صورت بلادرنگ به سیستم مدیریت بحران منتقل می‌شود. بنابراین از آنجایی که پیش‌بینی‌های انسانی همیشه درست و به موقع نبوده و به طور معمول ضریب خطای بالایی دارند بهتر است با طراحی تجهیزات تکنولوژیک و استفاده از فناوری اینترنت اشیا در ساخت محصولات امنیتی، سازه‌ها و سازمان‌های هوشمند، از وقوع این بلایای طبیعی و مصنوعی جلوگیری کرده و یا اثرات آنها را تا حد امکان کاهش دهیم.(قیصری و همکاران، ۱۳۹۵: ۱۲)

مرکز پژوهش‌های مجلس(۱۳۹۵)، در گزارشی عدم دسترسی به داده‌ها در دنیای مبتنی بر اینترنت اشیا را بی‌معنا دانسته و وجود چنین بستری را در افزایش کارآیی نیروهای کار موثر می‌داد. در ادامه نگرانی‌های مطرح در مورد امنیت و حریم شخصی را مد نظر قرار می‌دهد، زیرا با افزایش تعداد ابزارها و وسایل متصل به اینترنت، امکان حمله به آنها افزایش خواهد یافت و در چنین شرایطی ایجاد تعادل نسبی میان تأمین امنیت و استفاده از ابزارها و امکانات اینترنت اشیا به یک ضرورت تبدیل خواهد شد.

قیصری و همکاران(۱۳۹۶)، در کتاب با عنوان "اینترنت اشیا، چالش‌ها و مشکلات دنیای به‌هم متصل" ، چالش‌ها و مشکلات دنیای به هم متصل را بررسی نموده و به پیامدهای امنیتی، حریم خصوصی و مسائل مربوط به تعامل‌پذیری و استانداردها، مسائل قانونی و حقوقی و در نهایت مسائل مرتبط با توسعه و رشد اقتصاد نوظهور اینترنت اشیاء اشاره نموده‌اند.

قیصری و همکاران(۱۳۹۵)، در تحقیقی با عنوان" مدیریت بحران با سیاست گذاری فناوری اینترنتی از اشیا" با نگاهی نو به مبحث مدیریت بحران و یکی از زیر شاخه های اصلی آن یعنی پدافند غیر عامل، زمینه فکری جدیدی برای تولیدات نوآورانه‌ی وسایل و تجهیزات تکنولوژیک

۱. Wireless Sensor networks (WSN)

۲. Code Blue

جهت کاهش و یا حذف اثرات حاصل ازخسارات و صدمات مالی و جانی را ارائه می‌کنند. دراین مقاله پس از بیان تفصیلی درباره مفاهیم اصلی مدیریت بحران، پدافند غیر عامل و فناوری اینترنت اشیا به صورت جداگانه، و ضمن اشاره به تفاوت‌ها و کاربردهای هریک، به ایده جدیدی با نام «مدیریت هوشمند بحران» و ادغام فناوری اینترنت اشیا در مدیریت بحران و ذکر چند نمونه پرداخته شده است.

همچنین پژوهشگاه ارتباطات و فناوری اطلاعات(۱۳۹۴) "طرح ملی اینترنت اشیا" را به منظور تدوین نقشه راه و ارائه برنامه عملیاتی اینترنت اشیا در کشور، مطرح نموده است. در پی انجام مراحل طرح مذکور، تصمیم به ایجاد پارک اینترنت اشیا در کشور گرفته شده است. فاز نخست شبکه اختصاصی اینترنت اشیا با عنوان "شبکه اشیا تهران- ایران" در منطقه نارمک تهران راه‌اندازی شده است که دارای کاربردهایی نظیر ارائه خدمات رایگان شبکه اشیا به استارتاپ‌ها، کمک شبکه اینترنت اشیا برای مدیریت شهری و ... می باشد.

۵. نوع و روش تحقیق

این پژوهش از لحاظ روش توصیفی- پیمایشی است و از حیث هدف با توجه به ابعاد عملکردی موضوع کاربردی است. به منظور جمع آوری داده‌ها در پژوهش حاضر از روش کتابخانه‌ای، مطالعات میدانی و پرسشنامه استفاده شده است. در نتیجه کتاب‌ها، مقالات، اسناد، دستورالعمل‌ها و مبانی مربوطه و استانداردهای مربوط به موضوع پژوهش مورد بررسی و با توجه به آن و از طریق مصاحبه به شناسایی موانع پرداخته شده و سپس با استفاده از پرسشنامه، مطلب مورد نظر در خصوص کارکردها، چالش‌ها، راهبردها و راهکارها جمع‌آوری و بصورت توصیفی مورد تحلیل قرار گرفت تا چالش‌های پدافندغیرعامل با بکارگیری اینترنت اشیا، مشخص گردد.

سوالات پرسشنامه بر مبنای طیف ۵ گزینه‌ای لیکرت حاوی ۳۰ پرسش در ۴ شاخص اصلی شامل ارتقاء و هماهنگی و کاربردها(۸ پرسش)، تهدیدات و آسیب پذیری ها(۹پرسش)، راهبردها(۶پرسش) و راهکارهای فنی(۷پرسش) مطرح شده‌اند. سپس تعداد ۱۱۳ پرسشنامه در جامعه آماری توزیع و از پرسشنامه‌های وصول شده در تجزیه و تحلیل آماری پژوهش استفاده شدند و میزان آلفای کرونباخ برابر ۰,۸۱ بدست آمد که نشانگر پایائی بالای پرسشنامه مورد استفاده می‌باشد.

٦. جامعه آماری و قلمرو پژوهش

در تحقیق حاضر، جامعه آماری شامل مدیران، مسئولان و کارشناسان فناوری اطلاعات و پدافندغیرعامل است. داده‌های این پژوهش بر اساس آخرین وضعیت چالش‌های اینترنت اشیا،

در بازه زمانی اردیبهشت لغایت تیر ۱۳۹۶ گردآوری شده است. برای تعیین اندازه نمونه از فرمول کوکران استفاده شد. که در این پژوهش از روش پیش آزمون استفاده گردیده که با استفاده از ۱۰ پرسشنامه اولیه واریانس مولفه‌ها محاسبه گردید و بیشترین واریانس در فرمول قرار داده شد. روش های آماری مورد استفاده در پژوهش حاضر آمار توصیفی و استنباطی است و با استفاده از نرم‌افزارهای تحلیل آماری[1] تحلیل داده‌ها صورت پذیرفت. در آزمون فرضیه‌های این تحقیق و تجزیه و تحلیل آن ها از روش آزمون رتبه‌ای فریدمن استفاده شده است.

۷. مبانی نظری و مفاهیم

۱-۷. چالش‌های اینترنت اشیا

چالش‌ها ناظر به واقعیاتی عینی، جدید، معطوف به آینده و بیرونی‌اند که فراگیری و تاثیر آن، کل جامعه را به مبارزه می‌طلبد و تلاش سختی را برای پشت‌سرنهادن آن می‌طلبد. با این تحدید و تعریف، میان معنی چالش و معانی تعابیر و اصطلاحات مشابه و نزدیک، تفکیک حاصل می‌شود و جامعیت و مانعیت آن تامین می‌گردد. البته می‌توان معنای «چالش» را اعم از مشکلات و مسائل عینی و ذهنی، داخلی و خارجی، فراگیر و محدود، ریشه‌دار و جدید دانست که می‌تواند به اندازه‌های گوناگون حرکت متعادل جامعه را کند یا متوقف سازد و مستلزم تلاش و تدبیر برای چاره‌اندیشی باشد. (ماهنامه زمانه، شماره۳۶)

عواملی مانند دشواری بروزرسانی، پیکربندی مجدد، سطح پایین حفاظت فیزیکی دستگاه‌های اینترنت اشیا و نقض حریم خصوصی افراد از جمله چالش‌هایی هستند که در صورت بکارگیری اینترنت اشیا با آن روبرو خواهیم بود.

بررسی طیف گسترده مسائلی که اینترنت اشیاء را احاطه کرده‌اند، نیاز به زمان و بررسی‌های فراوانی دارد. امنیت و پایداری کلی اینترنت اشیاء تابعی از چگونگی ارزیابی و مدیریت ریسک‌های امنیتی است. عوامل متعددی بر ارزیابی ریسک‌ها و روش کاهش آن موثر خواهد بود. عواملی از جمله: داشتن درک واضحی از خطرات امنیتی کنونی و خطرات بالقوه آینده؛ هزینه‌های پیش‌بینی شده آسیب‌هایی که ممکن است بر اثر خطرات ایجاد شوند؛ و هزینه تخمین زده شده برای کاهش خطرات.(قیصری و همکاران، ۱۳۹۶: ۳۴)

سه اصل محرمانگی، صحت و حریم شخصی از جمله چالش‌های امنیتی اینترنت اشیا هستند. محرمانگی به تکنیک‌های مختلف کنترل و دسترسی برای اطمینان از محرمانه‌بودن اطلاعات

---

۱ SPSS

است. یکی از این روش‌ها "کنترل دسترسی بر مبنای نقش" نام دارد. در این شیوه دسترسی‌ها به نقش، به طور غیرمستقیم مجوز لازم را کسب می‌کنند. در رویکرد اینترنت اشیا، مزیت عمده این روش این است که امتیاز دسترسی از طریق تکالیف نقشی، به صورتی پویا قابل اصلاح است. سیستم مدیریت جریان داده به طور فزاینده‌ای برای حمایت از برنامه‌های کاربردی در زمان واقعی در یک گروه وسیع مورد استفاده قرار می‌گیرند. در اینترنتی از اشیا تکنیک‌های کنترل و دسترسی باید با سیستم‌های مدیریت جریان داده ادغام شوند. همچنین حفظ حریم خصوصی، قوانینی که تحت آن هر فرد کاربر باید به چه اطلاعاتی دسترسی پیدا کند را تعریف می‌نماید. شبکه‌های بی‌سیم به دلیل قابلیت دسترسی از راه دور، خطر نقض حریم خصوصی را افزایش می‌دهند چون باعث می‌شوند که سیستم در معرض خطر بالقوه استراق سمع و حملات پوششی قرار بگیرد.(پوریسینی، ۲۰۱۰ :۵۵)

فناوری اینترنت اشیا جهت پیاده‌سازی نیاز به بستری پایدار و امن دارد که می‌بایست همراه با الزامات پدافندغیرعامل باشد. از این رو سپردن بخشی از (یا تمام) زیرساخت مخابراتی و ارتباطی کشور توسط یک شرکت داخلی به دست شرکت‌های خارجی، اقدامی فوق‌العاده خطرناک و حتی غیرعاقلانه است که نه تنها امنیت و حریم خصوصی کاربران آن شرکت داخلی را از بین می‌برد، بلکه راه نفوذی را برای ورود بیگانگان به درون ساختار مخابراتی کشورمان باز می‌کند که پیامدهای تهدیدآمیز امنیتی برای کشور به دنبال خواهد داشت.(داوری، خبرگزاری مشرق، ۱۳۹۵)

۲-۷. چالش‌های امنیتی منحصربفرد دستگاه‌های اینترنت اشیا

دستگاه‌های اینترنت اشیا نسبت به رایانه‌ها و دیگر دستگاه‌های محاسباتی مرسوم، تفاوت‌های مهمی دارند که امنیت را به چالش می‌کشانند. (قیصری و همکاران،۱۳۹۶ :۳۶)

۱-۲-۷. مقیاس بزرگ

بسیاری از تجهیزات اینترنت اشیا (همچون سنسورها)، به منظور بکارگیری در مقیاسی بسیار وسیع (خیلی فراتر از تجهیزات سنتی متصل به اینترنت) هستند. در نتیجه تعداد لینک‌های مابین این تجهیزات بسیار بزرگ خواهد بود. بنابراین ابزارهای موجود، روش‌ها و استراتژی‌های مرتبط با امنیت اینترنت اشیا نیازمند ملاحظات جدید می‌باشد.

۲-۲-۷. تجهیزات و پروتکل‌های همگون

بسیاری از سناریوهای اینترنت اشیا شامل مجموعه‌ای از تجهیزات یکسان یا شبیه بهم می‌باشند. این همگونی و بکارگیری تعداد زیادی تجهیزات با مشخصات یکسان، پتانسیل آسیب‌پذیری امنیتی را افزایش می‌دهد. برای مثال، یک آسیب‌پذیری در پروتکل ارتباطی

بکارگرفته شده در لامپ‌های هوشمند متصل به اینترنت یک شرکت، می‌تواند منجر به آسیب‌پذیری هر تجهیزاتی شود که از آن پروتکل یا پروتکلی با طراحی مشابه استفاده می‌کند.

۳-۲-۷. پشتیبانی طولانی مدت

مدیریت و پشتیبانی طولانی مدت تجهیزات اینترنت اشیا یک چالش امنیتی بزرگ است. در واقع برخلاف کامپیوترها که طراحی آنها به گونه‌ای است که در طول زمان امکان به روزرسانی نرم‌افزاری آنها جهت مقابله با تهدیدات امنیتی وجود دارد، پیکربندی مجدد و به روزرسانی تجهیزات اینترنت اشیا سخت یا ناممکن بوده و از پشتیبانی طولانی مدت برخوردار نیستند. همچنین بسیاری از تجهیزات اینترنت اشیا عمدا به گونه‌ای طراحی شده‌اند که امکان ارتقاء آنها وجود ندارد یا فرآیند آن بسیار سخت و غیرعملی است. این موضوع باعث می‌شود اگر چه در زمان تولید یک تجهیز مکانیزم‌های امنیتی کافی دیده شده باشد، درطول زمان وبا به وجودآمدن تهدیدات امنیتی جدید، این تجهیزات آسیب‌پذیر شوند.

٤-۲-۷. عملکرد مخفی از دید کاربر

بسیاری از تجهیزات اینترنت اشیا به گونه‌ای عمل می‌کنند که کاربر هیچ اشرافی به نحوه عملکرد داخلی تجهیز یا جریان داده‌ای که تولید می‌کند ندارد. در واقع ممکن است در عمل، یک تجهیز آنچه را که کاربر تصور می‌کند انجام ندهد یا داده بیشتری را بدون خواست کاربر جمع‌آوری کند. این موضوع آسیب‌پذیری امنیتی را به همراه خواهد داشت.

۵-۲-۷. دسترسی فیزیکی

در برخی از موارد تجهیزات اینترنت اشیا در شرایطی بکارگرفته می‌شوند که فراهم کردن امنیت فیزیکی برای آنها سخت یا غیرممکن است. در این‌صورت هکرها دسترسی فیزیکی مستقیم به آنها خواهند داشت. بنابراین لازم است ویژگی‌های ضد دستکاری[۱] و طراحی‌های نوین برای تضمین امنیت دیده شود.

٦-۲-۷. محدودیت دسترسی

برخی از تجهیزات اینترنت اشیا، همچون حسگرهای محیطی، به گونه‌ای طراحی شده‌اند که در محیط نهفته شده و از دید کاربر مخفی باشند. علاوه بر این، چنین تجهیزاتی روش مشخصی برای اطلاع‌رسانی به کاربر در زمان بروز یک مشکل امنیتی ندارند. لذا مشکل امنیتی ممکن است برای مدت طولانی در تجهیز باقی بماند.

۷-۲-۷. استانداردهای امنیتی

۱. Anti-tamper

مدل‌های اولیه اینترنت اشیا فرض می‌کردند که این حوزه محصول سازمان‌های فناوری خصوصی یا عمومی خواهد بود. ولی با رشد انجمن‌های توسعه‌دهنده [1] به نظر می‌رسد در آینده هر کاربری بتواند سناریوهای اینترنت اشیا خودش را پیاده‌سازی کند. در این شرایط ممکن است استانداردهای امنیتی، آنچنان که لازم است، اعمال نشود.

۸-۲-۷. حریم خصوصی

احترام به حریم خصوصی و انتظارات کاربران، جهت ایجاد اعتماد نسبت به اینترنت، مسئله بسیار مهمی است و همچنین این امر به شکل معناداری در توانایی افراد برای تعامل، اتصال و انتخاب اثرگذار است. این حقوق و انتظارات، گاهی در قالب مدیریت اخلاقی داده‌ها مطرح می‌گردد که بر لزوم احترام به انتظارات هر شخص در حوزه حریم خصوصی و استفاده عادلانه از اطلاعات او، تاکید می‌نماید. اینترنت اشیا می‌تواند این انتظارات رایج را به چالش بکشاند.

به هنگام ارزیابی مجدد مدل‌های حریم خصوصی آنلاین در زمینه اینترنت اشیا، باید سوالاتی کلیدی را مطرح نمود. برخی از این سوالات مطرح شده عبارت‌اند از: بی‌طرفی در جمع‌آوری و استفاده از داده‌ها، شفافیت، بیان و اجرای اولویت‌های خصوصی، دامنه‌ی گسترده انتظارات از حفظ حریم خصوصی، حریم خصوصی در طراحی و شناسایی.(قیصری و همکاران، ۱۳۹۶ : ۴۱)

۳-۷.کاربردهای اینترنت اشیا

اینترنت اشیا که از آن به عنوان انقلاب صنعتی جدید یاد می‌شود، به دلیل تغییری که در شیوه زندگی، کار، سرگرمی و مسافرت مردم و ... ایجاد کرده‌است، تعاملات بین دولت‌ها و دنیای پیرامونشان را با دنیای مجازی و تکنولوژی نیز دگرگون ساخته است. (شکل شماره۱، مرکز تحقیقات اینترنت اشیا)

شش مورد از مزایایی که اینترنتی از اشیا به عنوان نقش رهبری می‌تواند تامین نماید عبارت خواهند بود از : پایش زیست محیطی، شهرهای هوشمند، کسب و کار هوشمند/ مدیریت تولید و موجودی، خانه‌های هوشمند/مدیریت ساختمان‌های هوشمند، مراقبت‌های بهداشتی و امنیتی. خانه هوشمند، محبوب ترین کاربرد اینترنت اشیا است. ماهانه بیش از ۶۰ هزار نفر عبارت خانه هوشمند[2] را در گوگل جستجو می کنند.

---

۱. Arduino & Raspberry Pi

۲ Smart Home

همچنین حوزه‌های مختلف کاربردی اینترنت اشیا را می‌توان در گروه‌های زیر دسته‌بندی کرد. ۱- حوزه حمل و نقل و پشتیبانی ۲- حوزه سلامت ۳- حوزه محیط‌های هوشمند ۴- حوزه شخصی و اجتماع ۵- حوزه‌های مربوط به آینده.(آتزوری و همکاران،۲۰۱۵: ۱۲)

۱-۳-۷. بهبود بهره‌وری فرایندها زیربنایی و نیروهای نظامی

در بعد نظامی، استفاده از فناوری‌های مرتبط با اینترنت اشیا، به کاربری‌های رزمی و درگیری-های نظامی محدود می‌شود. سیستم‌های مختلف (فرمان، کنترل، ارتباط، پردازش، اطلاعات، پایش و شناسایی)، از میلیون‌ها حسگر استفاده می‌کنند و هدف آن‌ها، ارائه کردن درک صحیحی از نیروها و تهدیدات میدان نبرد (در زمین، هوا و دریا) است.

برخی از فناوری‌های مرتبط با حوزه فناوری اینترنت اشیا در حوزه‌های غیررزمی نیز مورد استفاده قرار گرفته‌اند که موجب افزایش بهره‌وری و اثربخشی فرایندهای زیربنایی شده است. به عنوان نمونه، از این فناوری برای تمرین‌ها و شبیه‌سازهای نظامی استفاده شده است تا با کمک حسگرها و دریافت کننده‌های مختلف، شرایط واقعی صحنه نبرد به درستی شبیه‌سازی شود. علی‌رغم وجود چالش‌هایی در پذیرش و بهره‌برداری فراگیر از فناوری اینترنت اشیا، پتانسیل بسیار زیادی پیش روی این فناوری وجود دارد تا تحولی نو در ادوات نظامی مدرن ایجاد کنند تا با کاهش هزینه‌ها و افزایش اثربخشی، نیروهای نظامی را کارآمدتر و مقاوم‌تر در برابر تهدیدهای مختلف قرار دهد. (ژنگ و همکاران،۲۰۱۶ : ۳۲)

۲-۳-۷. افزایش سطح نظارت و کنترل زیرساخت‌های حیاتی

صنعت نفت از مؤثرترین و بزرگ‌ترین صنایع در جهان به‌ویژه در منطقه خاورمیانه است این صنعت علاوه بر منبع عمده تأمین انرژی، نقش مهمی در تأمین درآمد کشورهای نفت‌خیز و تعین میزان قدرت ملی و اعتبار بین‌المللی ایفا می‌کند استفاده از فناوری‌های نو در این صنعت به‌منظور افزایش اثرات مطلوب این صنعت همواره مدنظر مدیران ارشد بوده است. اینترنت اشیااست از مجموعه فناوری‌های نوینی است که می‌تواند در فرآیندهای اکتشاف و تولید، پالایشگاه‌ها، پتروشیمی، خط لوله، حمل‌ونقل و توزیع استفاده شود. استفاده از این فناوری در صنعت نفت و گاز باعث افزایش امنیت کارکنان، شناسایی مسائل بهداشتی و ایمنی، بهینه‌سازی تولید، تحمل خطا و کاهش هزینه‌های عملیاتی می‌شود.(گرامی راد،۱۳۹۵: ۳)

۸. تحلیل داده های پژوهش

۱-۸. تجزیه و تحلیل توصیفی داده‌ها

در این بخش با استفاده از جدول توزیع فراوانی، به تحلیل توصیفی داده‌ها پرداخته شده است و ویژگی‌های جمعیتی توصیف می‌شود.

	فراوانی	فراوانی نسبی	درصد صحیح	فراوانی انباشته
فناوری اطلاعات	۵۱	۴۵,۱	۴۵,۱	۴۵,۱
پدافندغیرعامل	۶۲	۵۴,۹	۵۴,۹	۱۰۰
مجموع	۱۱۳	۱۰۰	۱۰۰	

جدول ۸-۱: تخصص پرسش‌شوندگان

	فراوانی	فراوانی نسبی	درصد صحیح	فراوانی انباشته
۳۰-۳۵	۲۷	۲۳,۹	۲۳,۹	۲۳,۹
۳۵-۴۰	۷۶	۶۷,۳	۶۷,۳	۹۱,۲
۴۰-۴۵	۶	۵,۳	۵,۳	۹۶,۵
۴۵-۵۰	۴	۳,۵	۳,۵	۱۰۰
مجموع	۱۱۳	۱۰۰	۱۰۰	

جدول ۸-۲: سن پرسش‌شوندگان

	فراوانی	فراوانی نسبی	درصد صحیح	فراوانی انباشته
کارشناسی	۱۳	۱۱,۵	۱۱,۵	۱۱,۵
کارشناسی ارشد	۸۲	۷۲,۶	۷۲,۶	۸۴,۱
دکتری	۱۸	۱۵,۹	۱۵,۹	۱۰۰
مجموع	۱۱۳	۱۰۰	۱۰۰	

جدول ۸-۳: تحصیلات پرسش‌شوندگان

	فراوانی	فراوانی نسبی	درصد صحیح	فراوانی انباشته
تا حدودی	۵۱	۴۵,۱	۴۵,۱	۴۵,۱
زیاد	۴۱	۳۶,۳	۳۶,۳	۸۱,۴
خیلی زیاد	۲۱	۱۸,۶	۱۸,۶	۱۰۰
مجموع	۱۱۳	۱۰۰	۱۰۰	

جدول ۸-٤: میزان آشنایی پرسش‌شوندگان با اینترنت اشیا

۸-۲. تجزیه و تحلیل استنباطی داده‌ها

۸-۲-۱: آزمون تی تک‌نمونه‌ای

در تحقیق حاضر برای تعیین معنی‌داری اختلاف بین میانگین یک متغیر با یک مقدار ثابت از آزمون تی تک‌نمونه‌ای استفاده گردید که با توجه به طیف درنظر گرفته شده در پاسخنامه‌ها، مقدار آزمون برابر ۳ در نظر گرفته شده است. چنانچه میانگین پاسخنامه‌ها در هر یک از متغیرها از عدد ۳ بیشتر باشد وضعیت آن در جامعه مساعد خواهد بود در غیر این صورت از نظر جامعه مورد آزمون، متغیر بررسی شده وضعیت مساعدی نداشته است و مطابق با جدول شماره ۸-۵، کلیه متغیرها از وضعیت مساعدی برخوردار هستند.

آزمون تی استودنت تک نمونه‌ای			
	مقدار آزمون=۳		
	آماره تی	درجه آزادی	معنی داری
سوال۱	۲۴,۴۹۱	۱۱۲	.۰۰۰
سوال۲	۳۳,۴۵۰	۱۱۲	.۰۰۰
سوال۳	۲۹,۱۵۵	۱۱۲	.۰۰۰
سوال۴	۱۲,۵۷۸	۱۱۲	.۰۰۰
سوال۵	۲۷,۷۷۲	۱۱۲	.۰۰۰
سوال۶	۳۰,۶۱۵	۱۱۲	.۰۰۰
سوال۷	۵۴,۷۵۱	۱۱۲	.۰۰۰
سوال۸	۲۸,۳۶۰	۱۱۲	.۰۰۰
سوال۹	۳۶,۷۰۴	۱۱۲	.۰۰۰
سوال۱۰	۳۳,۸۵۶	۱۱۲	.۰۰۰
سوال۱۱	۳۰,۳۲۸	۱۱۲	.۰۰۰
سوال۱۲	۴۵,۳۵۲	۱۱۲	.۰۰۰
سوال۱۳	۱۷,۳۹۳	۱۱۲	.۰۰۰
سوال۱۴	۴۹,۷۰۴	۱۱۲	.۰۰۰
سوال۱۵	۲۰,۸۳۰	۱۱۲	.۰۰۰
سوال۱۶	۲۸,۵۰۰	۱۱۲	.۰۰۰

سوال۱۷	۴۷,۲۱۹	۱۱۲	.۰۰۰
سوال۱۸	۳۳,۴۵۰	۱۱۲	.۰۰۰
سوال۱۹	۷۹,۶۰۲	۱۱۲	.۰۰۰
سوال۲۰	۳۷,۲۶۹	۱۱۲	.۰۰۰
سوال۲۱	۳۰,۱۵۵	۱۱۲	.۰۰۰
سوال۲۲	۵۸,۲۴۲	۱۱۲	.۰۰۰
سوال۲۳	۳۷,۲۶۹	۱۱۲	.۰۰۰
سوال۲۴	۲۷,۹۴۶	۱۱۲	.۰۰۰
سوال۲۵	۲۹,۶۹۴	۱۱۲	.۰۰۰
سوال۲۶	۲۹,۹۷۸	۱۱۲	.۰۰۰
سوال۲۷	۲۷,۹۶۴	۱۱۲	.۰۰۰
سوال۲۸	۳۲,۶۹۶	۱۱۲	.۰۰۰
سوال۲۹	۳۱,۶۵۷	۱۱۲	.۰۰۰
سوال۳۰	۱۳,۴۸۲	۱۱۲	.۰۰۰

جدول شماره ۸-۵ : نتایج آزمون تی استودنت تک نمونه‌ای

۸-۲-۲: آزمون فریدمن

نتایج آزمون فریدمن برای شاخص‌های کاربردها، چالش‌ها، راهبردها و راهکارهای فنی به شرح زیر است.

۱-۲-۲-۸: تجزیه و تحلیل استنباطی فرضیه یک

سوالات	کاربردهای اینترنت اشیا	رتبه‌های فریدمن
سوال ۱	نظارت لحظه ای بر پیشگیری از بحران‌ها	۴,۰۸
سوال ۲	اتصال دائمی به اشیا و محیط در مقابله با بحران‌ها	۵,۳۵
سوال ۳	اقدام به هنگام در بازسازی خسارت‌های ناشی از بحران‌ها	۳,۵۸
سوال ۴	اطلاع رسانی دقیق بر آمادگی در مقابل بحران‌ها	۳,۵۰
سوال ۵	قابلیت‌های پایش نیروی انسانی بر افزایش بهره‌وری نیروهای نظامی	۴,۳۱
سوال ۶	فعال سازی محیط‌ها بر ایجاد شهرهای هوشمند	۴,۷۷

سوال۷	افزایش سطح نظارت و کنترل زیرساخت‌های حیاتی	۶,۳۷
سوال۸	تجزیه و تحلیل داده ها بر ایجاد سازه‌های امن	۴,۰۴

جدول ۸-۷ : ترتیب توالی اهمیت شاخص‌های اثرگذار در فرضیه اول

تعداد	۱۱۳
کای اسکوئر	۱۹۵,۵۴۲
درجه آزادی	۷
معنی داری	.۰۰۰

جدول ۸-۸: آزمون فریدمن

داده‌های جداول ۸-۷ حاکی از آن است که ارزش کای اسکوئر مشاهده شده (۱۹۵,۵۴۲) در درجه آزادی ۷ در آزمون فریدمن، معنی‌دار است. از طرفی داده‌های جدول ۸-۸ نشان می‌دهد که به ترتیب شاخص‌های افزایش سطح نظارت و کنترل زیرساخت‌های حیاتی و اتصال دائمی به اشیا و محیط در مقابله با بحران‌ها به ترتیب بیشترین رتبه را در کارکردهای اینترنت اشیا دارند. بدین ترتیب فرضیه اول به اثبات می‌رسد.

۲-۲-۲-۱۰: تجزیه و تحلیل استنباطی فرضیه دوم

سوالات	چالش‌های اینترنت اشیا	رتبه‌های فریدمن
سوال ۹	پایش فراگیر بر سازمانهای اطلاعاتی حریف	۶,۵۳
سوال ۱۰	سطح دسترسی بالا به اطلاعات بر حریم خصوصی افراد	۶,۲۹
سوال ۱۱	وجود لینک های فعال در اینترنت اشیا	۴,۲۲
سوال ۱۲	ایجاد لینک های صامت توسط اینترنت اشیا	۶,۳۹
سوال ۱۳	میزان یکپارچگی دستگاه های مجهز به اینترنت اشیا	۴,۲۷
سوال ۱۴		۳,۲۷
سوال ۱۵	مخفی بودن وضعیت عملکرد دستگاه‌های اینترنت اشیا	۳,۴۶
سوال ۱۶	دشواری پیکربندی مجدد دستگاه‌های اینترنت اشیا	۴
سوال ۱۷	سطح پایین حفاظت فیزیکی برخی دستگاه‌های اینترنت اشیا	۶,۵۶

جدول ۸-۹ : ترتیب توالی اهمیت شاخص‌های اثرگذار در فرضیه دوم

تعداد	۱۱۳
کای اسکوئر	۳۳۷,۴۷۵
درجه آزادی	۸
معنی داری	.۰۰۰

جدول ۸-۱۰: آزمون فریدمن

داده‌های جداول ۸-۹ حاکی از آن است که ارزش کای اسکوئر مشاهده شده (۳۳۷,۴۷۵) در درجه آزادی ۸ در آزمون فریدمن، معنی‌دار است. از طرفی داده‌های جدول ۸-۱۰ نشان می‌دهد که به ترتیب شاخص‌های سطح پایین حفاظت فیزیکی برخی دستگاه‌های اینترنت اشیا، پایش فراگیر بر سازمانهای اطلاعاتی حریف ، ایجاد لینک های صامت توسط اینترنت اشیا و سطح دسترسی بالا به اطلاعات بر حریم خصوصی افراد به ترتیب بیشترین رتبه را در کارکردهای اینترنت اشیا دارند. بدین ترتیب فرضیه دوم به اثبات می‌رسد.

۳-۲-۲-۸: تجزیه و تحلیل استنباطی فرضیه سوم

سوالات	راهبردها	رتبه‌های فریدمن
سوال ۱۸	انجام تحقیقات بنیادین به منظور شناخت تحولات حوزه اینترنت اشیا	۳,۱۶
سوال ۱۹	نهادینه سازی الزامات پدافندغیرعامل	۴,۲۵
سوال ۲۰	اعمال قوانین و مقررات جهت مسدودسازی شکاف‌های امنیتی	۳,۴۵
سوال ۲۱	تهیه پیوست‌های فرهنگی برای فناوری اینترنت اشیا	۲,۶۳
سوال ۲۲	تهیه دستورالعمل‌های امنیتی برای فناوری اینترنت اشیا	۴,۰۶
سوال ۲۳	همکاری مشترک دولت، صنعت و مردم به منظور افزایش امنیت اینترنت اشیا	۳,۴۵

جدول ۸-۱۱ : ترتیب توالی اهمیت شاخص‌های اثرگذار در فرضیه سوم

تعداد	۱۱۳
کای اسکوئر	۹۷,۶۸۰
درجه آزادی	۵
معنی داری	.۰۰۰

جدول ۸-۱۲: آزمون فریدمن

داده‌های جداول ۸-۱۱ حاکی از آن است که ارزش کای اسکوئر مشاهده شده (۹۷,۶۸۰) در درجه آزادی ۵ در آزمون فریدمن، معنی‌دار است. از طرفی داده‌های جدول ۸-۱۲ نشان می-دهد که به ترتیب شاخص‌های نهادینه سازی الزامات پدافندغیرعامل و تهیه دستورالعمل‌های امنیتی برای فناوری اینترنت اشیا به ترتیب بیشترین رتبه را در بین راهبردهای موثر در

کاهش آسیب‌پذیری‌ها و تهدیدات فناوری اینترنت اشیا دارند. بدین ترتیب فرضیه سوم به اثبات می‌رسد.

٤-٢-٢-٨: تجزیه و تحلیل استنباطی فرضیه چهارم

سوالات	راهکارهای فنی	رتبه‌های فریدمن
سوال ۲۴	تعیین استانداردهای فنی و موثر در توسعه و افزایش دستگاه‌های اینترنت اشیا	۴,۱۵
سوال ۲۵	استفاده از رمزنگاری قوی در دستگاه‌های اینترنت اشیا	۴,۳۷
سوال ۲۶	ایجاد یک سیستم مدیریت امنیت، جهت کنترل دستگاه‌های اینترنت اشیا	۴,۲۱
سوال ۲۷	طراحی راهکارهای امنیتی جهت بروزرسانی تجهیزات اینترنت اشیا	۳,۳۷
سوال ۲۸	استفاده از سیستم‌های احراز هویت پیشرفته در دستگاه‌های اینترنت اشیا	۴,۳۰
سوال ۲۹	حمایت از شرکت‌های دانش‌بنیان و متکی بر توان داخلی	۴,۱۴
سوال ۳۰	بهره‌برداری از اینترنت اشیا در بستر شبکه ملی اطلاعات	۳,۴۶

جدول ۸-۱۳ : ترتیب توالی اهمیت شاخص‌های اثرگذار در فرضیه چهارم

تعداد	۱۱۳
کای اسکوئر	۳۷,۰۷۳
درجه آزادی	۶
معنی داری	.۰۰۰

جدول ۸-١٤: آزمون فریدمن

داده‌های جداول ۸-۱۳ حاکی از آن است که ارزش خی دوی مشاهده شده (۳۷,۰۷۳) در درجه آزادی ۶ در آزمون فریدمن، معنی‌دار است. از طرفی داده‌های جدول ۸-۱۴ نشان می‌دهد که به ترتیب شاخص‌های استفاده از استفاده از رمزنگاری قوی، سیستم‌های احراز هویت پیشرفته و ایجاد یک سیستم مدیریت امنیت جهت کنترل دستگاه‌های اینترنت اشیا به ترتیب بیشترین

رتبه را در بین راهکارهای موثر در کاهش آسیب‌پذیری‌ها و تهدیدات فناوری اینترنت اشیا دارند. بدین ترتیب فرضیه فرعی چهارم به اثبات می‌رسد.

۹. یافته‌های پژوهش:

همانطور که در تحلیل فرضیه‌های تحقیق آمد اینترنت اشیا دارای کاربردهای موثری در حوزه پدافند غیرعامل نظیر، افزایش سطح نظارت و کنترل زیرساخت‌های حیاتی و اتصال دائمی به اشیا و محیط در مقابله با بحران‌ها است و در کنار این کاربردها چالش‌های مهم، سطح پایین حفاظت فیزیکی برخی دستگاه‌های اینترنت اشیا، پایش فراگیر بر سازمانهای اطلاعاتی حریف ، ایجاد لینک های صامت توسط اینترنت اشیا و سطح دسترسی بالا به اطلاعات بر حریم خصوصی افراد است.

در این خصوص راهبردها، سیاست‌ها و راهکارهای فنی جهت کاهش آسیب‌پذیری‌ها و تهدیدات وجود دارد که از مهمترین راهبردها، نهادینه سازی الزامات پدافندغیرعامل و تهیه دستورالعمل‌های امنیتی برای فناوری اینترنت اشیا و از مهمترین راهکارهای فنی به استفاده از رمزنگاری قوی، سیستم‌های احراز هویت پیشرفته و ایجاد یک سیستم مدیریت امنیت جهت کنترل دستگاه‌های اینترنت اشیا میتوان اشاره کرد.

۱۰. نتیجه‌گیری و پیشنهادها

با توجه به اینکه در شاخص راهکارهای فنی، راهکار بهره‌برداری از اینترنت اشیا در بستر شبکه ملی اطلاعات، کمترین رتبه و استفاده از رمزنگاری قوی، سیستم‌های احراز هویت پیشرفته و ایجاد یک سیستم مدیریت امنیت جهت کنترل دستگاه‌های اینترنت اشیا بیشترین رتبه را در تحلیل بدست آوردند، می‌توان نتیجه گرفت که رویکرد منفعلانه نسبت به فناوری اینترنت اشیا از دیدگاه صاحبنظران این حوزه مردود است و محدودسازی و ایجاد موانع بر سر راه این فناوری نتیجه‌ای در بر نخواهد داشت و این جریان عظیم دیر یا زود جای خود را در زندگی و فرایندهای کسب و کار باز خواهد کرد.

از طرفی در شاخص راهبردها و سیاست‌ها، راهبرد اعمال قوانین و مقررات جهت مسدودسازی شکاف‌های امنیتی کمترین رتبه و ایجاد بسترهای لازم برای پیاده‌سازی فناوری اینترنت اشیا با رعایت الزامات پدافندغیرعامل به عنوان راهبرد اصلی بیشترین رتبه را از نظر صاحبنظران کسب کرد و می‌توان نتیجه گرفت که اعمال مقررات سخت‌گیرانه در فضای سایبری کشور برای ورود فعالان این حوزه، تنها به سود شرکت‌های بزرگ خارجی خواهد بود و تجربه تلخ شبکه‌های اجتماعی که منجر به توقف استفاده از پیام

رسان‌های داخلی شد و در نهایت این تلگرام بود که از این حیاط خلوت استفاده نمود و فارغ از قونین و مقررات وضع شده قریب به اتفاق کاربران کشور را از آن خود کرد و علاوه بر خروج ارز از کشور پیامدهای خطرناک امنیتی برای کشور ایجاد کرد.

منابع

۱. یامی, نگار و محمد قیصری، ۱۳۹۵، مدیریت بحران با سیاست گذاری فناوری اینترنتی از اشیا(IOT) ، کنفرانس پدافند غیرعامل و توسعه پایدار، تهران، وزارت کشور،
۲. قیصری، محمد و شقایق سعادت فخیم، ۱۳۹۶، اینترنت اشیا؛ چالش‌های دنیای بهم متصل، تهران.
۳. دلاوری، ایمان و مصطفی جلال، نقش تعیین کننده پدافندغیرعامل در مدیریت بحران و روش‌های بکارگیری آن، نشریه عمران، مقاوم‌سازی و بهسازی، شماره۱۰، تهران.
۴. عاملی، سعید، ۱۳۹۵، مرکز ملی فضای مجازی.
۵. مرکز پژوهش‌های مجلس شواری اسلامی، ۱۳۹۵، کاربرد اینترنت در بخش های سلامت و بهداشت، انرژی، کارخانه ها، ساختمان ها و حمل و نقل.
۶. پژوهشگاه ارتباطات و فناوری اطلاعات، ۱۳۹۴، طرح ملی اینترنت اشیا.
۷. خبرگزاری مشرق، ۱۳۹۵، بیگانگان وارد می‌شوند؛ زیرساخت «اینترنت اشیاء» ایران به فرانسه واگذار شد.

References

۸. Azari, A., Miao, G. (۲۰۱۶). Battery Lifetime-Aware Base Station Sleeping Control with M۲M/H۲H coexistence. In: IEEE onference proceedings
۹. Carynthia, K., Chithralekha, T., Reena, V. (۲۰۱۶). A SDN Controller with Energy Efficient Routing in the Internet of Things (IoT). Pondicherry University, Pondicherry ۶۰۵ ۰۱۴, India.
۱۰. Chui, M., Löffler, M. & Roberts, R. (۲۰۱۰). The internet of things. McKinsey Quarterly, ۲: ۱-۹.
۱۱. Da Xu, L., He, W. & Li, S. (۲۰۱۴). Internet of things in industries: A survey, IEEE Transactions on Industrial Informatics, ۱۰(۴): ۲۲۳۳ - ۲۲۴۳.
۱۲. Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton., N. & Razafindralambo, T. (۲۰۱۴). A Survey on Facilities for Experimental Internet of Things Research. IEEE Communications Magazine, ۴۹(۱۱): ۵۸ - ۶۷.
۱۳. Harsha, M., Vaibhav, K., and Sini, S. (۲۰۱۵). Cluster Based Energy Efficient Routing Protocol for Wireless Sensor Network, Engineering Universe for Scientific Research and Management, vol. ۷, issue ۱.