فصلنامه علمی امنیت ملی
سال یازدهم، شماره سی‌ونهم، بهار ۱۴۰۰
مقاله هفتم از صفحات ۲۲۸-۱۹۹

مقاله پژوهشی: رتبه‌بندی تهدیدهای اینترنت اشیاء در محیط نظامی

۲۰,۱۰۰۱,۱,۳۳۲۹۲۵۳۸,۱۴۰۰,۱۱,۳۹,۷,۱

رسول رمضانی[۱] محمدرضا موحدی‌صفت[۲]

تاریخ دریافت: ۹۸/۰۹/۰۸ تاریخ پذیرش: ۹۹/۰۸/۱۰

چکیده

فناوری اینترنت اشیاء یکی از فناوری‌های نوظهور است که امکان ارسال و دریافت داده‌ها بین اشیاء از طریق شبکه‌های ارتباطی را فراهم نموده و منشأ ایجاد تغییرات شگرفی در حوزه‌های مختلف ازجمله حوزه نظامی می‌باشد. بهره‌گیری از این فناوری در کنار مزایای بسیاری که برای سازمان‌های نظامی خواهد داشت، تهدیدهایی را نیز به همراه دارد که امنیت مهم‌ترین آن‌ها است. درنتیجه شناسایی تهدیدهای ناشی از این فناوری نوظهور موضوعی بسیار حیاتی و قابل مطالعه است. از آنجا که تعیین راهبردهای به‌کارگیری فناوری اینترنت اشیاء در محیط نظامی منوط به تعیین میزان اهمیت تهدیدهای ناشی از این فناوری است، درنتیجه هدف از این تحقیق، رتبه‌بندی تهدیدهای اینترنت اشیاء در حوزه نظامی است و سؤال اصلی تحقیق آن است که در حوزه نظامی کدام‌یک از تهدیدهای فناوری اینترنت اشیاء از اهمیت بیشتری برخوردار است؟ این تحقیق به روش توصیفی (موردی) و با رویکرد آمیخته (کمی و کیفی) و بهره‌گیری از روش‌های پژوهش عملیاتی چندمعیاره (تاپسیس) است. برای سنجش تهدیدها از پنج معیار زمان لازم جهت اثرگذاری تهدید، میزان خسارت وارده در صورت وقوع تهدید، میزان تأثیر تهدید بر حوزه تصمیم‌گیری، میزان تأثیر تهدید درنتیجه نبرد و میزان بازگشت‌پذیری اثر تهدید، استفاده شده است. جامعه آماری این تحقیق شامل تعداد هفت نفر از خبرگان و ۵۰ نفر از صاحب‌نظران حوزه‌های سایبری و نظامی در رده‌های صف و ستاد می‌باشد. بر اساس نتایج این تحقیق، در سازمان‌های نظامی از میان تهدیدهای مختلف فناوری اینترنت اشیاء، تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها از اهمیت بیشتری برخوردار می‌باشند.

۱. دانش آموخته مدیریت راهبردی فضای سایبر، دانشکده امنیت، دانشگاه عالی دفاع ملی، تهران، ایران، (نویسنده مسئول) r.ramezany@sndu.ac.ir

۲. عضو هیئت علمی دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

کلیدواژه‌ها: آسیب‌پذیری، اینترنت اشیاء، تهدید، محیط نظامی.

۱. مقدمه

اینترنت اشیاء یکی از فناوری‌های نوین در عصر کنونی است که انقلاب آینده در فناوری‌های دیجیتال را رقم خواهد زد و افزایش سلامت، بهره‌وری، امنیت و راحتی را برای افراد و سازمان‌ها در پی خواهد داشت. به‌کارگیری اینترنت اشیاء فرصت‌های بی‌شماری را در اختیار سازمان‌های مختلف قرار می‌دهد و اگر این فناوری به نحو صحیحی به کار گرفته شود، برای کار و زندگی آینده تحولی عظیم به وجود خواهد آورد.

اینترنت اشیاء با ترکیب دو عرصه دیجیتالی و فیزیکی، دسترسی به فناوری اطلاعات را گسترده‌تر می‌سازد. امکانات بی‌شمار فراهم‌شده به کمک توانمندی نظارت و کنترل اشیاء، موج جدیدی از نوآوری‌ها را ارائه خواهد نمود. اینترنت اشیاء می‌تواند تغییرات وسیعی را در چگونگی نظارت از راه دور بر فعالیت‌های مختلف، ردیابی کالاها، مدیریت دارایی‌های فیزیکی، میزان توجه افراد به سلامت و شیوه عملکرد شهرها ایجاد نماید و منجر به شکل‌گیری چشم‌اندازهای مختلفی برای آینده گردد (گزارش شماره ۳ معاونت علمی و فناوری ریاست جمهوری، ۱۳۹۵: ۳).

بی‌شک ورود اینترنت اشیاء در عرصه امور دفاعی و نظامی نیز قابلیت‌های جدید و شگرفی را در اختیار این بخش‌ها قرار خواهد داد. بهره‌گیری از این فناوری نوین به یگان‌های نظامی و دفاعی فرصت خواهد داد تا از ظرفیت سنسورهای بسیار کم‌هزینه، متنوع و کنترل‌پذیر، در نظارت مستمر بر صحنه نبرد، نظارت بر محیط پیرامونی، نظارت بر سلامت و امنیت تجهیزات و کارکنان و کنترل ساختمان‌ها بهره گرفته و علاوه بر کاهش نیروی انسانی مورد نیاز، به برتری اطلاعاتی نیز دست یابند. از طرفی به‌کارگیری فناوری اینترنت اشیاء در محیط نظامی بدون توجه به تهدیداتی که به‌کارگیری این فناوری می‌تواند به همراه داشته باشد، موجب غفلت راهبردی نیروهای نظامی خواهد شد. از آنجا که نوع، میزان اهمیت و تأثیرگذاری تهدیدهای اینترنت اشیاء برای سازمان‌های مختلف، متفاوت است، درنتیجه پیش از به‌کارگیری فناوری اینترنت اشیاء در سازمان‌های نظامی بایستی نسبت به شناسایی و تعیین

میزان تأثیر تهدیدهای به‌کارگیری این فناوری اقدام نموده و بر اساس مهم‌ترین و با اولویت‌ترین تهدیدها، راهبردهای مورد نیاز تدوین گردد. رتبه‌بندی تهدیدها از جهت مشخص نمودن شیوه، سطح و راهبردهای به‌کارگیری فناوری اینترنت اشیاء در محیط نظامی و همچنین میزان تخصیص منابع در راستای مواجهه با تهدیدها حائز اهمیت بوده و در صورت عدم رتبه‌بندی صحیح تهدیدها، بیم آن می‌رود که تهدیدهای با اولویت بالاتر، مغفول واقع شده یا به میزان لازم مورد توجه قرار نگیرند؛ بنابراین هدف از این تحقیق، شناسایی و رتبه‌بندی تهدیدهای اینترنت اشیاء در سازمان‌های نظامی بوده و سؤال اصلی تحقیق آن است که در سازمان‌های نظامی کدام‌یک از تهدیدهای به‌کارگیری فناوری اینترنت اشیاء از اهمیت بیشتری برخوردار می‌باشند؟ همچنین با توجه به اینکه شناسایی تهدیدها در محیط نظامی انجام شده و رتبه‌بندی تهدیدها بر اساس معیارهای خاصی صورت گرفته است، این تحقیق از لحاظ محیط تحقیق و شیوه تحقیق دارای نوآوری می‌باشد.

۲. مبانی نظری تحقیق

در این تحقیق مرور کوتاهی بر مباحث تهدیدهای پیش روی این فناوری خواهیم داشت. به این منظور پس از بررسی تعدادی از تحقیق‌های انجام‌شده در زمینه تهدیدهای اینترنت اشیاء، به معرفی فناوری اینترنت اشیاء و کاربردهای نظامی آن پرداخته و سپس به بررسی و دسته‌بندی تهدیدهای این فناوری می‌پردازیم.

پیشینه تحقیق

عبدالغنی، کنستانتاس و محیوب (۲۰۱۸: ۳۵۵-۳۷۳)، در مقاله‌ای تحت عنوان «بررسی جامعی از حملات اینترنت اشیاء بر اساس یک مدل مرجع»، به بررسی منابع تهدیدات امنیتی اینترنت اشیاء در چهار لایه سنجش، شبکه، میان‌افزار و لایه کاربرد پرداخته و بیان می‌دارند که حملات امنیتی اینترنت اشیاء عبارت‌اند از: گرفتن گره، تزریق کد مخرب،

تزریق داده‌های غلط، حملات کانال جانبی، استراق سمع و تداخل، محرومیت از خواب و بوت کردن سامانه.

تاج، ترکمن و معدنی (۱۳۹۶: ۵۲-۳۷)، در مقاله‌ای تحت عنوان «طبقه‌بندی موضوعات اینترنت اشیاء و درجه‌بندی حساسیت آن‌ها»، نقش موضوعات مرتبط با اینترنت اشیاء (ارتباطات، حسگرها، فعال‌کننده‌ها، فضای ذخیره‌سازی، دستگاه‌ها، پردازش، محلی‌سازی و ردیابی، شناسایی و تعیین هویت) در مباحث امنیتی (محرمانگی، جامعیت، دسترس‌پذیری، احراز هویت و حریم خصوصی) را بررسی و میزان حساسیت هریک را مشخص نموده‌اند.

تونبو، اسکوبی و تدینی (۲۰۱۷: ۱۶۹-۱۸۵)، در پژوهشی تحت عنوان «تهدیدهای امنیت سایبری اینترنت اشیاء در حوزه خدمات و برنامه‌های کاربردی»، به بررسی آسیب‌پذیری‌ها و تهدیدهای امنیت سایبری اینترنت اشیاء پرداخته و با تجزیه‌وتحلیل آسیب‌پذیری‌های سامانه در مقابل بازیگران تهدید بالقوه، پنج نوع تهدید شامل حمله فیزیکی (دستگاه)، حمله به نرم‌افزار، حمله به شبکه، حمله به رابط وب و حمله به دادها را معرفی می‌نمایند.

تسنیم، ران، فادی و ایمران (۲۰۱۵: ۴۷-۵۵)، در مقاله‌ای تحت عنوان «امنیت اینترنت اشیاء: وضعیت فعلی، چالش‌ها و اقدامات متقابل»، بیان می‌دارند که مهم‌ترین نگرانی در تحقق چارچوبی به‌طور کامل هوشمند اینترنت اشیاء، امنیت است. اگر نگرانی‌های امنیتی مانند حریم خصوصی، محرمانه بودن، احراز هویت، کنترل دسترسی، امنیت پایدار، مدیریت اعتماد، سیاست‌های جهانی و استانداردها به‌طور کامل مورد توجه قرار گیرند، در آینده‌ای نزدیک، تغییر همه‌چیز توسط اینترنت اشیاء صورت می‌گیرد.

فناوری اینترنت اشیاء

وب‌سایت جهانی (وب ۱) در سال ۱۹۸۹ میلادی، با اولین و تنها سایت در آن زمان به دنیا آمد. ده سال بعد دنیای جدیدی از فرصت‌ها شروع به ظهور کرد، زمانی که کوین اشتون، از مؤسسه فناوری ماساچوست، اصطلاح اینترنت اشیاء را تعریف کرد. وی در

تعریف خود جهانی را توصیف کرد که در آن هر چیزی ازجمله اشیاء بی‌جان برای خود هویت دیجیتال دارند و رایانه‌ها این قابلیت را دارند که این اشیا را مدیریت نمایند. بخش استاندارد بین‌المللی، ارتباطات مخابراتی در اینترنت اشیاء را این‌گونه تعریف می‌نماید: یک زیرساخت جهانی برای جامعه اطلاعاتی، فراهم آوردن خدمات پیشرفته با اتصال (چیزهای فیزیکی و مجازی) با استفاده از فناوری‌های اطلاعاتی و ارتباطی موجود و درحال‌توسعه (حسن، رحمان‌خان و مدنی، ۲۰۱۸: ۳). همچنین وزارت دفاع آمریکا در تعریف اینترنت اشیاء بیان می‌دارد که: اینترنت اشیاء عبارت است از دستگاه‌های نیمه‌اتوماتیک (اشیاء)، با قابلیت استفاده از محاسبات ساده، شبکه، مشاهده و احساس و به‌کارگیری این قابلیت‌ها برای حس کردن و اقدام در دنیای فیزیکی (سند اینترنت اشیاء وزارت دفاع آمریکا، ۲۰۱۶: ۲). اینترنت اشیاء 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 سازمان 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 دارد (گزارش شماره ۱ معاونت علمی و فناوری ریاست جمهوری، ۱۳۹۵: ۴).

اینترنت اشیاء و کاربردهای حوزه نظامی

در حوزه نظامی اینترنت اشیاء، ظرفیت بالایی جهت روزآمدسازی جنگ‌افزارها، استفاده از داده‌ها و خودکارسازی جهت حفظ جان سربازان و از طرف دیگر کاهش هزینه‌ها و افزایش کارایی وجود دارد. شناسایی، کنترل و نظارت نیروها و جنگ‌افزارها، از مهم‌ترین کاربردهای اینترنت اشیاء در حوزه نظامی است (یزدان‌پناه، ۱۳۹۵: ۷-۶). تا به امروز، استقرار و کاربرد فناوری‌های مرتبط با اینترنت اشیاء در سازمان‌های نظامی، به‌طور کلی با هدف اجرای برنامه‌هایی برای سیستم‌های فرماندهی، کنترلی، ارتباطی، رایانه‌ای، هوشمند، نظارت و شناسایی و کنترل آتش بوده است. این موضوع ناشی از دیدگاهی است که بر طبق آن،

حسگرها، به‌عنوان ابـزاری جهـت جمـع‌آوری و بـه‌اشـتراک‌گـذاری داده‌هـا و همـین‌طـور اثربخشی بیشتر فرماندهی و کنترل شناخته شده‌اند(اراشی، پدرسن و هایلوک، ۲۰۱۷: ۹).

در صورت گسترش کاربرد اینترنت اشـیاء در حـوزه نظـامی، تجهیـزات نظـامی مـدرن به‌طور فزاینده‌ای با قابلیت پردازش و ارتباطات مجهز شده و برای بررسی و تغییر وضـعیت تجهیزات مورد استفاده قرار خواهند گرفت. این تجهیزات می‌توانند به‌عنوان سنسورها و یـا محرک‌ها در نظر گرفته شوند و در بقیه زیرساخت‌های اطلاعاتی ارتقـاء یابنـد (گـزارش فـروم جهانی اینترنت اشیاء، ۲۰۱۸).

بخش‌های بالقوه یگان‌های نظامی جهت استفاده از این فناوری عبارت‌اند از:

- لجستیک (فرماندهی و کنترل پشتیبانی و تدارکات عملیات ترکیبی)
- آگاهی وضعیتی (در سطح تاکتیکی یـک میـدان جنـگ ازجملـه نظـارت، سـنجش، شناسایی تهدید، موقعیت هدف، علامت‌گذاری وسایل نقلیه و سربازان، نظـارت بـر وضعیت و نظارت بر محیط زیست)
- مراقبت‌های پزشکی (نظارت بر سـلامت بیمـاران و جنگجویـان) (گـزارش گـروه کـاری آر.تی.او، ۲۰۱۵: ۴۷).

طبقه‌بندی کلی تهدیدهای اینترنت اشیاء

تهدیدهای اینترنت اشیاء را می‌توان بر اساس روش حمله، به هشت دسته تقسیم نمـود. این حمله‌ها عبارت‌اند: نقـض حـریم خصوصـی، اسـتراق سـمع، منـع سـرویس، تخریـب تجهیزات، شبیه‌سازی مجازی وسایل، سرقت اطلاعـات، انتشـار بـدافزار و سـرقت هویـت کاربر (استاندونن و وان، ۲۰۱۹: ۲۲).

همچنین تهدیدهای اینترنت اشیاء را می‌توان با توجه به حملـه‌هـایی کـه بـه لایـه‌هـای تشکیل‌دهنده اینترنت اشـیاء انجـام مـی‌شـود، بـه تهدیـدهای لایـه برنامـه‌هـای کـاربردی، تهدیدهای لایه شبکه و تهدیدهای لایه دریافت هوشمند تقسـیم‌بنـدی نمـود (مسـعودی، الام و صدیقی، ۲۰۱۹: ۷۰).

در دسته‌بندی دیگری، تهدیدهای اینترنت اشیاء بر اساس انگیزه‌های احتمالی حملات و نوع صدمه به قربانی به سه دسته کلی: تهدیدهای امنیت سامانه‌ها، تهدیدهای حریم خصوصی و تهدیدهای شهرت و اعتبار کارخانه سازنده تقسیم می‌شوند (میسرا، ماهسواران و هاشمی، ۲۰۱۷: ۲۵).

با توجه به تقسیم‌بندی‌های فوق، در این تحقیق تهدیدهای اینترنت اشیاء به پنج دسته تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها، تهدیدهای مبتنی بر نقض حریم خصوصی، تهدیدات مبتنی بر نقض امنیت اطلاعات، تهدیدهای مبتنی بر نقض امنیت شبکه و رایانش ابری و تهدیدهای مبتنی بر نقض امنیت تجهیزات دریافت هوشمند، تقسیم‌بندی می‌شوند و مورد بررسی قرار می‌گیرند.

الف. تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها

اینترنت اشیاء در حوزه‌های نظامی، اقتصاد جهانی، خدمات پزشکی و مراقبت‌های بهداشتی، حمل‌ونقل هوشمند و بسیاری دیگر از حوزه‌ها به کار گرفته می‌شود، درنتیجه نیازمندی‌های امنیتی در آن از اهمیت بالایی برخور می‌باشد (تریپاتی و آنورادها، ۲۰۱۸: ۱۷۸). رزمایش‌های سایبری در حوزه نظامی شامل «استفاده از برنامه‌های کاربردی جهت تسخیر، خرابکاری، انکار، تخریب، نابودی یا دست‌کاری در محاسبات و منابع اطلاعاتی» می‌باشند. حملات تسخیر، جهت به دست آوردن کنترل سامانه‌های سایبری دشمن (فیزیکی یا مجازی) در راستای به دست آوردن مزیت موقعیتی یا دسترسی به اطلاعات در راستای کسب مزیت جاسوسی طراحی شده است. حملاتی با هدف خرابکاری، تخریب، انکار یا نابودی سرویس، ضعف رقابتی را در قربانیان ایجاد می‌کند و حملات دست‌کاری با هدف تأثیر بر چرخه‌های تصمیم‌گیری و سامانه فرماندهی و کنترل دشمن صورت می‌پذیرد(اپلیگیت، ۲۰۱۶: ۹-۱).

همچنین امنیت ریزتراشه‌های به‌کاررفته در تجهیزات اینترنت اشیاء از اهمیت زیادی برخوردار است. دستیابی خرابکاران به کارخانه‌های تولیدکننده این ریزتراشه‌ها که در تمام

زیرساخت‌های فنی اینترنت اشیاء مورد استفاده قرار می‌گیرند، موجب به خطر افتادن امنیت فیزیکی تجهیزات اینترنت اشیاء خواهد شد (باساک، ۲۰۱۷: ۶).

- **تهدیدهای تسخیر**: این دسته شامل تهدیدهایی است که کنترل مهاجم بر یک بخش فیزیکی یا منطقی زیرساخت‌های اینترنت اشیاء را تأمین می‌کند. درنتیجه مهاجم مزیت موقعیتی/جاسوسی جهت کنترل تجهیزات را به دست می‌آورد یا به برخی از اطلاعات حیاتی سامانه‌های نظامی یا وضعیت صحنه نبرد دسترسی می‌یابد. برای مثال، اگر مهاجم یک کنترل‌کننده شبکه فرماندهی و کنترل هوشمند را در اختیار بگیرد، می‌تواند اهداف خودی را مورد حمله قرار داده یا از انجام اقدام تاکتیکی بر روی اهداف متخاصم جلوگیری نماید (میسرا و همکاران، ۲۰۱۷: ۲۷).
- **تهدیدهای اختلال**: تجهیزات اینترنت اشیاء به دلیل ساختار طراحی و عملکردی، نیازمند ارتباط دائم با مراکز کنترل می‌باشند. این نیازمندی تجهیزات اینترنت اشیاء را در معرض تهدیدهای خاصی قرار می‌دهد که منجر به ایجاد اختلال در عملکرد سامانه خواهد شد. این تهدیدها می‌تواند به‌منظور قطع روند ارائه خدمات، تخریب تجهیزات یا سوءقصد به جان افراد انجام گیرد (تریپاتی و آنورادها، ۲۰۱۸: ۲۱۹). محققان در محیط آزمایشگاهی توانسته‌اند برخی از نقص‌های تجهیزات اینترنت اشیاء که منجر به هک شدن آن‌ها می‌شود را پیدا کنند و این به آن معنا است که دشمن در صحنه نبرد واقعی نیز می‌تواند چنین اقداماتی را انجام دهد (پرستش، ۱۳۹۵: ۱۴).
- **تهدیدهای دست‌کاری**: این بخش از تهدیدهای امنیتی سامانه شامل تهدیدهای مؤثر بر چرخه تصمیم‌گیری فرماندهی و کنترل هدف است. چرخه تصمیم‌گیری با تولید داده‌ها آغاز می‌شود. تهدید دست‌کاری ممکن است مربوط به خرابی اطلاعات قبل از ورود به سامانه اینترنت اشیاء باشد. در این مورد حتی اگر محیط داخلی اینترنت اشیاء امن باشد و صحیح عمل کند، با توجه به اقدامات «صحیح» بر اساس اطلاعات نادرست، ممکن است موجب افزایش ملاحظات امنیتی شود. شکل نهایی تهدیدهای

دست‌کاری زمانی خواهد بود که به دلیل دخالت غیر مجاز، جامعیت داده‌ها بین سامانه تولیدکننده داده و سامانه فرماندهی و کنترل جابه‌جا می‌شود. حملاتی مانند «مردی در میان»[1] «تکرار»[2] و «جعل»[3] چنین تهدیدی را برای جامعیت داده‌ها ایجاد می‌کنند (میسرا و همکاران، ۲۰۱۷: ۲۸).

- **تهدیدهای مرتبط با ریزتراشه‌ها:** ریزتراشه‌ها که هسته اصلی پردازش و تصمیم‌گیری در تجهیزات اینترنت اشیاء می‌باشند، از میلیون‌ها ترانزیستور و هزاران مدار الکترونیکی تشکیل شده‌اند. با توجه به ابعاد این ریزپردازنده‌ها، امکان شناسایی مدارات اضافی تعبیه‌شده که موجب بروز شکاف امنیتی می‌گردند، بسیار دشوار خواهد بود. از آنجا که این ریزتراشه‌ها در سامانه‌های بسیار حساس نظامی و اطلاعاتی به کار خواهند رفت، لزوم توجه به شناسایی دقیق خرابکاری در آن‌ها بیش‌ازپیش هویدا می‌گردد. صاحب‌نظران بر دوگونه از این شکاف‌های عملکردی تمرکز کرده‌اند. گونه اول به «کلیدهای ازکارانداز» مشهور هستند. درواقع، کارخانه تولید ریزتراشه‌ها می‌تواند در هنگام ساخت یک ریزتراشه، مدارهایی را به طرح اصلی اضافه نماید. این مدارهای افزوده‌شده که تقریباً شناسایی آن‌ها غیرممکن است، می‌توانند با دریافت محرکی خاص، فعال شوند و کارکردهای اصلی ریزتراشه را مختل نمایند. برای مثال، ریزتراشه‌ای که در سامانه رادار پدافند هوایی سوریه وظیفه کنترل سامانه را بر عهده داشته است، با تحریک یک سیگنال ارسالی از یک فروند هواپیمای رژیم صهیونیستی ازکارافتاده است و کل کارکرد سامانه مختل شده است. دسته دوم از شکاف‌های عملکردی ریزتراشه‌ها، «حفره‌های امنیتی» هستند. این حفره‌ها به نفوذگران اجازه می‌دهند تا از طریق کدهای ویژه یا سخت‌افزار، به سامانه دسترسی یابند و یک کارکرد

1 Man-in-the-Middle
2 Replaying
3 Spoofing

ویژه را از کار بیاندازند یا آن را فعال کنند. توجه شود که کاربران اصلی سامانه از هیچ‌یک از این دو مورد باخبر نمی‌شوند (کاشیپور، ۱۳۹۴: ۳۳-۱۷).

ب. تهدیدهای مبتنی بر نقض حریم خصوصی

حریم خصوصی شامل پنهان کردن اطلاعات شخصی و همچنین توانایی کنترل آنچه با این اطلاعات اتفاق می‌افتد، می‌باشد. بر این اساس تهدید حریم خصوصی به‌صورت زیر تعریف می‌شود: احتمال قرار گرفتن اطلاعات حساس در اختیار اشخاصی (شخص، کشور یا هوش مصنوعی) که مجاز به داشتن آن داده‌ها نمی‌باشند. این تهدید زمانی که تعداد زیادی از تجهیزات اینترنت اشیاء، حجم زیادی از داده‌های مرتبط با افراد را تولید، ارسال و دریافت می‌کنند، منجر به نظارت دائمی بر فعالیت‌های افراد از طریق دستگاه‌های مختلف می‌شود. این نظارت ممکن است الزامات مختلفی را راجع به حفظ حریم خصوصی و محافظت از داده‌های شخصی ایجاد کند (حسام‌الدین و کایو، ۲۰۱۸: ۱۱). کمیسیون تجارت فدرال آمریکا گزارش کرده است که ده هزار خانوار می‌توانند به‌تنهایی در هر روز در حدود ۱۵۰ میلیون داده گسسته تولید کنند که این امر به معنای نقاط نفوذ بیشتر برای هکرها است که می‌تواند به نشر اطلاعات حساس منجر شود (پرستش، ۱۳۹۵: ۱۴).

بر اساس انگیزه بهره‌برداری، تمام تهدیدهای حریم خصوصی حاوی عناصر تهدید بنیادی زیر هستند:

- **تهدیدهای پیش‌بینی اقدام**: داده‌هایی که از طریق نفوذ به حریم خصوصی به‌دست‌آمده جهت جلوگیری از اقدامات آینده مالک اطلاعات استفاده می‌شوند. به‌عنوان مثال داده‌های مصرف انرژی یگان‌های نظامی می‌توانند برای برآورد حضور/ عدم حضور کارکنان یا تعداد نیروهای حاضر در یگان مورد تجزیه‌وتحلیل قرار گیرند.

- **تهدیدهای شرکت:** این تهدید شامل اتصال دستگاه‌های هوشمند خاص به یک فرد است. برای مثال، هنگامی که یک شیء با یک برچسب کد الکترونیکی محصول[1] توسط نیروهای نظامی خریداری و مورد بهره‌برداری قرار می‌گیرد، ارتباطی بین هویت مشتری و شماره سریال الکترونیکی آن شیء ایجاد می‌شود. این ارتباط را می‌توان در بسیاری از موارد مورد سوءاستفاده قرار داد، مانند ردیابی مخفیانه نیروهای نظامی صاحب دستگاه.
- **تهدیدهای ترجیحی:** بر اساس هویت دستگاه‌های متعلق به فرد/ حمل‌شده توسط یک فرد، می‌توان پیش‌بینی‌های مربوط به مزه/ ترجیحات و حتی وضعیت مالی فرد را انجام داد.
- **تهدیدهای حریم خصوصی مکانی:** خدمات مبتنی بر مکان، مزایای متعددی را برای کاربران از قبیل مزایای مالی ارائه می‌دهد. با این حال، احتمال افشای غیرمجاز اطلاعات مکان، یک نگرانی عمده است و تهدید جدی برای حریم خصوصی کاربران، به‌خصوص کارکنان نظامی است.
- **تهدیدهای نظارت بر تراکنش:** هنگامی که اشیاء برچسب‌دار از یک یگان به یگان دیگری منتقل می‌شوند، تراکنش بین اشخاص وابسته به دو یگان می‌تواند نتیجه‌گیری شود.
- **تهدیدهای ردیابی (جاسوسی) دیجیتالی:** ردیابی دیجیتالی به معنای یک میدان دید غیر صریح از یک فرد، سازمان یا شیئی است که می‌تواند از طریق اینترنت اشیاء یا سایر سوابق دیجیتالی یافت شود. ردیابی دیجیتالی منحصربه‌فرد از طریق دستگاه‌های هوشمند مرتبط با یک نهاد (فرد/ سازمان/ شیء) قابل انجام است.

ج. تهدیدهای مبتنی بر نقض امنیت اطلاعات

[1] Electronic Product Code(EPC)

مفاهیم اساسی امنیت داده، پیرامون سه محور محرمانگی، یکپارچگی و در دسترس بودن است. در اینترنت اشیاء، داده‌های مختلفی وجود دارد و هرگونه افشای غیرمجاز داده ممکن است منجر به نقض محرمانه بودن، تمامیت یا در دسترس بودن داده‌ها شود (بتان، استربرگ و سونگ، ۲۰۲۰: ۶۱۷). در ادامه برخی از تهدیداتی که منجر به بروز نقض امنیت داده می‌گردد مورد بررسی قرار می‌گیرد:

- **حمله منع خدمات:**[1] این حمله یکی از ساده‌ترین و در عین حال متداول‌ترین حمله‌های امنیتی می‌باشد و تعداد روزافزون دستگاه‌های اینترنت اشیاء با ویژگی‌های امنیتی ضعیف، این حمله را به ابزاری مورد علاقه برای مهاجمین تبدیل کرده است. در حمله منع خدمات، ارسال درخواست‌های نامعتبر منجر به فرسودگی منابع شبکه (به‌عنوان مثال، مصرف پهنای باند) شده و درنتیجه، خدمات برای کاربران اصلی در دسترس نخواهد بود. حمله منع خدمت توزیع‌شده، یک نسخه پیشرفته از این حمله است که در آن چندین منبع به یک هدف واحد حمله می‌کنند و ردیابی و جلوگیری از حمله را دشوارتر می‌کنند.
- **حمله مردی در میان:** این حمله یکی از قدیمی‌ترین حملات در دنیای سایبر است. کلاه‌برداری و جعل هویت را می‌توان در این حملات طبقه‌بندی کرد. بر اساس مطالعاتی که در حوزه امنیت داده در اینترنت اشیاء انجام شده است، وجود آسیب‌پذیری در برابر این حملات، در تجهیزات مراقبت‌های بهداشتی و همچنین در سامانه‌های تأیید هویت بی‌سیم اینترنت اشیاء، به اثبات رسیده است.
- **حمله نصب بدافزار:** استفاده از دستگاه‌های اینترنت اشیاء و بخش‌های نرم‌افزاری مربوطه روز به روز در حال افزایش است که این امر، احتمال حمله‌های بدافزاری و انجام فعالیت‌های مخرب بر روی این دستگاه‌ها را افزایش می‌دهد. به‌طور کلی بدافزارها تحت عنوان ویروس، نرم‌افزارهای جاسوسی، کرم، اسب تروجان و ... شناخته می‌شوند. تجهیزات خانه‌های هوشمند، مراقبت‌های بهداشتی و

1 Denial of Service (DoS)

حسگرهای وسایل نقلیه، چند نمونه از دستگاه‌های اینترنت اشیاء می‌باشند که در برابر نفوذ بدافزارها آسیب‌پذیر هستند (وحید، هی، اکرام، هاشمی و عثمان، ۲۰۲۰: ۴۴).

- **حمله تزریق کد مخرب:** در چنین حملاتی، مهاجم کدهای مخرب را در یک برنامه قرار داده و از این طریق به داده‌های شخصی هر کاربر اینترنت اشیاء دست یافته یا سوابق موجود در پایگاه داده را تغییر دهد (بتان، استربرگ و سونگ، ۲۰۲۰: ۶۱۹).

د. تهدیدهای مبتنی بر نقض امنیت شبکه و رایانش ابری

عملکرد اصلی لایه شبکه انتقال اطلاعات دریافتی از لایه سنجش برای پردازش به واحد محاسباتی یا فضای ابری است. تعدادی از مهم‌ترین تهدیدات امنیتی در لایه شبکه و فضای ابری عبارت‌اند از:

- **حملات فیشینگ:** حملات فیشینگ اغلب به حملاتی اطلاق می‌شود که چندین دستگاه اینترنت اشیاء توسط مهاجم مورد هدف قرار گیرند. هنگامی که کاربر از صفحات وب در اینترنت بازدید می‌کند، امکان مواجهه با سایت‌های فیشینگ وجود دارد. هنگامی که حساب کاربری و رمز عبور کاربر به خطر بیفتد، کل محیط اینترنت اشیاء که توسط کاربر استفاده می‌شود، در برابر حملات سایبری آسیب‌پذیر خواهد شد. لایه شبکه در اینترنت اشیاء در برابر حملات سایت‌های فیشینگ بسیار آسیب‌پذیر است (گزارش گروه کاری ضد فیشینگ، ۲۰۱۷).
- **حمله دسترسی (تهدید مداوم پیشرفته[1]):** در این حمله یک شخص غیرمجاز به شبکه اینترنت اشیاء دسترسی یافته و برای مدت طولانی در شبکه، ناشناس (کشف‌نشده) باقی می‌ماند. هدف این نوع حمله، سرقت داده‌ها یا اطلاعات باارزش است، نه اینکه باعث آسیب به شبکه شود. برنامه‌های اینترنت اشیاء به‌طور مداوم، داده‌های ارزشمند را دریافت و انتقال می‌دهند و به همین دلیل در برابر چنین حملاتی بسیار آسیب‌پذیر هستند.

1 advanced persistent threat (APT)

- **حمله جابه‌جایی داده‌ها:** برنامه‌های اینترنت اشیاء با ذخیره و تبادل داده‌های بسیاری سروکار دارند. داده‌هایی که در سرورهای محلی یا ابر ذخیره شده‌اند، دارای ریسک امنیتی می‌باشند، اما داده‌هایی که در حال انتقال از یک مکان به مکان دیگر می‌باشند، در برابر حملات سایبری آسیب‌پذیرتر خواهند بود. با توجه به اینکه در برنامه‌های اینترنت اشیاء، داده‌های بسیاری بین حسگرها، اقدامگرها، ابر و ... منتقل می‌شوند و از فناوری‌های مختلفی در این جابه‌جایی داده‌ها استفاده می‌شود، بنابراین برنامه‌های اینترنت اشیاء مستعد نقض امنیت داده‌ها می‌باشند(عبدالغنی، کنستانتاس و محیوب، ۲۰۱۸: ۶۳).
- **حمله به فضای ابری:** اینترنت اشیاء در راستای دستیابی به فضای ذخیره‌سازی و قدرت محاسباتی منعطف، ناچار به استفاده از رایانش ابری می‌باشد. هرچند بهره‌گیری از رایانش ابری، طراحی و روش‌های پیاده‌سازی برنامه‌های اینترنت اشیاء را دگرگون ساخته ولی مشکلات امنیتی جدیدی را نیز به وجود آورده است. مهم‌ترین مشکل امنیتی در رایانش ابری تمایل آن به گذر از دپارتمان‌های فناوری می‌باشد. اگر این استانداردها رعایت نشود، اینترنت اشیاء در برابر رخنه‌های امنیتی آسیب‌پذیر می‌گردد. مهم‌ترین تهدیدهای اینترنت اشیاء در رایانش ابری عبارت‌اند از: سرقت اطلاعات داخل ابر، از دست دادن اطلاعات در اثر آسیب فیزیکی به ابر، سرقت کلمه عبور و ترافیک سرویس، رابط‌های برنامه‌نویسی کاربردی[1] ناامن و حملات منع سرویس (فضل‌علی، ۱۳۹۵: ۵۳-۵۰).

هـ. تهدیدهای مبتنی بر نقض امنیت تجهیزات دریافت هوشمند

این بخش از تهدیدات مربوط به به‌کارگیری فناوری‌هایی از قبیل فناوری شناسایی بی‌سیم[2] و شبکه حسگر بی‌سیم[3] در لایه دریافت اینترنت اشیاء می‌شود. فناوری شناسایی

1 Aplication Programing Interface(API)
2 RFID
3 WSNs

بی‌سیم، جهت تبادل خودکار اطلاعات، بدون هیچ‌گونه دخالت دستی به کار می‌رود و حسگرهای بی‌سیم جهت جمع‌آوری اطلاعات مختلف از محیط مورد استفاده قرار می‌گیرند (کومار، ساهو، ماهاپاترا و سواین، ۲۰۱۷: ۱۵۳). برچسب‌های مورد استفاده در فناوری شناسایی بی‌سیم، در معرض حملات مختلفی قرار دارند که برخی از رایج‌ترین این تهدیدها عبارت‌اند از:

- **غیر فعال کردن غیر مجاز برچسب‌ها (تهدید اعتبار)**: این حملات منجر به غیر فعال شدن برچسب‌های شناسایی بی‌سیم به‌صورت موقت یا دائم می‌شوند. مهاجم به ارائه یک تگ شناسایی بی‌سیم که باعث اختلال و سوء رفتار در عملکرد خواندن دستگاه شناسایی برچسب می‌شود، می‌پردازد و کد الکترونیکی[1] این برچسب، اطلاعات اشتباهی را در مورد هویت ترکیبی عددی منحصربه‌فرد خود ارائه می‌کند.
- **شبیه‌سازی غیر مجاز برچسب (تهدید صحت)**: به دست آوردن اطلاعات شناسایی (مانند کد الکترونیکی محصول)، از طریق دست‌کاری برچسب‌ها توسط دستگاه‌های شناسایی برچسب مخرب در این دسته قرار می‌گیرند. هنگامی که اطلاعات شناسایی یک برچسب به خطر بیافتد، تکرار برچسب (شبیه‌سازی برچسب) ممکن خواهد شد.
- **مسیریابی غیر مجاز برچسب (تهدید محرمانگی)**: یک برچسب می‌تواند از طریق دستگاه‌های شناسایی برچسب مخرب ردیابی شود، این امر منجر به از دست دادن اطلاعات حساس مانند آدرس اشخاص خواهد شد؛ بنابراین از دیدگاه مصرف‌کننده، با توجه به اینکه خرید یک محصول که برچسب شناسایی بی‌سیم دارد، می‌تواند ردیابی شود، محرمانگی را برای آن‌ها تضمین نمی‌کند و درواقع حریم شخصی آن‌ها را به خطر می‌اندازد (عطاریان، ۱۳۹۵: ۱۱-۷).

3- Electronic Product Code(EPC)

- **حملات بازپخش (تهدید دسترس‌پذیری)**: در این نوع از حملات جعل هویت، مهاجم از واکنش برچسب نسبت به تهدیدهای دستگاه‌های شناسایی برچسب مخرب برای جعل برچسب استفاده می‌کند. در حملات بازپخش به محض دریافت هر درخواست از دستگاه‌های شناسایی برچسب، سیگنال ارتباطی بین دستگاه‌های شناسایی برچسب و برچسب مورد استراق سمع، ثبت بازبخش قرار و می‌گیرد و به این ترتیب در دسترس بودن برچسب جعل می‌شود (لیائو، شوای و وانگ، ۲۰۱۸: ۲).

با توجه به اینکه شبکه‌های حسگر بی‌سیم جهت انتقال داده‌های محیطی مورد استفاده قرار می‌گیرند، به‌راحتی در معرض حملات امنیتی اینترنت اشیاء قرار دارند. برخی از مهم‌ترین این تهدیدات عبارت‌اند از:

- **حملات فیزیکی**: حسگرها به‌گونه‌ای طراحی می‌شوند که امکان به‌کارگیری آن‌ها در هر دستگاهی میسر باشد، بنابراین محافظت فیزیکی از حسگرها در تمامی دستگاه‌ها و همچنین متوقف کردن دسترسی فیزیکی غیرمجاز، دشوار است. یک نفوذگر می‌تواند در داده‌های موجود در یک گره/ سنسور تغییراتی ایجاد نموده و کل شبکه حسگر را در معرض خطر قرار دهد.
- **تهدید فروریختن گودال**: این یک حمله مهم است که در آن حمله‌کننده، بسته‌های داده را در برخی از نقاط شبکه ضبط کرده و سپس آن‌ها را به مکان دیگری انتقال می‌دهد. این روند می‌تواند به‌صورت انتخابی انجام شود(حسام‌الدین و کایو، ۲۰۱۸: ۱۱).
- **تکرار گره**: در این حمله، یک شناسه یک حسگر موجود در گره، در همان شبکه به‌عنوان یک حسگر جدید کپی می‌شود. این اقدام باعث سوءاستفاده از بسته‌های داده، ضبط خوانش‌های حسگر کاذب یا قطع عملکرد شبکه از طریق این حسگر می‌گردد.

- **استراق سمع:** متجاوز هنگام انتقال داده‌ها بین دو گره از طریق شبکه، اطلاعات را گوش می‌دهد. این حمله منجر به سرقت داده‌های جمع‌آوری‌شده از طریق یک حسگر می‌شود (راجو و باپوجی، ۲۰۱۶: ۸).

۳. روش‌شناسی تحقیق

این تحقیق به لحاظ هدف از نوع توسعه‌ای/کاربردی و به لحاظ روش از نوع توصیفی (موردی) و با رویکرد آمیخته (کمی و کیفی)، کیفی به روش تحلیل محتوا و کمی به‌صورت آمار توصیفی و بهره‌گیری از روش‌های پژوهش عملیاتی چندمعیاره (تاپسیس) می‌باشد. ابزار گردآوری اطلاعات پرسشنامه است. در بخش کیفی تحقیق ابتدا با انجام مطالعات کتابخانه‌ای و بررسی تحقیقات صورت‌گرفته در داخل و خارج از کشور، دسته‌بندی‌های مختلف تهدیدها و چالش‌های اینترنت اشیاء مورد تحلیل و بررسی قرار گرفت و پس از برگزاری چندین جلسه خبرگی و انجام مصاحبه عمیق، شیوه دسته‌بندی تهدیدها و معیارهای کلیدی مورد نظر در محیط نظامی انتخاب گردید. در بخش کمی، طی دو مرحله انتشار پرسشنامه، از صاحب‌نظران خواسته شد که میزان و شدت تأثیرگذاری هر دسته از تهدیدها را بر اساس معیارهای مورد نظر در محیط نظامی مشخص نمایند.

در این تحقیق برای سنجش روایی پرسشنامه از روایی محتوا، استفاده شده است. روایی محتوا اطمینان می‌دهد که ابزار مورد نظر به تعداد کافی، پرسش مناسب برای اندازه‌گیری مفهوم مورد سنجش را دارد. هر قدر این عناصر، مقیاس گسترده‌تر و قلمرو مفهوم مورد سنجش را بیشتر در برگیرند، روایی محتوا بیشتر خواهد بود. در این تحقیق، سؤال‌های پرسشنامه متناسب با مبانی نظری طراحی شده و سپس با توزیع آن بین صاحب‌نظران مرتبط با موضوع، معیارهای نامفهوم و غیر مرتبط تعدیل یا حذف شد و با پیشنهادهای ارائه‌شده، معیارهایی نیز اضافه شده و پرسشنامه اصلی بعد از این مرحله تدوین و توزیع گردید. جامعه آماری پژوهش شامل تعداد هفت نفر از خبرگان حوزه‌های سایبری و نظامی (که به‌صورت هدفمند و به روش گلوله برفی تا رسیدن نظرات به اشباع انتخاب گردیدند) و

تعداد ۵۰ نفر از صاحب‌نظران، مدیران و فرماندهان نظامی (که دارای شرایط داشتن مدرک کارشناسی ارشد و بالاتر، آشنایی با فضای سایبر و دارا بودن جایگاه مسئولیتی راهبردی) می‌باشد و جامعه نمونه به‌صورت تمام‌شمار برابر با جامعه آماری در نظر گرفته شد.

در مسائل مربوط به گزینه‌های گسسته، تکنیک‌های تصمیم‌گیری چندشاخصه[1] ابزارهایی مفید برای حل مسئله بوده و تصمیم‌گیرنده با انتخاب، اولویت‌بندی و رتبه‌بندی تعدادی از فعالیت‌ها مواجه است (هوانگ و یون، ۲۰۱۵: ۱۰۵). تکنیک تاپسیس که توسط هوانگ و یون ارائه گردید، از مفهوم معیار فاصله گزینه‌ها از راه‌حل ایده‌آل و راه‌حل ایده‌آل منفی استفاده می‌کند که یکی از پرکاربردترین مدل‌های تصمیم‌گیری چندشاخصه می‌باشد (ونکاتا، ۲۰۱۴: ۷). در این روش فرض بر این است که تعداد k نفر تصمیم‌گیرنده به ارزیابی m گزینه می‌پردازند که توسط تعداد n معیار مورد ارزیابی قرار می‌گیرند (چو و لین، ۲۰۱۳: ۲۸۴). شاخص‌ها به دو نوع شاخصی از جنس سود که بیشتر بودن آن‌ها بهتر است و شاخصی از جنس هزینه که کمتر بودن آن‌ها بهتر می‌باشد، دسته‌بندی می‌گردند. مراحل اجرای روش تاپسیس به شرح زیر است:

روش تاپسیس ماتریس تصمیم ذیل که m گزینه برحسب n معیار می‌باشد را ارزیابی می‌کند (جدول ۱).

جدول ۱. ماتریس تصمیم‌گیری

	C1	C2	C3	...	Cn
آلترناتیوها	w1	w2	w3	...	Wn
A1	r11	r12	r13	...	r1n
A2	r21	r22	r23	...	r2n
A3	r31	r32	r33	...	r3n
⋮	⋮	⋮	⋮	⋮	⋮
Am	rm1	rm2	rm3	...	rmn

1. Multiple Attribute Decision Making (MADM)

در این جدول Ai، i امین گزینه، Cj، j امین معیار، wj وزن اختصاص داده‌شده به j امین معیار و rij رتبه i امین گزینه برحسب j امین معیار است. مراحل اجرا به‌صورت ذیل ارائه شده است:

گام ۱: به دست آوردن وزن نسبی معیارها. با استفاده از تکنیک آنتروپی شانون مطابق با رابطه (۱) به محاسبه وزن نسبی هریک از معیارها با توجه به ماتریس تصمیم می‌پردازیم.

$$P_{ij} = \frac{r_{ij}}{\sum_{i=1}^{m} r_{ij}}; \quad \forall i,j$$
$$E_j = -\frac{1}{\ln m} \sum_{i=1}^{m} [P_{ij}.\ln P_{ij}]; \quad \forall j \qquad (1)$$
$$d_j = 1 - E_j; \ \forall j \quad \Rightarrow \quad w_j = \frac{d_j}{\sum_{j=1}^{n} d_j}; \forall j \quad (\text{درجه انحراف})$$

گام ۲: ساختن ماتریس تصمیم نرمال‌شده. این گام معیارهای ابعادی عملکرد را به ویژگی‌های غیر ابعادی تبدیل می‌کند. درایه‌های ماتریس R به‌صورت رابطه (۲) نرمال می‌شوند:

$$n_{ij} = \frac{r_{ij}}{\sqrt{\sum_{i=1}^{m} r_{ij}^2}} \ ; \ i = 1,2,\dots m \ , j = 1,2,\dots, n. \qquad (2)$$

گام ۳: ساختن ماتریس موزون نرمال‌شده. مجموعه وزن‌های W = (w1, w2, …, wn) به شرط $\sum w_i = 1$ که توسط تکنیک آنتروپی شانون مشخص شده است، به همراه ماتریس نرمال‌شده N، ماتریس موزون نرمال‌شده V را به‌صورت رابطه (۳) تشکیل می‌دهد.

$$V = W.N = [V_{ij}]_{m \times n} \qquad (3)$$

گام ۴. تعیین راه‌حل‌های ایده‌آل و ایده‌آل منفی. راه‌حل‌های ایده‌آل (A^+) و ایده‌آل منفی (A^-) به‌صورت رابطه (۴) تعریف می‌شوند.

$$A^+ = \left\{ (\max_i v_{ij} \mid j \in J), (\min_i v_{ij} \mid j \in J') \ ; \ i = 1,2,\dots,m \right\}$$
$$= \left\{ v_1^+, v_2^+, \dots, v_m^+ \right\} \qquad (4)$$

$$A^- = \left\{ \left(\min_i v_{ij} \mid j \in J\right), \left(\max_i v_{ij} \mid j \in J'\right) \quad ; \quad i = ۱,۲,\dots,m \right\}$$

$$= \left\{ v_1^-, v_2^-, \dots, v_m^- \right\}$$

$$J = \left\{ \text{j های مربوط به معیارهای مثبت} \right\} \qquad J' = \left\{ \text{j های مربوط به معیارهای منفی} \right\}$$

در این رابطه‌ها A^+ ارجح‌ترین راه‌حل (ایده‌آل) و A^- کم‌ارجح‌ترین راه‌حل (ایده‌آل منفی) را نشان می‌دهد.

گام ۵. محاسبه جداگانه فواصل. در این گام، مفهوم فاصله اقلیدسی برای اندازه‌گیری فواصل جداگانه رتبه هر گزینه از راه‌حل ایده‌آل و راه‌حل ایده‌آل منفی استفاده می‌شود. رابطه‌های (۵) و (۶) فرمول مربوطه را نشان می‌دهند.

$$s_i^+ = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^+\right)^2} \quad \text{for} \quad \text{i=1, 2, 3, ...} \tag{۵}$$

$$s_i^- = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^-\right)^2} \quad \text{for} \quad \text{j=1, 2, 3, ...} \tag{۶}$$

s_i^+ فاصله اقلیدسی رتبه گزینه i از راه‌حل ایده‌آل و s_i^- فاصله اقلیدسی رتبه گزینه i از راه‌حل ایده‌آل منفی است.

گام ۶. محاسبه ضریب نزدیکی نسبی. ضریب نزدیکی نسبی گزینه Ai با توجه به راه‌حل ایده‌آل A^+ به‌صورت رابطه (۷) تعریف می‌شود.

$$C_i = \frac{s_i^-}{s_i^- + s_i^+} \qquad (۰ \le C_i \le ۱ \quad i = ۱,۲,\dots,m) \tag{۷}$$

گام ۷. اولویت‌بندی گزینه‌ها. بهترین گزینه می‌تواند مطابق با بیشترین مقدار Ci تصمیم‌گیری شود. به این معنا که کمترین فاصله از راه‌حل ایده‌آل را دارد (یانگ و چو، ۲۰۱۵: ۶۸).

۴. یافته‌ها و تجزیه‌وتحلیل داده‌ها

با توجه به تقسیم‌بندی‌های مختلفی که برای تهدیدهای اینترنت اشیاء مورد استفاده قرار گرفته است، در این تحقیق پس از ارائه نتایج بررسی‌ها به خبرگان و انجام مصاحبه عمیق، تهدیدهای اینترنت اشیاء در پنج دسته تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها، تهدیدهای مبتنی بر نقض حریم خصوصی، تهدیدات مبتنی بر نقض امنیت اطلاعات، تهدیدهای مبتنی بر نقض امنیت شبکه و رایانش ابری و تهدیدهای مبتنی بر نقض امنیت تجهیزات دریافت هوشمند، تقسیم‌بندی شدند و مورد بررسی قرار گرفتند.

تهدیدهای یادشده فوق در میزان دانش تخصصی کارکنان جهت مقابله با تهدید، میزان خسارت وارده در صورت وقوع تهدید، میزان تأثیر تهدید بر حوزه تصمیم‌گیری، زیرساخت-های مورد نیاز جهت مقابله با تهدید، میزان تأثیر تهدید درنتیجه نبرد، میزان بازگشت‌پذیری اثر تهدید و زمان لازم جهت اثرگذاری تهدید، با یکدیگر متفاوت بوده و معیارهای قابل قبولی جهت رتبه‌بندی تهدیدها می‌باشند که با نظر خبرگان از بین معیارهای ذکرشده، پنج معیار زمان لازم جهت اثرگذاری تهدید، میزان خسارت وارده در صورت وقوع تهدید، میزان تأثیر تهدید بر حوزه تصمیم‌گیری، میزان تأثیر تهدید درنتیجه نبرد و میزان بازگشت‌پذیری اثر تهدید، انتخاب و جهت وزن‌دهی (مثبت و منفی) از طریق پرسشنامه به جامعه نمونه ارائه شد و میانگین وزن‌های داده‌شده در جدول شماره ۲ مورد استفاده قرار گرفت.

۴-۱. یافته‌های تحقیق

همان‌طور که اشاره شد در این تحقیق، پنج دسته تهدید (تهدیدهای مبتنی بر نقض حریم خصوصی کارکنان (A)، تهدیدات مبتنی بر نقض امنیت اطلاعات (B)، تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها (C)، تهدیدهای مبتنی بر نقض امنیت شبکه و رایانش ابری (D) و تهدیدهای مبتنی بر نقض امنیت تجهیزات دریافت هوشمند (E)) با پنج معیار انتخابی (زمان لازم جهت اثرگذاری تهدید (الف)، میزان خسارت وارده در صورت وقوع تهدید (ب)، میزان تأثیر تهدید بر حوزه تصمیم‌گیری (ج)، میزان تأثیر تهدید درنتیجه نبرد (د) و میزان بازگشت‌پذیری اثر تهدید (ه)) جهت رتبه‌بندی در نظر گرفته شده است.

معیارهای مذکور جهت وزن‌دهی (مثبت و منفی) از طریق پرسشنامه به جامعه نمونه ارائه شد و پس از جمع‌آوری پرسشنامه‌ها ابتدا میانگین وزن‌های داده‌شده، محاسبه گردید که در جدول شماره ۲ قابل مشاهده است. همان‌طور که از جدول ۲ مشخص است، معیارها به دو دسته مثبت و منفی تفکیک شده است.

جدول ۲. ارزیابی هر روش با توجه به معیارها

تهدیدها	معیارها				
	– الف	+ ب	+ ج	+ د	– ه
A	۳/۲۷	۲/۱۳	۱/۱۱	۱/۲۵	۳/۸۴
B	۲/۷۱	۴/۲۳	۳/۳۵	۴/۷۲	۲/۵۳
C	۱/۷۲	۳/۲۵	۴/۶۱	۴/۱۱	۲/۱
D	۳/۸۴	۲/۵۴	۳/۵۲	۲/۷۱	۳/۷۵
E	۲/۳۲	۳/۳۴	۲/۷۶	۲/۷۱	۱/۶۳

اکنون برای به دست آوردن وزن نسبی هر معیار مطابق گام ۱ از داده‌های جدول ۲ استفاده شده است و نتایج در جدول ۳ ارائه شده است.

جدول ۳. اهمیت (وزن) نسبی معیارها

	– الف	+ ب	+ ج	+ د	– ه
wj	۰/۲۵۶	۰/۰۲۷۲	۰/۲۱۰۴	۰/۲۰۳۶	۰/۳۰۲۷
Ej	۰/۹۴۸۸	۰/۹۹۴۶	۰/۹۵۷۹	۰/۹۵۹۳	۰/۹۳۹۵
dj	۰/۰۵۱۲	۰/۰۰۵۴	۰/۰۴۲۱	۰/۰۴۰۷	۰/۰۶۰۵

بعد از محاسبه ماتریس نرمال‌شده در گام ۲ (جدول ۴)، به محاسبه ماتریس موزون نرمال‌شده مطابق با گام ۳ می‌پردازیم (جدول ۵).

جدول ۴. ماتریس نرمال‌شده

روش‌های اجرا	معیارها				
	– الف	+ ب	+ ج	+ د	– ه
A	۱/۶۶۷	۰/۶۳۸	۰/۱۶۸	۰/۲۱	۲/۲۶۸

B	۱/۱۴۵	۲/۵۱۵	۱/۵۳۱	۲/۹۹۳	۰/۹۸۵
C	۰/۴۶۱	۱/۴۸۵	۲/۸۹۹	۲/۲۶۹	۰/۶۷۸
D	۲/۲۹۹	۰/۹۰۷	۱/۶۹۱	۰/۹۸۷	۲/۱۶۳
E	۰/۸۳۹	۱/۵۶۸	۱/۰۳۹	۰/۹۸۷	۰/۴۰۹

جدول ۵. ماتریس موزون نرمال‌شده

روش‌های اجرا	معیارها				
	– الف	+ ب	+ ج	+ د	– ه
A	۰/۴۲۷	۰/۰۱۷	۰/۰۳۵	۰/۰۴۳	۰/۶۸۷
B	۰/۲۹۳	۰/۰۶۸	۰/۳۲۲	۰/۶۰۹	۰/۲۹۸
C	۰/۱۱۸	۰/۰۴	۰/۶۱	۰/۴۶۲	۰/۲۰۵
D	۰/۵۸۹	۰/۰۲۵	۰/۳۵۶	۰/۲۰۱	۰/۶۵۵
E	۰/۲۱۵	۰/۰۴۳	۰/۲۱۹	۰/۲۰۱	۰/۱۲۴

مطابق با گام ۴ راه‌حل‌های ایده‌آل مثبت و ایده‌آل منفی با استفاده از جدول ۵ به‌صورت ذیل تعریف می‌شود:

$$A^* = \left\{ \max_j v_{ij} \quad \text{for } i = ۱, ۲, \dots, n \right\} = \quad \{۰/۱۱۸, ۰/۰۶۸, ۰/۶۱, ۰/۶۰۹, ۰/۱۲۴\}$$

$$A^- = \left\{ \min_j v_{ij} \quad \text{for } i = ۱, ۲, \dots, n \right\} = \quad \{۰/۵۸۹, ۰/۰۱۷, ۰/۰۳۵, ۰/۰۴۲, ۰/۶۸۷\}$$

درنهایت برای اولویت‌بندی روش‌ها ابتدا مطابق با گام ۵ بـه محاسـبه فواصـل جداگانـه رتبه هر آلترناتیو از راه‌حل ایده‌آل و راه‌حل ایده‌آل منفی پرداخته و سپس مطابق با گام ۶ بـر اساس بیشترین مقدار ضریب نزدیکی به اولویت‌بندی روش‌ها می‌پردازیم.

جدول ۶. فاصله اقلیدسی، ضریب نزدیکی و رتبه‌بندی

روش‌های اجرا	فاصله اقلیدسی		ضریب نزدیکی	رتبه‌بندی
	Si*	Si-	Ci	
A	۱/۰۳۳	۰/۱۶۲	۰/۱۳۶	۵
B	۰/۳۷۹	۰/۸۰۳	۰/۶۷۹	۲
C	۰/۱۷۱	۰/۹۷۹	۰/۸۵۲	۱
D	۰/۸۵۸	۰/۳۵۹	۰/۲۹۵	۴

E	۰/۵۷۵	۰/۷۱۸	۰/۵۵۶	۳

همان‌طور که از جدول ۶ مشخص است، روش‌های اجرا در ستون آخر برحسب مقدار ضریب نزدیکی (Ci) بیشتر اولویت‌بندی شده است.

۲-۴. تجزیه‌وتحلیل

با توجه به میانگین وزن‌های به‌دست‌آمده از پرسشنامه، وزن نسبی معیار زمان لازم جهت اثرگذاری تهدید برابر با ۰/۲۵۶۰، وزن نسبی معیار میزان خسارت وارده در صورت وقوع تهدید برابر با ۰/۰۲۷۲، وزن نسبی معیار میزان تأثیر تهدید بر حوزه تصمیم‌گیری برابر با ۰/۲۱۰۴، وزن نسبی معیار میزان تأثیر تهدید درنتیجه نبرد برابر با ۰/۲۰۳۶ و وزن نسبی معیار میزان بازگشت‌پذیری اثر تهدید برابر با ۰/۳۰۲۷ به دست آمده است؛ بنابراین می‌توان نتیجه گرفت که معیار میزان بازگشت‌پذیری اثر تهدید با داشتن بیشترین وزن نسبی، بالاترین رتبه اهمیت را داشته و معیارهای زمان لازم جهت اثرگذاری تهدید، میزان تأثیر تهدید بر حوزه تصمیم‌گیری، میزان تأثیر تهدید درنتیجه نبرد و میزان خسارت وارده در صورت وقوع تهدید، در رتبه‌های بعدی قرار دارند.

مطابق با محاسبات انجام‌شده و نتایج ارائه‌شده در جدول ۶، فاصله تهدیدهای مبتنی بر نقض حریم خصوصی کارکنان (A) از معیارهای مثبت برابر ۱/۰۳۳ و از معیارهای منفی برابر ۰/۱۶۲ می‌باشد، فاصله تهدیدهای مبتنی بر نقض امنیت اطلاعات (B) از معیارهای مثبت برابر ۰/۳۷۹ و از معیارهای منفی برابر ۰/۸۰۳ است، فاصله تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها (C) از معیارهای مثبت برابر ۰/۱۷۱ و از معیارهای منفی برابر ۰/۹۷۹ می‌باشد، فاصله تهدیدهای مبتنی بر نقض امنیت شبکه و رایانش ابری (D) از معیارهای مثبت برابر ۰/۸۵۸ و از معیارهای منفی برابر ۰/۳۵۹ است و فاصله تهدیدهای مبتنی بر نقض امنیت تجهیزات دریافت هوشمند (E) از معیارهای مثبت برابر ۰/۵۷۵ و از معیارهای منفی برابر ۰/۷۱۸ می‌باشد.

ضریب نزدیکی که به معنی میزان دور بودن از معیارهای منفی و نزدیک بودن به معیارهای مثبت است، برای تهدیدهای مبتنی بر نقض حریم خصوصی کارکنان (A) برابر با ۰/۱۳۶، برای

تهدیدهای مبتنی بر نقض امنیت اطلاعات(B) برابر با ۰/۶۷۹، برای تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها(C) برابر با ۰/۸۵۲، برای تهدیدهای مبتنی بر نقض امنیت شبکه و رایانش ابری(D) برابر با ۰/۲۹۵ و برای تهدیدهای مبتنی بر نقض امنیت تجهیزات دریافت هوشمند(E) برابر با ۰/۵۵۶ می‌باشد؛ بنابراین از میان تهدیدهای فوق، تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها به‌صورت هم‌زمان از معیارهای منفی دورتر و به معیارهای مثبت نزدیک‌تر بوده و از نظر اهمیت بالاترین رتبه را دارا می‌باشد.

۵. نتیجه‌گیری و پیشنهادات

الف. نتیجه‌گیری

اینترنت اشیاء در حوزه نظامی به اتصال و ارتباط گسترده تجهیزات و دارایی‌های فیزیکی و کارکنان نظامی از طریق شبکه اینترنت و با بهره‌گیری از ابزارهای موجود در فناوری‌های اینترنتی (شناسه‌های فرکانس رادیویی، حسگرها، ابزارهای برقراری ارتباط ماشین با ماشین و ...) اشاره دارد، به نحوی که تعامل و همکاری این اشیاء و افراد به ارتقای بهره‌وری در بخش‌های مختلف سازمان‌های نظامی منجر شده و منشأ ایجاد تغییرات وسیعی در چگونگی نظارت و مدیریت از راه دور بر فعالیت‌های مختلف، ردیابی کالاها، مدیریت دارایی‌های فیزیکی سازمان‌ها و ... گردد. توانمندی ایجاد پیوند میان جهان فیزیکی و اینترنت و نیز سایر شبکه‌های داده، پیامدهای عمیقی در محیط نظامی داشته و موجب ارتقای کارایی بخش‌های دفاعی می‌گردد. از طرفی استفاده از اینترنت اشیاء حجم بی‌سابقه‌ای از اطلاعات را در اختیار واحدهای نظامی قرار می‌دهد که تأثیر زیادی بر نحوه عمل نیروهای نظامی در حین عملیات خواهد داشت. اگرچه استفاده از این فناوری در محیط نظامی مزایای بسیاری دارد، ولی مانند هر فناوری نوظهور دیگری، تهدیدهایی را نیز به همراه خواهد داشت که بایستی مورد توجه و بررسی قرار گرفته و بر اساس میزان اهمیت هر تهدید، راهبردهای مورد نیاز تدوین و به مرحله اجرا گذارده شود.

هدف این تحقیق بررسی و رتبه‌بندی تهدیدهای به‌کارگیری فناوری اینترنت اشیاء در محیط نظامی است. به این منظور تهدیدهای مرتبط با فناوری اینترنت اشیاء در پنج محور تهدیدهای مبتنی بر نقض حریم خصوصی کارکنان، تهدیدات مبتنی بر نقض امنیت اطلاعات، تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها، تهدیدهای مبتنی بر نقض امنیت شبکه و رایانش ابری و تهدیدهای مبتنی بر نقض امنیت تجهیزات دریافت هوشمند، دسته‌بندی گردید. همچنین با توجه به نظرات خبرگان نظامی و سایبری، از پنج معیار زمان لازم جهت اثرگذاری تهدید، میزان خسارت وارده در صورت وقوع تهدید، میزان تأثیر تهدید بر حوزه تصمیم‌گیری، میزان تأثیر تهدید درنتیجه نبرد و میزان بازگشت‌پذیری اثر تهدید، جهت رتبه‌بندی تهدیدهای مورد نظر استفاده شد و معیارهای مذکور توسط جامعه نمونه مورد سنجش و وزن‌دهی قرار گرفت. از آنجایی که بعضی از معیارها جنبه مثبت و برخی جنبه منفی دارند، تهدیدی به‌عنوان مخاطره‌آمیزترین تهدید در نظر گرفته می‌شود که از معیارهای مثبت کمترین فاصله و از معیارهای منفی بیشترین فاصله را داشته باشد.

یافته‌های این تحقیق حاکی از آن است که معیار میزان بازگشت‌پذیری اثر تهدید با داشتن بیشترین وزن نسبی، بالاترین رتبه اهمیت را دارا بوده و معیارهای زمان لازم جهت اثرگذاری تهدید، میزان تأثیر تهدید بر حوزه تصمیم‌گیری، میزان تأثیر تهدید درنتیجه نبرد و میزان خسارت وارده در صورت وقوع تهدید، از نظر اهمیت در رتبه‌های بعدی قرار دارند. همچنین در راستای پاسخ به سؤال تحقیق، تهدیدهای مرتبط با به‌کارگیری اینترنت اشیاء در محیط نظامی به ترتیب اهمیت به شرح زیر رتبه‌بندی می‌گردند:

۱. تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها (شامل: تسخیر سامانه، تخریب سامانه، دست‌کاری سامانه و تهدیدهای مرتبط با ریزتراشه‌ها).
۲. تهدیدات مبتنی بر نقض امنیت اطلاعات (شامل: حمله منع خدمات، حمله مردی در میان، حمله نصب بدافزار و حمله تزریق کد مخرب).

۳. تهدیدهای مبتنی بر نقض امنیت تجهیزات دریافت هوشمند (شامل: کشتن برچسب، شبیه‌سازی برچسب، مسیریابی برچسب، جعل برچسب، آنالیز توان برچسب، حملات فیزیکی، تهدید فروریختن گودال و ...).
۴. تهدیدهای مبتنی بر نقض امنیت شبکه و رایانش ابری (شامل: حملات فیشینگ، حمله دسترسی، حمله جابه‌جایی داده‌ها، سرقت اطلاعات، نابودی اطلاعات، تسخیر اطلاعات و...).
۵. تهدیدهای مبتنی بر نقض حریم خصوصی کارکنان (شامل: تهدیدهای پیش‌بینی اقدام، تهدیدهای ترجیحی، تهدیدهای مکان‌یابی، تهدیدهای نظارت بر تراکنش و تهدیدهای ردیابی دیجیتالی).

با توجه به نتایج فوق، در سازمان‌های نظامی از میان تهدیدهای فناوری اینترنت اشیاء، تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها به دلایل زیر از اهمیت بیشتری برخوردار می‌باشند: به زمان کمتری جهت اثرگذاری نیاز دارند، تأثیرهای به‌جامانده از آن‌ها به میزان کمتری قابل بازگشت است، تأثیر بیشتری بر حوزه تصمیم‌گیری دارند، خسارت‌های بیشتری به تجهیزات اینترنت اشیاء وارد می‌نمایند و تأثیر بیشتری درنتیجه نبرد خواهند داشت.

ب. پیشنهادها

با توجه به روند رو به رشد فناوری اینترنت اشیاء و نفوذ این فناوری در بخش‌های مختلف نظامی، پیشنهاد می‌گردد:

الف. محققین محترم در حوزه نظامی، با در نظر گرفتن نتایج حاصل از این تحقیق، نسبت به ارائه راه‌کار مناسب در راستای مقابله با این تهدیدهای برشمرده‌شده اقدام نمایند.

ب. با توجه به اینکه برابر نتایج به‌دست‌آمده در این تحقیق تهدیدهای مبتنی بر عملکرد ریزپردازنده‌ها، بالاترین رتبه را در بین تهدیدها کسب نموده است، مدیران و

فرماندهان محترم در وزارت دفاع و پشتیبانی نیروهای مسلح نسبت به ایجاد زیرساخت‌های مورد نیاز جهت تست و بررسی ریزپردازنده‌های مورد استفاده در سامانه‌های نظامی اقدام نمایند.

فهرست منابع ومآخذ

الف. منابع فارسی

- پرستش، مریم (۱۳۹۵)، دیوار شیشه‌ای IoT، تهران، ماهنامه خبری، تحلیلی، آموزشی، پژوهشی، اطلاع‌رسانی طیف برق، سال ۱۱، شماره ۵۵، ص ۱۴.
- تاج، نسرین؛ ترکمن، عاطفه و معدنی، افسانه (۱۳۹۶)، طبقه‌بندی موضوعات اینترنت اشیاء و درجه‌بندی حساسیت آن‌ها، تهران، پژوهشگاه ارتباطات و فناوری اطلاعات وزارت ارتباطات و فناوری اطلاعات.
- عطاریان، آیه (۱۳۹۵)، پارادایم امنیت در پلتفرم اینترنت اشیاء، تهران، ششمین همایش پژوهش‌های نوین در علوم و فناوری، صص ۱۱-۷.
- فضل‌علی، پویا (۱۳۹۵)، نُه تهدید امنیتی رایج رایانش ابری، روزنامه همشهری، ویژه‌نامه هفته پدافند غیرعامل، صص ۵۳- ۵۰.
- کاشیپور، میثم (۱۳۹۴)، دیده‌بانی و رصد تهدیدها و فرصت‌های موجود در شکاف‌های عملکردی ریزتراشه‌ها و بهره‌برداری از آن در جنگ‌های اطلاعاتی آینده، تهران، مرکز آینده‌پژوهی علوم و فناوری دفاعی مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، چاپ دوم.
- معاونت علمی و فناوری ریاست جمهوری، بدون نویسنده (۱۳۹۵)، گزارش شماره ۱: از سلسله مطالعات برنامه ملی آینده‌نگاری در حوزه فناوری اطلاعات و ارتباطات اینترنت اشیاء و چگونگی ارزش‌آفرینی آن از نگاه مؤسسه جهانی مکنزی، دبیرخانه برنامه ملی آینده‌نگاری علم و فناوری در حوزه فناوری اطلاعات و ارتباطات، صص ۴-۳.
- معاونت علمی و فناوری ریاست جمهوری، بدون نویسنده (۱۳۹۵)، گزارش شماره ۳: اینترنت اشیاء و چگونگی ارزش‌آفرینی آن از نگاه مؤسسه جهانی مکنزی، دبیرخانه برنامه ملی آینده‌نگاری علم و فناوری.
- یزدان‌پناه، حمیدرضا و حسنی آهنگر، محمدرضا (۱۳۹۵)، اینترنت اشیاء: کاربردها، فناوری‌ها و چالش‌های مورد بحث، تهران، هشتمین کنفرانس بین‌المللی فناوری اطلاعات و دانش، صص ۷-۶.

ب. منابع لاتین

- AbdulGhani, H.; Konstantas D. & Mahyoub M. (2018). "A comprehensive iot attacks survey based on a building-blocked reference model," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 9, no. 3, 2018
- Applegate, S. (2016). The principle of maneuver in cyber operations. 4th International Conference on Cyber Conflict (CYCON), pp. 1–13.

- APWG, (2017). Phishing Activity Trends Report. Retrieved From https://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf//, online; accessed 12 Feburary 2019.
- Arashi, R.; Pedersen, L.& Hillock, A. (2017). Defense Policy and the Internet of Things. Disrupting Global Cyber Defenses, Deloitte Group.
- Basak, A. (2017). Security Assurance for System-on-Chip Designs With Untrusted IPs, IEEE Trans. Information Forensics and Security, 1515-1528, June-2017.
- Butun, I.; Österberg, P. & Song. H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. IEEE Communications Surveys Tutorials 22, 1 (2020), 616–644.
- Chu, T. & Lin Y., (2013). A Fuzzy TOPSIS Method for Robot Selection. Int J Adv Manuf Technol 21:284–290.
- Hassan Q.F.; Rehman Khan, A. & Madani, S. (2018). Internet of Things Challenges, Advances, and Applications. CRC Press, Taylor & Francis Group, p. 4.
- Husamuddin, M. & Qayyu, M. (2018). Internet of Things: A study on Security and Privacy Threats. In Second International Conference on Anti-Cyber Crimes (ICACC), 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7905270 [March 26, 2018].
- Hwang, C. & Yoon, K. (2015), multiple attribute decision making: methods and applications. Springer, Berlin Heidelberg New York.
- Word Forum On Internet Of Things, (2018). "MILITARY APPLICATIONS OF IOT". RETRIEVED FROM http://wfiot2018.iot.ieee.org/sps2-military-applications-iot/
- Kumar, S.; Sahoo, S.; Mahapatra, A. & Swain, A.K (2017). Security enhancements to system on chip devices for iot perception layer. in 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS). IEEE, 2017, pp. 151–156.
- Liao, C.; Shuai, H. & Wang, L. (2018). Eavesdropping prevention for heterogeneous internet of things systems. in 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2018, pp. 1–2.
- Masoodi, F.; Alam, S. & Siddiqui S.T. (2019). SECURITY& PRIVACY THREATS, ATTACKS AND COUNTERMEASURES IN INTERNET OF THINGS. International Journal of Network Security & Its Applications (IJNSA) Vol. 11, No.2, March 2019, P. 67-77.
- Misra, S.; Maheswaran, M. & Hashmi, S. (2017). "Security Challenges and Approaches in Internet of Things". Springer International Publishing AG Switzerland. (pp. 25-38)
- Raju, K. & Bapauji, V. (2016). Internet of Things (IoT): Security and privacy threats. In IEEE International Conference Robot Autom, 2016. [Online]. Available: https://www.researchgate.net/publication/305302451 [March 26, 2018] P. 1-13.
- RTO Task Group, (2015). "Military Applications Of Internet Of Things (IST-147)". Contact STO/CSO Panel Office, P 2, Retrieved From https://www.cso.nato.int/activity_meta.asp.

- Staalduinen, M. & van, J. (2019). THE IoT SECURITY LANDSCAPE. Cyber Security Agency of Singapore, Ministry of Economic Affairs and Climate Policy of the Netherlands.
- Tasneem, Y.; Rwan, M.; Fadi, A. & Imran (2015). Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures. International Journal for Information Security Research (IJISR), Volume 5, Issue 4, P. 47-55.
- Tripathy B.K. & Anuradha J. (2018) INTERNET OF THINGS (IoT) Technologies, Applications, Challenges, and Solutions. CRC Press, Taylor & Francis Group. P. 78
- Tweneboah, K.S.; Skouby, K.E. & Tadayoni R. (2017). Cyber Security Threats to IoT Applications and Service Domains. Wireless Personal Communications Journal, Volume 94, Number 4, June 2017, ISSN 0929-6212, DOI 10.1007/s11277-017-4434-6.
- U.S. Department of Defense, (2016). Policy Recommendations for The Internet of Things (IoT). Chief Information Officer.
- Venkata R. (2017). Decision making in the manufacturing environment: using graph theory and fuzzy multiple attribute decision making methods. (Springer series in advanced manufacturing), Springer.
- Waheed, N.; He, X.; Ikram, M.; Hashmi, S. & Usman, M. (2020). Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures. ACM Comput. Surv., Vol. 53, No. 3, Article 1 (April 2020), P. 35-51.
- Yang, T. & Chou, P. (2015). solving a multiresponse simulation–optimization problem with discrete variables using a multi-attribute decision-making method, Mathematics and Computers in Simulation.