فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)
سال بیست و یکم: شماره ۷۹- پاییز ۱۴۰۱
صص: ۱۷۱ - ۲۰۷

Amniat Pajouhi: Security Research Quarterly
Vol.21, No.79,Autumn 2022
P-P: 171 - 207

اینترنت اشیا و سازمان‌های امنیتی

جمشید نصرت‌آبادی[۱]
احمد زوار تربتی [۲]
ابراهیم نصیری اردلی[۳]

چکیده:

فنّاوری اینترنت اشیا یکی از فنّاوری‌های نو در عصر کنونی است که امکان ارسال و دریافت داده‌ها بین اشیا از طریق شبکه‌های ارتباطی را فراهم نموده و منشأ ایجاد تغییرات شگرفی در حوزه‌های مختلف ازجمله حوزه امنیتی است؛ به‌گونه‌ای که افزایش بهره‌وری و راحتی را برای افراد و سازمان‌ها در پی خواهد داشت. فراگیرشدن اینترنت اشیا اجتناب‌ناپذیر است؛ اما بهره‌گیری از این فنّاوری در کنار مزایا و فرصت‌های بسیاری که برای سازمان‌های امنیتی خواهد داشت، تهدیدهایی را نیز به همراه دارد. درنتیجه شناسایی تهدیدهای ناشی از این فنّاوری نوظهور و راه‌کارهای مقابله‌ای، موضوعی بسیار حیاتی و قابل‌مطالعه است. در این پژوهش کاربردی که با روش آمیخته (کمّی- کیفی) انجام‌شده، ضمن معرفی فنّاوری اینترنت اشیا، ابتدا فرصت‌ها و تهدیدات مختلفی که سازمان‌های امنیتی در به‌کارگیری این فنّاوری با آن مواجه هستند، جمع‌بندی شد و در ادامه، راه‌کارهای مقابله با تهدیدات به‌کارگیری فنّاوری اینترنت اشیا به دودسته سازوکارهای مدیریتی و فنّاورانه تقسیم شدند و درمجموع، ۹۸ مؤلفه در قالب یک پرسش‌نامه محقق‌ساخته استخراج شد که فرصت‌ها، ۲۲ مؤلفه، تهدیدات ۲۵ مؤلفه و راه‌کارهای مقابله‌ای مدیریتی و فنّاورانه نیز به ترتیب ۱۶ و ۳۵ مؤلفه را به خود اختصاص دادند. اطلاعات از طریق مصاحبه، پرسش‌نامه، اسناد و مدارک، منابع الکترونیکی و وبگاه‌های معتبر علمی و نیز از دو روش کتابخانه‌ای و میدانی جمع‌آوری گردیده است. نتایج تجزیه‌وتحلیل سؤالات پژوهشی نشان‌داد که پرسش‌شوندگان معتقدند ۸۲% فرصت‌های اینترنت اشیا، ۸۴% تهدیدات اینترنت اشیا، ۸۸% راه‌کارهای مقابله‌ای مدیریتی و ۸۸% راه‌کارهای مقابله‌ای فنّاورانه استخراج‌شده، در حد زیاد و خیلی زیاد بر به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی مؤثر است. هرکدام از فرضیه‌های پژوهشی نیز با استفاده از آزمون خی‌دو مورد تجزیه‌وتحلیل قرار گرفتند و با استفاده از آزمون فریدمن، مشخص شد که مؤلفه "کاهش هزینه‌های عملیاتی" با اولویت‌ترین فرصت و مؤلفه "ناتوانی و عقب‌ماندگی در تقابل با سرویس‌های امنیتی حریف که از فنّاوری بهره می‌برند". با

۱. دکتری مدیریت راهبردی فضای سایبر و استادیار دانشکده علوم فنون فارابی (نویسنده مسئول) *nosratabadi110@chmail.com*
۲. دکتری برق-مخابرات سیستم، پژوهشگر و مدرس دانشکده علوم و فنون فارابی *zavvarahmad@gmail.com*
۳. دانش‌آموخته کارشناسی ارشد اطلاعات و حفاظت اطلاعات دانشکده علوم فنون فارابی *ardali378@chmail.ir*

اولویت‌ترین تهدید و مؤلفه "افزایش حمایت‌های مسئولان سازمان" با اولویت‌ترین راه‌کار مقابله‌ای مدیریتی و مؤلفه "رصد پیشرفت فنّاوری‌ها و تأمین، طراحی و استفاده از نرم‌افزار، سخت‌افزار و تجهیزات پیشرفته و جدید اینترنت اشیا" با اولویت‌ترین راه‌کار مقابله‌ای فنّاورانه در به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی هستند.

واژگان کلیدی: اینترنت اشیا، سازمان‌های امنیتی، فرصت‌ها، تهدیدات، راه‌کارهای مقابله.

جستارگشایی

ظهور اینترنت تحولی بزرگ در جهان ایجاد کرد و با توجه به میزان استقبال مردم از آن، فعالان حوزه فنّاوری و فنّاوری به فکر استفاده از اینترنت در بخش‌های مختلف زندگی مردم افتادند (سهرابی و همکاران، ۱۳۹۹). دسترسی راحت و ارزان به اینترنت و توسعه قابلیت‌های شبکه و اشیا همانند اشیا هوشمند باعث ایجاد پیوند بین اینترنت و اشیا شده است که امروزه به‌عنوان اینترنت اشیا شناخته می‌شود (طهماسبی لیمونی و همکاران، ۱۳۹۸). به زبان ساده اینترنت اشیا، ارتباط حسگرها و دستگاه‌ها با شبکه‌ای است که از طریق آن می‌توانند با یکدیگر و با کاربرانشان تعامل کنند (خدابنده و همکاران، ۱۳۹۸). حالا دیگر بیش از یک دهه است که این تنها انسان‌ها نیستند که از طریق اینترنت با یکدیگر تعامل دارند؛ بلکه مفاهیم جدیدی شکل گرفته و محصولات هوشمندی به بازار راه پیدا کرده‌اند که از طریق فنّاوری اشیا، با یکدیگر و همچنین با انسان‌ها ارتباط برقرار می‌کنند (سهرابی و همکاران، ۱۳۹۹). مؤسسه آینده‌پژوهی گارتنر،۱۰ پیش‌بینی خود از نوآوری در دنیای فنّاوری طی سال‌های آینده تا ۲۰۲۲ را اعلام کرده که در این میان اینترنت اشیا در دگرگون کردن دنیای فنّاوری نقش بسزایی ایفا خواهد کرد (لک، ۱۳۹۹)؛ ازاین‌رو با توجه به بند ۳ سیاست‌های کلی خودکفایی دفاعی و امنیتی ابلاغی مقام معظم رهبری (مدظله‌العالی) مبنی بر دستیابی به فنّاوری‌های برتر موردنیاز دفاعی و امنیتی به نظر می‌رسد اینترنت اشیا به‌عنوان یکی از فنّاوری‌های برتر تأثیرگذار در حوزه دفاعی- امنیتی می‌تواند در جهت ارتقای توان رزمی و اطلاعاتی-امنیتی تأثیرگذار باشد (غلام‌نژاد و همکاران، ۱۳۹۸).

اینترنت اشیا با ترکیب دو عرصه دیجیتالی و فیزیکی دسترسی به فنّاوری اطلاعات را گسترده‌تر می‌سازد. امکانات بی‌شمار فراهم‌شده به کمک توانمندی نظارت و کنترل اشیا، موج جدیدی از نوآوری‌ها را ارائه خواهد نمود. اینترنت اشیا 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 فنّاوری ریاست جمهوری ۳ :۱۳۹۵).

این فنّاوری، پتانسیل ایجاد نوآوری در هر یک از حوزه‌ها ازجمله کسب‌وکارهای نوپدید و بازاریابی و... و حتی کارکردهای امنیتی را دارد، بنابراین نیاز است در آینده به‌منظور بالفعل شدن کاربردهای اینترنت اشیا از بین عناصر دخیل در توفیق سازمان‌های امنیتی روی آموزش عناصر نیروی انسانی در این زمینه، تخصیص بودجه و مکان مناسب، استفاده فیزیکی از آن در عملیات‌ها مانند تعقیب و مراقبت و... سرمایه‌گذاری کیفی بیشتری صورت گیرد و با پژوهش بر روی سازوکارهای امنیتی آن به بهبود و رفع نگرانی‌های امنیتی دست‌یافت (کریمی قهرودی و همکاران، ۸۳ :۱۳۹۴).

بی‌شک ورود اینترنت اشیا در عرصه امور دفاعی و نظامی نیز قابلیت‌های جدید و شگرفی را در اختیار این بخش‌ها قرار خواهد داد. بهره‌گیری از این فنّاوری نوین به یگان‌های امنیتی فرصت خواهد داد تا از ظرفیت حسگرهای بسیار کم‌هزینه، متنوع و کنترل‌پذیر در نظارت مستمر بر صحنه عملیات، نظارت بر محیط پیرامونی، نظارت بر سلامت و امنیت تجهیزات و کارکنان و کنترل ساختمان‌ها بهره گرفته و علاوه بر کاهش نیروی انسانی موردنیاز، به برتری اطلاعاتی نیز دست یابند (رمضانی و همکاران، ۱۴۰۰).

اما نکته قابل‌توجه این‌که فنّاوری‌های جدید، نظیر فنّاوری اینترنت اشیا، به علت ماهیت جذاب و نوآورانه خود بدون توجه به تهدیدهای آشکار و پنهان این فضا، موردپذیرش عمومی قرار خواهند گرفت. این پذیرش عمومی و گسترده موجب بروز چالش‌های هویتی، فرهنگی، سیاسی و اقتصادی خواهد شد و احتمال بروز چالش‌های امنیتی را در پی خواهد داشت. در عصر سایبر با درهم‌تنیده شدن گستره زندگی و فنّاوری‌های غیربومی تهدیدهای نوینی متوجه سازمان‌ها به‌ویژه سازمان‌های امنیتی و درنهایت امنیت ملی خواهد شد. ازآنجایی‌که این فنّاوری‌ها عموماً بومی نبوده و متعلق به کشورهای متخاصم و یا هم‌پیمانان آن‌ها است، چالش‌هایی را متوجه سازمان‌های امنیتی و امنیت ملی خواهد کرد (کریمی قهرودی و همکاران، ۸۳ :۱۳۹۴). انفجار سریع اینترنت اشیا به نفع سازمان‌ها بوده؛ بااین‌حال چنین انفجار کنترل نشده‌ای باعث افزایش چالش‌های حریم خصوصی و امنیتی شده به‌طوری‌که موضوع امنیت و محرمانگی آن توجه زیادی را به سمت خود جلب کرده و به موضوعی بحث‌برانگیز در این حوزه مبدل شده است. بیشتر متخصصان امنیت اینترنت اشیا را به دلیل ضعف پروتکل‌ها و سیاست‌های امنیتی، نقطه آسیب‌پذیر حملات سایبری می‌دانند. چالش‌های موجود در اینترنت اشیا مانند کلان‌داده، حریم خصوصی، محرمانگی، اعتبار، یکپارچگی و کسب سایر دسترسی‌های غیرمجاز و... بوده که امکان بهره‌برداری و اشراف اطلاعاتی دشمن بر تعاملات اجتماعی را برای سازمان‌های اطلاعاتی و امنیتی فراهم می‌سازد (کریمی قهرودی و همکاران، ۸۳ :۱۳۹۴). به‌کارگیری فنّاوری اینترنت اشیا در محیط اطلاعاتی– امنیتی بدون توجه به تهدیداتی که به‌کارگیری این فنّاوری می‌تواند به همراه داشته باشد موجب غفلت راهبردی نیروهای امنیتی خواهد شد. ازآنجاکه نوع، میزان اهمیت و تأثیرگذاری تهدیدهای اینترنت اشیا برای سازمان‌های مختل متفاوت است؛ درنتیجه پیش از به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی

بایستی نسبت به شناسایی و تعیین میزان تأثیر تهدیدهای به‌کارگیری این فنّاوری اقدام نموده و بر اساس مهم‌ترین و با اولویت‌ترین تهدیدها، راهبردهای موردنیاز تدوین گردد. رتبه‌بندی تهدیدها از جهت مشخص نمودن شیوه، سطح و راهبردهای به‌کارگیری فنّاوری اینترنت اشیا در محیط اطلاعاتی- امنیتی 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 واقع‌شده یا به میزان لازم موردتوجه قرار نگیرند (رمضانی و همکاران، ۱۴۰۰).

ورود و به‌کارگیری همه‌جانبهٔ فنّاوری اینترنت اشیا در سازمان‌های امنیتی، می‌تواند موجب تغییرات کمی و کیفی در انجام مأموریت‌ها شود؛ اما پذیرش یک فنّاوری در یک سازمان و فاصله‌گرفتن از بسیاری از روش‌های سنتی و رو آوردن به روش‌های جدید متناسب با ظرفیت‌های ناشی از ورود فنّاوری به عوامل زیادی بستگی دارد. بایستی بررسی شود که اگر از ورود فنّاوری جلوگیری شود، چه پیامدها و تهدیداتی متوجه سازمان خواهد شد و درواقع جنبه‌های جبری استفاده از فنّاوری چه هستند و آیا مزایای استفاده از فنّاوری بر چالش‌ها و تهدیدات ناشی از استفاده از آن برتری دارند یا خیر؛ بنابراین مسائلی از قبیل استفاده از مزایای و فرصت‌های ناشی از به‌کارگیری فنّاوری، جلوگیری از عقب‌ماندگی ناشی از استفاده نکردن از فنّاوری، سازمان‌ها را ملزم می‌کند که از این فنّاوری نوظهور استفاده کنند؛ اما باید دانست که استفاده از فنّاوری‌های نو، نظیر اینترنت اشیا، دو وجه دارد و بسته به این‌که خودی یا دشمن از این فنّاوری استفاده کند، چالش‌ها و تهدیدات متفاوتی مطرح هستند؛ یعنی یک‌مرتبه بایستی در مقام استفاده‌کننده از فنّاوری، فرصت‌ها و تهدیدات را بررسی نمود و بار دیگر بایستی با این نگاه که فنّاوری در اختیار دشمن است به موضوع پرداخت.

بررسی‌های انجام‌شده نشان می‌دهد که تاکنون به‌صورت منسجم و هدفمند "فرصت‌ها، تهدیدات و راه‌کارهای مقابله‌ای به‌کارگیری اینترنت اشیا در سازمان‌های امنیتی" ارائه نشده است. از طرفی نیز، اشراف ناقص و مبهم بودن مفهوم اینترنت اشیا، مانند هر فنّاوری دیگری می‌تواند سبب ایجاد درک ناصحیح از این فنّاوری شود که در تصمیم‌سازی مدیران مؤثر واقع می‌گردد؛ بنابراین می‌توان مدعی شد با بررسی دقیق تمام ابعاد فنّاوری، می‌توان مدیران سازمانی را در زمینهٔ تصمیم‌گیری برای به‌کارگیری و یا به کار نگرفتن این فنّاوری یاری رساند؛ ازاین‌رو در این پژوهش، ضمن معرفی فنّاوری اینترنت اشیا و بررسی و دسته‌بندی تهدیدات به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی، راه‌کارهای متناظر مطرح و اولویت‌بندی خواهند شد و می‌توان گفت که پیامدهای ناشی از انجام این پژوهش عبارتند از:

- آشنایی با کاربردهای فنّاوری اینترنت اشیا در سازمان‌های امنیتی.
- تبیین ملاحظات به‌کارگیری تجهیزات اینترنت اشیا در عملیات‌های پنهان.
- شناسایی و تعریف بهینه نیازمندی‌های پژوهشی سازمان‌های امنیتی درزمینهٔ تأمین تجهیزات و سامانه‌های مبتنی بر اینترنت اشیا.

- ایجاد آمادگی و مقدمات (مدیریت و فنّاورانه) سازمان‌های امنیتی برای پیاده‌سازی و یا استفاده از سامانه‌های مبتنی بر اینترنت اشیا.
- آشنایی با ماهیت فنّاوری اینترنت اشیا و شناسایی مزایا و فرصت‌های مدیریتی، فنّاورانه ناشی از به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی.
- شناسایی و اولویت‌بندی معایب، خلأها، تهدیدات مدیریتی و فنّاورانه به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی.
- تبیین ملاحظات و ارائه راه‌کارهای مدیریتی و فنّاورانه برای به‌کارگیری بهینه فنّاوری اینترنت اشیا در سازمان‌های امنیتی و همچنین تعیین اولویت‌های عملکردی.

اما واقعیت این است که امروزه محیط پیرامونی سازمان‌ها، متناسب با تغییراتِ سریعِ فنّاوری اطلاعات و ارتباطات، در حال تغییر است و سازمان‌هایی می‌توانند به حیات و حرکت روبه‌جلوی خود ادامه دهند که سازوکارهای لازم را برای رویارویی با این تغییرات دارا باشند. انتقال اطلاعات در بستر اینترنت جهانی در فنّاوری اینترنت اشیا و استفاده از تجهیزات و سامانه‌های غیربومی موجب می‌شود تا تهدیدات و آسیب‌پذیری‌های بیشتری داشته و هدفی جذاب برای مهاجمان باشد. درصورتی‌که کاربران خصوصی و سازمان‌ها با لحاظ‌نمودن سازوکارهایی بتوانند اطمینان حاصل نمایند که اطلاعات آن‌ها در محیطی منتقل می‌شود که امکان ازبین‌رفتن آن و دسترسی غیرمجاز کاربران و حتی فروشندگان خدمات اینترنت اشیا به داده‌ها وجود ندارد، قطعاً استقبال بیشتری از این فنّاوری خواهند داشت. شناسایی تهدیدات به‌کارگیری فنّاوری نوظهور در سازمان‌ها و پیش‌بینی راه‌کارهای مقابله‌ای می‌تواند در کنار بهره‌برداری حداکثری از مزایا، آسیب‌پذیری را به حداقل برساند. عدم انجام این پژوهش، تبعات مشروحه زیر را در پی خواهد داشت:

- درزمینهٔ به‌کارگیری فنّاوری نوظهور اینترنت اشیا، درک لازم برای مدیران تصمیم‌گیر در سازمان‌های امنیتی ایجاد نخواهد شد و به‌تبع آن در آینده عقب‌ماندگی و غافلگیری رخ خواهد داد.
- عدم آشنایی با تهدیدات ناشی از استفاده دشمن از فنّاوری اینترنت اشیا در مأموریت‌های امنیتی که به‌تبع آن پیش‌بینی راه‌کارهای مقابله‌ای رخ نخواهد داد.
- عدم شناسایی و تبیین فرصت‌ها، چالش‌ها و تهدیدات مدیریتی، فنّاورانه و امنیتی – عملیاتی به‌کارگیری فنّاوری اینترنت اشیا.
- مغفول واقع‌شدن الزامات امنیتی و کنترلِ امنیتی در مراحل پیاده‌سازی و بهره‌برداری از فنّاوری اینترنت اشیا، در آیین‌نامه‌ها و شیوه‌نامه‌های مربوطه.

موارد یادشده بر ضرورت این پژوهش دلالت می‌کنند؛ ازاین‌رو "تبیین فرصت‌ها، تهدیدات و راه‌کارهای

مقابله‌ای به‌کارگیری اینترنت اشیا در سازمان‌های امنیتی" به‌عنوان هدف اصلی این پژوهش مطرح گردیده و فرض شده که راه‌کارهای مدیریتی و فنّاورانه، می‌توانند در به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی مؤثر باشند و تلاش شده با بهره‌گیری از تجارب علمی داخلی و خارجی و در چارچوب نظریه‌ها و الگوهای مرجع اینترنت اشیا، با در نظر داشتن اسناد بالادستی کشور و سازمان‌های امنیتی در حوزه فنّاوری اطلاعات و ارتباطات، به اهداف فرعی بدین شرح پرداخته شود: ۱- احصاء فرصت‌های به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی. ۲- احصاء تهدیدات به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی. ۲- تعیین راه‌کارهای مدیریتی به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی. ۳-تعیین راه‌کارهای فنّاورانه به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی. در رابطه با اهداف فرعی نیز فرض شده ۱- مهم‌ترین فرصت‌های به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی عبارتند از کاهش هزینه‌های عملیاتی، ارتقای توان عملیاتی در مأموریت‌ها و افزایش بهره‌وری، آشنایی با شیوه و شگردهای حریف مبتنی بر فنّاوری اینترنت اشیا، مدیریت هوشمندانه محیط عملیاتی، کنترل از راه دور تجهیزات و سامانه‌ها و ...۲- مهم‌ترین تهدیدات به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی عبارتند از ناتوانی و عقب‌ماندگی در تقابل با سرویس‌های امنیتی حریف که از فنّاوری بهره می‌برند، عقب‌ماندگی از سازمان‌های اطلاعاتی رقیب داخلی و عدم بهره‌برداری از مزیت‌های رقابتی ناشی از فنّاوری، تهدیدات ناشی از استفاده دشمن از فنّاوری اینترنت اشیا در فرآیند جاسوسی. وابستگی به فنّاوری و غفلت و فراموشی روش‌های غیر وابسته به فنّاوری و دیگر روش‌های خلاقانه و ... و ۳- راه‌کارهای مدیریتی به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی عبارتند از افزایش حمایت‌های مسئولان سازمان در خصوص به‌کارگیری فنّاوری اینترنت اشیا، تأمین اعتبارات مالی موردنیاز برای راه‌اندازی، توسعه، پشتیبانی و امن‌سازی فنّاوری اینترنت اشیا سازمان‌های امنیتی، تدوین، ابلاغ و اعمال مستمر سیاست‌های امنیتی (طبقه‌بندی داده‌ها و سطوح دسترسی و...)، ایجاد ساختار مناسب و جذب نیروی انسانی متخصص برای راه‌اندازی، توسعه، پشتیبانی، امنیت و کنترل امنیت فنّاوری اینترنت اشیا و...۴- راه‌کارهای فنّاورانه در به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی عبارتند از رصد پیشرفت فنّاوری‌ها و تأمین، طراحی و استفاده از نرم‌افزار، سخت‌افزار و تجهیزات پیشرفته و جدید اینترنت اشیا، تأمین زیرساخت‌ها، سامانه‌های امنیتی، سامانه‌های کنترلی و ... برای پیاده‌سازی و امن‌سازی فنّاوری اینترنت اشیا، بررسی توانمندی‌ها و رویکردهای سازمان‌های اطلاعاتی- امنیتی حریف در حوزه به‌کارگیری فنّاوری اینترنت اشیا، راه‌اندازی آزمایشگاه ارزیابی امنیتی سخت‌افزارها، نرم‌افزارها و آزمون نفوذ به شبکه‌های ارتباطی و استخراج آسیب‌پذیری‌ها و...

برابر بررسی‌های انجام‌گرفته از طریق مراجعه به آثار مکتوب اعم از کتاب‌ها، مقاله‌های علمی و منابع

الکترونیکی و وبگاه‌های معتبر علمی، پژوهشی درزمینهٔ "تبیین فرصت‌ها، تهدیدات و راه‌کارهای مقابله‌ای به‌کارگیری اینترنت اشیا در سازمان‌های امنیتی" صورت نپذیرفته است ولی در پژوهش‌های متعددی، موضوعات مرتبط با فنّاوری اینترنت اشیا مطرح شده است که ابر موضوعی پیرامون این فنّاوری بدین‌صورت است:

- در برخی از مقالات به موضوع **به‌کارگیری و پیاده‌سازی فنّاوری اینترنت اشیا** پرداخته شده است؛ به‌عنوان‌مثال باقری‌منش و همکاران در پژوهشی امکان‌سنجی پیاده‌سازی فنّاوری اینترنت اشیا در آماد یک سازمان دفاعی را بررسی کرده‌اند (باقری‌منش و همکاران، ۱۳۹۸). لک نیز به راهبردهای به‌کارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی پرداخته است که نتیجه این پژوهش نشان‌داد راهبرد مناسب به‌کارگیری اینترنت اشیا در پلیس آگاهی راهبرد محافظه‌کارانه است (لک، ۱۳۹۹). زرگر نیز در پژوهشی موانع استقرار اینترنت اشیا در کتابخانه‌های ایران را ارزیابی کرده و نتایج به‌دست‌آمده از تلاش وی نشان‌داد که برای استقرار اینترنت اشیا در کتابخانه‌های ایران، مانع امنیت در رتبه اول و موانع زیرساخت، مالی و انسانی به ترتیب، در رتبه‌های بعدی قراردارند (زرگر، ۱۳۹۸-۱۳۷۱ :۱۳۹۸).
- در برخی مقالات نیز به **کاربردهای فنّاوری اینترنت اشیا** بیشتر توجه شده است. مثلاً خاقانی‌فرد و همکارش در پژوهشی به هوشمندسازی خانه‌ها با استفاده از فنّاوری اینترنت اشیا پرداخته و امنیت درب و اطفاء حریق از طریق حسگرها و عملگرهای مختلفی را بررسی نموده‌اند (خاقانی‌فرد و همکاران، ۱۴۰۰). بهرامی زنوز و همکارانش در پژوهش خود به شناسایی و اولویت‌بندی عوامل مؤثر بر کاربرد اینترنت اشیا در دولت باز پرداختند و نتیجه پژوهش آن‌ها نشان‌داد که دسته فنی و عامل‌های تأمین زیرساخت، تدوین استانداردها، تنظیم قوانین و مقررات، تأمین نیروی متخصص و حفظ امنیت داده‌ها به ترتیب از بیشترین اولویت برخوردار می‌باشند (بهرامی زنوز و همکاران، ۱۳۹۹). غلام‌نژاد و همکاران در پژوهشی به بررسی مسیرهای ایجاد بستر لازم برای بهره‌برداری از فنّاوری اینترنت اشیا در مأموریت‌های نیروی هوایی ارتش جمهوری اسلامی ایران پرداختند که مهم‌ترین دستاورد این مقاله کمک به شناخت فنّاوری اینترنت اشیا و استفاده از آن در بخش‌های مختلف نظامی و محیط‌های جنگی ذکر شده است (غلام‌نژاد و همکاران، ۱۳۹۸). قهرمان‌خانی و همکارش در کار خود به توصیف اینترنت اشیا، ساختار و سبک‌های آن پرداختند و کاربردها و چالش‌های مهم این فنّاوری را موردبررسی قراردادند (قهرمان‌خانی و همکاران، ۲۰۱۶). اسماعیل‌پور و همکاران نیز در پژوهشی با اعمال اصول شبکه‌های اجتماعی به اینترنت اشیا و با در نظر گرفتن بازاریابی در شبکه‌های اجتماعی انسانی، تأثیری که اینترنت اشیا می‌تواند در بازاریابی‌های اینترنتی و هوشمند کردن آن بگذارد را بررسی کردند (اسمعیل‌پور و همکاران، ۲۰۱۶).

در برخی مقالات به فنّاوری‌های **توانمندساز و مرتبط با اینترنت اشیا** توجه شده است. به‌عنوان‌مثال

علایی و همکاران به فنّاوری داده‌کاوی پرداخته‌اند و برای مدیریت داده‌های خانه‌های هوشمند مبتنی بر اینترنت اشیا با بهره برده از فن‌های داده‌کاوی، با یک جست‌وجوی آگاه از متن به انتخاب و رتبه‌بندی حسگرها پرداختند (علایی و همکاران، ۱۳۹۶). پورشایسته فرد و همکاران در پژوهشی به فنّاوری بلاک‌چین پرداختند و امنیت در اینترنت اشیا با استفاده از راه‌کارهای فنّاوری بلاک چین را بررسی کردند (پورشایسته فرد و همکاران، ۱۳۹۶). اکراقلی‌پور و همکاران در مقاله خود ظهور و رشد کلان داده‌ها در رایانش ابری و اینترنت اشیا و چالش‌های به‌کارگیری این ترکیب را از جنبه‌های گوناگون موردبحث و بررسی قرار داده‌اند (اکراقلی‌پور و همکاران، ۱۳۹۵).

- تعدادی زیادی از پژوهش‌ها به **چالش‌ها، تهدیدات اینترنت اشیا** پرداخته‌اند. به‌عنوان نمونه رمضانی و همکاران در پژوهشی به رتبه‌بندی تهدیدهای اینترنت اشیا در حوزه نظامی پرداختند که بر اساس نتایج این پژوهش، در سازمان‌های نظامی از میان تهدیدهای مختلف فنّاوری اینترنت اشیا تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها از اهمیت بیشتری برخوردارند (رمضانی و همکاران، ۱۴۰۰). آقایی طوق و همکاران در پژوهشی به چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا پرداختند (آقایی طوق و همکاران، ۱۳۹۹). عبدالغنی و همکاران در مقاله‌ای تحت عنوان "بررسی جامعی از حملات اینترنت اشیا بر اساس یک مدل مرجع" به بررسی منابع تهدیدات امنیتی اینترنت اشیا در چهار لایه سنجش شبکه، میان‌افزار و لایه کاربرد پرداخته و بیان می‌دارند که حملات امنیتی اینترنت اشیا عبارت‌اند از: گرفتن گره، تزریق کد مخرب، تزریق داده‌های غلط حملات کانال جانبی، شنود و تداخل، محرومیت از خواب و بوت‌کردن سامانه (*AbdulGhani et al، 2018: 355-373*). رهسپار فرد و همکاران در پژوهشی مدل ساختاریافته از چالش‌های پیاده‌سازی اینترنت اشیا ارائه دادند که با این پژوهش مشخص شد مدیران سازمانی در رابطه با پیاده‌سازی اینترنت اشیا با چه نوع چالش‌هایی روبرو هستند و اهمیت و ارتباطات هرکدام از چالش‌ها به چه صورت است و همچنین چالش نیروی انسانی به‌عنوان یکی از چالش‌های مهم در سطح اول مطرح است (رهسپار فرد و همکاران، ۱۳۹۷). تاج و همکاران در مقاله‌ای تحت عنوان "طبقه‌بندی موضوعات اینترنت اشیا و درجه‌بندی حساسیت آن‌ها"، نقش موضوعات مرتبط با اینترنت اشیا (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 (تاج و همکاران، ۳۷- ۵۲ :۱۳۹۶). تنبو و همکاران در پژوهشی تحت عنوان "تهدیدهای امنیت سایبری اینترنت اشیا در حوزه خدمات و برنامه‌های کاربردی"، به بررسی آسیب‌پذیری‌ها و تهدیدهای امنیت سایبری اینترنت اشیا 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 داده‌ها را معرفی می‌نمایند (*Tweneboah et al*، 2017: 169-185). تسنیم و همکاران در مقاله‌ای تحت عنوان "امنیت اینترنت اشیا: وضعیت فعلی، چالش‌ها و اقدامات متقابل"، بیان می‌دارند که مهم‌ترین نگرانی در تحقق چارچوبی به‌طور کامل هوشمند اینترنت اشیا، امنیت است. اگر نگرانی‌های امنیتی مانند حریم خصوصی، محرمانه بودن، احراز هویت، کنترل دسترسی، امنیت پایدار، مدیریت اعتماد، سیاست‌های جهانی و استانداردها به‌طور کامل موردتوجه قرار گیرند، در آینده‌ای نزدیک تغییر همه‌چیز توسط اینترنت اشیا صورت می گیرد (*Tasneem et al*, 2015:74-55).

که به نظر می‌آید پژوهش‌های دسته آخر، نزدیک‌ترین پژوهش‌های مرتبط با موضوع این پژوهش هستند.

پژوهش حاضر ازلحاظ ماهیت آمیخته کیفی مقدم بر کمّی است و ازنظر روش، موردی- زمینه‌ای است و ازنظر هدف، کاربردی بوده چراکه با انجام این پژوهش و تبیین فرصت‌ها، تهدیدات و راه‌کارهای مقابله‌ای به‌کارگیری اینترنت اشیا در سازمان‌های امنیتی، می‌توان دستاوردهای این پژوهش را در به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی در راستای مهاجرت از روش‌های سنتی به روش‌های مدرن، کاهش هزینه‌های عملیاتی، ارتقای توان عملیاتی در مأموریت‌ها و افزایش بهره‌وری، مدیریت هوشمندانه محیط عملیاتی و کنترل از راه دور تجهیزات و سامانه‌ها و... مدنظر قرار داد و بهره برد. در بخش آمار کیفی، ابتدا جمع‌آوری اطلاعات از طریق مصاحبه با روش گلوله برفی تا رسیدن به اشباع انجام شد و سپس بررسی اسناد و مدارک، مقالات و منابع کتابخانه‌ای صورت گرفت. در بخش اسنادی، روش تجزیه‌وتحلیل اطلاعات کیفی بوده و با کمک تحلیل محتوی انجام شد؛ یعنی در پژوهش حاضر ضمن به‌کارگیری تجارب پژوهشگران و محققین، محورها و خطوط کلی متون، اسناد و مدارک، مقالات و ... استخراج و برای تعیین، مؤلفه‌های تأثیرگذار بر موضوع موردپژوهش در اختیار کارشناسان و متخصصان قرارگرفته است. در بخش آمار کمی، برای تحلیل داده‌های حاصل از پرسش‌نامه و نظرات صاحب‌نظران از آمار توصیفی برای تجزیه‌وتحلیل داده‌ها استفاده شد.

جامعه آماری در این پژوهش را تعداد ۶۵ نفر از کارشناسان، صاحب‌نظران و مدیران حوزه فنّاوری سازمان‌های امنیتی و آشنا با مباحث عملیاتی تشکیل دادند. به دلیل محدودبودن جامعه آماری، در این پژوهش از نمونه‌گیری استفاده‌نشده و به‌صورت تمام‌شمار همه افراد جامعه هدف در نظر گرفته شدند. گردآوری اطلاعات و داده‌ها در این پژوهش با استفاده از روش کتابخانه‌ای و میدانی و با مصاحبه و پرسش‌نامه انجام شد. به‌منظور تعیین روایی پرسش‌نامه ازنظر متخصصین و خبرگان حوزه پژوهش (روایی محتوایی) استفاده شد و بعد از اعمال نظرات و اصلاحات لازم و اخذ پایایی درونی (آلفای کرونباخ = ۰/۹۴۸) پرسش‌نامه در بین اعضای جامعه آماری توزیع گردید. به‌منظور پاسخگویی، مقیاس لیکرت ۵

تایی (از کاملاً موافق تا کاملاً مخالف) در نظر گرفته‌شده که با توجه به آن پاسخ‌دهندگان وضعیت هر شاخص را مشخص نمودند.

مبانی نظری و مفاهیم:

اینترنت اشیا یک مفهوم و یک پارادایم است که حضور گسترده‌ای در محیط‌های مختلف اعم از اتصالات بی‌سیم و سیمی و طرح‌های نشانی‌دهی منحصربه‌فرد اشیا داشته و قادر به تعامل و همکاری اشیا با یکدیگر و دیگر چیزها برای ایجاد برنامه‌ها یا خدمات جدید و رسیدن به اهداف مشترک را در نظر گرفته است. چالش‌های فراوانی درزمینهٔ پژوهش و توسعه برای ایجاد یک جهان هوشمند، وجود دارد. جهان‌های واقعی، دیجیتال و مجازی در حال یکپارچگی و همگرا شدن برای ایجاد محیط‌های هوشمند هستند که به تولید انرژی، حمل‌ونقل، شهرها و بسیاری از حوزه‌های دیگر برسند. هدف از اینترنت اشیا قادر ساختن اشیا برای متصل شدن در هر زمان و هر جا، به هر شیء، موجودیت و انسان دیگر است. در حالت ایدئال، قابلیت استفاده‌کردن از هر طریق، مسیر، شبکه و هرگونه خدمات را اینترنت اشیا می‌گویند. اینترنت اشیا انقلاب جدیدی در اینترنت است. اشیا، خود را قابل‌تشخیص و شناسایی می‌سازند (عطاریان، ۱۳۹۵).

اکوسیستم اینترنت اشیا

اکوسیستم اینترنت اشیا بسیار متنوع و دربرگیرنده اجزای مختلفی است و توسعه آن بدون شناسایی و ارتباط میان اجزا امکان‌پذیر نیست. اکوسیستم اینترنت اشیا بر اساس لایه‌های مختلفی نظیر سخت‌افزارها، ارتباطات، امنیت، پلتفرم‌ها، نگهداری و پردازش اطلاعات و نرم‌افزارها است. هدف اینترنت اشیا، قابلیت‌بخشی به اشیا برای ارتباط باهم در همه‌جا، همه زمان و با هر وسیله، راه و شبکه‌ای است. باوجوداین، تعامل چند دنیا (حوزه) بوده که دارای اجزای مختلفی است که خود حاصل تعامل سه دنیا است و گاهی از این سه دنیا تحت عنوان اجزای اینترنت اشیا نیز یاد می‌شود: دنیای دیجیتال، دنیای سایبری، دنیای فیزیکی واقعی. در تعامل دنیای فیزیکی با دنیای دیجیتال ما شاهد اجتماعات هستیم و در این زمان باید که اشیا باهم یکپارچه گردند، در تعامل دنیای دیجیتال با دنیای سایبری باید که داده‌ها تجمیع یافته و یکپارچه گردند و در تعامل دنیای فیزیکی با دنیای سایبری باید که معانی یکپارچه گردند. در این هنگام رخ دادهایی مانند: سازه‌های هوشمند، سلامت هوشمند، انرژی هوشمند، زندگی هوشمند، حمل‌ونقل هوشمند، شهر هوشمند، صنایع هوشمند و حتی سیاره هوشمند به وجود می‌آید. خود این حوزه‌ها نیز تا حد بسیاری قلمرو اینترنت اشیا را مشخص می‌نمایند (مرکز ملی فضای مجازی).

عناصر سازنده اینترنت اشیا

در تمام زمینه‌ها، از معماری گرفته تا دستگاه‌ها، محدوده گسترده‌ای از فنّاوری‌های رایج با عنوان اینترنت

اشیا نام‌گذاری می‌شوند. چندین سازمان و مؤسسه اقدام به تعیین معماری‌ها یا مدل‌های مرجع برای اینترنت اشیا کرده‌اند. اتحادیه اروپا از پیشگامان حوزه معماری و ایجاد پلتفرم اینترنت اشیا بوده است. عناصر سازنده اینترنت اشیا در شکل ۱ ارائه شده است (شامی زنجانی، ۱۳۹۶).

شکل ۱– عناصر سازنده اینترنت اشیا (شامی زنجانی، ۱۳۹۶)

به‌طورکلی، اینترنت اشیا می‌تواند به چهار سطح کلی تقسیم شود:

سطح اول، اساسی‌ترین پایه، لایه ادراک یا لایه تشخیص بوده که تمامی اطلاعات را از طریق تجهیزات فیزیکی جمع‌آوری کرده و دنیای فیزیکی را شناسایی می‌کند، این اطلاعات شامل خصوصیات اشیا، شرایط محیطی و... هست و تجهیزات فیزیکی شامل خواننده RFID، تمامی انواع حسگرها، GPS و دیگر تجهیزات است. مؤلفه اساسی در این لایه، حسگرها برای دریافت و بیان دنیای واقعی در دنیای دیجیتال است.

سطح دوم، لایه شبکه است. لایه شبکه مسئول ارسال اطلاعات از لایه ادراک، پردازش اولیه اطلاعات، دسته‌بندی و بسپارش[1] است. در این لایه، ارسال اطلاعات مبتنی بر چندین شبکه پایه بوده که شامل اینترنت، شبکه مخابرات سیار، گره‌های ماهواره‌ای، شبکه بی‌سیم، ساختار شبکه بوده و پروتکل‌های مخابراتی نیز برای تبادل اطلاعات بین تجهیزات ضروری است.

سطح سوم، لایه پشتیبانی است. لایه پشتیبانی یک بستر پشتیبانی قابل‌اطمینان را برای لایه برنامه کاربردی، تنظیم می‌کند، در این بستر پشتیبانی، تمامی توان محاسباتی هوشمند از طریق شبکه اتصال و محاسبات ابری، سازماندهی می‌شود. این لایه نقش یک لایه ترکیب کاربردها را ایفا می‌کند.

سطح چهارم، لایه برنامه کاربردی و مدیریت یک نقش اساسی در هر سطح بالا را ایفا می‌کند. آنگاه، ویژگی‌های امنیت را تحلیل خواهیم کرد.

1. *polymerization*

فنّاوری‌های شکل‌دهنده و پشتیبان اینترنت اشیا

اینترنت اشیا یک فنّاوری نیست، بلکه مجموعه‌ای از فنّاوری‌های مختلف و اغلب نوینی است که وقتی دست‌به‌دست هم می‌دهند، زنجیره‌ای را به وجود می‌آورند که به آن فنّاوری اینترنت اشیا گفته می‌شود. برخی از فنّاوری‌ها هستند که کاربردهای اینترنت اشیا را پشتیبانی می‌کنند. این فنّاوری‌ها شامل موارد زیر هستند (شامی زنجانی، ۱۳۹۶):

فنّاوری‌هایی که در معماری اینترنت اشیا نقش دارند	فنّاوری‌های سخت‌افزاری
فنّاوری‌های مورداستفاده در تعیین هویت	فنّاوری‌های کاربردی در پردازش سیگنال و داده
فنّاوری‌هایی که در ارتباطات کاربرد دارد	فنّاوری‌های مورداستفاده در اکتشاف و جست‌وجو
فنّاوری‌های مورداستفاده در شبکه‌ها	فنّاوری‌های مورداستفاده در مدیریت شبکه
فنّاوری‌های کشف شبکه	فنّاوری‌های مورداستفاده در ذخیره قدرت و انرژی
فنّاوری‌های الگوریتم و نرم‌افزار مورداستفاده در اینترنت اشیا	فنّاوری‌های مورداستفاده در حوزه‌های امنیت، اعتماد، وابستگی و حریم خصوصی.

در یک تقسیم‌بندی کلی می‌توان فنّاوری‌هایی که به شکل‌دهی اینترنت اشیا کمک می‌کنند را در سه دسته قرار داد (شامی زنجانی، ۱۳۹۶):

۱) فنّاوری‌هایی که ابزارها را تحت‌تأثیر قرار می‌دهند: حسگرها با مصرف توان پایین/ هوشمندسازی حسگرها/ کوچک‌سازی تراشه‌ها/ فنّاوری‌های شناسایی مانند شناسایی با امواج رادیویی/ فنّاوری‌های جمع‌آوری داده مانند شناسایی با امواج رادیویی و گره‌های حسگرها

۲) فنّاوری‌هایی که مسائل شبکه‌ای را پوشش می‌دهند: فنّاوری‌های آدرس‌دهی/ فنّاوری‌های ارتباطی/ فنّاوری‌های افزایش گذردهی شبکه و کاهش تأخیر/ پردازش ابری/ شبکه‌های نرم‌افزاری تعیین‌شده/ شبکه‌های حسگر بی‌سیم

۳) فنّاوری‌هایی که سرویس‌های مدیریتی را تحت‌تأثیر قرار می‌دهند: فنّاوری‌های تصمیم‌گیری هوشمند مانند سرویس‌های پردازشی آگاه از محتوا، تجزیه‌وتحلیل رفتاری، پردازش رخدادهای پیچیده/ فنّاوری‌های پردازش سریع داده مانند تحلیل‌های جریانی یا داخل حافظه

فنّاوری‌های توانمندساز در بستر اینترنت اشیا:

فنّاوری‌های توانمندساز، فنّاوری‌هایی هستند که مستقلاً مورداستفاده قرار می‌گیرند و مفهومی مجزا دارند ولی تحت پلتفرم و بستر اینترنت اشیا کنار یکدیگر قرار می‌گیرند تا حداکثر سرویس‌دهی و بهره‌وری را شاهد باشیم. درواقع فنّاوری‌های توانمندساز برای ارزش‌افزوده مورداستفاده قرار می‌گیرند. عناوین تعدادی از پراستفاده‌ترین فنّاوری‌های توانمندساز در زیر آورده شده (سخایی، ۱۳۹۴):

رایانش ابری[1]	سرویس مکان‌یابی[2]
رایانش مه[3]	بلاک‌چین[4]
داده‌های کلان[5] و یادگیری ماشین[6]	واقعیت افزوده[7]
شبکه حسگر بی‌سیم[8]	واقعیت مجازی[9]

پلتفرم داده اینترنت اشیا:

نیاز به یک نوع جدید از پلتفرم داده برای راه‌حل‌های اینترنت اشیا یکی از ضروریات مهم محسوب می‌گردد. مؤسسه تحقیقات و پژوهشی گارتنر در گزارشی که تحت عنوان "ویژگی‌های سامانه مدیریت بانک اطلاعاتی برای اینترنت اشیا"، منتشر شده است، به این موضوع مهم اشاره کرده است که اکثریت داده تولیدشده توسط دستگاه‌های اینترنت اشیا به‌صورت سری زمانی و داده مبتنی بر رویداد است و نیاز به یک بانک اطلاعاتی است که بتواند با توجه به ماهیت این نوع از داده‌ها در ابعادی نظیر حجم، سرعت و تنوع پاسخگو باشد. همچنین استقرار یک چارچوب امنیتی فعالانه در محیط‌های مختلف متناسب با مقررات مختص هر حوزه صنعتی، از دیگر الزامات این نوع بانک‌های اطلاعاتی است (سخایی، ۱۳۹۴).

اینترنت اشیا، نه‌تنها دارای این ظرفیت است که بر نحوه زندگی ما تأثیر بگذارد بلکه می‌تواند تأثیرگذاری به‌مراتب بیشتری بر روی فضای سازمان‌ها به دنبال داشته باشد و فرصت‌های بی‌شماری را ایجاد نماید. مجموعه اتفاقات خوبی باعث گسترش روزافزون اینترنت اشیا شده است. سرعت بالای اینترنت، کاهش هزینه‌های اتصال به شبکه، کاهش قیمت دستگاه‌ها و حسگرها، ضریب نفوذ بالای تلفن‌های هوشمند و... جملگی باعث شکل‌گیری تحولی عظیم در حوزه اینترنت اشیا شده است. با توجه به ماهیت الگوهای معماری اینترنت اشیا، انتخاب مناسب یک پلتفرم داده که تأمین‌کننده نیاز فعلی و آینده باشد، یکی از الزامات اساسی برای ورود به این بازار جذاب و گسترده است.

طبقه‌بندی کلی تهدیدهای اینترنت اشیا

تهدیدهای اینترنت اشیا را می‌توان بر اساس روش حمله به هشت دسته تقسیم نمود. این حمله‌ها عبارتند: نقض حریم خصوصی، شنود، منع سرویس، تخریب تجهیزات شبیه‌سازی مجازی وسایل، سرقت اطلاعات انتشار بدافزار و سرقت هویت کاربر (استاندون و همکاران، ۲۲ :۲۰۱۹). همچنین تهدیدهای اینترنت اشیا را

1. *Cloud computing*
2. *Navigation*
3. *Fog Computing*
4. *Block chain*
5. *Big Data*
6. *Machine Learning*
7. *Augmented Reality*
8. *Wireless sensor network (WSN)*
9. *Virtual Reality*

می‌توان با توجه به حمله‌هایی که به لایه‌های تشکیل‌دهنده اینترنت اشیا انجام می‌شود، به تهدیدهای لایه برنامه‌های کاربردی، تهدیدهای لایه شبکه و تهدیدهای لایه دریافت هوشمند تقسیم‌بندی نمود (مسعودی و همکاران، ۲۰۱۹:۷۰). در دسته‌بندی دیگری، تهدیدهای اینترنت اشیا 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 و همکاران، ۲۵ :۲۰۱۷).

اما بررسی‌های انجام‌شده در این پژوهش نشان‌داد که با توجه به موضوعات مختلف مطرح و مرتبط با فنّاوری اینترنت اشیا، هر یک از دسته‌بندی‌های بالا نمی‌تواند به‌تنهایی و به‌طور کامل مجموعه تهدیدات را پوشش دهد. به‌عنوان‌مثال در اکثر دسته‌بندی‌های بالا، فقط موضوعات فنّاوری مدنظر قرارگرفته؛ این در صورتی است که موضوعاتی نظیر پذیرش فنّاوری نو در سازمان‌ها، برون‌سپاری پیاده‌سازی زیرساخت‌های فنّاوری و ...نیز می‌توانند تهدیداتی را ایجاد کنند. از طرفی فنّاوری اینترنت اشیا در اختیار دشمن نیز است و تهدیدات ناشی از به‌کارگیری این فنّاوری توسط دشمن نیز مطرح هستند؛ بنابراین بایستی از جنبه‌های مختلف، تهدیدات طرح و راه‌کارهای پیشگیرانه و مقابله‌ای موردبررسی قرار گیرد؛ ازاین‌رو در این پژوهش، تهدیدات از سه جنبه موردبررسی قرارگرفته‌اند: ۱- تهدیدات ناشی از عدم ورود فنّاوری اینترنت اشیا به سازمان‌های اطلاعاتی ۲- تهدیدات ناشی از استفاده دشمن از فنّاوری اینترنت اشیا ۳- تهدیدات ناشی از استفاده خودی از فنّاوری.

در این پژوهش، برای در نظر گرفتن تهدیدات مرتبط با فنّاوری، دسته‌بندی که رمضانی و همکاران در کار خود ارائه داده‌اند مبنا قرار داده شد؛ یعنی 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، در نظر گرفته شد (رمضانی و همکاران، ۱۴۰۰)؛ اما برخی موارد تکمیلی نیز (نظیر فنّاوری‌های ایمن‌ساز و فنّاوری‌های توانمندساز)، به علت اهمیت موضوع، در زمره تهدیدات مرتبط با فنّاوری آورده شدند. نکته قابل‌توجه اینکه هر یک از تهدیدات، به کلیات اشاره دارد و ذکر جزئیات، ابعاد پژوهش را گسترده می‌کند؛ ازاین‌رو شاید در برخی موارد هم‌پوشانی‌هایی دیده شود. با توجه به دسته‌بندی‌هایی که در تهدیدات انجام گردید، ناچار راه‌کارهای مقابله‌ای نیز در دودستهٔ راه‌کارهای مدیریتی و راه‌کارهای فنّاورانه (مرتبط با فنّاوری) طرح و بررسی شدند.

یافته‌های پژوهش

تجزیه‌وتحلیل توصیفی و استنباطی سؤالات پرسش‌نامه:

در جداول ۱، ۲، ۳ و ۴ با استفاده از داده‌های حاصل از پرسش‌نامه و نظرات صاحب‌نظران، آمار توصیفی (میانگین، انحراف معیار، بیشینه و کمینه) و آمار استنباطی اولیه (مقدار خی دو به همراه درجه آزادی) آورده شده است. شرح سؤالات پرسش‌نامه‌ها به علت محدودیت فضا، در این جداول آورده نشده

و فقط شماره سؤالات در پرسش‌نامه درج گردیده و برای اطلاع از شرح سؤالات پرسش‌نامه‌ها بایستی به جداول ۶، ۷، ۸ و ۹ مراجعه شود.

جدول ۱– تحلیل اولیه داده‌های پرسش‌نامه فرضیه اول (فرصت‌های به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی)

ردیف	شماره سؤالات در پرسش‌نامه	میانگین	انحراف معیار	بیشینه	کمینه	دیدگاه خبرگان					Chi-square آزمون خی دو	
						درجات ارزیابی (درصد)						
						خیلی زیاد	زیاد	متوسط	کم	خیلی کم	مقدار	درجه آزادی
۱	۱	٤	۰,۹۱۸	۵	۱	۳۰,۸	٤۶,۲	۱۸,۵	۱,۵	۳,۱	٤۶,٤۶۲	٤
۲	۲	٤,۱۵۳	۰,۹۲۲	۵	۱	٤۱,۵	٤۰	۱۲,۳	٤,۶	۱,۵	٤۸,۷۶۹	٤
۳	۳	٤,۱۳۸	۰,۸۶۳	۵	۱	۳۸,۵	٤۱,۵	۱۶,۹	۱,۵	۱,۵	٤۸,۶۱۵	٤
٤	٤	٤,۲۳۰	۰,۹۶٤	٤	۱	۵۰,۸	۲۷,۷	۱۸,۵	۰	۳,۱	۳۱,۰۶۲	۳
۵	۵	٤,۲۷۶	۰,۹۱۰	۵	۱	۵۰,۸	۳۲,۳	۱۲,۳	۳,۱	۱,۵	۵۸	٤
۶	۶	٤,۰٤۶	۰,۹٤۲	۵	۱	۳۶,۹	۳۸,۵	۱۸,۵	٤,۶	۱,۵	۳۹,۲۳۱	٤
۷	۷	٤,۰۷۶	۰,۷۹۶	۵	۲	۳۲,۳	٤۶,۲	۱۸,۵	۳,۱	۰	۲۶,۶۳۱	۳
۸	۸	٤,۲۷۶	۰,۶۷۳	۵	۲	۳۸,۵	۵۲,۳	۷,۷	۱,۵	۰	٤۶,۲	۳
۹	۹	٤,۳۳۸	۰,۸۳٤	۵	۱	۵۲,۳	۳۲,۳	۱۳,۸	۰	۱,۵	۳۸,۳۲۳	۳
۱۰	۱۰	٤,۲۹۲	۰,۸۹۶	۵	۱	۵۰,۸	۳۳,۸	۱۰,۸	۳,۱	۱,۵	۶۰,۱۵٤	٤
۱۱	۱۱	٤,۳۰۷	۰,۷۸۹	۵	۲	٤۷,۷	۳۸,۵	۱۰,۸	۳,۱	۰	۳۵,۸۶۲	۳
۱۲	۱۲	٤,۲۱۵	۰,۸۹۲	۵	۱	٤٤,۶	۳۸,۵	۱۲,۳	۳,۱	۱,۵	۵۳,۰۷۷	٤
۱۳	۱۳	٤,۲۷۶	۰,۷۸۰	۵	۲	٤٤,۶	٤۱,۵	۱۰,۸	۳,۱	۰	۳٤,۸۷۷	۳
۱٤	۱٤	٤,۳۶۹	۰,۷۸۲	۵	۲	۵۳,۸	۳۰,۸	۱۳,۸	۱,۵	۰	٤۰,۰٤۶	۳
۱۵	۱۵	٤,۲۹۲	۰,۸۲۳	۵	۲	٤۷,۷	۳۸,۵	۹,۲	٤,۶	۰	۳۵,۳۶	۳
۱۶	۱۶	٤,۳۲۳	۰,۷۹۲	۵	۱	٤۷,۷	٤۰	۱۰,۸	۰	۱,۵	۳۸,۸۱۵	۳
۱۷	۱۷	٤,۱۶۹	۰,۷۶۱	۵	۱	۳۳,۸	۵۲,۳	۱۲,۳	۰	۱,۵	۳۹,۹۲۳	۳
۱۸	۱۸	٤,۲۱۵	۰,۷۶۰	۵	۲	٤۰	٤۳,۱	۱۵,٤	۱,۵	۰	۳۱,۰۶۲	۳
۱۹	۱۹	۳,۹۲۳	۰,۹۲۳	۵	۱	۲۹,۲	٤۱,۵	۲۳,۱	٤,۶	۱,۵	۳۶,۹۲۳	٤
۲۰	۲۰	٤,۰۷۶	۰,۷۹۶	۵	۲	۳۲,۳	٤۶,۲	۱۸,۵	۳,۱	۰	۲۶,۶۳۱	۳
۲۱	۲۱	٤,۲۷۶	۰,۷۸۰	۵	۲	٤٤,۶	٤۱,۵	۱۰,۸	۳,۱	۰	۳٤,۸۷۷	۳
۲۲	۲۲	٤,۳۶۹	۰,۷۸۲	۵	۲	۵۳,۸	۳۰,۸	۱۳,۸	۱,۵	۰	٤۰,۰٤۶	۳

جدول ۲- تحلیل اولیه داده‌های پرسش‌نامه فرضیه اول (تهدیدات به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی)

ردیف	شماره سؤالات در پرسش‌نامه	میانگین	انحراف معیار	بیشینه	کمینه	دیدگاه خبرگان					Chi-square آزمون خی دو	
						درجات ارزیابی (درصد)						
						خیلی زیاد	زیاد	متوسط	کم	خیلی کم	مقدار	درجه آزادی
۱	۱	٤	۰,۸٤۷	۵	۲	۳۰,۸	٤۳,۱	۲۱,۵	٤,۶	۰	۲۰,٤۷۷	۳
۲	۲	٤,۲۷۶	۰,۷۸۰	۵	۲	٤۶,۲	۳۶,۹	۱۵,٤	۱,۵	۰	۳۲,۰٤	۳
۳	۳	٤,٤۷۶	۰,۶۱۵	۵	۳	۵۳,۸	٤۰	۶,۲	۰	۰	۲۳,٤۷	۲
٤	٤	٤,۲۷۶	۰,۸۰۰	۵	۲	٤۷,۷	۳۳,۸	۱۶,۹	۱,۵	۰	۳۱,٤۳	۳
۵	۵	٤,۱۲۳	۰,۸۳۸	۵	۲	۳۸,۵	۳۸,۵	۲۰	۳,۱	۰	۲۲,۵۶۹	۳
۶	۶	٤,٤۱۵	۰,۵۸۳	۵	۳	٤۶,۲	٤۹,۲	٤,۶	۰	۰	۲٤,۲۱۵	۲
۷	۷	٤,٤۱۵	۰,۷۲۶	۵	۲	۵۳,۸	۳۵,٤	۹,۲	۱,۵	۰	٤۵,۲۱	۳
۸	۸	٤	۰,۸۳۸	۵	۱	٤۱,۵	٤۳,۱	۱۲,۳	۱,۵	۱,۵	۵۶,٤۶	٤
۹	۹	٤,۲۷۶	۰,۸۰۰	۵	۲	٤۷,۷	۳۳,۸	۱۶,۹	۱,۵	۰	۳۱,٤۳	۳
۱۰	۱۰	٤,۳۸٤	۰,۷٤۳	۵	۲	۵۲,۳	۳۵,٤	۱۰,۸	۱,۵	۰	٤۱,۷۶	۳
۱۱	۱۱	٤,۳۰۷	۰,۸٤۶	۵	۱	۵۰,۸	۳۲,۳	۱۵,٤	۰	۱,۵	۳۵,۳۶۹	۳
۱۲	۱۲	٤,۳۶۹	۰,۷۸۲	۵	۲	۵۰,۸	٤۰	٤,۶	٤,۶	۰	٤٤,۷۲۳	۳
۱۳	۱۳	٤,۱۳۸	۰,۸۲۶	۵	۲	۳۸,۵	٤۰	۱۸,۵	۳,۱	۰	۲٤,۱۶۹	۳
۱٤	۱٤	٤,۰۷۶	۰,۷۳۵	۵	۲	۲۷,۷	۵۵,٤	۱۳,۸	۳,۱	۰	۳۹,۹۲	۳
۱۵	۱۵	٤,۱۳۸	۰,۹۱۶	۵	۱	٤۱,۵	۳۶,۹	۱۶,۹	۳,۱	۱,۵	٤۵,۰۷۷	٤
۱۶	۱۶	٤,۱۲۳	۰,۸۳۸	۵	۲	۳۸,۵	۳۸,۵	۲۰	۳,۱	۰	۲۲,۵۶۹	۳
۱۷	۱۷	٤,۲٤۶	۰,۸۲۹	۵	۲	٤٤,۶	٤۰	۱۰,۸	٤,۶	۰	۳۱,۹۲۳	۳
۱۸	۱۸	٤,۲۷۶	۰,۸۰۰	۵	۲	٤۷,۷	۳۳,۸	۱۶,۹	۱,۵	۰	۳۱,٤۳	۳
۱۹	۱۹	٤,۰۱۵	۰,۸۰۰	۵	۲	۲۹,۲	٤۶,۲	۲۱,۵	۳,۱	۰	۲٤,۹۰۸	۳
۲۰	۲۰	۳,۹۸٤	۱,۰۲۳	۵	۱	۳۵,٤	۳۸,۵	۲۰	۱,۵	٤,۶	۳۷,۵۳۸	٤
۲۱	۲۱	٤,٤۷۶	۰,۶۱۵	۵	۳	۵۳,۸	٤۰	۶,۲	۰	۰	۲۳,٤۷	۲
۲۲	۲۲	٤,۲۷۶	۰,۸۰۰	۵	۲	٤۷,۷	۳۳,۸	۱۶,۹	۱,۵	۰	۳۱,٤۳	۳
۲۳	۲۳	٤,۱۲۳	۰,۸۳۸	۵	۲	۳۸,۵	۳۸,۵	۲۰	۳,۱	۰	۲۲,۵۶۹	۳
۲٤	۲٤	٤,٤۱۵	۰,۵۸۳	۵	۳	٤۶,۲	٤۹,۲	٤,۶	۰	۰	۲٤,۲۱۵	۲
۲۵	۲۵	٤,٤۱۵	۰,۷۲۶	۵	۲	۵۳,۸	۳۵,٤	۹,۲	۱,۵	۰	٤۵,۲۱	۳

جدول ۳- تحلیل اولیه داده‌های پرسش‌نامه فرضیه دوم (راه‌کارهای مدیریتی به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی)

ردیف	شماره سؤالات در پرسش‌نامه	میانگین	انحراف معیار	بیشینه	کمینه	دیدگاه خبرگان (درجات ارزیابی (درصد))					Chi-square آزمون خی دو	
						خیلی زیاد	زیاد	متوسط	کم	خیلی کم	مقدار	درجه آزادی
۱	۱	٤,٤۳۰	۰,۷۲۸	۵	۲	۵۵,٤	۳۳,۸	۹,۲	۱,۵	۰	٤۶,۸۱۵	۳
۲	۲	٤,۳۵۳	۰,۹۵۹	۵	۱	۵۸,۵	۲۶,۲	۱۰,۸	۱,۵	۳,۱	۷۲,٤۶۲	٤
۳	۳	٤,۵۰۷	۰,۶٤۰	۵	۳	۵۸,۵	۳۳,۸	۷,۷	۰	۰	۲۵,۱۳۸	۲
٤	٤	٤,۵۳۸	۰,۵۶۱	۵	۳	۵۶,۹	٤۰	۳,۱	۰	۰	۲۹,۵۶۹	۲
۵	۵	٤,۱۵۳	۰,۸۵۲	۵	۱	۳۸,۵	٤۳,۱	۱۵,٤	۱,۵	۱,۵	۵۱,۲۳۱	٤
۶	۶	٤,۳۳۸	۰,۷۳٤	۵	۲	٤۶,۲	٤٤,۶	۶,۲	۰	۰	٤۳,۳۶۹	۳
۷	۷	٤,۵۰۷	۰,۵۸۹	۵	۳	۵۵,٤	٤۰	٤,۶	۰	۰	۲۶,٤۳	۲
۸	۸	٤,٤۹۲	۰,۷۹۳	۵	۱	۶۳,۱	۲۶,۲	۹,۲	۰	۱,۵	۵۸,۵۰۸	۳
۹	۹	٤,۲۷۶	۰,۷۸۰	۵	۱	٤۳,۱	٤٤,۶	۱۰,۸	۰	۱,۵	۳۹,۰۷۷	۳
۱۰	۱۰	٤,۳۵۳	۰,۹۵۹	۵	۱	۵۸,۵	۲۶,۲	۱۰,۸	۱,۵	۳,۱	۷۲,٤۶۲	٤
۱۱	۱۱	٤,۲۹۲	۰,۸٤۲	۵	۱	٤۷,۷	۳۸,۵	۱۰,۸	۱,۵	۱,۵	۶۰,۹۲۳	٤
۱۲	۱۲	٤,۲۷۶	۰,۸۰۰	۵	۱	٤۳,۱	٤۶,۲	۷,۷	۱,۵	۱,۵	۶۶,۶۱۵	٤
۱۳	۱۳	٤,۲٤۶	۰,۸۶۶	۵	۱	٤۳,۱	٤٤,۶	۹,۲	۰	۳,۱	۳۷,٤۶۲	۳
۱٤	۱٤	٤,۳۰۷	۰,۷٤۸	۵	۲	٤۶,۲	٤۰	۱۲,۳	۱,۵	۰	۳۵,۹۸۵	۳
۱۵	۱۵	٤,۲۳۰	۰,۷۰۱	۵	۲	۳۶,۹	۵۰,۸	۱۰,۸	۱,۵	۰	٤۰,۵۳۸	۳
۱۶	۱۶	٤,٤۹۲	۰,۷۳۱	۵	۲	۶۰	۳۲,۳	٤,۶	۳,۱	۰	۵۶,۵۳۸	۳

جدول ۴- تحلیل اولیه داده‌های پرسش‌نامه فرضیه دوم (راه‌کارهای فنّاورانه به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی)

ردیف	شماره سؤالات در پرسش‌نامه	میانگین	انحراف معیار	بیشینه	کمینه	دیدگاه خبرگان (درجات ارزیابی (درصد))					Chi-square آزمون خی دو	
						خیلی زیاد	زیاد	متوسط	کم	خیلی کم	مقدار	درجه آزادی
۱	۱	٤,۰۹	۰,۹۵٤	۵	۱	۳۹	۳۹	۱۷	۲	۳	۶۲,۲	٤
۲	۲	٤,۳۷	۰,۷۰۶	۵	۳	۵۰	۳۷	۱۳	۰	۰	۲۱,۱٤	۲

ردیف	شماره سؤالات در پرسش‌نامه	میانگین	انحراف معیار	بیشینه	کمینه	دیدگاه خبرگان					Chi-square آزمون خی دو	
						درجات ارزیابی (درصد)						
						خیلی زیاد	زیاد	متوسط	کم	خیلی کم	مقدار	درجه آزادی
۳	۳	٤,۲۶	۰,۷۳۳	۵	۲	٤۰	٤۹	۸	۳	۰	۶۲,۹۶	۳
٤	٤	٤,۳۳	۰,۸۸۸	۵	۲	۵۶	۲۶	۱۳	۵	۰	۶۰,۲٤	۳
۵	۵	٤,۳	۰,۷۸۵	۵	۳	۵۰	۳۰	۲۰	۰	۰	۱٤	۲
۶	۶	٤,۱۹	۰,۸	۵	۲	٤۰	٤۲	۱۵	۳	۰	٤۳,۹۲	۳
۷	۷	۳,۹۷	۱,۳۲۹	۵	۱	٤۵	۳۶	۲	۵	۱۲	۷٤,۷	٤
۸	۸	٤,۰۶	۰,۹۳	۵	۲	٤۱	۲۹	۲۵	۵	۰	۲۶,۸۸	۳
۹	۹	٤,۲۷	۰,۹۳	۵	۲	٤۹	٤۰	۰	۱۱	۰	۲۳,۶۶	۲
۱۰	۱۰	٤,۳۵	۰,۸۹۲	۵	۱	۵٤	۳۳	۱۰	۰	۳	۶٤,۵۶	۳
۱۱	۱۱	۳,۵۵	۰,۸۹۲	۵	۱	۱۱	٤۶	۳۳	۷	۳	۶۹,۲	٤
۱۲	۱۲	۳,۵۹	۱,۰۳۶	۵	۲	۵۶	۲۲	۱۳	۵	٤	۲۱,۱٤	۳
۱۳	۱۳	۳,۶۲	۰,۸۲۶	۵	۲	۱٤	٤۲	۳۶	۸	۰	۳۲,۸	۳
۱٤	۱٤	٤,٤	۰,۷۲۵	۵	۲	۵۲	۳۸	۸	۲	۰	۶۸,۶٤	۳
۱۵	۱۵	٤,۰٤	۰,۷۵۱	۵	۲	۲۸	۵۰	۲۰	۲	۰	٤۷,۵۲	۳
۱۶	۱۶	٤,۲۲	۰,۹۳۸	۵	۱	٤۶	۳۸	۱۱	۲	۳	۸٤,۷	٤
۱۷	۱۷	٤,۳۵	۰,۸٤۵	۵	۲	۵۵	۲۹	۱۲	٤	۰	۶۱,۰٤	۳
۱۸	۱۸	٤,۱۲	۰,۹۵۶	۵	۱	۳۸	٤۶	۱۰	۲	٤	۸٤	٤
۱۹	۱۹	۳,۹۶	۰,۹۲	۵	۲	۲۹	٤۹	۱۱	۱۱	۰	۳۹,۳۶	۳
۲۰	۲۰	٤,۰۹	۰,۹۵٤	۵	۱	۳۹	۳۹	۱۷	۲	۳	۶۲,۲	٤
۲۱	۲۱	٤,۳۷	۰,۷۰۶	۵	۳	۵۰	۳۷	۱۳	۰	۰	۲۱,۱٤	۲
۲۲	۲۲	٤,۲۶	۰,۷۳۳	۵	۲	٤۰	٤۹	۸	۳	۰	۶۲,۹۶	۳
۲۳	۲۳	٤,۳۳	۰,۸۸۸	۵	۲	۵۶	۲۶	۱۳	۵	۰	۶۰,۲٤	۳
۲٤	۲٤	٤,۳	۰,۷۸۵	۵	۳	۵۰	۳۰	۲۰	۰	۰	۱٤	۲
۲۵	۲۵	٤,۱۹	۰,۸	۵	۲	٤۰	٤۲	۱۵	۳	۰	٤۳,۹۲	۳
۲۶	۲۶	۳,۹۶	۱,۰٤٤	۵	۱	۳۷	۳۵	۱۷	۹	۲	٤۸,٤	٤
۲۷	۲۷	٤,۶۱	۰,۶۸	۵	۲	۶۹	۲۶	۲	۳	۰	۱۱۸	۳
۲۸	۲۸	٤,۰۹	۰,۷۸۰	۵	۲	۳۳	٤۵	۲۰	۲	۰	٤۰,۷۲۰	۳
۲۹	۲۹	٤,۲۲	۰,۸۱۱	۵	۲	٤۳	۳۹	۱۵	۳	۰	٤٤,۱۶	۳

ردیف	شماره سؤالات در پرسش‌نامه	میانگین	انحراف معیار	بیشینه	کمینه	دیدگاه خبرگان					Chi-square آزمون خی دو	
						درجات ارزیابی (درصد)						
						خیلی زیاد	زیاد	متوسط	کم	خیلی کم	مقدار	درجه آزادی
۳۰	۳۰	٤,٥٥	۰,٥٧٥	٥	۳	٥٩	۳۷	٤	۰	۰	٤٥,۹۸	۲
۳۱	۳۱	٤,۱۱	۰,۹٤۲	٥	۲	۳۹	٤٤	۶	۱۱	۰	٤٤,٥۶۰	۳
۳۲	۳۲	٤,۳۳	۰,۹۲۲	٥	۱	٥٥	۲۹	۱۳	۰	۳	۶۱,۷۶۰	۳
۳۳	۳۳	٤,۳٥	۰,۸۰۹	٥	۲	٥۲	۳٥	۹	٤	۰	۶۱,۰٤	۳
۳٤	۳٤	٤,٥۱	۰,۶۸۹	٥	۲	٥۹	۳۶	۲	۳	۰	۹۱,۶	۳
۳٥	۳٥	٤,۳٥	۰,۶۰۹	٥	۳	٤۲	٥۱	۷	۰	۰	۳۲,٤۲	۲

داده‌های چهار جدول یادشده حاکی از آن است که ارزش خی‌دوی مشاهده‌شده در درجه آزادی مربوطه، معنی‌دار است. درنتیجه تفاوت بین فراوانی‌های مشاهده‌شده تأیید می‌شود. روایی پرسش‌نامه صوری و با تأیید خبرگان حوزه پژوهش تحصیل شد و پایایی پرسش‌نامه بر اساس آلفای کرونباخ محاسبه شد و ضریب آلفای کرونباخ کلی مقدار ۹۴۸/۰ را به خود اختصاص داد که بسیار مطلوب است.

تجزیه‌وتحلیل استنباطی فرضیه‌ها:

در این قسمت فرضیه‌های پژوهشی به ترتیب مورد تجزیه‌وتحلیل توصیفی و استنباطی قرارمی‌گیرد. به این منظور برای هرکدام از فرضیه‌ها پس از تبدیل فرضیه پژوهشی به فرضیه آماری، فرضیه با استفاده از آزمون خی دو مورد تجزیه‌وتحلیل قرارگرفته و درنهایت به رتبه‌بندی عوامل مؤثر فرضیه با استفاده از آزمون فریدمن پرداخته شده است.

جدول ۵– تحلیل اولیه داده‌های فرضیه‌ها

ردیف	عنوان فرضیه	Chi-square آزمون خی دو	Chi-square آزمون فریدمن
		درجه آزادی	درجه آزادی
۱	فرصت‌های به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی عبارتند از ۱- کاهش هزینه‌های عملیاتی، ۲- ارتقای توان عملیاتی در مأموریت‌ها و افزایش بهره‌وری، ۳- آشنایی با شیوه و شگردهای حریف مبتنی بر فنّاوری اینترنت اشیا، ...۳- مدیریت هوشمندانه محیط عملیاتی، کنترل از راه دور تجهیزات و سامانه‌ها.	۶۵,۷۵۰	۵۲,۳۹۵
		۲	۲۱

ردیف	عنوان فرضیه	Chi-square آزمون خی دو	Chi-square آزمون فریدمن
		درجه آزادی	درجه آزادی
۲	تهدیدات به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی عبارتند از ۱- ناتوانی و عقب‌ماندگی در تقابل با سرویس‌های امنیتی حریف که از فنّاوری بهره می‌برند، ۲- عقب‌ماندگی از سازمان‌های اطلاعاتی رقیب داخلی و عدم بهره‌برداری از مزیت‌های رقابتی ناشی از فنّاوری، تهدیدات ناشی از استفاده دشمن از فنّاوری اینترنت اشیا در فرآیند جاسوسی،... ۳- وابستگی به فنّاوری و غفلت و فراموشی روش‌های غیر وابسته به فنّاوری و دیگر روش‌های خلاقانه.	۶۸،۵۶۰	۷۱،۴۹۲
		۳	۲۴
۳	راه‌کارهای مدیریتی به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی عبارتند از ۱- افزایش حمایت‌های مسئولان سازمان در خصوص به‌کارگیری فنّاوری اینترنت اشیا، ۲- تأمین اعتبارات مالی موردنیاز برای راه‌اندازی، توسعه، پشتیبانی و امن‌سازی فنّاوری اینترنت اشیا سازمان‌های امنیتی، تدوین، ابلاغ و اعمال مستمر سیاست‌های امنیتی (طبقه‌بندی داده‌ها و سطوح دسترسی و...) ۳- ایجاد ساختار مناسب و جذب نیروی انسانی متخصص برای راه‌اندازی، توسعه، پشتیبانی، امنیت و کنترل امنیت فنّاوری اینترنت اشیا.	۸۱۳/۳۴	۲۴۳/۲۸
		۳	۱۵
۴	راه‌کارهای فنّاورانه در به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی عبارتند از ۱- رصد پیشرفت فنّاوری‌ها و تأمین، طراحی و استفاده از نرم‌افزار، سخت‌افزار و تجهیزات پیشرفته و جدید اینترنت اشیا، ۲- تأمین زیرساخت‌ها، سامانه‌های امنیتی، سامانه‌های کنترلی و ... برای پیاده‌سازی و امن‌سازی فنّاوری اینترنت اشیا، ۳- بررسی توانمندی‌ها و رویکردهای سازمان‌های اطلاعاتی- امنیتی حریف در حوزه به‌کارگیری فنّاوری اینترنت اشیا،... ۴- راه‌اندازی آزمایشگاه ارزیابی امنیتی سخت‌افزارها، نرم‌افزارها و آزمون نفوذ به شبکه‌های ارتباطی و استخراج آسیب‌پذیری‌ها.	۵۸،۳۴۰	۴۳،۹۳۴
		۳	۳۴

با توجه به اینکه در هر مورد، ارزش خی دوی مشاهده‌شده در درجه آزادی مربوطه معنی‌دار است، درنتیجه استنباط می‌شود که بین فراوانی‌های مشاهده‌شده تفاوت معنی‌داری وجود دارد، یعنی فرضیه مربوطه پذیرفته می‌شود و فرضیه مقابل آن رد می‌گردد. با توجه به اینکه در هر مورد، داده‌های جدول آزمون

فریدمن نیز نشان می‌دهد که ارزش خی دوی مشاهده‌شده در درجه آزادی مربوطه معنی‌دار است، درنتیجه استنباط می‌شود که تفاوت بین میانگین‌های رتبه‌ای متغیرهای مربوطه در هر مورد معنی‌دار است.

تجزیه‌وتحلیل فرضیه اصلی:

با توجه به تأیید فرضیه‌های فرعی نتیجه می‌گیریم که فرضیه اصلی تأیید و موردپذیرش قرارمی‌گیرد یعنی اینکه "فرصت‌ها، تهدیدات و راه‌کارهای مقابله‌ای به‌کارگیری اینترنت اشیا در سازمان‌های امنیتی به‌درستی تبیین شده‌اند".

جدول ۶– ترتیب و توالی شاخص‌های اثرگذار در فرضیه فرعی اول از دیدگاه جامعه آماری

ردیف	شرح فرصت	میانگین رتبه‌های فریدمن	رتبه
۱	کنترل آمدورفت‌ها در اماکن عمومی سازمان‌های امنیتی (نظارت دوربینی، کنترل و نظارت بر آمدورفت کارکنان و مهمانان، آگاهی از مسیر حرکتی آن‌ها با استفاده از کارت‌های کارکنان مبتنی بر RFID و ...)	۱۰,۹۶	۱۱
۲	حفاظت فیزیکی هوشمند (دوربین‌های امنیتی هوشمند و ...)	۹,۶۸	۱۵
۳	هوشمندسازی خانه‌های امن و بازداشتگاه‌های مورداستفاده سازمان‌های امنیتی.	۹,۳٤	۱۷
٤	تسهیل ارتباطات در سازمان‌های امنیتی و ایجاد ارتباط پوششی و امن با منابع، عوامل.	۷,۲٤	۱۹
۵	مقاومت و تاب‌آوری بالا سامانه‌ها در برابر اقدامات خصمانه نظیر اختلالات ارتباطی با استفاده از ماهیت چندلایه و گسترده و نامتجانس اینترنت اشیا.	۱۲,۱۷	٤
۶	کاهش حساسیت‌ها و آسیب‌های ناشی از حضور و آمدورفت نیروی انسانی در محیط عملیاتی.	۱۱,۰۱	۱۰
۷	شنود محیطی موقعیت سوژه‌های عملیاتی از راه دور.	۷,۳۷	۱۸
۸	شبکه‌سازی و جمع‌آوری اطلاعات بلادرنگ از محیط عملیاتی.	۱۱,۱۲	۹
۹	موقعیت‌یابی و ره‌گیری خودروهای عملیاتی در بستر اینترنت اشیا.	۶,۷۵	۲۱
۱۰	کنترل و نظارت دقیق بر روی موقعیت‌ها مکانی و اقدامات فیزیکی سوژه‌های عملیاتی (آمدورفت‌ها، مکان‌ها و ...)	۱۰,۶۳	۱۲

ردیف	شرح فرصت	میانگین رتبه‌های فریدمن	رتبه
۱۱	جمع‌آوری اطلاعات و تولید حجم عظیم و آزاد داده‌ها برای تجزیه‌وتحلیل و تصمیم‌گیری عملیاتی بهینه و برتری در رسیدن به اشراف اطلاعاتی.	۹٫۶۵	۱۶
۱۲	کنترل از راه دور تجهیزات و سامانه‌ها.	۱۰٫۲۳	۱۳
۱۳	مدیریت هوشمندانه و خودکارسازی محیط عملیاتی	۱۱٫۱٤	۸
۱٤	انعطاف‌پذیری و امکان اتصال تجهیزات مختلف کوچک و بزرگ با مشخصات مختلف (از حسگرهای بسیار کوچک و ریز گرفته تا یک مرکز داده بزرگ) با اتکا به ویژگی تنوع و گستردگی فیزیکی گره‌ها و قابلیت آن‌ها.	۶٫۸۱	۲۰
۱۵	تقلیل در آسیب‌پذیری و برگشت سریع به حالت عملیاتی سامانه‌های مبتنی بر اینترنت اشیا با اتکا به ویژگی لایه‌بندی و خوشه‌بندی به‌گونه‌ای که آسیب رساندن به یک گره مرکزی موجب اختلال در کارکرد کلی سامانه نخواهد شد.	۱۱٫۹۱	۷
۱۶	جمعیت‌سنجی (جمع‌آوری اطلاعات و آنالیز تحلیل داده‌ای مناسب و کشف مدل‌ها و الگوهای قابل پیش‌بینی رفتارها و عادت‌های جامعه هدف) در حوزه شناسایی سرویس‌های اطلاعاتی مبتنی بر فنّاوری اینترنت اشیا.	۶٫۶۶	۲۲
۱۷	عملیات‌های هک، نفوذ، ایجاد نویز و اختلال، شنود لینک‌های ارتباطی، شنود، مانیتورینگ، آلوده‌سازی تجهیزات، تجهیز از راه و ... سوژه‌های عملیاتی و اشراف اطلاعاتی بر سازمان‌های اطلاعاتی حریف.	۱۰٫۱۱	۱٤
۱۸	نظارت هوشمند به تمام اجزای عملیات و هدایت عملیاتی در بستر اینترنت اشیا (موقعیت نیروهای انسانی، مکان‌یابی خودروهای خودی و حریف، وضعیت سلامتی مأموران و ...)	۱۱٫۹۳	۶
۱۹	کاهش هزینه‌های عملیاتی (کاهش نیروی انسان موردنیاز، جلوگیری از قرارگیری نیروها در معرض تهدید بالقوه، صرفه‌جویی در زمان و نظارت هوشمند و بی‌درنگ محیط عملیاتی از راه دور، کاهش حساسیت‌ها و آسیب‌های ناشی از حضور و آمدورفت نیروی انسانی در صحنه عملیات و ...)	۱۲٫۲۲	۱

ردیف	شرح فرصت	میانگین رتبه‌های فریدمن	رتبه
۲۰	ارتقای توان عملیاتی در مأموریت‌ها و افزایش بهره‌وری (سرعت و دقت و...) اقدام‌های عملیاتی و امنیتی نظیر ورود پنهان، تعقیب و مراقبت، رصد و پایش و ...	۱۲,۲۱	۲
۲۱	مهاجرت از روش‌های سنتی به روش‌های فنّاوری محور در مأموریت‌های امنیتی.	۱۲,۱۰	۵
۲۲	آشنایی با شیوه و شگردهای حریف در استفاده از فنّاوری اینترنت اشیا در مأموریت‌های امنیتی.	۱۲,۲۰	۳

جدول ۷– ترتیب و توالی شاخص‌های اثرگذار در فرضیه فرعی دوم از دیدگاه جامعه آماری

ردیف	شرح تهدید		میانگین رتبه‌های فریدمن	رتبه
تهدیدات ناشی از عدم ورود فنّاوری اینترنت اشیا به سازمان‌های اطلاعاتی				
۱	ناتوانی و عقب‌ماندگی در تقابل با سرویس‌های امنیتی حریف که از فنّاوری اینترنت اشیا بهره می‌برند.		۱۱,٤۱	۱
۲	عقب‌ماندگی از سازمان‌های اطلاعاتی رقیب داخلی و عدم بهره‌برداری از مزیت‌های رقابتی ناشی از فنّاوری اینترنت اشیا نظیر صرفه‌جویی در هزینه، نیروی انسانی، بلادرنگی در عملیات و ...		۱۱,۱۷	۲
تهدیدات ناشی از استفاده دشمن از فنّاوری اینترنت اشیا				
۳	تجهیز مکان‌ها، نرم‌افزارها و سخت‌افزارهای مورداستفاده جاسوسان به‌منظور اطلاع از اقدامات عملیاتی سرویس امنیت ما نظیر ورود پنهان، تعقیب و مراقبت، رصد و پایش.		۱۰,۷۶	٤

ردیف	شرح تهدید		میانگین رتبه‌های فریدمن	رتبه
٤	جمع‌آوری اطلاعات پنهان و شخصی افراد برای اهداف جاسوسی (تجهیز، بدافزار، هک، باج افزار و ...)		۸,۲۶	۲۰
۵	اشراف دشمن بر محیط عملیاتی با رصد و دیده‌بانی مکان‌ها، آمدورفت‌ها، وقایع با جمع‌آوری اطلاعات مبتنی بر اینترنت اشیا از راه دور.		۸,۶۸	۱۷
۶	کنترل از راه دور تجهیزات به‌منظور اهداف تروریستی و ...		۹,۶۹	۱۲
۷	تجهیز یا دست‌کاری سخت‌افزارها یا نرم‌افزارهای اینترنت اشیا برای اهداف سوءِ (جاسوسی، خرابکاری و ...)		۸,٤٤	۱۸
۸	ارتباط با جاسوسان و رهبری عملیات در بستر فنّاوری اینترنت اشیا		۹,۰۵	۱۳
۹	تهدیدات ناشی از استفاده خودی از فنّاوری	وابستگی به فنّاوری و غفلت و فراموشی روش‌های غیر وابسته به فنّاوری و دیگر روش‌های خلاقانه	۷,۶۶	۲۵
افشای تجهیزات و سامانه‌های نرم‌افزاری و سخت‌افزاری اینترنت اشیا، افشای مأموریت و روش عملیات اطلاعاتی				
۱۰		شناسایی ناشی از ابعاد بزرگ تجهیزات	۸,۸٤	۱۵
۱۱		شناسایی الکترونیکی و سیگنالی با تجهیزات شناسایی	۸,۹۹	۱٤
۱۲		افشای عملیات امنیتی با شناسایی تجهیزات نصب‌شده در محل نامناسب به علت محدودیت‌هایی نظیر تأمین منبع تغذیه، بستر ارتباطی و ...	۱۰,۸۲	۳

ردیف	شرح تهدید		میانگین رتبه‌های فریدمن	رتبه
۱۳		تجزیه‌وتحلیل تجهیزات افشاشده که به سامانه خودکشی مجهز نیستند.	۸,۲٤	۲۱
موفق نبودن در مأموریت و عملیات اطلاعاتی-امنیتی به علت عدم کارایی سامانه‌های مبتنی بر اینترنت اشیا				
۱٤		تهدیدات ناشی از ضعف‌ها و محدودیت‌های فنّاوری (ضعیف‌شدن ارتباط، پهنای باند کم، قطع دسترسی اینترنتی، سرعت کم، چالش داده حجیم و...)	۹,۷٤	۱۱
۱۵		استفاده از تجهیزات قدیمی که منجر به عقب‌ماندگی از به‌روزرسانی‌های فنّاوری و درنتیجه ناکارآمدی فنّاوری می‌شود (عدم آگاهی از پیشرفت‌های به‌روز فنّاوری‌های اینترنت اشیا و درنتیجه متناسب با نیازها و پیشرفت‌های فنّاوری، تأمین تجهیزات، به‌کارگیری و پشتیبانی از سامانه‌ها در مأموریت‌ها، انجام نمی‌شود) و در تقابل با دشمن در این حوزه شکست می‌خوریم.	۹,۸۲	۱۰
۱۶		تهدیدات ناشی از تجربه کم کاربران سامانه‌های مبتنی بر اینترنت اشیا (انتخاب محل نصب نامناسب، عدم اطلاع از وضعیت سامانه‌ها از راه دور، عدم آشنایی و شناخت دقیق تجهیزات و ملاحظات کارکردی آن‌ها، استفاده نکردن از چند حسگری و چند مسیری)	۹,۸۶	۹
۱۷		تهدیدات ناشی از فقدان برنامه عملیاتی در به‌کارگیری تجهیزات اینترنت اشیا در فرآیندها و مأموریت‌های عملیاتی و اطلاعاتی	۸,۰۲	۲۲
تهدیدات مرتبط با نیروی انسانی				

ردیف	شرح تهدید		میانگین رتبه‌های فریدمن	رتبه
۱۸		نفوذ بیگانه در نیروی انسانی دارای دسترسی به سامانه‌های مبتنی بر اینترنت اشیا	۷,۷۶	۲٤
۱۹		استفاده شخصی از بسترهای سازمانی مبتنی بر فنّاوری اینترنت اشیا	۷,۹۰	۲۳
۲۰		استفاده نامناسب کارکنان و مدیران از سامانه‌های مبتنی بر اینترنت اشیا به‌صورت عمدی و به علل مختلف که موجب القای عدم کارایی سامانه می‌شود.	۸,۳۱	۱۹
هک و نفوذ در سامانه‌های مبتنی بر اینترنت اشیا و شنود، سرقت اطلاعات، سرقت هویت، تخریب، تغییر، فریب، غیرفعال‌سازی و یا اخلال در کار آن‌ها می‌گردد.				
۲۱		تهدیدهای مبتنی بر نقض امنیت فیزیکی سامانه‌ها	۱۰,٤۷	۵
۲۲		تهدیدهای مبتنی بر نقض حریم خصوصی	۸,۸۳	۱۶
۲۳		تهدیدات مبتنی بر نقض امنیت اطلاعات	۱۰,۲۷	۶
۲٤		تهدیدهای مبتنی بر نقض امنیت شبکه و رایانش ابری	۱۰,۰۲	۸
۲۵		تهدیدهای مبتنی بر نقض امنیت تجهیزات دریافت هوشمند	۱۰,۰۹	۷

جدول ۸– ترتیب و توالی شاخص‌های اثرگذار در فرضیه فرعی سوم از دیدگاه جامعه آماری

ردیف	شرح راه‌کار مدیریتی	میانگین رتبه‌های فریدمن	رتبه
۱	اتخاذ تدابیر لازم برای فرهنگ‌سازی و افزایش سطح دانش، آگاهی و تقویت بنیه علمی کارکنان، تصمیم‌سازان و تصمیم‌گیران سازمانی در خصوص به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های اطلاعاتی-امنیتی.	۱۰,۵۸	۳
۲	افزایش حمایت‌های مسئولان سازمان در خصوص به‌کارگیری فنّاوری اینترنت اشیا.	۱۱,۱۱	۱

ردیف	شرح راه‌کار مدیریتی	میانگین رتبه‌های فریدمن	رتبه
۳	اعزام کارکنان فاوای سازمان‌های امنیتی به دوره‌های تخصصی در خصوص فنّاوری اینترنت اشیا.	۸,۱۵	۱۵
٤	آگاه‌سازی فنی و طراحی دوره‌های آموزشی کوتاه‌مدت و بلندمدت برای ارتقای دانش و آگاهی کاربران سازمان پیرامون فنّاوری اینترنت اشیا.	۹,۰٤	۱۳
۵	تدوین، ابلاغ و اعمال مستمر سیاست‌های امنیتی (طبقه‌بندی داده‌ها و سطوح دسترسی و...) که بایستی توسط کاربران مراعات گردد و برخورد قانونی با تخلفات و شکست‌های احتمالی.	۹,۱۵	۱۱
۶	ایجاد ساختار مناسب و جذب نیروی انسانی متخصص برای راه‌اندازی، توسعه، پشتیبانی، امنیت و کنترل امنیت فنّاوری اینترنت اشیا در سازمان‌های امنیتی.	۱۰,۳۷	۷
۷	طراحی ساختار سازمانی و ایجاد گروه‌های رصد و پایش مستمر و مداوم تهدیدات و آسیب‌های سامانه‌های مبتنی بر فنّاوری اینترنت اشیا بر اساس پیشرفت‌های فنّاوری و در قالب بخش‌های SOC، NOC و Cert به‌منظور واکنش به‌موقع.	۱۰,۵۵	۵
۸	تشکیل گروه‌های کاری متخصص طراحی، اجرا، پشتیبانی مستمر زیرساخت‌ها فنّاوری اینترنت اشیا و واکنش به تهدیدات احصاءِ شده، آزمون نفوذ و ارزیابی امنیتی، ارائه گزارش کار به مسئولان در سازمان‌های امنیتی.	۱۰,۱۵	۸
۹	تدوین نقشه راه (اتخاذ راهبرد، تعیین خط‌مشی، هدف‌گذاری، برنامه‌ریزی، اولویت‌بندی، زمان‌بندی، تعیین برنامه عملیاتی) پیاده‌سازی و به‌کارگیری فنّاوری اینترنت اشیا به‌صورت امن و متناسب با نیاز واقعی سازمان‌های اطلاعاتی-امنیتی.	۱۰,۵۷	٤
۱۰	بازنگری در اسناد بالادستی موجود (آیین‌نامه‌ها) و تدوین شیوه‌نامه‌ها و استانداردهای امنیت و کنترل امنیت پیرامون پیاده‌سازی، به‌کارگیری و توسعه تجهیزات اینترنت اشیا در سازمان‌های اطلاعاتی-امنیتی و نظارت بر حسن اجرای آن از سوی مراجع ذی‌صلاح.	۹,۱۹	۱۰
۱۱	تعامل با سازمان‌های اطلاعاتی داخلی در جهت اشتراک تجارب و تجهیزات، سامانه‌ها، فنّاوری‌ها و رویکردها در حوزه اینترنت اشیا.	۸,۸۷	۱٤
۱۲	برگزاری مستمر کمسیون اثربخشی هوشمندسازی در مأموریت‌های سازمانی و کمیته تخصصی تصمیم‌گیری در خصوص به‌کارگیری صحیح و به‌جا از تجهیزات هوشمند در سازمان‌های امنیتی.	۹,۸۷	۹

ردیف	شرح راه‌کار مدیریتی	میانگین رتبه‌های فریدمن	رتبه
۱۳	آگاه‌سازی عمومی و تخصصی درزمینهٔ حساسیت و گزارش وقایع غیرعادی به سازمان‌های امنیتی نظیر آمدورفت‌ها یا اقدامات غیرعادی در موقعیت‌های زمانی و مکانی عمومی یا خصوصی (مثلاً استقرار در مکان و تجهیز آن به تجهیزات تروریستی).	۹,۰۹	۱۲
۱٤	بررسی مستمر میزان استفاده و بیلان استفاده از سامانه‌های مبتنی بر اینترنت اشیا و ارزیابی اقدامات و بازخوردگیری و تصحیح روندها و سامانه‌ها.	۸,۰۶	۱۶
۱۵	تهیه دستورالعمل مقابله با سطوح مختلف بحران‌های مرتبط با سامانه‌های مبتنی بر اینترنت اشیا.	۱۰,٤۷	۶
۱۶	تأمین اعتبارات مالی موردنیاز برای راه‌اندازی، توسعه، پشتیبانی و امن‌سازی فنّاوری اینترنت اشیا سازمان‌های امنیتی.	۱۰,۹۲	۲

جدول ۹– ترتیب و توالی شاخص‌های اثرگذار در فرضیه فرعی چهارم از دیدگاه جامعه آماری

ردیف	شرح راه‌کار فنّاورانه	میانگین رتبه‌های فریدمن	رتبه
۱	تأمین زیرساخت‌ها، سامانه‌های امنیتی، سامانه‌های کنترلی و ... برای پیاده‌سازی و امن‌سازی فنّاوری اینترنت اشیا در سازمان‌های امنیتی.	۱۱,۰۲	۲
۲	تدبیر و استفاده از روش‌های عملی یا سخت‌افزاری ضد جمع‌آوری غیرمجاز اطلاعات (بستن پورت‌ها، چسب بر روی دوربین گوشی همراه و لب تاپ و ...).	۸,۱۹	۳۳
۳	آزمون نفوذ و ارزیابی امنیتی زیرساخت‌های فنّاوری اینترنت اشیا در سازمان‌های امنیتی.	۱۰,۱۵	۲۱
٤	بررسی و به‌کارگیری راه‌کارهای ضد سامانه‌های مبتنی بر اینترنت اشیا برای خنثی‌سازی اقدامات دشمن و عبور از سامانه‌های نظارتی.	۱۰,۷۵	۵
۵	تدبیر و استفاده از روش‌های نرم‌افزاری ضد نفوذ و جمع‌آوری غیرمجاز اطلاعات (تنظیمات نرم‌افزاری دوربین‌های مداربسته، استفاده از نرم‌افزارهای ضد بدافزار، ضد هک و ...).	۹,۲۹	۲۷
۶	بررسی توانمندی‌ها و رویکردهای سازمان‌های اطلاعاتی- امنیتی حریف در حوزه به‌کارگیری فنّاوری اینترنت اشیا.	۱۰,۹۵	۳

ردیف	شرح راه‌کار فنّاورانه	میانگین رتبه‌های فریدمن	رتبه
۷	تدبیر و استفاده از روش‌های ضد رصد و دیده‌بانی، تصویربرداری و جمع‌آوری سیگنالی (استفاده از جمر، منعکس‌کننده‌های نوری، اخلالگرهای سامانه‌های ارتباطی مختلف و ...) در اماکن مدنظر.	۹,۲۲	۲۸
۸	بررسی و استفاده از روش‌های نفوذ به سامانه‌های مبتنی بر اینترنت اشیا حریف و استفاده در برای شنود، دست‌کاری، تغییر، اخلال و ...آن‌ها.	۸,۷۸	۳۰
۹	پیش‌بینی روش‌های غیر وابسته به فنّاوری اینترنت اشیا و استفاده موازی از آن‌ها در مأموریت‌های اطلاعاتی برای اطمینان و جلوگیری از غافلگیری.	۸,۳٤	۳۲
۱۰	طراحی و تأمین پوشش‌های ضد آشکارساز الکترونیکی برای تجهیزات اینترنت اشیا.	۱۰,۳۲	۱۸
۱۱	اعمال راه‌کارهای به‌روز برای حفاظت الکترومغناطیسی سامانه‌های اینترنت اشیا.	۱۰,۳۷	۱۶
۱۲	طراحی و استفاده از فن‌های ضد آشکارسازی در انتقال اطلاعات در سامانه‌های مبتنی بر اینترنت اشیا (نظیر طیف گسترده و ...).	۱۰,۳۵	۱۷
۱۳	طراحی و استفاده از فن‌های جاسازی تجهیزات در اشیا موجود در صحنه و ایجاد پوشش‌های عادی و غیر حساسیت‌زا.	۹,۶۳	۲۳
۱٤	بررسی و استفاده از روش‌های مدرن تأمین انرژی تجهیزات الکترونیکی نظیر القای الکترونیکی.	۹,۳۷	۲۶
۱۵	استفاده از بسترهای انتقال اطلاعات غیر حساسیت‌زا (نظیر برق شهری).	۹,۸۷	۲۲
۱۶	طراحی و استفاده از راه‌کارهای تجهیز سامانه‌های اینترنت اشیا به سامانه خودکشی برای جلوگیری از سوءاستفاده از تجهیزات افشاشده.	۹,٤۶	۲۵
۱۷	بررسی و اعمال راه‌کارهای پیشرفته و جدید برای حفاظت فیزیکی تجهیزات اینترنت اشیا نظیر پلمپ دست‌یابی ناپذیر تجهیزات برای جلوگیری از دسترسی غیرمجاز.	۷,٤۸	۳٤
۱۸	پیش‌بینی راه‌کارهای استفاده ترکیبی و موازی از تجهیزات و بسترهای ارتباطی برای جلوگیری از تهدیدات ناشی از ضعف‌ها و محدودیت‌های فنّاوری.	۱۰,۳۹	۱۵
۱۹	رصد پیشرفت فنّاوری‌ها و تأمین، طراحی و استفاده از نرم‌افزار، سخت‌افزار و تجهیزات پیشرفته و جدید اینترنت اشیا قابل‌استفاده در مأموریت‌های امنیتی و مهاجرت از سامانه‌های سنتی به سامانه‌های به‌روز و پیشرفته و تجهیزات امروزی.	۱۱,۱۱	۱

ردیف	شرح راه‌کار فنّاورانه	میانگین رتبه‌های فریدمن	رتبه
۲۰	شناسایی شرکت‌های داخلی و خارجی قابل‌اطمینان تأمین‌کننده و ارائه‌دهنده خدمات فنّاوری اینترنت اشیا و دریافت مشاوره از شرکت‌ها و مراکز علمی و دانشگاهی فعال در حوزه فنّاوری اینترنت اشیا برای اطلاع از پیشرفت‌ها و تجهیزات به‌روز.	۷،۴۲	۳۵
۲۱	پیش‌بینی و استفاده از زیرساخت‌های جایگزین و بسترهای موازی بومی (چند حسگری یا چند بستر ارتباطی) برای پایداری شبکه در شرایط بحرانی و جلوگیری از غافلگیری ناشی از افشا یا ازکارافتادن یک حسگر یا بستر ارتباطی.	۱۰،۴۲	۱۴
۲۲	تهیه و تدوین و اجرای روش‌های تهیه نسخه پشتیبان از اطلاعات و آزمایش صحت آن.	۹،۵۴	۲۴
۲۳	استفاده از امکانات کنترل، مانیتورینگ و وقایع‌نگاری وضعیت سخت‌افزارها و نرم‌افزارهای مورداستفاده در بستر اینترنت اشیا و اطمینان از صحت عملکرد آن‌ها.	۱۰،۴۷	۱۳
۴	اجرای آزمایشی به‌کارگیری فنّاوری اینترنت اشیا در قسمت‌های با حساسیت پایین‌تر در سازمان‌های امنیتی.	۸،۵۵	۳۱
۲۵	بررسی و طراحی برنامه عملیاتی به‌کارگیری اینترنت اشیا با توجه به تجهیزات، بسترهای ارتباطی و سامانه‌های در اختیار و شرایط محیطی و موقعیتی عملیات.	۱۰،۳۰	۱۹
۲۶	راه‌اندازی آزمایشگاه ارزیابی امنیتی سخت‌افزارها، نرم‌افزارهای اینترنت اشیا و استخراج آسیب‌پذیری‌ها.	۱۰،۲۷	۲۰
۲۷	طراحی و استفاده از زیرساخت‌های نرم‌افزاری و سخت‌افزاری، کانال‌های ارتباطی بومی به‌منظور پیاده‌سازی، به‌کارگیری و امن‌سازی فنّاوری اینترنت اشیا در سازمان‌های امنیتی.	۱۰،۸۱	۴
۲۸	استفاده از فنّاوری‌های ایمن‌ساز اطلاعات در تمام مراحل (تولید، انتقال، پردازش، ذخیره) نظیر رمزنگاری، پنهان‌نگاری، گمنامی متناسب با سامانه‌ها، بسترهای ارتباطی و شرایط عملیاتی.	۱۰،۵۷	۱۰
۲۹	شناسایی و اعمال سازوکارهای مقابله با تهدیدات مبتنی بر نقض امنیت فیزیکی سامانه‌ها (تسخیر، اخلال، دست‌کاری سامانه و تهدیدهای مرتبط با ریزتراشه‌ها) متناسب با سامانه‌ها، بسترهای ارتباطی و شرایط عملیاتی.	۱۰،۷۱	۶

ردیف	شرح راه‌کار فنّاورانه	میانگین رتبه‌های فریدمن	رتبه
۳۰	شناسایی و اعمال سازوکارهای مقابله با تهدیدات مبتنی بر نقض حریم خصوصی (پیش‌بینی اقدام، شرکت، ترجیحی، مکان‌یابی، نظارت بر تراکنش، ردیابی دیجیتالی) متناسب با سامانه‌ها، بسترهای ارتباطی و شرایط عملیاتی.	۱۰،۵۵	۱۱
۳۱	شناسایی و اعمال سازوکارهای مقابله با تهدیدات مبتنی بر نقض امنیت اطلاعات متناسب با سامانه‌ها، بسترهای ارتباطی و شرایط عملیاتی.	۱۰،۶۲	۷
۳۲	شناسایی و اعمال سازوکارهای مقابله با تهدیدات مبتنی بر نقض امنیت شبکه و رایانش ابری متناسب با سامانه‌ها، بسترهای ارتباطی و شرایط عملیاتی.	۱۰،۵۸	۹
۳۳	شناسایی و اعمال سازوکارهای مقابله با تهدیدات مبتنی بر نقض امنیت تجهیزات دریافت هوشمند (غیرفعال کردن غیرمجاز برچسب‌ها (تهدید اعتبار)، شبیه‌سازی غیرمجاز برچسب (تهدید صحت)، مسیریابی غیرمجاز برچسب (تهدید محرمانگی)، حمله بازپخش (تهدید دسترس‌پذیری)، حملات فیزیکی، تهدید فروریختن گودال، تکرار گره، شنود) متناسب با سامانه‌ها، بسترهای ارتباطی و شرایط عملیاتی.	۱۰،۶۰	۸
۳٤	شناسایی و اعمال سازوکارهای مقابله با تهدیدات فنّاوری‌های توانمندساز اینترنت اشیا (رایانش ابری، رایانش مه، داده حجیم، یادگیری ماشین، شبکه‌های حسگر بیسیم، سرویس مکان‌یابی، بلاک چین، واقعیت افزوده و واقعیت مجازی).	۱۰،۵۲	۱۲
۳۵	تهیه مدل مفهومی و اعمال معماری بومی و امن برای پیاده‌سازی اینترنت اشیا در سازمان‌های اطلاعاتی متناسب با امکانات و شرایط حاکم.	۸،۸۷	۲۹

نتیجه‌گیری

بررسی‌های انجام‌شده نشان‌داد که به سه علت عمده ۱- بهره‌مندی از مزیت‌های استفاده از فنّاوری اینترنت اشیا و ۲- جلوگیری از عقب‌افتادگی از دیگر سازمان‌های اطلاعاتی داخلی و ۳- جلوگیری از ناتوانی و عقب‌ماندگی در تقابل با سرویس‌های امنیتی حریف که از فنّاوری اینترنت اشیا بهره می‌برند، سازمان‌های امنیتی بایستی از فنّاوری‌های نو نظیر فنّاوری اینترنت اشیا استفاده کنند. ازاین‌رو، در این پژوهش برای " تبیین فرصت‌ها، تهدیدات و راه‌کارهای مقابله‌ای به‌کارگیری اینترنت اشیا در سازمان‌های امنیتی"، ابتدا فرصت‌ها (۲۲ مؤلفه) و تهدیدات به‌کارگیری فنّاوری اینترنت اشیا (۲۵ مؤلفه) استخراج شدند و در ادامه، راه‌کارهای مقابله‌ای نیز در دودسته ۱- راه‌کارهای مدیریتی (۱۶ مؤلفه) و ۲- راه‌کارهای فنّاورانه (۳۵ مؤلفه) مطرح و موردبررسی قرار گرفتند.

تجزیه‌وتحلیل فرضیه‌ها با استفاده از آزمون خی‌دو نشان‌داد که بین فراوانی‌های مشاهده‌شده برای

مؤلفه‌های هر سه حوزه مذکور، تفاوت معنی‌داری وجود دارد و می‌توان گفت مؤلفه‌های مطرح شده برای هر حوزه ایفای نقش می‌کنند. رتبه‌بندی عوامل مؤثر بر فرضیه‌ها با استفاده از آزمون فریدمن نیز نشان‌داد که تفاوت بین میانگین‌های رتبه‌ای مؤلفه‌های هر حوزه معنی‌دار است. میانگین رتبه‌های آزمون فریدمن که ترتیب و توالی اهمیت مؤلفه‌های اثرگذار در فرضیه‌ها را از دیدگاه جامعه آماری مشخص می‌کند، نشان‌داد که:

۱) از میان مؤلفه‌های مربوط به فرصت‌های به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی (۲۲ مؤلفه)، سه مؤلفهٔ زیر به ترتیب بالاترین رتبه‌ها را به خود اختصاص داده‌اند:

۱- کاهش هزینه‌های عملیاتی (با میانگین رتبه‌ای فریدمن ۱۲/۲۲)

۲- ارتقای توان عملیاتی در مأموریت‌ها و افزایش بهره‌وری (با میانگین رتبه‌ای فریدمن ۱۲/۲۱).

۳- آشنایی با شیوه و شگردهای حریف مبتنی بر فنّاوری اینترنت اشیا، مدیریت هوشمندانه محیط عملیاتی (با میانگین رتبه‌ای فریدمن ۱۲/۲۰).

۲) از میان مؤلفه‌های مربوط به تهدیدات به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی (۲۵ مؤلفه)، سه مؤلفهٔ زیر به ترتیب بالاترین رتبه‌ها را به خود اختصاص داده‌اند:

۱- ناتوانی و عقب‌ماندگی در تقابل با سرویس‌های امنیتی حریف که از فنّاوری بهره می‌برند (با میانگین رتبه‌ای فریدمن ۱۱/۴۱).

۲- عقب‌ماندگی از دیگر سازمان‌های اطلاعاتی داخلی (با میانگین رتبه‌ای فریدمن ۱۱/۱۷).

۳- افشای عملیات امنیتی با شناسایی تجهیزات نصب‌شده در محل نامناسب به علت محدودیت‌هایی نظیر تأمین منبع تغذیه، بستر ارتباطی و ... (با میانگین رتبه‌ای فریدمن ۱۰/۸۲).

۳) از میان مؤلفه‌های مربوط به راه‌کارهای مدیریتی به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی (۱۶ مؤلفه)، سه مؤلفهٔ زیر به ترتیب بالاترین رتبه‌ها را به خود اختصاص داده‌اند:

۱- افزایش حمایت‌های مسئولان سازمان در خصوص به‌کارگیری فنّاوری اینترنت اشیا (با میانگین رتبه‌ای فریدمن ۱۱/۱۱).

۲- تأمین اعتبارات مالی موردنیاز برای راه‌اندازی، توسعه، پشتیبانی و امن‌سازی فنّاوری اینترنت اشیا سازمان‌های امنیتی. (با میانگین رتبه‌ای فریدمن ۱۰/۹۲).

۳- اتخاذ تدابیر لازم برای فرهنگ‌سازی و افزایش سطح دانش، آگاهی و تقویت بنیه علمی کارکنان، تصمیم‌سازان و تصمیم‌گیران سازمانی در خصوص به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های اطلاعاتی-امنیتی (با میانگین رتبه‌ای فریدمن ۱۰/۵۸).

۴) از میان مؤلفه‌های مربوط به راه‌کارهای فنّاورانه به‌کارگیری فنّاوری اینترنت اشیا در سازمان‌های امنیتی

(۳۵ مؤلفه)، سه مؤلفهٔ زیر به ترتیب بالاترین رتبه‌ها را به خود اختصاص داده‌اند:

۱- رصد پیشرفت فنّاوری‌ها و تأمین، طراحی و استفاده از نرم‌افزار، سخت‌افزار و تجهیزات پیشرفته و جدید اینترنت اشیا (با میانگین رتبه‌ای فریدمن ۱۱/۱۱).

۲- تأمین زیرساخت‌ها، سامانه‌های امنیتی، سامانه‌های کنترلی و ... برای پیاده‌سازی و امن‌سازی فنّاوری اینترنت اشیا (با میانگین رتبه‌ای فریدمن ۱۱/۰۲).

۳- بررسی توانمندی‌ها و رویکردهای سازمان‌های اطلاعاتی- امنیتی حریف در حوزه به‌کارگیری فنّاوری اینترنت اشیا (با میانگین رتبه‌ای فریدمن ۱۰/۹۵).

منابع:

- رمضانی رسول، موحدی صفت محمدرضا، **رتبه‌بندی تهدیدهای اینترنت اشیا در محیط نظامی**، فصلنامه علمی امنیت ملی، مقاله هفتم، ۱۴۰۰.
- سهرابی شهلا، سلیمی غلامرضا، **ظهور اینترنت اشیا و ضرورت حکمرانی داده**، دومین همایش ملی حکمرانی اسلامی، دانشگاه و پژوهشگاه عالی دفاع ملی و پژوهش‌های راهبردی، تهران، ۱۳۹۹.
- شامی زنجانی مهدی، **اینترنت اشیا؛ روند توسعه، زنجیره ارزش و کاربردها، اجلاس بین‌المللی تحول دیجیتال**، دانشکده مدیریت، دانشگاه تهران، ۱۳۹۶.
- طهماسبی لیمونی صفیه، قاسمی شهرزاد، قربانلو رقیه، **شناسایی تهدیدها و آسیب‌پذیری‌های رایج در فضای اینترنت اشیا و ارائه راهکارهای امنیتی برای مواجهه با آن‌ها**، فصلنامه دانش‌شناسی، علوم کتابداری و اطلاع‌رسانی و فنّاوری اطلاعات، دانشگاه آزاد اسلامی واحد تهران شمال، ایران، سال دوازدهم، شماره ۴۴، ۱۳۹۸.
- عطاریان آیه، **پارادایم امنیت در پلت فرم اینترنت اشیا**، ششمین همایش پژوهش‌های نوین در علوم و فنّاوری، کرمان، ۱۳۹۵.
- کریمی قهرودی، محمدرضا؛ کیان‌خواه احسان، **چالش آفرینی اینترنت اشیا بر ارکان امنیت ملی کشور**، فصلنامه امنیت ملی، سال چهارم، شماره ۱۶، ۱۳۹۴.
- قیصری، محمد. یزدان نژاد، فاطمه. عرب، سعید رضا. رضایی، کیاناز، **استانداردها و چالش‌های اینترنت اشیا**، انتشارات علوم رایانه. مرکز پژوهش‌های اینترنت اشیا ایران، ۱۳۹۸.
- خدابنده بهار، خدابنده پوریا، وحدت داود، **شناسایی حملات، تهدیدات و آسیب‌پذیری‌های امنیتی اینترنت اشیا و طبقه‌بندی تهدیدات**، شانزدهمین اجلاس بین‌المللی مهندسی صنایع ایران، دانشگاه الزهرا، بهمن ۱۳۹۸.
- رهسپار فرد خیرالله، مولایی رضا، **بررسی چالش‌های اینترنت اشیا با استفاده از روش مدل‌سازی ساختاری تفسیری**، فصلنامه علوم و فنون مدیریت اطلاعات، سال چهارم، شماره ۴، شماره پیاپی ۱۳، ۱۳۹۷.
- آقایی طوق مسلم، ناصر مهدی، **چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایرانی و اتحاد اروپا**، فصلنامه حقوق اداری، سال هفتم، شماره ۲۳، ۱۳۹۹.
- اکراقلی‌پور مائده، خداوردی فهیمه، صفا رامین، **بررسی ارتباط رایانش ابری، کلان داده و اینترنت اشیا، سومین اجلاس ملی توسعه علوم مهندسی**، مؤسسه آموزش عالی آیندگان، تنکابن، ایران، ۱۳۹۵.
- باغبان اورندی محمود، **وضعیت فنّاوری اینترنت اشیا در ایران**، معاونت راهبری فنی، مرکز ملی فضای مجازی، ۱۳۹۹.
- بهشتی آتشگاه محمد، برتری مرتضی، عارف محمدرضا، بیات مجید، **اینترنت اشیای نظامی: مفهوم و چالش‌های امنیتی**، نهمین اجلاس ملی فرماندهی و کنترل ایران، تهران، دانشگاه خوارزمی. انجمن علمی فرماندهی و کنترل ایران، ۱۳۹۷.
- رفیقی مسعود، معتضدی نغمه، **بررسی پروتکل‌ها و استانداردهای اینترنت اشیا در لایه‌های مختلف**، مجتمع برق و کامپیوتر دانشگاه صنعتی مالک اشتر تهران، ایران، ۱۳۹۸.

- پورشایسته فرد سید علیرضا، امیدی مهدی، **بررسی امنیت در اینترنت اشیا با استفاده از راه‌کارهای فنّاوری بلاک چین**، هشتمین همایش سالانه بانکداری الکترونیک و نظام‌های پرداختی، تهران، مرکز همایش‌های بین‌المللی برج میلاد، ۱۳۹۶.
- علایی محمدباقر، بهزادی رکسانا، **مدیریت داده‌های خانه‌های هوشمند مبتنی بر اینترنت اشیا با بهره بردن از فن‌های داده‌کاوی**، چهارمین اجلاس بین‌المللی مطالعات نوین در علوم کامپیوتر و فنّاوری اطلاعات، مشهد، دانشگاه صنعتی سجاد، ۱۳۹۶.
- اسمعیل‌پور سعیده، خوب‌بین خوش‌نظر سید محمد، عندلیب اعظم، **تأثیر اینترنت اشیای اجتماعی بر هوشمند کردن بازاریابی‌های اینترنتی**، دومین اجلاس بین‌المللی وب‌پژوهی، جهاد دانشگاهی، دانشگاه علم و فرهنگ، ۲۰۱۶.
- قهرمان‌خانی بهنام، امیری اکرم، **کاربردها و چالش‌های اینترنت اشیا**، سومین اجلاس بین‌المللی الکترونیک و مهندسی کامپیوتر، ۲۰۱۶.
- غلام‌نژاد پژمان، غلامی محمود، پورمکاری علیرضا، **کاربردهای نظامی اینترنت اشیا با تأکید بر مأموریت‌های نیروی هوایی ارتش جمهوری اسلامی ایران**، فصلنامه علوم و فنون نظامی، سال پانزدهم، شماره ۴۹، پاییز ۱۳۹۸.
- بهرامی زنوز پرستو، فقیهی، البرزی محمود، **شناسایی و اولویت‌بندی عوامل مؤثر بر کاربرد اینترنت اشیا در دولت باز**، فصلنامه خط‌مشی گذاری عمومی در مدیریت، سال یازدهم، شماره ۳۷، ۱۳۹۹.
- خاقانی‌فرد جلال، حسن‌زاده قاسمی رضا، **افزایش امنیت و هوشمندسازی خانه‌ها با استفاده از فنّاوری اینترنت اشیا**، دوازدهمین اجلاس ملی علوم و مهندسی کامپیوتر و فنّاوری اطلاعات، مازندران، مؤسسه علم‌آوران دانش، ۱۴۰۰.
- زرگر سید محمد، **ارزیابی موانع به‌کارگیری اینترنت اشیا در کتابخانه‌های ایران بر اساس یک رویکرد ترکیبی**، پژوهش‌نامه پردازش و مدیریت اطلاعات، دوره ۳۴، شماره ۳، صفحه ۱۳۹۸-۱۳۷۱، ۱۳۹۸.
- لک بهزاد، **راهبردهای به‌کارگیری اینترنت اشیا در مأموریت‌های پلیس آگاهی**، فصلنامه پژوهش‌های مدیریت انتظامی، ۱۵ (۱)، ۱۳۹۹، صفحه ۱۰۰-۷۵.
- حق روستا طاهره، **نگاهی به اینترنت اشیا (*IoT*): برنامه‌ها، چالش‌ها و فرصت‌ها با دیدگاه چین**، شرکت ارتباطات زیرساخت، دفتر مدیریت استراتژیک و کسب‌وکارهای نوین، تهران، ایران، ۱۳۹۸.
- حسین‌پور بهروز، اوسطی عراقی نفیسه، بهرامی شیرین، **اینترنت اشیا: یکپارچگی فنّاوری‌ها برای محیط‌های هوشمند، دومین اجلاس ملی فنّاوریهای نوین در مهندسی برق و کامپیوتر**، دانشگاه آزاد اسلامی اراک، مرکزی، ایران، ۱۳۹۷.
- سخایی محمدجواد، **اینترنت اشیا و ضرورت انتخاب یک پلتفرم مناسب داده**، مدیر گروه فابک (فنّاوری اطلاعات برای کسب‌وکار)، ۱۳۹۴، *http://www.fabak.ir*.
- باقری منش محمد، غلامی محمود، کاویانی حسن، **امکان‌سنجی پیاده‌سازی فنّاوری اینترنت اشیا در آماد یک سازمان دفاعی**، فصلنامه علوم و فنون نظامی، سال ۱۵، شماره ۴۸، ۱۳۹۸، صفحه ۵-۲۵.
- تاج نسرین، ترکمن عاطفه و معدنی افسانه، **طبقه‌بندی موضوعات اینترنت اشیا و درجه‌بندی حساسیت آن‌ها**، تهران، پژوهشگاه ارتباطات و فنّاوری اطلاعات وزارت ارتباطات و فنّاوری اطلاعات، ۱۳۹۶.

- *AbdulGhani, H; Konstantas D. & Mahyoub M, "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.*
- *Tweneboah, K.S; Skouby, K.E. & Tadayoni R, "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.*
- *Tasneem, Y; Rwan, M; Fadi, A. & Imran, Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures, International Journal for Information Security Research (IJISR), 2015, Volume 5, Issue 4, P. 47-55.*
- *Sattarian, M, Rezazadeh, J, Farahbakhsh, R. et al. Indoor navigation systems based on data mining techniques in internet of things: a survey. Wireless Netw 25, 1385–1402, 2019.*
- *Staalduinen, M. & van, J, THE IoT SECURITY LANDSCAPE. Cyber Security Agency of Singapore, Ministry of Economic Affairs and Climate Policy of the Netherlands, 2019.*
- *White G, Cabrera C, Palade A, Clarke S, Augmented Reality in IoT. In: Liu X. et al. (eds) Service-Oriented Computing – ICSOC 2018 Workshops. ICSOC 2018. Lecture Notes in Computer Science, vol 11434. Springer, Cham. https://doi.org/10.1007/978-3-030-17642-6_13.*
- *Masoodi, F; Alam, S. & Siddiqui S.T, 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, "Security Challenges and Approaches in Internet of Things". Springer International Publishing AG Switzerland, pp. 25-38, 2017.*
- *Subramanian Balaji, Eanoch Golden Julie, Yesudhas Harold Robinson, Raghvendra Kumar, Pham Huy Thong, Le Hoang Son, Design of a security-aware*

routing scheme in Mobile Ad-hoc Network using repeated game model, Computer Standards & Interfaces, Volume 66, 2019, 103358, ISSN 0920-5489.

- L. Xie, Y. Ding, H. Yang and X. Wang, "Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs," in IEEE Access, vol. 7, pp. 56656-56666, 2019
- Tawalbeh, L; Muheidat, F; Tawalbeh, M; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. Appl. Sci. 2020, 10, 4102.
- El-hajj, M; Fadlallah, A; Chamoun, M; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. Sensors 2019, 19, 1141.
- R. K. Shrivastava, S. Mishra, V. E. Archana and C. Hota, "Preventing data tampering in IoT networks," 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), GOA, India, 2019, pp. 1-6.
- M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah and M. Gidlund, "A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8462-8471, Sept. 2020.