

ارائه یک چارچوب مفهومی برای دسته‌بندی تهدیدهای امنیتی در اینترنت اشیا

حمیدرضا خدمتگزار^{۱*}، ساناز قربانلو^۲

^۱ استادیار پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، khedmatgozar@irandoc.ac.ir

^۲ پژوهشگر پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، sghorbanloo@gmail.com

چکیده: یکی از موضوعات مهم در حوزه اینترنت اشیا، مدیریت مخاطرات امنیت اطلاعات است. یکی از اقدامات کلیدی در این حوزه، شناسایی و تحلیل تهدیدهای امنیتی اینترنت اشیا است. در این مطالعه مبتنی بر مرور پیشینه و نظر متخصصان چارچوب مفهومی پیشنهادی به منظور دسته‌بندی تهدیدهای امنیتی حوزه اینترنت اشیا ارائه شده است. مبتنی بر این چارچوب تهدیدهای حوزه اینترنت اشیا بر پایه معیار انگیزه‌های حملات احتمالی و نوع صدمه به قربانی، در سه دسته اصلی شامل تهدیدهای امنیتی سیستم (شامل سه دسته تهدیدهای دستکاری، اختلالی و تصرفی)، حریم خصوصی (شامل چهار دسته تهدیدهای نظارت ناخواسته/ غیرقانونی، نمایه‌سازی کاربر، نفوذ فعال، و رد پای ماندگار)، و اعتماد انعکاسی و شهرت (شامل سه دسته تهدیدهای سوءرفتار موجودیت‌های وابسته، سوءاستفاده از کالا یا خدمات، و ارائه نادرست) جای گرفتند. این چارچوب مفهومی پیشنهادی می‌تواند مورد استفاده پژوهشگران و متخصصان حوزه مدیریت مخاطرات امنیت اطلاعات در حوزه اینترنت اشیا قرار گیرد.

کلیدواژه‌ها: اینترنت اشیا، امنیت اطلاعات، تهدید

۱- مقدمه

یک مسأله مدیریتی است. مدیریت مؤثر تهدیدهای مرتبط با اینترنت اشیا، نیازمند ارزیابی کامل از مخاطرات باتوجه به محیط و تدوین برنامه‌ای برای کاهش تهدیدهای شناسایی شده است. از این‌رو، در این مقاله سعی شده است تا با تحلیل فضاهای تهدید مشخص، یک دسته‌بندی کاربردی در قالب یک چارچوب مفهومی از تهدیدهای اینترنت اشیا ارائه شود. در ادامه و در بخش دوم، مفاهیم مرتبط با چارچوب اینترنت اشیا، امنیت در اینترنت اشیا و مفهوم تهدید معرفی خواهند شد؛ سپس در بخش سوم، روش پژوهش را بررسی کرده و در بخش چهارم، چارچوب مفهومی پیشنهادی ارائه خواهد شد و در نهایت در بخش پایانی، نتایج پژوهش مورد بررسی قرار خواهند گرفت.

۲- مبانی نظری پژوهش

۲-۱- اینترنت اشیا

اینترنت اشیا، به اشیا یا به‌طور منحصربه‌فرد قابل شناسایی هستند و نمایش مجازی آن‌ها در ساختاری مانند اینترنت شکل می‌گیرد، اشاره دارد [۳][۴][۵]. عبارت اینترنت اشیا نخستین بار توسط کوین اشتون در سال ۱۹۹۹ و دیوید ال بروک در سال ۲۰۰۱ مطرح شد [۶][۷]. در جدول ۱ تعاریف متفاوتی از منابع مختلف نقل شده است. با درنظرگرفتن این جدول، اینترنت اشیا را می‌توان به عنوان پارادایمی فراگیر در محیط‌های متنوع از اشیا

اینترنت اشیا با سرعت خیلی زیادی در حال رشد است. بنابراین دور از ذهن نیست که در آینده‌ای نزدیک در انتظار یک دنیای فوق‌العاده متصل باشیم. همان‌طور که اینترنت اشیا گسترشی از معماری اینترنت است، بسیاری از مسائل دیگر مانند امنیت و حریم خصوصی نیز توسط اینترنت اشیا از اینترنت به ارث گرفته شده است [۱]. طبیعی است که ایجاد چنین شبکه‌ای، مخاطرات فراوانی را به همراه دارد. از دیدگاه کاربران شبکه جهانی اینترنت که از همگانی شدن آن سال‌ها می‌گذرد، هنوز دارای ضعف‌های امنیتی بسیاری است که موجب به خطر افتادن اموال و حتی جان انسان‌ها نیز شده است [۲].

در چنین شرایطی، برقراری امنیت در یک شبکه جهانی از اشیا که هر کدام با ویژگی‌ها و محدودیت‌های خود به ارتباط با یکدیگر و با انسان‌ها می‌پردازند، طبیعتاً از پیچیدگی بسیار بالاتری برخوردار خواهد بود. شرایط جدید محیط و ویژگی‌های مختلف دستگاه‌ها، سبب می‌شود تا امنیت اینترنت اشیا به طور ویژه موردتوجه قرار گیرد.

اینترنت اشیا با تهدیدهای امنیتی جدیدی همراه است که وضعیت کلی مخاطره امنیت اطلاعات را تغییر می‌دهد. اگرچه بکارگیری راه‌حل‌های فناورانه ممکن است به تهدیدها و آسیب‌پذیری‌های اینترنت اشیا پاسخ دهد، اما امنیت اینترنت اشیا در درجه اول

۲-۳- تهدید

در چارچوب اینترنت، تهدید (یا تهدید سایبری) به عنوان "احتمال تلاش مخرب برای مختل کردن یا تخریب یک شبکه یا سیستم رایانه‌ای" تعریف شده است [۱۲]. از دیدگاه امنیت سیستم و اطلاعات، تهدید یک موجودیت (شیء، شخص یا شرایط) است که عمداً یا غیرعمد خطری برای سیستم ایجاد می‌کند [۱]. تعریف تهدید برای اینترنت اشیا می‌تواند شکل گسترده این تعریف باشد. فضای یکپارچه سایبری-فیزیکی، پیامدهای تهدیدهای اینترنت اشیا را حتی شدیدتر می‌کند، زیرا تحقق آن‌ها ممکن است جهان فیزیکی را نیز تحت تأثیر قرار دهد [۱].

۳- روش پژوهش

به منظور شناسایی چارچوب تهدیدهای اینترنت اشیا، دو گام اصلی مدنظر قرار گرفت. در گام اول مبتنی بر مرور پیشینه چارچوبی اولیه از تهدیدهای اینترنت اشیا بدست آمد. در گام دوم نیز با برگزاری دو جلسه مصاحبه گروه متمرکز با دو گروه متخصصان حوزه‌های اینترنت اشیا و همچنین امنیت اطلاعات و سپس تحلیل محتوا، چارچوب پیشنهادی مورد اعتباریابی قرار گرفت و نهایی شد.

۴- چارچوب پیشنهادی

در این چارچوب مفهومی تهدیدها براساس معیار انگیزه‌های حملات احتمالی و نوع صدمه به قربانی دسته‌بندی شده‌اند. شکل ۱ چارچوب تهدید پیشنهادی در حوزه اینترنت اشیا را به تصویر

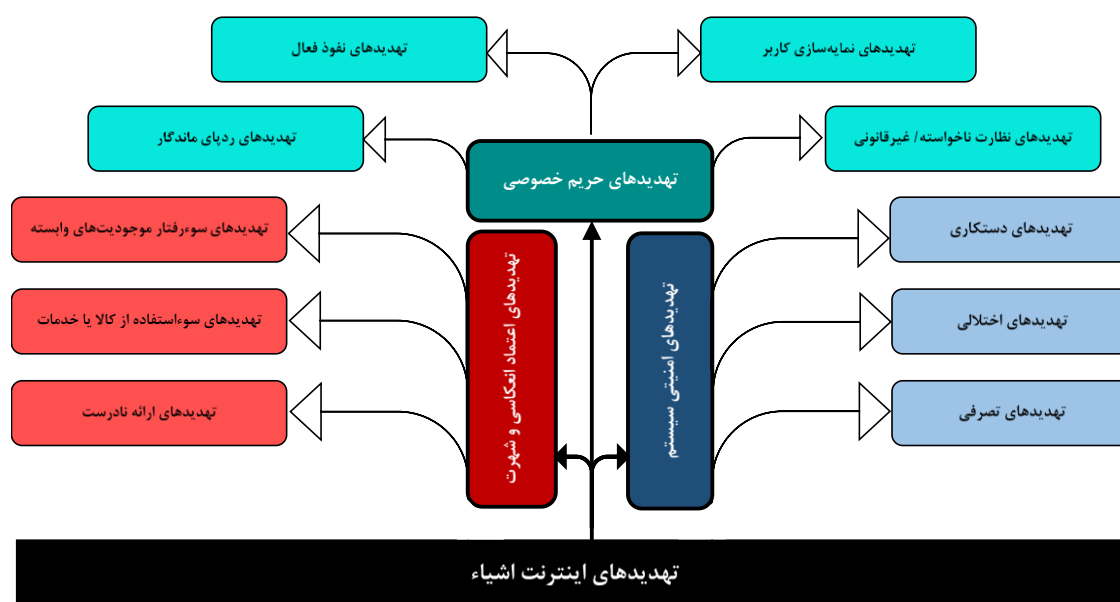
تعریف کرد که از طریق بی‌سیم و یا باسیم قادر به تعامل و همکاری با سایر اشیا متصل شده به‌منظور ایجاد ارتباطات یکپارچه و ارائه خدمات بافت‌آگاه و نیل به اهداف مشترک باشند.

جدول ۱ تعاریف اینترنت اشیا

منبع	تعریف
[۸]	اشیا دارای هویت و شخصیت‌های مجازی هستند که در فضای هوشمند با استفاده از واسطه‌های هوشمند برای اتصال و ارتباط در بافت‌های اجتماعی، محیط زیستی و کاربری فعالیت می‌کنند.
[۹]	از لحاظ معنایی، اینترنت اشیا به معنای یک شبکه جهانی گسترده از اشیا متصل شده و به‌طور یکتا قابل شناسایی، براساس پروتکل‌های ارتباطی استاندارد است.
[۱۰]	اینترنت اشیا به مردم و اشیا این امکان را می‌دهد که در هر زمان و مکانی با هر شیء و شخصی، در حالت ایده‌آل با استفاده از هر مسیر یا شبکه و هر سرویسی، در ارتباط باشند.
[۱۱]	اینترنت اشیا به نمایش مجازی انواع مختلفی از اشیا در اینترنت و یکپارچگی آن‌ها در اینترنت یا سرویس‌های مبتنی بر وب می‌پردازد.

۲-۲- امنیت در اینترنت اشیا

در اینترنت اشیا، اصطلاح امنیت شامل طیف گسترده‌ای از مفاهیم است که شامل مؤلفه‌های اساسی محرمانگی، احراز هویت، صحت، مجوز، عدم انکار و حتی دسترس‌پذیری اطلاعات و سیستم را نیز دربرمی‌گیرد [۱]. همچنین برخی از مفاهیم مانند تشخیص تکراری و به موقع بودن را نیز شامل می‌شود [۱۱].



شکل ۱: چارچوب مفهومی پیشنهادی دسته‌بندی تهدیدهای اینترنت اشیا

اشیا باشد. در این حالت، حتی اگر محیط داخلی اینترنت اشیا امن و کارآمد باشد، نگرانی‌های امنیتی همچنان ممکن است به دلیل اقدامات سیستم صحیح براساس اطلاعات نادرست افزایش یابند. برای مثال در یک سیستم گرمایش مرکزی برای یک خانه، کسی می‌تواند چرخه تصمیم‌گیری کنترل‌کننده را به سادگی با نگه داشتن یک فندک روشن در مقابل سنسورهای ترموستات، برای تشخیص و گزارش افزایش دمای غیرطبیعی تغییر دهد. براساس اطلاعات نادرست دریافت شده از این سنسور، کنترل‌کننده ممکن است دمای خانه را به شدت کاهش دهد تا دمای موردنیاز را حفظ کند. شکل نهایی تهدیدهای دستکاری زمانی خواهد بود که یکپارچگی و صحت داده‌های انتقالی بین دو موجودیت، به دلیل دخالت غیرمجاز دستکاری می‌شود. حملاتی مانند حمله شخص میانی^۱، بازپخش^۲ و جعل^۳، تهدیدهایی برای یکپارچگی و صحت داده هستند.

تهدیدهای حریم خصوصی شامل پنهان‌سازی اطلاعات شخصی و همچنین توانایی کنترل آنچه با این اطلاعات اتفاق می‌افتد، است [۱۵]. براساس گزارش منتشرشده از سوی [۱۶] در ارتباط با تعاریف حریم خصوصی، [۱] تهدید حریم خصوصی را به عنوان یک رویداد احتمالی از افشای اطلاعات حساس به موجودیت‌هایی (شخص، شرکت، یا هوش مصنوعی) تعریف می‌کند که مجاز به داشتن آن نیستند یا نیازی به داشتن آن ندارند. این می‌تواند به شکل داده‌های غلط در اختیار موجودیت‌های غیرمجاز یا داده‌های بیشمار در اختیار موجودیت‌های مجاز باشد. تهدیدهای حریم خصوصی ممکن است بر صاحب واقعی داده تأثیر جدی و مؤثری نداشته باشند. در چارچوب پیشنهادی چهار نوع تهدید در این دسته جای گرفته‌اند که در ادامه شرح داده خواهد شد.

تهدیدهای نظارت ناخواسته/غیرقانونی، اینترنت اشیا می‌تواند به راحتی توسط یک گروه مخرب برای نظارت غیرقانونی مورد سوءاستفاده قرار گیرد. برای مثال یک فرد خرابکار می‌تواند از طریق دوربین‌هایی که در اسباب‌بازی‌ها نصب شده‌اند بر کودکان نظارت کند، حرکت افراد را از طریق سیستم تعبیه شده در کفش‌های هوشمند آنان رصد کند، و یا ورود و خروج اعضای یک خانواده را با متصل شدن به قفل درب خانه متصل به اینترنت و استفاده از منبع برق از طریق کنترل‌کننده‌های هوشمند تشخیص دهد.

تهدیدهای نمایه‌سازی کاربر می‌تواند به عنوان جمع‌آوری، تطبیق و

کشیده است. همان‌طور که در شکل نشان داده شده است، سه دسته کلی از تهدیدهای مطرح برای اینترنت اشیا پیشنهاد شده است که در ادامه شرح داده خواهد شد:

تهدیدهای امنیتی سیستم، هر فعالیت بالقوه‌ای که ممکن است به صورت عمدی یا غیرعمدی ارکان امنیت را نقض کند و اشیا را به صورت فردی یا کل یک شبکه را به خطر بیاندازد به عنوان یک تهدید امنیتی سیستم برای اینترنت اشیا شناخته می‌شود [۱]. با الهام از [۱۳]، تهدیدهای امنیتی سیستم را می‌توان براساس اهداف حملات سایبری به سه دسته تهدیدهای تصرفی، تهدیدهای اختلالی و تهدیدهای دستکاری دسته‌بندی کرد.

تهدیدهای تصرفی، شامل تهدیدهایی است که منجر به کنترل مهاجم بر یک بخش فیزیکی یا منطقی زیرساخت اینترنت اشیا یا دسترسی به اطلاعاتی که در سیستم ذخیره می‌شود، خواهد شد. تهدیدهای تصرفی ممکن است خسارت فوری یا مستقیم بر قربانی نداشته باشند. با این وجود، مفاهیم ضروری امنیت، یعنی محرمانگی داده (کسب‌وکار کنترل) و استفاده برای افراد دارای دسترسی مجاز را نقض می‌کند. علاوه‌براین، چنین کنترل یا دسترسی غیرمجازی، شانس تهدیدها شدیدتر و فعال‌تر، مانند اختلال، تخریب، انکار یا تخریب عملکرد هدف را بیشتر می‌کند. برای مثال، اگر مهاجم کنترل یک کنترل‌کننده شبکه هوشمند را در دست بگیرد، می‌تواند اطلاعات مربوط به مصرف برق هر مکان یا حتی تک‌تک لوازم منزل را مشاهده کند. در حقیقت، افشای اطلاعات خصوصی مانند الگوهای مصرف برق هر وسیله خانگی ممکن است مهاجم را قادر سازد تا به راحتی از اطلاعات برای اهداف مخرب استفاده کند.

تهدیدهای اختلالی شامل تهدیدهای مستقیمی است که از طریق حملات به منظور اختلال، تضعیف، انکار سرویس و نابودکردن سیستم هدف، باعث آسیب‌رساندن به سیستم و ذی‌نفعان می‌شود. برای مثال اگر کنترل‌کننده هوشمند شبکه توسط یک مهاجم تصرف شود، می‌تواند با تغییر عملکرد شبکه هوشمند، باعث اختلال در سیستم توزیع برق یا سیستم شارژ شود، یا باعث خراب‌کاری در منبع تغذیه برق شود، و یا حتی کل سیستم را خاموش کند.

تهدیدهای دستکاری شامل تهدیدهای اثرگذار بر چرخه تصمیم‌گیری هدف است [۱۴]. در حقیقت یک تهدید دستکاری ممکن است خراب کردن داده قبل از ورود به سیستم اینترنت

^۳ Spoofing attack^۱ Man-in-the-middle attack^۲ Replay attack

موجودیت واقعی که به نادرستی نمایانده شده است، دچار خدشه می شود. این نوع تهدید مشابه حملات فیشینگ در تعاملات وب است [۱۷]. در یک حمله فیشینگ، مهاجم تلاش می کند تا اطلاعات حساس (مانند اطلاعات ورودی، جزئیات کارت اعتباری) را با وانمود کردن اینکه یک موجودیت قابل اعتماد است، به دست آورد. کاربران قربانی از طریق ارتباطاتی که ادعا می شود از وبسایت های اجتماعی، مؤسسات مالی و یا پورتال پرداخت آنلاین معتبر، هستند مورد کلاهبرداری قرار می گیرند.

تهدیدهای سوءاستفاده از کالا یا خدمات، اعتبار یک ارائه دهنده خدمات همچنین می تواند توسط استفاده از خدمات یا محصولاتش توسط یک موجودیت خارجی برای انجام فعالیت هایی که امنیت، حریم خصوصی و حتی شهرت افراد را نقض می کند، تضعیف شود. این تهدیدها می توانند اثرات منفی بر شهرت و موقعیت مالی ارائه دهندگان خدمت، به رغم عدم وجود کاستی در محصولات یا خدماتشان داشته باشند. برای مثال، کاربران خرابکار ممکن است از دستگاه هایی مانند عینک گوگل یا ساعت های هوشمند سوء استفاده کنند تا اطلاعات را از مکان هایی که چنین فعالیت های غیرقانونی یا غیرمجاز هستند، جمع آوری کنند. این موارد نقض حریم خصوصی ممکن است به تهدیدهای امنیتی و یا تهدیدهای شهرت تبدیل شوند.

در تهدیدهای سوءرفتار موجودیت های وابسته، استحکام امنیت و حریم خصوصی ارائه دهنده خدمات تحت تأثیر عملکرد موجودیت های مرتبط قرار می گیرد. کیفیت امنیت و حفظ حریم خصوصی حوادث مرتبط با موجودیت های مرتبط ممکن است تحت نظر ارائه دهنده خدمات قرار نگیرد. اگر رفتار این موجودیت ها ناسازگار یا مخرب باشد، در نهایت عملکرد و شهرت ارائه دهنده خدمات را تضعیف خواهد کرد.

۵- نتیجه گیری

در ادبیات حوزه امنیت اطلاعات، دارایی اطلاعاتی هر آن چیزی تعریف شده است که در تولید، پردازش، انتقال و استفاده اطلاعات مورد استفاده قرار می گیرد و برای سازمان مهم است. یکی از انواع این دارایی ها، دارایی های اطلاعاتی کاربردی در حوزه اینترنت اشیا هستند. از سوی دیگر مبتنی بر ادبیات این حوزه، یک حادثه امنیت اطلاعات هنگامی رخ می دهد که یک تهدید از یک یا چند آسیب پذیری استفاده می کند و به یک یا چند دارایی اطلاعاتی صدمه وارد می کند. یک حادثه بالقوه با نام مخاطره امنیت اطلاعات

تجزیه و تحلیل داده های کاربر تعریف شود که شناسایی، جداسازی، طبقه بندی و تصمیم گیری در مورد کاربر را تسهیل می کند. برای مثال فرض کنید یک بیمار مبتلا به بیماری قلبی دارای یک دستگاه ضربان ساز بلوتوث است. هنگامی که دستگاه ضربان ساز ریتم نامنظمی را تشخیص می دهد، به تلفن همراه اطلاع می دهد. تلفن همراه پیشنهاد می کند که بیمار بنشیند، سپس به بیمارستان اطلاع داده و یک آمبولانس را فرا می خواند. در همین حال بیمار در زمان تلاش برای استراحت، تبلیغاتی را درباره داروهای شگفت انگیز برای بیماری های قلبی در گوشی خود دریافت می کند. تهدیدهای نفوذ فعال، به نقض های امنیتی یا حریم خصوصی در یک شرکت یا فرد اشاره دارد که می تواند به عواقب فاجعه بار منجر شود. برای مثال در حالی که شما در حال رانندگی یک ماشین هوشمند هستید، هکرها قادر به نفوذ به سیستم عامل آن هستند و اطلاعاتی را که در داشبورد نشان داده می شود را دستکاری می کنند تا سرعت را پایین تر یا بیشتر از سرعت واقعی خودرو نشان دهند، اطلاعات سوخت را دستکاری می کنند و یا حتی بدتر از آن، کیسه های هوا را بدون رخ دادن تصادف فعال می کنند و یا فرمان خودروی در حال حرکت را می چرخانند.

تهدیدهای رد پای ماندگار، احتمال سوءاستفاده از شیء هوشمند حذف شده را برای انجام برخی از اقدام های مخرب در نظر می گیرد. برای مثال، هنگامی که افراد اشیاء هوشمند را جمع آوری می کنند، آن ها یک پایگاه اطلاعاتی مرتبط با هویت خود را در سیستم های اطلاعات شرکت ایجاد می کنند. این ارتباط ممکن است حتی پس از حذف آن شیء نیز ادامه یابد.

تهدیدهای اعتماد انعکاسی و شهرت، این تهدیدها شامل هیچ گونه نفوذ در سیستم اصلی که امن است، نیستند. در واقع، ممکن است هیچ ارتباطی بین مهاجم و زیرساخت اصلی وجود نداشته باشد. این تهدیدها از نارسایی های موجود در رابط کاربری بین سیستم اینترنت اشیا و کاربران، همچنین وابستگی یک ارائه دهنده خدمت به عوامل دیگر برای ارائه خدمات خود به کاربران سوءاستفاده می کنند. تهدیدهایی که در ذیل این دسته تعریف می شوند عبارتند از:

تهدیدهای ارائه نادرست، در اکوسیستم اینترنت اشیا کاربران توسط موجودیت هایی فریب می خورند که غیرقانونی هستند و به دروغ خود را به عنوان نماینده یک شرکت، ارائه دهنده خدمات یا سازنده دستگاه معرفی می کنند تا به منافع شخصی دست پیدا کنند، حریم خصوصی کاربران را نقض کنند و یا حداقل یک تجربه کاری ناخوشایند را به کاربر ارائه دهند. در چنین مواردی، شهرت

- [7] "Oxford Dictionaries Online," 2014.
- [8] S. Misra, M. Maheswaran and S. Hashmi, Security challenges and approaches in internet of things, Cham: Springer International Publishing, 2017.
- [9] O. Garcia-Morchon, S. Kumar, S. Keoh, R. Hummen and R. Struik, "Security Considerations in the IP-based Internet of Things draft-garciacore-security-06," *Internet Engineering Task Force*, 2013.
- [10] M. Covington and R. Carskadden, "Threat implications of the internet of things," in *In 2013 5th International Conference on Cyber Conflict (CYCON 2013)*.
- [11] S. Applegate, "The principle of maneuver in cyber operations," in *In 2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 2012.
- [12] "ETICA: Ethical Issues of Emerging ICT Applications," 2014.
- [13] J. Van Den Hoven, Â. Guimarães Pereira, F. Dechesne, J. Timmermans and H. Vom Lehn, "Fact Sheet-Ethics Subgroup IoT-Version 4.0," *Delft University of Technology, Chair Ethics Subgroup IoT Expert Group*, 2012.
- [14] "Internet of Things," *World Wide Web Consortium (W3C)*, 2014.
- [15] Z. Ramzan, "Phishing Attacks and Countermeasures," *Handbook of information and communication security*, pp. 433-448, 2010.
- [16] "Privacy," 2014; <http://plato.stanford.edu/entries/privacy/>," 2014.
- [17] "Privacy and Security," 2014; <http://msdn.microsoft.com/en-us/library/ms976532.aspx>," 2014.
- [18] International Organization for Standardization, "IOS/IEC 27005- Information technology — Security techniques — Information security risk management," International Organization for Standardization, 2018.

معرفی شده است [۱۸]. بنابراین یکی از اجزای مهم در حوزه مدیریت مخاطره امنیت اطلاعات شناسایی و دسته‌بندی تهدیدها است. در این پژوهش چارچوبی پیشنهادی برای دسته‌بندی تهدیدهای موجود در اینترنت اشیا پیشنهاد شد. در این چارچوب تهدیدهای فضای اینترنت اشیا در سه دسته اصلی تهدیدهای امنیت سیستم، حریم خصوصی و اعتماد انعکاسی و شهرت جای گرفتند.

در مجموع این پژوهش پنجره‌های تازه‌ای برای پژوهش‌های میان‌رشته‌ای در شناسایی و دسته‌بندی تهدیدهای اینترنت اشیا باز می‌کند. تمرکز بر پژوهش به منظور توسعه دسته‌بندی ارائه انجام شده در این چارچوب می‌تواند مورد توجه پژوهشگران این حوزه قرار گیرد.

مراجع

- [1] A. Arabsorkhi, M. Haghighi and R. Ghorbanloo, "A conceptual trust model for the internet of things interactions," in *In 2016 8th International Symposium on Telecommunications (IST)*, 2016.
- [2] H. R. Khedmatgozar, "The impact of perceived risks on internet banking adoption in Iran: a longitudinal survey," *Electronic Commerce Research*, vol. 21, no. 1, pp. 147-167, 2021.
- [3] L. Atzori and I. a. G. Morabito, "The internet of Things: A survey," *Computer Network*, vol. 54, no. 15, pp. 2787-2805, 2010.
- [4] H. Sundmaeker, P. Guillemin, P. Friess and S. Woelfflé, "Vision and challenges for realising the Internet of Things," *Cluster of European research projects on the internet of things, European Commission*, vol. 3, no. 3, pp. 34-36, 2010.
- [5] A. Bassi, G. H. Sintef and E. Hitachi, "Internet of Things in 2020: A Roadmap for the future," European Commission/ EPoSS Expert workshop on RFID/ Internet of Things, Brussels, 2008.
- [6] L. Tan and N. Wang, "Future internet: The internet of things," in *In 2010 3rd international conference on advanced computer theory and engineering (ICACTE)*, 2010.