وزارت ارتباطات و فناوری اطلاعات شرکت ارتباطات زیرساخت	عنوان مقاله: **مروری بر استانداردها و چارچوب‌های امنیتی برای محیط‌های هوشمند مبتنی بر اینترنت اشیا**

تهیه کننده: حجت صالحی — مدرک تحصیلی: کارشناسی ارشد مخابرات

رشته شغلی: کارشناس و مسوول شبکه انتقال — اداره کل: مدیریت زیرساخت استان اصفهان

حوزه تحقیقاتی مورد نیاز شرکت: شبکه دیتا — شماره ردیف حوزه تحقیقاتی: 43 و 82

چکیده

بررسی امنیت محیط‌های هوشمند مبتنی بر اینترنت اشیا مانند خانه‌های هوشمند و شهرهای هوشمند برای اجرای اقدامات کنترلی صحیح و کاهش مؤثر تهدیدها و خطرات امنیتی ناشی از آن امری ضروری است. با این حال، مشکل در ایجاد استانداردهای امنیتی و چارچوب‌های ارزیابی که بتواند به بهترین وجه الزامات امنیتی و همچنین وضعیت امنیتی محیط‌های هوشمند مبتنی بر اینترنت اشیا را به‌طور جامع ارزیابی و آشکار کند وجود دارد. برای بررسی این شکاف، این مقاله مروری بر استانداردهای امنیتی موجود و چارچوب‌های ارزیابی را ارائه می‌کند که شامل چندین نشریه ویژه NIST در مورد تکنیک‌های امنیتی که حوزه‌های اصلی تمرکز آنها کشف مواردی که به طور بالقوه می‌توانند برخی از نیازهای امنیتی هوشمند مبتنی بر اینترنت اشیا را برطرف کنند، بررسی شده است. محیط‌ها در مجموع 80 استاندارد امنیتی ISO/IEC، 32 استاندارد ETSI و 37 چارچوب ارزیابی امنیتی مرسوم مختلف که شامل 7 نشریه ویژه NIST در مورد تکنیک‌های امنیتی بود، بررسی شدند. برای ارائه یک تحقیق جامع و به‌روز، باید فرآیند بررسی استانداردهای امنیتی منتشر شده و چارچوب‌های ارزیابی و همچنین مواردی که در دست توسعه هستند را در نظر گرفت. یافته‌ها نشان می‌دهد که اکثر استانداردهای امنیتی مرسوم و چارچوب‌های ارزیابی مستقیماً نیازهای امنیتی محیط‌های هوشمند مبتنی بر اینترنت اشیا را برآورده نمی‌کنند، اما این پتانسیل را دارند که با محیط‌های هوشمند مبتنی بر اینترنت اشیا سازگار شوند. با این بینش نسبت به تحقیقات پیشرفته در مورد استانداردهای امنیتی و چارچوب‌های ارزیابی، این مطالعه با باز کردن مسیرهای تحقیقاتی جدید و همچنین فرصت‌هایی برای توسعه استانداردهای امنیتی جدید و چارچوب‌های ارزیابی که به آینده مبتنی بر اینترنت اشیا می‌پردازد، به پیشرفت IoT_Eld و نگرانی‌های امنیتی محیط‌های هوشمند کمک می‌کند. این مقاله همچنین مشکلات و چالش‌های باز مربوط به مسائل امنیتی محیط‌های هوشمند مبتنی بر اینترنت اشیا را مورد بحث قرار می‌دهد. به عنوان یک مشارکت جدید، طبقه‌بندی چالش‌ها برای نگرانی‌های امنیتی محیط هوشمند مبتنی بر اینترنت اشیا برگرفته از ادبیات گسترده مورد بررسی در این مطالعه پیشنهاد شده است که چالش‌های شناسایی‌شده را برای راه‌حل‌های پیشنهادی بالقوه نیز ترسیم می‌کند.

کلمات کلیدی: اقدامات کنترلی، محیط‌های هوشمند مبتنی بر اینترنت اشیا، ریسک‌ها، چارچوب‌های ارزیابی امنیتی، استانداردهای امنیتی، طبقه‌بندی، تهدیدها

مقدمه

اینترنت اشیا (IoT) یک فناوری نسبتا جدید و در حال ظهور بوده که در بین بسیاری از ذینعفان محبوبیت پیدا کرده است. بر این اساس فناوری اینترنت اشیا تأثیرات انقلابی در بسیاری از زمینه‌های زندگی ما به همراه داشته است. علاوه بر این، به یک

عامل کلیدی برای نوآوری و موفقیت در طیف وسیعی از صنعت‌ها از جمله محیط‌های هوشمند مبتنی بر اینترنت اشیا تبدیل شده است.

همچنین راه را برای ظهور سایر فناوری‌های هوشمند مبتنی بر اینترنت اشیا هموار کرده است که به افراد امکان می‌دهد دستگاه‌ها و لوازم هوشمند را از راه دور با استفاده از رایانه، تلفن هوشمند یا تبلت از طریق اینترنت کنترل کنند. دستگاه‌های متصل به هم در یک محیط هوشمند مجهز به اینترنت اشیا به افراد اجازه می‌دهند تا عملکردهای مختلف دستگاه را از راه دور از طریق اینترنت کنترل کنند. با این حال، در یک محیط هوشمند معمول است که هم اینترنت اشیا و هم سایر دستگاه‌ها و خدمات غیر اینترنت اشیا با هم ترکیب شوند تا کیفیت زندگی افراد را افزایش دهند.

با این حال، اتصال دستگاه‌ها به اینترنت و همچنین سنجش، جمع‌آوری و مبادله داده‌ها، آن‌ها را در معرض طیف وسیعی از تهدیدات و خطرات امنیتی قرار می‌دهد. علاوه بر این، هر دستگاه متصل می‌تواند به یک نقطه ورود یا حمله بالقوه برای حمله‌های امنیتی تبدیل شود، بنابراین نیاز به ارزیابی و تقویت امنیت محیط‌های هوشمند مبتنی بر اینترنت اشیا است.

در حالی که انتظار می‌رود اینترنت اشیا بر بسیاری از حوزه‌های آینده زندگی ما تأثیر بگذارد، نگرانی‌های امنیتی و حریم خصوصی وجود دارد که باید به طور پیوسته مورد توجه قرار گیرد. با این حال، به دلیل ماهیت پویا و ناهمگون در محیط‌های هوشمند مبتنی بر اینترنت اشیا، پرداختن به بسیاری از مسائل امنیتی و حریم خصوصی همیشه یک چالش است. ارزیابی امنیتی محیط‌های هوشمند مبتنی بر اینترنت اشیا مانند خانه‌های هوشمند و شهرهای هوشمند، می‌تواند در محیط‌هایی که وضعیت یا چشم‌انداز امنیتی و همچنین میزان گستردگی شبکه مشخص نیست، سخت باشد. چیزی که ارزیابی امنیت در محیط‌های هوشمند فعال‌شده اینترنت اشیا را چالش‌برانگیزتر می‌کند، این واقعیت است که زمانی که نوع و ماهیت اکثر دستگاه‌ها یا لوازم متصل به اینترنت اشیا به کار گرفته می‌شوند، به ندرت پشتیبانی حرفه‌ای مستمری را برای افراد در مراحل طراحی یا عملیات ارائه می‌دهند. بنابراین فقدان پشتیبانی حرفه ای مستمر بر نیازهای امنیتی و حریم خصوصی بسیاری از محیط‌های هوشمند مبتنی بر اینترنت اشیا تأثیر می گذارد. در مواجهه با چالش‌های امنیتی در محیط‌های هوشمند مبتنی بر اینترنت اشیا، نویسندگان در این مقاله به بررسی ارزیابی استانداردهای امنیتی متداول موجود که حوزه‌های اصلی تمرکز آنها برای کشف مواردی که به طور بالقوه می‌توانند برخی از نیازهای امنیتی محیط‌های هوشمند مبتنی بر اینترنت اشیا را برطرف کنند، پرداختند . در مجموع 80 استاندارد امنیتی ISO/IEC، 32 استاندارد ETSI و 37 چارچوب امنیتی مختلف که شامل 7 نشریه ویژه NIST در مورد تکنیک‌های امنیتی

بود، بررسی شدند. یافته‌های این مطالعه می‌تواند به متخصصان اینترنت اشیا، محققان و سایر ذینفعان کمک کند تا وضعیت این فناوری را درک و همچنین به آنها کمک کند تا جهت‌های تحقیقاتی جدید را شناسایی و بحث‌های بیشتری را در مورد توسعه استانداردهای امنیتی جدید و مشکلات امنیتی آینده در محیط‌های هوشمند مبتنی بر اینترنت اشیا بررسی نمایند.

بنابراین، اهداف این مقاله به شرح ذیل می‌باشد :

1- بررسی استانداردهای امنیتی موجود و چارچوب‌های ارزیابی که شامل انتشارات ویژه NIST است در مورد تکنیک‌های امنیتی برای کشف حوزه‌های اصلی تمرکز آنها و نشان دادن وضعیت

2- شناسایی و بحث در مورد مشکلات و چالش‌های باز مرتبط با نگرانی‌های امنیتی محیط هوشمند مبتنی بر اینترنت اشیا.

3- پیشنهاد و بحث در مورد یک طبقه‌بندی از چالش‌ها برای محیط هوشمند مبتنی بر اینترنت اشیا، برگرفته از طیف گسترده پیشینه و ادبیاتی که در طول این مطالعه مورد بررسی قرار گرفت، همچنین راه‌حل‌های بالقوه برای چالش‌های باز شناسایی‌شده و دیگر مسائل امنیتی فناوری‌های هوشمند IoT آینده را ترسیم می‌کند.

در مورد قسمت های باقی مانده از مقاله، بخش دوم یک مرور کلی برای این مطالعه ارائه می‌کند، همچنین پیشینه و کار تحقیقاتی موجود در بخش سوم ارائه شده است. بخش چهارم روش تحقیق مورد استفاده در این مطالعه را توضیح می‌دهد و پس از آن بخش پنجم که بررسی‌هایی در مورد استانداردهای امنیتی معمولی و چارچوب‌های ارزیابی ارائه می‌دهد. بخش ششم مشکلات و چالش‌های باز مرتبط با محیط‌های هوشمند مبتنی بر اینترنت اشیا را ارائه می‌کند. بخش هفتم، طبقه‌بندی چالش‌ها را برای

محیط هوشمند مبتنی بر اینترنت اشیا در کنار راه‌حل‌های بالقوه پیشنهادی برای چالش‌های شناسایی‌شده پیشنهاد و مورد بحث قرار می‌دهد. در نهایت، مقاله در بخش هشتم به کارهای تحقیقاتی آتی اشاره می‌کند.

نمای کلی و انگیزه

انگیزه این بررسی این است که بدانیم استانداردهای امنیتی متعارف و چارچوب‌های ارزیابی برای استفاده در محیط‌های غیر اینترنت اشیا بسیار متفاوت هستند و بسیاری ممکن است مستقیماً نیازهای محیط‌های هوشمند مبتنی بر اینترنت اشیا را برطرف نکنند.

بنابراین، این مقاله به بررسی استانداردهای امنیتی رایج که چارچوب‌های ارزیابی آنها نگرانی‌های امنیتی محیط‌های هوشمند مبتنی بر اینترنت اشیا است، می پردازد. در حالی که مزایا و چشم اندازهای یک محیط هوشمند مبتنی بر اینترنت اشیا گسترده است، سطح حملات به این نوع ساختارها نیز بسیار زیاد است. در نتیجه، افزایش تعداد دستگاه‌های اینترنت اشیا، اکوسیستم‌ها و یکپارچه‌سازی به این معناست که روزانه نقاط پایانی آسیب‌پذیر زیادی به‌ویژه در خانه‌های هوشمند، شهرهای هوشمند، شرکت‌های جهانی و زیرساخت‌های حیاتی مشاهده می‌شود.

محیط های هوشمند مبتنی بر اینترنت اشیا در حال حاضر هر روز در حال گسترش است، با این حال، این گسترش با پیچیدگی، یکپارچگی و مسائل امنیتی زیادی در زمینه‌های مختلف همراه است.

به دلیل موارد فوق، بررسی استانداردهای امنیتی رایج موجود و چارچوب‌های ارزیابی برای کشف مسائل امنیتی کلیدی و همیشگی در محیط‌های هوشمند مبتنی بر اینترنت اشیا قرار گرفته است. علاوه بر این، نویسندگان خاطرنشان می‌کنند که بر اساس ادبیاتی که در این مقاله بررسی شده است، هنوز کمبود استانداردهای امنیتی تخصصی و چارچوب‌های ارزیابی که عمدتاً به محیط‌های هوشمند مبتنی بر اینترنت اشیا متمایل هستند، وجود دارد. به همین دلیل، اکتشافات و نتیجه‌گیری‌های کلیدی در این مطالعه به صراحت مبتنی بر استفاده از محتوای استانداردهای امنیتی مرسوم موجود و چارچوب‌های ارزیابی است که به نظر می‌رسد پتانسیل استفاده در محیط‌های هوشمند مبتنی بر اینترنت اشیا را دارند. این مطالعه همچنین مشکلات و چالش‌های باز را شناسایی و مورد بحث قرار می‌دهد و در عین حال طبقه‌بندی

چالش‌ها را برای محیط هوشـمند مبتنی بر اینترنت اشـیاء ارائه می‌کند که چالش‌های شـناسـایی‌شده را برای راه‌حل‌های بالقوه ترسیم می‌کند که می‌تواند به رسیدگی به مسائل امنیتی موجود و آینده اینترنت اشیا کمک کند.

علاوه بر این، بر اساس کاوش و بررسی انجام شده در این مقاله، بدیهی است که بسیاری از راه حل های موجود یا پیشنهادی در هنگام بررسی استانداردهای امنیتی و چارچوب های ارزیابی، دامنه محدودی داشته اند، با این حال، این مطالعه صراحتاً به استانداردهای امنیتی محدود نمی شود. در نظر گرفتن چارچوب های ارزیابی نیز برای غنی سازی مطالعه و همچنین امکان یافتن یافته های گسترده و عمیق گنجانده شده است. ترکیب ادبیات مرتبط در استانداردهای امنیتی و چارچوب‌های ارزیابی در این مطالعه به جلوگیری از تعمیم کمک می‌کند و این مطالعه را به دامنه وسیع‌تری باز می‌کند. شکل 1 نمای کلی از جنبه‌های کلیدی همپوشانی را نشان می‌دهد که انگیزه این مطالعه را ایجاد کرده است و حوزه‌های تمرکز اصلی این مقاله را تشکیل می‌دهد.

شکل 1. مروری بر جنبه های کلیدی بررسی شده در این مطالعه

نویسندگان همچنین اذعان می‌کنند که جنبه‌های کلیدی بررسی‌شده در این مطالعه همانطور که در شکل 1 نشان داده شده است، نه تنها در این مطالعه قابل استفاده هستند، بلکه می‌توانند در حوزه‌های مختلف کاربرد اینترنت اشیا از جمله موارد خارج از محدوده این مقاله استفاده شوند. این مقاله به صراحت بر استانداردهای امنیتی مرسوم موجود و چارچوب‌های ارزیابی و پتانسیل‌های آن‌ها برای انطباق با محیط‌های هوشمند مبتنی بر اینترنت اشیا متمرکز شده است. با این حال، این مقاله همچنین

به مشکلات و چالش‌های باز مختلف نگاه می‌کند و در عین حال یک طبقه‌بندی از چالش‌ها را پیشنهاد می‌کند که برای راه‌حل‌های بالقوه ترسیم شده است، همانطور که در شکل 1 مشخص شده است.

پیشینه و کار تحقیقاتی در این زمینه

مانند بسیاری از زمینه‌های دیگر، دامنه اینترنت اشیا بسیار سریع در حال رشد است. با این حال، با این رشد، چالش‌های امنیت سایبری زیادی به وجود می‌آید. تحقیقات قبلی در حوزه اینترنت اشیا بیشتر بر روی یافتن اقدامات کنترلی برای رسیدگی به کمبودها در حوزه‌های مختلف اینترنت اشیا از جمله امنیت، حریم خصوصی، آسیب‌پذیری‌ها و انعطاف‌پذیری متمرکز بوده است. با این حال، نیاز به استانداردهای امنیتی و چارچوب‌های ارزیابی که به طور خاص روی محیط‌های هوشمند مبتنی بر اینترنت اشیا تمرکز دارند نیز به اندازه خود تحقیق مهم است. به عنوان بخشی از پس زمینه تحقیقاتی، این بخش بر نگرانی‌های امنیتی و حفظ حریم خصوصی برای محیط‌های هوشمند مبتنی بر اینترنت اشیا و همچنین تحقیقات موجود در مورد استانداردهای امنیتی یا چارچوب‌های ارزیابی تمرکز خواهد کرد. توجه به این نکته نیز مهم است که حریم خصوصی تمرکز اصلی این مطالعه نیست.

نگرانی‌های مربوط به امنیت و حفظ حریم خصوصی در محیط های هوشمند مبتنی بر اینترنت اشیا، داده ها و اطلاعات زیادی بین دستگاه‌های مختلف به اشتراک گذاشته می‌شود. بدون وجود یک استاندارد امنیتی خوب یا مکانیزم ارزیابی امنیتی، داده ها و اطلاعات در حال ارسال در این محیط‌ها و اطراف آن می‌توانند در برابر انواع تهدیدها و خطرات امنیتی حساس یا آسیب‌پذیر شوند. برخی از نگرانی‌های مربوط به داده‌ها و اطلاعات در محیط‌های هوشمند مبتنی بر اینترنت اشیا در بخش‌های فرعی زیر خلاصه شده‌اند.

نگرانی‌های امنیتی

- نشت داده‌ها و اطلاعات: در هر محیط هوشمند اینترنت اشیا، بدون مکانیسم‌های امنیتی مناسب که از داده‌ها و اطلاعات در برابر بدافزارها و سایر مزاحمان مخرب محافظت می‌کند، اطلاعات شخصی به راحتی می‌تواند فاش شود و منجر به نقض امنیت شود.

- استراق سمع: با انتقال اطلاعات در داخل و اطراف محیط‌های هوشمند مبتنی بر اینترنت اشیا و به سمت اینترنت، مهاجمان مخرب می‌توانند از ارتباطات شبکه ناامن استفاده کرده و داده‌ها را به همان شکلی که هست به سرقت ببرند. بین دستگاه‌های IoT متصل منتقل می‌شود که می‌تواند منجر به سایر نقض‌های امنیتی جدی شود.
- هک کردن: بیشتر داده‌ها و اطلاعات جمع آوری شده توسط دستگاه‌های اینترنت اشیا در محیط‌های هوشمند ممکن است ذخیره شوند. در سیستم‌های قابل دسترسی به اینترنت مانند "ابر" بسیاری از دستگاه‌ها و سیستم‌های اینترنت اشیا مبتنی بر ابر دارند که آسیب پذیری‌های امنیتی به راحتی می‌توانند قربانی هک و حملات سایبری به عنوان انتقال داده مانند ویدئو شوند. حتی ممکن است داده‌های دوربین‌ها هنگام ارسال از طریق اینترنت رمزگذاری نشوند.
- بهره برداری از نرم افزار: به دلیل عدم استانداردسازی در بسیاری از محیط‌های هوشمند مبتنی بر اینترنت اشیا، نرم افزارهای نفوذگر به راحتی می‌توانند راه خود را به دستگاه‌های اینترنت اشیا از طریق ارتقاء سیستم عامل و راه اندازی قابل اعتماد، خرید دستگاه و همچنین برنامه‌ها و خدمات بیابد. این می‌تواند با تغییر تنظیمات دستگاه، بر ارائه خدمات تأثیر بگذارد. علاوه بر این، بسیاری از دستگاه‌های اینترنت اشیا روی نسخه‌های سبک‌وزن مستقل سیستم عامل معرفی می‌شوند که هکرها می‌توانند آن را پردازش کنند، اجرا می‌شوند. بهر صورت آسیب‌پذیری‌های نرم‌افزاری را جستجو کرده و از آنها برای دستیابی به دسترسی ممتاز به اطلاعات حساس بهره‌برداری میکند.
- امنیت دستگاه اینترنت اشیا: به دلیل فقدان استانداردهای امنیتی یا امنیت جهانی تایید شده تخصصی اینترنت اشیا و چارچوب‌های ارزیابی، برخی از دستگاه‌ها ممکن است با خطوط پایه امنیتی ضعیف مانند سیستم‌عامل‌ها و نرم‌افزارهای تعبیه‌شده وصله‌نشده، گذرواژه‌های ضعیف، قابل حدس زدن یا رمزگذاری‌شده سخت و ناامن انتقال و ذخیره‌سازی داده‌ها مواجه شوند. این باعث می‌شود چنین دستگاه‌های IoT در برابر تهدیدات امنیتی مختلف آسیب پذیر باشند.

حملات

- ربودن دستگاه‌های اینترنت اشیا و باج افزار: در نتیجه امنیت ضعیف، فقدان استانداردهای تخصصی امنیتی مورد تایید جهانی اینترنت اشیا، چارچوب‌های ارزیابی و افزایش تعداد استفاده از دستگاه‌های اینترنت اشیا، بسیاری از این دستگاه‌ها ممکن است به زودی به اهداف آسانی برای حملات باج افزار تبدیل شوند.

- کاربران آگاه به فناوری و امنیت: با نوآوری روزافزون فناوری‌های اینترنت اشیا، بسیاری از کاربران هنوز نحوه طراحی و عملکرد دستگاه‌های مدرن اینترنت اشیا را درک نکرده‌اند. این امر استفاده مهاجمان از مهندسی اجتماعی را برای فریب کاربران دستگاه‌های اینترنت اشیاء برای ارائه داده‌ها یا اطلاعات حساس که می‌تواند برای دسترسی به شبکه‌های محیط هوشمند مانند خانه‌های هوشمند و شهرهای هوشمند مورد استفاده قرار گیرد، آسان کند و زندگی همه را به خطر می اندازد.
- تست و به روز رسانی ناکافی دستگاه اینترنت اشیا: اکثر دستگاه‌های اینترنت اشیا به سرعت تولید می‌شوند تا نیازهای روزافزون بازار را برآورده کنند و از این رو بعضا تحت آزمایش مناسب قرار نمی‌گیرند یا از هیچ استاندارد امنیتی قابل قبولی پیروی نمی‌کنند. کاربران اکثراً برای آزمایش دستگاه‌های اینترنت اشیا و همچنین چارچوب‌های ارزیابی به تولیدکنندگان اعتماد می‌کنند. با این حال، به دلیل تقاضاهای بالا، بسیاری از تولیدکنندگان بیشتر بر روی ایجاد و عرضه محصولات جدید به بازار بدون انجام تست مناسب یا اعمال تدابیر کنترل امنیتی تمرکز می‌کنند. علاوه بر این، دستگاه‌های قدیمی اینترنت اشیا ممکن است دیگر به‌روزرسانی نشوند یا زمان زیادی طول بکشد تا به‌روزرسانی شوند و در نتیجه خطرات امنیتی در محیط های هوشمند مبتنی بر اینترنت اشیا ایجاد شود.
- عدم نظارت فعال دستگاه: نظارت بر دستگاه‌های اینترنت اشیا می‌تواند چالش برانگیز باشد. این مهم به این دلیل است که اکثراً از ابزارها و شیوه‌های نظارتی موجود، به‌ویژه آن‌هایی که بر روی ابر تمرکز می‌کنند، برای نظارت بر داده‌های متریک سری زمانی و بدون تمرکز بر دستگاه‌های مدرن اینترنت اشیا یا فرآیندهای آنها به‌طور سنتی استفاده شده است. عدم فعال بودن ابزارهای نظارت بر دستگاه‌های اینترنت اشیا، دید کامل شبکه را در محیط‌های هوشمند مبتنی بر اینترنت اشیا دشوار می‌کند.

علاوه بر این، کمبود چنین ابزارهایی وجود دارد که بتوان از آنها برای نظارت مستقیم بر دستگاه‌های IoT مستقر در آن استفاده کرد.

کمبود امنیت کارآمد و قوی

- پروتکل‌ها : فقدان پروتکل‌های امنیتی کارآمد و قوی از جمله استانداردهای امنیتی IoT مناسب، چارچوب‌های ارزیابی و پادمان‌ها می‌تواند منجر به نقض امنیت در محیط‌های هوشمند شود که باعث افزایش داده‌های شخصی می‌شود.

- جعل هویت: با بسیاری از دستگاه‌های اینترنت اشیا در محیط‌های هوشمند فاقد احراز هویت قوی یا کنترل دسترسی مکانیسم‌ها، جعل هویت کاربر قانونی و استفاده از اعتبارنامه یا هر اطلاعات دیگری که به آنها امکان دسترسی به منابع اینترنت اشیا موجود در یک محیط هوشمند مبتنی بر اینترنت اشیا را می‌دهد، برای متجاوزان آسان می‌شود. موفقیت آمیز بودن جعل هویت می‌تواند بیشتر برای تشدید سایر حملات امنیتی جدی مورد استفاده قرار گیرد.
- سلامت و ایمنی کاربران: اگر هکری به یک محیط هوشمند مبتنی بر اینترنت اشیا مانند خانه‌های هوشمند دسترسی پیدا کند، برای مثال ممکن است سعی کند نسخه‌های پزشکی را تغییر دهد یا محصولاتی را سفارش دهد که صاحب‌خانه به آنها نیازی ندارد یا به آن حساسیت دارد. در نتیجه، سلامت صاحب‌خانه و کل خانواده در خطر است زیرا ممکن است زمان لازم برای تأیید فرآیندهای اتوماسیون آغاز شده توسط هکرها را نداشته باشند.
- Denial of Service (DoS/DDoS): با پیشرفت تکنولوژی، هکرها سعی می‌کنند تا هاب‌های موجود DoS/DDoSرا در شبکه‌های محیط هوشمند مبتنی بر اینترنت اشیا یا خود حسگرها ایجاد کنند. با این حال، مهاجمان همچنین می‌توانند به شبکه دسترسی داشته باشند و پیام‌های انبوه را به دستگاه‌های IoT مانند Clear To Send (CTS)و Request To Send (RTS) ارسال کنند که باعث حملات DoS به دستگاه‌های IoT قانونی می‌شود.

سایر تهدیدات امنیتی

با رشد سریع تعداد و استفاده از دستگاه‌های اینترنت اشیا، تهدیدات امنیتی دیگری نیز ممکن است در محیط‌های هوشمند مبتنی بر اینترنت اشیا مانند تهاجم به خانه، تجاوز، جعل دستگاه‌های اینترنت اشیای سرکش و تقلبی، حملات باتنت، حملات فیزیکی ،آسیب یا از دست دادن غیر عمدی، بلایا و قطع، خرابی یا نقص، سیستم‌های پویا، احراز هویت، مشکلات شبکه بی سیم ناامن، حمله کانال جانبی، سرقت هویت، تهدید مداوم پیشرفته (APT) ، پارازیت، اختلال عملکرد، سرریز بافر، داده‌کاوی غیرمجاز در مقیاس بزرگ، نظارت، دسترسی یا حذف یا اصلاح غیرمجاز داده‌ها، کرم‌ها، ویروس‌ها و کدهای مخرب، باز بودن سیستم های شبکه، رمزهای عبور ضعیف، سیستم عامل ثابت، محدودیت‌های منابع، ماهیت بدون سر دستگاه‌های اینترنت اشیا، بسته‌های مقاوم در برابر دستکاری، پروتکل‌های ناهمگن، ویژگی‌های پویا، انتظارات طول عمر در میان بسیاری از تهدیدات امنیتی دیگر وجود داشته باشد.

نگرانی‌های حفظ حریم خصوصی

حریم خصوصی در محیط‌های هوشمند مبتنی بر اینترنت اشیا به این معنی است که «اطلاعات مربوط به افراد باید محافظت شود و تحت هیچ شرایطی نباید بدون رضایت صریح صاحبان در معرض دید قرار گیرد.» به دلیل سهولت اتصال دستگاه‌های اینترنت اشیا به اینترنت و فقدان مکانیسم‌های امنیتی مناسب یا استانداردهای امنیتی رایج و چارچوب‌های ارزیابی طراحی‌شده برای محیط‌های هوشمند مبتنی بر اینترنت اشیا، در معرض خطر قرار گرفتن داده‌ها یا اطلاعات شخصی در دست مهاجمان مخرب می‌تواند بالا باشد. برخی از نگرانی‌های حفظ حریم خصوصی مرتبط با محیط‌های هوشمند مبتنی بر اینترنت اشیا عبارتند از:

– ذخیره‌سازی و استفاده از داده‌ها :با معرفی ذخیره‌سازی ابری توسط اشخاص ثالث، بسیاری از دستگاه‌های اینترنت اشیا می‌توانند به راحتی داده‌های تولید شده یا جمع آوری شده از محیط‌های هوشمند را در زیرساخت ابر عمومی ذخیره کنند. با این حال، مشکل این است که عدم استانداردسازی در مورد نحوه ذخیره و پردازش داده‌های IoT از منابع مختلف وجود دارد که عمدتاً ساختاری ندارند و می‌توانند منجر به نقض حریم خصوصی شوند. بنابراین، این امر مستلزم توسعه استانداردهای جهانی امنیت و حفظ حریم خصوصی، بهترین شیوه‌ها، روش‌ها و ابزارهایی است که می‌توانند به طور مداوم داده‌های اینترنت اشیا را مدیریت کنند و همچنین اطمینان حاصل کنند که داده‌های توزیع شده به طور ایمن با سطوح بالایی از حریم خصوصی یا به ابرهای عمومی یا خصوصی قابل دسترسی و انتقال هستند.

– ردیابی و حریم خصوصی موقعیت مکانی: به دلیل سهولت و در دسترس بودن اتصال اینترنت به دستگاه‌های اینترنت اشیا، ردیابی کاربران بر اساس موقعیت مکانی بسیار رایج است. هنگامی که یک مهاجم مخرب یک کاربر را شناسایی کرد، می‌تواند داده‌هایی را جمع‌آوری کند که رفتار کاربر را دنبال می‌کند، از جمله تاریخچه موقعیت مکانی که مهاجم می‌تواند از آن برای تعقیب کاربر که منجر به نقض حریم خصوصی می‌شود استفاده کند.

– حریم خصوصی آگاه از زمینه یا موقعیت: در نتیجه مکانیسم‌های امنیتی ضعیفی که در برخی از دستگاه‌های اینترنت اشیا اجرا می‌شود، شناسایی و مکان‌یابی حرکت، فعالیت‌ها و جمع‌آوری داده‌های کاربران بر اساس اقدامات ممکن است منجر به نقض حریم خصوصی شود.

– حریم خصوصی داده‌های حس‌شده، تولیدشده یا جمع‌آوری شده: برخی از تولیدکنندگان دستگاه‌های اینترنت اشیا می‌توانند سخت‌افزار خود را طراحی کنند.

برای جمع آوری داده های حس‌شده یا تولید شده توسط دستگاه‌ها به ویژه در مورد استفاده از خدمات و سایر داده‌های مربوط به مشتریان خود. داده‌ها یا اطلاعات جمع‌آوری‌شده به این روش ممکن است به طور کامل با نیازهای حریم خصوصی کاربران، به‌ویژه در حین انتقال، مطابقت نداشته باشد و ممکن است منجر به نقض حریم خصوصی کاربر شود.

– واکاوی اطلاعات حریم خصوصی کاربر: به دلیل ارتباطات شبکه‌ای که به طور کامل محافظت نشده در شبکه هایIoT ، استخراج حریم خصوصی همانطور که در [22] بحث شده است، می‌تواند برای استخراج اطلاعات خصوصی از خانه‌های هوشمند یا شهرهای هوشمند که منجر به نقض جدی امنیت و حریم خصوصی می‌شود، استفاده شود.

دیگر نگرانی‌های مربوط به حریم خصوصی که در مقالات شناسایی شده‌اند عبارتند از پروفایل کاربر، نظارت و کنترل ابزار، جمع آوری، استفاده و افشای داده‌های اینترنت اشیا بدون رضایت کاربران، عدم شناسایی داده‌های اینترنت اشیا، وابستگی به فروشندگان، قابلیت همکاری، مدیریت دستگاه‌های اینترنت اشیا، مسئولیت‌پذیری و شفافیت.

همانطور که قبلا ذکر شد، این مقاله نگرانی‌های مربوط به حریم خصوصی را بیشتر مورد بحث قرار نخواهد داد. بخش بعدی برخی از کارهای تحقیقاتی موجود در چارچوب‌های ارزیابی امنیتی را تشریح می‌کند.

ب. کارهای تحقیقاتی موجود

در ادبیات تحقیق، چندین استاندارد امنیتی و چارچوب‌های ارزیابی در مورد تکنیک‌های امنیتی وجود دارد که می‌توانند در محیط‌های مختلف مورد استفاده قرار گیرند (به عنوان مثال، امنیت شبکه، امنیت وب جهانی، امنیت برنامه‌ها، ارتباطات راه دور در میان سایر زمینه‌ها). با این حال، این استانداردهای امنیتی و چارچوب‌های ارزیابی اساساً با در نظر گرفتن محیط‌های کاربردی خاص طراحی شده‌اند، از این رو مراحل یا فرآیندهای متنوعی برای محیط‌های مختلف درگیر می‌شوند که بعداً در بخش پنج مشخص می‌شود. محققان در حوزه اینترنت اشیا همچنین رویکردها و تکنیک‌های مختلفی را برای پرداختن به اینترنت اشیا مختلف پیشنهاد کرده‌اند. که تصمیمات و اساس کار تحقیقاتی موجود در این بخش را تشکیل می دهد.

در [24]، نویسندگان سیستم نظارت و امنیت خانه یکپارچه مبتنی بر اینترنت اشیا را پیشنهاد کردند. نویسندگان استدلال کردند که امنیت خانه همچنان یک مسئله حیاتی است، بنابراین نیاز به یک سیستم امنیتی و نظارتی برای محیط‌های خانه هوشمند مبتنی بر اینترنت اشیا است. با این حال، سیستم پیشنهادی آنها روی تشخیص مزاحمان، دمای اتاق، رطوبت، باران، آتش‌سوزی و همچنین نظارت بر وضعیت نور متمرکز بود. ولی امنیت تک‌تک دستگاه‌ها و کل چشم انداز امنیتی خانه هوشمند پس از استقرار دستگاه در تحقیقات آنها در نظر گرفته نشده است که می تواند خانه هوشمند را در برابر انواع تهدیدها و خطرات امنیتی آسیب‌پذیر کند.

یک چارچوب ارزیابی امنیتی مبتنی بر شبکه تعریف‌شده توسط نرم‌افزار (SDN) برای ارزیابی سطح امنیت CloudIoT توسط [25] ایجاد شد. انگیزه مطالعه آنها وجود انتخاب‌های متعدد از ارائه‌دهندگان منابع ابری و دستگاه‌های اینترنت اشیا و نه لزوماً محیط های هوشمند مبتنی بر اینترنت اشیا بود. تحقیقات این مقاله بیان کرد که ارزیابی سطوح امنیتی ارائه‌دهندگان منابع ابری و دستگاه‌های IoT در ترویج پذیرش CloudIoT و کاهش خطرات امنیتی کسب‌وکار بسیار مهم است.

با این حال، مقاله فعلی بر بررسی استانداردهای امنیتی و چارچوب‌های ارزیابی برای شناسایی مواردی که پتانسیل رسیدگی به نگرانی‌های امنیتی محیط‌های هوشمند مبتنی بر اینترنت اشیا را دارند، تمرکز دارد. مطالعه دیگری توسط [26] استدلال کرد که امنیت به یک عامل حیاتی برای هر محیط هوشمند IoT تبدیل شده است. به همین دلیل، آنها در تحقیقات خود چارچوب ویژگی‌های امنیتی شناسایی شده (ISA) را برای ارزیابی ویژگی‌های امنیتی دستگاه‌های مبتنی بر اینترنت اشیاء حوزه سلامت (IoHT)در محیط مراقبت‌های بهداشتی پیشنهاد کردند. انگیزه مطالعه آنها این بود که داده‌های بیمار همیشه از دستگاه های IoTبه سرورها منتقل می‌شود. در حین انتقال، داده‌های بیمار می‌تواند به دست مهاجمان مخرب بیفتد. به همین دلیل، مطالعه آنها به این نتیجه رسید که امنیت مناسب برای تجهیزات مبتنی بر IoHT به دلیل قرار گرفتن در معرض حملات امنیتی مختلف ضروری است.

تحقیقات مرجع [27] بیان کرد که رشد سریع سیستم‌های مبتنی بر اینترنت اشیا نگرانی‌های امنیتی را ایجاد می‌کند و یک چارچوب ارزیابی امنیتی برای سیستم‌های اینترنت اشیا ضروری است. سپس نویسندگان یک چارچوب ارزیابی برای ارزیابی ویژگی‌های امنیتی تجهیزات مبتنی بر اینترنت اشیا با استفاده از روش تصمیم‌گیری چند معیاره ترکیبی (MCDM) پیشنهاد کردند و بعداً یک مطالعه تجربی روی ارزیابی دستگاه‌های مراقبت بهداشتی مبتنی بر اینترنت اشیا انجام دادند.

تحقیقات بیشتر توسط [28] ادعا کرد که داده‌های بیمار بسیار حیاتی است و همچنین انتقال ایمن آن در برنامه‌های کاربردی مراقبت های بهداشتی هوشمند بسیار حیاتی است. در تحقیقات مرجع [28] چارچوبی را برای محافظت از اطلاعات پزشکی در برابر تهدیدات خارجی پیشنهاد کردند که نویسندگان ادعا می‌کنند که دارای اهمیت علمی و اقتصادی است. زیرا منابع احتمالی کمتری از دستگاه های پزشکی کم مصرف را مصرف می‌کند. بنابراین، می توان از آن برای برنامه‌های کاربردی مراقبت‌های بهداشتی بلادرنگ استفاده کرد.

در تحقیق دیگری، نویسندگان [29] بیان می‌کنند که «در اتوماسیون موجودی، بررسی بلادرنگ اقلام، مدیریت اطلاعات آنها و مدیریت وضعیت، نظارت می‌تواند با استفاده از اینترنت اشیا انجام شود». با این حال، داده‌هایی که در بین دستگاه‌های موجود در شبکه جریان می‌یابند، نیازمند یک چارچوب ارزیابی امنیتی است که از احراز هویت، مجوز، یکپارچگی و محرمانه بودن اطمینان می‌دهد. به همین دلیل، نویسندگان» یک چارچوب ارزیابی امنیتی سبک وزن مبتنی بر اینترنت اشیا برای اتوماسیون موجودی با استفاده از شبکه‌های حسگر بی‌سیم پیشنهاد کردند.

تحقیقات مرجع [30] یک چارچوب ارزیابی مستمر ایمن و سازگار برای ارزیابی سطوح امنیت و انطباق خدمات ابری پیشنهاد کرد. چارچوب پیشنهادی خدمات ابری را به مشتریان تسهیل می‌کند تا یک ارائه‌دهنده خدمات ابری بهینه (CSP) را انتخاب کنند که الزامات امنیتی مورد نظر آنها را برآورده کند. با این حال، این چارچوب همچنین مشتریان خدمات ابری را قادر می‌سازد تا انطباق CSP انتخابی را در فرآیند استفاده از خدمات ابری ارزیابی کنند.

تحقیقات [31] چارچوب ارزیابی ریسک را برای ارائه‌دهندگان خدمات ابری طراحی و اجرا کرد که به منظور ارائه اطمینانی است که منجر به اطمینان بیشتر مصرف‌کنندگان خدمات ابری از یک طرف و بهره‌وری مقرون به صرفه و قابل اعتماد ارائه‌دهندگان خدمات ابری و منابع سازماندهی شده توسط زیرساخت‌های فردی می‌شود. ارائه‌دهندگان در طرف دیگر دنینگ و همکاران [32] چارچوبی را برای ارزیابی خطرات امنیتی مرتبط با فناوری‌های مورد استفاده در خانه پیشنهاد کردند.

در همین راستا، کانگ و همکاران در [33] چارچوب امنیتی پیشرفته‌ای را برای دستگاه‌های هوشمند در محیط خانه‌های هوشمند ارائه کردند که هدف آن ارائه یکپارچگی با استفاده از تکنیک‌های خود امضا و کنترل دسترسی برای جلوگیری از تهدیدات امنیتی مانند اصلاح داده‌ها، نشت و ساخت کد است. جدول 1 خلاصه ای از کارهای موجود مورد بحث و حوزه‌های تمرکز اصلی آنها را ارائه می‌کند:

جدول 1 خلاصه‌ای از کارهای انجام شده

چارچوب های پیشنهادی	مناطق تمرکز اولیه		
	smart home	cloud IOT	IOT health
سیستم نظارت و امنیت یکپارچه خانه	✓		
چارچوب ارزیابی امنیت سرتاسر بر اساس شبکه تعریف شده با نرم افزار(SDN)		✓	
یک چارچوب از مشخصه‌های امنیتی (ISA)			✓
یک چارچوب ارزیابی برای ویژگی‌های امنیتی تجهیزات مبتنی بر اینترنت اشیاء			✓
چارچوبی برای محافظت از اطلاعات پزشکی	✓		✓
یک چارچوب امنیتی سبک برای اتوماسیون موجودی با استفاده از شبکه حسگر بی‌سیم	✓	✓	✓
یک چارچوب ارزیابی مستمر ایمن و سازگار برای ارزیابی سطوح امنیت و انطباق خدمات ابری	✓	✓	
یک چارچوب ارزیابی ریسک موثر و کارآمد برای ارائه دهندگان خدمات ابری	✓	✓	
چارچوبی برای ارزیابی خطرات امنیتی مرتبط با فناوری‌های مورد استفاده در خانه	✓		
یک چارچوب امنیتی پیشرفته برای دستگاه‌های هوشمند در محیط خانه	✓		

از کارهای پژوهشی خلاصه شده در جدول 1 استنباط می‌شود که بیشتر آنها مستقیماً بر تأمین امنیت تمرکز ندارند ارزیابی برای محیط‌های هوشمند مبتنی بر اینترنت اشیا انجام شده، ولی حوزه‌های کاربردی خاص به طور کامل برای همه برآورده نمی‌شوند.

نیازهای امنیتی اولیه محیط های هوشمند مبتنی بر اینترنت اشیا

جدول 1 نیاز به توسعه استانداردهای امنیتی جدید و چارچوب‌های ارزیابی برای محیط‌های هوشمند مبتنی بر اینترنت اشیا را توجیه می‌کند. بخش بعدی روش تحقیق مورد استفاده برای انجام مرور در این مقاله را مورد بحث قرار می‌دهد.

روش تحقیق

در انجام فرآیند بررسی، نویسندگان در این مقاله دستورالعمل‌ها و اصولی را اتخاذ کردند که روش‌های سیستماتیکی را نشان می‌دهد که اعتبار نظری مطالعه را تأیید می‌کند. این دستورالعمل‌ها نیاز به شناسایی منطقه کلیدی مطالعه، نمونه‌گیری، استخراج داده‌های مفید و تفسیر اعتبار این داده‌ها و در نهایت ترسیم نتیجه به عنوان نتایج بالقوه را مشخص می‌کنند. بر اساس همین مفهوم، این مطالعه در درجه اول بر شناسایی مقالات مرتبط در مورد استانداردهای امنیتی و چارچوب‌های ارزیابی از جمله انتشارات ویژه NIST در مورد تکنیک‌های امنیتی، بررسی آنها برای یافتن اینکه آیا معیارهای انتخابی پیشنهادی را برآورده می‌کنند و انتشار یافته‌ها در حین شناسایی شکاف‌های تحقیقاتی موجود متمرکز شده است. یا چالش‌هایی که در شکل 2 نشان داده شده است. روش بررسی مورد استفاده در این مطالعه شامل سه مرحله اولیه به شرح زیر است:

- مرحله اول: شناسایی منطقه مطالعه، تعریف سوالات تحقیق، نمونه گیری و تعریف کلید جستجو. استراتژی یا معیارها

- مرحله دوم: اعمال استراتژی یا معیارهای جستجو در ادبیات شناخته شده، انجام جستجوی بولینگ برفی، جستجوی پایگاه داده، ارزیابی جستجو و تعریف معیارهای انتخاب.

- مرحله سوم: شناسایی مقالات، وب سایت‌ها و اسناد وب پذیرفته‌شده برای بررسی و مرور بر اساس موضوع اصلی مطالعه انتخاب شده.

الف. مرحله اول: شناسایی منطقه مطالعه

شناسایی منطقه مورد مطالعه در چارچوب این مقاله بر طبق چندین سؤال پژوهشی است که اساس کل مطالعه را نیز تشکیل می‌دهد. با توجه به اینکه هدف بررسی وضعیت فعلی استانداردهای امنیتی و چارچوب‌های ارزیابی است، این به عنوان یک اصل راهنما است که فعالیت‌های کلیدی را که می‌توان برای محیط‌های هوشمند مبتنی بر اینترنت اشیا اعمال کرد، نشان می‌دهد. بر این اساس سوالات کلیدی تحقیق برای این پژوهش به شرح زیر مطرح شده است:

: QR1

وضعیت فعلی استانداردهای امنیتی متعارف و چارچوب‌های ارزیابی با توجه به نگرانی‌های امنیتی محیط‌های هوشمند مبتنی بر اینترنت اشیا چگونه است؟

: QR2

کدام یک از استانداردهای امنیتی مرسوم موجود و چارچوب‌های ارزیابی می‌تواند برای کمک به شما تطبیق داده شود برخی از الزامات امنیتی اولیه محیط‌های هوشمند مبتنی بر اینترنت اشیا را برطرف می‌کند؟

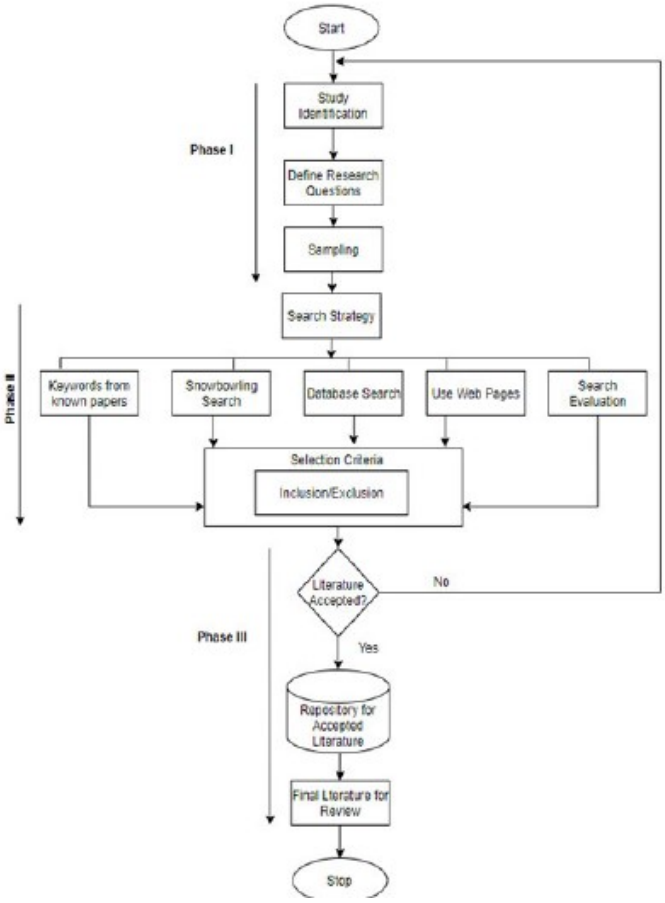
: QR3

مشکلات و چالش‌های باز بر اساس استثنائات موجود در استانداردهای امنیتی و چارچوب های ارزیابی کدامند؟

بر اساس مطالعه ما بر اساس سؤال تحقیق فوق، مرحله بعدی به استراتژی جستجوی کلیدی می‌پردازد.

ب. مرحله دوم: استراتژی جستجو

مرحله دوم مبتنی بر انجام جستجوی آنلاین است. دامنه این مطالعه به سمت استانداردهای امنیتی و چارچوب‌های ارزیابی متمایل شده است که شامل انتشارات ویژه NIST در مورد تکنیک‌های امنیتی نیز می‌شود.



شکل2.روش تحقیق

بعنوان نتیجه، نویسندگان Google Scholar ، ACM، Springer Link، IEEE Xplore، Web of Science، Web Search Engines و Scopus را با پرس و جوها و رشته‌های جستجو نشان داده شده در جدول 2 نشان داده اند.

جدول 2. پرس و جوها و رشته‌های جستجو شده

پرس و جو جستجو	رشته‌های جستجو
RQ1	استاندارد امنیتی یا چارچوب ارزیابی امنیتی یا تکنیک‌های امنیتی

RQ2	استاندارد امنیتی برای محیط‌های هوشمند مبتنی بر اینترنت اشیا یا چارچوب ارزیابی امنیتی برای محیط‌های هوشمند مبتنی بر اینترنت اشیا
RQ3	مسائل باز و چالش‌های امنیتی در محیط‌های هوشمند مبتنی بر اینترنت اشیا

پس از انجام جستجوی کلیدواژه بر اساس معیارهای ذکر شده در جدول 2، تعداد مقالات، مقالات آنلاین، اسناد وب و سایر نشریات ویژه به دست آمده در جدول 3 خلاصه شده است.

جدول 3. تعداد کل منابع شناسایی شده بر اساس معیارهای جستجو

Article Source	RQ1	RQ2	RQ3	Total
IEEE Xplore	38	50	28	116
Google Scholar	74	62	52	188
Search Engines	118	95	104	317
ScienceDirect	42	48	37	127
SpringerLink	8	15	10	33
Web of Science	20	12	18	50
Total	**300**	**282**	**249**	**831**

ج.مرحله سوم : شناسایی و بازنگری مقالات

برای فیلتر کردن مقالات انتخابی، مقالات آنلاین و نشریات ویژه، رویکرد زیر اتخاذ شد:

- مقالات، وب سایت‌ها، سند وب یا سایر نشریات ویژه تنها زمانی در مرحله بعدی گنجانده می‌شوند که همه نویسندگان توافق کنند که بر اساس اهداف مطالعه دارای ارتباط هستند.

- مقالات مشکوک، وب سایت‌ها، اسناد وب یا هر نشریه خاص دیگر به طور مشترک بررسی می‌شوند تا مشخص شود که آیا معیارهای انتخاب را تا حدی یا به طور کامل مطابق شکل 2 برآورده می‌کنند.
- مقالات، وب‌سایت‌ها، اسناد وب یا هر نشریه خاصی که توسط همه نویسندگان مرتبط نبود، حذف یا از معیارهای انتخاب حذف شدند.

- کلیه مقالات پذیرفته‌شده، وب‌سایت‌ها، اسناد وب و نشریات ویژه در یک مخزن جهت بررسی گنجانده شد. در طول این مرحله، کل مقالات جمع‌آوری‌شده، در مجموع 831 مقاله و با دو هدف مورد مطالعه کامل نویسندگان قرار گرفت: هدف اول استخراج تمام داده‌های مرتبط مورد نیاز برای مطالعه و هدف دوم بررسی صحت و درستی آن بود. و ارتباط داده‌های استخراج شده در نظر گرفته شده به سمت اهداف اولیه این مطالعه گرایش داشت . پس از بررسی عناوین، چکیده‌ها و بخش‌های تمام 831 مرجع شناسایی‌شده نشان داده شده در جدول 3، در مجموع 617 منبع نامربوط تلقی شدند و از معیارهای انتخاب حذف شدند. از 214 مورد باقی مانده، 131 مورد مشکوک طبقه بندی شدند. رایزنی و گفتگو اساس این فرآیند را تشکیل می‌دهد، به‌ویژه در مورد هرگونه توافقی که باید برای هر یک از منابع مورد بحث یا مشکوک منظور شود. پس از بررسی‌های فراوان بر اساس محتوای هر مقاله، وب سایت، اسناد وب و سایر منابع، در مجموع 149 مورد پذیرفته شده استخراج شد که توسط نویسندگان مرتبط تشخیص داده شد که شامل 80 استاندارد امنیتی ISO/IEC، 32 استاندارد ETSI و 37 چارچوب ارزیابی امنیتی مختلف (شامل 7 نشریه ویژه NIST در مورد تکنیک‌های امنیتی) شد. 149 مورد داده شناسایی‌شده مخزن نهایی را برای بررسی تشکیل می‌دهند و در جدول 4 خلاصه شده‌اند. بخش بعدی، مروری بر تمام استانداردهای امنیتی انتخاب شده و چارچوب‌های ارزیابی از جمله انتشارات ویژه NIST در مورد تکنیک های امنیتی ارائه می دهد. هدف این بخش، کشف حوزه تمرکز هر یک از استانداردهای امنیتی و چارچوب‌های ارزیابی شناسایی و انتخاب شده از متون است تا مشخص شود کدام یک از آنها به طور بالقوه برخی از الزامات امنیتی یا نیازهای محیط‌های هوشمند مبتنی بر اینترنت اشیا را برآورده می‌کنند و در غیر این صورت، می‌توانند برای رسیدگی به نگرانی‌های امنیتی محیط‌های هوشمند مبتنی بر اینترنت اشیا سازگار باشند.

بررسی استانداردهای امنیتی موجود و چارچوب‌های ارزیابی

استانداردهای امنیتی موجود بینشی را در مورد کنترل‌های امنیتی، فرآیندها، رویه‌ها، خطوط پایه و دستورالعمل‌های توصیه‌شده ارائه می‌کنند که برای شبکه‌ها ایده‌آل و در برخی موارد برای انطباق، اجباری تلقی می‌شوند. از سوی دیگر، اکثر چارچوب‌های ارزیابی امنیتی موجود، بهترین شیوه‌ها، روش‌ها و دستورالعمل‌های امنیتی را ارائه می‌دهند که سازمان‌ها می‌توانند برای به دست آوردن بهترین نتایج برای اجرای یک برنامه موفق، از آنها استفاده کنند. با این حال، شبکه‌های محیط‌های هوشمند مبتنی بر اینترنت اشیا نگرانی‌های امنیتی جدیدی ایجاد می‌کنند که به‌طور مستقیم توسط اکثر استانداردهای امنیتی مرسوم موجود و چارچوب‌های ارزیابی مورد توجه قرار نمی‌گیرند. بنابراین، این بخش از مقاله، استانداردهای امنیتی موجود و چارچوب‌های ارزیابی را بررسی می‌کند، از جمله برخی از نشریات ویژه NIST که از متون بررسی شده شناسایی و انتخاب شده‌اند و حوزه‌های اصلی تمرکز خود را برای کشف مواردی که می‌تواند به طور بالقوه برای رفع نیازهای امنیتی محیط‌های هوشمند مبتنی بر اینترنت اشیا سازگار شود.

الف. استانداردهای امنیتی موجود و چارچوب‌های ارزیابی

جدول 4 خلاصه‌ای از استانداردهای امنیتی مختلف و چارچوب‌های ارزیابی شناسایی، انتخاب و مورد بحث در این بخش را نشان می‌دهد که شامل مالک و حوزه اصلی تمرکز هر استاندارد و چارچوب است. همچنین توجه داشته باشید که برخی از استانداردها و چارچوب‌های ارزیابی که در این بخش مورد بحث قرار گرفته‌اند، بر اساس صنعت یا منطقه جغرافیایی تخصصی هستند. شرح دقیق‌تر هر استاندارد و چارچوب ارزیابی شناسایی‌شده در بخش فرعی ارائه شده است.

1) چارچوب امنیت سایبری NIST

چارچوب امنیت سایبری NIST بر اساس مجموعه‌ای از استانداردهای صنعتی و بهترین شیوه‌ها برای کمک به سازمان‌ها برای مدیریت ریسک‌های امنیت سایبری زیرساخت حیاتی خود ایجاد شد. از آنجایی که اینترنت اشیا در حال تبدیل شدن به بخشی از زیرساخت‌های حیاتی است، این چارچوب پتانسیل استفاده در محیط‌های هوشمند مبتنی بر اینترنت اشیا را دارد. این چارچوب شامل مجموعه‌ای از فعالیت‌های امنیت سایبری، نتایج و مراجع اطلاعاتی است که در بخش‌های زیرساخت حیاتی رایج هستند و راهنمایی‌های دقیقی را برای توسعه پروفایل‌های سازمانی ارائه می‌دهند. به طور خاص، این چارچوب به عملکردهای کلیدی

شناسایی، محافظت، تشخیص، پاسخگویی و بازیابی تقسیم می‌شود که ریسک‌های مربوط به امنیت داده‌ها و اطلاعات را مدیریت می‌کند.

– شناسایی: به سازمان‌ها کمک می‌کند تا درک درستی از نحوه مدیریت ریسک امنیت سایبری برای سیستم‌ها، افراد، دارایی‌ها، داده‌ها و قابلیت‌ها از جمله مدیریت دارایی، محیط کسب‌وکار، و حاکمیت فناوری اطلاعات از طریق فرآیندهای ارزیابی و مدیریت ریسک جامع داشته باشند.

– محافظت: به سازمان‌ها کمک می‌کند تا پادمان‌های مناسب را برای اطمینان از ارائه خدمات حیاتی ایجاد و اجرا کنند. این مرحله همچنین شامل تعریف کنترل‌های امنیتی برای حفاظت از داده‌ها و سیستم‌های اطلاعاتی است از جمله کنترل دسترسی، آموزش و آگاهی، امنیت داده‌ها، رویه‌های حفاظت از اطلاعات و حفظ فناوری‌های حفاظتی.

– تشخیص: به سازمان‌ها کمک می‌کند تا فعالیت‌های مناسبی را برای شناسایی وقوع یک رویداد امنیت سایبری توسعه و پیاده سازی‌کنند و همچنین دستورالعمل‌هایی برای تشخیص ناهنجاری‌ها در سیستم‌های امنیتی، نظارتی ارائه دهد و شبکه‌هایی برای کشف حوادث امنیتی.

– پاسخ: به سازمان‌ها کمک می‌کند تا فعالیت‌های مناسب را برای اقدام در رابطه با یک حادثه امنیت سایبری شناسایی شده توسعه و اجرا کنند. این همچنین شامل توصیه‌هایی برای برنامه‌ریزی پاسخ‌ها به رویدادهای امنیتی، روش‌های کاهش، فرآیندهای ارتباطی در طول یک پاسخ و فعالیت‌هایی برای بهبود انعطاف‌پذیری امنیتی است.

– بازیابی: به سازمان‌ها کمک می‌کند تا فعالیت‌های مناسب را برای حفظ برنامه‌های انعطاف‌پذیری و بازیابی هر گونه قابلیت یا خدماتی که به دلیل یک حادثه امنیت سایبری آسیب دیده است توسعه و اجرا کنند و همچنین دستورالعمل‌هایی که یک شرکت می‌تواند برای بازیابی از حملات استفاده کند.

2) چارچوب مدیریت ریسک NIST (RMF)

چارچوب مدیریت ریسک (RMF) جامع، منعطف، تکرارپذیر و قابل اندازه‌گیری را فراهم می‌کند. فرآیند 7 مرحله ای (تهیه، طبقه بندی، انتخاب، اجرا، ارزیابی، مجوز و نظارت) که هر سازمانی می‌تواند برای مدیریت خطرات امنیت اطلاعات و حریم خصوصی از آن استفاده کند.

– آماده‌سازی: از فعالیت‌های ضروری جهت آماده‌سازی سازمان برای مدیریت خطرات امنیتی و حریم خصوصی مراقبت می‌کند.

– دسته‌بندی: به سازمان کمک می‌کند تا سیستم و اطلاعات پردازش، ذخیره و ارسال شده را بر اساس تحلیل میزان تاثیر دسته‌بندی کند.

– انتخاب: به سازمان‌ها کمک می‌کند تا مجموعه‌ای از کنترل‌های NIST SP 800-53 را برای محافظت از سیستم بر اساس ارزیابی ریسک انتخاب کنند.

– پیاده‌سازی: به سازمان کمک می‌کند تا کنترل‌ها را اجرا کند و نحوه استقرار کنترل‌ها را مستند کند.
– ارزیابی: به سازمان در ارزیابی کمک می‌کند تا تعیین کند که آیا کنترل‌ها وجود دارند یا خیر یا همانطور که در نظر گرفته شده عمل می‌کنند و نتایج مورد نظر را تولید می‌کنند.

– مجوز: این شامل مقامات ارشد یک سازمان می‌شود که تصمیمات مبتنی بر ریسک را برای مجوز دادن به سیستم اتخاذ می‌کنند.

– مانیتور: به سازمان کمک می‌کند تا به طور مداوم بر اجرای کنترل و خطرات سیستم‌ها نظارت کند. با افزایش نگرانی‌های امنیتی و حفظ حریم خصوصی در محیط‌های هوشمند مبتنی بر اینترنت اشیا، این چارچوب این پتانسیل را دارد که برای استفاده در حوزه‌های عملکردی خاص با امنیت اینترنت اشیا و مدیریت ریسک‌های حریم خصوصی سازگار شود.

3) NIST PRIVACY FrameWork

چارچوب حریم خصوصی NIST برای کمک به سازمان‌ها در شناسایی و مدیریت خطرات حریم خصوصی و همچنین ایجاد محصولات و خدمات نوآورانه و در عین حال محافظت از حریم خصوصی افراد توسعه داده شد. توابع اصلی چارچوب به شرح زیر است:

- شناسایی: به سازمان‌ها کمک می‌کند تا درک درستی از نحوه مدیریت خطرات حریم خصوصی از پردازش داده‌ها برای افراد ایجاد کنند.

- حکومت: به سازمان‌ها کمک می‌کند که ساختار حاکمیت سازمانی را توسعه و پیاده‌سازی کنند تا درک مستمری از اولویت‌های مدیریت ریسک سازمان که با خطر حفظ حریم خصوصی مشخص می‌شوند، فراهم کنند.
- کنترل: به سازمان‌ها کمک می‌کند که فعالیت‌های مناسب را توسعه و اجرا کنند تا آنها یا افراد بتوانند داده‌ها را با جزئیات کافی برای مدیریت خطرات حریم خصوصی مدیریت کنند.

- ارتباط: به سازمان ها کمک می‌کند که فعالیت‌های مناسبی را توسعه و اجرا کنند تا آنها و همچنین افراد بتوانند درک قابل اعتمادی از نحوه پردازش داده‌ها و خطرات مربوط به حریم خصوصی داشته باشند.
- محافظت: به سازمان‌ها کمک می‌کند تا پادمان‌های مناسب پردازش داده را توسعه و پیاده‌سازی کنند. از این چارچوب، شناسایی، کنترل و محافظت از عملکردها می‌تواند به مدیریت مسائل حریم خصوصی در محیط‌های هوشمند مبتنی بر اینترنت اشیا کمک کند.

4) NIST SP 800-53

این نشریه ویژه در مورد مسائل امنیتی، کنترل‌های امنیتی و حریم خصوصی را برای سیستم‌ها و سازمان‌های اطلاعاتی جهت محافظت از عملیات و دارایی‌های سازمانی، افراد، سایر سازمان‌ها و کشور در برابر مجموعه‌ای از تهدیدات و خطرات امنیتی، از جمله حملات خصمانه، خطاهای انسانی، بلایای طبیعی، شکست‌های ساختاری، نهادهای اطلاعاتی خارجی و خطرات حریم خصوصی فراهم می‌کند.

5) NIST SP 800-30

این نشریه ویژه برای راهنمایی سازمان‌ها در انجام ارزیابی ریسک سیستم های اطلاعاتی توسعه یافته است.

6) NIST SP 800-37

انتشارات ویژه NIST SP 800-37 دستورالعمل‌هایی را برای اعمال RMF در سیستم‌ها و سازمان‌های اطلاعاتی تشریح و ارائه می‌کند.

7) NIST SP 800-39

این نشریه ویژه به منظور راهنمایی یک برنامه یکپارچه در سطح سازمان برای مدیریت ریسک امنیت اطلاعات برای عملیات سازمانی (ماموریت، عملکردها، تصویر و شهرت)، دارایی‌های سازمانی، افراد، سایر سازمان‌ها و کشور حاصل از عملیات و استفاده سیستم‌های اطلاعات فدرال ایجاد شده است.

8) NIST SP 800-12

NIST SP 800-12 اساساً برای سازمان‌های فدرال و دولتی طراحی شده است، اما می‌تواند توسط دیگرانی که بر کنترل و امنیت رایانه در یک سازمان تمرکز دارند نیز استفاده شود.

9) NIST SP 800-14

NIST SP 800-14 برای کمک به سازمان‌ها در درک سیاست‌های امنیت سایبری، توضیحات کلی از اصول امنیتی رایج مورد استفاده را ارائه می‌دهد.

10) NIST SP 800-53R1

NIST SP 800-53R1 با تمرکز بر حفاظت از محرمانه بودن، یکپارچگی و در دسترس بودن سیستم و اطلاعات آن طراحی شده است.

11) قانون قابل حمل و پاسخگویی بیمه سلامت (HIPAA)

HIPAA به منظور ارائه دستورالعمل‌هایی برای توانمند ساختن برنامه‌های بهداشتی، ارائه‌دهندگان مراقبت‌های بهداشتی و مراکز تسویه مراقبت‌های بهداشتی برای اجرای کنترل‌های کافی برای ایمن کردن اطلاعات سلامت کارکنان یا مشتریان و محافظت از اطلاعات حساس سلامت بیمار در برابر افشای بدون رضایت یا آگاهی بیمار توسعه داده شد. با افزایش تعداد دستگاه‌های پزشکی اینترنت اشیا، HIPAA می‌تواند برای استفاده در سیستم‌های سلامت هوشمند مبتنی بر اینترنت اشیا سازگار شود.

12) قانون حقوق آموزشی خانواده و حریم خصوصی(FERPA)

FERPA برای محافظت از حریم خصوصی سوابق تحصیلی دانش‌آموزان توسعه داده شد و برای همه مدارسی که تحت برنامه‌ای قابل اجرا از وزارت آموزش ایالات متحده بودجه دریافت می‌کنند اعمال می‌شود.

13) استانداردهای امنیت داده های صنعت کارت پرداخت(PCI-DSS)

PCI DSS برای کمک به حفاظت از ایمنی داده‌های کارت طراحی شده است و مجموعه‌ای از الزامات در نظر گرفته شده را تعریف می‌کند. باید اطمینان حاصل شود که همه سازمان‌هایی که اطلاعات کارت اعتباری را پردازش، ذخیره یا انتقال می‌دهند، یک محیط امن را حفظ می‌کنند. برای کاهش کلاهبرداری کارت اعتباری با افزایش استفاده از ارتباطات میدان نزدیک، PCI-DSS می‌تواند در دستگاه‌های IoT مانند گوشی‌های هوشمند که گاهی برای پردازش اطلاعات کارت اعتباری استفاده می‌شوند، اعمال شود.

14) گواهینامه مدل توسعه امنیت سایبری (CMMC)

CMMC که توسط وزارت دفاع ایالات متحده (DoD) توسعه یافته است، برای اندازه‌گیری قابلیت‌ها، آمادگی و پیچیدگی پیمانکاران دفاعی در امنیت سایبری استفاده می‌شود. مدل توسعه امنیت سایبری چارچوب یا مسیری را برای سازمان‌ها فراهم

می‌کند تا به طور دوره‌ای توسعه یک برنامه امنیتی را ارزیابی یا اندازه‌گیری کرده و در مورد چگونگی رسیدن به سطح بعدی راهنمایی کنند.

7- مراجع

1. H. Lin and N. W. Bergmann, ‘‘IoT privacy and security challenges for smart home environments,’’ Information, vol. 7, no. 3, p. 44, 2016.

2. N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, ‘‘IoT threat detection advances, challenges and future directions,’’ in Proc. IEEE Workshop Emerg. Technol. Secur. IoT (ETSecIoT), Sydney, NSW, Australia, Apr. 2020, pp. 22–29.

3. L. Cédric, D. Eleni, T. Guillaume, D. Guillaume, and A. Mouhannad. (Dec. 2015). Security and Resilience of Smart Home Environments. Good Practices and Recommendations. Accessed: Mar. 30, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/securityresilience-good-practices/at_download/fullReport

4. V. R. Kebande, N. M. Karie, and H. S. Venter, ‘‘Adding digital forensic readiness as a security component to the IoT domain,’’ Int. J. Adv. Sci., Eng. Inf. Technol., vol. 8, no. 1, pp. 1–11, 2018.

5. W. M. S. Stout and V. E. Urias, ‘‘Challenges to securing the Internet of Things,’’ in Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST), Orlando, FL, USA, Oct. 2016, pp. 1–8, doi: 10.1109/CCST.2016.7815675.

6. Z. A. Solangi, Y. A. Solangi, S. Chandio, M. B. S. A. Aziz, M. S. B. Hamzah, and A. Shah, ‘‘The future of data privacy and security concerns in Internet of Things,’’ in Proc. IEEE Int. Conf. Innov. Res. Develop. (ICIRD), Bangkok, Thailand, May 2018, pp. 1–4, doi: 10.1109/ICIRD.2018.8376320.

7. D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, ‘‘Security and privacy issues for an IoT based smart home,’’ in Proc. 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO), Opatija, Croatia, May 2017, pp. 1292–1297, doi: 10.23919/MIPRO.2017.7973622.

8. W. Ali, G. Dustgeer, M. Awais, and M. A. Shah, ‘‘IoT based smart home: Security challenges, security requirements and solutions,’’ in Proc. 23rd Int. Conf. Autom. Comput. (ICAC), Huddersfield, U.K., Sep. 2017, pp. 1–6, doi: 10.23919/IConAC.2017.8082057

9. V. R. Kebande, J. Bugeja, and J. A. Persson, ‘‘Internet of threats introspection in dynamic intelligent virtual sensing,’’ in Proc. 1st Workshop CyberPhys. Social Syst. (CPSS), Bilbao, Spain, 2020, pp. 1–8.

10. L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, ‘‘IoT privacy and security: Challenges and solutions,’’ Appl. Sci., vol. 10, no. 12, p. 4102, Jun. 2020.
11M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, ‘‘Security issues in the Internet of Things (IoT): A comprehensive study,’’ Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 6, p. 383, 2017.

12. V. R. Kebande and I. Ray, ‘‘A generic digital forensic investigation framework for Internet of Things (IoT),’’ in Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud), Vienna, Austria, Aug. 2016, pp. 356–362.
13. A. Jurcut, T. Niculcea, P. Ranaweera, and N.-A. Le-Khac, ‘‘Security considerations for Internet of Things: A survey,’’ Social Netw. Comput. Sci., vol. 1, no. 4, pp. 1–19, Jul. 2020.
14. H. M. T. Gadiyar, G. S. Thyagaraju, and T. P. Bhavya, ‘‘Privacy and security issues in IoT based smart home applications,’’ Int. J. Eng. Res. Technol., vol. 6, no. 15, pp. 1–3, 2018.

15. D. J. MacInnis, V. M. Patrick, and C. W. Park, ‘‘Looking through the crystal ball,’’ in Review of Marketing Research, vol. 2. Bingley, U.K.: Emerald Group Publishing, 2006, pp. 43–80.

16. S. Nagarkar and V. Prasad, ‘‘Evaluating privacy and security threats in IoT-based smart home environment,’’ Int. J. Appl. Eng. Res., vol. 14, no. 7, pp. 1–4, 2019.
17. J. Bugeja, A. Jacobsson, and P. Davidsson, ‘‘On privacy and security challenges in smart connected homes,’’ in Proc. IEEE Eur. Intell. Secur. Informat. Conf. (EISIC), Uppsala, Sweden, Aug. 2016, pp. 172–175.
18. M. Seliem, K. Elgazzar, and K. Khalil, ‘‘Towards privacy preserving IoT environments: A survey,’’ Wireless Commun. Mobile Comput., vol. 2018, p. 15, Nov. 2018, doi: 10.1155/2018/1032761.
19. F. Hall, L. Maglaras, T. Aivaliotis, L. Xagoraris, and I. Kantzavelou, ‘‘Smart homes: Security challenges and privacy concerns,’’ 2020, arXiv:2010.15394. [Online]. Available: http://arxiv.org/abs/2010.15394

20. A. Cook, M. Robinson, M. A. Ferrag, L. A. Maglaras, Y. He, K. Jones, and H. Janicke, ‘‘Internet of cloud: Security and privacy issues,’’ in Cloud Computing for Optimization: Foundations, Applications, and Challenges. Cham, Switzerland: Springer, 2018, pp. 271–301.