فصل‌نامه دانش شناسی
(علوم کتابداری و اطلاع رسانی و فناوری اطلاعات)
دانشگاه آزاد اسلامی واحد تهران شمال
سال دوازدهم، شماره ٤٤، بهار ١٣٩٨، از صفحه ٣٢ الی ٥٤

شناسایی تهدیدها و آسیب‌پذیری‌های رایج در فضای اینترنت اشیاء و ارائه راهکارهای امنیتی جهت مواجهه با آن‌ها

صفیه طهماسبی لیمونی[1] | شهرزاد قاسمی[2] | رقیه قربانلو[3]

۱. گروه علم اطلاعات و دانش‌شناسی، واحد بابل، دانشگاه آزاد اسلامی، بابل، ایران(نویسنده مسئول)، sa.tahmasebi2@gmail.com
۲. گروه علم اطلاعات و دانش‌شناسی، واحد بابل، دانشگاه آزاد اسلامی، بابل، ایران، sh.gh_20@yahoo.com
۳. کارشناس ارشد مهندسی فناوری اطلاعات، پژوهشگر پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران، sghorbanloo@gmail.com

تاریخ دریافت: ۹۷/۸/۱۲ تاریخ پذیرش: ۹۸/۱/۲۵

چکیده

هدف: هدف از این پژوهش، شناسایی تهدیدها و آسیب‌پذیری‌های رایج اینترنت اشیاءو ارائه راهکارهای امنیتی جهت مواجهه با آن ها است.

روش پژوهش: روش پژوهش ازنظر هدف کاربردی و ازنظر گردآوری داده توصیفی - پیمایشی است. جامعه آماری شامل کلیه اساتید و متخصصان حوزه اینترنت اشیاء در دانشگاههای شهر تهران به تعداد ۵۰ نفر بودند. روش نمونه گیری از نوع نمونه گیری غیرتصادفی در دسترس بود. حجم نمونه برابر با جامعه آماری مشخص شد. ابزار پژوهش پرسشنامه محقق ساخته از مطالعه سیستماتیک ادبیات موضوعی بود. اعتبار پرسشنامه ها با رجوع به متخصصان درحوزه اینترنت اشیاء اخذ گردید. پایایی ابزار با استفاده از آلفای کرونباخ برای پرسشنامه ۰/۸۸ بود. تحلیل داده ها با استفاده از آمار توصیفی و استنباطی توسط نرم‌افزار اس.پی. اس. اس انجام شد.

یافته ها: با اینکه استانداردهای مختلفی در حوزه مسئله امنیت و محرمانگی در اینترنت اشیاء در حال توسعه است ولی همچنان نیازمندی‌های امنیتی اینترنت اشیاء و حتی مخاطره‌های آن به‌خوبی شناسایی و تحلیل نشده‌است و نیازمند سازوکارهای محرمانگی، صحت، احرازهویت و کنترل‌دسترسی به‌صورت دقیق است. بر اساس یافته های حاصل از آزمون های این پژوهش آسیب‌پذیری‌ها در ۲۱ گروه قابل طبقه بندی و استناد خواهند بود.

نتیجه گیری: نتایج آزمون ها نشان دهنده آن است خبرگان مختلف حسب دیدگاه و حوزه فعالیت خود، مجموعه متنوعی را به‌عنوان راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در حوزه اینترنت اشیاء تبیین نموده‌اند، اما با جمع‌بندی نظرات ارائه‌شده توسط شرکت‌کنندگان می‌توان مهمترین راهکارهای امنیتی در برابر تهدیدهای امنیتی در فضای اینترنت اشیاء را شامل احراز و تصدیق هویت کارآمد دوطرفه، کنترل‌دسترسی، پیکربندی معماری امن، رمزنگاری ارتباطات و داده‌ها و وقایع‌نگاری و مانیتورینگ دانست.

واژه‌های کلیدی: اینترنت اشیاء، تهدید امنیتی، آسیب‌پذیری، الزام امنیتی

مقدمه

اینترنت اشیاء[1] پدیده جدیدی است که در آن وسایل پیرامون ما مانند سیستم تهویه منزل یا چراغ‌های اتاق به شبکه متصل‌شده و توسط برنامه‌های کاربردی اختصاصی تلفن‌های هوشمند و یا از طریق وب، مدیریت و داده‌های آن‌ها در سیستم‌های ابری، ذخیره‌سازی یا پردازش می‌شوند (آلم، چودری و نال[2]، ۲۰۱۰). اشیاء هنگامی که بتوانند خود را به‌صورت دیجیتالی عرضه کنند، با اشیاء اطراف، نظیر یک پایگاه‌داده بزرگ در ارتباط خواهند بود. وقتی اشیاء با یکدیگر شبکه شدند، می‌توان سخن از یک "محیط هوشمند" به میان آورد (ورمیزن و فریس[3]، ۲۰۱۳).

فناوری اینترنت اشیاء مانند هر نوع فناوری دیگری برای سودجویان و تبهکاران فضای سایبر انگیزه خرابکاری و سوءاستفاده ایجاد می‌کند. این انگیزه به‌معنای وجود تهدید امنیتی علیه اینترنت اشیاء است. تهدیدهای امنیتی در اینترنت اشیاء ممکن است متوجه کاربران، سرویس‌دهندگان، مشتریان و یا دارایی‌های یک سازمان مصرف‌کننده این فناوری باشد. با افزایش کاربردهای این فناوری در زندگی، داشتن شناختی درست و دقیق از تهدیدهای امنیتی در اینترنت اشیاء -به خصوص در محیط‌هایی که از این فناوری استفاده می‌کنیم- امری مهم و ضروری محسوب می‌شود. رشد فزاینده اینترنت اشیاء -به‌واسطه گستردگی و افزایش ارتباطات در این پدیده- نگرانی عظیمی را به‌وجود آورده‌است. نقض حریم‌خصوصی، حمله‌های سایبری -علی‌الخصوص حمله‌هایی که علیه زیرساخت‌های کشورهای رقیب و متخاصم انجام می‌شود- و اقدام‌های تروریستی از این دست نگرانی‌ها هستند. از طرف دیگر، آسیب‌پذیری‌ها[4]، بروز حمله‌ها، نقص‌های امنیتی و ایمنی، عدم‌وجود راهکارهای مناسب و در عین حال سرعت خیره‌کننده پیشرفت و گسترش اینترنت اشیاء اهمیت این موضوع را چندین برابر نموده‌است. آنچه که می‌تواند باعث کاهش نگرانی و جلب اعتماد افراد -از مشتریان و عموم افراد تا توسعه‌دهندگان- به این فناوری باشد برقراری امنیت در این فضا است. امنیت در اینترنت اشیاء با پرداخت به آسیب‌پذیری‌ها، تهدیدها[5] و راهکارهای رفع این مشکل‌ها محقق می‌شود و جلوگیری از بروز چنین تهدیدهایی است که باعث جلب اعتماد و توسعه این فناوری خواهد شد (محمودحسین و دیگران[6]، ۲۰۱۵).

پیشینه های پژوهش به صورت زیر دسته بندی شده ارائه می شود:

اینترنت اشیاء: عبارت اینترنت اشیاء یا به اصطلاح اتصال شبکه‌ای اشیاء، برای اولین بار در سال ۱۹۹۹ در آزمایشگاه Auto-ID در انستیتو فناوری ماساچوست[7] (MIT) توسط کوین اشتون[8] مطرح شد. اگر تمامی اشیاء موجود در زندگی روزمره مجهز به تراشه‌های رادیویی شوند، آنگاه سایر وسائل می‌توانند آن‌ها را شناسایی نموده و با آن‌ها ارتباط برقرار نمایند (کوین اشتون[9]، ۲۰۰۹). نسل آینده کاربردهای اینترنت از نسخه ۶ اینترنت (IPv6) استفاده می‌کنند که به‌دلیل فضای بسیار گسترده برای آدرس‌دهی در آن، تمامی اشیاء ساخته‌شده قابلیت دریافت شناسه اختصاصی را خواهند داشت. بنابراین تمامی اشیاء در زندگی روزمره ما قابلیت آدرس‌دهی، اتصال و کنترل‌شدن را پیدا می‌کنند (آنتونیو، مرابیتو و لِرا[10]، ۲۰۱۰).

تعاریف مختلفی از اینترنت اشیاء مطرح شده‌است که برخی از آن‌ها در جدول ۱ تبیین گردیده‌است. در جدول ۱ ابتدا نام مؤلف یا گروه تحقیقاتی و سپس سال ارائه تعریف و بعد از آن حوزه تمرکز تعریف آمده است.

[1] Internet of Things
[2] Alam, Chowdhury & Noll
[3] Vermesan & Friess
[4] Vulnerabilities
[5] Threats
[6] Mahmud Hossain et al
[7] Massachusetts Institute of Technology
[8] Kevin Ashton
[9] Ashton
[10] Antonio, Morabito & Iera

جدول ۱. اینترنت اشیاء و تعاریف آن(مبانی نظری پژوهش)

مؤلف/ مرجع	سال	تعریف	حوزه‌های تمرکز
بسی و همکاران	۲۰۰۸	یک شبکه جهانی از اشیاء متصل به هم که براساس پروتکل‌های ارتباطی استاندارد به‌شکل منحصربه‌فردی آدرس‌دهی شده‌اند.	شبکه جهانی، اشیاء متصل، پروتکل‌های ارتباطی، آدرس‌دهی
CASAGRAS[1]	۲۰۰۹	یک زیرساخت شبکه جهانی که اتصال اشیاء مجازی و فیزیکی را از طریق بهره‌برداری از جمع‌آوری داده‌ها و فن‌آوری‌های ارتباطی تسهیل می‌کند.	زیرساخت، اشیاء فیزیکی و مجازی، جمع‌آوری داده، فن‌آوری ارتباطی
گروه تحقیقاتی آر.اف.آی.دی[2]	۲۰۰۹	شبکه‌ای جهانی از اشیاء قابل آدرس‌دهی بصورت یکتا، براساس یک پروتکل ارتباطی استاندارد.	شبکه فراگیر، ارتباط اشیاء، آدرس‌دهی
گروه تحقیقاتی فارستر[3]	۲۰۱۰	استفاده از فناوری‌های ارتباطی و اطلاعاتی برای ایجاد اجزای زیرساخت حیاتی و ارائه خدمات مربوط به دانش، بهداشت و درمان، امنیت عمومی، حمل‌ونقل و خدمات شهری به صورت آگاهانه، تعاملی و کارآمد.	خدمات اشیاء، تعامل اشیاء، فناوری‌های اطلاعات و ارتباطات
آنتونیو، مرابیتو و لِرا	۲۰۱۰	اینترنت اشیاء در سه پارادایم مشخص می‌شود: اینترنت‌گرا (میان‌افزار)، شی‌گرا (حسگرها) و معناگرا (دانش).	اشیاء، اینترنت، حسگرها، دانش و اطلاعات
گروه پروژه‌های تحقیقاتی اروپا[4]	۲۰۱۰	مشارکت فعال اشیاء در تجارت، فرآیندهای گردآوری اطلاعات و پردازش آن‌ها با قابلیت برقراری ارتباط با یکدیگر و با محیط اطراف بدون دخالت مستقیم انسانی.	کاربرد اشیاء در تجارت، ارتباطات، پردازش
سیسکو[5]	۲۰۱۱	هنگامی که تعداد اشیاء متصل به شبکه جهانی از تعداد انسان‌ها بیشتر شود.	اشیاء، ارتباطات
توماس و همکاران	۲۰۱۲	برقراری ارتباط بین افراد و اشیاء با سایر افراد در بهترین زمان و مکان و با ارائه خدمات مناسب و با صرفه‌ترین هزینه.	اشیاء، انسان، ارتباطات، خدمات کارآمد
اتحادیه بین‌المللی مخابرات[6]	۲۰۱۲	یک زیرساخت جهانی برای جامعه اطلاعاتی که خدمات پیشرفته را از طریق اتصال (فیزیکی و مجازی) اشیاء بر پایه فن‌آوری‌های ارتباطی و اطلاعاتی سازگار موجود و در حال تحول ممکن می‌سازد.	زیرساخت، اطلاعات، اشیاء فیزیکی و مجازی، فن‌آوری ارتباطی
مداف، بگواف و کلیفتون[7]	۲۰۱۴	شبکه‌ای شامل اتصالات داخلی، ارتباطات بین افراد، فرآیندهای کسب‌وکار، داده‌ها و اشیاء می‌باشد.	تجارت و کسب و کار، ارتباطات، اشیاء
یزدان پناه و حسنی آهنگر	۱۳۹۵	اینترنت اشیا اصطلاحی است برای توصیف دنیایی که درآن اشیا قادر خواهند بود با اتصال به اینترنت یا به کمک ابزارهای ارتباطی، با سایر اشیا تعامل داشته باشند و اطلاعات خود را با هم و یا با انسان ها به اشتراک بگذارند و کلاس جدیدی از قابلیت ها، برنامه های کاربردی و سرویسها را ارائه دهند	کاربردهای اینترنت اشیاء، چالش های اینترنت اشیاء
پژنگ، ابطحی ، رجب زاده فطری	۱۳۹۵	توصیف یک سیستم که در آن می توان تمام اشیا فیزیکی در جهان را با سنسور به اینترنت متصل کر	چالش های یکپارچگی اتصالات اینترنت در اینترنت اشیا
زرگر	۱۳۹۸	اینترنت اشیا حاصل تکامل در فناوری اینترنت است که امکان اتصال اشیا به هم را فراهم ساخته و می تواند به شکلی گسترده فرایندها و نحوه خدمات دهی کتابخانه ها را تغییر دهد.	تقسیم بندی موانع تمرکز اینترنت اشیاء در کتابخانه ها به ۳ دسته عوامل امنیتی، انسانی، و زیرساخت‌ها

[1] Coordination And Support Action for Global RFID-Related Activities and Standardisation
[2] RFID Research Group
[3] Forrester Research
[4] European Research Council
[5] Cisco
[6] ITU Telecommunication Standardization
[7] Modoff, Bhagavath & Clifton

باتوجه به جدول ۱، می‌توان گفت که اینترنت اشیاء مجموعه‌ای از اشیاء است که از طریق اینترنت به یکدیگر متصل هستند و توانایی برقراری ارتباط و به‌اشتراک‌گذاری اطلاعات با دیگر دستگاه‌های هوشمند را دارند. این دستگاه‌ها می‌تواند شامل لوازم خانگی، تجهیزات ورزشی، کنترل سلامت، سیستم‌های امنیتی منازل، لامپ‌ها، سیستم‌های صوتی، تجهیزات کنترل دما و... باشد. در واقع، اینترنت اشیاء را می‌توان شبکه‌ای از اشیاء متصل به‌هم که در حال تعامل با سایر اشیاء و حتی انسان‌ها هستند تعریف نمود.

آسیب‌پذیری‌های حوزه اینترنت اشیاء: آنچه موجب ایجاد نگرانی و چالش‌ها در فضای اینترنت اشیاء می‌شود، آسیب‌پذیری‌ها و تأثیرهای ناشی از آن‌ها است. شناخت آسیب‌پذیری‌ها می‌تواند عامل هدایت‌کننده به سمت عوامل و منشاء تهدیدها باشد ازاین‌رو، بررسی و شناخت آسیب‌پذیری‌ها بسیار مهم و حیاتی است (محمودحسین و دیگران، ۲۰۱۵). در جدول ۲ به مجموعه‌ای از آسیب‌پذیری‌های حوزه اینترنت اشیاء اشاره شده‌است.

جدول ۲. آسیب‌پذیری‌های حوزه اینترنت اشیاء(مبانی نظری پژوهش)

نام آسیب‌پذیری	شرح آسیب‌پذیری	مرجع
احراز و تشخیص هویت ناکافی	احراز اصالت و مجوزدهی ناکافی در برابر کابران داخل شبکه شایع است. به‌صورت دستی و با استفاده از ابزارهای خودکار می‌توان به راحتی این نوع آسیب‌پذیری را تشخیص داد. از دست دادن داده، خرابی، عدم مسئولیت، انکار دسترسی از مهم‌ترین عوارض این نوع آسیب‌پذیری است که می‌تواند منجر به از کارافتادن سیستم نیز شود.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام[1]، ۲۰۱۲)،
نقض حریم‌خصوصی	شبکه‌های بی‌سیم، به دلیل قابلیت دسترسی از راه‌دور، خطر نقض حریم خصوصی را افزایش می دهند چون باعث می شوند که سیستم در معرض خطر بالقوه استراق سمع و حملات پوششی قرار بگیرد. در واقع، همه ابزار هوشمندی که به اینترنت متصل خواهد شد توسط آژانس‌های اطلاعاتی شنود و جاسوسی می‌شوند و از آن مهمتر به راحتی از سوی هکرها نفوذ به اطلاعات شخصی شما ممکن می‌شود.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
رابط ابری ناامن	بسیاری از سرویس‌های اینترنت اشیاء درفضای ابری میزبانی می‌شوند، بنابراین دستگاه‌ها و برنامه‌های‌کاربردی در هر زمان و هر مکان قابل دسترسی است. بدین ترتیب مرزهای دسترسی حذف می‌شود، ولی همزمان خطر امنیتی افزایش می‌یابد. به طور مثال، نگرانی‌های امنیتی حریم‌خصوصی و محرمانگی افزایش می‌یابد.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
رابط سیّار ناامن	زمانی نمود پیدا می‌کند که حدس اعتبارنامه‌های مورد استفاده، آسان و یا ارتقاء سطح دسترسی امکان‌پذیر باشد. این نوع آسیب‌پذیری آشکارسازی داده کاربر و کنترل غیرمجاز دستگاه‌ها را با خود به‌همراه دارد.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
توسعه نادرست پچ سیستم‌عامل و نرم‌افزار	اگر به صورت منظم به روزرسانی نشوند، نسخه‌های پیش‌فرض و منسوخ شده همیشه تحت خطرات امنیتی هستند. نسخه‌های به‌روز باید به طور امن اعمال شوند و مهاجمان قادر نباشند تا اطلاعات حیاتی (مانند اطلاعات پیکربندی و یا گواهینامه‌های رمزنگاری) را در حین فرآیند به‌روزرسانی کشف کنند.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
پیکربندی نادرست و استفاده از تنظیمات پیش‌فرض	هکرها از امنیت بسیار پایین ابزارهای اینترنت اشیاء و تنظیمات امنیتی ضعیف آن‌ها که غالباً همان تنظیمات پیش‌فرض کارخانه هستند آگاهند و از آن‌ها در راستای رسیدن به اهداف خود استفاده می‌کنند.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
سیاست‌گذاری‌های نادرست	دو اصل عمومی که در سیاست‌گذاری اینترنت اشیاء می بایستی درنظرگرفته شود: الف) اینترنت اشیاء نباید هویت، صحت، حریم خصوصی و حقوق بشری یا آزادی‌های فردی یا عمومی را نقض کند. ب) افراد باید کنترل داده‌های شخصی خودشان که توسط یا درون اینترنت اشیاء تولید و پردازش می‌شود را در اختیار	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،

[1] Kombade & Meshram

	داشته باشند، به جز زمانی که این اصل با اصل اول در تعارض باشد.	
عدم مدیریت تغییرات امنیتی	منظور زمانی است که امنیت برقرارشده برای محیط فیزیکی و امنیت سیستم‌ها و... (هر تغییری را می‌تواند شامل شود که قبلاً امنیت داشته‌است) تغییر کند. به‌عنوان مثال، محیط بزرگ‌تر می‌شود، سیستم‌ها تغییر می‌کنند و پیکربندی آن‌ها نسبت به قبل متفاوت باشد، در این صورت اگر این تغییرات مدیریت نشود و امنیت آن‌ها در شرایط جاری برقرار نشود عدم مدیریت تغییرات امنیتی را با خود به همراه دارد.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
عدم کنترل‌های محیطی	می‌تواند همه کنترل‌های محیطی از جمله، کنترل شرایط جوی، سرما، گرما، فشار و... یا کنترل از لحاظ وجود سیستم اطفاء حریق، آشکارکننده نشت گازها و... یا حوادث طبیعی –از جمله بارش باران، رعدوبرق، سیل، آتش‌سوزی، زلزله، یخزدگی و آفتابزدگی– را که باید جهت امینت سیستم‌ها برقرار باشد شامل شود که در غیراینصورت با عدم کنترل‌های محیطی روبرو خواهیم شد.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
ذخیره‌سازی ناامن داده‌ها و پیکربندی‌های مهم	اینترنت اشیاء این امکان را فراهم می‌کند که داده‌ها هم در دستگاه‌های فیزیکی و هم در فضای ابری ذخیره شود. ممکن است اطلاعات شخصی و گواهینامه‌های امنیتی در یک دستگاه اینترنت اشیاء ذخیره شود. بنابراین، امنیت فیزیکی ضعیف باعث می‌شود داده‌های ذخیره‌سازی شده روی دستگاه نسبت به نفوذ آسیب‌پذیر باشند.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
ناهمگونی دستگاه‌ها	در این نوع آسیب‌پذیری، سازندگان دستگاه‌ها بایستی حداکثر الزام‌های امنیتی را برای دستگاه‌هایی که در این بستر قرار می‌گیرند فراهم نمایند. به‌عنوان نمونه از یک جی.پی.اس ساده تا یک توربین بخار	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
محدودیت قابلیت توسعه	زمانی‌که امکان توسعه سیستم وجود نداشته و یا به سختی امکان‌پذیر است. به‌عنوان نمونه، امکان برقراری شبکه اینترنت میسر نباشد یا برای شهری که در دامنه کوه بنا نهاده شده‌است به سختی بتوان سرویس‌های مختلف را در آن زمینه‌سازی و فراهم نمود. در این صورت قابلیت‌های توسعه‌ای محدود گردیده و با چالش همراه خواهد بود.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
اتصال وب ناامن	به منظور اتصال اشیاء هوشمند گوناگون در سراسر جهان، شبکه اینترنت اشیاء نوع ساختار ارتباطی را از میان گزینه‌های بی‌سیم، کابلی، خصوصی و عمومی انتخاب می‌کند. این چندگانگی پروتکل باعث می‌شود شبکه اینترنت اشیاء نسبت به مسائل امنیتی فراوانی از جمله صحت داده، کیفیت سرویس نامناسب و غیره آسیب‌پذیر باشد.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
سرویس شبکه ناامن	یک سرویس شبکه آسیب‌پذیر می‌تواند باعث توقف فعالیت یک دستگاه اینترنت اشیاء شود به طوریکه دستگاه برای کاربران غیر قابل دسترس شود. این حالت زمانی رخ می‌دهد که یک سرویس شبکه نسبت به حملات انسداد سرویس و یا سرریز حافظه بافر آسیب‌پذیر باشد و یا یک پورت غیرضروری شبکه باز و دردسترس باشد.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
رمزگذاری نادرست انتقال	به دلیل داشتن توانایی محاسباتی ضعیف، دستگاه‌های اینترنت اشیاء از رمزنگاری در انتقال داده استفاده نمی‌کنند و یا از انواع ضعیف آن استفاده می‌کنند. بنابراین، ارتباطات برای عوامل مخرب به راحتی قابل کشف و ردیابی می‌باشد.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
پیکربندی امنیتی ناامن	زمانی که کاربر دستگاه توانایی تغییر آن را ندارد، در قالب این آسیب‌پذیری نمود پیدا می‌کند. با مرور دستی رابط وب می‌توان این آسیب‌پذیری را آشکار نمود. پیکربندی امنیتی ناامن می‌تواند منجر به از دست رفتن اطلاعات و آسیب به دستگاه یا سرویس شود.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
نرم‌افزار و میان‌افزار ناامن	عدم توانایی به‌روزرسانی دستگاه، نوعی آسیب‌پذیری امنیتی محسوب می‌شود. به این ترتیب نرم‌افزار و سخت‌افزار مربوطه آسیب‌پذیر خواهند بود. با تحلیل ترافیک شبکه در زمان به‌روزرسانی و بررسی رمزنگاری و... به راحتی می‌توان این آسیب‌پذیری را شناسایی نمود. این آسیب‌پذیری می‌تواند منجر به از دست رفتن اطلاعات، کنترل دستگاه‌ها و صدمه به دیگر دستگاه‌ها از همین طریق شود.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
حفاظت فیزیکی	زمانی که مهاجم می‌تواند دستگاه را به‌منظور دستیابی به رسانه ذخیره‌سازی و داده‌های ذخیره شده آن،	(محمودحسین و همکاران،

ناکافی	مجزا نماید، نمود پیدا می کند. همچنین، این آسیب‌پذیری زمانی که پورت‌های USB یا دیگر پورت‌های خارجی به‌منظور دسترسی به دستگاه مورد استفاده قرار می گیرند، نمایان می‌شود. این آسیب‌پذیری از کارافتادن دستگاه، آشکار شدن و از دست رفتن داده‌های ذخیره شده بر روی آن را با خود به همراه دارد.	۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
کمبود صحت ارتباطات	این آسیب‌پذیری می‌تواند شنود ارتباطات، افزایش نفوذپذیری سیستم و در نتیجه از بین رفتن امنیت را با خود به‌همراه داشته‌باشد.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
معماری امنیت شبکه شکننده	اگر معماری امنیت شبکه سیستم مناسب نباشد و از پیکربندی مناسبی برخوردار نباشد اصطلاحاً گفته می‌شود معماری امنیت شبکه شکننده است. در این صورت اطلاعات سیستم و شبکه می‌تواند شنود گردد و سیستم دچار خدشه شود. دراین‌صورت لازم است معماری مناسبی برای امنیت سیستم برقرار شود و نفوذپذیری سیستم از بین برود.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،
عدم وجود فایروال یا پیکربندی نادرست	سیستم‌های تحت شبکه باید از فایروال مناسب با هدف جلوگیری از نفوذپذیری شبکه استفاده کنند. همچنین شبکه و سیستم باید بطور دقیق و مناسبی پیکربندی شود تا امنیت در آن برقرار شود. درغیر این‌صورت با عدم وجود فایروال یا پیکربندی نادرست روبرو هستیم.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،

آسیب‌پذیری‌ها موجب بروز تهدیدها هستند و از عوامل اصلی ایجاد تهدیدها محسوب می‌شوند. در قسمت بعد تهدیدهای مربوطه معرفی و در راستای روند پژوهش جاری به معرفی تهدیدهای امنیتی در اینترنت اشیاء پرداخته می شود:

تهدیدهای امنیتی حوزه اینترنت اشیاء: هرگونه اقدام برنامه‌ریزی‌شده جهت افشاء، نابودی یا تغییر در داده‌های حیاتی شبکه یا ایجاد اختلال در خدمات معمول سرویس‌دهنده‌ها؛ و به‌طور عام هرگونه اقدام برنامه‌ریزی‌شده برای تحقق یک رخداد خطرناک، یک تهدید امنیتی تلقی می‌شود. در واقع، تهدید امنیتی به عاملی اتلاق می‌شود که می‌تواند موجب بروز یک حادثه امنیتی و زمینه‌ساز بروز خسارت به یک سیستم، سازمان و یا دارایی‌های آن سازمان بشود. تهدیدهای امنیتی در فضای اینترنت اشیاء نقش انکارناپذیری را در مدیریت و عرضه مناسب خدمات این حوزه ایفا می‌نمایند (احمد و اندرو، ۲۰۱۴). در جدول ۳ ابتدا نام تهدید یا حمله، سپس شرح مختصری از هر تهدید و بعد از آن نام مؤلف یا گروه تحقیقاتی به‌همراه سال ارائه آمده‌است:

جدول ۳. تهدیدهای امنیتی حوزه اینترنت اشیاء(مبانی نظری پژوهش)

نام تهدید	توضیحات	مرجع
حمله‌های فیزیکی[1]	این دسته از حمله‌ها با سخت‌افزار اینترنت اشیاء سروکار دارند، به‌طوری‌که اگر یک دستگاه اینترنت اشیاء در دست مهاجم قرار گیرد ممکن است حمله‌های متعددی از قبیل سرقت اطلاعات محرمانه، دستکاری نرم‌افزاری و سخت‌افزاری رخ دهد.	(گائو و همکاران[2]، ۲۰۱۳)، (ساچین و همکاران[3]، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران[4]، ۲۰۱۲)، (ژی و همکاران[5]، ۲۰۱۵)، (قاضی و محمّد[6]، ۲۰۱۴)
خرابی تجهیزات	تجهیزات عملکردشان را ناشی از نیروهای خارجی، محیط و یا قدیمی‌شدن از دست می‌دهند.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
نقص خط	این حمله خرابی خط، خرابی خطوط برق در گره‌ها را با خود به همراه دارد.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
ممانعت از سرویس[7]	حمله‌هایی هستند که پیاده‌سازی آن‌ها باعث وقفه در ارائه خدمات خواهد شد اما برای رسیدن به این هدف، ترکیبی از حمله‌ها متفاوت می‌تواند بوقوع بپیوندد.	(گائو و همکاران، ۲۰۱۳)، (ریاحی و همکاران، ۲۰۱۴) ، (زینگ‌می و همکاران[8]، ۲۰۱۳)، (زینگ و همکاران، ۲۰۱۰)، (لی و ژو، ۲۰۱۱)، (ابومحارا و همکاران، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)، (سارخانا، ۲۰۱۳)
حمله سیل پاکت	این نوع حمله، خسته‌کردن و از پای درآوردن منابع سرورهای شبکه روی لایه شبکه و منجر شدن به حمله DDoS را به همراه دارد.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
تخریب داده دریافتی	مهاجم به‌صورت غیرمجاز، نسبت به افزودن حذف، اصلاح و تخریب داده‌های دریافتی اقدام می‌کند.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
رهگیری داده[9]	در این حمله، مهاجم از طریق متوقف‌کردن کانال‌های ارتباطی به‌صورت غیرمجاز به منابع داده‌ای دسترسی پیدا می‌کند.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
دستکاری داده[10]	در این نوع حمله، مهاجم داده‌ها را رهگیری و تغییر می‌دهد سپس داده‌های تغییریافته را به سمت گیرنده ارسال می‌کند.	(لی و ژو،۲۰۱۱)، (گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)
دسترسی غیرمجاز[11]	منابع، داده‌های شبکه و سیستم توسط کاربران غیرمجاز قابل دسترس می‌شود.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
انسداد سرویس	تلاشی است که سعی دارد منابع یک کامپیوتر را برای کاربران از	(گائو و همکاران، ۲۰۱۳)، (ریاحی و همکاران، ۲۰۱۴) ،

[1] Physical Attack
[2] Gao et al
[3] Sachin et al
[4] Suo et al
[5] Zhi et al
[6] Qazi & Mohamed
[7] Deny of Service
[8] Xu Xingmei et al
[9] Data Tracking
[10] Manipulation
[11] Unauthorized Access

توزیع‌شده[1]	دسترس خارج کند. این حمله به صورتی است که سیلی از درخواست‌هایی که بیش از ظرفیت پاسخ‌دهی قربانی است به سمت وی جاری می‌شود.	(زینگ‌می و همکاران، ۲۰۱۳)، (زینگ و همکاران، ۲۰۱۰)، (لی و ژو، ۲۰۱۱)، (ابومحارا و همکاران، ۲۰۱۴)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)، (سارخانا، ۲۰۱۳)
حمله‌های مسیریابی	مهاجم در فرآیند مسیریابی طبیعی با ارسال اطلاعات مسیریابی جعلی تداخل ایجاد می کند.	(گائو و همکاران، ۲۰۱۳)، (بهاتاسالی و همکاران، ۲۰۱۳)، (لی و ژو، ۲۰۱۱)، (زینگ و همکاران، ۲۰۱۰)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
حمله گمراه‌کننده جهت	گره مخرب، آدرس مبدأ و مقصد بسته‌های داده را تغییر داده و سپس آن‌ها را به یک مسیر اشتباه ارسال می کند، در نتیجه مسیریابی شبکه دچار سردرگمی می‌شود.	(بهاتاسالی و همکاران، ۲۰۱۳)، (لی و ژو، ۲۰۱۱)، (زینگ و همکاران، ۲۰۱۰)، (گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
حمله سیاه چاله[2]	حمله سیاه چاله باعث می‌شود تا همه بسته‌ها دریافت شود ولی ارسال نشود. جذب ترافیک بر مسیر ترافیک اثر خواهد گذاشت و می‌تواند منجر به قطع سرویس شود.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
حمله Sybil	در این حمله، یک گره (شئ) برای خود هویت‌های چندگانه‌ای را ایجاد می کند و این بدان معنا است که یک مهاجم می‌تواند در یک زمان دارای چندین هویت باشد. این حمله باعث کاهش یکپارچگی و امنیت داده‌ها می‌شود. در واقع مهاجم به وسیله حمله Sybil یک لباس مبدل می‌پوشد و سعی می کند رفتار خود را عادی نشان دهد.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
حمله گودال[3]	این حمله، توسط یک نود که اطلاعات و مشخصات آن جعلی است، نودهای همسایه و همجوار آن را گمراه می کند تا اطلاعات آن‌ها را به نود خرابکار بسپارد و مهاجم می‌تواند بر روی اطلاعات هرگونه تغییری از جمله تغییر پیام و یا حتی ردکردن بسته‌ها و سایر حمله‌ها را اعمال نماید.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
حمله کرم چاله[4]	در این حمله، گره‌های بدخواه، پیغام‌هایی را از یک ناحیه از شبکه از روی یک لینک اختصاصی (پر سرعت) هدایت می کنند و آن‌ها را در ناحیه دورتری از شبکه بازپخش می کند.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
حمله حلقه مسیریابی	در این نوع حمله، گره مخرب مسیر داده‌ها را تغییر می‌دهد که منجر به حلقه مسیریابی بی‌نهایت می‌شود.	(گائو و همکاران، ۲۰۱۳)، (بهاتاسالی و همکاران، ۲۰۱۳)، (لی و ژو، ۲۰۱۱)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
اطلاعات مسیریابی کاذب	گره‌مخرب با دستکاری در اطلاعات مسیریابی به لایه شبکه حمله می کند.	(گائو و همکاران، ۲۰۱۳)، (بهاتاسالی و همکاران، ۲۰۱۳)، (لی و ژو، ۲۰۱۱)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
کد بدخواه[5]	مهاجم از طریق ارسال یک کد بدخواه به سیستم موردنظر، امکان انجام فعالیت‌های مخرب روی سیستم هدف را پیدا می کند.	(گائو و همکاران، ۲۰۱۳)، (ردی، ۲۰۱۴)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و

[1] Distributed Denial of Service (DDOS)
[2] Blackhole
[3] Sinkhole
[4] Wormhole
[5] Malicious code

		همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
اسب‌های تروجان	اسب تروا نرم‌افزار مخربی است که ظاهر خود را تغییر می‌دهد تا مقصود اصلی‌اش را از کاربران پنهان کند. تروجان‌ها می‌توانند به هر شکلی از جمله لینک‌های دانلود بی‌آزار، پیوست‌های ایمیلی که از طرف همکاران شما ارسال شده یا تصویری که از رسانه‌های اجتماعی آمده درآیند.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
حمله تزریق کد SQL[1]	به سوءاستفاده مهاجم از کاربردهایی اشاره دارد که بدون بررسی ورودی‌های کاربر و اعتبارسنجی وی، به‌طورمستقیم از روی آن‌ها اقدام به ساخت SQL Query می‌کند.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
تروجان‌های سخت‌افزاری[2]	به هر نوع دستکاری و اعمال تغییرات مخرب با اهداف خاص در مدارات تجهیزات سخت‌افزاری گفته می‌شود.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)، (بونیا و همکاران، ۲۰۱۴)، (شیلا و همکاران، ۲۰۱۴)، (تهرانی‌پور و همکاران، ۲۰۱۰)
استراق سمع[3]	مهاجم به صورت محرمانه اطلاعاتی که در یک ارتباط خصوصی مبادله می‌شود را شنود می‌کند. دستگاه‌های RFID یکی از آسیب‌پذیرترین انواع دستگاه‌ها نسبت به این نوع حملات در فناوری اینترنت اشیاء محسوب می‌شوند. این دسته از حملات محرمانگی پیام‌ها را مورد تهدید قرار می‌دهند.	(ریاحی و همکاران، ۲۰۱۴) ، (لی و همکاران ۲۰۱۴)، (بَت‌سالی و همکاران، ۲۰۱۳)، (زینگ و همکاران،۲۰۱۰)، (لی و ژو،۲۰۱۱)، (گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)، (مورجی، ۲۰۱۵)
ارتباطات غیرمعتبر	هر گره برای به‌اشتراک‌گذاشتن داده‌ها و دسترسی به داده‌های سایر گره‌ها نیازمند برقراری ارتباط با سایر گره‌ها است. این گره فقط باید با مجموعه‌ای از گره‌هایی که به اطلاعات آن‌ها نیاز دارد، ارتباط برقرار کند و این نیازمندی یک موضوع حیاتی برای سیستم‌های اینترنت اشیاء متشکل از گره‌های امن و غیرامن می‌باشد.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)
تزریق پاکت مخرب	مهاجم می‌تواند به سه طریق مختلف ارسال، تغییر و تکرار این پاکت-های مخرب را در لینک‌های ارتباطی تزریق کند. در سناریوی ارسال، مهاجم می‌تواند یک سری پاکت مخرب که به نظر معتبر می‌رسند را تولید و در لینک‌های ارتباطی ارسال کند. در سناریوی تغییر، فرد مهاجم یک پاکت معتبر را دریافت و پس از آن با ایجاد تغییراتی در آن، پاکت خراب شده را در لینک ارتباطی ارسال کند. در سناریوی تکرار هم فرد مهاجم اقدام به ارسال پاکتی می‌کند که قبلا بین دو گره شبکه رد و بدل شده است.	(گائو و همکاران، ۲۰۱۳)، (ساچین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمّد، ۲۰۱۴)

[1] SQL Injection
[2] Hardware Trojan
[3] Eavesdropping

تهدیدهای اینترنت اشیاء برای عملیاتی شدن نیاز به عوامل پیاده‌سازی نیز دارند. این عوامل را می‌توان منشاء تهدید به حساب آورد. عوامل پیاده‌سازی تهدیدها می‌تواند از جانب کاربران مخرب، سازندگان و فروشندگان متقلب و مهاجمین خارجی به‌کار گرفته شوند. لذا از دیدگاهی دیگر عوامل ذکرشده می‌توانند جزئی از تهدیدهای اینترنت اشیاء محسوب گردند.

هدف اصلی این پژوهش، شناسایی آسیب‌پذیری‌ها و تهدیدهای امنیتی در فضای اینترنت اشیاء و ارائه راهکارهای امنیتی جهت مواجهه با آن‌ها است. باتوجه به هدف اصلی، اهداف فرعی موردنظر در این پژوهش عبارتند از: تحلیل و شناسایی آسیب‌پذیری‌ها و تهدیدهای رایج و نگاشت هریک از تهدیدهای شناخته‌شده به آسیب‌پذیری‌های مربوطه است.

در راستای دستیابی به‌هدف پژوهش، سؤالاتی که در این باره مطرح می‌شود به شرح ذیل است:

۱. آسیب‌پذیری‌های امنیتی رایج در فضای اینترنت‌اشیاء کدامند؟

۲. تهدیدهای امنیتی که اینترنت اشیاء را تحت تأثیر قرار می‌دهند کدامند؟

۳. تهدیدهای امنیتی نشأت‌گرفته از آسیب‌پذیری‌های شناخته شده کدامند؟

۴. راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در فضای اینترنت‌اشیاء کدامند؟

روش پژوهش

هدف از تحقیق حاضر ارائه راهکارهای امنیتی جهت مواجهه با تهدیدهای شناسایی شده در فضای اینترنت اشیاء است. باتوجه به نوظهور بودن مفهوم اینترنت اشیاء و به تبع آن موضوع امنیت، تحقیق حاضر از منظر هدف کاربردی و از منظر روش تحقیق توصیفی-پیمایشی است. باتوجه به اینکه مبنای این تحقیق بر پایه توصیف وقایع موجود استوار است و به شرایط، روابط موجود، عقاید متداول، فرآیندهای جاری و روندها توجه دارد. تمرکز آن در درجه اول به زمان حال است، هرچند غالباً رویدادها و آثار گذشته را نیز که به شرایط موجود مرتبط اند مورد بررسی قرار می‌دهد. از دیگر ویژگی‌های این تحقیق این است که محققان دخالتی در موقعیت، وضعیت و نقش متغیرها نخواهند داشت و در آن‌ها هیچگونه دستکاری یا تغییر اعمال نمی‌کنند و صرف آنچه را وجود دارد، مطالعه می‌نمایند و به تشریح آن می‌پردازند.

باتوجه به زمان و منابع در اختیار، برای انجام تحقیق از اساتید دانشگاهی و متخصصان حوزه فناوری اطلاعات دانشگاه های دولتی شهر تهران استفاده شده‌است که مقوله اینترنت اشیاء را در سرفصل‌های آموزشی یا پژوهشی خود قرار داده‌اند؛ پیرامون آن تألیفی داشته؛ و یا مقاله‌ای را به رشته تحریر درآورده‌اند. براین اساس، جامعه آماری محدودی با ۵۰ نفر از اساتید دانشگاهی و متخصصان حوزه فناوری اطلاعات دانشگاه های دولتی شهر تهران پیش‌روی محققین شناسایی شد. همه افراد دارای سوابق تدریس در مقطع کارشناسی ارشد و دکترای دانشگاه‌های دولتی هستند و از فعالیت‌های پژوهشی مرتبط با اینترنت اشیاء برخوردارند.

در این پژوهش به دلیل محدود بودن جامعه آماری، نمونه آماری به‌صورت هدفمند و به روش نمونه گیری سرشماری انتخاب شده است. در نمونه‌گیری هدفمند، قصد محقق انتخاب مواردی است که باتوجه به هدف تحقیق، اطلاعات زیادی داشته باشند. در نمونه‌گیری هدفمند، هدف، انتخاب نمونه‌ای که دقیقاً معرف جامعه تعریف شده باشد نیست. بلکه قصد آن است که از طریق افراد انتخاب‌شده درک عمیقی از موضوع موردمطالعه حاصل گردد.

در این پژوهش برای شناسایی تهدیدها و آسیب‌پذیری‌های رایج در حوزه اینترنت اشیاء از مطالعه نظام مند ادبیات موضوعی استفاده شده‌است و چون به‌صورت پژوهشی از پرسشنامه برای جمع‌آوری داده‌های آن استفاده شده و محققین عملاً در جریان تحقیق درگیر شده‌اند، لذا تحقیق از لحاظ نحوی گردآوری داده‌ها، از نوع تحقیقات میدانی به‌شمار می‌رود.

در پژوهش حاضر، روش تجزیه و تحلیل داده ها به دو صورت زیر انجام گرفته است:

۱. *آمار توصیفی:* شامل جداول آماری و توزیع فراوانی است

۲. *آمار استنباطی:* برای بررسی سوالات پژوهش و نتیجه‌گیری از روش‌های آماری و آزمون های متفاوت با استفاده از نرم‌افزار SPSS22 استفاده گردید.

یافته‌ها

یافته‌های حاصل از این پژوهش را می‌توان در دو مرحله تجزیه‌وتحلیل آمار توصیفی و آمار استنباطی به شرح زیر بررسی نمود:

جدول ٤. توزیع فراوانی نمونه براساس جنسیت

جنسیت			
	مرد	زن	مجموع
فراوانی	۳۹	۱۱	۵۰
درصد	۷۸	۲۲	۱۰۰
سطح تحصیلات			
	کارشناسی‌ارشد	دکتری	مجموع
فراوانی	۳۲	۱۸	۵۰
درصد	۶۴	۳۶	۱۰۰
گروه سنی			
	زیر ۲۵ سال	۲۵ تا ۳۵ سال	۳۶ تا ۴۵ سال	مجموع
فراوانی	۵	۲۸	۱۷	۵۰
درصد	۱۰	۵۶	۳۴	۱۰۰
سابقه خدمت				
	زیر ۱۰ سال	۱۰ تا ۱۵ سال	بیش از ۱۵ سال	مجموع
فراوانی	۱۵	۳۰	۵	۵۰
درصد	۳۰	۶۰	۱۰	۱۰۰

در نمونه مورد مطالعه در این تحقیق (۷۸) درصد از پاسخگویان مرد و بقیه (۲۲) درصد زن بودند. هرچند در این تحقیق، اثر جنسیت بر نتایج تحقیق موردتوجه محقق نبوده‌است، اما این مسئله که اکثریت نمونه مورد مطالعه مرد بوده اند ممکن است بر نتایج تحقیق مؤثر بوده باشد؛ اکثر پاسخ دهندگان (۵۶ درصد) در گروه سنی (۳۵-۲۵) سال قرار دارند؛ از نظر تحصیلات نیز اکثر افراد فوق‌لیسانس(۳۶ درصد) و دکترا (۶۴ درصد) بوده اند. سابقه خدمت اکثر آنها نیز ۱۰ تا ۱۵ سال (۶۰ درصد) بوده است. در تحقیق حاضر، محقق به دنبال پاسخ به دو سؤال کلیدی بود که شناسایی آسیب‌پذیری‌ها و تهدیدهای امنیتی در فضای اینترنت اشیاء و ارائه راهکارهای امنیتی جهت مواجهه با این تهدیدها را شامل می‌شد. در این راستا، مبنای عمل محقق بر ارائه راهکارهای امنیتی جهت مواجهه با گستره وسیعی از تهدیدها و آسیب‌پذیری‌های امنیتی شناسایی شده قرار گرفته‌است. برای این منظور تحلیل ادبیات موضوعی و استفاده از نظرهای خبرگان در دستور کار محقق قرار گرفته که نتیجه امر در قالب جدول ۲۸ ارائه شده‌است.

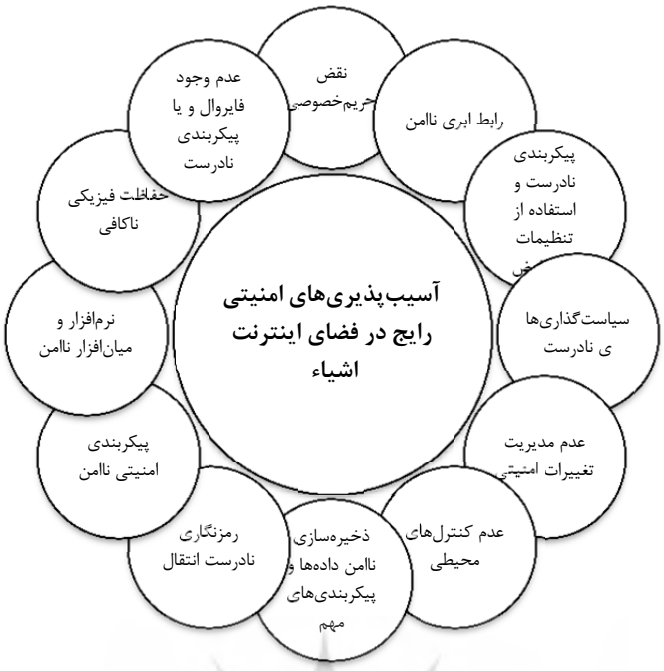
سوال اول پژوهش: آسیب‌پذیری‌های امنیتی رایج در فضای اینترنت اشیاء کدامند؟

آنچه در مرور اجمالی نظرسنجی افراد در جامعه مورد بررسی به چشم می‌خورد، این بود که از منظر عمده آن‌ها آسیب‌پذیری‌هایی که در جدول ۵ و شکل ۱ به‌تصویر کشیده شده‌است به‌عنوان آسیب‌پذیری‌های امنیتی رایج در حوزه اینترنت اشیاء مطرح هستند:

جدول ٥. توزیع فراوانی آسیب‌پذیری‌ها

آسیب‌پذیری	کاملاً موافق	موافق	نظری ندارم	مخالف	کاملاً مخالف	مجموع
احراز و تشخیص هویت ناکافی	۹	۳۱	۵	۳	۲	۵۰
نقض حریم‌خصوصی	۳۰	۶	۹	۳	۲	۵۰
رابط ابری ناامن	۳۲	۶	۷	۴	۱	۵۰
رابط سیار ناامن	۶	۲۹	۱۰	۲	۳	۵۰
توسعه نادرست پچ سیستم‌عامل و نرم‌افزار	۷	۳۰	۵	۳	۵	۵۰
پیکربندی نادرست و استفاده از تنظیمات پیش‌فرض	۳۵	۵	۴	۳	۳	۵۰
سیاست‌گذاری‌های نادرست	۲۸	۸	۶	۵	۳	۵۰
عدم مدیریت تغییرات امنیتی	۳۲	۱۰	۵	۲	۱	۵۰
عدم کنترل‌های محیطی	۲۹	۷	۱۰	۲	۲	۵۰
ذخیره‌سازی ناامن داده‌ها و پیکربندی‌های مهم	۲۷	۱۰	۵	۴	۴	۵۰
ناهمگونی دستگاه‌ها	۵	۷	۳۳	۳	۲	۵۰
محدودیت قابلیت توسعه	۲	۳	۱۰	۳۰	۵	۵۰
اتصال وب ناامن	۲	۴	۵	۳۳	۶	۵۰
سرویس شبکه ناامن	۶	۳۲	۴	۴	۴	۵۰
رمزگذاری نادرست انتقال	۳۱	۶	۵	۶	۲	۵۰
پیکربندی امنیتی ناامن	۲۸	۸	۷	۵	۲	۵۰
نرم‌افزار و میان‌افزار ناامن	۳۰	۶	۴	۷	۳	۵۰
حفاظت فیزیکی ناکافی	۳۵	۵	۴	۴	۲	۵۰
کمبود صحت ارتباطات	۶	۴	۳۰	۵	۵	۵۰
معماری امنیت شبکه شکننده	۷	۳۱	۶	۳	۳	۵۰
عدم وجود فایروال یا پیکربندی نادرست	۳۰	۸	۷	۳	۲	۵۰

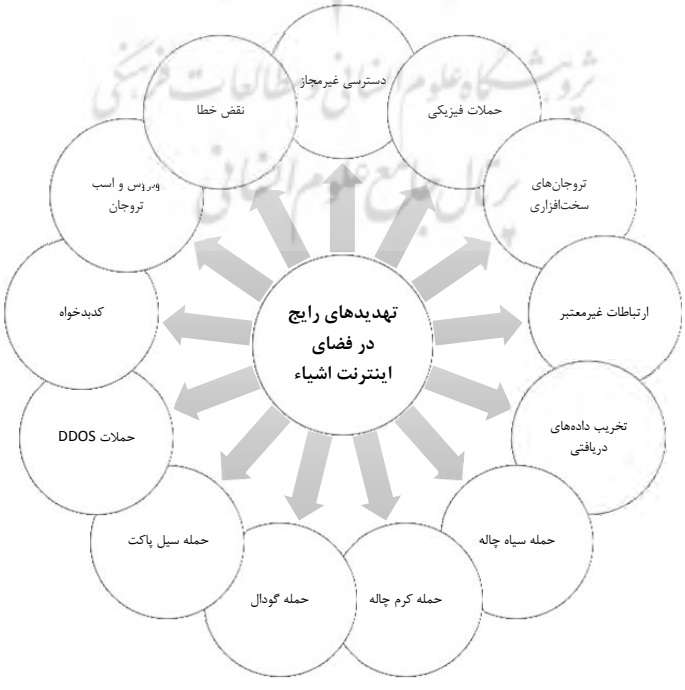
مطابق جدول ۵ آسیب‌پذیری‌ها در ۲۱ آیتم طبقه‌بندی شده‌اند که در ۱۲ گروه کلی می توان جمع بندی نمود. این ۱۲ گروه آسیب پذیری به ترتیب نقض حریم‌خصوصی، رابط ابری ناامن، پیکربندی نادرست و استفاده از تنظیمات پیش‌فرض، سیاست‌گذاری‌های نادرست، عدم مدیریت تغییرات امنیتی، عدم کنترل‌های محیطی، ذخیره‌سازی ناامن داده‌ها و پیکربندی‌های مهم، رمزگذاری نادرست انتقال، پیکربندی امنیتی ناامن، نرم‌افزار و میان‌افزار ناامن، حفاظت فیزیکی ناکافی، عدم وجود فایروال یا پیکربندی نادرست دارای بیشترین اهمیت بوده‌است(شکل ۱):



شکل ۱. آسیب‌پذیری‌های رایج در حوزه اینترنت اشیاء

سوال دوم پژوهش: تهدیدهای امنیتی که اینترنت اشیاء را تحت تأثیر قرار می‌دهند کدامند؟

باتوجه به تجزیه‌وتحلیل نظرات افراد در جامعه مورد بررسی پیرامون تأیید نقش تهدیدهای امنیتی در حوزه اینترنت اشیاء، این سئوال به ذهن مخاطب خطور می‌کند که تهدیدهای امنیتی که فضای اینترنت اشیاء را تحت تأثیر قرار می‌دهد کدامند. در پاسخ به این سئوال، تهدیدهای امنیتی که دارای بیشترین حوزه اثر در این فضا هستند در قالب شکل ۲ به تصویر کشیده شده‌است:



شکل ۲: تهدیدهای رایج در حوزه اینترنت اشیاء

سوال سوم پژوهش: تهدیدهای امنیتی نشأت گرفته از آسیب‌پذیری‌های شناخته شده کدامند؟

باتوجه به اینکه آسیب‌پذیری‌ها منشأ اصلی بروز تهدیدها هستند. به ازای هر آسیب‌پذیری، حمله‌ها و تهدیدهای بالقوه‌ای وجود دارند که از محل آسیب‌پذیری امکان بروز پیدا می‌کنند. همچنین برای مقابله با این تهدیدها راهکارها و الزام‌های امنیتی وجود دارد که باید رعایت شوند.

جدول ٦. توزیع فراوانی تهدیدهای نشأت گرفته از آسیب پذیری ها

آسیب پذیری	تهدید	کاملاً موافق	موافق	نظری ندارم	مخالف	کاملاً مخالف	مجموع
آسیب‌پذیری احراز و تشخیص هویت ناکافی	دسترسی غیرمجاز	۸	۲۸	۷	۵	۲	۵۰
	حملات فیزیکی	۳۰	۶	۴	۷	۳	۵۰
	تروجان‌های سخت‌افزاری	۳۵	۵	۴	۴	۲	۵۰
	استراق سمع	۷	۳۱	۶	۴	۲	۵۰
آسیب‌پذیری نقض حریم‌خصوصی	استراق سمع	۸	۲۹	۷	۴	۲	۵۰
	دسترسی غیرمجاز	۳۰	۷	۶	۵	۲	۵۰
	ارتباطات غیر معتبر	۳۱	۹	۷	۲	۱	۵۰
	حملات فیزیکی	۶	۳۰	۵	۶	۳	۵۰
آسیب‌پذیری پیکربندی نادرست و استفاده	خرابی تجهیزات	۷	۲۹	۸	۳	۳	۵۰
	نقص خط	۳۱	۷	۶	۳	۳	۵۰
	تخریب داده‌های دریافتی	۳۰	۸	۶	۴	۲	۵۰
	رهگیری داده	۸	۳۰	۶	۳	۳	۵۰
آسیب‌پذیری رمزگذاری نادرست انتقال	تزریق پاکت مخرب	۶	۳۲	۵	۴	۳	۵۰
	حمله سیاه چاله	۳۱	۷	۶	۳	۳	۵۰
	حمله کرم چاله	۲۹	۸	۶	۵	۲	۵۰
	حملات مسیریابی	۵	۳۳	۵	۴	۳	۵۰
آسیب‌پذیری اتصال وب ناامن	DOS حملات	۷	۲۹	۸	۳	۳	۵۰
	حمله سیاه چاله	۳۱	۷	۶	۳	۳	۵۰
	حمله گودال	۳۰	۸	۶	۴	۲	۵۰
	حملات مسیریابی	۸	۳۰	۶	۳	۳	۵۰
آسیب‌پذیری معماری امنیت شبکه شکننده	Sybilحمله	۶	۳۲	۵	۴	۳	۵۰
	حمله سیل پاکت	۳۱	۷	۶	۳	۳	۵۰
	DDOSحملات	۲۹	۸	۶	۵	۲	۵۰
	حمله حلقه مسیریابی	۵	۳۳	۵	۴	۳	۵۰
آسیب‌پذیری پیکربندی امنیتی ناامن	دسترسی غیرمجاز	۸	۲۹	۷	۴	۲	۵۰
	کدبدخواه	۳۰	۷	۶	۵	۲	۵۰
	ویروس و اسب تروژان	۳۱	۹	۷	۲	۱	۵۰
	SQL حمله تزریق	۶	۳۰	۵	۶	۳	۵۰

مطابق جدول ۶، در مورد **تهدیدهای نشأت گرفته از آسیب پذیری ها** می توان گفت اگر هر یک از این آسیب پذیری ها صورت نپذیرد این تهدیدها می توانند به عنوان عاملی برای آسیب‌رسانی به سیستم محسوب شوند. باتوجه به جدول فوق، تروجان سخت‌افزاری، استراق سمع، دسترسی غیرمجاز و حملات فیزیکی به‌ترتیب به‌عنوان بیشترین تهدید برای آسیب‌پذیری احراز و تشخیص هویت ناکافی درنظرگرفته می‌شوند؛ همین طور، ارتباطات غیرمعتبر، دسترسی غیرمجاز، استراق سمع و حملات فیزیکی به‌ترتیب به‌عنوان بیشترین تهدید برای آسیب‌پذیری نقض حریم‌خصوصی درنظرگرفته می‌شوند؛ نقص خط، تخریب داده‌های دریافتی، رهگیری داده و خرابی تجهیزات نیز به‌ترتیب به‌عنوان بیشترین تهدید برای آسیب‌پذیری پیکربندی نادرست و استفاده از تنظیمات پیش‌فرض درنظرگرفته می‌شوند؛ حمله سیاه چاله، و حمله کرم چاله، تزریق پاکت مخرب و حملات مسیریابی را می توان به‌ترتیب به‌عنوان بیشترین تهدید برای آسیب‌پذیری رمزگذاری نادرست انتقال در نظر گرفت؛ حمله سیاه چاله، حمله گودال، حملات مسیریابی و حملات DOS به‌ترتیب به‌عنوان بیشترین تهدید برای آسیب‌پذیری اتصال وب ناامن درنظرگرفته می‌شوند؛ همچنین حمله سیل پاکت، حملات DDOS، حمله Sybil، و حمله حلقه مسیریابی به‌ترتیب به‌عنوان بیشترین تهدید برای آسیب‌پذیری معماری امنیت شبکه شکننده درنظرگرفته می‌شوند ودرنهایت اگر پیکربندی امن برای سیستم صورت نپذیرد این تهدید می‌تواند به‌عنوان عاملی برای آسیب‌رسانی به سیستم درنظرگرفته شود. باتوجه به جدول فوق، ویروس و اسب تروژان، کد بدخواه، دسترسی غیرمجاز و حمله تزریق SQL به ترتیب به‌عنوان بیشترین تهدید برای آسیب‌پذیری پیکربندی امنیتی ناامن درنظرگرفته می‌شوند.

اما از آنجایی‌که هدف اصلی این پژوهش ارائه راهکارهای امنیتی در فضای اینترنت اشیاء است و هر آسیب‌پذیری منجر به ایجاد تهدیدها و حمله‌ها می‌شود، به نگاشت تهدیدها بر آسیب‌پذیری‌ها پرداخته می شود. جدول ۶ نگاشت تهدیدها بر آسیب‌پذیری‌ها را نشان می‌دهد:

جدول ۷. نگاشت تهدیدها بر آسیب‌پذیری‌ها

آسیب‌پذیری / تهدید	احراز و تشخیص هویت ناکافی	نقض حریم‌خصوصی	پیکربندی نادرست و استفاده از تنظیمات پیش‌فرض	رمزنگاری نادرست انتقال	اتصال وب ناامن	معماری امنیت شکننده	پیکربندی امنیتی ناامن
دسترسی غیرمجاز	✓	✓					✓
حملات فیزیکی	✓	✓					
تروجان‌های سخت‌افزاری	✓						
ارتباطات غیرمعتبر		✓					
نقض خطا			✓				
تخریب داده‌های دریافتی			✓				
حمله سیاه چاله				✓	✓		
حمله انسداد سرویس توزیع شده					✓	✓	
کدبدخواه							✓
حمله کرم چاله				✓			
اسب تروجان							✓
حمله گودال					✓		
حمله سیل پاکت						✓	

یافته های جدول بالا نیز موید نگاشت انواع تهدیدهای مطرح شده بر آسیب پذیری ها است.

سوال چهارم پژوهش: راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در حوزه اینترنت‌اشیاء کدامند؟

اما آخرین سئوال تحقیق به راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در فضای اینترنت اشیاء اشاره دارد. در پاسخ به این سئوال، باتوجه به بررسی‌های به‌عمل آمده از مبانی نظری تحقیق و نتایج بدست آمده از نظرسنجی افراد در جامعه مورد بررسی در جداول زیر می‌توان راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در حوزه اینترنت اشیاء را به‌صورت شکل ۳ پیشنهاد نمود:

جدول ۸. توزیع فراوانی الزام‌های امنیتی جهت مواجهه با آسیب‌پذیری ها

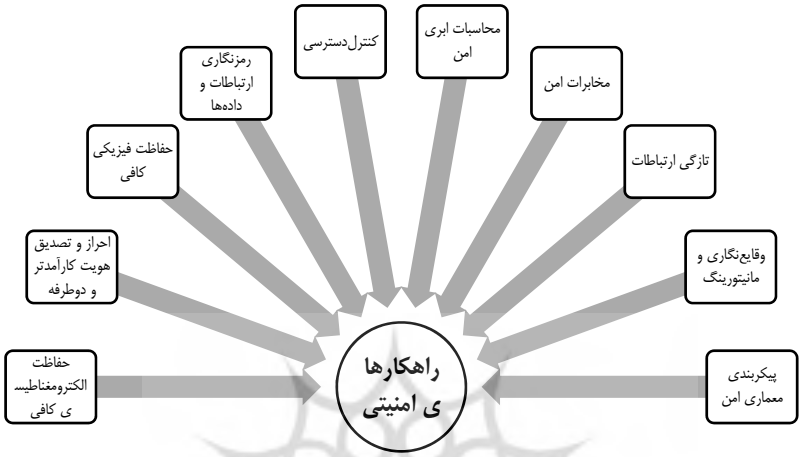
آسیب پذیری	الزام‌های امنیتی	کاملاً موافق	موافق	نظری ندارم	مخالف	کاملاً مخالف	مجموع
آسیب‌پذیری احراز و تشخیص هویت ناکافی	حفاظت الکترومغناطیسی کافی	۶	۳۲	۵	۴	۳	۵۰
	احراز و تصدیق هویت کارآمدتر	۳۱	۷	۶	۳	۳	۵۰
	حفاظت فیزیکی کافی	۲۹	۸	۶	۵	۲	۵۰
	رمزنگاری ارتباطات و داده‌ها	۵	۳۳	۵	۴	۳	۵۰
آسیب‌پذیری نقض حریم‌خصوصی	حفاظت الکترومغناطیسی کافی	۷	۲۹	۸	۳	۳	۵۰
	احراز و تصدیق هویت کارآمدتر و دو طرفه	۳۱	۷	۶	۳	۳	۵۰
	کنترل دسترسی	۳۰	۸	۶	۴	۲	۵۰
	رمزنگاری ارتباطات و داده‌ها	۸	۳۰	۶	۳	۳	۵۰
آسیب پذیری رابط ابری ناامن	حفاظت فیزیکی کافی	۸	۲۹	۷	۴	۲	۵۰
	حفاظت الکترومغناطیسی کافی	۳۰	۷	۶	۵	۲	۵۰
	محاسبات ابری امن	۳۱	۹	۷	۲	۱	۵۰
	رمزنگاری ارتباطات و داده‌ها	۶	۳۰	۵	۶	۳	۵۰
آسیب‌پذیری رابط سیّارناامن	مخابرات امن	۷	۳۱	۶	۳	۳	۵۰
	احراز و تصدیق هویت کارآمدتر	۳۲	۶	۵	۴	۳	۵۰
	محاسبات ابری امن	۳۰	۵	۴	۶	۵	۵۰
	رمزنگاری ارتباطات و داده‌ها	۵	۳۲	۶	۵	۲	۵۰
آسیب‌پذیری اتصال وب ناامن	حفاظت الکترومغناطیسی کافی	۷	۲۹	۸	۳	۳	۵۰
	احرازو تصدیق هویت کارآمدترو دوطرفه	۳۱	۷	۶	۳	۳	۵۰
	کنترل دسترسی	۳۰	۸	۶	۴	۲	۵۰
	رمزنگاری ارتباطات و داده‌ها	۸	۳۰	۶	۳	۳	۵۰
آسیب‌پذیری سرویس شبکه ناامن	حفاظت الکترومغناطیسی کافی	۶	۳۲	۵	۴	۳	۵۰
	احراز و تصدیق هویت کارآمدتر	۳۱	۷	۶	۳	۳	۵۰
	تازگی ارتباطات	۲۹	۸	۶	۵	۲	۵۰
	کنترل دسترسی	۵	۳۳	۵	۴	۳	۵۰
آسیب‌پذیری رمزگذاری نادرست	تازگی ارتباطات	۷	۳۱	۶	۳	۳	۵۰
	احرازوتصدیق هویت کارآمدتر ودوطرفه	۳۲	۶	۵	۴	۳	۵۰
	کنترل دسترسی	۳۰	۵	۴	۶	۵	۵۰
	رمزنگاری ارتباطات و داده‌ها	۵	۳۲	۶	۵	۲	۵۰

آسیب‌پذیری پیکربندی امنیتی ناامن	وقایع نگاری و مانیتورینگ	۶	۳۲	۵	۴	۳	۵۰
	پیکربندی معماری امن	۳۱	۷	۶	۳	۳	۵۰
	کنترل دسترسی	۲۹	۸	۶	۵	۲	۵۰
	رمزنگاری ارتباطات و داده ها	۵	۳۳	۵	۴	۳	۵۰
آسیب‌پذیری نرم‌افزار و میان‌افزار ناامن	حفاظت الکترومغناطیسی کافی	۸	۲۹	۷	۴	۲	۵۰
	احراز و تصدیق هویت کارآمدترو دو طرفه	۳۰	۷	۶	۵	۲	۵۰
	کنترل دسترسی	۳۱	۹	۷	۲	۱	۵۰
	رمزنگاری ارتباطات و داده‌ها	۶	۳۰	۵	۶	۳	۵۰
آسیب‌پذیری حفاظت فیزیکی ناکافی	حفاظت فیزیکی کافی	۷	۳۱	۶	۳	۳	۵۰
	احراز و تصدیق هویت کارآمدتر	۳۲	۶	۵	۴	۳	۵۰
	کنترل دسترسی	۳۰	۵	۴	۶	۵	۵۰
	رمزنگاری ارتباطات و داده‌ها	۵	۳۲	۶	۵	۲	۵۰
آسیب‌پذیری کمبود صحت ارتباطات	حفاظت فیزیکی کافی	۸	۲۹	۷	۴	۲	۵۰
	احراز و تصدیق هویت کارآمدتر و دوطرفه	۳۰	۷	۶	۵	۲	۵۰
	کنترل دسترسی	۳۱	۹	۷	۲	۱	۵۰
	رمزنگاری ارتباطات و داده ها	۶	۳۰	۵	۶	۳	۵۰

داده های جدول ۸ نشان دهنده آن است که، اگر هر کدام از این آسیب‌پذیری ها در سیستم وجود داشته باشد، می‌تواند به‌عنوان عاملی برای تهدیدها و آسیب‌رسانی به سیستم درنظرگرفته شوند. باتوجه به جدول فوق، احراز و تصدیق هویت کارآمدتر، حفاظت فیزیکی کافی، حفاظت الکترومغناطیسی کافی و رمزنگاری ارتباطات و داده‌ها به‌ترتیب به‌عنوان بیشترین الزام امنیتی برای مواجهه با آسیب‌پذیری احراز و تشخیص هویت ناکافی درنظرگرفته می‌شوند؛ احراز و تصدیق هویت کارآمدتر و دوطرفه، کنترل دسترسی، حفاظت الکترومغناطیسی کافی و رمزنگاری ارتباطات و داده‌ها به‌ترتیب به‌عنوان بیشترین الزام امنیتی برای مواجهه با آسیب‌پذیری نقض حریم‌خصوصی درنظرگرفته می‌شوند؛ محاسبات ابری امن، حفاظت الکترومغناطیسی کافی، حفاظت فیزیکی کافی و رمزنگاری ارتباطات و داده‌ها به‌ترتیب به‌عنوان بیشترین الزام امنیتی برای مواجهه با آسیب‌پذیری رابط ابری ناامن درنظرگرفته می‌شوند؛ احراز و تصدیق هویت کارآمدتر و دوطرفه، کنترل‌دسترسی، رمزنگاری ارتباطات و داده ها و حفاظت الکترومغناطیسی کافی به‌ترتیب به‌عنوان بیشترین الزام امنیتی برای مواجهه با آسیب‌پذیری اتصال وب ناامن درنظرگرفته می‌شوند؛ احراز و تصدیق هویت کارآمدتر، تازگی ارتباطات، حفاظت الکترومغناطیسی کافی و کنترل‌دسترسی به ترتیب به‌عنوان بیشترین الزام امنیتی برای مواجهه با آسیب‌پذیری سرویس شبکه ناامن درنظرگرفته می شوند.

همچنین، احراز و تصدیق هویت کارآمدتر و دوطرفه، کنترل دسترسی، تازگی ارتباطات و رمزنگاری ارتباطات و داده ها به ترتیب به‌عنوان بیشترین الزام امنیتی برای مواجهه با آسیب‌پذیری رمزگذاری نادرست انتقال درنظرگرفته می‌شوند؛ پیکربندی معماری امن، کنترل‌دسترسی، وقایع نگاری و مانیتورینگ و رمزنگاری ارتباطات و داده‌ها به‌ترتیب به‌عنوان بیشترین الزام امنیتی برای مواجهه با آسیب‌پذیری پیکربندی امنیتی ناامن درنظرگرفته می‌شوند؛کنترل‌دسترسی، احراز و تصدیق هویت کارآمدتر و دوطرفه، حفاظت الکترومغناطیسی کافی و رمزنگاری ارتباطات و داده‌ها به‌ترتیب به‌عنوان بیشترین الزام امنیتی برای مواجهه با آسیب‌پذیری نرم‌افزار و میان‌افزار ناامن درنظرگرفته می

شوند؛ احراز و تصدیق هویت کارآمدتر و دو طرفه، کنترل دسترسی، حفاظت فیزیکی کافی و رمزنگاری ارتباطات و داده‌ها به‌ترتیب به‌عنوان بیشترین الزام امنیتی برای مواجهه با آسیب‌پذیری حفاظت فیزیکی ناکافی درنظرگرفته می‌شوند و درنهایت، احراز و تصدیق هویت کارآمدتر و دو طرفه، حفاظت فیزیکی کافی و رمزنگاری ارتباطات و داده‌ها به‌ترتیب به‌عنوان بیشترین الزام امنیتی برای مواجهه با آسیب‌پذیری کمبود صحت ارتباطات درنظرگرفته می‌شوند.



شکل ۳. راهکارهای امنیتی امنیتی حوزه اینترنت اشیاء

بحث و نتیجه گیری

هدف از این پژوهش شناسایی تهدیدها و آسیب‌پذیری‌های رایج اینترنت اشیاءو ارائه راهکارهای امنیتی جهت مواجهه با آن ها است اینترنت اشیاء می‌تواند به آینده بهتر و رویایی منجر شود که حداکثر بهره برداری با کم‌ترین تلاش را داشته باشد و این سیستم را آسان تر و کاربر پسند می‌دانند که یک رویکرد منظم در مدیریت اطلاعات است(وندانا، باتاچارجی و گوپتا، ۲۰۱۷). ولی با این حال بنسال، آرورا ،سوری (۲۰۱۸) بیان می‌کنند که فن‌آوری‌های جدید چالش‌های جدیدی را نیز به همراه دارند. مانند نحوه استفاده، نوع اشکالات و چگونگی بهبودآ نها و غیره. آن‌ها برخی از چالش‌های این فن‌آوری را چنین اعلام می‌کنند:

۱ – حریم خصوصی و امنیت: کاربران برای بهره‌مندی از فن‌آوری اینترنت اشیاء تلفن همراه خود را همیشه فعال نگه میدارند و با فعال شدن وضعیت موقعیت مکانی، موقعیت مکانی آن‌ها ردیابی می شود. یا به حریم خصوصی آن‌ها ورود کنند و از محتویات تلفن آن‌ها مانند عکس و اسناد و غیره سوء استفاده کنند و حریم شخصی آن‌ها به خطر افتد.

۲ – دقت در درک و فهمیدن: این که فن‌آوری اینترت اشیاء بسیار دقیق باشد ضروری است و بایستی سیستم معنایی را درک کند تا نیاز کاربر را بدون ابهام درک کند در غیر این صورت کل سیستم شکست خواهد خورد.

۳- معاملات: امروزه معاملات متعددی با تلفن همراه انجام می‌شود و کارت بانکی یا کیف پول با تلفن همراه همگام سازی می شود. با قرار گرفتن(ناخودآگاه یا آگاهانه) تلفن همراه مقابل سنسور پرداخت و یا خرید این موارد در معرض خطر وجود دارد.

۴ – هک شدن: تلفن ها قابل هک شدن هستند و اطلاعات قابل دسترسی هستند.

۵ – هزینه: هزینه‌هایی مانند برچسب‌ها، سنسورها، محرک ها، دستگاه‌های ارتباط، اتصال به اینترنت و غیره که نیاز به سرمایه گذاری دارد.

این فن‌آوری نوپا، در بدو تولد خود به شدت به موضوع امنیت توجه نشان داده است. شرکت‌های گوگل، سامسونگ، سونی و دیگر غول‌های فن‌آوری که به نوعی در رشد یافتن این فن‌آوری نقش داشته‌اند، رعایت ایمنی را یکی از اصول اولیه کار قرار داده‌اند

اما به اعتقاد کارشناسان، اینترنت اشیاء بعد از عبور از مرحله "ایمن نمایشی" به مرحله "خطرناک در حال کار" خواهد رسید و بی‌شک، برخورد واقعی با بدافزار نویسان، شرایط را به گونه دیگری تغییر خواهد داد(شفیعی،-۱۳۹۴).

در راستای این مباحث، نتایج این پژوهش نیز بیان می دارد اگرچه اساتید و متخصصان حوزه فناوری اطلاعات دانشگاه های مذکور حسب دیدگاه و حوزه فعالیت خود، مجموعه متنوعی را به‌عنوان راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در حوزه اینترنت اشیاء تبیین نموده‌اند، اما در یک نگاه کلی و با جمع‌بندی نظرات ارائه‌شده توسط شرکت‌کنندگان می‌توان انواع راهکارهای امنیتی در برابر تهدیدهای امنیتی در فضای اینترنت اشیاء را در قالب جدول ۶ پیشنهاد نمود:

جدول ۹. راهکارهای امنیتی جهت مواجهه با تهدیدهای نشأت‌گرفته از آسیب‌پذیری‌ها حوزه اینترنت اشیاء

آسیب‌پذیری / تهدید	احراز و تشخیص هویت ناکافی	نقض حریم‌خصوصی	پیکربندی نادرست و استفاده از تنظیمات پیش‌فرض	رمزنگاری نادرست انتقال	اتصال وب ناامن	معماری امنیت شکننده	پیکربندی امنیتی ناامن
دسترسی غیرمجاز	احراز و تصدیق هویت کارآمد دوطرفه	کنترل‌دسترسی					پیکربندی معماری امن
حملات فیزیکی	احراز و تصدیق هویت کارآمد دوطرفه	حفاظت فیزیک کافی					
تروجان‌های سخت‌افزاری	احراز و تصدیق هویت کارآمد دوطرفه وقایع‌نگاری و مانیتورینگ						
ارتباطات غیرمعتبر		رمزنگاری ارتباطات و داده‌ها احراز و تصدیق هویت کارآمد					
نقض خطا			پیکربندی معماری امن حفاظت فیزیکی کافی مخابرات امن				
تخریب داده‌های دریافتی			کنترل‌دسترسی	رمزنگاری ارتباطات و داده‌ها			
حمله سیاه چاله				رمزنگاری ارتباطات و داده‌ها	احراز و تصدیق هویت کارآمد دوطرفه		

حمله انسداد سرویس توزیع شده				رمزنگاری ارتباطات و داده‌ها	احراز و تصدیق هویت کارآمد دوطرفه	کنترل‌دسترسی	
کدبدخواه							احراز و تصدیق هویت کارآمد دوطرفه کنترل‌دسترسی
حمله کرم چاله				رمزنگاری ارتباطات و داده‌ها احراز و تصدیق هویت کارآمد و دوطرفه			
اسب تروجان							احراز و تصدیق هویت کارآمد دوطرفه کنترل‌دسترسی پیکربندی معماری امن
حمله گودال					احراز و تصدیق هویت کارآمد دوطرفه کنترل‌دسترسی		
حمله سیل پاکت						احراز و تصدیق هویت کارآمد دوطرفه کنترل‌دسترسی	

هر تحقیق با توجه به ماهیت خاص خود دارای محدودیت هایی است که تحقیق حاضر هم از این امر مستثنی نیست. پیشرفت های سریع در حوزه فناوری اطلاعات و به طور مثال ، دسترسی به روش های جدید محافظت از داده ها و اطلاعات، و یا دسترسی به روش های کم هزینه برای استقرار اینترنت اشیاء و.... می تواند موانع و چالش های اشاره شده در این تحقیق را دستخوش تغییر نماید و یا منجر به تغییر در رتبه بندی آنها شود.

لذا، باتوجه به یافته‌های تحقیق حاضر می‌توان مواردی را برای تحقیقات آتی پیشنهاد نمود:

- بررسی عوامل اثرگذار بر الزام‌های امنیتی در حوزه اینترنت اشیاء،
- بررسی عوامل موفقیت و شکست موجود در پیاده‌سازی امنیت میان سازمان‌های دولتی-خصوصی یا سازمان‌های تولیدی و خدماتی

- بررسی تاثیر استقرار اینترنت اشیاء بر جنبه های مختلف ء ملکرد سازمان ها با تاکید برکتابخانه ها
- بررسی تاثیر اینترنت اشیاء براستقبال بیشتر مردم از سازمان های خدماتی علی الخصوص کتابخانه ها

منابع

A. Bassi, G. H. Sintef and E. Hitachi,(2008). *Internet of Things in 2020: A Roadmap for the future*. European Commission/ EPoSS Expert workshop on RFID/ Internet of Things, Brussels, 2008.

Ahmad, W. A., & Andrew, M. (2014). *Threat-Based Security Analysis for the Internet of Things*. In Secure Internet of Things (SIoT). IEEE, 35–43

Alam, S.; Chowdhury, M., & Noll, J. (2010). *Senaas: An event-driven sensor virtualization approach for internet of things cloud.* IEEE International Conference, 1-6

Antonio, I.; Morabito, G., & Iera, L. (2010). The Internet of Things: A survey. *Computer Networks, 54*, 2787-2805.

Arbia R.; Enrico N.; Yacine Ch.; and et. al. (2014). *A systemic and cognitive approach for IoT security*. International Conference on Computing, Networking and Communications (ICNC).

Ashton, K. (2009). That ‘‘Internet of Things’’ thing. RFiD Journal.

Bansal, A.; Arora, D.; Suri, A. (2018). Internet of Things: Beginning of New Era for Library. *Library Philsophy and Practicec e-Journal.*

Bhunia, S.; and et al.(2014). *Hardware Trojan attacks: threat analysis and countermeasures*. Proceedings of the IEEE 102.8, 1229-1247.

CASAGRAS, "Final Report, RFID and Inclusive Model for the Internet of Things," Coordination and support action for global RFID-related activities and standardization (EU Framework 7 Project), 2009.

Changmin L.; Luca Z.; Kwanghee Ch.; and Hyeong-Ah Ch. (2014). *Securing Smart Home: Technologies, Security Challenges, and Security Requirements*, IEEE Conference on Communications and Network Security (CNS).

Cisco System. (2011). *http://www.cisco.com/IoT*. Retrieved from http://www.cisco.com.

Forrester Research Council. (2010). *https://www.forrester.com/IoT*. Retrieved from https://www.forrester.com.

Gao, Y., Peng, Y., Xie, F., Zhao, W., Wang, D., Han, X., Li, Z. (12-13 Oct. 2013). Analysis of security threats and vulnerability for cyber-physical systems. Paper presented at the Proceedings of 2013 3rd International Conference on Computer Science and Network Technology

Hui L. and Xin Z. (2011). *Study on Security Architecture for Internet of Things*. International Conference, ICAIC.

ITU Telecommunication Standardization, "*ITU-T Recommendation database*," 15 06 2012. [Online].

Kombade, R. D., & Meshram, B. (2012). CSRF Vulnerabilities and Defensive Techniques. *International Journal of Computer Network and Information Security*, 4(1), 31.

Md. Mahmud Hossain, Fotouhi, M.; and Ragib Hasan, (2015). *Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things.* IEEE World Congress on Services (SERVICES).

Modoff, B.; Bhagavath, V.; & Clifton, K. (2014). *The Internet of Things.* Retrieved from www.db.com.

Abomhara m.; Køien,G. M. (2014). Security and Privacy in the Internet of Things :Current Status and Open Issues. IEEE, 2014.

Mukherjee, A. (2015). *Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints.* Proceedings of the IEEE 103, 1747-1761.

Pejang, A.; Abtahi, A., Rajabzadeh, A. (2016). *Examining the challenges of Internet connection integrity in the Internet of Things.* Fourth International Conference on Electrical, Computer and Electronics Engineering,Ahar.

Qazi, M. A.; Mohamed, H. H. (2014). Autonomic schemes for threat mitigation in Internet of Things. *Elsevier Ltd*, (49), 112-127.

RFID Research Group. (2009). *http://www.fridjournalevents.com/IoT*. Retrieved from http://www.fridjournalevents.com.

Sachin, B.; Parikshit, M.; Antonietta, S.; Neeli, P., & Ramjee, P. (2010). Proposed security model and threat taxonomy for the Internet of Things (IoT). *Springer Berlin Heidelberg,(*89), 420-429.

Shafi'i, S.(2016). Analysis of challenges to the development of IoT technology. Security

Vandana, C. P. M.; Bhattacharjee, M. A..; Gopta, M. A. (2017). *library management system Based on IOT*. *TJRDO-Journal of Computer Science Engineering*, 3 (4).

Vermesan, O.; Friess, P. (2013). *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. Denmark: River Publishers.

Xu Xingmei; Zhou Jing, Wang He, (2013). *Research on the Basic Characteristics, the Key Technologies, the Network Architecture and Security Problems of the Internet of Things*. 3rd International Conference on Computer Science and Network Technology (ICCSNT).

Yazdanpanah, H.; Hasana Ahangar, M.(2016). *Internet of Things (IoT): Applications, technologies and challenges discussed*. 8th International Conference on Information Technology and Knowledge. Hamedan.

Yenumula B Reddy, (2014). Cloud-based Cyber Physical Systems: Design Challenges and Security Needs. 10th International Conference on Mobile Ad-hoc and Sensor Networks (MSN).

Zargar, M. (2019). Assessment of Barriers to Establishing the Internet of Things in Libraries in Iran based on a Combined Approach. *Iranian Journal of Information Processing and Management*., 34(3),1371-1398.

Zhi, K. Z.; Michael, C. Y.; Shiuhpyng, S.; IEEE, f. (2015). *Emerging Security Threats and Countermeasures in IoT*. ACM ,1-6.

threats and digital divide. *Monthly short article*.,1(7), 1-8

Qusay Idrees, S. (2013). Security Attacks and Countermeasures for Wireless Sensor Networks: Survey. *International Journal of Current Engineering and Technology* ,3.2, 628-635.

Manikantan, S. D.; Venugopal V.(2014). Design, implementation and security analysis of hardware Trojan threats in FPGA. Communications (ICC), IEEE International Conference on. IEEE, 2014.

Sun, Y.; Yan, H.; Lu, C. and et. al. (2012). *A holistic approach to visualizing business models for the internet of things*. Communications in Mobile Computing.

Suo, H.; Wan, J.; Zou, C.; & et. al (2012). *Security in the internet of things: a review (2012)*. Paper presented at the Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on.

Tapalina B.; Rituparna C.; and Nabendu C. (2013). Study of Security Issues in Pervasive Environment of Next Generation Internet of Things. Computer Information Systems and Industrial Management,Volume 8104 of the series Lecture Notes in Computer Science pp 206-217.

Tehranipoor, M.; Koushanfar, F. (2010). A survey of hardware trojan taxonomy and detection." IEEE Design & Test of Computers 27.1

Quarterly Journal of Knowledge Studies
(Library and Information Science and Information Technology)
Islamic Azad University North Tehran Branch
Vol. 12, No. 44, Spring 2019

Identifying the common threats and vulnerabilities in the Internet of Things (IoT) and offering security policies for confronting them

Safiyeh Tahmasebi Limooni[1] | Shahrzad Ghasemi[2] | Roghayeh Ghorbanloo[3]

1. Department of information sciences and knowledge studies, Babol Branch, Islamic Azad University, Babol, Iran(Corresponding author) sa.tahmasebi2@gmail.com
2. Department of information sciences and knowledge studies, Babol Branch, Islamic Azad University, Babol, Iran
3. MSc. Information Technology Engineering, Iran Telecommunication Research Center, Tehran, Iran

Abstract

Objective: the objective of this research is to identify the common threats and vulnerabilities in IoT and offering security policies to cope with them.

Methods: the methodology of this research is applied based on its objective, and descriptive-surveying based on data collection. The statistical population includes all exerts and professors of IoT in universities of Tehran with 50 members. The sampling method was convenience non-random. The sample volume detected was similar to the statistical population. The research tool was the researcher-made questionnaire from the systematic study of thematic literature. The validity of the questionnaires was obtained by referring to the experts of the IoT field. The reliability of the tool was 0.88 using Cronbach's alpha coefficient for the questionnaire. Data was analyzed using descriptive and inferential statistics by SPSS software.

Results: Although various standards have been developed in the field of security and confidentiality in IoT, the security needs of IoT and even its risks have not been still identified and analyzed. In addition, it needs confidentiality mechanisms, accuracy, authentication, and access control precisely. According to the findings of the tests of this research, vulnerabilities can be classified and cited in 21 groups.

Conclusion: the results of tests show that various experts based on their landscapes and activity fields determined a varied set of security policies to cope with Internet threats in the IoT field. However, the most important security policies against the security threats in IoT include mutual and efficient authentication, access control, secure architecture configuration, encryption of communications and data, chronology, and monitoring by concluding the provided ideas.

Keywords: IoT, security threat, vulnerability, security requirement, research centers