

فصل نامه دانش شناسی

(علوم کتابداری و اطلاع رسانی و فناوری اطلاعات)

دانشگاه آزاد اسلامی واحد تهران شمال

سال دوازدهم، شماره ۴۴، بهار ۱۳۹۸، از صفحه ۳۲ الی ۵۴

شناسایی تهدیدها و آسیب پذیری های رایج در فضای اینترنت اشیا و ارائه راهکارهای امنیتی جهت مواجهه با آنها

صفیه طهماسبی لیمونی^۱ | شهرزاد قاسمی^۲ | رقیه قربانلو^۳

۱. گروه علم اطلاعات و دانش شناسی، واحد بابل، دانشگاه آزاد اسلامی، بابل، ایران (نویسنده مسئول)، sa.tahmasebi2@gmail.com

۲. گروه علم اطلاعات و دانش شناسی، 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 آسیب پذیری های رایج اینترنت اشیا و ارائه راهکارهای امنیتی جهت مواجهه با آنها است. **روش پژوهش:** روش پژوهش از نظر هدف کاربردی و از نظر گردآوری داده توصیفی - پیمایشی است. جامعه آماری شامل کلیه اساتید و متخصصان حوزه اینترنت اشیا در دانشگاه های شهر تهران به تعداد ۵۰ نفر بودند. روش نمونه گیری از نوع نمونه گیری غیر تصادفی 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 در حوزه اینترنت اشیا 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 نرم افزار اس. پی. اس. انجام شد.

یافته ها: با اینکه استانداردهای مختلفی در حوزه مسئله امنیت و محرمانگی در اینترنت اشیا در حال توسعه است ولی همچنان نیازمندی های امنیتی اینترنت اشیا و حتی مخاطره های آن به خوبی شناسایی و تحلیل نشده است و نیازمند سازوکارهای محرمانگی، صحت، احراز هویت و کنترل دسترسی به صورت دقیق است. بر اساس یافته های حاصل از آزمون های این پژوهش آسیب پذیری ها 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 به عنوان راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در حوزه اینترنت اشیا تبیین نموده اند، اما با جمع بندی نظرات ارائه شده توسط شرکت کنندگان می توان مهمترین راهکارهای امنیتی در برابر تهدیدهای امنیتی در فضای اینترنت اشیا را شامل احراز و تصدیق هویت کارآمد دوطرفه، کنترل دسترسی، پیکربندی معماری امن، رمزنگاری ارتباطات و داده ها و وقایع نگاری و مانیتورینگ دانست.

واژه های کلیدی: اینترنت اشیا، تهدید امنیتی، آسیب پذیری، الزام امنیتی

مقدمه

اینترنت اشیاء^۱ پدیده جدیدی است که در آن وسایل پیرامون ما مانند سیستم تهویه منزل یا چراغ‌های اتاق به شبکه متصل شده 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^۲، ۲۰۱۰). اشیاء هنگامی که بتوانند خود را به صورت دیجیتالی عرضه کنند، با اشیاء اطراف، نظیر یک پایگاه داده بزرگ در ارتباط خواهند بود. وقتی اشیاء با یکدیگر شبکه شدند، می‌توان سخن از یک "محیط هوشمند" به میان آورد (ورمیزن و فریس^۳، ۲۰۱۳).

فناوری اینترنت اشیاء مانند هر نوع فناوری دیگری برای سودجویان و تبهکاران فضای سایر انگیزه خرابکاری و سوءاستفاده ایجاد می‌کند. این انگیزه به معنای وجود تهدید امنیتی علیه اینترنت اشیاء است. تهدیدهای امنیتی در اینترنت اشیاء ممکن است متوجه کاربران، سرویس دهندگان، مشتریان و یا دارایی‌های یک سازمان مصرف کننده 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 - به واسطه گستردگی و افزایش ارتباطات در این پدیده - نگرانی عظیمی را به وجود آورده است. نقض حریم خصوصی، 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^۴، بروز حمله‌ها، نقص‌های امنیتی و ایمنی، عدم وجود راهکارهای مناسب و در عین حال سرعت خیره کننده پیشرفت و گسترش اینترنت اشیاء اهمیت این موضوع را چندین برابر نموده است. آنچه که می‌تواند باعث کاهش نگرانی و جلب اعتماد افراد - از مشتریان و عموم افراد تا توسعه دهندگان - به این فناوری باشد برقراری امنیت

در این فضا است. امنیت در اینترنت اشیاء با پرداخت به آسیب‌پذیری‌ها، تهدیدها^۵ 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^۶، ۲۰۱۵).

پیشینه‌های پژوهش به صورت زیر دسته بندی شده ارائه می‌شود:

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^۷ (MIT) توسط کوین اشتون^۸ 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^۹، ۲۰۰۹). نسل آینده کاربردهای اینترنت از نسخه ۶ اینترنت (IPv6) استفاده می‌کنند که به دلیل فضای بسیار گسترده برای آدرس‌دهی در آن، تمامی اشیاء ساخته شده قابلیت دریافت شناسه اختصاصی را خواهند داشت. بنابراین تمامی اشیاء در زندگی روزمره ما قابلیت آدرس‌دهی، اتصال و کنترل شدن را پیدا می‌کنند (آنتونیو، مرابیتو و لرا^{۱۰}، ۲۰۱۰).

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

⁵ Threats

⁶ Mahmud Hossain et al

⁷ Massachusetts Institute of Technology

⁸ Kevin Ashton

⁹ Ashton

¹⁰ Antonio, Morabito & Iera

¹ Internet of Things

² Alam, Chowdhury & Noll

³ Vermesan & Friess

⁴ Vulnerabilities

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

مؤلف / مرجع	سال	تعریف	حوزه های تمرکز
بسی و همکاران	۲۰۰۸	یک شبکه جهانی از اشیاء متصل به هم که براساس پروتکل های ارتباطی استاندارد به شکل منحصر به فردی آدرس دهی شده اند.	شبکه جهانی، اشیاء متصل، پروتکل های ارتباطی، آدرس دهی
CASAGRAS ^۱	۲۰۰۹	یک زیرساخت شبکه جهانی که اتصال اشیاء مجازی و فیزیکی را از طریق بهره برداری از جمع آوری داده ها و فن آوری های ارتباطی تسهیل می کند.	زیرساخت، اشیاء فیزیکی و مجازی، جمع آوری داده، فن آوری ارتباطی
گروه تحقیقاتی آ.راف.آی.دی ^۲	۲۰۰۹	شبکه ای جهانی از اشیاء قابل آدرس دهی بصورت یکتا، براساس یک پروتکل ارتباطی استاندارد.	شبکه فراگیر، ارتباط اشیاء، آدرس دهی
گروه تحقیقاتی فارسستر ^۳	۲۰۱۰	استفاده از فناوری های ارتباطی و اطلاعاتی برای ایجاد اجزای زیرساخت حیاتی و ارائه خدمات مربوط به دانش، بهداشت و درمان، امنیت عمومی، حمل و نقل و خدمات شهری به صورت آگاهانه، تعاملی و کارآمد.	خدمات اشیاء، تعامل اشیاء، فناوری های اطلاعات و ارتباطات
آنتونیو، مریابیتو و لرا	۲۰۱۰	اینترنت اشیاء در سه پارادایم مشخص می شود: اینترنت گرا (میان افزار)، شی گرا (حسگرها) و معناگرا (دانش).	اشیاء، اینترنت، حسگرها، دانش و اطلاعات
گروه پروژه های تحقیقاتی اروپا ^۴	۲۰۱۰	مشارکت فعال اشیاء در تجارت، فرآیندهای گردآوری اطلاعات و پردازش آن ها با قابلیت برقراری ارتباط با یکدیگر و با محیط اطراف بدون دخالت مستقیم انسانی.	کاربرد اشیاء در تجارت، ارتباطات، پردازش
سیسکو ^۵	۲۰۱۱	هنگامی که تعداد اشیاء متصل به شبکه جهانی از تعداد انسان ها 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 صرفه ترین هزینه.	اشیاء، انسان، ارتباطات، خدمات کارآمد
اتحادیه بین المللی مخابرات ^۶	۲۰۱۲	یک زیرساخت جهانی برای جامعه اطلاعاتی که خدمات پیشرفته را از طریق اتصال (فیزیکی و مجازی) اشیاء بر پایه فن آوری های ارتباطی و اطلاعاتی سازگار موجود و در حال تحول ممکن می سازد.	زیرساخت، اطلاعات، اشیاء فیزیکی و مجازی، فن آوری ارتباطی
مداف، بگواف و کلیفتون ^۷	۲۰۱۴	شبکه ای شامل اتصالات داخلی، ارتباطات بین افراد، فرآیندهای کسب و کار، داده ها و اشیاء می باشد.	تجارت و کسب و کار، ارتباطات، اشیاء
یزدان پناه و حسنی آهنگر	۱۳۹۵	اینترنت اشیا اصطلاحی است برای توصیف دنیایی که در آن 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 اشیا، چالش های اینترنت اشیا
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 اشیا در کتابخانه ها به ۳ دسته عوامل امنیتی، انسانی، و زیرساخت ها

^۱ Coordination And Support Action for Global RFID-Related Activities and Standardisation

^۲ RFID Research Group

^۳ Forrester Research

^۴ European Research Council

^۵ Cisco

^۶ ITU Telecommunication Standardization

^۷ Modoff, Bhagavath & Clifton

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 از این رو، بررسی و شناخت آسیب‌پذیری‌ها بسیار مهم و حیاتی است (محمودحسین و دیگران، ۲۰۱۵). در جدول ۲ به مجموعه‌ای از آسیب‌پذیری‌های حوزه اینترنت اشیاء اشاره شده است.

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 به اشتراک گذاری 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 به هم که در حال تعامل با سایر اشیاء و حتی انسان‌ها هستند تعریف نمود.

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

نام آسیب‌پذیری	شرح آسیب‌پذیری	مراجع
احراز و تشخیص هویت ناکافی	احراز اصالت و مجوزدهی ناکافی در برابر کاربران داخل شبکه شایع است. به صورت 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، ۲۰۱۲)
نقض حریم خصوصی	شبکه‌های بی‌سیم، به دلیل قابلیت دسترسی از راه دور، خطر نقض حریم خصوصی را افزایش می‌دهند چون باعث می‌شوند 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 شوند 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 نامن	بسیاری از سرویس‌های اینترنت اشیاء در فضای ابری میزبانی می‌شوند، بنابراین دستگاه‌ها و برنامه‌های کاربردی 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 حریم خصوصی و محرمانگی افزایش می‌یابد.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)
رابط سیار نامن	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 به همراه دارد.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)
توسعه نادرست پیچ سیستم عامل و نرم افزار	اگر به صورت منظم به روزرسانی نشوند، نسخه‌های پیش فرض و منسوخ شده همیشه تحت خطرات امنیتی هستند. نسخه‌های به روز باید به طور امن اعمال شوند و مهاجمان قادر نباشند تا اطلاعات حیاتی (مانند اطلاعات پیکربندی و یا گواهینامه‌های رمزنگاری) را در حین فرآیند به روزرسانی کشف کنند.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)
پیکربندی نادرست و استفاده از تنظیمات پیش فرض	هکرها از امنیت بسیار پایین ابزارهای اینترنت اشیاء و تنظیمات امنیتی ضعیف آن‌ها که غالباً همان تنظیمات پیش فرض کارخانه هستند آگاهند و از آن‌ها در راستای رسیدن به اهداف خود استفاده می‌کنند.	(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)
سیاست گذاری‌های نادرست	دو اصل عمومی که در سیاست گذاری اینترنت اشیاء می‌بایستی در نظر گرفته 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)

	داشته باشند، به جز زمانی که این اصل با اصل اول در تعارض باشد.	
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	منظور زمانی است که امنیت برقرار شده برای محیط فیزیکی و امنیت سیستم ها و... (هر تغییری را می تواند شامل شود که قبلاً امنیت داشته است) تغییر کند. به عنوان مثال، محیط بزرگ تر می شود، سیستم ها تغییر می کنند و پیکربندی آن ها نسبت به قبل متفاوت باشد، در این صورت اگر این تغییرات مدیریت نشود و امنیت آن ها در شرایط جاری برقرار نشود عدم مدیریت تغییرات امنیتی را با خود به همراه دارد.	عدم مدیریت تغییرات امنیتی
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	می تواند همه کنترل های محیطی از جمله، کنترل شرایط جوی، سرما، گرما، فشار و... یا کنترل از لحاظ وجود سیستم اطفاء حریق، آشکار کننده نشت گازها و... یا حوادث طبیعی -از جمله بارش باران، رعدوبرق، سیل، آتش سوزی، زلزله، یخ زدگی و آفتابزدگی- را که باید جهت امنیت سیستم ها برقرار باشد شامل شود که در غیر این صورت با عدم کنترل های محیطی روبرو خواهیم شد.	عدم کنترل های محیطی
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	اینترنت اشیاء این امکان را فراهم می کند که داده ها هم در دستگاه های فیزیکی و هم در فضای ابری ذخیره شود. ممکن است اطلاعات شخصی و گواهی نامه های امنیتی در یک دستگاه اینترنت اشیاء ذخیره شود. بنابراین، امنیت فیزیکی ضعیف باعث می شود داده های ذخیره سازی شده روی دستگاه نسبت به نفوذ آسیب پذیر باشند.	ذخیره سازی ناامن داده ها و پیکربندی های مهم
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	در این نوع آسیب پذیری، سازندگان دستگاه ها بایستی حداقل الزام های امنیتی را برای دستگاه هایی که در این بستر قرار می گیرند فراهم نمایند. به عنوان نمونه از یک جی.پی.اس ساده تا یک توربین بخار	ناهمگونی دستگاه ها
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	زمانی که امکان توسعه سیستم وجود نداشته و یا به سختی امکان پذیر است. به عنوان نمونه، امکان برقراری شبکه اینترنت میسر نباشد یا برای شهری که در دامنه کوه بنا نهاده شده است به سختی بتوان سرویس های مختلف را در آن زمینه سازی و فراهم نمود. در این صورت قابلیت های توسعه ای محدود گردیده و با چالش همراه خواهد بود.	محدودیت قابلیت توسعه
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	به منظور اتصال اشیاء هوشمند گوناگون در سراسر جهان، شبکه اینترنت اشیاء نوع ساختار ارتباطی را از میان گزینه های بی سیم، کابلی، خصوصی و عمومی انتخاب می کند. این چندگانگی پروتکل باعث می شود شبکه اینترنت اشیاء نسبت به مسائل امنیتی فراوانی از جمله صحت داده، کیفیت سرویس نامناسب و غیره آسیب پذیر باشد.	اتصال وب ناامن
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	یک سرویس شبکه آسیب پذیر می تواند باعث توقف فعالیت یک دستگاه اینترنت اشیاء شود به طوریکه دستگاه برای کاربران غیر قابل دسترس شود. این حالت زمانی رخ می دهد که یک سرویس شبکه نسبت به حملات انسداد سرویس و یا سرریز حافظه بافر آسیب پذیر باشد و یا یک پورت غیر ضروری شبکه باز و در دسترس باشد.	سرویس شبکه ناامن
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	به دلیل داشتن توانایی محاسباتی ضعیف، دستگاه های اینترنت اشیاء از رمزنگاری در انتقال داده استفاده نمی کنند و یا از انواع ضعیف آن استفاده می کنند. بنابراین، ارتباطات برای عوامل مخرب به راحتی قابل کشف و ردیابی می باشد.	رمز گذاری نادرست انتقال
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	زمانی که کاربر دستگاه توانایی تغییر آن را ندارد، در قالب این آسیب پذیری نمود پیدا می کند. با مرور دستی رابط وب می توان این آسیب پذیری را آشکار نمود. پیکربندی امنیتی ناامن می تواند منجر به از دست رفتن اطلاعات و آسیب به دستگاه یا سرویس شود.	پیکربندی امنیتی ناامن
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	عدم توانایی به روزرسانی دستگاه، نوعی آسیب پذیری امنیتی محسوب می شود. به این ترتیب نرم افزار و سخت افزار مربوطه آسیب پذیر خواهند بود. با تحلیل ترافیک شبکه در زمان به روزرسانی و بررسی رمزنگاری و... به راحتی می توان این آسیب پذیری را شناسایی نمود. این آسیب پذیری می تواند منجر به از دست رفتن اطلاعات، کنترل دستگاه ها و صدمه به دیگر دستگاه ها از همین طریق شود.	نرم افزار و میان افزار ناامن
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	زمانی که مهاجم می تواند دستگاه را به منظور دستیابی به رسانه ذخیره سازی و داده های ذخیره شده آن،	حفاظت فیزیکی

مجزا نماید، نمود پیدا می کند. همچنین، این آسیب پذیری زمانی که پورت های USB یا دیگر پورت های خارجی به منظور دسترسی به دستگاه مورد استفاده قرار می گیرند، نمایان می شود. این آسیب پذیری از کارافتادن دستگاه، آشکار شدن و از دست رفتن داده های ذخیره شده بر روی آن را با خود به همراه دارد.	ناکافی
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	کمبود صحت ارتباطات
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	معماری امنیت شبکه شکننده
(محمودحسین و همکاران، ۲۰۱۵)، (کمبت و مشرام، ۲۰۱۲)،	عدم وجود فایروال یا پیکربندی نادرست

خطرناک، یک تهدید امنیتی تلقی می شود. در واقع، تهدید امنیتی به عاملی اطلاق می شود که می تواند موجب بروز یک حادثه امنیتی و زمینه ساز بروز خسارت به یک سیستم، سازمان و یا دارایی های آن سازمان بشود. تهدیدهای امنیتی در فضای اینترنت اشیاء نقش انکارناپذیری را در مدیریت و عرضه مناسب خدمات این حوزه ایفا می نمایند (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 به همراه سال ارائه آمده است:

آسیب پذیری ها موجب بروز تهدیدها هستند و از عوامل اصلی ایجاد تهدیدها محسوب می شوند. 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 برنامه ریزی شده جهت افشاء، نابودی یا تغییر در داده های حیاتی شبکه یا ایجاد اختلال در خدمات معمول سرویس دهنده ها؛ و به طور عام هرگونه اقدام برنامه ریزی شده برای تحقق یک رخداد

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

نام تهدید	توضیحات	مرجع
حمله های فیزیکی ^۱	این دسته از حمله ها با سخت افزار اینترنت اشیاء سروکار دارند، به طوری که اگر یک دستگاه اینترنت اشیاء در دست مهاجم قرار گیرد ممکن است حمله های متعددی از قبیل سرقت اطلاعات محرمانه، دستکاری نرم افزاری و سخت افزاری رخ دهد.	(گائو و همکاران ^۱ ، ۲۰۱۳)، (ساجین و همکاران ^۲ ، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران ^۳ ، ۲۰۱۲)، (ژی و همکاران ^۴ ، ۲۰۱۵)، (قاضی و محمد ^۵ ، ۲۰۱۴)
خرابی تجهیزات	تجهیزات عملکردشان را ناشی از نیروهای خارجی، محیط و یا قدیمی شدن از دست می دهند.	(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)
نقص خط	این حمله خرابی خط، خرابی خطوط برق در گره ها را با خود به همراه دارد.	(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)
ممانعت از سرویس ^۶	حمله هایی هستند که پیاده سازی آن ها باعث وقفه در ارائه خدمات خواهد شد اما برای رسیدن به این هدف، ترکیبی از حمله ها متفاوت می تواند بوقوع بپیوندد.	(گائو و همکاران، ۲۰۱۳)، (ریاحی و همکاران، ۲۰۱۴)، (زینگ می و همکاران ^۷ ، ۲۰۱۳)، (زینگ و همکاران، ۲۰۱۰)، (لی و ژو، ۲۰۱۱)، (ابومحار و همکاران، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)، (سارخانا، ۲۰۱۳)
حمله سیل پاکت	این نوع حمله، خسته کردن و از پای درآوردن منابع سرورهای شبکه روی لایه شبکه و منجر شدن به حمله DDoS را به همراه دارد.	(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)
تخریب داده دریافتی	مهاجم به صورت غیرمجاز، نسبت به افزودن حذف، اصلاح و تخریب داده های دریافتی اقدام می کند.	(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)
رهگیری داده ^۸	در این حمله، مهاجم از طریق متوقف کردن کانال های ارتباطی به صورت غیرمجاز به منابع داده ای دسترسی پیدا می کند.	(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)
دستکاری داده ^۹	در این نوع حمله، مهاجم داده ها را رهگیری و تغییر می دهد سپس داده های تغییر یافته را به سمت گیرنده ارسال می کند.	(لی و ژو، ۲۰۱۱)، (گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)
دسترسی غیرمجاز ^{۱۰}	منابع، داده های شبکه و سیستم توسط کاربران غیرمجاز قابل دسترس می شود.	(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، 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

<p>زینگ می و همکاران، (۲۰۱۳)، (زینگ و همکاران، ۲۰۱۰)، (لی و ژو، ۲۰۱۱)، (ابومحار و همکاران، ۲۰۱۴)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)، (سارخانا، ۲۰۱۳)</p>	<p>دسترس خارج کند. این حمله به صورتی است که سیلی از درخواست‌هایی که بیش از ظرفیت پاسخ‌دهی قربانی است به سمت وی جاری می‌شود.</p>	<p>توزیع شده^۱</p>
<p>(گائو و همکاران، ۲۰۱۳)، (بهاتاسالی و همکاران، ۲۰۱۳)، (لی و ژو، ۲۰۱۱)، (زینگ و همکاران، ۲۰۱۰)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)</p>	<p>مهاجم در فرآیند مسیریابی طبیعی با ارسال اطلاعات مسیریابی جعلی تداخل ایجاد می‌کند.</p>	<p>حمله‌های مسیریابی</p>
<p>(بهاتاسالی و همکاران، ۲۰۱۳)، (لی و ژو، ۲۰۱۱)، (زینگ و همکاران، ۲۰۱۰)، (گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)</p>	<p>گره مخرب، آدرس مبدأ و مقصد بسته‌های داده را تغییر داده و سپس آن‌ها را به یک مسیر اشتباه ارسال می‌کند، در نتیجه مسیریابی شبکه دچار سردرگمی می‌شود.</p>	<p>حمله گمراه کننده جهت</p>
<p>(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)</p>	<p>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.</p>	<p>حمله سیاه چاله^۲</p>
<p>(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)</p>	<p>در این حمله، یک گره (شیء) برای خود هویت‌های چندگانه‌ای را ایجاد می‌کند 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 می‌کند رفتار خود را عادی نشان دهد.</p>	<p>حمله Sybil</p>
<p>(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)</p>	<p>این حمله، توسط یک نود که اطلاعات و مشخصات آن جعلی است، نودهای همسایه و همجوار آن را گمراه می‌کند تا اطلاعات آن‌ها را به نود خرابکار بسپارد و مهاجم می‌تواند بر روی اطلاعات هر گونه تغییری از جمله تغییر پیام و یا حتی رد کردن بسته‌ها و سایر حمله‌ها را اعمال نماید.</p>	<p>حمله گودال^۳</p>
<p>(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)</p>	<p>در این حمله، گره‌های بدخواه، پیغام‌هایی را از یک ناحیه از شبکه از روی یک لینک اختصاصی (پر سرعت) هدایت می‌کنند و آن‌ها را در ناحیه دورتری از شبکه بازپخش می‌کند.</p>	<p>حمله کرم چاله^۴</p>
<p>(گائو و همکاران، ۲۰۱۳)، (بهاتاسالی و همکاران، ۲۰۱۳)، (لی و ژو، ۲۰۱۱)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)</p>	<p>در این نوع حمله، گره مخرب مسیر داده‌ها را تغییر می‌دهد که منجر به حلقه مسیریابی بی‌نهایت می‌شود.</p>	<p>حمله حلقه مسیریابی</p>
<p>(گائو و همکاران، ۲۰۱۳)، (بهاتاسالی و همکاران، ۲۰۱۳)، (لی و ژو، ۲۰۱۱)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)</p>	<p>گره مخرب با دستکاری در اطلاعات مسیریابی به لایه شبکه حمله می‌کند.</p>	<p>اطلاعات مسیریابی کاذب</p>
<p>(گائو و همکاران، ۲۰۱۳)، (ردی، ۲۰۱۴)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و</p>	<p>مهاجم از طریق ارسال یک کد بدخواه به سیستم موردنظر، امکان انجام فعالیت‌های مخرب روی سیستم هدف را پیدا می‌کند.</p>	<p>کد بدخواه^۵</p>

¹ Distributed Denial of Service (DDOS)

² Blackhole

³ Sinkhole

⁴ Wormhole

⁵ Malicious code

همکاران، (۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)		
(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)	اسب های تروجان	اسب تروا نرم افزار مخربی است که ظاهر خود را تغییر می دهد تا مقصود اصلی اش را از کاربران پنهان کند. تروجان ها می توانند به هر شکلی از جمله لینک های دانلود بی آزار، پیوست های ایمیلی که از طرف همکاران شما ارسال شده یا تصویری که از رسانه های اجتماعی آمده در آیند.
(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)	حمله تزریق کد SQL ^۱	به سوء استفاده مهاجم از کاربردهایی اشاره دارد که بدون بررسی ورودی های کاربر و اعتبارسنجی وی، به طور مستقیم از روی آن ها اقدام به ساخت SQL Query می کند.
(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)، (بونیا و همکاران، ۲۰۱۴)، (شیلا و همکاران، ۲۰۱۴)، (تهرانی پور و همکاران، ۲۰۱۰)	تروجان های سخت افزاری ^۲	به هر نوع دستکاری و اعمال تغییرات مخرب با اهداف خاص در مدارات تجهیزات سخت افزاری گفته می شود.
(ریاحی و همکاران، ۲۰۱۴)، (لی و همکاران، ۲۰۱۴)، (بت سالی و همکاران، ۲۰۱۳)، (زینگ و همکاران، ۲۰۱۰)، (لی و ژو، ۲۰۱۱)، (گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)، (مورچی، ۲۰۱۵)	استراق سمع ^۳	مهاجم به صورت محرمانه اطلاعاتی که در یک ارتباط خصوصی مبادله می شود را شنود می کند. دستگاه های RFID یکی از آسیب پذیرترین انواع دستگاه ها نسبت به این نوع حملات در فناوری اینترنت اشیا محسوب می شوند. این دسته از حملات محرمانگی پیام ها را مورد تهدید قرار می دهند.
(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)	ارتباطات غیر معتبر	هر گره برای به اشتراک گذاشتن داده ها و دسترسی به داده های سایر گره ها نیازمند برقراری ارتباط با سایر گره ها است. این گره فقط باید با مجموعه ای از گره هایی که به اطلاعات آن ها نیاز دارد، ارتباط برقرار کند و این نیازمندی یک موضوع حیاتی برای سیستم های اینترنت اشیا متشکل از گره های امن و غیر امن می باشد.
(گائو و همکاران، ۲۰۱۳)، (ساجین و همکاران، ۲۰۱۰)، (احمد و اندرو، ۲۰۱۴)، (سو و همکاران، ۲۰۱۲)، (ژی و همکاران، ۲۰۱۵)، (قاضی و محمد، ۲۰۱۴)	تزریق پاکت مخرب	مهاجم می تواند به سه طریق مختلف ارسال، تغییر و تکرار این پاکت های مخرب را در لینک های ارتباطی تزریق کند. در سناریوی ارسال، مهاجم می تواند یک سری پاکت مخرب که به نظر معتبر می رسند را تولید و در لینک های 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 می کند که قبلا بین دو گره شبکه رد و بدل شده است.

^۱ SQL Injection^۲ Hardware Trojan^۳ Eavesdropping

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 دانشگاه‌های دولتی شهر تهران استفاده شده است که مقوله اینترنت اشیا را در سرفصل‌های آموزشی یا پژوهشی خود قرار داده‌اند؛ پیرامون آن تألیفی داشته؛ و یا مقاله‌ای را به رشته تحریر در آورده‌اند. براین اساس، جامعه آماری محدودی با ۵۰ نفر از اساتید دانشگاهی و متخصصان حوزه فناوری اطلاعات دانشگاه‌های 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 اشیا برخوردارند.

در این پژوهش به دلیل محدود بودن جامعه آماری، نمونه آماری به صورت هدفمند و به روش نمونه‌گیری 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 مورد مطالعه حاصل گردد.

در این پژوهش برای شناسایی تهدیدها و آسیب‌پذیری‌های رایج در حوزه اینترنت اشیا از مطالعه نظام مند ادبیات موضوعی استفاده شده است و چون به صورت 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 داده‌ها به دو صورت زیر انجام گرفته است:

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

است

تهدیدهای اینترنت اشیا برای عملیاتی شدن نیاز به عوامل پیاده‌سازی نیز دارند. این عوامل را می‌توان منشأ تهدید به حساب آورد. عوامل پیاده‌سازی تهدیدها می‌تواند از جانب کاربران مخرب، سازندگان و فروشندگان متقلب و مهاجمین خارجی به کار گرفته شوند. لذا از دیدگاهی دیگر عوامل ذکر شده می‌تواند جزئی از تهدیدهای اینترنت اشیا محسوب گردند.

هدف اصلی این پژوهش، شناسایی آسیب‌پذیری‌ها و تهدیدهای امنیتی در فضای اینترنت اشیا 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 هر یک از تهدیدهای شناخته‌شده به آسیب‌پذیری‌های مربوطه است.

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

۱. آسیب‌پذیری‌های امنیتی رایج در فضای اینترنت اشیا کدامند؟
۲. تهدیدهای امنیتی که اینترنت اشیا را تحت تأثیر قرار می‌دهند کدامند؟
۳. تهدیدهای امنیتی نشأت گرفته از آسیب‌پذیری‌های شناخته شده کدامند؟
۴. راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در فضای اینترنت اشیا کدامند؟

روش پژوهش

هدف از تحقیق حاضر ارائه راهکارهای امنیتی جهت مواجهه با تهدیدهای شناسایی شده در فضای اینترنت اشیا است. باتوجه به نوظهور بودن مفهوم اینترنت اشیا 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

یافته‌ها

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

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

جدول ۴. توزیع فراوانی نمونه براساس جنسیت

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

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 به تصویر کشیده شده‌است به‌عنوان آسیب‌پذیری‌های امنیتی رایج در حوزه اینترنت اشیاء مطرح هستند:

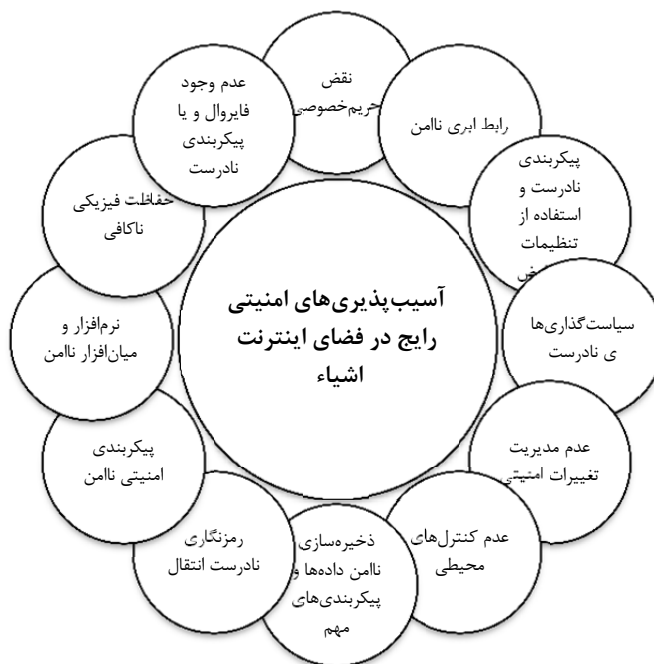
در نمونه مورد مطالعه در این تحقیق (۷۸) درصد از پاسخگویان مرد و بقیه (۲۲) درصد زن بودند. هرچند در این تحقیق، اثر جنسیت بر نتایج تحقیق مورد توجه محقق نبوده‌است، اما این مسئله که اکثریت نمونه مورد مطالعه مرد بوده اند ممکن است بر نتایج تحقیق مؤثر بوده باشد؛ اکثر پاسخ دهندگان (۵۶) درصد) در گروه سنی (۲۵-۳۵) سال قرار دارند؛ از نظر تحصیلات نیز اکثر افراد فوق‌لیسانس (۳۶ درصد) و دکترا (۶۴ درصد) بوده‌اند. سابقه خدمت اکثر آنها نیز ۱۰ تا ۱۵ سال (۶۰ درصد) بوده‌است. 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

جدول ۵. توزیع فراوانی آسیب پذیری‌ها

مجموع	کاملاً مخالف	مخالف	نظری ندارم	موافق	کاملاً موافق	آسیب پذیری
۵۰	۲	۳	۵	۳۱	۹	احراز و تشخیص هویت ناکافی
۵۰	۲	۳	۹	۶	۳۰	نقض حریم خصوصی
۵۰	۱	۴	۷	۶	۳۲	رابط ابری ناامن
۵۰	۳	۲	۱۰	۲۹	۶	رابط سیار ناامن
۵۰	۵	۳	۵	۳۰	۷	توسعه نادرست پچ سیستم عامل و نرم افزار
۵۰	۳	۳	۴	۵	۳۵	پیکربندی نادرست و استفاده از تنظیمات پیش فرض
۵۰	۳	۵	۶	۸	۲۸	سیاست گذاری‌های نادرست
۵۰	۱	۲	۵	۱۰	۳۲	عدم مدیریت تغییرات امنیتی
۵۰	۲	۲	۱۰	۷	۲۹	عدم کنترل‌های محیطی
۵۰	۴	۴	۵	۱۰	۲۷	ذخیره سازی ناامن داده‌ها و پیکربندی‌های مهم
۵۰	۲	۳	۳۳	۷	۵	ناهمگونی دستگاه‌ها
۵۰	۵	۳۰	۱۰	۳	۲	محدودیت قابلیت توسعه
۵۰	۶	۳۳	۵	۴	۲	اتصال وب ناامن
۵۰	۴	۴	۴	۳۲	۶	سرویس شبکه ناامن
۵۰	۲	۶	۵	۶	۳۱	رمز گذاری نادرست انتقال
۵۰	۲	۵	۷	۸	۲۸	پیکربندی امنیتی ناامن
۵۰	۳	۷	۴	۶	۳۰	نرم افزار و میان افزار ناامن
۵۰	۲	۴	۴	۵	۳۵	حفاظت فیزیکی ناکافی
۵۰	۵	۵	۳۰	۴	۶	کمبود صحت ارتباطات
۵۰	۳	۳	۶	۳۱	۷	معماری امنیت شبکه شکننده
۵۰	۲	۳	۷	۸	۳۰	عدم وجود فایروال یا پیکربندی نادرست

کنترل‌های محیطی، ذخیره سازی ناامن داده‌ها و پیکربندی‌های مهم، رمز گذاری نادرست انتقال، پیکربندی امنیتی ناامن، نرم افزار و میان افزار ناامن، حفاظت فیزیکی ناکافی، عدم وجود فایروال یا پیکربندی نادرست دارای بیشترین اهمیت بوده است (شکل ۱):

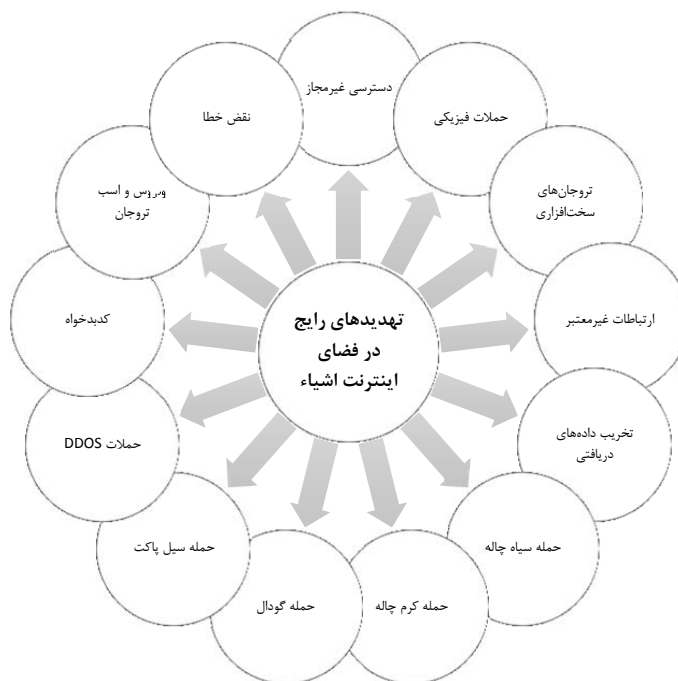
مطابق جدول ۵ آسیب پذیری‌ها در ۲۱ آیت طبقه بندی شده‌اند که در ۱۲ گروه کلی می توان جمع بندی نمود. این ۱۲ گروه آسیب پذیری به ترتیب نقض حریم خصوصی، رابط ابری ناامن، پیکربندی نادرست و استفاده از تنظیمات پیش فرض، سیاست گذاری‌های نادرست، عدم مدیریت تغییرات امنیتی، عدم



شکل ۱. آسیب پذیری های رایج در حوزه اینترنت اشیاء

سؤال به ذهن مخاطب خطور می کند که تهدیدهای امنیتی که فضای اینترنت اشیاء را تحت تأثیر قرار می دهد کدامند. در پاسخ به این سؤال، تهدیدهای امنیتی که دارای بیشترین حوزه اثر در این فضا هستند در قالب شکل ۲ به تصویر کشیده شده است:

سؤال دوم پژوهش: تهدیدهای امنیتی که اینترنت اشیاء را تحت تأثیر قرار می دهند کدامند؟
 با توجه به تجزیه و تحلیل نظرات افراد در جامعه مورد بررسی پیرامون تأیید نقش تهدیدهای امنیتی در حوزه اینترنت اشیاء، این



شکل ۲: تهدیدهای رایج در حوزه اینترنت اشیاء

سوال سوم پژوهش: تهدیدهای امنیتی نشأت گرفته از وجود دارند که از محل آسیب پذیری امکان بروز پیدا می کنند. همچنین برای مقابله با این تهدیدها راهکارها و الزامهای امنیتی وجود دارد که باید رعایت شوند.

آسیب پذیری های شناخته شده کدامند؟
 باتوجه به اینکه آسیب پذیری ها منشأ اصلی بروز تهدیدها هستند. به ازای هر آسیب پذیری، حمله ها و تهدیدهای بالقوه ای

جدول ۶. توزیع فراوانی تهدیدهای نشأت گرفته از آسیب پذیری ها

مجموع	کاملاً مخالف	مخالف	نظری ندارم	موافق	کاملاً موافق	تهدید	آسیب پذیری
۵۰	۲	۵	۷	۲۸	۸	دسترسی غیرمجاز	آسیب پذیری احراز و تشخیص هویت ناکافی
۵۰	۳	۷	۴	۶	۳۰	حملات فیزیکی	
۵۰	۲	۴	۴	۵	۳۵	تروجان های سخت افزاری	
۵۰	۲	۴	۶	۳۱	۷	استراق سمع	آسیب پذیری نقض حریم خصوصی
۵۰	۲	۴	۷	۲۹	۸	استراق سمع	
۵۰	۲	۵	۶	۷	۳۰	دسترسی غیرمجاز	
۵۰	۱	۲	۷	۹	۳۱	ارتباطات غیر معتبر	
۵۰	۳	۶	۵	۳۰	۶	حملات فیزیکی	آسیب پذیری پیکربندی نادرست و استفاده
۵۰	۳	۳	۸	۲۹	۷	خرابی تجهیزات	
۵۰	۳	۳	۶	۷	۳۱	نقص خط	
۵۰	۲	۴	۶	۸	۳۰	تخریب داده های دریافتی	آسیب پذیری رمز گذاری نادرست انتقال
۵۰	۳	۳	۶	۳۰	۸	رهگیری داده	
۵۰	۳	۴	۵	۳۲	۶	تزریق پاکت مخرب	آسیب پذیری رمز گذاری نادرست انتقال
۵۰	۳	۳	۶	۷	۳۱	حمله سیاه چاله	
۵۰	۲	۵	۶	۸	۲۹	حمله کرم چاله	
۵۰	۳	۴	۵	۳۳	۵	حملات مسیریابی	آسیب پذیری امنیت وب نامن
۵۰	۳	۳	۸	۲۹	۷	DOS حملات	
۵۰	۳	۳	۶	۷	۳۱	حمله سیاه چاله	
۵۰	۲	۴	۶	۸	۳۰	حمله گودال	
۵۰	۳	۳	۶	۳۰	۸	حملات مسیریابی	آسیب پذیری معماری امنیت شبکه شکننده
۵۰	۳	۴	۵	۳۲	۶	حمله Sybil	
۵۰	۳	۳	۶	۷	۳۱	حمله سیل پاکت	
۵۰	۲	۵	۶	۸	۲۹	حملات DDOS	
۵۰	۳	۴	۵	۳۳	۵	حمله حلقه مسیریابی	آسیب پذیری پیکربندی امنیتی نامن
۵۰	۲	۴	۷	۲۹	۸	دسترسی غیرمجاز	
۵۰	۲	۵	۶	۷	۳۰	کد بدخواه	
۵۰	۱	۲	۷	۹	۳۱	ویروس و اسب تروژان	
۵۰	۳	۶	۵	۳۰	۶	SQL حمله تزریق	

بیشترین تهدید برای آسیب پذیری اتصال وب ناامن در نظر گرفته می شوند؛ همچنین حمله سیل پاکت، حملات DDOS، حمله Sybil، و حمله حلقه مسیریابی به ترتیب به عنوان بیشترین تهدید برای آسیب پذیری معماری امنیت شبکه شکننده در نظر گرفته می شوند و در نهایت اگر پیکربندی امن برای سیستم صورت نپذیرد این تهدید می تواند به عنوان عاملی برای آسیب رسانی به سیستم در نظر گرفته شود. با توجه به جدول فوق، ویروس و اسب تروژان، کد بدخواه، دسترسی غیرمجاز و حمله تزریق SQL به ترتیب به عنوان بیشترین تهدید برای آسیب پذیری پیکربندی امنیتی ناامن در نظر گرفته می شوند.

اما از آنجایی که هدف اصلی این پژوهش ارائه راهکارهای امنیتی در فضای اینترنت اشیاء است و هر آسیب پذیری منجر به ایجاد تهدیدها و حمله ها می شود، به نگاشت تهدیدها بر آسیب پذیری ها پرداخته می شود. جدول ۶ نگاشت تهدیدها بر آسیب پذیری ها را نشان می دهد:

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 آسیب رسانی به سیستم محسوب شوند. با توجه به جدول فوق، تروجان سخت افزاری، استراق سمع، دسترسی غیرمجاز و حملات فیزیکی به ترتیب به عنوان بیشترین تهدید برای آسیب پذیری احراز و تشخیص هویت ناکافی در نظر گرفته می شوند؛ همین طور، ارتباطات غیرمعتبر، دسترسی غیرمجاز، استراق سمع و حملات فیزیکی به ترتیب به عنوان بیشترین تهدید برای آسیب پذیری نقض حریم خصوصی در نظر گرفته می شوند؛ نقض خط، تخریب داده های دریافتی، رهگیری داده و خرابی تجهیزات نیز به ترتیب به عنوان بیشترین تهدید برای آسیب پذیری پیکربندی نادرست و استفاده از تنظیمات پیش فرض در نظر گرفته می شوند؛ حمله سیاه چاله، و حمله کرم چاله، تزریق پاکت مخرب و حملات مسیریابی را می توان به ترتیب به عنوان بیشترین تهدید برای آسیب پذیری رمزگذاری نادرست انتقال در نظر گرفت؛ حمله سیاه چاله، حمله گودال، حملات مسیریابی و حملات DOS به ترتیب به عنوان

جدول ۷. نگاشت تهدیدها بر آسیب پذیری ها

تهدید	آسیب پذیری	احراز و تشخیص هویت ناکافی	نقض حریم خصوصی	پیکربندی نادرست و استفاده از تنظیمات پیش فرض	رمزنگاری نادرست انتقال	اتصال وب ناامن	معماری امنیت شکننده	پیکربندی امنیتی ناامن
	دسترسی غیرمجاز	✓	✓					✓
	حملات فیزیکی	✓						
	تروجان های سخت افزاری	✓						
	ارتباطات غیرمعتبر		✓					
	نقض خطا			✓				
	تخریب داده های دریافتی			✓				
	حمله سیاه چاله				✓	✓		
	حمله انسداد سرویس توزیع شده					✓	✓	
	کد بدخواه							✓
	حمله کرم چاله				✓			
	اسب تروجان							✓
	حمله گودال					✓		
	حمله سیل پاکت						✓	

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

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

اما آخرین سؤال تحقیق به راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در فضای اینترنت اشیا اشاره دارد. در پاسخ به این سؤال، باتوجه به بررسی های به عمل آمده از مبانی نظری تحقیق و نتایج بدست آمده از نظرسنجی افراد در جامعه مورد بررسی در جداول زیر می توان راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در حوزه اینترنت اشیا را به صورت شکل ۳ پیشنهاد نمود:

جدول ۸. توزیع فراوانی الزامهای امنیتی جهت مواجهه با آسیب پذیری ها

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

۵۰	۳	۴	۵	۳۲	۶	وقایع نگاری و مانیتورینگ	آسیب پذیری پیکربندی امنیتی ناامن
۵۰	۳	۳	۶	۷	۳۱	پیکربندی معماری امن	
۵۰	۲	۵	۶	۸	۲۹	کنترل دسترسی	
۵۰	۳	۴	۵	۳۳	۵	رمزنگاری ارتباطات و داده ها	
۵۰	۲	۴	۷	۲۹	۸	حفاظت الکترومغناطیسی کافی	آسیب پذیری نرم افزار و میان افزار ناامن
۵۰	۲	۵	۶	۷	۳۰	احراز و تصدیق هویت کارآمدتر و دو طرفه	
۵۰	۱	۲	۷	۹	۳۱	کنترل دسترسی	
۵۰	۳	۶	۵	۳۰	۶	رمزنگاری ارتباطات و داده ها	
۵۰	۳	۳	۶	۳۱	۷	حفاظت فیزیکی کافی	آسیب پذیری حفاظت فیزیکی ناکافی
۵۰	۳	۴	۵	۶	۳۲	احراز و تصدیق هویت کارآمدتر	
۵۰	۵	۶	۴	۵	۳۰	کنترل دسترسی	
۵۰	۲	۵	۶	۳۲	۵	رمزنگاری ارتباطات و داده ها	
۵۰	۲	۴	۷	۲۹	۸	حفاظت فیزیکی کافی	آسیب پذیری کمبود صحت ارتباطات
۵۰	۲	۵	۶	۷	۳۰	احراز و تصدیق هویت کارآمدتر و دو طرفه	
۵۰	۱	۲	۷	۹	۳۱	کنترل دسترسی	
۵۰	۳	۶	۵	۳۰	۶	رمزنگاری ارتباطات و داده ها	

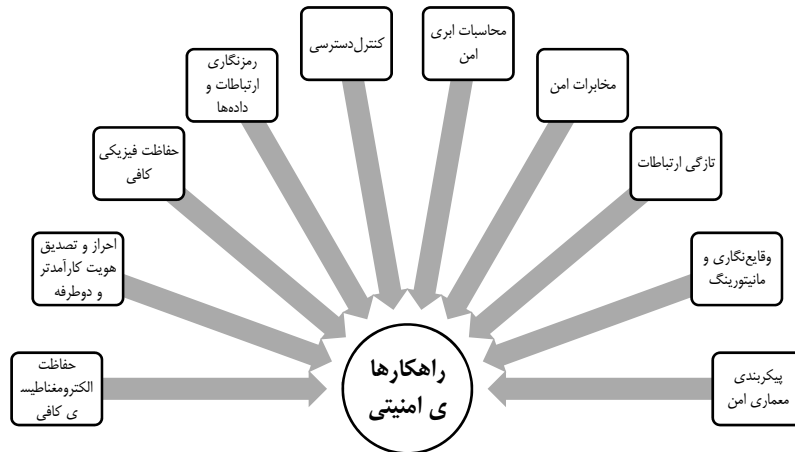
به ترتیب به عنوان بیشترین الزام امنیتی برای مواجهه با آسیب پذیری اتصال وب ناامن در نظر گرفته می شوند؛ احراز و تصدیق هویت کارآمدتر، تازگی ارتباطات، حفاظت الکترومغناطیسی کافی و کنترل دسترسی به ترتیب به عنوان بیشترین الزام امنیتی برای مواجهه با آسیب پذیری سرویس شبکه ناامن در نظر گرفته می شوند.

همچنین، احراز و تصدیق هویت کارآمدتر و دو طرفه، کنترل دسترسی، تازگی ارتباطات و رمزنگاری ارتباطات و داده ها به ترتیب به عنوان بیشترین الزام امنیتی برای مواجهه با آسیب پذیری رمزگذاری نادرست انتقال در نظر گرفته می شوند؛ پیکربندی معماری امن، کنترل دسترسی، وقایع نگاری و مانیتورینگ و رمزنگاری ارتباطات و داده ها به ترتیب به عنوان بیشترین الزام امنیتی برای مواجهه با آسیب پذیری پیکربندی امنیتی ناامن در نظر گرفته می شوند؛ کنترل دسترسی، احراز و تصدیق هویت کارآمدتر و دو طرفه، حفاظت الکترومغناطیسی کافی و رمزنگاری ارتباطات و داده ها به ترتیب به عنوان بیشترین الزام امنیتی برای مواجهه با آسیب پذیری نرم افزار و میان افزار ناامن در نظر گرفته می

داده های جدول ۸ نشان دهنده آن است که، اگر هر کدام از این آسیب پذیری ها در سیستم وجود داشته باشد، می تواند به عنوان عاملی برای تهدیدها و آسیب رسانی به سیستم در نظر گرفته شوند. با توجه به جدول فوق، احراز و تصدیق هویت کارآمدتر، حفاظت فیزیکی کافی، حفاظت الکترومغناطیسی کافی و رمزنگاری ارتباطات و داده ها به ترتیب به عنوان بیشترین الزام امنیتی برای مواجهه با آسیب پذیری احراز و تشخیص هویت ناکافی در نظر گرفته می شوند؛ احراز و تصدیق هویت کارآمدتر و دو طرفه، کنترل دسترسی، حفاظت الکترومغناطیسی کافی و رمزنگاری ارتباطات و داده ها به ترتیب به عنوان بیشترین الزام امنیتی برای مواجهه با آسیب پذیری نقض حریم خصوصی در نظر گرفته می شوند؛ محاسبات ابری امن، حفاظت الکترومغناطیسی کافی، حفاظت فیزیکی کافی و رمزنگاری ارتباطات و داده ها به ترتیب به عنوان بیشترین الزام امنیتی برای مواجهه با آسیب پذیری رابط ابری ناامن در نظر گرفته می شوند؛ احراز و تصدیق هویت کارآمدتر و دو طرفه، کنترل دسترسی، رمزنگاری ارتباطات و داده ها و حفاظت الکترومغناطیسی کافی

و تصدیق هویت کارآمدتر و دو طرفه، حفاظت فیزیکی کافی و رمزنگاری ارتباطات و داده‌ها به ترتیب به عنوان بیشترین الزام امنیتی برای مواجهه با آسیب پذیری کمبود صحت ارتباطات در نظر گرفته می شوند.

شوند؛ احراز و تصدیق هویت کارآمدتر و دو طرفه، کنترل دسترسی، حفاظت فیزیکی کافی و رمزنگاری ارتباطات و داده‌ها به ترتیب به عنوان بیشترین الزام امنیتی برای مواجهه با آسیب پذیری حفاظت فیزیکی ناکافی در نظر گرفته می شوند و در نهایت، احراز



شکل ۳. راهکارهای امنیتی امنیتی حوزه اینترنت اشیا

بحث و نتیجه گیری

هدف از این پژوهش شناسایی تهدیدها و آسیب پذیری های رایج اینترنت اشیا و ارائه راهکارهای امنیتی جهت مواجهه با آنها است. اینترنت اشیا می تواند به آینده بهتر و رویایی منجر شود که حداکثر بهره برداری با کم ترین تلاش را داشته باشد و این سیستم را آسان تر و کاربر پسند می دانند که یک رویکرد منظم در مدیریت اطلاعات است (وندانا، باتاچارجی و گوپتا، ۲۰۱۷). ولی با این حال بنسال، آرورا، سوری (۲۰۱۸) بیان می کنند که فن آوری های جدید چالش های جدیدی را نیز به همراه دارند. مانند نحوه استفاده، نوع اشکالات و چگونگی بهبود آنها و غیره. آنها برخی از چالش های این فن آوری را چنین اعلام می کنند:

۱ - حریم خصوصی و امنیت: کاربران برای بهره مندی از فن آوری اینترنت اشیا 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 فن آوری اینترنت اشیا 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 می شود 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: هزینه هایی مانند برجسبها، سنسورها، محرک ها، دستگاه های ارتباط، اتصال به اینترنت و غیره که نیاز به سرمایه گذاری دارد.

این فن آوری نوپا، در بدو تولد خود به شدت به موضوع امنیت توجه نشان داده است. شرکت های گوگل، سامسونگ، سونی و دیگر غول های فن آوری که به نوعی در رشد یافتن این فن آوری نقش داشته اند، رعایت ایمنی را یکی از اصول اولیه کار قرار داده اند

مذکور حسب دیدگاه و حوزه فعالیت خود، مجموعه متنوعی را به عنوان راهکارهای امنیتی جهت مواجهه با تهدیدهای امنیتی در حوزه اینترنت اشیاء تبیین نموده‌اند، اما در یک نگاه کلی و با جمع‌بندی نظرات ارائه شده توسط شرکت کنندگان می‌توان انواع راهکارهای امنیتی در برابر تهدیدهای امنیتی در فضای اینترنت اشیاء را در قالب جدول ۶ پیشنهاد نمود:

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 می‌دارد اگرچه اساتید و متخصصان حوزه فناوری اطلاعات دانشگاه های

جدول ۹. راهکارهای امنیتی جهت مواجهه با تهدیدهای نشأت گرفته از آسیب پذیری ها حوزه اینترنت اشیاء

آسیب پذیری تهدید	احراز و تشخیص هویت ناکافی	نقض حریم خصوصی	پیکربندی نادرست و استفاده از تنظیمات پیش فرض	رمزنگاری نادرست انتقال	اتصال وب ناامن	معماری امنیت شکننده	پیکربندی امنیتی ناامن
دسترسی غیرمجاز	احراز و تصدیق هویت کارآمد دوطرفه	کنترل دسترسی					پیکربندی معماری امن
حملات فیزیکی	احراز و تصدیق هویت کارآمد دوطرفه	حفاظت فیزیکی کافی					
تروجان های سخت افزاری	احراز و تصدیق هویت کارآمد دوطرفه وقایع نگاری 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			کنترل دسترسی	رمزنگاری ارتباطات و داده‌ها			
حمله سیاه چاله				رمزنگاری ارتباطات و داده‌ها	احراز و تصدیق هویت کارآمد دوطرفه		

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

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

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

هر تحقیق با توجه به ماهیت خاص خود دارای محدودیت‌هایی است که تحقیق حاضر هم از این امر مستثنی نیست. پیشرفت‌های سریع در حوزه فناوری اطلاعات و به طور مثال، دسترسی به روش‌های جدید محافظت از داده‌ها و اطلاعات، و یا دسترسی به روش‌های کم هزینه برای استقرار اینترنت اشیا و.... می‌تواند موانع و چالش‌های اشاره شده در این تحقیق را دستخوش تغییر نماید و یا منجر به تغییر در رتبه بندی آنها شود.

- 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.fridjournal-events.com/IoT>. Retrieved from <http://www.fridjournal-events.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
- بررسی تاثیر استقرار اینترنت اشیاء بر جنبه های مختلف عملکرد سازمان ها با تاکید بر کتابخانه ها
- بررسی تاثیر اینترنت اشیاء بر استقبال 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 Philosophy and Practice e-Journal*.
- Bhunja, 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>.

- Vandana, C. P. M.; Bhattacharjee, M. A.; Gupta, 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.; Shiuhyng, 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.
- Tehraniipoor, M.; Koushanfar, F. (2010). *A survey of hardware trojan taxonomy and detection*." IEEE Design & Test of Computers 27.1

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

Safiyeh Tahmasebi Limooni¹ | Shahrzad Ghasemi² | Roghayeh Ghorbanloo³

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 experts 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