اولین کنفرانس بین المللی مدیریت و صنعت
۱۲ شهریور ۱۴۰۰ - تفلیس / گرجستان
1ST National Conference on Management & Industry
3 September 2021 - Georgia

حفظ امنیت در شهرهای هوشمند مبتنی بر اینترنت اشیا (مطالعه موردی: شهر اصفهان)

سیما لطفی [۱]
[۱] کارشناس ارشد مدیریت فناوری اطلاعات، مهرالبرز، تهران، ایران، sima.00.lotfi@gmail.com

چکیده

اینترنت اشیا(IoT) یک تکنیک نوظهور برای اتصال دستگاه‌هایی است که به شکل حسگر، محرک، تلفن همراه، رایانه، کنتور یا حتی وسایل نقلیه درمی‌آیند تا بتوانند آدرس‌پذیر و قابل شناسایی باشند. اینترنت اشیا مزایای نامحدودی برای محیط زیست ما دارد و به یکی از روندهای تحقیقاتی برای هر دو سازمان دانشگاهی و تجاری تبدیل شده است. بسیاری از معماری‌ها و برنامه‌های کاربردی با استفاده از بستر اینترنت اشیا از یک زنجیره تأمین ساده تا سیستم‌های پیچیده پیشنهاد و اجرا شده‌اند. مزایای آشکار بسیاری از این‌گونه شبکه‌ها وجود دارد اما این سیستم‌ها می‌توانند در صورت به خطر افتادن باعث تهدید مالی و زندگی شوند. رسیدگی به این مسائل و اطمینان از امنیت و حریم خصوصی محصولات و خدمات اینترنت اشیا با رعایت اصول اخلاقی باید یک اولویت اساسی باشد. این امر مستلزم یک معماری قوی است که بتواند تأیید اعتبار کاربر، کنترل دسترسی و همچنین حریم خصوصی و اعتماد کاربران سیستم را فراهم کند. در شبکه IoT به عنوان یک شبکه ناهمگن برای اتصال بسیاری از دستگاه‌های محدودکننده سخت‌افزار کوچک، نمی‌توان از معماری‌ها و تکنیک‌های امنیتی سنتی استفاده کرد. در این مقاله، چالش‌های امنیتی و اخلاقی IoT و راه‌حل‌هایی برای حفظ سطح امنیتی قابل توجه در شهر هوشمند اصفهان ارائه شده است که یک شهر صنعتی و توریستی می‌باشد. همچنین به ارزیابی وضعیت فعلی و جهت‌گیری‌های آینده اینترنت اشیا در اصفهان، در قالب پرسش‌نامه با مقیاس طیف لیکرت می‌پردازد. نتایج تحقیق می‌تواند با ادغام بهترین جنبه‌های امنیتی دستگاه‌های مبتنی بر اینترنت اشیا، از جامعه تحقیقاتی در اینترنت اشیا پشتیبانی کند.

واژگان کلیدی: امنیت و اصول اخلاقی اینترنت اشیا، تهدیدهای اینترنت اشیا، شهر هوشمند

مقدمه

همه اشیای موجود در محیط ما می‌توانند از طریق اینترنت با قابلیت اتصال به یکدیگر بدون دخالت انسان متصل شوند. اینترنت اشیا شامل اشیای مختلفی است که می‌توانند با استفاده از شبکه‌های بی سیم یا سیمی متصل شوند. این اشیا دارای یک طرح آدرس‌دهی منحصر به فرد هستند که به آن‌ها امکان می‌دهد برای ایجاد برنامه‌ها و خدمات جدید مانند خانه‌های هوشمند، حمل و نقل هوشمند، اتومبیل‌های متصل، شبکه‌های هوشمند، شهرهای هوشمند، کنترل ترافیک هوشمند و موارد دیگر با یکدیگر تعامل و همکاری کنند. اینترنت اشیا در شهر هوشمند بسیاری از فناوری‌ها مثل فناوری حسگرها، فناوری شبکه و فناوری‌های مربوط به داده‌ها را بکار می‌گیرد. با توجه به توسعه سریع فناوری حسگرها و فناوری شبکه، حجم داده‌های بدست آمده حاصل از توسعه فناوری‌ها، رشد زیادی خواهد داشت که موجب بروز چالش‌هایی است. به منظور درک چالش‌ها و ارائه راه حل‌هایی که شهر هوشمند، در این زمینه با آن مواجه است لزوم مطالعه و بررسی ابعاد مختلف مسئله مهم و لازم به نظر می‌رسد. موضوع شهر هوشمند در بین داغ‌ترین بحث‌های پژوهشی و کسب‌وکار قرن بیست و یکم قرارگرفته است. در سخنرانی نمایش محصولات الکترونیکی قابل فروش سال ۲۰۱۴ لاس وگاس آمریکا، مدیرعامل شرکت سیسکو، جان چمبرز اذعان داشت که در دهه آینده، فرصت اقتصادی حاصل از اینترنت اشیا در بخش خصوصی و دولتی، به مبلغی در حدود ۱۹ تریلیون دلار خواهد رسید. انتظار می‌رود تا سال ۲۰۲۵، بیش از ۴۱ درصد از جمعیت جهان در شهرهای هوشمند زندگی کنند. امروزه با توسعه و گسترش فناوری‌های اطلاعات و ارتباطات، بهره‌گیری از آن‌ها در مدیریت بهینه و اصولی، مورد توجه قرار گرفته است و فعالیت‌های روزمره را به سمت استفاده از ارتباطات هوشمند تعاملات و اطلاعات سوق داده است و بدین شکل، شهرهای سنتی در حال حرکت به سمت شهر هوشمند می‌باشند. اینترنت اشیا در هر زمان، در هر مکان، برای هر شخص و برای هر چیزی قابل استفاده است. بر طبق اعلامیه بانک جهانی در سال ۲۰۱۹ و با توجه به رشد روزافزون جمعیت شهرنشین تا سال ۲۰۴۵، در حدود ۸۰ درصد تولید ناخالص جهانی توسط شهرها تولید می‌شود.

اینترنت اشیا به عنوان محیط بین دستگاهی ساخته‌شده توسط دستگاه‌هایی است که روی سه کار مهم متمرکز هستند: انتقال داده‌ها، دریافت داده‌ها و پردازش داده‌های دریافتی. در ابتدا، دستگاه‌های فیزیکی محلی متصل به اینترنت برای تجزیه و تحلیل داده‌های زمان واقعی، شبکه اینترنت اشیا محسوب می‌شدند. با گذشت زمان، مقیاس IoT خود را از ایستگاه کاری محلی تا چارچوب‌های IoT صنعتی گسترش داده است. کارهای تحقیقاتی در زمینه اینترنت اشیا، گسترش اینترنت اشیا در زمینه بهداشت و درمان، تنظیمات صنعتی، تجزیه و تحلیل تجارت، آموزش و غیره را نشان می‌دهد. از سال ۲۰۱۹، اینترنت اشیا که قبلاً در فضاهای شبکه کوچک‌تر کار می‌کرد، برای شبکه‌های وسیع ارتقا یافته است.

مقبولیت اجتماعی برنامه‌ها و سرویس‌های اینترنت اشیا به شدت به قابلیت اطمینان اطلاعات و محافظت از داده‌های خصوصی بستگی دارد. از آنجا که اینترنت اشیا یک سیستم پیچیده، توزیع شده و ناهمگن است، با چالش‌های متعددی در رابطه با امنیت و حریم خصوصی مواجه است. در حال حاضر ، ایجاد یک تکنیک امنیتی مؤثر و قابل اعتماد یکی از بالاترین اولویت‌هایی است که باید در نظر گرفته شود که باید برای معماری‌های جدید طراحی شود که یک محیط سیستم ایمن و قابل اعتماد را فراهم می‌کند [7]. علاوه بر این، نیاز به تدوین چارچوبی اخلاقی وجود دارد که اطمینان حاصل کند اینترنت اشیا به نفع بشریت است و نه برعکس. یک استاندارد اخلاقی قوی باعث انگیزه شرکت‌ها برای تولید محصولات هوشمندانه‌تر و فراگیرتر می‌شود تا از مسائل جدید جلوگیری کنند و از اتصال جهانی اطمینان حاصل کنند. برخی از مشکلات مانند مدیریت و امنیت اطلاعات کارآمد و مؤثر، هنوز هم وجود دارند، زیرا مقدار زیادی داده در زمان واقعی داریم. با این وجود پیش‌بینی می‌شود هزینه‌های دستگاه‌های اینترنت اشیا در

سال ۲۰۲۲ بیش از ۱ تریلیون دلار باشد [8] و پیش‌بینی می‌شود که تمرکز جمعیت شهری تا سال ۲۰۵۰ به ۶۶٪ افزایش یابد [9].

سرویس‌های ابری اغلب می‌توانند یک راه حل برای حل مشکلات فوق باشند، زیرا سیستم‌های ناهمگن در شهرهای هوشمند یا محیط‌هایی که مقدار زیادی داده در آن‌ها رخ می‌دهد، برای مدیریت اطلاعات به طور فزاینده‌ای پیچیده و چالش برانگیز است[7-8] برای چالش‌های محیط و مدیریت داده‌های عظیم، کاربران اینترنت اشیا در درجه اول از ابرهای عمومی خارجی استفاده می‌کنند. داده‌های موجود در دستگاه‌های اینترنت اشیا که توسط کاربران در محیط‌های شهر هوشمند تولید می‌شوند، حاوی اطلاعات شخصی می‌باشند که نباید برای عموم افشا شود. سیستم‌های عملیاتی مختلف، انتقال داده را با توجه به نیازهای عملیاتی کسب و کار ادغام و تنظیم می‌کنند، بهره‌وری عملیات شهری را بهبود می‌بخشند و سطح زندگی و کیفیت زندگی مردم را ارتقا می‌دهند. اساس عملیاتی شهرهای هوشمند؛ اشتراک داده‌ها، و تجزیه و تحلیل هوشمند و تصمیم‌گیری داده‌ها است. سیستم‌های مختلف هوشمند از یکدیگر مستقل هستند، اطلاعات و داده‌ها نمی‌توانند به صورت پویا و در زمان واقعی از طریق شبکه به خوبی منتقل شوند و درجه همکاری بین مشاغل کافی نیست. از دلایل این وضعیت می‌توان به سطح ناهموار عملکرد سرویس‌های سخت‌افزاری سیستم‌های هوشمند در زمینه‌های مختلف و اختلافات زیاد در محیط نرم‌افزار اشاره کرد که منجر به هزینه بسیار بالای انتقال داده‌ها می‌شود. برای حل مشکل سخت‌افزار، سازمان‌های دولتی شهرها می‌توانند مطابق با الزامات به طور یکنواخت هماهنگ باشند و برای مسئله تطبیق محیط نرم‌افزار، سازمان‌های دولتی شهرها می‌توانند رابط‌های انتقال اطلاعات را برای نرم‌افزارهای کاربردی مختلف ایجاد کنند.

امروزه، تکامل فناوری اطلاعات(IT) فقط انفجاری از وسایل اینترنت اشیا نیست بلکه آن‌ها را در زندگی واقعی مانند شهر هوشمند دیجیتالی می‌کند. این تغییر فراتر از یک فضای فردی کوچک مانند خانه‌های هوشمند است و مفهوم شهرهای هوشمند بوجود آمده است. شهر هوشمند به معنای شهری پیشرفته است که فناوری اطلاعات و منابع شهری آن علاوه بر ایجاد راحتی، نوآوری‌های کارآمد و هوشمندی را جمع می‌کند [9]. شهر هوشمند اخیراً همراه با توسعه سریع IT در جامعه مدرن و پدیده شهرنشینی با تراکم جمعیت بالا بسیار مورد توجه قرار گرفته است [10]. ایده یک شهر هوشمند از مفهوم زمین هوشمند که در سال ۲۰۰۸ توسط IBM پیشنهاد شد، سرچشمه گرفت. پس از بیش از ده سال توسعه، شهرهای هوشمند به هدف مهم ساخت و ساز شهری در برخی از کشورهای پیشرفته تبدیل شده‌اند. ایالات متحده و اتحادیه اروپا تلاش زیادی برای ساختن آن‌ها می‌کنند. نتیجه رتبه‌بندی "شاخص پویایی شهری IESE" در سال ۲۰۱۸ نشان داد که بهترین شهرهای هوشمند جهان نیویورک، لندن و پاریس هستند. در چین، دولت ملی راهنمایی‌هایی را برای ساخت شهرهای هوشمند ارائه داد و پیشنهاد شد مجموعه‌ای از شهرهای هوشمند با ویژگی های متمایز چینی در سال ۲۰۲۰ ساخته شود. ساخت شهرهای هوشمند به شاخص مهمی برای اندازه‌گیری سطح اطلاعات و صنعتی شدن یک شهر تبدیل شده است. شهرهای هوشمند شامل تمام جنبه‌های عملکرد شهری هستند، مانند سیستم‌های عملیاتی دولتی، سیستم‌های حمل و نقل شهری، سیستم‌های پزشکی و بهداشتی، آموزش و تحقیقات علمی، سیستم‌های فرهنگ و گردشگری، سیستم‌های کنترل صنعتی و سیستم‌های اتوماسیون کشاورزی و ... .

شهر هوشمند با تکیه بر فناوری اطلاعات و ارتباطات بر افراد هوشمند، زندگی هوشمند، محیط هوشمند، اقتصاد هوشمند، حمل و نقل هوشمند و حکمروایی هوشمند تأکید دارد. در سال ۱۳۹۴، شهرهای ارومیه، اصفهان، تهران، مشهد و تبریز به عنوان پنج شهر هوشمند ایران معرفی شدند. در این مقاله، به هوشمندسازی شهر اصفهان پرداخته شده است. اصفهان، سومین شهر پرجمعیت

ایران پس از تهران و مشهد و همچنین یکصد و شصت و پنجمین شهر پرجمعیت جهان و نهمین شهر پرجمعیت باختر آسیا به‌شمار می‌رود. کلان‌شهر اصفهان نیز چهاردهمین کلان‌شهر پرجمعیت خاورمیانه است.

سؤال اساسی این می‌باشد که آیا حملات و خطرات امنیتی در اینترنت اشیا به خوبی شناسایی شده‌اند و روش‌هایی که برای افزایش امنیت در اینترنت اشیا ارائه شده است توانایی مقابله با خطرات امنیتی را دارد؟ **هدف اصلی این پژوهش**، بررسی چالش‌های امنیتی ایجاد شده توسط اینترنت اشیا و ارائه راهکار بهبود امنیت آن در مدیریت شهری برای رسیدن به شهر هوشمند است.

اهداف فرعی این پژوهش عبارتند از:

شناسایی خطرات امنیتی و آسیب‌پذیری اینترنت اشیا با پیاده‌سازی این فناوری

شناسایی پارامترهای تاثیرگذار بر امنیت سیستم‌های اینترنت اشیا در برابر نفوذ

تبیین راهکارهایی جهت بهبود امنیت شبکه هوشمند اینترنت اشیا

و همچنین **سؤالات دیگر این پژوهش** عبارتند از:

با در نظر گرفتن چه عوامل و فاکتورهایی می‌توان نفوذ به سیستم اینترنت اشیا را کاهش داد؟

چه خطرات امنیتی با بکارگیری اینترنت اشیا در شهرهای هوشمند پدیدار می‌شود؟

آیا پیاده‌سازی اینترنت اشیا منجر به کاهش مشکلات امنیتی شهری می‌شود؟

چه راه حل‌هایی را می‌توان در جهت بهبود امنیت شهرهای هوشمند مبتنی بر اینترنت اشیا بکار گرفت؟

انگیزه کار برای کشف نگرانی‌های امنیتی در دستگاه‌های مبتنی بر اینترنت اشیا به دلیل کاربردهای مختلف اینترنت اشیا است. اول، برای درک جنبه امنیتی اینترنت اشیا، داشتن دانش قبلی در مورد زیرساخت‌هایی که با آن‌ها سر و کار داریم، مهم است. بنابراین، ما در مورد معماری اینترنت اشیا بحث کرده ایم و یک تحلیل مقایسه ای از پروتکل‌ها و استانداردهای مورد استفاده در اینترنت اشیا انجام داده ایم. سهم تحقیق دوم ما شامل بررسی تمام جنبه‌های احتمالی تحقیقات اخیر در زمینه امنیت اینترنت اشیا است که در ایجاد چارچوب امنیتی اینترنت اشیا سودمند خواهد بود. یک بررسی دقیق ارائه شده در این بررسی، تهدیدات برجسته حاکم در سیستم‌های اینترنت اشیای کنونی، همراه با آخرین راه حل‌های امنیتی بهره گرفته شده برای محیط اینترنت اشیا در سال‌های اخیر است.

پیشینه تحقیقات مرتبط اخیر

هنگام بازبینی کارهای موجود در زمینه امنیت اینترنت اشیا، چند مقاله تحقیقاتی مرتبط با این پژوهش، مطالعه و در این بخش تلفیق شدند:

- **Xin Zhang و Fengtong Wen (11)**

تأیید اعتبار WSN کاربر ناشناس جدیدی را برای اینترنت اشیا ارائه می‌دهد که در آن دو مدل الگوریتمی UDS و USD ساخته شده است. دو مدل الگوریتمی UDS(کاربر-دستگاه سرور) و USD(دستگاه سرور کاربر). جنبه امنیتی تحت تأثیر قرار گرفته: احراز هویت می‌باشد. این یک روش چند منظوره برای تأمین امنیت در طی فرآیند احراز هویت با سربارهای ذخیره‌سازی سبک‌تر،

هزینه‌های ارتباطی مؤثر سرعت محاسبات سریع‌تر است. این کار از نظر وسعت راه حل امنیتی ارائه شده محدود است، فقط برای دستگاه‌های حسگر سبک در برابر لایه‌های برجسته شبکه و حملات مبتنی بر لایه فیزیکی.

- **Mohammad Dahman Alshehri و Farookh Khadeer Hussain (12)**

مدل پیاده‌سازی منطق فازی مبتنی بر خوشه همراه با الگوی پیامرسانی ایمن بین گره‌های اینترنت اشیا با استفاده از مقادیر هگزادسیمال. جنبه امنیتی تحت تأثیر قرار گرفته: محرمانه بودن و مدیریت اعتماد می‌باشد، اما خطرات مربوط به سطح حمله ممیزی داده‌ها در این مدل پوشش داده نمی‌شود. این مطالعه همچنین از پرداختن به تجزیه و تحلیل عملکرد نسبت به هزینه‌های ارتباطی و هزینه‌های محاسبه در عملیات رخ می‌دهد.

- **Priyanka Anurag Urla, Girish Mohan, Sourabh Tyagi و Smitha N. Pai (13)**

مدلی که در اینجا مورد بهره‌برداری قرار گرفته است، یک مدل امنیتی چند مرحله ای است که از رمزنگاری منحنی بیضوی (ECC) و رمزگذاری کاملاً هوموورفیک (FHE) برای کاهش حملات رمزنگاری استفاده می‌کند که یکپارچگی داده‌های منتقل شده در محیط اینترنت اشیا با قدرت محاسبه کم‌تر را تضمین می‌کند و جنبه امنیتی تحت تأثیر قرار گرفته: تمامیت و یکپارچگی می‌باشد. با این وجود، در مورد هزینه‌های اضافی هزینه داده ای که در طی فرآیند تولید می‌شود، عدم تصفیه وجود دارد. هزینه محاسباتی مسئله دیگری در مورد این مدل است.

- **Hongsong Chen, Caixia Meng, Zhiguang Shan, Zhongchuan Fu و Bharat K. Bhargava (14)**

یک رویکرد جدید برای تشخیص حمله در مقیاس Denial-of-Service ارائه می‌دهد که شامل ارزیابی اعتماد با تحول HilbertHuangدر Zigbee WSN است. جنبه امنیتی تحت تأثیر قرار گرفته: در دسترس بودن و مدیریت اعتماد می‌باشد. این کار به دلیل روش تشخیص سرعت کم سیگنال، در بازسازی سطح حمله مفید است. این ویژگی از معماری مقیاس پذیر برخوردار است زیرا هم از رایانش ابری و هم از دستگاه‌های اینترنت اشیا لبه محاسبه می‌شود که یک مزیت است، اما سربارهای ذخیره‌سازی بزرگ‌تر همچنان مسئله‌ساز هستند. سیستم‌های تشخیص نفوذ (IDS) وظیفه دارند فعالیت‌های تهدید را در حوزه امنیت شبکه معمولی شناسایی و نظارت کنند.

- **Michail Sidorov, Ming Tze Ong, Ravivarma Vikneswaran, Junya Nakamura, Ren Ohmura و Jing Huey Khor (15,16)**

مایکل سیدوروف و همکاران یک پروتکل RFID بسیار سبک وزن و ایمن ارائه داد که هدف آن ادغام در سیستم مدیریت زنجیره تأمین است که از شبکه بلاکچین مجاز همراه با رمزگذاری ارائه شده در سطوح مختلف دسترسی استفاده می‌کند. جنبه امنیتی تحت تأثیر قرار گرفته: احراز هویت می‌باشد. تجزیه و تحلیل عملکرد نتایج امیدوار کننده ای را با هزینه ذخیره‌سازی کم‌تر و سرعت محاسباتی بالا به تصویر می‌کشد. اعتقاد بر این است که تأثیر قابل توجهی بر دستگاه‌های اینترنت اشیا دارد. با این حال، کل تنظیمات هزینه نامشخص است.

- **Munkenyi Mukhandi, David Portugal, Samuel Pereira و Micael S. Couceiro (17)**

مدل امنیتی مبتدی تازه کار شامل ارتباطات رباتیک در اینترنت اشیای صنعتی با استفاده از MQTT و سیستم عامل ربات. جنبه امنیتی تحت تأثیر قرار گرفته: احراز هویت و یکپارچگی می‌باشد که کارایی آن‌ها را در ایمن‌سازی مراحل ارتباطی ثابت کرده است. این کار بینشی ارزشمند در مورد تأثیر روش‌های رمزنگاری در ایمن‌سازی کانال‌های ارتباطی ارائه می‌دهد. برعکس، این مطالعه تناقض بین معیارهای عملکرد و توابع رمزنگاری را بیان می‌کند. یادگیری عمیق و یادگیری ماشینی بینش خود را در محیط

اینترنت اشیا با محصولات عمده Alexa، Echo، که دستورات متن را نادیده می‌گیرند و دستورات صوتی را برای عمل به صورت زمان واقعی می‌گیرند، درک کرده اند. اما موضوعات مربوط به نشت بسته داده‌ها بوجود آمده است.

- **Pooja Shree Singh, Vineet Khanna (18)**

برای شناسایی و احراز هویت کاربر که برای اطمینان از یکپارچگی داده‌ها، محرمانه بودن و حفظ حریم خصوصی اطلاعات، یک برنامه شناسایی صدا مبتنی بر ضرایب cepstral Mel-frequency (MFCC) را ارائه می‌دهد. جنبه امنیتی تحت تأثیر قرار گرفته: رازداری، صداقت و حریم خصوصی می‌باشد. با این وجود، وابستگی زیاد به معماری سخت افزاری مورد نیاز برای ورودی بدون سر و صدا و کیفیت، مهم‌ترین نقطه نزول آن است. اینترنت اشیا از زمان ورود خود با مشکلات مربوط به کنترل دسترسی دست به گریبان است.

- **Zhao K, Ge L (19)**

یک نظرسنجی در مورد امنیت اینترنت اشیا انجام داد که مسائل امنیتی مربوط به ساختار سه لایه اینترنت اشیا را بیان می‌کند. سه لایه ادراک، شبکه و کاربرد در برابر امنیت اطلاعات، فیزیکی و مدیریت مورد بررسی قرار می‌گیرند. به عنوان مسائل مربوط به لایه درک، ضبط گره، گره‌های جعلی، داده‌های مخرب، انکار سرویس (DoS) ، زمان بندی، تهدیدهای مسیریابی، حملات کانال جانبی (SCA) و حملات پخش مجدد شناسایی می‌شوند. به همین ترتیب، مسائل امنیتی لایه شبکه و لایه کاربرد ارائه شده است، در حالی که اقدامات امنیتی قابل اتخاذ برای هر لایه برای کاهش خطرات ذکر شده است.

- **Ammar M, Russello G, Crispo B (20)**

چارچوب‌های اینترنت اشیا در مورد تأکید بر امنیت و حریم خصوصی بررسی شده است. این مقاله معماری پیشنهادی را توضیح می‌دهد و بخش سخت افزاری به ویژگی‌های امنیتی ۸ چارچوب اینترنت اشیا اشاره می‌کند. چارچوب‌های در نظر گرفته شده شامل IoT سرویس آمازون وب (AWS) ، ARM mbed IoT، مجموعه Azure IoT، Brillo / Weave، Calvin، HomeKit، Kura و SmartThings است. جنبه‌های تأیید اعتبار، کنترل دسترسی، ارتباطات، رمزنگاری با این سیستم عامل‌های جدید مقایسه می‌شود. این یک نظرسنجی جامع است که بینندگان ارزشمندی را در زمینه انتخاب مناسب‌ترین بستر برای کاربردشان به توسعه دهندگان اینترنت اشیا ارائه می‌دهد.

- **Granjal J, Monteiro E, Silva JS (21)**

یک بررسی جامع برای تجزیه و تحلیل پروتکل‌های ارتباطی موجود برای شناسایی نیازهای امنیتی به منظور ایمن‌سازی کانال‌های ارتباطی انجام داد. پروتکل‌های موجود برای فیزیکی (PHY) ، کنترل دسترسی رسانه (MAC) ، شبکه / مسیریابی و لایه‌های برنامه برای استخراج الزامات امنیتی به طور گسترده برای استانداردهای امنیتی آن‌ها مورد تجزیه و تحلیل قرار گرفت. در این میان، IPv6 از طریق شبکه‌های بی سیم منطقه شخصی کم مصرف (LoWPAN۶) و پروتکل مسیریابی برای پروتکل‌های کم مصرف و شبکه-های با ضرر (RPL) به دلیل سازگاری گسترده در برنامه‌های IoT آینده، کاملاً مورد بررسی قرار گرفت. علاوه بر این، چالش‌های تحقیق باز مطابق با الزامات امنیتی مشخص شده برطرف می‌شوند.

- **امیدی و شایسته فرد، ۱۳۹۵**، در پژوهش خود راجع به بررسی امنیت اینترنت اشیا با استفاده از بلاکچین پرداخته‌اند. فناوری بلاکچین، یک راه‌حل مقیاس‌پذیر برای بسیاری از مسائل امنیتی مشترک که در مواجهه با کلان داده‌ها مطرح است، ارائه‌شده است. تکنیک‌های احراز هویت موجود با استفاده از سیستم‌های متمرکز می‌توانند داده‌های بزرگ را بسیار در معرض

خطرات و آسیب‌پذیرهای امنیتی قرار دهند. اکثر پروتکل‌های تأیید هویت بهینه‌شده که در محیط‌های توزیعی استفاده می‌شوند. باید از زیرساخت‌های غیرمتمرکز که مقیاس‌پذیر و قابل‌اطمینان هستند استفاده کنند. بنابراین پیشنهاد استفاده از مزایای فناوری بلاکچین می‌تواند برای تقویت سیستم‌های امنیتی از جمله تأیید اعتبار و مجوز دسترسی به داده‌ها مؤثر واقع شود. [۲]

- **تقوایی و همکاران، ۱۳۹۷**، به بررسی کاربرد بلاکچین در حوزه سلامت پرداختند.

فناوری بلاکچین در مدیریت داده‌های مراقبت سلامت و ارزیابی و بهبود رابط کاربری و اتصال یک سیستم متصل استاندارد توانسته بسیاری از چالش‌های موجود در جهان را از بین ببرد. بلاکچین و دفتر کل توزیع‌شده نقش مهمی در سیستم مراقبت سلامت ایفا خواهند کرد. بهبود تصمیم‌گیری و کاهش هزینه‌ها در مراقبت‌های پزشکی از نتایج مهم استفاده در این فناوری است. با استفاده از فناوری بلاکچین می‌توان اطمینان از حریم خصوصی، امنیت، دسترسی و کنترل دسترسی غیرمستقیم به داده‌ها را تأمین کرد. سوابق یا درواقع بلاک‌ها، می‌توانند با دقت بالایی شناسایی و تأیید شوند. استفاده از بلاکچین در زمینه اینترنت اشیا و سلامت الکترونیک به عنوان یک دفترکل مشترک می‌تواند امنیت بالاتری فراهم کند. بلاکچین می‌تواند با مدیریت رکوردهای پزشکی همچون تایید و ثبت سوابق، پرداخت‌های درمانی، کاهش زمان ثبت خسارات بیمه ای و افزایش کارایی آن، بسیاری از چالش‌های موجود را از بین ببرد. [۳]

نتیجه حاصل از بررسی و مطالعه پیشینه‌ها: کار نویسندگان برای نظرسنجی حاضر بسیار ارزشمند است زیرا باعث آگاهی بیش‌تر در مورد نوع دیگری از حمله در حال افزایش می‌شود که اینترنت اشیا، محصولات و خدمات را تهدید می‌کند. با نگاهی به روند و تحولات بازار، می‌توان دریافت که هنوز نگرانی‌هایی در رابطه با امنیت در محصولات و خدمات اینترنت اشیا وجود دارد.

مبانی نظری

شرکت مخابرات اصفهان فراهم‌کننده خدمات اینترنت پهنای باند ثابت و VDSL و اینترنت فیبر نوری در شهر است. از مهم‌ترین فرصت‌ها و قابلیت‌های استان اصفهان می‌توان به این موارد اشاره کرد: موقعیت مکانی ویژه استان (قرارگرفتن استان در مرکز کشور و در مسیر راه‌های ترانزیتی شمال- جنوب و شرق- غرب و همجواری با ۹ استان)، وجود پتانسیل‌های قوی کارآفرینی رو به رشد، تبدیل استان به یک قطب مهم گردشگری کشور در زمینه‌های تاریخی، طبیعی همچون رودخانه زاینده‌رود و انسان‌ساخت با ارزش ملی و فراملی و وجود بیش از پنج هزار اثر تاریخی غیرمنقول و ده هزار اثر شناخته‌شده منقول بازمانده از ادوار مختلف در جای جای استان، وجود سرمایه‌های انسانی انباشته‌شده به عنوان مکمل فعالیت‌های سرمایه‌گذاری در راستای اقتصاد دانایی‌محور، وجود ظرفیت‌های قوی دانشگاهی و مراکز بزرگ علمی- تحقیقاتی و تولید فناوری‌های متعدد، وجود بخش غیر دولتی توانمند و زمینه‌ساز جذب سرمایه‌گذاری خارجی، دارای فرصت‌های خوبی برای جویندگان اقتصادی در سطح استان با استقرار صنایع مادر و بزرگ در سطح ملی همچون ذوب آهن، فولاد مبارکه، پالایشگاه، دی ام تی، داروسازی، پتروشیمی، هواپیما و هلیکوپترسازی، صنایع و مراکز نظامی، انرژی اتمی، راه‌های اصلی و فرعی مناسب، فرودگاه بین‌المللی، خطوط راه آهن و از همه مهم‌تر رودخانه زاینده‌رود.
در سال‌های گذشته شرایط به سمتی پیش رفته که دانشگاه از نیاز واقعی جامعه و بخش صنعت دور شده و صنعت نیز تنها به رفع نیاز روزمره خود پرداخته است. بنابراین در حال حاضر دانشگاه اصفهان بعنوان دانشگاه جامع و مادر استان اصفهان در راستای کم

کردن این فاصله، قدم‌هایی برداشته است. با استفاده از توان علمی بیش از ۶۵۰ عضو هیئت علمی با ۵۳ ٪ مرتبه استاد تمام و دانشیاری و تعلیم و تربیت بیش از ۱۶۰۰۰ دانشجو با ۴۵٪ دانشجوی تحصیلات تکمیلی در ۷۱ رشته تحصیلی در مقطع کارشناسی، ۱۸۵ رشته تحصیلی در مقطع کارشناسی ارشد و ۱۱۹ رشته در مقطع دکترا در قالب ۱۴ دانشکده و ۵۵ گروه آموزشی در زمینه فنی و مهندسی، علوم انسانی، علوم پایه و زبان‌های خارجی فعالیت می‌کند و یکی از دانشگاه‌های برتر کشور است. در این دانشگاه اصفهان ۵۴ انجمن علمی، ۷ قطب علمی، ۱۰ پژوهشکده و ۳۲ گروه پژوهشی فعال، آزمایشگاه مرکزی و حدود ۱۹۰ آزمایشگاه آموزشی و پژوهشی گروه‌های علمی، کتابخانه مرکزی و ۵ کتابخانه دانشکده‌ها و ۴ سالن مطالعه برای بهره-مندی بهتر و بیش‌تر دانشجویان فراهم شده است. دانشگاه اصفهان یکی از ۵ دانشگاه فعال کشور در امور بین‌الملل می‌باشد و عقد بیش از ۱۵۰ تفاهم‌نامه با ۴۷ دانشگاه اروپایی و ۴۲ دانشگاه آسیایی از ۲۷ کشور جهان و بیش از ۴۰ تفاهم‌نامه عملیاتی شده از سال ۱۳۷۶ تاکنون و با سایر دانشگاه‌های معتبر دنیا نیز ارتباط مستمر علمی دارد.

کمیته اینترنت اشیا در خرداد ماه سال ۹۵ در دانشگاه اصفهان تاسیس شده است. وظایف این کمیته:

- تشکیل جلسات بصورت ماهیانه، تدوین سیاست‌گذاری‌های قطب، برگزاری همایش‌ها و کارگاه‌ها، نیازسنجی تجهیزات، برنامه‌ریزی آزمایشگاه‌های مورد نیاز، تعریف پروژه‌های خرد و کلان در این مجموعه و زیرمجموعه‌های مورد نیاز، تعریف پروژه‌های پایانی دانشجویان دوره کاشناسی ارشد و دکترا و تربیت آن‌ها، پیگیری ایجاد قطب IoT
- گشترش فعالیت‌های پژوهشی مرتبط با اینترنت اشیا
- مدیریت و برنامه‌ریزی کلیه فعالیت‌های جمعی دانشکده مهندسی کامپیوتر در زمینه اینترنت اشیا
- اطلاع رسانی در زمینه تحقیقات و پروژه‌های انجام گرفته در زمینه اینترنت اشیا در دانشکده

آزمایشگاه اینترنت اشیا در این دانشگاه شامل چند دستگاه کامپیوتر بسیار قوی با کارت گرافیک ۱۰۸۰ و کلاستر متشکل از ۵ کامپیوتر می‌باشد. راه اندازی ۲ مرکز تخصصی آپا (آگاهی رسانی، پشتیبانی، امداد) امنیت اینترنت اشیا و آزمایشگاه تایید نمونه امنیتی تجهیزات در دانشگاه اصفهان در کنار هم بستری را را فراهم می‌کند تا در سال‌های آینده با گسترش فناوری اینترنت اشیا و کاربردهای آن در کشورمان، مانع از ایجاد بازار مخرب و تهدیدهای امنیتی شود.

به گفته معاون پژوهشی و فناوری دانشگاه اصفهان در پنجمین کنفرانس بین‌المللی "اینترنت اشیاء و کاربردها"؛ «اینکه هر شخصی که یک سیستم کامپیوتری داشته باشد و قادر به جستجو باشد، درک دقیقی از اینترنت اشیا دارد، سخن درستی نیست و باید بدانیم عصرIT ، عصر اندیشه‌های اطلاعاتی است و بدانیم که چگونه آینده انسان را تحت تاثیر قرار می‌دهد. باید به تحولات آینده به عنوان دغدغه نگاه شود و دلیل اینکه انسان دچار مشکلات بزرگ ناشی از توسعه یک طرفه شده است، ریشه یابی شود». همچنین رئیس دانشکده کامپیوتر دانشگاه اصفهان در این برنامه، مقاله محوری و دور افتادن از نیاز واقعی را یک آسیب دانست و اظهار کرد: «در توسعه فناوری فرصت‌هایی پیش می‌آید که میان‌بر ایجاد می‌کند. همیشه لازم نیست راه دیگر کشورها برویم. فراموش نکنیم دانش جهش ایجاد می‌کند. در بعد آموزشی در دانشکده کامپیوتر دانشگاه اصفهان، چندین سرفصل آموزشی در مقطع لیسانس در حوزه اینترنت اشیا در جهت مهارت افزایی و ارتقای قابلیت ورود به بازار کار تعریف شد، همچنین در بعد پژوهشی تلاش شده تا پژوهش‌ها را به پنج لایه کلی و هفت خوشه پژوهشی برای توسعه این شبکه تقسیم کنیم. نقش اینترنت اشیا در توسعه اقتصادی، صنعتی و جهش تولید بر کسی پوشیده نیست و اینترنت اشیا فرصتی برای آشتی دانشگاه و صنعت است.

فعالیت در حوزه اینترنت اشیا نباید به مباحث تئوری ختم شود؛ خوشبختانه مرکزی با هدف توسعه این شبکه در دانشگاه اصفهان ایجاد شده که فولاد مبارکه یکی از حامیان اصلی آن است». [۱]

مروری بر اینترنت اشیا

ویژگی‌های اساسی اینترنت اشیا

اینترنت اشیا یک فناوری امیدوار کننده است که هدف آن بهبود کیفیت زندگی مردم با تولید برنامه‌های جدید است که فعالیت‌های روزمره افراد را تسهیل می‌کند.

برای سیستم اینترنت اشیا، مجموعه ای از ویژگی‌های مشترک وجود دارد که شامل موارد زیر است:

• مقیاس بزرگ: شبکه وسیع از دستگاه‌ها باید کنترل شود تا دستگاه‌ها بتوانند با یکدیگر ارتباط برقرار کنند.

علاوه بر این، این شبکه در مقیاس بزرگ مقدار زیادی داده تولید می‌کند که یک مسئله مهم در مورد تفسیر و تجزیه و تحلیل داده‌ها ایجاد می‌کند.

• هوش: تلفیق الگوریتم‌های نرم افزار پیچیده و سخت افزار به دستگاه‌های اینترنت اشیا هوشمند می‌شود. این توانایی‌های هوش به دستگاه‌های اینترنت اشیا اجازه می‌دهد تا در موقعیت‌های مختلف تصمیم‌های هوشمندانه بگیرند و تعامل هوشمندانه‌ای با سایر دستگاه‌های ارتباطی برقرار کنند.

• حسگر: حسگرها قسمت اصلی سیستم اینترنت اشیا هستند که برای درک تغییرات در محیط اطراف و ایجاد داده‌هایی که وضعیت آن‌ها را نشان می‌دهد، استفاده می‌شوند. حسگرها با استفاده از فناوری‌های مختلف سنجش، کم توجهی به محیط اطراف می‌دهند و آگاهی انسان را در مورد دنیای فیزیکی افزایش می‌دهند [22].

• سیستم پیچیده: سیستم اینترنت اشیا متشکل از میلیاردها شی با قابلیت‌های مختلف سخت افزاری و نرم افزاری است که فرایند مدیریت را به ویژه با محدودیت‌های مرتبط با حافظه، انرژی و زمان، کاری بسیار دشوار می‌کند.

• محیط پویا: اینترنت اشیا توانایی اتصال تقریباً همه اشیای محیط ما را بدون نیاز به تعیین مرزهای شبکه اینترنت اشیا دارد که آن را به یک سیستم پویا در طبیعت تبدیل می‌کند. همچنین، دستگاه‌های اینترنت اشیا می‌توانند بر اساس تغییر شرایط تنظیم شوند.

• مقدار انبوه داده: دستگاه‌های اینترنت اشیا محیط اطراف خود را حس می‌کنند و مقدار زیادی داده تولید می‌کنند که آن را به یکی از منابع آنچه Big Data نامیده می‌شود، تبدیل می‌کنند.

• ناهمگنی: سیستم اینترنت اشیا شامل میلیاردها دستگاه با ویژگی‌های ناهمگن مانند سیستم عامل‌ها، پروتکل‌های ارتباطی و سایر موارد است. این ویژگی‌های ناهمگن، عملیات مدیریتی را به یک وظیفه پیچیده برای انجام تبدیل می‌کند.

• انرژی محدود: اکثر دستگاه‌های اینترنت اشیا کوچک و سبک با منابع محدود هستند، بنابراین برای کار با حداقل مصرف انرژی طراحی شده اند.

• اتصال: یکی از ویژگی‌های اصلی سیستم اینترنت اشیا توانایی اتصال دستگاه‌های مختلف با ویژگی‌های مختلف و استفاده از اطلاعات مشترک آن‌ها برای ایجاد برنامه‌ها و خدمات جدید است.

• پیکربندی خودکار: دستگاه‌ها برای انجام یک کار خاص پیکربندی شده اند. اما برای دستگاه‌های اینترنت اشیا، آن‌ها توانایی پیکربندی خود را دارند که آن‌ها را قادر می‌سازد بدون دخالت انسان کار کنند. دستگاه‌های اینترنت اشیا می‌توانند بدون مشارکت کاربر، خود را در نرم افزار به روز شده در ارتباط با سازنده دستگاه تنظیم کنند.

• هویت منحصر به فرد: در شبکه اینترنت اشیا، هر شی IoT با استفاده از یک شناسه منحصر به فرد مانند آدرس IP شناسایی می-شود. این هویت‌ها توسط IoT تولید شده است تا از آن برای ارتقای دستگاه‌ها به سیستم عامل‌های مناسب استفاده کند. علاوه بر این، این دستگاه‌ها دارای رابط‌هایی هستند که کاربران را قادر می‌سازد تا اطلاعات مورد نیاز دستگاه‌ها را جمع آوری کرده، وضعیت خود را ضبط کرده و از راه دور مدیریت کنند.

• آگاهی از متن: در محیط اینترنت اشیا، چندین سنسور وجود دارد که محیط اطراف خود را حس می‌کنند، اطلاعات مورد نیاز را جمع آوری و ذخیره می‌کنند، این سنسورها ممکن است براساس داده‌های جمع آوری شده تصمیم بگیرند که آن را به یک زمینه آگاه می‌کند.

معماری لایه ای اینترنت اشیا

کمیته معماری IoT World Forum (IWF) یک مدل مرجع اینترنت اشیا را در اکتبر ۲۰۱۴ منتشر کرد [23]. این مدل به عنوان یک چارچوب مشترک برای کمک به صنعت در سرعت بخشیدن به استقرار اینترنت اشیا کار می‌کند. این مدل مرجع برای تحکیم و تشویق همکاری و توسعه مدل‌های استقرار اینترنت اشیا در نظر گرفته شده است. این به عنوان هفت لایه طراحی شده است به طوری که هر لایه اطلاعات بیش‌تری را برای ایجاد اصطلاحات مشترک فراهم می‌کند، همچنین طبقه‌بندی می‌کند که انواع مختلف پردازش از طریق لایه‌های مختلف مدل مرجع اینترنت اشیا انجام می‌شود. علاوه بر این، این مدل تولیدکنندگان مختلف را قادر می‌سازد تا محصولات اینترنت اشیا را با یکدیگر سازگار کنند که اینترنت اشیا را از یک مدل مفهومی به یک سیستم واقعی و قابل دسترسی تبدیل می‌کند. لایه ۱ لایه فیزیکی است. این شامل دستگاه‌ها و کنترل کننده‌های فیزیکی است که اشیای مختلف را مدیریت می‌کنند. این اشیا مواردی را در اینترنت اشیا نشان می‌دهند که شامل انواع مختلفی از دستگاه‌ها است که اطلاعات را ارسال و دریافت می‌کنند، به عنوان مثال سنسورهایی که اطلاعات مربوط به محیط اطراف را جمع می‌کنند [24]. ارتباطات و اتصال در لایه ۲ است. این لایه برای اتصال چیزهای مختلف اینترنت اشیا با یکدیگر با استفاده از دستگاه‌های اتصال مانند سوئیچ‌ها، دروازه، روتر و فایروال‌ها استفاده می‌شود. لایه ۳ محاسبات لبه ای است. این لایه به روز از لایه اتصال وارد می‌شود و آن را به اطلاعات مناسب برای پردازش سطح بالاتر تبدیل می‌کند. در این لایه، مؤلفه‌های پردازش با حجم عظیمی از داده‌ها کار می‌کنند و ممکن است برای کاهش اندازه داده‌ها، برخی از داده‌های تغییر شکل را انجام دهد. لایه ۴ تجمع داده است. این لایه مربوط به ذخیره داده‌های حاصل از دستگاه‌های مختلف اینترنت اشیا است. این داده‌ها توسط لایه محاسبه لبه فیلتر شده و پردازش می‌شوند که مقادیر زیادی از داده‌ها را جذب کرده و در آن‌ها قرار می‌دهد. فضای ذخیره‌سازی در سطوح بالاتر قابل دسترسی است. انواع مختلف داده‌ها در فرمت‌های مختلف و پردازنده‌های ناهمگن ممکن است از لایه محاسبه لبه برای ذخیره‌سازی بیرون بیایند. لایه ۵ لایه انتزاع داده‌ها، داده‌ها را ذخیره می‌کند و قالب بندی می‌کند به گونه ای که دسترسی آن‌ها به برنامه‌ها با روشی قابل کنترل‌تر و کارآمدتر امکان پذیر می‌شود. لایه ۶ لایه کاربرد است. این لایه مربوط به تفسیر اطلاعات برنامه‌های مختلف اینترنت اشیا است. این لایه برنامه‌های مختلفی را شامل می‌شود که از داده‌های ورودی اینترنت اشیا استفاده می‌کنند یا دستگاه‌های اینترنت اشیا را کنترل

می‌کنند [23]. همکاری و فرآیندها در لایه ۷ است. این لایه افرادی را شناسایی می‌کند که می‌توانند برای مفیدتر کردن سیستم اینترنت اشیا با یکدیگر ارتباط برقرار کرده و همکاری کنند. همچنین شامل برنامه‌های مختلف برای تبادل داده و کنترل اطلاعات از طریق اینترنت است.

پروتکل‌ها و استانداردهای اینترنت اشیا

پروتکل‌ها و استانداردهای اینترنت اشیا به طور کلی در دو دسته جداگانه طبقه‌بندی می‌شوند: پروتکل‌های داده اینترنت اشیا (لایه-های ارائه / برنامه)، پروتکل‌های شبکه برای اینترنت اشیا (لینک داده / لایه‌های فیزیکی).

پروتکل‌های داده IoT از پروتکل‌های داده اینترنت اشیا برای اتصال دستگاه‌های کم مصرف اینترنت اشیا استفاده می‌شود. آن‌ها ارتباطات را با سخت افزار در سمت کاربر بدون نیاز به اتصال به اینترنت فراهم می‌کنند.

اتصال در پروتکل‌ها و استانداردهای داده اینترنت اشیا از طریق یک شبکه سیمی یا تلفن همراه است. چند نمونه از پروتکل‌های داده اینترنت اشیا عبارتند از:

- **MQTT (Message Queue Telemetry Transport)**

MQTT (پیام از راه دور تله متری حمل و نقل) یک پروتکل داده سبک اینترنت اشیا است. این مدل از مدل پیام ناشر و مشترک برخوردار است و جریان ساده داده را بین دستگاه‌های مختلف امکان پذیر می‌کند. اصلی‌ترین نقطه فروش MQTT معماری آن است. آرایش ژنتیکی آن سبک است و بنابراین می‌تواند انرژی کم‌تری را برای دستگاه‌ها فراهم کند. همچنین در بالای پروتکل TCP / IP کار می‌کند. پروتکل‌های داده اینترنت اشیا برای مقابله با شبکه‌های ارتباطی غیر قابل اطمینان طراحی شده اند. این امر به دلیل افزایش تعداد اجسام کوچک، ارزان و کم مصرف که طی چند سال گذشته در شبکه ظاهر شده اند، در دنیای اینترنت اشیا به یک نیاز تبدیل شد. با وجود انطباق گسترده MQTT - به ویژه به عنوان استاندارد IoT با کاربردهای صنعتی - از نمایش داده تعریف شده و حالت ساختار مدیریت دستگاه پشتیبانی نمی‌کند. در نتیجه، اجرای قابلیت‌های مدیریت داده و دستگاه کاملاً مختص پلتفرم یا فروشنده است. مسئله اصلی امنیتی: سرورهای MQTT در معرض اینترنت، اشتراک مخرب شخص ثالث در پیام‌های MQTT.

- **CoAP**

پروتکل کاربرد محدود است. این برنامه برای رفع نیازهای سیستم‌های اینترنت اشیای مبتنی بر HTTP طراحی شده است. HTTP مخفف Hypertext Transfer Protocol است، و پایه ارتباطات داده برای شبکه جهانی وب است. در حالی که ساختار موجود اینترنت به راحتی توسط هر دستگاه اینترنت اشیا در دسترس و قابل استفاده است، اما برای اکثر برنامه‌های اینترنت اشیا اغلب بسیار سنگین و انرژی بر است. این امر منجر به این شده است که بسیاری از افراد در اینترنت اشیا، HTTP را به عنوان پروتکلی که برای اینترنت اشیا مناسب نیست رد کنند. با این حال، CoAP با ترجمه مدل HTTP به استفاده در دستگاه‌های محدودکننده و محیط شبکه، این محدودیت را برطرف کرده است. سربار فوق العاده کمی دارد، استفاده از آن آسان است و توانایی پشتیبانی از چندپخشی را دارد. بنابراین، برای استفاده در دستگاه‌هایی با محدودیت منابع، مانند میکروکنترلرهای IoT یا گره‌های WSN، ایده آل است. به طور سنتی در برنامه‌هایی شامل انرژی هوشمند و اتوماسیون ساختمان استفاده می‌شود. مسئله اصلی امنیتی: حمله DDoS شامل یک بازیگر شخص ثالث است که به طور همزمان بسته‌های جعلی IP را برای هدف قرار دادن آدرس‌های IP در طی اصلاح و تقویت CoAP ارسال می‌کند.

- **AMQP (Advanced Message Queuing Protocol)**

پروتکل صف پیشرفته پیام (AMQP) یک پروتکل لایه نرم افزار استاندارد باز است که برای پیام‌های معاملاتی بین سرورها استفاده می‌شود. توابع اصلی این پروتکل اینترنت اشیا به شرح زیر است: دریافت و قرار دادن پیام در صف، ذخیره پیام‌ها، ایجاد رابطه بین این مؤلفه‌ها.

با سطح امنیت و قابلیت اطمینان، معمولاً در تنظیماتی استفاده می‌شود که به محیط‌های تحلیلی مبتنی بر سرور، مانند صنعت بانکی نیاز دارند. با این حال، در جاهای دیگر به طور گسترده ای استفاده نمی‌شود. به دلیل سنگینی آن، برای دستگاه‌های حسگر اینترنت اشیا با حافظه محدود مناسب نیست. در نتیجه، استفاده از آن هنوز در دنیای اینترنت اشیا کاملاً محدود است.

- **DDS (Data Distribution Service)**

DDS(سرویس توزیع داده) یکی دیگر از پروتکل‌های مقیاس پذیر اینترنت اشیا است که امکان برقراری ارتباط با کیفیت بالا در اینترنت اشیا را فراهم می‌کند. مشابه MQTT، DDS در مدل ناشر - مشترک نیز کار می‌کند. می‌توان آن را در چندین تنظیم، از ابر گرفته تا دستگاه‌های بسیار کوچک، مستقر کرد. این امر آن را برای سیستم‌های بلادرنگ و جاسازی شده عالی می‌کند. علاوه بر این، بر خلاف MQTT، پروتکل DDS امکان تبادل داده‌های قابل همکاری را دارد که مستقل از سخت افزار و بستر نرم افزاری نیست. در واقع ، این اولین استاندارد بین المللی IoT میان افزار باز است. مسئله اصلی امنیتی: با توجه به ویژگی قابلیت توسعه، ضعف در اجرا و مدیریت دستگاه‌ها می‌تواند منجر به حملات DDoS یا حملات میانه شود.

- **HTTP (HyperText Transfer Protocol)**

پروتکل HTTP (پروتکل انتقال متن فوق متن) به دلیل هزینه، عمر باتری، مصرف زیاد انرژی و مشکلات وزن به عنوان استاندارد IoT ترجیح داده نمی‌شود. البته هنوز در بعضی از صنایع استفاده می‌شود. به عنوان مثال، تولید و چاپ ۳ بعدی به دلیل مقادیر زیادی از داده‌هایی که می‌تواند منتشر کند، به پروتکل HTTP متکی هستند. اتصال رایانه به چاپگرهای ۳ بعدی در شبکه و چاپ اشیای سه بعدی را امکان پذیر می‌کند.

- **WebSocket**

وب سوکت در ابتدا به عنوان بخشی از ابتکار HTML5 در سال ۲۰۱۱ توسعه داده شد. از طریق یک اتصال TCP ، پیام‌ها می‌توانند بین سرویس گیرنده و سرور ارسال شوند. مانند CoAp، پروتکل اتصال استاندارد WebSocket به ساده‌سازی بسیاری از پیچیدگی‌ها و مشکلات مربوط به مدیریت اتصالات و ارتباطات دو جهته در اینترنت کمک می‌کند. این می‌تواند به یک شبکه اینترنت اشیا اعمال شود که در آن ارتباط داده‌ها به طور مداوم از طریق چندین دستگاه برقرار می‌شود. بنابراین معمولاً در مکان‌هایی که به عنوان مشتری یا سرور عمل می‌کنند، مورد استفاده قرار می‌گیرد.

Network Protocols for IoT

پروتکل‌های شبکه اینترنت اشیا برای اتصال دستگاه‌ها از طریق شبکه استفاده می‌شود. این مجموعه از پروتکل‌ها معمولاً در اینترنت استفاده می‌شوند که عبارتند از:

- **WiFi**

نمی‌توان انکار کرد که Wi-Fi شناخته‌شده ترین پروتکل اینترنت اشیا در این لیست است. برای ایجاد شبکه Wi-Fi، به دستگاهی نیاز دارید که بتواند سیگنال‌های بی سیم ارسال کند. این شامل: تلفن، کامپیوترها، روترها. Wi-Fi در محدوده خاصی اتصال به اینترنت با دستگاه‌های اطراف را فراهم می‌کند. روش دیگر استفاده از Wi-Fi ایجاد نقطه اتصال Wi-Fi است. تلفن‌های همراه یا رایانه‌ها ممکن است با پخش یک سیگنال، یک اتصال اینترنتی بی سیم یا سیمی را با دستگاه‌های دیگر به اشتراک بگذارند.

Wi-Fi از امواج رادیویی استفاده می‌کند که اطلاعات را روی فرکانس‌های خاص مانند کانال‌های ۴.۲ گیگاهرتز یا ۵ گیگاهرتز پخش می‌کنند. بعلاوه، هر دو این محدوده فرکانس دارای تعدادی کانال است که از طریق آن‌ها دستگاه‌های بی سیم مختلف می‌توانند کار کنند. این از سرریز شدن شبکه‌های بی سیم جلوگیری می‌کند.

برد ۱۰۰ متری معمول اتصال Wi-Fi است. متداول ترین آن‌ها به ۳۵-۱۰ متر محدود می‌شود. تأثیرات اصلی بر دامنه و سرعت اتصال Wi-Fi محیط و اینکه آیا پوشش داخلی یا خارجی را فراهم می‌کند.

- **Bluetooth**

وقتی با سایر پروتکل‌های شبکه اینترنت اشیا ذکر شده در اینجا مقایسه می‌شود، بلوتوث تمایل به فرکانس هاپ دارد و دامنه آن معمولاً کوتاه تر است. با این وجود، به دلیل ادغام در دستگاه‌های تلفن همراه مدرن – تلفن‌های هوشمند و تبلت‌ها، و همچنین فناوری پوشیدنی، مانند هدفون‌های بی سیم، یک پایگاه کاربر عظیم پیدا کرده است. فناوری استاندارد بلوتوث از امواج رادیویی در باند فرکانس ۲,۴ گیگاهرتز ISM استفاده می‌کند و به صورت بسته به یکی از ۷۹ کانال ارسال می‌شود. با این حال، آخرین استاندارد بلوتوث ۴,۰ دارای ۴۰ کانال و پهنای باند ۲ مگاهرتز است. این حداکثر انتقال داده تا ۳ Mb / s را تضمین می‌کند. این فناوری جدید در غیر این صورت با عنوان Bluetooth Low Energy (BLE) شناخته می‌شود و می‌تواند پایه و اساس برنامه‌های اینترنت اشیا باشد که به انعطاف پذیری قابل توجه، مقیاس پذیری و مصرف کم انرژی نیاز دارند. مسئله اصلی امنیتی BLE: در هنگام انتقال و دریافت داده‌ها برای رهگیری و حملات باز است.

- **ZigBee**

شبکه‌های مبتنی بر ZigBee از این نظر شبیه شبکه بلوتوث هستند که از قبل دارای پایگاه کاربری قابل توجهی در دنیای اینترنت اشیا است. با این حال، مشخصات آن بلوتوث جهانی را که بیشتر مورد استفاده قرار گرفته است، کمی محو می‌کند. مصرف برق آن کمتر است، دامنه داده کم، امنیت بالایی دارد و دامنه ارتباطی آن بیشتر است (ZigBee می‌تواند به ۲۰۰ متر برسد، در حالی که بلوتوث حداکثر ۱۰۰ متر است). این یک پروتکل تبادل داده بسته ای نسبتاً ساده است و اغلب در دستگاه‌هایی با نیازهای کوچک مانند میکروکنترلرها و سنسورها اجرا می‌شود. بعلاوه، به راحتی در هزاران گره مقیاس بندی می‌شود. این تعجب آور نیست که بسیاری از تامین کنندگان دستگاه‌هایی را ارائه می‌دهند که از مدل توپولوژی شبکه خود باز مونتاژ استاندارد و خود ترمیم ZigBee پشتیبانی می‌کنند. این یک پروتکل تبادل داده بسته ای نسبتاً ساده است و اغلب در دستگاه‌هایی با نیازهای کوچک مانند میکروکنترلرها و سنسورها اجرا می‌شود. بعلاوه، به راحتی در هزاران گره مقیاس بندی می‌شود. این تعجب آور نیست که بسیاری از تأمین کنندگان دستگاه‌هایی را ارائه می‌دهند که از مدل توپولوژی شبکه خود باز مونتاژ استاندارد و خود ترمیم ZigBee پشتیبانی می‌کنند. مسئله اصلی امنیتی: حملات مبتنی بر گره مخرب، توزیع انکار سرویس (DDoS)

- **Z-Wave**

Z-Wave یک پروتکل اینترنت اشیا است که به طور فزاینده ای محبوب است. این یک فناوری ارتباطی بی سیم، فرکانس رادیویی (RF) است که در درجه اول برای برنامه‌های خانگی اینترنت اشیا استفاده می‌شود. با فرکانس رادیویی ۹۰۰ MHz-۸۰۰ کار می‌کند. از طرف دیگر، Zigbee با فرکانس ۲,۴ گیگاهرتز کار می‌کند، که همچنین فرکانس اصلی WiFi است. Z-Wave با کار در محدوده خود به ندرت از مشکلات تداخل قابل توجهی رنج می‌برد. با این حال، فرکانسی که دستگاه‌های Z-Wave بر روی آن کار می‌کنند به مکان بستگی دارد، بنابراین باید مطمئن شد که یک مورد مناسب برای کشور خود خریداری کرده ایم. Z-Wave یک پروتکل قابل توجه IoT است. با این حال، مانند ZigBee ، بهتر است در خانه استفاده شود و نه در دنیای تجارت.

- **LoRaWAN**

LoRaWAN یک پروتکل IoT کنترل دسترسی رسانه (MAC) است. LoRaWAN به دستگاه‌های کم قدرت اجازه می‌دهد تا مستقیماً با برنامه‌های متصل به اینترنت از طریق اتصال بی سیم دوربرد ارتباط برقرار کنند. علاوه بر این، این قابلیت را دارد که به هر دو لایه ۲ و ۳ مدل OSI ترسیم شود. این در بالای مدولاسیون LoRa یا FSK برای باندهای رادیویی صنعتی، علمی و پزشکی (ISM) پیاده‌سازی شده است.

- **The Bottom Line**

انتخاب پروتکل‌ها و استانداردهای IoT مناسب برای پروژه‌های شما امری حیاتی است. با یک گزینه اشتباه، کل مجموعه فناوری سقوط می‌کند. بنابراین، شما باید برنامه مناسب خود را برای کاربرد اینترنت اشیا انتخاب کنید.

- **Near Field Communication (NFC)**

یک برنامه اصلی معامله پرداخت بدون تماس است. اطمینان حاصل کنید که ارتباط دو طرفه ارتباط ایمن است. تلفن‌های هوشمند گره‌های انتهایی هستند. بین دستگاه‌های الکترونیکی، استفاده از مطالب دیجیتالی. مسئله اصلی امنیتی: حمله مبتنی بر گره مخرب.

- **EnOcean**

شبکه حسگر بی سیم خود-کاربر مبتنی بر کاربر که داده‌ها را در سیستم‌های هوشمند پردازش و جمع می‌کند. جریان بیکار کمتر و در نتیجه مصرف انرژی کمتر، نزدیک یا کمتر از ۱۰۰ نانو آمپر جریان (nA) است. مسئله اصلی امنیتی: داشتن پروتکل اینترنت اشیا توسط کاربر یا خود-تهیه‌شده، مسدود کردن اختیاری، کلیدهای امنیتی از قبل مشترک، همگام‌سازی مجدد و غیرقابل استفاده Rolling Codes اغلب فراموش یا نادیده گرفته می‌شوند.

- **SigFOX**

پشتیبانی از شبکه گره متراکم با توپولوژی شبکه ستاره. دارای دسترسی ابری و کنترل دسترسی محدود به نقطه نهایی است. با مصرف کم انرژی نزدیک به ۵۰ میکروووات، بهترین کیفیت را از هر دو شبکه Cellular و Wifi به ارمغان می‌آورد. مسئله اصلی امنیتی: رمزگذاری ضعیف بار IoT .

طبقه‌بندی حملات در اینترنت اشیا

شناخت تهدیدات احتمالی در معماری بر اساس رفتار و مجموعه اهداف برای تدوین راه حل‌های امنیتی بسیار مهم است. بسیاری از شرکت‌های تجاری مقدار زیادی دارایی را برای تأمین امنیت شبکه مبتنی بر اینترنت اشیای خود در توسعه اخیر سرمایه‌گذاری کرده‌اند. حملات به اینترنت اشیا به دو ماژول تقسیم می‌شوند:

(۱) حملات مبتنی بر پروتکل - این نوع حملات از ساختار مبتنی بر پروتکل داخلی اجزای اینترنت اشیا استفاده می‌کنند که بر رسانه ارتباطی و کانال‌های ارسال سیستم تعبیه شده تأثیر می‌گذارند. این‌ها بیش‌تر در سایر بخش‌ها طبقه‌بندی می‌شوند. مبتنی بر پروتکل دارای دو مورد است:

(الف) حملات مبتنی بر پروتکل ارتباطی - این توضیح دهنده اشکال بهره‌برداری است که در طی مراحل گذرا در میان گره‌ها رخ می‌دهد. این موارد شامل حملات Flooding، حملات کلیدی Pre-Shred و حمله snifng است.

ب) حملات مبتنی بر پروتکل شبکه - این موضوع بهره‌برداری در ایجاد اتصال را توضیح می‌دهد. حملات شامل حملات Wormhole، حملات Selective Forward و حملات Snifng است.

(۲) حملات مبتنی بر داده - حملات مبتنی بر داده شامل تهدیدهایی مربوط به بسته‌های داده اصلی و پیام‌هایی است که در سایت‌های گره ای سفر می‌کنند. Hash collision، DoS، ایجاد Malicious Node VM و افشای اطلاعات از مهم‌ترین سوء استفاده‌های امنیتی آن است.

خلاصه تهدیدات و حملات عمومی احتمالی برای اینترنت اشیا

۱_ تهدید مداوم پیشرفته (APT)

یک دشمن یک سیستم اطلاعاتی را هدف قرار می‌دهد که به طور مداوم اقدام به هک می‌کند

عواقب: کنترل کامل سیستم هک شده و دارایی‌های آن

۲_ سرقت هویت داده‌ها

یک تلاش هک با اعتبار واقعی کاربر به عنوان حمله جعل هویت آغاز شده است

عواقب: نشت حریم خصوصی

۳_ انکار سرویس توزیع شده (DDoS)

حمله کردن

حمله DoS به طور همزمان از چندین مکان آغاز شد

عواقب: قطع خدمات به دلیل اضافه بار

۴_ حمله Botnet

شبکه ربات‌هایی که برای به خطر انداختن اهداف منفرد یا چندگانه اقدام می‌کنند

عواقب: حمله DDoS

۵_ Ransomware (باج افزار)

یک بدافزار که یک بار روی سیستم نصب شده از مالک باج (به طور معمول مالی) می‌خواهد

عواقب: دسترسی به بخشی یا کل سیستم را ممنوع کرده یا تهدید به انتشار اطلاعات حساس تا زمان تسویه حساب باج می‌کند

۶_ Man-in-the-middle (MitM)

تلاش برای دسترسی به اطلاعات پیمایشی یک پیوند ارتباطی بین فرستنده و گیرنده

عواقب: افشای اطلاعات و پروتکل، تزریق محتوای نادرست / مخرب

۷_ حمله کانال جانبی (SCA)

ویژگی فیزیکی دستگاه را از طریق دستکاری تجزیه و تحلیل می‌کند

عواقب: اطلاعات، کلیدها یا حتی یک پروتکل می‌تواند آشکار شود

خلاصه ای از روش‌های جلوگیری از خطرات امنیتی برای اینترنت اشیا

Honeypots

مکانیزمی که دشمنانی را که قصد انجام کارهای غیرمجاز را دارند به دام بیندازد

مزایا: شناسایی و مقابله با تهدیدها بدون تأثیر بر سیستم اطلاعاتی

افزایش آگاهی از طریق آموزش

معرفی برنامه‌های آموزش حرفه ای برای کاربران و توسعه دهندگان اینترنت اشیا

مزایا: در حالی که آگاهی مردم برای غلبه بر حملات امنیتی عمومی مانند حملات فیشینگ افزایش می‌یابد، کاربران روش‌های ایمن را دنبال خواهند کرد.

پاسخ فوری به آسیب پذیری‌های شناسایی شده

تولید سریع به روزرسانی‌ها و وصله‌های اصلاح شده برای fows شناسایی شده، به ویژه در نرم افزارهای منبع باز

مزایا: جلوگیری از بهره‌برداری از آسیب‌پذیری‌های انتشار یافته در موارد منبع باز

امنیت روی تراشه

یکپارچه‌سازی امنیت برای تراشه‌های IoT / سخت افزار در مرحله تولید

مزایا: یک لایه امنیتی اضافی، که به دلیل پیاده‌سازی در حوزه درک، پاسخ سریع تری را به شما می‌افزاید

تست امنیت جامع

برای پوشش جنبه‌های نفوذی، دسترسی، فیزیکی، محاسباتی، باید طرح‌های آزمایش بهتر ارائه شود

مزایا: حداکثر اطمینان قبل از عرضه دستگاه اینترنت اشیا به بازار اعطا می‌شود

امنیت در SDLC

اقدامات امنیتی باید در مراحل طراحی نرم افزار در SDLC ادغام شود

مزایا: امنیت به عنوان هدف اصلی تمام محصولات نرم افزاری با سازگاری و قابلیت کارایی بهتر مورد توجه قرار می‌گیرد

GDPR

قانونی که توسط اتحادیه اروپا برای حفاظت از داده‌ها ارائه شده است

مزایا: ارتقای سطح آگاهی عموم مردم و در دسترس بودن یک چارچوب قانونی برای پاسخگویی در موارد نقض دیجیتال و حریم خصوصی

چالش‌های امنیتی اینترنت اشیا

محدودیت منابع: اکثر دستگاه‌های اینترنت اشیا به دلیل ویژگی‌هایشان که باعث می‌شود با انرژی کمتری کار کنند، قابلیت پردازش و ذخیره‌سازی محدودی دارند. بنابراین، الگوریتم‌های پیچیده امنیتی برای این دستگاه‌های محدود مناسب نیستند زیرا آن‌ها قادر به انجام عملیات پردازش پیچیده در زمان واقعی نیستند. در عوض، این دستگاه‌ها معمولاً فقط از الگوریتم‌های رمزنگاری سریع و سبک استفاده می‌کنند [25].

سیاست به روزرسانی شبکه پراکنده: دستگاه‌های اینترنت اشیا در سراسر جهان، چه در یک سازمان چه در فضای کاری شخصی، از طریق سرورهای توزیع شده مدیریت می‌شوند و سیاست امنیتی نیز برای هر دستگاه در سیستم متفاوت است. بنابراین، به طور منظم، همه دستگاه‌ها باید به روز شوند، که یک کار خسته کننده و پیچیده برای سازمان است و مداخله از طرف ثالث برای پشتیبانی در موضوع مورد بحث می‌تواند کنترل دسترسی سیستم را به خطر بیندازد.

خط مشی امنیتی افزونه‌ها: اینترنت اشیا برای تهیه ویژگی‌های امنیتی هرگز مدل‌سازی نشده اند. افزونه‌ها و کنترل‌های امنیتی اضافی برای ارائه راه حل‌های ایمن بر روی معماری لایه ای IoT ضمیمه می‌شوند. بنابراین، برخلاف الگوی شبکه متداول، کارایی ویژگی‌های امنیتی به قابلیت عملکرد منابع اضافی در معماری اینترنت اشیا بستگی دارد. اقدامات مشتری مانند نحوه انتخاب برخی از گزینه‌های امنیتی موجود نیز بر اثربخشی امنیت IoT تأثیر می‌گذارد.

تهدیدهای IoT فیزیکی: تهدیدهای امنیتی فیزیکی در تنظیمات IoT فیزیکی در واحدهای صنعتی، سیستم‌های بهداشتی و درمانی یکپارچه و دامنه‌های سازمانی شبکه واقعی هستند. دو تهدید اصلی عبارتند از: کانال‌های ارتباطی و کارمندان حسابرسی داده‌ها [26].

Data Audit با چالش‌های امنیتی خاص، نقاط ضعف امنیتی حاکم در طی انتقال اطلاعات از طریق شبکه و لایه جمع کننده معماری IoT را نشان می‌دهد.

سایر چالش‌های امنیت فیزیکی شامل تخریب دستی یا طبیعی اجزای پیچیده شبکه است. در سیستم‌های صنعتی، تهدیدهای فیزیکی در عملکرد نادرست تجهیزات اینترنت اشیا مانند رباتیک، سنسورها و دستگاه‌های سخت افزاری است که ممکن است بر اشخاص فیزیکی تأثیر منفی بگذارد [27].

دستگاه‌های نهایی در اینترنت اشیا، مانند سنسورها و دوربین‌های IP که در محیط‌های باز نصب می‌شوند، نقاط تهدیدی هستند که دسترسی به آن‌ها برای دشمن دشوار نیست. چالش‌های امنیتی مربوط به این مسئله در این است که چگونه می‌توان در پروتکل یا سازوکار ارتباطی، اصلاح معماری را ایجاد کرد تا چنین دستگاه‌هایی را در برابر دشمنان ایمن سازد.

کلان داده: سیستم اینترنت اشیا شامل میلیاردها دستگاه است که مقدار زیادی داده تولید می‌کنند. این داده‌ها از نظر ساختار متغیر هستند و غالباً در زمان واقعی هستند. حجم، سرعت و تنوع این داده‌ها، فرایند ذخیره‌سازی و تجزیه و تحلیل را که برای تولید اطلاعات معنی دار استفاده می‌شود، کار بسیار پیچیده ای می‌کند. اینترنت اشیا یکی از منابع اصلی داده‌های کلان است. استفاده از رایانش ابری می‌تواند ذخیره این مقدار عظیم داده را برای مدت زمان طولانی تسهیل کند. با این حال، مدیریت این داده‌های عظیم یک چالش اساسی است. علاوه بر این، یکی از جنبه‌های اساسی داده‌های کلان، یکپارچگی داده‌ها است. اطمینان از امنیت این حجم عظیم از داده‌ها با افزایش گسترده منابع داده‌ها به روشی که نیاز به اتخاذ تدابیر امنیتی بیشتری است، دشوار می-شود [28].

مجوز و کنترل دسترسی: ارائه یک مجوز و کنترل دسترسی کارآمد برای سیستم اینترنت اشیا یکی از اصول اساسی تهیه سیستم ایمن است. با این حال، مشکلات زیادی در رابطه با احراز هویت دستگاه وجود دارد مانند استفاده از رمزهای عبور ضعیف یا رمز عبور پیش فرض که منجر به دسترسی به مهاجمانی می‌شود که می‌توانند داده‌های دستگاه را دستکاری کنند یا حتی به آن‌ها آسیب جسمی وارد کنند. اتخاذ امنیت با طراحی در دستگاه‌های اینترنت اشیا، امکان احراز هویت دو عاملی و اعمال استفاده از رمزهای عبور قوی می‌تواند به رفع این چالش‌ها کمک کند [29].

ارتباط امن: ایمن‌سازی دستگاه‌های اینترنت اشیا برای اطمینان از دستیابی کامل به امنیت در سیستم اینترنت اشیا کافی نیست. بنابراین کانال ارتباطی متصل کننده گره‌های ارتباطی مختلف مانند دستگاه‌های اینترنت اشیا و سرویس‌های ابری باید از هرگونه حمله محافظت شود. اکثر دستگاه‌های اینترنت اشیا داده‌ها را در قالب متن ساده و بدون رمزگذاری ارسال می‌کنند که آن را به راحتی به انواع مختلف حملات شبکه تبدیل می‌کند. از این رو، باید از یک روش رمزگذاری مناسب استفاده شود. همچنین، استفاده از شبکه‌های جداگانه می‌تواند امنیت را از طریق جداسازی دستگاه‌ها و ایجاد کانال‌های ارتباطی خصوصی افزایش دهد.

انعطاف پذیری سیستم: تاب آوری یکی از اصلی ترین چالش‌هایی است که باید در سیستم اینترنت اشیا مورد توجه قرار گیرد. انعطاف پذیری سیستم به توانایی سیستم در پاسخگویی به حملات / موقعیت‌های پیش بینی نشده بدون پس زدن اشاره دارد. از این رو، اگر برخی از دستگاه‌های اینترنت اشیا هک شوند، سیستم باید بتواند از دیگر گره‌های شبکه در برابر هرگونه حمله محافظت کند.

سیستم پیچیده: سیستم اینترنت اشیا شامل میلیاردها دستگاه ناهمگن است که مدیریت این شبکه در مقیاس بزرگ را به ویژه با محدودیت‌های مرتبط با حافظه، انرژی و زمان، کاری بسیار دشوار می‌کند. هرچه دستگاه‌ها، افراد، تعاملات و رابط‌ها بیشتر باشند، خطر نقض امنیت بیشتر است.

بزرگ‌ترین تهدیدها و چالش‌ها چیست؟ از سرورهای سازمانی گرفته تا ذخیره‌سازی ابری، مجرمان اینترنتی می‌توانند راهی برای بهره‌برداری از اطلاعات در بسیاری از نقاط یک اکوسیستم اینترنت اشیا پیدا کنند. شرکت‌ها باید دستگاه‌های شناخته‌شده و ناشناخته را رصد کنند. مهم است که سازمان‌ها توانایی جلوگیری از وسایل متقلب را در اوایل زنجیره داشته باشند تا از دسترسی یا سرقت هرگونه اطلاعات جلوگیری کنند. صفحات ورود جعلی یکی از متداول ترین روش‌های سرقت اطلاعات است. در غیر این صورت هکرها به نام "دوقلوهای شیطانی(evil twins)" شناخته می‌شوند، هکرها می‌توانند شبکه‌های Wi-Fi جدیدی را ایجاد کنند که شبیه دامنه‌های عمومی است تا کارمندان را فریب دهند تا اطلاعات حساس را به وب سایت‌ها و سیستم عامل‌ها وارد کنند و داده‌های شرکت را به خطر بیندازند. کارکنان باید مراقب باشند تا از تبدیل شدن ابزار شنود دستگاه‌هایشان جلوگیری کنند. با افزایش سیاست‌های BYOD، این مسئله فقط به مسئله بزرگتری تبدیل شده است زیرا کارمندان دستگاه‌های شخصی محافظت نشده بیشتری را به محل کار خود وارد می‌کنند. رمزگذاری ابزاری قدرتمند برای امنیت داده است اما چالش‌ها و وابستگی‌های خاص خود را نیز به همراه دارد. بسیاری از دستگاه‌ها توانایی پردازش یا ذخیره‌سازی مورد نیاز برای رمزگذاری قوی را ندارند.

چه صنایعی بیشتر تحت تأثیر تهدیدهای امنیتی اینترنت اشیا قرار دارند؟

دولت: امکانات آژانس‌های دولتی نیاز به محافظت از اطلاعات بسیار حساس دارند. سازمان‌های امنیتی و فدرال دولت فوری برای اطمینان از رعایت دستورالعمل‌ها و مناطق امن با مکالمات، مطالب و فعالیت‌های کاملاً محرمانه و طبقه‌بندی شده، به Inpixon Aware اعتماد دارند. **شرکت‌های بزرگ، دارای شخصیت حقوقی:** بیشتر سازمان‌های سازمانی اسرار تجاری دارند که محدود به انتخاب کارمندان است. یک خطر بزرگ برای مشاغل وجود دستگاه‌های شنود در اتاق‌های هیئت مدیره یا داشتن دستگاه‌های ناشناخته‌ای است که توسط کارمندان بی خبر مورد استفاده قرار می‌گیرد و به هکرها اجازه می‌دهد به منابع شرکت دسترسی پیدا کنند. **مراقبت‌های بهداشتی:** نقض داده‌های بیمار تهدیدی برای سازمان‌های مراقبت‌های بهداشتی است، زیرا داده‌های بیمار به طور معمول بسیار حساس هستند و باید به شدت محافظت شوند.

هنگام ارزیابی راه حل‌های امنیتی اینترنت اشیا چه مواردی را باید در نظر گرفت؟ باید دستگاه، ابر و کانال بین دستگاه‌ها و ابر را ایمن کنند. با اجرای سیاست‌های مدیریت دستگاه تلفن همراه (MDM) ، تیم‌های امنیتی می‌توانند نظارت کنند که کدام دستگاه‌ها غیر مجازند. اهرم راه حل امنیتی داخلی Inpixon برای پرورش آگاهی از موقعیت در داخل ساختمان با شناسایی دستگاه‌های بی سیم و حرکات آن‌ها. Inpixon Aware به سازمان‌ها امکان مشاهده در امکانات خود و یک راه حل قوی برای شناسایی بی سیم را

در یک داشبورد امنیتی زنده و مستقیم می‌دهد که با دیگر سیستم‌های امنیتی بی سیم شما ادغام می‌شود. و اجازه می‌دهد تا سازمان‌ها تصمیمات اساسی پیرامون امنیت، ایمنی عمومی و کاهش خطرات را در مقیاس وسیع اتخاذ کنند.

امنیت توسط طراحی IoT

امنیت از طریق طراحی یک رویکرد جدید است که توسط چندین سازمان برای پیاده‌سازی اقدامات امنیتی مورد نیاز در چرخه عمر نرم افزار و سخت افزار و نه پس از تشخیص نقض امنیت پیشنهاد شده است. از آنجایی که این دستگاه‌ها به اینترنت متصل هستند، به نقطه ضعفی تبدیل می‌شوند که می‌تواند توسط هر مهاجم امنیتی مورد استفاده قرار گیرد تا اطلاعات حساس را بدزدد یا سرویس را مختل کند. همچنین، اکثر این دستگاه‌ها بدون امنیت داخلی در سیستم خود ساخته شده اند و این اهداف آسان برای حمله‌کنندگان امنیتی است [30]. استراتژی آن‌ها شامل تشویق شرکت‌ها و توسعه دهندگان برای ایجاد ویژگی‌های ایمنی در محصولات خود از ابتدا، برای اطمینان از ایمنی دستگاه‌های متصل در مرحله طراحی و در طول چرخه عمر محصولات مختلف است.

بهترین روش‌ها برای ایمن‌سازی دستگاه‌های اینترنت اشیا

نگرانی‌های امنیتی مرتبط با دستگاه‌های اینترنت اشیا خطرات بالقوه ای را در زندگی ما ایجاد می‌کند. قبل از اینترنت اشیا، نقض امنیت می‌تواند منجر به از دست دادن پول شما شود، اما با اینترنت اشیا، حمله امنیتی به معنای واقعی کلمه منجر به از دست دادن زندگی شما می‌شود. ایمن‌سازی دستگاه‌های اینترنت اشیا مستلزم استفاده از بهترین روش‌ها است که شامل موارد زیر است:

• مقاوم در برابر دستکاری سخت افزار: منزوی نگه داشتن دستگاه‌های اینترنت اشیا و تنها افراد خاص که به آن دسترسی فیزیکی دارند. همچنین، سخت شدن دستگاه اینترنت اشیا با امنیت فیزیکی مانند مسدود کردن پورت‌های استفاده نشده و پوشش دوربین نقاط خوبی برای جلوگیری از دستیابی مهاجمین بالقوه به داده‌های شما است [31].

• احراز هویت قوی: بسیاری از کاربران اینترنت اشیا هنوز از رمزهای عبور ضعیف و پیش فرض و بدون هیچ گونه بروزرسانی استفاده می‌کنند. تولیدکنندگان باید از مشتری بخواهند قبل از استفاده از دستگاه، رمزعبور پیش فرض را با گذرواژه‌های قوی به روز کند.

علاوه بر این، روش‌های جایگزینی برای شناسایی هویت و اعتماد دستگاه‌ها مورد نیاز است زیرا نام کاربری و رمز ورود برای هر دستگاه واقع بینانه نیست، به ویژه برای ارتباطات (M2M) که رشد قابل توجهی دارد [32].

• به روزرسانی سیستم‌عامل: دستگاه‌های اینترنت اشیا باید با امضای دیجیتالی مناسب قابل اصلاح یا ارتقا باشند. چندین تهدید جدی در اینترنت وجود دارد که دستگاه‌های اینترنت اشیا را تحت تأثیر قرار می‌دهد. فروشندگان و ارائه دهندگان خدمات باید برنامه ریزی کنند در آینده این به روزرسانی‌ها باید به صورت مقطعی انجام شوند یا با توجه به اهمیت بروزرسانی [33].

• جعل هویت دستگاه: گره‌های ارسال و دریافت باید به عنوان دستگاه‌های قانونی شناسایی شوند. بنابراین، ایمن‌سازی در برابر جعل هویت دستگاه اینترنت اشیا از اهمیت زیادی برخوردار است.

• آزمایش پویا: برای دستگاه‌های اینترنت اشیا بسیار مهم است که آزمایش را انجام دهند و حداقل اقدامات استاندارد را برای امنیت ایجاد کنند. برای آزمایش امنیت دستگاه‌های اینترنت اشیا، دو نوع وجود دارد: ایستا و پویا. در مقابل آزمایش ایستا که مربوط به

کشف تهدیدات در نرم افزار است، آزمایش پویا می‌تواند تهدیدات و آسیب پذیری‌ها را هم در سخت افزار و هم در نرم افزار کشف کند [34].

• Failover Design: دستگاه‌های اینترنت اشیا باید در صورت از بین رفتن یا اختلال در اتصال اینترنت به طور مناسب کار کنند. با این حال، تعداد کمی از دستگاه‌های اینترنت اشیا ساخته شده اند تا با چنین شرایط خرابی مانند مشکل اینترنت یا قطع ارتباط داده کار کنند. طراحی Failover برای دستگاه‌های اینترنت اشیا که شامل ایمنی کاربر هستند، مانند مکانیسم‌های قفل در، مانیتورهای محیطی و هشدارها ضروری است. این دستگاه‌ها باید دارای ویژگی‌های اضافی در صورت قطع فعالیت باشند [35].

چالش‌های اخلاقی در اینترنت اشیا

اگرچه سیستم اینترنت اشیا به طور گسترده ای در جامعه ما پذیرفته شده است و میلیاردها دستگاه موجود است، اما چندین مورد برای اعمال اخلاق در زمینه اینترنت اشیا وجود دارد. این چالش‌ها شامل موارد زیر است:

• شناسایی مالک: تعریف دقیق مالک داده‌های جمع آوری شده در یک سیستم معمولی اینترنت اشیا دشوار است. جمع آوری انواع داده‌ها بدون رضایت و اجازه کاربر مسئله مهمی است که باید در سیستم اینترنت اشیا مورد بررسی قرار گیرد.

• خط مرزی عمومی و خصوصی: سیستم اینترنت اشیا شامل چندین حسگر است که هم داده‌های عمومی و هم خصوصی را جمع-آوری می‌کند. در صورت عدم وجود مرزهای مشخص برای اطلاعات کاربران، مرز بین اطلاعات خصوصی و عمومی باید در برنامه-های مختلف اینترنت اشیا تعریف شود.

• حملات زندگی مردم: در یک سیستم رایانه ای خالص، نقض امنیت می‌تواند منجر به از دست رفتن داده‌ها یا آسیب فیزیکی به سیستم رایانه ای شود. در حالی که در سیستم اینترنت اشیا، همانطور که تمام محیط ما از جمله خانه، اتومبیل، کنتور هوشمند و غیره در شبکه اینترنت اشیا متصل هستند، نقض اینترنت اشیا می‌تواند به معنای واقعی کلمه زندگی افراد را تحت تأثیر قرار دهد.

طراحی اخلاقی برای اینترنت اشیا

با میلیاردها دستگاه اینترنت اشیا، مقدار داده تولید شده توسط این دستگاه‌ها قابل پیش بینی نخواهد بود. ادغام این مقدار داده با نوآوری‌ها و توسعه ابزارهای تجزیه و تحلیل داده‌های کارآمد باعث تغییر تفکر افراد در مورد اینترنت اشیا و پیشرفت اقتصادی عظیمی می‌شود که با استفاده از این داده‌ها می‌توان به دست آورد. از طرف دیگر، هنوز اصول اخلاقی مناسبی برای تنظیم نحوه جمع آوری این داده‌ها بدون نقض حریم خصوصی افراد وجود ندارد. بنابراین، یک طرح اخلاقی برای دستگاه‌ها و سرویس‌های اینترنت اشیا در آینده لازم است تا گزینه‌های اخلاقی مختلفی را برای کاربران در بستر دیجیتال باز کند و باعث شود درصورتی که کاربر بخواهد آن را بپردازد، به عنوان یک ارزش افزوده عمل کند [36]. طراحی اخلاقی در محصولات اینترنت اشیا به عنوان ابزاری برای اجازه دادن به مصرف کنندگان اینترنت اشیا برای مدیریت و محافظت از داده‌های شخصی و سایر اطلاعات مرتبط استفاده می‌شود. همه گزینه‌های اخلاقی مختلف در الگوریتم‌هایی که توسط برنامه نویسان و توسعه دهندگان ایجاد می‌شوند، جاسازی می-شود. از آنجا که ارائه این ویژگی‌های جدید رایگان نیست، یک دستگاه IoT اخلاقی هزینه اضافی را شامل می‌شود که شامل پیاده-سازی و استقرار قالب بندی اخلاقی و اطمینان از سطح بالاتر آزادی کاربران اینترنت اشیا است.

طبق نظر W. Pollard [37]، دستگاه‌های اینترنت اشیا شامل طراحی اخلاقی باید از ویژگی‌های زیر برخوردار باشند:

- توانایی مدیریت و کنترل جمع آوری و توزیع داده‌های شخصی یا خدمات.
- توانایی اعمال قوانین و سیاست‌های مختلف بدون در نظر گرفتن زمان و مکان.
- توانایی پشتیبانی از زمینه‌های پویا مانند خانه و دفتر.
- توانایی مشاهده، شناخت و پشتیبانی از روابطی که به گزینه‌های اخلاقی نیاز دارند.

تهدیدهای امنیتی در شهرهای هوشمند از جمله کلان‌شهر اصفهان

مانند سایر برنامه‌های اینترنت اشیا، شهرهای هوشمند طیف گسترده ای از آسیب پذیری‌ها را فراهم می‌کند که می‌تواند توسط مهاجمان و سایر بازیگران مخرب مورد سو استفاده قرار گیرد و آسیب جدی به مردم یا دستگاه‌های فیزیکی وارد کند. تهدیدهای امنیتی در زمینه یک شهر هوشمند را نباید نادیده گرفت زیرا می‌تواند بر بهره‌وری و کارایی خدمات ارائه شده توسط شهر هوشمند تأثیر بگذارد. تهدیدهای امنیتی متعددی در شهرهای هوشمند وجود دارد، برخی از رایج ترین تهدیدات شامل موارد زیر است:

•سرقت اطلاعات و هویت: داده‌های ایجاد شده توسط زیرساخت‌های محافظت نشده از شهرهای هوشمند

• حمله MITM :این یکی از تهدیدات رایج در شهرهای هوشمند است که در آن یک مهاجم یک گره مخرب بین دو گره ارتباطی تزریق می‌کند تا اطلاعات مکالمه را بدزدد.

• Device Hijacking: در این نوع حمله، مهاجم دستگاه خاصی را بدون تغییر در عملکرد اصلی آن ضبط و کنترل می‌کند که شناسایی آن را بسیار دشوار می‌کند.

• سخت افزار ناامن: سنسورها نقطه شروع هر حمله هستند. در صورت عدم آزمایش مناسب، تهدیدهای بزرگی برای کل سیستم اینترنت اشیا ایجاد می‌شود. عدم استانداردسازی سخت افزاری دستگاه‌های اینترنت اشیا، چندین نقطه ضعف ایجاد می‌کند که می-تواند توسط مهاجمان مورد سو استفاده قرار گیرد.

• Larger Attack Surface: مقیاس بزرگ یک شبکه هوشمند شهری سطح حمله بزرگی را ایجاد می‌کند. از آنجا که شهرهای هوشمند حاوی هزاران سیستم و دستگاه برای کنترل خدمات مختلف هستند، هر دستگاهی در شبکه شهر هوشمند آسیب پذیر است و در هر زمان قابل حمله است. بعلاوه، حمله به یک دستگاه ممکن است کل شبکه را به خطر بیندازد [38].

• اشکالات نرم افزاری: از آنجا که شهرهای هوشمند حاوی هزاران سیستم و دستگاه هستند، یک اشکال ساده نرم افزاری می‌تواند تأثیر زیادی بر روی دستگاه‌ها و برنامه‌های سیستم بگذارد.

همچنین در ادامه به راه حل‌های پیشنهادی برای تهدیدهای امنیتی مهم در کلان‌شهرهای هوشمند همچون اصفهان پرداخته شده است:

ارائه مکانیزم‌های امنیتی مختلف برای تأمین امنیت یک شهر هوشمند عملیاتی اجباری برای حفظ نوآوری خدمات و برنامه‌های جدید است که باعث بهبود زندگی مردم و کیفیت زندگی آن‌ها می‌شود. مجموعه ای از راه حل‌های امنیتی برای ساخت یک شهر هوشمند امن وجود دارد. این راه حل‌ها شامل: احراز هویت متقابل، نظارت و تجزیه و تحلیل امنیتی و یکپارچگی و رازداری داده‌ها است.

• احراز هویت متقابل: انواع مختلف دستگاه‌های متصل به شبکه شهر هوشمند باید قبل از هرگونه انتقال داده احراز هویت شوند. با این کار هویت دستگاه‌های ارتباطی تأیید می‌شود و اطمینان حاصل شود که فقط دستگاه‌های قانونی اجازه ارسال و دریافت داده را

دارند. بنابراین، احراز هویت متقابل، جایی که دو دستگاه و سرویس هویت خود را برای یکدیگر تأیید می‌کنند، می‌تواند به محافظت در برابر حملات مخرب کمک کند [39].

• نظارت و تجزیه و تحلیل امنیت: داده‌های سیستم باید کشف و کنترل شوند تا تخلفات احتمالی امنیتی یا تهدیدهای امنیتی احتمالی شناسایی شود. پس از شناسایی تهدید امنیتی، اقدامات مناسب مطابق سیاست امنیتی سیستم باید انجام شود [40].

• یکپارچگی و رازداری داده‌ها: شهرهای هوشمند از داده‌ها برای بهبود خدمات و کیفیت زندگی شهروندان استفاده می‌کنند. این داده‌ها باید مطمئن و دقیق باشند. به عبارت دیگر، برای اطمینان از صحت داده‌ها و عدم دستکاری از طریق فرایند انتقال، باید از اقدامات یکپارچگی استفاده شود. علاوه بر این، باید اقدامات امنیتی برای محافظت در برابر افشای غیر مجاز اطلاعات حساس انجام شود.

ساختمان هوشمند: تهدیدات امنیتی: خرابی سیستم‌ها، کنترل سیستم آتش سوزی، تغییر کنتورهای هوشمند، باز کردن دروازه‌های پارکینگ، آلوده شدن توسط بدافزار، آسیب رساندن یا کنترل آسانسورها، از کار انداختن منابع آب و برق

راه حل‌ها: احراز هویت دو عاملی، مدل تهدید و خطر، پزشکی قانونی اینترنت اشیا، پشتیبان گیری و بازیابی اطلاعات (راه حل‌هایی برای تضمین قابلیت اطمینان و تداوم خدمات)

حمل و نقل هوشمند: تهدیدات امنیتی: ارسال پیام‌های اضطراری اشتباه، توقف موتور وسیله نقلیه، تغییر سیگنال‌های GPS، ایجاد اختلال در سیستم واکنش اضطراری خودرو، ایجاد اختلال در سیستم ترمز خودرو

راه حل‌ها: راه حل‌های تشخیص رفتار نادرست، شبه هویت، زیرساخت کلید عمومی (PKI) ، گواهینامه‌های دیجیتال (ECDSA)، راه حل‌های رمزگذاری داده‌ها (ECIES و AES)

مراقبت‌های بهداشتی: تهدیدات امنیتی: ارسال اطلاعات نادرست، ارسال هشدار اضطراری، حملات مسدود کننده، استراق سمع اطلاعات حساس، ایجاد اختلال در سیستم نظارت، ایجاد اختلال در خدمات اضطراری

راه حل‌ها: شبکه‌های Wi-Fi امن برای تضمین مدیریت ایمن اطلاعات محرمانه و داده‌های شخصی، ارزیابی ریسک

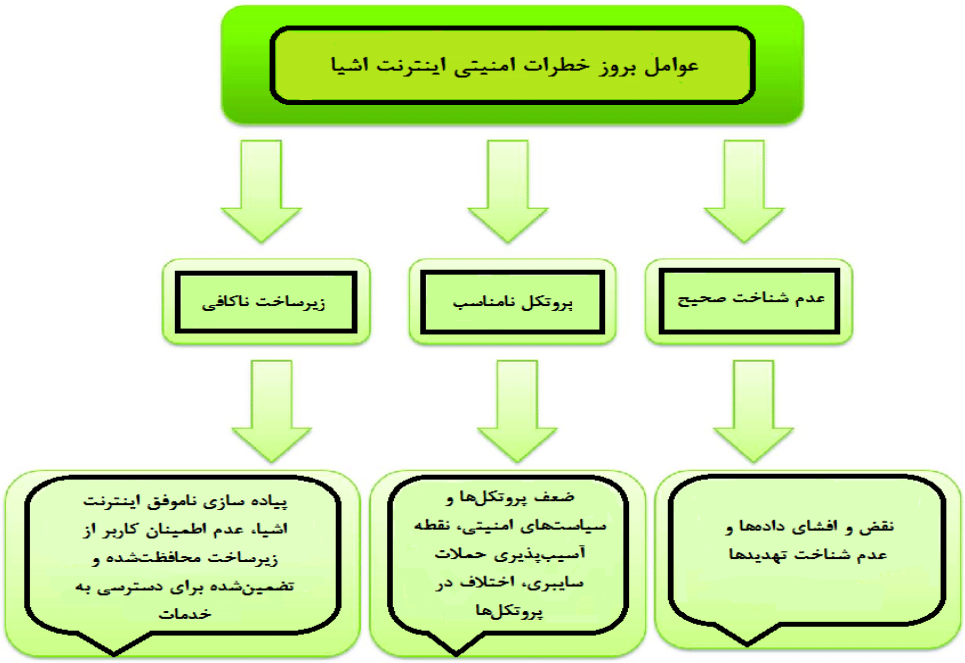
انرژی: تهدیدات امنیتی: جعل آدرس و نام کاربری، دسترسی و کنترل‌های غیرمجاز، حملات صفر روزه، انکار سرویس و انکار سرویس توزیع شده (DDoS)

راه حل‌ها: تکنیک‌های تشخیص و پیشگیری از نفوذ، ارزیابی ریسک، تجزیه و تحلیل تهدیدات داخلی، هوش جرایم اینترنتی

چارچوب نظری

در بررسی آگاهی کاربران از پروتکل‌ها و راهکارهای امنیتی در زیرساخت اینترنت اشیای شهر اصفهان، قصد داریم از یک جامعه آماری متنوع برای شرکت در نظرسنجی و پر کردن پرسش‌نامه، دعوت به همکاری کنیم. در نظر داشته باشید که شهر هوشمند اصفهان که به اینترنت اشیا مجهز شده است، یک جامعه آماری وسیعی را شامل می‌شود. از این رو باید از هر قشر و بخش مرتبط با اینترنت اشیا، گروه مشخصی را هدف قرار داده و برای شرکت در پر کردن پرسش‌نامه، دعوت به همکاری شود. در این خصوص، در کل از ۱۰۰۰ نفر برای شرکت در پر کردن پرسش‌نامه، دعوت به همکاری شده است.

مدل مفهومی پژوهش



روش تحقیق

رویکرد پژوهش ترکیبی و از نوع اکتشافی است و از نظر هدف، کاربردی می‌باشد. در بخش کیفی از روش تحقیق، در ابتدا، به بررسی میزان دانش و آشنایی جامعه آماری نسبت به اینترنت اشیا پرداخته شده است. در ادامه نیز، به بررسی میزان آشنایی جامعه آماری با مسائل امنیتی حوزه اینترنت اشیا پرداخته شده است. جامعه آماری مربوط به این پژوهش، به تعداد ۱۰۰۰ نفر از افراد مختلف در شهر اصفهان می‌باشد. این افراد به صورت نمونه‌گیری تصادفی از گروه‌های دارای مدرک کارشناسی ارشد، کارشناسی، دانش‌آموزان و دانشجویان، افراد دارای مدرک دیپلم یا بدون مدرک انتخاب شده‌اند. روش گردآوری داده‌ها، به صورت میدانی بوده و اطلاعات به وسیله مصاحبه و پرسش‌نامه بدست آمده است. هدف اصلی در طراحی پرسش‌نامه، ارائه سوالاتی بوده که بتوانند سطح آگاهی کاربران را از پروتکل‌های امنیتی و چگونگی استفاده از اینترنت اشیا، مورد بررسی قرار دهند. این پرسش‌نامه دارای ۱۵ پرسش با ۵ گزینه ارزیابی کاملا مخالفم، مخالفم، نظری ندارم، موافقم، کاملا موافقم جهت پاسخ‌دهی می‌باشد. پرسش‌ها بر اساس اهداف پژوهش و رابطه فرضیه‌ها(متغیرها) و شاخص‌های هر یک، از مقیاس طیف لیکرت طراحی شده‌اند. پایایی و اعتبار پرسش‌نامه تحقیق حاضر، با محاسبه ضریب آلفای کرونباخ، سنجیده شده است. پایایی اولیه بر اساس نمونه، ۰,۷۹۹ بدست آمد. این مقدار،

نشان از قابل قبول بودن پرسش‌نامه می‌باشد. از این رو بعد از رسیدن به نتایج قابل قبول، پرسش‌نامه در بین جامعه آماری مدنظر توزیع شد.

فرضیه‌ها

با توجه به سؤالی که در ابتدای مقاله آورده شده و همچنین با توجه به مدل مفهومی پژوهش، می‌خواهیم میزان تاثیر سه فرضیه مؤثر و مهم در بروز خطرات امنیتی را بررسی کنیم. بنابراین سه فرضیه، به صورت زیر می‌باشند:

- عدم شناخت صحیح
- پروتکل نامناسب
- زیرساخت ناکافی

در این راستا، برای نظرسنجی جامعه آماری، به منظور سنجش متغیرهای پژوهش، از پرسش‌نامه استفاده شده است. باید توجه داشت که در بررسی موضوع امنیت اینترنت اشیا در شهر اصفهان، پیاده‌سازی اینترنت اشیا یک موضوع و چگونگی استفاده از این تکنولوژی یک موضوع جداست. در نظر داشته باشید که در موقع پیاده‌سازی زیرساخت اینترنت اشیا در یک شهر هوشمند، همواره پروتکل‌های امنیتی خاصی را در نظر می‌گیریم. به طوری که با استفاده از این پروتکل‌های امنیتی، قادر هستیم تا حدودی زیرساخت ایمنی مربوط به اینترنت اشیای شهر هوشمند را فراهم آوریم. ولی موضوع مهم دیگر، این است که کاربران، تا چه حد با پروتکل‌های امنیتی و نحوه استفاده از اینترنت اشیا آشنا هستند. توجه داشته باشید که اکثر حملات سایبری انجام گرفته در مورد اینترنت اشیا، از ضعف دانش کاربران این تکنولوژی به وجود می‌آید.

گروه‌های مربوط به این جامعه آماری عبارتند از:

گروه الف

در این ۱۰۰۰ نفر، ۵۰۰ نفر دارای مدارک کارشناسی ارشد می‌باشند. از بین این افراد که دارای مدرک کارشناسی ارشد هستند، نصف افراد در مشاغل سازمانی عضویت دارند و نصف دیگر نیز یا تازه فارغ‌التحصیل شده‌اند و یا اینکه به صورت دورکاری و شغل آزاد مشغول کار می‌باشند.

گروه ب

همچنین، ۲۵۰ نفر جامعه آماری نیز مربوط به افرادی هستند که دارای مدرک کاشناسی بوده و در ادارات دولتی، شرکت‌های خصوصی و یا شغل آزاد مشغول به فعالیت می‌باشند.

گروه ج

از طرفی دیگر، ۱۵۰ نفر جامعه آماری، به جوانان و نوجوانانی تعلق دارد که در حال تحصیل در مدرسه و یا دانشگاه می‌باشند.

گروه د

در نهایت، ۱۰۰ نفر باقی‌مانده نیز به افراد دارای مدرک تحصیلی دیپلم و یا بدون مدرک تحصیلی، خانه‌دارها، اصناف و غیره تعلق می‌گیرند.

بعد از مشخص کردن جامعه آماری، پرسش‌نامه مدنظر بین این افراد تقسیم شده است. از افراد برای پر کردن پرسش‌نامه دعوت شده و در نهایت، نتایج بدست آمده، برای بررسی و تحلیل وارد نرم افزار SPSS شده است.

یافته‌های پژوهش

بعد از ارائه پرسش‌نامه به جامعه آماری و گرفتن اطلاعات از افراد دعوت شده، نتایج بدست آمده در قالب جداول داده، در نرم افزار SPSS وارد شدند. در نرم افزار SPSS، تحلیل‌های مشخصی بر روی داده‌های وارد شده انجام شد. در نهایت، نتایج مشخص و جالبی در مورد آشنایی گروه‌ها با اینترنت اشیا، پروتکل‌های امنیتی آن و زیرساخت شهر اصفهان بدست آمد. این نتایج به صورت زیر می‌باشند.

در بین افراد شرکت‌کننده، به ترتیب گروه‌های ج، الف، ب و د نسبت به اینترنت اشیا، پروتکل‌های امنیتی آن و زیرساخت اصفهان آشنایی دارند. در این راستا، از گروه ج ۷۵ درصد، بیش‌ترین آشنایی را با اینترنت اشیا، پروتکل آن و زیرساخت شهر اصفهان دارند. این در حالی است که گروه د با ۵ درصد، کم‌ترین آشنایی را با این حوزه دارند. همچنین، بسیار تعجب‌آور است گروه‌های الف و ب که گروه‌های فارغ‌التحصیل از دانشگاه‌ها هستند، با این حوزه، آشنایی کمی دارند. بر این اساس، از افراد گروه‌های الف و ب جامعه آماری، به ترتیب تنها ۵۴ و ۳۹ درصد، نسبت به این حوزه آشنایی دارند. همچنین در گروه الف از جامعه آماری، تنها ۲۲ درصد از افراد نسبت به انواع تهدیدات امنیتی اینترنت اشیا آگاهی دارند. این نتایج، نشان می‌دهد که قبل از پیاده‌سازی هر نوع پروتکل امنیتی، باید در ابتدا، کاربران را در شهر هوشمند اصفهان با اینترنت اشیا بیش‌تر آشنا کنیم. در این خصوص، باید سمینارهای آموزشی در بازه‌های زمانی مشخصی در شهر اصفهان برگزار شود و برای افرادی که قصد بهره‌مند شدن از امکانات این زیرساخت را داشته باشند، باید گرفتن گواهی آشنایی با اینترنت اشیا، به یک ضرورت تبدیل شود. بدین ترتیب از حضور افراد با آگاهی کم‌تر نسبت به اینترنت اشیا و موضوعات امنیتی مربوط به این حوزه در درون زیرساخت جلوگیری به عمل آورده خواهد شد. از این رو یکی از حفره‌های بسیار خطرناک امنیتی یعنی دانش پایین کاربران برداشته خواهد شد.

همچنین نتایج آماری نشان می‌دهد که در کل ۴۳ درصد از افراد با اینترنت اشیا به صورت نزدیک و یا دورا دور آشناییت دارند. همچنین از بین این ۴۳ درصد، ۷۸ درصد از امکانات زیرساخت اینترنت اشیا هیجان زده هستند و بسیار مشتاق به استفاده از این امکانات و تمهیدات دولت در راستای تامین این زیرساخت می‌باشند. از طرفی دیگر، از بین این گروه، تنها ۱۵ درصد، از پروتکل-های امنیتی و احتمال بروز حملات سایبری آگاهی دارند. لذا در نظر دارند تا با پروتکل‌های امنیتی بیش‌تری از این زیرساخت ارزشمند استفاده کنند.

نتیجه‌گیری و پیشنهادها

با توجه به هدف اصلی این پژوهش، بررسی شد که در شهر هوشمند اصفهان، تا چه حد به اینترنت اشیا، پروتکل‌های امنیتی و زیرساخت مناسب آن و نحوه ایمن کردن حساب‌های کاربری خود آگاه می‌باشند.

باید دوره‌های آموزشی مشخصی را در مورد امنیت اینترنت اشیا، انواع چک‌لیست‌های امنیتی اینترنت اشیا و غیره برای کاربران در نظر بگیریم. در کل، افرادی که بتوانند گواهی آشناییت با اینترنت اشیا و نیز گواهی پروتکل‌های امنیتی آن را بگیرند، می‌توانند به صورت کامل از امکانات اینترنت اشیا در شهر هوشمند اصفهان برخوردار شوند.

در کل، گروه‌های الف، ب و ج از جامعه آماری، تقریباً بیش‌ترین ارتباط را با زیرساخت اینترنت اشیا در شهر اصفهان دارد. به عبارتی دیگر، این بخش از جامعه آماری، به دلیل نوع فعالیت و نیازهایی که دارند، بیش‌ترین استفاده را از زیرساخت فناوری اطلاعات می‌برند. لذا در مورد انواع تهدیدات امنیتی، باید این گروه را بیش‌تر مدنظر قرار دهیم.

بدین ترتیب نتایج پرسش‌نامه نشان می‌دهد که با افزایش سطح آگاهی مردم اصفهان از اینترنت اشیا و انواع پروتکل‌های امنیتی و زیرساخت آن، می‌توان راهکارهای مؤثرتری را در راستای افزایش میزان امنیت در این حوزه در دستور کار قرار داد.

اگرچه این پژوهش، به سازندگان اینترنت اشیا توصیه می‌کند که به دنبال روش‌های به روز برای انطباق خدمات خود با اکوسیستم جدید و دور شدن از روش‌های سنتی امنیت فناوری اطلاعات باشند، اما تحقیقات بیشتری در این زمینه لازم است. مسئولیت اجرای راه حل‌های امنیتی مناسب به یک طرف واحد اکوسیستم اینترنت اشیا بستگی ندارد، بلکه به همه بازیگران درگیر، مربوط است، از تامین‌کنندگان سیلیکون گرفته تا تولیدکنندگان، توسعه‌دهندگان، قانون‌گذاران و مشتری نهایی. اگر امنیت از برنامه‌ریزی و طراحی اولیه محصول مورد توجه قرار گیرد و برخی از مکانیزم‌های اساسی پیشگیری وجود داشته باشد، کاهش خطرات مرتبط با نقض امنیت امکان‌پذیر است. بنابراین، این پژوهش، پایه‌ای برای تحقیقات بعدی محققان می‌باشد و پیشنهاد آینده، همکاری همه تاثیرگذاران در حفظ امنیت این فناوری، بخصوص پررنگ شدن نقش دولت در تامین زیرساخت اینترنت اشیا و پیاده‌سازی آن می‌باشد که نقش بسزایی در فرهنگ‌سازی و بکارگیری این حوزه ایفا می‌کند.

منابع

۱. وبسایت دانشگاه اصفهان (https://ui.ac.ir).

۲. شایسته فرد ، سید علیرضا، امیدی ، مهدی (۱۳۹۵)، بررسی امنیت اینترنت اشیا با استفاده از راهکارهای بلاکچین، هفتمین همایش ملی بانکداری الکترونیک و نظام‌های پرداخت.

۳. تقوایی, فاطمه؛ ساسان رجبی و رامین صفا، (۱۳۹۷)، استفاده از بلاکچین در اینترنت اشیا و کاربرد آن در مراقبت سلامت، دومین همایش انفورماتیک پزشکی و هفتمین همایش سلامت الکترونیک و کاربردهای ICT در پزشکی ایران، تهران، دانشگاه تربیت مدرس.

4. Atlam, H.F., Walters, R.J., Wills, G.B.: Intelligence of Things: Opportunities & Challenges. 3rd Cloudification of the Internet of Things (CIoT), pp. 1–6 (2018).

5. Pawar L, Bajaj R, Singh J, Yadav V. Smart city IoT: smart architectural solution for networking, congestion and heterogeneity. In: 2019 international conference on intelligent computing and control systems (ICCS). IEEE; 2019. p. 124–9.

6. Camero A, Alba E. Smart city and information technology: a review. Cities 2019; 93:84–94.

7. Sookhak M, Tang H, He Y, Yu FR. Security and privacy of smart cities: a survey, research issues and challenges. IEEE Commun Surv Tutor 2018;21(2):1718–43.

8. Singh SK, Jeong YS, Park JH. A deep learning-based IoT-oriented Infrastructure for secure smart city. Sustain Cities Soc 2020;60:102252.
9. Ren Y, Liu Y, Yin X, Shen Z, Kim HJ. Blockchain-based trusted electronic records preservation in cloud storage. ComputMater Continua 2019;58(1):135–51.
10. Liu Z, Xia J. A cross-tenant RBAC model for collaborative cloud services. CMCComput Mater Continua 2019;60(1):395–408.
11. Capellupo M, Liranzo J, Bhuiyan MZA, Hayajneh T, Wang G (2017) Security and attack vector analysis of IoT devices. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, Cham, pp 593–606.
12. Vervier PA, Shen Y (2018) Before toasters rise up: a view into the emerging iot threat landscape. In: International Symposium on Research in Attacks, Intrusions, and Defenses, Springer, Cham, pp 556–576.
13. https://www.statista.com/statistics/471264/iot-number-ofconnected-devices-worldwide/
14. Wang K-H, Chen C-M, Fang W, Tsu-Yang Wu (2018) On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. J Supercomput 74(1):65–70.
15. Bhattacharjya A, Zhong X, Wang J, and Li X (2019) Security challenges and concerns of Internet of Things (IoT). In: Cyber-Physical Systems: architecture, security and application, Springer, Cham, pp 153–185.
16. Singh S, Sharma PK, Moon SY, Park JH (2017) Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Humaniz Comput. https://doi. org/10.1007/s12652-017-0494-4.
17. Grooby S, Dargahi T, Dehghantanha A (2019) A bibliometric analysis of authentication and access control in IoT devices. Handbook of big data and IoT security. Springer, Cham, pp 25–51.
18. Atlam HF, Wills GB (2020) IoT security, privacy, safety and ethics. Digital twin technologies and smart cities. Springer, Cham, pp 123–149.
19. Zhao K, Ge L. A survey on the internet of things security. In: 2013 Ninth international conference on computational intelligence and security. IEEE; 2013. p. 663–7.
20. Ammar M, Russello G, Crispo B. Internet of things: a survey on the security of iot frameworks. J Inf Secur Appl. 2018;38:8–27.
21. Granjal J, Monteiro E, Silva JS. Security for the internet of things: a survey of existing protocols and open research issues. IEEE Commun Surv Tutor. 2015;17(3):1294–312.
22. ITU: Overview of the Internet of things. Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. next-generation networks - Fram. Funct. Archit. Model., p. 22 (2012).
23. Stallings, W.: The internet of things: network and security architecture. Internet Protocol J. 18(4), 2–24 (2015).
24. Cisco: The Internet of Things Reference Model. White Paper, pp. 1–12 (2014).
25. Atlam, H.F., Attiya, G., El-Fishawy, N.: Integration of color and texture features in CBIR system. Int. J. Comput. Appl. 164(3), 23–29 (2017).
26. Hou J, Leilei Qu, Shi W (2019) A survey on internet of things security from data perspectives. Comput Netw 148:295–306.
27. Shamsoshoara A, Korenda A, Afghah F, Zeadally S (2019) A survey on hardware-based security mechanisms for internet of things. arXiv preprint.
28. Aman, W.: Modeling adaptive security in IoT Driven eHealth. In: Norwegian Information Security Conference (NISK 2013), pp. 61–69 (2013).
29. Atlam, H.F., Walters, R.J., Wills, G.B.: Fog computing and the internet of things: a review. Big Data Cognitive Comput. 2(2), 1–18 (2018).
30. Atlam, H.F., Walters, R.J., Wills, G.B.: Internet of things: state-of-the-art, challenges, applications, and open issues. Int. J. Intell. Comput. Res. 9(3), 928–938 (2018).
31. George, C., Fink, G.A., Mandal, S., Hrivnak, C.: Internet of things (IoT) security best practices. IEEE Internet Technol. Policy Community White Paper, no. February (2017).
32. Atlam, H.F., Alenezi, A., Alharthi, A., Walters, R., Wills, G.B.: Integration of cloud computing with internet of things: challenges and open issues. In: 2017 IEEE International Conference on Internet of Things (iThings) and

IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), no. June, pp. 670–675 (2017).
33. Kvarda, L., Hnyk, P., Vojtech, L., Neruda, M.: Software implementation of secure firmware update in IoT concept. Adv. Electrical Electron. Eng. 15(4), 626–632 (2017).
34. George, C., Fink, G.A., Mandal, S., Hrivnak, C.: Internet of things (IoT) security best practices. IEEE Internet Technol. Policy Community White Paper, no. February (2017).
35. Venkatesh, J., Diego, S.: Scalable- application design for the IoT. IEEE Comput. Soc., 62–70 (2017).
36. Popescul, D., Georgescu, M.: Internet of things—some ethical issues. USV Ann. Econ. Public Adm. 13(2), 208–214 (2013).
37. Pollard, W.: IoT governance, privacy and security issues. Eur. Res. Clust. Internet Things, 23–31 (2015).
38. Kitchin, R., Dodge, M.: The (In)Security of smart cities: vulnerabilities, risks, mitigation, and prevention. J. Urban Technol., 1–19 (2017).
39. Khatoun, R., Zeadally, S.: Cybersecurity and privacy solutions in smart cities. IEEE Commun. Mag. 55(3), 51–59 (2017).
40. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of things for smart cities. IEEE Internet Things J. 1(1), 22–32 (2014).