فصلنامه پژوهش‌های حفاظتی ـ امنیتی
دانشگاه جامع امام حسین(علیه‌السلام)
سال دوازدهم، شمارهٔ ۴۷ پاییز ۱۴۰۲

چارچوب ارزیابی امنیتی شبکه و تجهیزات اینترنت اشیا در اماکن هوشمند نیروهای مسلح

●وحید یادگاری ●
دانشجوی دکتری فناوری اطلاعات دانشگاه علامه طباطبایی تهران، ایران (نویسنده مسئول)
●احمدرضا متین‌فر ●
استادیار دانشگاه جامع امام حسین(ع)، تهران، ایران
●صمد سهراب ●
کارشناس ارشد فناوری اطلاعات (امنیت اطلاعات)، مؤسسه آموزش عالی تعالی قم، قم، ایران

تاریخ دریافت: ۱۴۰۲/۰۷/۱۰ تاریخ پذیرش: ۱۴۰۲/۰۹/۱۸

چکیده

توسعه اینترنت اشیا و فناوری‌های مکمل مثل هوش مصنوعی در حوزه‌های مختلف مثل سلامت، خانه هوشمند و... پرکاربرد شده است. توسعهٔ اماکن هوشمند با استفاده از فناوری خانه‌های هوشمند مبتنی بر اینترنت اشیا، از بسترهای ارتباطی و سنسورهای قابل‌برنامه‌ریزی به‌منظور هوشمندسازی و یکپارچه کردن بخش‌های مختلف یک ساختمان و باهدف کاهش مصرف انرژی، بهره‌برداری مؤثر از منابع، امنیت بالا و سبک زندگی راحت بهره می‌برد. این مهم در کنار خلق مزایای فراوان، به‌دلایل مختلفی همچون آسیب پذیری‌های رمز عبور، عدم به‌روزرسانی دستگاه‌ها، پیکربندی ضعیف لایه‌های نرم‌افزاری و ارتباطی، پروتکل‌های ضعیف و... همواره افزایش تهدیدات سامانه‌های اینترنت اشیا را در پی دارد. در این پژوهش باتوجه به مشکلات مورد اشارهٔ امنیتی به‌ویژه در اماکن نیروهای مسلح، پاسخ سؤالِ چارچوب ارزیابی امنیتی اینترنت اشیا در اماکن هوشمند نیروهای مسلح چگونه است؟ با بهره‌گیری از نگاشت استانداردها و چارچوب‌های معتبر جهانی و نظریه خبرگی مورد بررسی و واکاوی قرار گرفت. نتایج بررسی بیانگر این است که به ترتیب مؤلفه‌های گذرواژه‌های ضعیف (۹۱,۲٪)، خدمات شبکه ناامن (۸۹,۳٪)، حفاظت ناکافی از حریم خصوصی (۸۸,۱٪)، عدم وجود مکانیسم‌های به‌روزرسانی امن (۸۷٪)، انتقال و ذخیره‌سازی ناامن داده (۸۶,۳٪)، عدم وجود مدیریت دستگاه (۸۳,۹٪)، و واسط‌های اکوسیستم ناامن (۷۹,۳٪) در ارزیابی امنیتی در اماکن هوشمند نیروهای مسلح دارای اولویت هستند.

کلید واژه‌ها: اینترنت اشیا، اماکن هوشمند، سنسور، ارزیابی امنیتی

مقدمه

اینترنت اشیا دیدگاهی نوین در صنعت فناوری اطلاعات است که تمامی مفاهیم فنی، اجتماعی و اقتصادی را شامل می‌شود. در این دیدگاه محصولات، کالاهای مصرفی، خودروها و ساختمان‌ها، صنایع پزشکی، تجهیزات صنعتی و صنایع (برق، تلفن و ...)، حسگرها و دیگر مؤلفه‌ها هر روزه توسط اتصالات اینترنتی و همچنین قابلیت‌های قدرتمند تحلیلی داده‌ها با یکدیگر ترکیب می‌شوند تا نحوه کارکرد و زندگی ما را دگرگون کنند. یکی از مصادیق مهم کاربرد اینترنت اشیا، توسعه خانه‌های هوشمند می‌باشد (پورخلیلی و خوش ادب، ۱۳۹۶).

اماکن یا خانه‌های هوشمند مبتنی بر اینترنت اشیا، از بستر اینترنت به‌منظور هوشمندسازی و یکپارچه کردن بخش‌های مختلف یک ساختمان و باهدف کاهش مصرف انرژی، بهره‌برداری مؤثر از منابع، امنیت بالا و سبک زندگی راحت بهره می‌برد. راه‌کار ساختمان هوشمند از بخش‌های مختلفی از جمله پارکینگ هوشمند، روشنایی هوشمند، سیستم‌های گرمایشی و سرمایشی، حفاظت پیرامونی، مدیریت هوشمند ضایعات و... تشکیل گردیده است (اولیورا و همکاران، ۲۰۱۹). توسعه اینترنت اشیا و فناوری‌های مکمل مثل هوش مصنوعی، بلاک‌چین، داده‌کاوی و... در جهت هوشمندسازی ساختمان‌ها، در کنار خلق مزایای زیاد، چالش‌های خاصی را نیز به همراه خواهد داشت که حریم خصوصی و امنیت از مهم‌ترین چالش‌های اینترنت اشیا می‌باشد (اگراوال، ۲۰۱۹). استفاده ناخودآگاه، تغییر رمز عبور، عدم به‌روزرسانی دستگاه‌ها، پیکربندی ضعیف لایه‌های نرم‌افزاری و ارتباطی، پروتکل‌های ضعیف و... باعث افزایش خطرات مربوط به امنیت سایبری و دسترسی برنامه‌های مخرب به اطلاعات حساس سیستم‌های اینترنت اشیا شده است (نجفی و ملامطلبی، ۱۳۹۹). چنین اقدامات نامناسب امنیتی احتمال نقض داده‌ها و سایر تهدیدات را افزایش می‌دهد. بیشتر متخصصان، امنیت اینترنت اشیا را به‌دلیل ضعف پروتکل‌ها و سیاست‌های امنیتی، نقطه آسیب‌پذیر حملات سایبری می‌دانند. حتی اگر چندین مکانیسم امنیتی برای محافظت از دستگاه‌های اینترنت اشیا در برابر حملات سایبری ایجاد شده باشد، دستورالعمل‌های امنیتی به‌طور مناسب مستند نشده‌اند. بدین ترتیب، کاربران نهایی نمی‌توانند از اقدامات محافظتی برای جلوگیری از حملات داده استفاده کنند (فرجامی و ملامطلبی، ۱۳۹۷). این تحقیق در نظر دارد باتوجه به مشکلات مورد اشاره، چارچوبی برای ارزیابی امنیتی اینترنت اشیا در اماکن هوشمند نیروهای مسلح را ارائه نماید. برای این کار نگاشت استانداردهای و چارچوب‌های معتبر مثل NIST,HIPPA,OWASP ,... نظریه خبرگی مورد توجه بوده و در نهایت چارچوب در یکی از اماکن هوشمند نیروهای مسلح مورد ارزیابی قرار گرفته است (بیات و همکاران، ۱۳۹۷).

مفاهیم پایه

اینترنت اشیا[1]

به‌طور مفهومی می‌تواند به‌عنوان یک زیرساخت شبکه سراسری پویا با قابلیت‌های خود پیکره‌بندی و مبتنی بر استانداردها و پروتکل‌های ارتباط‌جمعی و مشارکتی تعریف شود که در آن اشیای فیزیکی و مجازی دارای شناسه‌ها، صفات فیزیکی و مشخصه‌های مجازی، از واسطه‌های هوشمند استفاده کرده و به‌طور یکنواخت و مستمر در یک شبکه اطلاعات مجتمع شده‌اند (پور خلیلی و همکاران، ۱۳۹۵).

سنسور[2]

سنسور یا حس‌گر ابزاری است که به یک محرک فیزیکی خاص واکنش نشان می‌دهد و یک سیگنال الکتریکی قابل اندازه‌گیری تولید می‌کند. سنسورها می‌توانند مکانیکی، الکتریکی، مغناطیسی یا نوری باشند. به معنای دیگر زیربنای خانه هوشمند اینترنت اشیا است. همین بستر و فناوری باعث می‌شود که به توان در هر جایی و در هر زمانی به این امکانات دسترسی داشت و آنها را کنترل کرد (لورنز، لیورت، ۲۰۲۰).

ارتباطات[3]

ارتباطات در شکل مفرد، فرآیند انتقال پیام از فرستنده به گیرنده به‌شرط همسان بودن معانی بین آنهاست. معنا در علم ارتباط شامل مفاهیم ذهنی و احساسات می‌شود. ارتباطات فرآیندی است که در آن معنا بین موجودات زنده تعریف و به اشتراک گذاشته می‌شود که بسیاری بر این باورند که ریشه آن از یونان نشأت می‌گیرد. ارتباط به یک فرستنده، پیام، رسانه و گیرنده نیاز دارد (بهشتی و عارف، ۱۳۹۷).

پلتفرم[4]

پلتفرم یک مفهوم گسترده است. همچنین دارای قابلیت انعطاف و تغییر است. یعنی می‌توان برای کاربردهای خاص، موارد متفاوتی را به‌عنوان پلتفرم در نظر گرفت. تعریف تئوری، به مجموعه‌ای از سخت‌افزار، نرم‌افزار و سیستم عامل (که خود سیستم عامل هم عضوی از نرم‌افزار است) گفته می‌شود؛ بنابراین سیستم عامل هم یک قسمت از پلتفرم است. این دو با هم فرق دارند و هرکدام وظایف خاص خود را دارند (فهمیده و ذوقی، ۱۳۹۹.)

---

1. IoT (Internet of Things)
2 Sensor.
3. connections
4. Platform

خانه هوشمند[1]

یک تعریف مشخص شده از سوی وزارت بازرگانی و صنعت بریتانیا برای خانه هوشمند وجود دارد که در سال ۲۰۰۳ منتشر شد. این تعریف عبارت است از؛ خانه‌ای که شامل یک شبکه ارتباطی بین تمامی لوازم الکتریکی و خدماتی مهم است و امکان کنترل و دسترسی به آنها را از راه دور فراهم می‌کند (حسین‌پور، ۱۳۹۹). در تعریف دیگر، خانه‌ای را هوشمند می‌نامیم که در آن با ایجاد شبکه ارتباطی بین تمامی تجهیزات و تأسیسات برقی، مکانیکی و... به‌طور یکپارچه ما می‌توانیم از هر نقطه در خارج یا داخل خانه آنها را کنترل نماییم و یا این امور را به سیستم هوشمند سپرده تا در مواقع لزوم از محیط بازخورد گرفته واکنش‌های مناسب را شبیه یک موجود زنده انجام دهد (آلبنی و السهفی، ۲۰۲۲).

امنیت اینترنت اشیا[2]

امنیت اینترنت اشیا به معنی حفاظت از دستگاه‌های متصل به اینترنت و شبکه در دنیای اینترنت اشیا است. با تعریف امنیت در اینترنت اشیا و ضمانت سرویس‌ها و فضای اینترنت جهت استفاده از اینترنت اشیا، می‌توان جهت استفاده از سرویس‌های اینترنت اشیا، اعتماد کامل را برای کاربران این فناوری به‌وجود آورد (سو، ژانگ، دو، ۲۰۱۹). درصورتی‌که مخاطبان قانع نشوند که سرویس‌های اینترنت اشیا از امنیت کافی برخوردار هستند، قطعاً میزان استفاده از اینترنت اشیا کاهش پیدا می‌کند. در تعاریف سنتی، امنیت اینترنتی بر سه اصل محرمانه بودن اطلاعات، ادغام اطلاعات و قابل دسترس بودن داده‌ها استوار است (تانگ و دیگران، ۲۰۲۰)

ارزیابی امنیتی اینترنت اشیا[3]

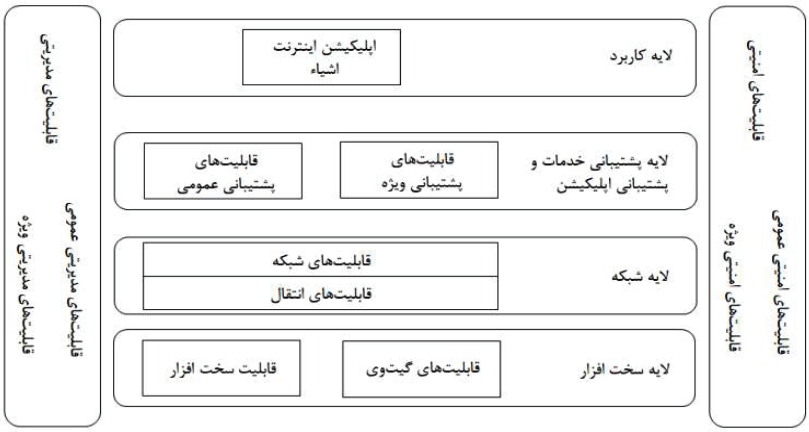
استانداردها و چارچوب‌های معتبر مثل NIST,HIPPA,OWASP,... معتبری در سطح جهان برای ارزیابی امنیتی اینترنت اشیا طراحی شده است. تلفیق و نگاشت چارچوب‌ها و استانداردهای مختلف برای یکپارچگی ارزیابی اینترنت اشیا متناسب با محیط، از راه‌کارهای مورد تأکید است (دوان و دیگران، ۲۰۲۱).

مدل مرجع شبکه اینترنت اشیا[4]

سازمان جهانی فناوری و ارتباطات در حوزه مخابرات ثابت و موبایل دارای سه مجموعه T- ITU-R، ITU D، است. مجموعه T-ITU ،بخش استانداردسازی این سازمان است که در این

1. Smart Home
2. Internet of Things security
3. Internet of Things security assessment
4. Internet of Things reference model

بخش گروهی با نام GSI-IoT به منظور اطلاع رسانی و توسعه استانداردهای شبکه اینترنت اشیا تشکیل شده است. این گروه با سایر نهادها و سازمان‌ها به منظور هماهنگ شدن با رویکردهای مختلف جهانی در معماری اینترنت اشیا همکاری می‌کند. یکی از اسنادی که در سال ۲۰۱۲ توسط T-ITU ارائه شده، ۲۰۶۰. T-ITU است که در بخشی از آن به معرفی مدل مرجع اینترنت اشیا می‌پردازد. این مدل که در شکل۱ نمایش داده شده است و به این موضوع تأکید می‌کند که شبکه اینترنت اشیا از چهار لایه اصلی ۱-لایه اپلیکیشن ۲-لایه پشتیبانی خدمات و پشتیبانی اپلیکیشن ۳-لایه شبکه ۴-لایه سخت‌افزار تشکیل شده است (رازا و همکاران، ۲۰۱۷)، (نسیمی راد، ۱۳۹۴)، (بهشتی، ۲۰۱۸).



شکل(۱) مدل مرجع شبکه اینترنت اشیا (بهشتی، ۲۰۱۸)

بیان مسأله

ضعف‌های امنیتی در پلتفرم خانه‌های هوشمند چالشی جدی به شمار می‌رود و تلاش برای برقراری ارتباط امن میان شبکه خانگی و اینترنت نیز این چالش را پیچیده‌تر می‌کند. به‌علاوه، افزایش تعداد برنامه‌های کاربردی گوشی‌های هوشمند که دسترسی از راه دور به دستگاه‌های اینترنت اشیا محور را امکان‌پذیر می‌سازند، این چالش‌ها را به‌ویژه با درنظرگرفتن علاقه هکرها به این حوزه، به‌شدت افزایش می‌دهد و به همین دلیل، امنیت محصولات مصرفی و در مجموع حفظ امنیت خانه‌های هوشمند بسیار حائز اهمیت است. این مهم به‌واسطه جایگاه و اهمیت اماکن هوشمند در نیروهای مسلح برجسته‌تر است و از طرفی عدم استفاده از فناوری‌های خانه هوشمند در نیروهای مسلح ممکن نبوده و به جهت رویکردهای هوشمندسازی، اجتناب‌ناپذیر می‌باشد. ازاین‌رو ابعاد و مؤلفه‌های چارچوب بومی ارزیابی امنیتی اینترنت اشیا در خانه‌های (اماکن ن.م) هوشمند کدام‌اند؟ مسئله مد نظر در این تحقیق می‌باشد.

پیشینه تحقیق

۱- هاشمی و ستوده، در مقاله‌ای تحت عنوان «ارائه چارچوبی برای ارتقای امنیت خانه‌های هوشمند مبتنی بر اینترنت اشیا با استفاده از - معماری مرجع IoT-A » بیان داشته‌اند که: امروزه خانه هوشمند به‌عنوان یکی از کاربردهای اصلی و رو به رشد اینترنت اشیا محسوب می‌شود که راحتی، امنیت، کاهش مصرف انرژی و هزینه‌های زندگی را به همراه دارد. در کنار مزایا و محاسنی که این فنّاوری به ارمغان آورده است مسئله امنیت و حریم خصوصی به یکی از نگرانی‌های عمده تبدیل‌شده است که نیاز به توجه جدی دارد. معماری مرجع IoT-A باهدف بررسی پروتکل‌ها و منابع موجود، حصول اطمینان از سازگاری اشیا و پروتکل‌های ارتباطی و همچنین ارائه راه‌کاری جامع برای کاربردهای مختلف اینترنت اشیا پایه‌گذاری شده است (هاشمی و ستوده، ۱۳۹۷).

۲- ذوالفقاری‌پور و طیرانی‌راد، در مقاله‌ای تحت عنوان «یک طرح احراز هویت انتخابی برای سیستم خانه هوشمند مبتنی بر اینترنت اشیا» بیان داشته‌اند که: اینترنت اشیا بخشی از اینترنت آینده است که شامل اینترنت موجود و درحال رشد و همچنین توسعه‌های آینده شبکه می‌شود. مسئله امینت در اینترنت اشیا را می‌توان مهم‌ترین چالش توسعه این فناوری در نظر گرفت. دراین رابطه استانداردهای مختلفی درحال توسعه است؛ ولی همچنان نیازمندی‌های امنیتی اینترنت اشیا به‌خوبی شناسایی و تحلیل نشده است. از دیدگاه امنیتی، هم کاربران و هم دستگاه‌های هوشمند باید یک کانال ارتباطی امن و هویت دیجیتالی خود را داشته باشند. احراز هویت از اولین گام‌ها به‌سوی هر گونه اقدام امنیتی است (ذوالفقاری پور و طیرانی راد، ۱۳۹۶).

۳- حمیدی فشکی و دیگران، در مقاله‌ای تحت عنوان «ارائه یک طرح احراز هویت امن با هدف حفظ حریم خصوصی در سیستم خانه هوشمند» بیان داشته‌اند که: در این مقاله ابتدا یک طرح احراز هویت با هدف امنیت و حفظ حریم خصوصی برای حوزهٔ خانه هوشمند که اخیراً ارائه شده است مورد بررسی قرار داده و سپس ضعف‌های امنیتی آن را بیان می‌کند. در ادامه یک طرح احراز اصالت بهبودیافته به‌منظور رفع ایرادات امنیتی طرح مذکور ارائه می‌دهد که طرح پیشنهادی همهٔ ویژگی‌های امنیتی الزام برای طرح احراز اصالت سیستم خانه هوشمند را دارا می‌باشد. همچنین طرح پیشنهادی را از لحاظ امنیت و کارایی با طرح‌های مشابه مقایسه می‌کند. بر اساس تحلیل امنیتی ارائه شده و مقایسه با طرح‌های مرتبط، طرح پیشنهادی ما یک طرح احراز اصالت امن و مناسب برای خانه هوشمند می‌باشد (حمیدی‌فشکی و همکاران، ۱۳۹۸).

۴- آرماندو خوزه مارتینس دو اولیویرا در پایان‌نامه‌ای تحت عنوان «ارزیابی امنیت اینترنت اشیا در یک شهر هوشمند» بیان داشته که: هدف اصلی این کار استفاده از روش ارزیابی خطر امنیتی برای

موارد خاص استفاده از اینترنت اشیا در دامنه شهرهای هوشمند است. این به شما اجازه می‌دهد تا درک کنید که سیستم‌های اینترنت اشیای امروزی در حوزه شهرهای هوشمند از نظر امنیت با چه چالش‌هایی روبه‌رو هستند، برای پیداکردن مهم‌ترین خطرات امنیتی این موارد استفاده، کنترل‌های امنیتی سنتی که می‌توانند این خطرات را کاهش دهند و محدودیت‌های احتمالی هنگام استفاده چیست کنترل‌های امنیتی سنتی به سناریوی اینترنت اشیا. روش مورد استفاده برای تدوین این نتیجه‌گیری از چندین مرحله تشکیل شده است. ابتدا درباره تحقیق در زمینه امنیت، بررسی کارهای انجام شده در این زمینه توسط مشهورترین نهادهای حوزه امنیت اطلاعات. دوم، در تعریف سناریوی مورد استفاده از اینترنت اشیا که محیط آزمایش برای مرحله بعدی است. سوم، استفاده از چارچوب ارزیابی ریسک برای ارزیابی ریسک‌هایی که سناریوی اینترنت اشیا با آن روبه‌رو خواهد شد و درمان این خطرات با استفاده از کنترل‌های امنیتی «فناوری اطلاعات و ارتباطات سنتی» سرانجام در شناسایی مشکلات احتمالی ویژگی‌های اینترنت اشیا هنگام استفاده از این کنترل‌ها (اولیویرا، آرماندو،۲۰۱۹).

۵- جی منیجمنت و دیگران، در مقاله‌ای تحت عنوان «چارچوبی برای خودکارسازی تجزیه‌وتحلیل امنیت اینترنت اشیا» بیان داشته‌اند که: اینترنت اشیا برنامه‌های ابتکاری را در حوزه‌های مختلف امکان‌پذیر می‌کند. به‌دلیل ساختار ناهمگن و در مقیاس گسترده، بسیاری از موضوعات امنیتی جدید را به شما معرفی می‌کند. برای رفع این مشکل، ما چارچوبی را برای مدل‌سازی و ارزیابی امنیت اینترنت اشیا ارائه می‌دهیم و یک تعریف رسمی از چارچوب ارائه می‌دهیم. به‌طورکلی، این چارچوب از پنج مرحله تشکیل شده است: (۱) پردازش داده‌ها، (۲) تولید مدل امنیتی، (۳) تجسم امنیت، (۴) تجزیه‌وتحلیل امنیت، و (۵) به‌روزرسانی‌های مدل. با استفاده از چارچوب، می‌توانیم سناریوهای بالقوه حمله را در اینترنت اشیا پیدا کنیم، امنیت اینترنت اشیا را از طریق معیارهای امنیتی کاملاً مشخص تجزیه‌وتحلیل کنیم و کارایی استراتژی‌های دفاعی مختلف را ارزیابی کنیم. این چارچوب از طریق سه سناریو ارزیابی می‌شود که عبارت‌اند از: خانه هوشمند، نظارت بر مراقبت‌های بهداشتی پوشیدنی و سناریوهای نظارت بر محیط. ما از نتایج تجزیه‌وتحلیل برای نشان‌دادن توانایی‌های چارچوب پیشنهادی برای یافتن مسیرهای بالقوه حمله و کاهش تأثیر حملات استفاده می‌کنیم (منیجمنت، جی،۲۰۱۷).

۶- دیمیتریس ژنیاتاکیس و دیگران، در مقاله‌ای تحت عنوان «مسایل امنیتی و حریم خصوصی برای یک خانه هوشمند مبتنی بر اینترنت اشیا» بیان داشته‌اند که: اینترنت اشیا می‌تواند از برنامه‌ها و خدمات بی‌شماری در حوزه‌های مختلف مانند شهرهای هوشمند و خانه‌های هوشمند پشتیبانی کند. اشیای

هوشمند اینترنت اشیا برای مدیریت، به‌اشتراک‌گذاری داده‌ها و سایر فعالیت‌ها در زمینه خدمات ارائه شده با اجزای دیگر به‌عنوان مثال، پروکسی‌ها، دستگاه‌های تلفن همراه و جمع‌کننده‌های داده ارتباط برقرار می‌کنند (ژنیاتاکیس و همکاران، ۲۰۱۷).

۷- باکو علی و دیگران، در مقاله‌ای تحت عنوان «ارزیابی آسیب‌پذیری سایبری و امنیت فیزیکی برای خانه‌های هوشمند مبتنی بر اینترنت اشیا» بیان داشته‌اند که: شناسایی خطرات احتمالی امنیتی برای تهیه تصویر کاملی از وضعیت امنیتی خانه‌های هوشمند ضروری است. این مقاله روش ارزیابی تهدیدات حیاتی، دارایی و آسیب‌پذیری، معروف به OCTAVE ALLEGRO را برای ارزیابی خطرات امنیتی خانه‌های هوشمند اعمال می‌کند. روش OCTAVE ALLEGRO بر دارایی‌های اطلاعاتی متمرکز است و ظروف مختلف اطلاعاتی مانند پایگاه‌داده، مقالات فیزیکی و انسان را در نظر می‌گیرد. اهداف اصلی این مطالعه برجسته‌سازی آسیب پذیری‌های مختلف امنیتی خانه‌های هوشمند مبتنی بر اینترنت اشیا، ارائه خطرات موجود بر روی ساکنان خانه و پیشنهاد روش‌هایی برای کاهش خطرات شناسایی شده است (علی و آواد، ۲۰۱۸).

مدل مفهومی تحقیق:

چارچوب ارزیابی امنیت برای اینترنت اشیا در خانه‌های (اماکن) هوشمند	✓ گذرواژه‌های ضعیف، قابل حدس‌زدن یا رمزگذاری شده. ✓ خدمات شبکه ناامن ✓ واسطهای اکوسیستم ناامن ✓ عدم وجود مکانیسم‌های به‌روزرسانی امن ✓ حفاظت ناکافی از حریم خصوصی ✓ انتقال و ذخیره‌سازی ناامن داده ✓ عدم وجود مدیریت دستگاه	Application/Data Layer لایه اپلیکیشن Transport Layer لایه انتقال Network Layer لایه شبکه و ارتباطات Datalink Layer لایه پیوند داده Physical/Sensor Layer لایه سنسور	استانداردهای IOT NIST SP ۸۰۰-۵۳ NIST CSF HIPAA OWASP top ۱۰ list	فعالیت این تحقیق
خروجی	۳(ابعاد ۷گانه)	۲	۱	مراحل

شکل(۲) مدل مرجع شبکه اینترنت اشیا

روش تحقیق

این تحقیق از نظر هدف، کاربردی و از نظر روش، آمیخته شامل مصاحبه با خبرگان و توصیفی - تحلیلی با رویکرد پیمایشی می‌باشد. برای مرحله کیفی پس از مطالعه اسناد کتابخانه‌ای و استخراج ابعاد و مؤلفه‌ها، مراتب با طرح سؤالات باز و مصاحبه با افراد متخصص مرکز تحقیقات اینترنت اشیا و جمعی از متخصصان فناوری در سطح نیروهای مسلح در حوزه اینترنت اشیا طرح و پس از رسیدن به چارچوب خاصی که مبتنی بر آخرین استانداردهای بین‌المللی همانند: NIST و پروژه اینترنت اشیا

OWASP (برای کمک به تولیدکنندگان، توسعه‌دهندگان و مصرف‌کنندگان در درک بهتر مسائل امنیتی مرتبط با اینترنت اشیا طراحی شده است و کاربران را در هر زمینه‌ای قادر می‌سازد تا تصمیمات امنیتی بهتری را هنگام ساخت، استقرار یا ارزیابی فناوری‌های اینترنت اشیا اتخاذ کنند.) و مستندات NIST و... می‌باشد، مدل مفهومی تحقیق تهیه و متناسب با آن پرسش‌نامه با طیف لیکرت تهیه و در اختیار جامعه نمونه قرار گرفت. برای تحلیل داده از ابزارهای SPSS, LISREL استفاده گردید.

جامعه آماری

برای جامعه آماری این پژوهش از تعدادی از نخبگان متخصص مرکز تحقیقات اینترنت اشیا ایران و جمعی از متخصصان فاوا و حوزه‌های سایبری نیروهای مسلح که آشنا به اینترنت اشیا هستند استفاده شده است که باتوجه‌به محدودیت خبرگی در این حوزه به‌صورت تمام‌شمار هدفمند به تعداد ۲۲ نفر انتخاب شده‌اند.

روایی و پایایی پرسش‌نامه

برای افزایش روایی و اعتبار پرسش‌نامه ابتدا تعدادی پرسش‌نامه بین جمعی از شرکت‌کنندگان توزیع گردید و کلیه ابهامات شرکت‌کنندگان دررابطه با سؤالات مشخص شد. بدین ترتیب تعدادی از سؤالات حذف و تعدادی دیگر جایگزین شد و در نهایت پس از شفاف شدن و رفع ابهامات، پرسش‌نامه نهایی تهیه و توزیع گردید. برای برآورد پایایی پرسش‌نامهٔ این پژوهش از فرمول ضریب آلفای کرونباخ استفاده شده است. ضریب آلفای محاسبه شده از طریق نرم‌افزار SPSS، ALPHA =۰٫۸۷ می‌باشد. بنابراین می‌توان گفت که پرسش‌نامهٔ نگاشت شده از پایایی کافی برخوردار است.

یافته‌ها: اطلاعات جمعیت‌شناختی

در این بخش، اطلاعات جمعیت‌شناختی مشتمل بر محل خدمت، جنسیت، درجه، میزان تحصیلات، سنوات خدمتی و سابقهٔ کار در حوزه اطلاعات و ارتباطات بیان می‌گردد که در قالب جدول و نمودار به توصیف این ویژگی می‌پردازیم.

تحصیلات شرکت‌کنندگان

جدول(۱) تحصیلات شرکت‌کنندگان

ردیف	تحصیلات	فراوانی	درصد
۱	کارشناسی	۳	۱۳٫۶
۲	کارشناسی ارشد	۱۴	۶۳٫۶
۳	دکتری	۵	۲۲٫۷
جمع کل		۲۲	۱۰۰

جدول فوق، تحصیلات شرکت‌کنندگان را نشان می‌دهد که کارشناسی ارشد با ۱۴ مورد (۶۳٫۶٪) بیشترین آمار و کارشناسی با ۳ مورد (۱۳٫۶٪) کمترین آمار را به خود اختصاص داده‌اند.

رشته تحصیلی شرکت‌کنندگان

جدول(۲) رشته تحصیلی شرکت‌کنندگان

ردیف	رشته تحصیلی	فراوانی	درصد
۱	حوزهٔ فناوری اطلاعات و سایبر	۱۲	۵۵
۲	حوزهٔ اطلاعاتی - امنیتی	۵	۲۲٫۷
۳	حوزهٔ مدیریتی	۳	۱۳٫۶
۴	سایر حوزه‌ها	۲	۹٫۱
جمع کل		۲۲	۱۰۰

جدول فوق، رشته تحصیلی شرکت‌کنندگان را نشان می‌دهد که حوزه سایبر با ۱۲ مورد (۵۵٪) بیشترین آمار و سایر حوزه‌ها با ۲ مورد (۹٫۱٪) کمترین آمار را به خود اختصاص داده‌اند.

تحلیل پرسش‌نامه

نرمالیتی توزیع داده‌ها

با استناد به انحراف کم مشاهدات در متغیرهای پژوهش، میزان کجی و کشیدگی متغیرهای پژوهش در بازه عددی ۲+ تا ۲- قرار گرفته است (برابر جدول ۵) فرض نرمالیتی توزیع داده‌ها تأیید می‌گردد و برای آزمون پژوهش از روش‌های آماری پارامتریک استفاده می‌شود.

جدول (۳) توصیف کجی و کشیدگی متغیرهای پژوهش

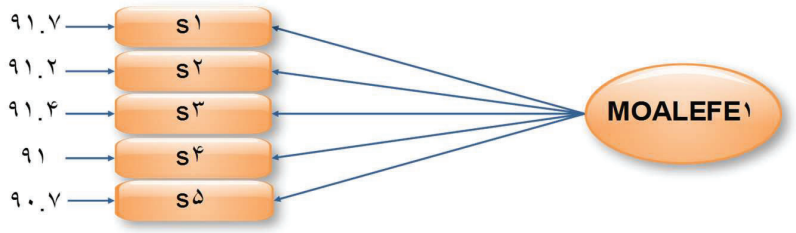
One-Sample Kolmogorov-Smirnov Test								
ابعاد		مؤلفه ۱	مؤلفه ۲	مؤلفه ۳	مؤلفه ۴	مؤلفه ۵	مؤلفه ۶	مؤلفه ۷
N		۲۲	۲۲	۲۲	۲۲	۲۲	۲۲	۲۲
Normal Parameters	Mean	۹۱٫۲	۸۹٫۳	۷۹٫۳	۸۷	۸۸٫۱	۸۶٫۳	۸۳٫۹
	Std. Deviation	۸٫۱۸	۱۱٫۱۹	۸٫۱۵	۱۱٫۲۳	۸٫۱۶	۱۱٫۱۴	۱۱٫۰۲
Most Extreme Differences	Absolute	.۳۴۶	.۳۴۱	.۳۴۲	.۳۵۱	.۳۴۶	.۳۴۱	.۳۷۱
Differences	Positive	.۲۶۵	.۲۸۲	.۲۶۸	.۲۸۵	.۲۶۱	.۲۸۱	.۲۶۹
Negative		-.۳۴۶	-.۳۴۱	-.۳۴۳	-.۳۴۲	-.۳۴۷	-.۳۴۴	-.۳۷۱
Kolmogorov-Smirnov Z		۴٫۵	۴٫۴۹	۴	۴٫۳۵	۴٫۴	۴٫۴۶	۴٫۳۳
Asymp. Sig.(2-tailed)		.۰۰۰	.۰۰۰	.۰۰۰	.۰۰۰	.۰۰۰	.۰۰۰	.۰۰۰
Test distribution is Normal								

مؤلفه اول: تحلیل و رتبه‌بندی مؤلفه‌ها و شاخص‌های مؤلفه اول یعنی گذرواژه‌های ضعیف، قابل حدس‌زدن یا رمزگذاری‌شدن با استفاده از آزمون فریدمن در جدول ۴ آورده شده است.

جدول (۴) تحلیل آزمون فریدمن (گذرواژه‌های ضعیف، قابل حدس‌زدن یا رمزگذاری‌شدن)

مؤلفه	میانگین بارعاملی	گزاره	رتبه	بار عاملی
مؤلفه اول: گذرواژه‌های ضعیف، قابل حدس‌زدن یا رمزگذاری‌شدن	٪۹۱,۲	۱. گذرواژه‌های پیش‌فرض ثابت و غیرقابل‌تغییر در اکثر تجهیزات اینترنت اشیا که توسط تولیدکنندگان در نظر گرفته می‌شود، از دلایل شکست و نفوذ به شبکه و تجهیزات است.	۱	۹۱,۷
		۲. اختصاص گذرواژه‌های ضعیف و قابل حدس (ذهنی و ماشینی از طریق حملات Brute force,...) در تجهیزات اینترنت اشیا، از دلایل شکست و نفوذ به شبکه و تجهیزات است.	۳	۹۱,۲
		۳. استفاده از گذرواژه‌های پیش‌فرض و عدم توجه به تغییر آن از دلایل شکست و نفوذ به شبکه است.	۲	۹۱,۴
		۴. ایجاد دسترسی از راه دور توسط سازندگان و شرکت‌های خدمات پشتیبانی با تعریف گذرواژه‌های ثابت، از دلایل شکست و نفوذ به تجهیزات و شبکه است.	۴	۹۱
		۵. احتمال آشکار شدن رمز عبور یا سایر داده‌های حساس در زمان برداشتن کارت حافظه برای خواندن محتوای آن.	۵	۹۰,۷

در ادامه تحلیل آماری مؤلفه اول تحقیق که شامل ۵ شاخص است، با استفاده از نرم‌افزار لیزرل انجام که برابر شکل ۳ است.



Chi-Square=۵۸۳.۴۲ Df=۲۲ P-valu=۰.۰۰ Rmsea=۰.۱۱۱

Normed Fit Index (NFI) =۹۵%

شکل(۳) تحلیل آماری مؤلفه اول تحقیق با استفاده از نرم‌افزار لیزرل

خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل‌قبولی برخوردار است؛ بنابراین گزاره گذرواژه‌های پیش‌فرض ثابت و غیرقابل‌تغییر در اکثر تجهیزات اینترنت اشیا که توسط تولیدکنندگان در نظر گرفته می‌شود، از دلایل شکست و نفوذ

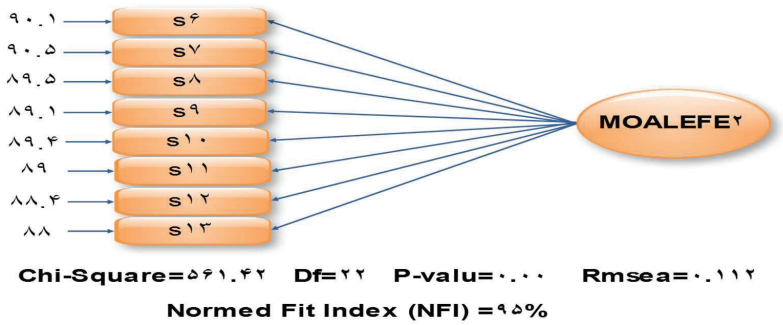
به شبکه و تجهیزات است. به‌عنوان مهم‌ترین گزاره در مؤلفه اول تحقیق مورد قبول واقع شده است

مؤلفه دوم: تحلیل و رتبه‌بندی مؤلفه‌ها و شاخص‌های مؤلفه دوم یعنی خدمات شبکه ناامن با استفاده از آزمون فریدمن در جدول ۵ آورده شده است.

جدول (۵) تحلیل آزمون فریدمن (خدمات شبکه ناامن)

مؤلفه	میانگین بار عاملی	گزاره	رتبه	بار عاملی
مؤلفه دوم: خدمات شبکه ناامن	٪۸۹,۳	۶. عدم نصب و به‌روزرسانی‌های تجهیزات امنیتی (آپدیت نرم‌افزار، نصب پچ‌های امنیتی و...) مرتبط با IPS/IDS,UTM,Firewall,...	۲	۹۰,۱
		۷. عدم تأمین محصولات امن تولید شده توسط تولیدکنندگان معتبر تجهیزات امنیتی اینترنت اشیا اعم از IPS/IDS,UTM,Firewall,... (خرید برندهای نامعتبر با دلایل مختلف مثل مدیریت هزینه و...)	۱	۹۰,۵
		۸. عدم انجام تنظیمات امنیتی مناسب مانند بستن پورت‌های غیرضروری و سرویس‌های آسیب‌پذیر مثل دسترسی از راه دور و...	۳	۸۹,۵
		۹. عدم داشتن شبکه مستقل و مجزا برای دستگاه‌های هوشمند و استفاده از سایر بسترهای عمومی مانند Wi-Fi عمومی.	۵	۸۹,۱
		۱۰. عدم استفاده از شبکه‌های LPWAN (شبکه‌های کم‌مصرف و کم‌توان ویژه اینترنت اشیا مثل LoRAWAN,SIXFOX) متناسب با پروژه خانه هوشمند به جهت مقیاس‌پذیری، مدیریت امنیت شبکه و...	۴	۸۹,۴
		۱۱. عدم وجود تجهیزات قوی(الگوریتم به‌روز امنیتی، رمزنگاری، و... در بازار مثل IPS/IDS,UTM,Firewall,... در حوزه شبکه‌های LPWAN در مقایسه با شبکه‌های سلولار، رایانه‌ای و... برای مقابله با حملات جدید.	۶	۸۹
		۱۲. عدم توجه و پیش‌بینی تجهیزات امنیتی در پروژه‌های اینترنت اشیا به جهت کاهش هزینه‌ها و یا عدم درک ضرورت مباحث امنیتی در حوزهٔ شبکه‌های LPWAN در مقایسه با شبکه‌های سلولار، رایانه‌ای و...	۸	۸۸,۴
		۱۳. خطرات مرتبط با زنجیره تأمین می‌تواند فرآیند تولید را در مراحل اولیه مختل کند و شناسایی نشده باقی بماند و به‌شدت بر امنیت تجهیزات اینترنت اشیا تأثیر بگذارد.	۷	۸۸,۸

در ادامه تحلیل آماری مؤلفه دوم تحقیق که شامل ۸ شاخص است، با استفاده از نرم‌افزار لیزرل انجام شده که برابر شکل ۴ است.



شکل(۴) تحلیل آماری مؤلفه دوم تحقیق با استفاده از نرم‌افزار لیزرل

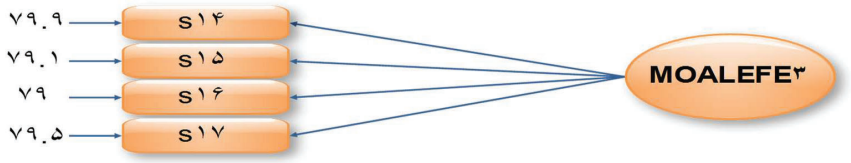
خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل قبولی برخوردار است؛ بنابراین گزاره عدم تأمین محصولات امن تولید شده توسط تولیدکنندگان معتبر تجهیزات امنیتی اینترنت اشیا اعم از IPS/IDS,UTM,Firewall,... (خرید برندهای نامعتبر با دلایل مختلف مثل مدیریت هزینه و...) به‌عنوان مهم‌ترین گزاره در مؤلفه دوم تحقیق مورد قبول واقع شده است.

مؤلفه سوم: تحلیل و رتبه‌بندی مؤلفه‌ها و شاخص‌های مؤلفه سوم یعنی اکوسیستم ناامن با استفاده از آزمون فریدمن در جدول ۶ آورده شده است.

جدول (۶) تحلیل آزمون فریدمن (واسط‌های اکوسیستم ناامن)

مؤلفه	میانگین بار عاملی	گزاره	رتبه	بار عاملی
مؤلفه سوم: واسط‌های اکوسیستم ناامن	٪۷۹,۳	۱۴. رابط‌های وب پایه (WEB BASE) و دارای تنظیمات امنیتی ضعیف و قابل هک از دلایل دسترسی به پیکربندی شبکه‌ها و تجهیزات اینترنت اشیا است.	۱	۷۹,۹
		۱۵. اپلیکیشن‌های موبایل پایه (mobile BASE) و دارای تنظیمات امنیتی ضعیف و قابل هک از دلایل دسترسی به پیکربندی تجهیزات اینترنت اشیا می‌باشد.	۳	۷۹,۱
		۱۶. استفاده از خدمات رایانش ابری (Cloud) از دلایل دسترسی به پیکربندی تجهیزات اینترنت اشیا می‌باشد.	۴	۷۹
		۱۷. استفاده از خدمات رابط تعاملی نرم‌افزاری (back-end API) از دلایل دسترسی به پیکربندی تجهیزات اینترنت اشیا می‌باشد.	۲	۷۹,۵

در ادامه تحلیل آماری مؤلفه سوم تحقیق که شامل ۴ شاخص است، با استفاده از نرم‌افزار لیزرل انجام که برابر شکل ۵ می‌باشد.



Chi-Square=۵۶۱.۴۲ Df=۲۲ P-valu=۰.۰۰ Rmsea=۰.۱۱۲

Normed Fit Index (NFI) =۹۵%

شکل (۵) تحلیل آماری مؤلفه سوم تحقیق با استفاده از نرم‌افزار لیزرل

خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل قبولی برخوردار است؛ بنابراین گزاره رابط‌های وب پایه[1] و دارای تنظیمات امنیتی ضعیف و قابل هک از دلایل دسترسی به پیکربندی شبکه‌ها و تجهیزات اینترنت اشیا می‌باشد. به‌عنوان مهم‌ترین گزاره در مؤلفه سوم تحقیق مورد قبول واقع شده است.

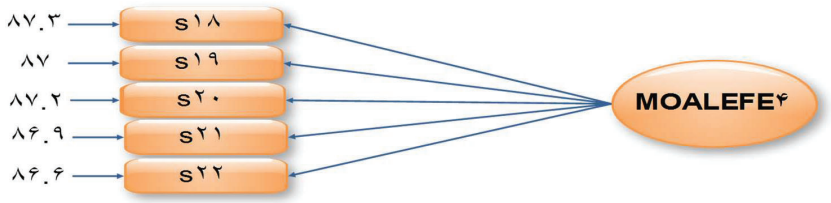
مؤلفه چهارم: تحلیل و رتبه‌بندی مؤلفه‌ها و شاخص‌های مؤلفه چهارم یعنی اکوسیستم ناامن با استفاده از آزمون فریدمن در جدول ۷ آورده شده است.

جدول (۷) تحلیل آزمون فریدمن (عدم وجود مکانیسم‌های به‌روزرسانی امن)

مؤلفه	میانگین بار عاملی	گزاره	رتبه	بار عاملی
مؤلفه چهارم: عدم وجود مکانیسم‌های به‌روزرسانی امن	٪۸۷	۱۸. عدم پیش‌بینی قابلیت احیا، بازیابی و بازگشت‌پذیری تنظیمات و خدمات امنیتی به قبل از وقوع حادثه برای استمرار عملکرد تجهیزات و شبکه اینترنت اشیا.	۱	۸۷,۳
		۱۹. عدم پیش‌بینی راه‌کارهای به‌روزرسانی و وصله‌های امنیتی (Patch) خودکار.	۳	۸۷
		۲۰. عدم استفاده از میان‌افزارهای (Firmware) امن و مطمئن در تجهیزات اینترنت اشیا	۲	۸۷,۲
		۲۱. عدم پیکربندی مناسب سیستم‌عامل‌های منبع‌باز لینوکس پایه (Linux Base) شخصی‌سازی شده در سامانه‌های نهفته اینترنت اشیا (Embedded system).	۴	۸۶,۹
		۲۲. استفاده از کدها و نرم‌افزارهای قدیمی و یا ارجاع به کتابخانه‌های ناامن در Git Hub ,... .	۵	۸۶,۶

در ادامه تحلیل آماری مؤلفه چهارم تحقیق که شامل ۵ شاخص است، با استفاده از نرم‌افزار لیزرل انجام که برابر شکل ۶ می‌باشد.

1. WEB BASE



Chi-Square=۴۸۱.۴۸ Df=۲۲ P-valu=۰.۰۰ Rmsea=۰.۱۱۵

Normed Fit Index (NFI) =۹۵%

شکل (۶) تحلیل آماری مؤلفه چهارم تحقیق با استفاده از نرم‌افزار لیزرل

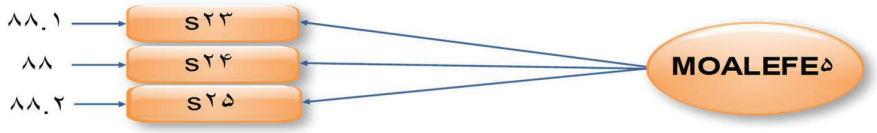
خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل قبولی برخوردار است؛ بنابراین گزاره عدم پیش‌بینی قابلیت احیا، بازیابی و بازگشت‌پذیری تنظیمات و خدمات امنیتی به قبل از وقوع حادثه برای استمرار عملکرد تجهیزات و شبکه اینترنت اشیا به‌عنوان مهم‌ترین گزاره در مؤلفه چهارم تحقیق مورد قبول واقع شده است.

مؤلفه پنجم: تحلیل و رتبه‌بندی مؤلفه‌ها و شاخص‌های مؤلفه چهارم یعنی حفاظت ناکافی از حریم خصوصی با استفاده از آزمون فریدمن در جدول ۸ آورده شده است.

جدول (۸) تحلیل آزمون فریدمن (حفاظت ناکافی از حریم خصوصی)

مؤلفه	میانگین بار عاملی	گزاره	رتبه	بار عاملی
مؤلفه پنجم: حفاظت ناکافی از حریم خصوصی	٪۸۸,۱	۲۳. ذخیره‌سازی ناامن داده‌های شخصی، پردازش یا افشای آن بدون اجازه کاربر	۲	۸۸,۱
		۲۴. جمع‌آوری و تجزیه‌وتحلیل غیرمجاز ترافیک شبکه اینترنت اشیا (حتی زمانی که این ترافیک رمزگذاری شده است) توسط خدمات‌دهندگان (Provider).	۳	۸۸
		۲۵. به‌خطر انداختن امنیت در دنیای فیزیکی با جمع‌آوری و حفظ بیش از حد داده‌های اینترنت اشیا.	۱	۸۸,۲

در ادامه تحلیل آماری مؤلفه پنجم تحقیق که شامل ۳ شاخص است، با استفاده از نرم‌افزار لیزرل انجام که برابر شکل ۷ است



شکل (۷) تحلیل آماری مؤلفه پنجم تحقیق با استفاده از نرم‌افزار لیزرل

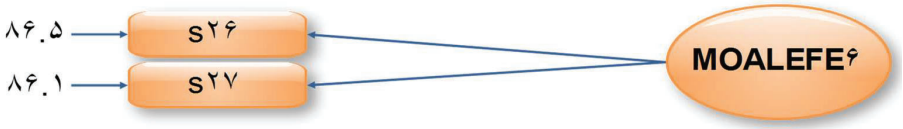
خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل قبولی برخوردار است؛ بنابراین گزاره به‌خطر انداختن امنیت در دنیای فیزیکی با جمع‌آوری و حفظ بیش از حد داده‌های اینترنت اشیا به‌عنوان مهم‌ترین گزاره در مؤلفه پنجم تحقیق مورد قبول واقع شده است.

مؤلفه ششم: تحلیل و رتبه‌بندی مؤلفه‌ها و شاخص‌های مؤلفه چهارم یعنی انتقال و ذخیره‌سازی ناامن داده با استفاده از آزمون فریدمن در جدول ۹ آورده شده است.

جدول (۹) تحلیل آزمون فریدمن (انتقال و ذخیره‌سازی ناامن داده)

مؤلفه	میانگین بار عاملی	گزاره	رتبه	بار عاملی
مؤلفه ششم: انتقال و ذخیره‌سازی ناامن داده	٪۸۶,۳	۲۶. تأثیر عدم طبقه‌بندی داده‌ها و مدیریت صحیح اطلاعات حساس در حفظ امنیت داده‌های ذخیره شده تجهیزات اینترنت اشیا	۱	۸۶,۵
		۲۷. میزان آسیب‌پذیر دستگاه‌های هوشمند اگر رمزگذاری وجود نداشته باشد یا اگر رمزگذاری داده‌ها به‌طور دقیق اجرا نشود.	۲	۸۶,۱

در ادامه تحلیل آماری مؤلفه ششم تحقیق که شامل ۲ شاخص است، با استفاده از نرم‌افزار لیزرل انجام که برابر شکل ۸ است



شکل (۸) تحلیل آماری مؤلفه ششم تحقیق با استفاده از نرم‌افزار لیزرل

خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از

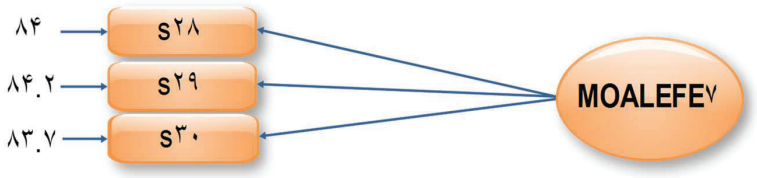
برازش قابل قبولی برخوردار است؛ بنابراین گزاره تأثیر عدم طبقه‌بندی داده‌ها و مدیریت صحیح اطلاعات حساس، در حفظ امنیت داده‌های ذخیره شده تجهیزات اینترنت اشیا به‌عنوان مهم‌ترین گزاره در مؤلفه ششم تحقیق مورد قبول واقع شده است.

مؤلفه هفتم: تحلیل و رتبه‌بندی مؤلفه‌ها و شاخص‌های مؤلفه چهارم یعنی عدم وجود مدیریت دستگاه با استفاده از آزمون فریدمن در جدول ۱۰ آورده شده است.

جدول (۱۰) تحلیل آزمون فریدمن (عدم وجود مدیریت دستگاه)

مؤلفه	میانگین بار عاملی	گزاره	رتبه	بار عاملی
مؤلفه هفتم: عدم وجود مدیریت دستگاه	٪۸۳,۹	۲۸. تأثیر عدم دانستن دارایی‌های سیستم مدیریت روش‌مند در شبکه تعامل تجهیزات اینترنت اشیا.	۲	۸۴
		۲۹. عدم مدیریت مؤثر دستگاه‌های اینترنت اشیا (مانند تکیه بر روش‌های قدیمی مانند ردیابی دارایی با استفاده از صفحات گسترده اکسل).	۱	۸۴,۲
		۳۰. عدم استفاده از بوتامن، و تأثیر آن بر اعتبار سیستم عامل و اجرای نرم‌افزارهای غیرقابل اعتماد.	۳	۸۳,۷

در ادامه تحلیل آماری مؤلفه هفتم تحقیق که شامل ۳ شاخص است، با استفاده از نرم‌افزار لیزرل انجام که برابر شکل ۹ می‌باشد.



Chi-Square=۴۸۱.۴۸ Df=۲۲ P-valu=۰.۰۰ Rmsea=۰.۱۱۵

Normed Fit Index (NFI) =۹۵%

شکل (۹) تحلیل آماری مؤلفه هفتم تحقیق با استفاده از نرم‌افزار لیزرل

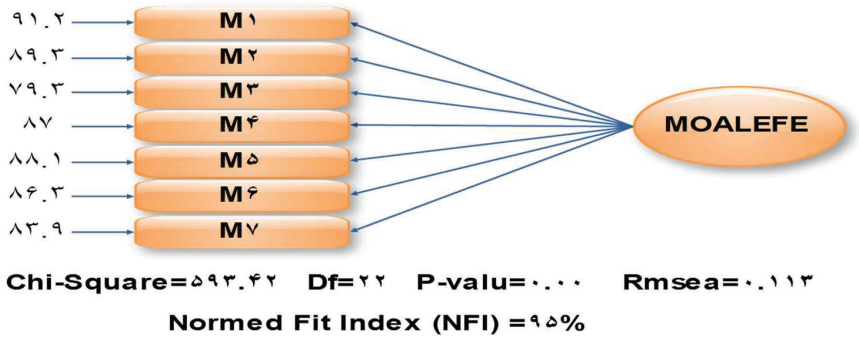
خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل قبولی برخوردار می‌باشد؛ بنابراین گزاره عدم مدیریت مؤثر دستگاه‌های اینترنت اشیا (مانند تکیه بر روش‌های قدیمی مانند ردیابی دارایی با استفاده از صفحات گسترده اکسل) به‌عنوان مهم‌ترین گزاره در مؤلفه هفتم تحقیق مورد قبول واقع شده است.

جمع‌بندی نتایج و تجزیه‌وتحلیل

برابر روش پیش‌گفته (روند تحلیل مراحل تحلیل ۷ گانه)، مدل معادلات ساختاری تحقیق تحت عنوان ارائه چارچوب بومی ارزیابی امنیت اینترنت اشیا در اماکن هوشمند نیروهای مسلح با استفاده از تهیه پرسش‌نامه و جمع‌آوری نظر نخبگان حوزه اینترنت اشیا و تحلیل فریدمن برای پاسخ به یک سؤال اصلی طرح شده با هفت مؤلفه برابر جدول ۱۳ و تحلیل آماری آن با نرم‌افزار لیزرل برابر شکل ۱۰ است.

جدول (۶) رتبه‌ای (فریدمن) مؤلفه‌های تحقیق با توجه به بار عاملی

ردیف	مؤلفه	بار عاملی	رتبه
۱	مؤلفه گذرواژه‌های ضعیف، قابل حدس‌زدن یا رمزگذاری شده	۹۱,۲	۱
۲	مؤلفه خدمات شبکه ناامن	۸۹,۳	۲
۳	مؤلفه واسط‌های اکوسیستم ناامن	۷۹,۳	۷
۴	مؤلفه عدم وجود مکانیسم‌های به‌روزرسانی امن	۸۷	۴
۵	مؤلفه حفاظت ناکافی از حریم خصوصی	۸۸,۱	۳
۶	مؤلفه انتقال و ذخیره‌سازی ناامن داده	۸۶,۳	۵
۷	مولفه عدم وجود مدیریت دستگاه	۸۳,۹	۶
میانگین کلی		٪۸۶,۴	



شکل (۱۳) تحلیل آماری هفت مؤلفه تحقیق با استفاده از نرم‌افزار لیزول

خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل قبولی برخوردار است؛ بنابراین مؤلفه گذرواژه‌های ضعیف، قابل حدس‌زدن یا رمزگذاری شده به‌عنوان مهم‌ترین بعد مورد قبول واقع شده است.

پیشنهادها

الف) پیشنهادها برای متولیان اجرایی:

۱- در خرید و تأمین تجهیزات اینترنت اشیا از تجهیزاتی که رمز پیش‌فرض آن غیرقابل تغییر و ثابت می‌باشد اجتناب گردد.

۲- تأمین‌کنندگان امنیت و مراقبت تجهیزات اینترنت اشیا به‌محض نصب و راه‌اندازی، گذرواژه‌ای پیش‌فرض را که بیشتر بسیار ساده هستند تغییر داده و از گذرواژه‌های قوی که شامل حداقل ۸ کاراکتر، حروف کوچک و بزرگ، اعداد و علائم و.. باشد، استفاده نمایند تا از حملات BRUTE FORCE,... آسیب کمتری وارد شود و تا حدودی جلوگیری نمایند.

۳-کارشناسان نصب و راه‌اندازی به‌محض نصب تجهیزات اینترنت اشیا، دسترسی‌های از راه دور تجهیزات را غیرفعال نمایند تا راه‌های نفوذ کاهش یابند.

۴- به‌محض نصب تجهیزات اینترنت اشیا آخرین آپدیت‌های نرم‌افزار و پچ‌های امنیتی (اعم از IPS/ IDS, UTM, FIREWALL,...) ارائه شده توسط شرکت سازنده در دستگاه بروز رسانی گردد.

۵- حتماً از شرکت‌های معتبر که دارای استانداردهای روز دنیا می‌باشند تجهیزات خریداری گردد

۶- حتی‌الامکان از شبکه‌های مستقل و امن برای ایجاد ارتباط تجهیزات با بخش‌های کنترلی استفاده گردد.

۷- بحث امنیت زنجیره تأمین بسیار مورد توجه قرار گرفته و توسط مراجع امنیتی (به‌ویژه اماکن نیروهای مسلح) رصد و پایش شود.

۸- باتوجه‌به گستردگی خانه‌های هوشمند و افزایش مشکلات و جرائم و تخلفات در این حوزه، ساختار و قوانینی در متناسب با جرائم نوظهور این حوزه در سطح نیروهای مسلح ایجاد گردد.

۹- باتوجه به اهمیت هوشمندسازی در نیروهای مسلح، قطعاً اماکن نیروهای مسلح همانند یک خانهٔ هوشمند می‌بایست به تجهیزات اینترنت اشیا مجهز و هوشمند شوند. دراین‌خصوص تهیه سازوکارهای تأمین و پایش امنیت ضروری می‌باشد.

ب) پیشنهاد برای محققان:

- تحقیق در خصوص لایه‌های نرم‌افزاری اینترنت اشیا و چگونگی امنیت آن
- تحقیق در خصوص فناوری‌های همگرا با اینترنت اشیا و چالش‌های امنیتی آن

فهرست منابع

منابع فارسی

۱. ارکیان، حمیدرضا و دیگران (۲۰۱۶)، امنیت و حریم خصوصی در اینترنت اشیا ، دوفصل‌نامه علمی ترویجی منادی امنیت فضای تولید و تبادل اطلاعات.

۲. هاشمی، ستار و شهروز ستوده (۱۳۹۷)، ارائه چارچوبی برای ارتقای امنیت خانه‌های هوشمند مبتنی بر اینترنت اشیا با استفاده از معماری مرجع، فصلنامه فناوری اطلاعات و ارتباطات ایران.

۳. ذوالفقاری‌پور، لیلی و احسان طیرانی‌راد (۱۳۹۶)، یک طرح احراز هویت انتخابی برای سیستم خانه هوشمند مبتنی بر IoT، سومین کنفرانس حوادث و آسیب‌پذیری‌های امنیت فضای تبادل اطلاعات، زاهدان: ۷۴۹۱۶۳/HTTPS://CIVILICA.COM/DOC

۴. بهشتی آتشگاه، محمد و دیگران (۱۳۹۷)، مفاهیم امنیتی و چالش های اینترنت نظامی اشیا، (IoT) با تمرکز بر مکانیسم MIoT-USA. ، فصلنامه علمی – پژوهشی فرماندهی و کنترل‌ریال تهران: دانشگاه صنعتی مالک اشتر.

۵. اسدنجفی، نرگس و مهدی ملامطلبی (۱۳۹۹)، بهبود احراز هویت در خانه هوشمند مبتنی بر رمز یکبار مصرف و رمزنگاری منحنی بیضوی، فصلنامه علمی علوم و فناوری‌های پدافند نوین، دانشگاه آزاد اسلامی واحد بویین زهرا.

۶. فرجامی، یعقوب و سیدمرتضی پورنقی (۱۳۹۷)، چارچوبی برای ممانعت از ورود تبلیغات هرزنامه به دستگاه‌های سیار هوشمند در شبکه IoT. پدافند الکترونیکی و سایبری.

۷. بهشتی آتشگاه، محمد و عارف بیات (۱۳۹۷)، مفاهیم و چالش‌های امنیتی اینترنت اشیای نظامی با محوریت مکانیزم MIoT ایالات متحده آمریکا، تهران: فصلنامه علمی- پژوهشی فرماندهی و کنترل.

۸. محمد بهشتی آتشگاه و دیگران (۱۳۹۶)، یک طرح امضای مبتنی بر شناسه با تأییدکننده مشخص جدید به همراه کاربرد آن در خانه‌های هوشمند، فصلنامه پدافند الکترونیکی و سایبری، ش۴.

۹. نسیمی راد، علی (۱۳۹۴)، اینترنت اشیا یکپارچگی فناوری‌ها برای محیط‌های هوشمند.

۱۰. حسین پور، کسرا (۱۳۹۹)، اینترنت اشیا و راه‌های محافظت از آن در برابر نفوذگران، https://ashnasecure.com

۱۱. حمیدی فشکی، فاطمه و دیگران (۱۳۹۸)، ارائه یک طرح احراز هویت امن با هدف حفظ حریم خصوصی در سیستم خانه هوشمند، چهارمین کنفرانس بین المللی ترکیبات، رمزنگاری، علوم کامپیوتر و محاسبات، تهران: دانشگاه علم و صنعت ایران.

منابع لاتین

1. Oliveira، A. J. M. D. ((2019). IOT SECURITY ASSESSMENT IoT Security Assessment in an IoT Smart City Scenario.

2.Geneiatakis، D.، Kounelis، I.، Neisse، R.، Nai-Fovino، I.، Steri، G.، & Baldini، G. (2017، May). Security and privacy issues for a smart home based on the Internet of Things. In, the 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).

3.Hassan، W. H. (2019) Current Research on Internet of Things (IoT) Security: A Survey. computer networks.

4. Dorri، A.، Kanhere، S. S.، Jurdak، R.، & Gauravaram، P. (March 2017)Blockchain for Internet of Things Security and Privacy: A Case Study of a Smart Home. In 2017, the International Conference on Computer Workshops and Pervasive Communication (PerCom Workshops.

5.Agarwal، K.، Agarwal، A.، & Misra، G. (December2019)I-SMAC) Performance review and analysis in wireless smart home and home automation using iot. In 2019, the third I-SMAC International Conference (Internet of Things in Social Affairs, Mobile, Analytics and Cloud).

6. García, L., Parra, L., Jimenez, J. M., Lloret, J., & Lorenz, P. (2020). IoT-based smart irrigation systems: An overview on the recent trends on sensors and IoT systems for irrigation in precision agriculture. Sensors, 20(4), 1042.

7. Su, Y., Lu, X., Zhao, Y., Huang, L., & Du, X. (2019). Cooperative communications with relay selection based on deep reinforcement learning in wireless sensor networks. IEEE Sensors Journal, 19(20), 9561-9569.

8. Fahmideh, M., & Zowghi, D. (2020). An exploration of IoT platform development. Information Systems , 87, 101409.

9. Albany, M., Alsahafi, E., Alruwili, I., & Elkhediri, S. (2022). A review: Secure Internet of thing System for Smart Houses. Procedia Computer Science, 201, 437-444.

10. Tange, K., De Donno, M., Fafoutis, X., & Dragoni, N. (2020). A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities. IEEE Communications Surveys & Tutorials, 22(4), 2489-2520.

11. Ali، B.، & Awad، A. I. (2018).Assessing cyber vulnerability and physical security for smart homes based on the Internet of (2019 Armando José Martins de Oliveira)IOT SECURITY ASSESSMENT IoT Security Assessment in an IoT Smart City Scenario.

12. Shouran، Z.، Ashari، A.، & Priyambodo،T. (2019)Safe and efficient smart home architecture of the Internet of Things based on cloud computing and blockchain technology.

13. Ge، M.، Hong، J. B.، Guttmann، W.، & Kim، D. S. (2017)Iman and efficient protocol for route optimization in Internet networks of smart home appliances based on PMIPv6.

14. Shouran، Z.، Ashari، A.، & Priyambodo،T. (2019)An advanced secure network architecture for detecting security threats in a smart home.

15. Duan, X., Ge, M., Le, T. H. M., Ullah, F., Gao, S., Lu, X., & Babar, M. A. (2021, December). Automated Security Assessment for the Internet of Things. In 2021 IEEE 26th Pacific Rim International Symposium on Dependable Computing (PRDC) (pp. 47-56). IEEE.

16. Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). Low power wide area networks: An overview. ieee communications surveys & tutorials, 19(2), 855-873.