

ارائه چارچوبی برای ارتقاء امنیت خانه‌های هوشمند مبتنی بر

اینترنت اشیاء با استفاده از معماری مرجع IoT-A

* ستار هاشمی

** شهروز ستوده

* دانشیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه شیراز، ایران

** پژوهشگر، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

تاریخ دریافت: ۱۳۹۸/۰۹/۲۳

تاریخ پذیرش: ۱۳۹۸/۱۱/۰۲

چکیده

امروزه خانه هوشمند به‌عنوان یکی از کاربردهای اصلی و رو به رشد اینترنت اشیاء محسوب می‌شود که راحتی، امنیت، کاهش مصرف انرژی و هزینه‌های زندگی را به همراه دارد. در کنار مزایا و محاسنی که این فناوری به ارمغان آورده است مسئله امنیت و حریم خصوصی به یکی از نگرانی‌های عمده تبدیل شده است که نیاز به توجه جدی دارد. معماری مرجع IoT-A باهدف بررسی پروتکل‌ها و منابع موجود، حصول اطمینان از سازگاری اشیاء و پروتکل‌های ارتباطی و همچنین ارائه راه‌کاری جامع برای کاربردهای مختلف اینترنت اشیاء پایه‌گذاری شده است. این مقاله باهدف قرار دادن چالش امنیت در اینترنت اشیاء و خانه‌های هوشمند، با استفاده از معماری مرجع IoT-A سعی در ارائه یک چارچوب کلی جهت بهبود امنیت در کلیه سطوح طراحی، اجرا و استفاده از تجهیزات و پروتکل‌ها دارد. در این مقاله از اصطلاح چارچوب امنیتی برای شناسایی مجموعه فناوری‌ها، سازوکارها، نرم‌افزارها و مؤلفه‌های موردنیاز برای تأمین مجموعه‌ای از نیازهای امنیتی استفاده شده است. این مقاله پس از بررسی و نگاشت آسیب‌پذیری‌ها و تهدیدات در مدل کاربردی معماری، یک چارچوب امنیتی بهبودیافته نسبت به چارچوب استاندارد معماری مرجع ارائه می‌کند. بر اساس ارزیابی نظری انجام‌شده، چارچوب جدید که با اضافه شدن دو مؤلفه مدیریت تهدیدات و آسیب‌پذیری‌ها و مدیریت زمینه و انجام برخی تغییرات در مؤلفه صدور مجوز شکل‌گرفته، الزامات امنیتی خانه‌های هوشمند را تا حد قابل قبولی برآورده کرده و به میزان مناسبی درجه امنیت و حفظ حریم خصوصی خانه هوشمند مبتنی بر معماری اینترنت اشیاء IoT-A را ارتقاء می‌بخشد.

واژه‌های کلیدی: خانه هوشمند، اینترنت اشیاء، امنیت و حریم خصوصی، معماری امنیت.

۱- مقدمه

چیزی در هر زمان و مکان فراهم می‌آورد [۱]. این فن‌آوری شامل اشیاء و فن‌آوری‌های گوناگون مانند حسگرها، ماشین به ماشین، میان‌افزار، داده‌های بزرگ، پردازش ابری، پردازش مه است که در یک شبکه جهانی کار می‌کنند [۲-۱۱]. اینترنت اشیاء یک الگوی تحول‌گرا و در حال تحول است که

اینترنت اشیاء، به امکان برقراری ارتباط تمام اشیاء با یکدیگر و با انسان‌ها، به همراه شناسایی و کشف آن‌ها تحت یک شبکه یکپارچه با شناسه مشخص اطلاق شده و امکان برقراری ارتباط هرکسی، در هر زمان و مکان را به هر

¹ Anyone, Anytime, Anywhere

ممکن است در کنار مزایای زیادی که ارائه می‌کنند دارای چالش‌ها و مشکلات امنیتی نیز باشند که البته این امر دور از ذهن نیست [۱۸]. موضوع امنیت در یک‌خانه هوشمند از مسائل کلیدی است که قبل از انتخاب سگویی مناسب جهت پیاده‌سازی آن مطرح می‌گردد و اساساً ارائه یک سگویی ناامن می‌تواند بستر مناسبی را برای وقوع حملاتی از قبیل شنود، استراق سمع، مردی در میان و حمله بازپخش ایجاد کند [۱۹]؛ بنابراین یکی از مهم‌ترین چالش‌ها در به‌کارگیری این فناوری، پذیرش معماری است که دارای راه‌حل‌های امنیتی مناسبی بوده و نه تنها مسائل مربوط به ارتباط و عملکرد سیستم‌ها را پوشش دهد، بلکه قادر به تأمین امنیت کاربران نیز باشد. این مقاله به ارائه‌ی یک چارچوب مناسب برای ارتقاء امنیت، حفظ حریم خصوصی و ایجاد اعتماد کاربران در خانه‌های هوشمند می‌پردازد.

این مقاله در ۴ بخش ارائه‌شده است. بخش ۲ به بررسی مبانی نظری پژوهش در حوزه اینترنت اشیا، خانه هوشمند، امنیت، معماری‌ها و موضوعات امنیتی مرتبط با پژوهش می‌پردازد. در بخش ۳ روش پژوهش در قالب ارائه و بررسی راهکار پیشنهادی مقاله مورد بحث قرار می‌گیرد و در نهایت بخش ۴ به تحلیل راهکارهای پیشنهادی و بررسی نتایج اختصاص یافته است.

۲- مبانی نظری پژوهش

این بخش به ارائه مبانی نظری پژوهش در مورد چالش‌ها و تهدیدات امنیتی خانه هوشمند مبتنی بر اینترنت اشیا خواهد پرداخت.

۲-۱- خانه هوشمند مبتنی بر اینترنت اشیا^۲

امروزه خانه‌ها با استفاده از فناوری‌های هوشمند به صورت خودکار درآمده و توانایی برطرف ساختن نیازهای ساکنین از جمله راحتی، امنیت و حفظ حریم خصوصی را داشته و نسبت به نیازهای انسان مدرن و محیط زندگی او حساس و پاسخگوست [۲۰، ۲۱]. کاربرد اصلی خودکارسازی در محیط یک‌خانه هوشمند، کنترل نور، حرارت و تهویه هوا،

در چندین حوزه کاربرد از جمله خانه‌های هوشمند، محیط هوشمند، مراقبت‌های بهداشتی از راه دور مورد توجه قرار گرفته است [۱۲]. این حوزه‌های کاربردی همگی با استفاده از فناوری اینترنت اشیا می‌توانند انسان‌ها را در جهت بهبود سلامت، کاهش مصرف انرژی و ایمنی یاری رسانند [۱۳]. شرایط جدید محیط و ویژگی‌های مختلف دستگاه‌ها، به‌ویژه سیستم‌های هوشمند در منازل، سبب شده است تا امنیت در به‌کارگیری این فناوری به‌طور ویژه مورد توجه قرار گیرد و معماری‌ها و سگوه‌های متعددی برای آن ارائه شود. به‌علاوه، حجم زیادی از ارتباط بین دستگاه‌ها به‌صورت ماشین به ماشین بوده و این بدان معنی است که بر روی این ارتباط کنترل چندانی نخواهیم داشت [۱۴]. همچنین به دلیل وجود بحث مالکیت اشیا و همین‌طور حفظ حریم خصوصی افراد، توجه به نکات امنیتی مرتبط با شناسایی و کشف، دسترس‌پذیری، کنترل دسترسی، حریم خصوصی و اعتماد نیز در مبحث اشیا هوشمند از اهمیت بیشتری برخوردار خواهد بود [۱۵]. سوءاستفاده از فناوری اینترنت اشیا در خانه هوشمند، امکان به خطر انداختن جان انسان‌ها را در پی خواهد داشت؛ بنابراین، امنیت یک مبحث کلیدی در برابر اجرایی شدن این فناوری است که مستلزم تحقیقات گسترده است. تضمین ایمنی زندگی انسان‌ها، جلوگیری از زنجیره حوادث نامطلوب، در دسترس بودن اشیا، رمزنگاری و فناوری‌های حفاظت، محرمانگی و یکپارچگی اطلاعات، انکارناپذیری، سازگاری اطلاعات و سطوح امنیتی آن‌ها در سیستم‌های مختلف، احراز هویت اشیا و اشخاص با استفاده از چند عامل مانند رمز عبور، مکان و بیومتریک، مدل‌های مختلف برای اعتماد و احراز هویت غیر مرکزی از جمله این نیازها است [۱۶]. با این وجود، با افزایش توسعه در برخی از دستگاه‌های خانگی متصل به اینترنت، ریسک‌های امنیتی و حریم خصوصی به‌طور هم‌زمان در حال افزایش است [۱۷]. پنج مشخصه کلی شامل خودکارسازی، چندمنظوره بودن، انطباق، تعامل، بهره‌وری می‌بایست در یک‌خانه هوشمند فراهم گردد [۱۷]. با توجه به اینکه امکان اتصال به اینترنت جهت ارائه خدمات بهتر و هوشمندانه‌تر خانه‌های هوشمند امروزه بسیار مورد توجه است و فناوری‌های به‌کاررفته در این خانه‌ها

² Internet of things based smart home

را در این حوزه تحت پوشش قرار دهد [۲۶، ۲۷]. تحقیقات متعددی به منظور افزایش امنیت در اینترنت اشیا صورت انجام شده است؛ اما مواردی همچون مکانیسم‌های مناسب جهت رمزنگاری، پروتکل‌های شبکه، مدیریت داده و شناسه‌ها، حریم خصوصی کاربران و معماری‌های قابل اعتماد هنوز قابل بحث می‌باشند [۲۸-۳۰]. طبق تحقیقات انجام شده در مورد امنیت خانه هوشمند، حریم خصوصی، اعتماد، امنیت و ارتباطات از عمده چالش‌های تأثیرگذار بر خانه هوشمند هستند [۲۵]. این موارد در جدول ۱ قابل مشاهده است.

مانیتورینگ، ایجاد امنیت و محافظت، پزشکی از راه دور، کنترل مصرف انرژی، کنترل عوامل محیطی بوده و دسترسی به اطلاعات موردنیاز نیز از کاربردهای دیگر آن است. ورود خانه هوشمند به بحث اینترنت اشیا به معنی سپردن امر ذخیره‌سازی، پردازش و تحلیل داده‌ها به امکانات عرضه شده در فضای مجازی است که موجب ایجاد چالش‌های امنیتی جدیدی شده است [۲۲-۲۵].

۲-۲- امنیت^۳، چالش‌ها^۴ و تهدیدات^۵

امنیت و حریم خصوصی از مهم‌ترین چالش‌ها برای استفاده از اینترنت اشیا در خانه‌های هوشمند است و معماری مناسب امنیتی باید چرخه حیات و قابلیت‌های اینترنت اشیا

جدول ۱- چالش‌های اینترنت اشیا در حوزه خانه هوشمند

عنوان چالش	مراجع	توضیح
حریم خصوصی	[۳۴-۳۱، ۲۵]	حفظ حریم خصوصی و مسائل وابسته مانند امنیت اطلاعات و افشای اطلاعات و داده‌ها
ارتباطات	[۳۶، ۳۵، ۳۳، ۲۵]	استحکام، پایداری امنیت و پروتکل‌های زیاد ارتباطی و ناهمگونی این ارتباطات
ایمنی	[۳۷، ۳۵، ۳۱]	ایمنی فیزیکی اشیا، دسترسی فیزیکی و قابلیت خود ایمنی
شبکه و امنیت	[۳۳، ۳۱، ۲۵]	شبکه به‌واسطه ارتباطات و گستردگی و تنوع ارتباطات نیز از نگرانی‌ها است
امنیت	[۳۴، ۳۲، ۳۱]	حفظ امنیت به‌صورت مستقل از چالش‌های اینترنت اشیا است
اعتماد	[۳۵، ۳۳، ۲۵]	مکانیسم‌های اعتماد
محرمانگی و رمزنگاری	[۳۳، ۳۱، ۲۵]	حفظ محرمانگی و راهکارهای وابسته مانند رمزنگاری و محدودیت‌های اشیا چالش‌هایی را ایجاد نموده است
امنیت اطلاعات	[۳۳، ۳۱]	افزایش حجم اطلاعات، تعداد اشیا و ناهمگونی‌ها، حفظ امنیت اطلاعات را در برابر اینترنت اشیا قرار داده است
نام‌گذاری و مدیریت هویت	[۳۶، ۳۱]	احراز هویت‌ها، شناسایی و اشیا و استاندارد گذاری در این زمینه از نگرانی‌های اینترنت اشیا است.
تعداد زیاد اشیا	[۳۶، ۳۵، ۳۳]	تعدد اشیا و ارتباطات گوناگون و داده‌های زیاد تولید شده و پردازش و کنترل حجم اطلاعات و ارتباطات نیز جز چالش‌ها است
مصرف انرژی	[۳۵، ۳۴، ۳۱]	توسعه اینترنت اشیا موجب افزایش مصرف انرژی برق و بالا رفتن هزینه و تأثیر بر روی محیط خواهد شد که ارائه راهکارهای کنترل مصرف انرژی نیز از چالش‌های اینترنت اشیا است
داده بزرگ و ابر	[۳۸، ۳۳، ۲۵]	افزایش حجم داده‌های تولید شده و راهکارهای انتقال آن و ایجاد داده‌های بزرگ، نگرانی‌های در جمع‌آوری، نگهداری و کنترل پردازش این نوع داده‌ها را ایجاد کرده است
قابلیت کار دستگاه‌ها و اشیا با یکدیگر	[۳۶، ۳۳، ۲۵]	جهت برقراری ارتباطات و حداکثر بهره‌وری از اینترنت اشیا با توجه به گسترش تعداد و ناهمگونی اشیا قابلیت کار با اشیا متنوع را تحت تأثیر قرار داده است
ذخیره‌سازی	[۳۲، ۳۱]	افزایش حجم داده نگرانی ذخیره‌سازی در حجم داده‌های تولید شده را در برداشته
ناهمگونی اشیا	[۳۵، ۳۳، ۳۱]	افزایش تعداد ناهمگونی‌ها و نیاز به برقراری ارتباطات و انواع مختلف داده ایجاد شده و مدیریت و پردازش آن‌ها

³ Security
⁴ Challenge
⁵ Threat

پرداخته می‌شود و ضمن انجام مقایسه بین قابلیت‌های آن‌ها، معماری مناسب برای ادامه کار پیشنهاد می‌شود. نگاشت آسیب‌پذیری‌ها و تهدیدات امنیتی بر اجزاء معماری انتخاب شده انجام شده و مجموعه نیازها جهت ارتقاء امنیت معماری در حوزه کاربردی خانه هوشمند مشخص می‌شود. با تغییر و تکمیل چارچوب امنیتی معماری انتخاب‌شده، راهکاری برای ارتقاء امنیت خانه هوشمند ارائه خواهد شد (شکل ۱).



شکل ۱- روش تحقیق

۳-۱- پیشنهاد معماری مناسب

مراکز تحقیقاتی مختلف اقدام به ارائه راهکارهای جامعی با عنوان معماری‌های مرجع برای حل چالش‌های موجود در زمینه اینترنت اشیا نموده‌اند. معماری Wso2 باهدف فراهم نمودن خدمات ابری، معماری مرجع Korean باهدف ورود این فناوری به عرصه صنعت و معماری مرجع Chinese برای استانداردسازی این حوزه در کشور چین ارائه شده است [۴۹، ۴۸].

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 در اتحادیه اروپا پایه‌گذاری شد. این معماری شامل چند زیر مدل است که برای پیشبرد اهداف

آسیب‌پذیری‌های^۶ موجود در اینترنت اشیا و خانه هوشمند موجب بروز تهدیدات متنوعی می‌شوند. برخی از این تهدیدات بر اساس پژوهش‌های انجام‌شده در جدول ۲ معرفی شده است.

جدول ۲- معرفی تهدیدات

ردیف	عنوان تهدید	مراجع
۱	دست‌کاری ترافیک ^۷	[۴۳-۳۹]
۲	جعل هویت	[۴۴، ۴۳، ۴۱، ۴۰]
۳	استراق سمع	[۴۵-۴۱، ۳۹]
۴	بلاک کانال ^۸ و جَمینگ ^۹	[۴۵، ۴۳، ۴۲، ۴۰]
۵	تحلیل ترافیک ^{۱۰}	[۴۳-۳۹]
۶	ممانعت از سرویس	[۴۶-۴۳، ۴۱، ۳۹]
۷	باچ افزارها ^{۱۱}	[۴۳]
۸	برنامه‌های تقلبی کنترل گوشی	[۴۳، ۳۹]
۹	فردی در میان ^{۱۲}	[۴۵، ۴۳، ۳۹]
۱۰	جعل	[۴۳، ۳۹]
۱۱	حمله اکتشافی ^{۱۳}	[۴۷، ۴۳]
۱۲	کدک‌های مخرب ^{۱۴}	[۴۴، ۴۳، ۳۹]
۱۳	حمله بازتاب ^{۱۵}	[۴۳، ۴۰، ۳۹]
۱۴	تکه‌تکه سازی ^{۱۶}	[۴۷، ۴۴، ۴۳، ۳۹]
۱۵	حمله تکثیر ^{۱۷}	[۴۳، ۳۹]

۳- روش پژوهش

در قسمت قبل به معرفی چالش‌ها، آسیب‌پذیری‌ها و تهدیدات امنیتی اینترنت اشیا در حوزه کاربردی خانه هوشمند پرداخته شد. در ادامه به معرفی معماری‌های مرجع

⁶ Vulnerability

⁷ Tampering

⁸ Block Channel

⁹ Jamming

¹⁰ Traffic Analyzing

¹¹ RansomWare

¹² Man in the middle

¹³ Reconnaissance

¹⁴ Malicious Codec

¹⁵ Replay

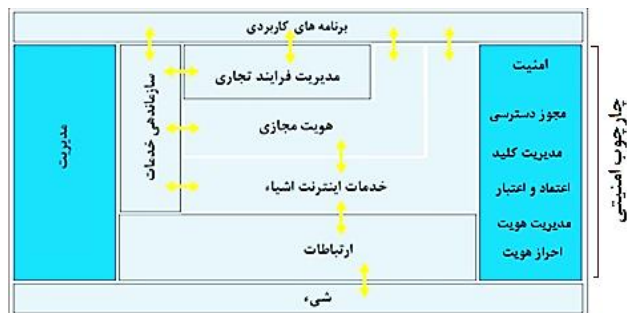
¹⁶ Fragmentation

¹⁷ Replication

به منظور پیشنهاد معماری مناسب، با توجه به بررسی و مقایسه رویکرد معماری‌های معرفی شده، می‌توان دریافت که مدل و معماری ارائه شده توسط IoT-A با توجه به هدف، تنوع مستندات، گستردگی گروه تحقیق و گستره جغرافیایی آن یعنی اتحادیه اروپا، از جامعیت بیشتری نسبت به سه معماری دیگر برخوردار است. همچنین با توجه به نتایج حاصله از تحقیقات قبل که در جدول ۳ قابل مشاهده است، می‌توان دریافت که معماری IoT-A در مقایسه با معماری‌های دیگر دو مورد نیازهای کاربردی موضوع مقاله را همزمان برآورده می‌کند [۵۱]؛ بنابراین به دلیل جامعیت معماری IoT-A و همچنین ارضای برخی الزامات کاربردی مورد پژوهش، در ادامه از این معماری جهت ادامه روند پژوهش استفاده می‌شود.

مقاله از مدل کاربردی^{۱۸} آن استفاده می‌شود. مدل کاربردی یک چارچوب انتزاعی برای درک گروه‌های کاربردی اصلی و روابط آن‌ها در محیط IoT-A است. این چارچوب معنای مشترکی را جهت استفاده در توسعه دیدگاه‌های کاربردی سازگار با IoT-A تعریف می‌کند [۵۰].

مدل کاربردی معماری مرجع IoT-A شامل هفت قابلیت عمودی و دو گروه عملکرد افقی مدیریت و امنیت است. چارچوب امنیت در مدل کاربردی از ۵ مؤلفه تشکیل شده است؛ که برای ارتقاء سطح امنیت در معماری، نیاز به بهینه‌سازی دارد. در شکل ۲ اجزاء تشکیل دهنده مدل کاربردی نمایش داده شده است [۵۰].



شکل ۲- مدل کاربردی و مؤلفه‌های چارچوب امنیتی معماری IoT-A [۵۰]

جدول ۳- الزامات کاربردی معماری‌های مرجع [۵۱]

معماری		<i>IoT-A ARM</i>	<i>WSO2</i>	<i>Korean ARM</i>	<i>Chinese ARM</i>
نیاز کاربردی	الزامات پشتیبانی از برنامه‌ها	√	-	-	√
	الزامات حفاظت امنیت و محرمانگی	√	√	-	-

¹⁸ Functional Model

۲-۳- نگاشت آسیب‌پذیری‌ها و تهدیدات در معماری مرجع IoT-A

این زیر بخش باهدف شناسایی نقاط ضعف امنیتی مؤلفه‌های مدل کاربردی معماری IoT-A، به نگاشت

حملات، تهدیدات و آسیب‌پذیری‌ها بر روی هریک از مؤلفه‌ها پرداخته و نتایج را در جدول ۴ خلاصه می‌کند (جدول ۳).

جدول ۴- نگاشت آسیب‌پذیری‌ها و تهدیدات بر اجزای معماری IoT-A

نام مؤلفه	آسیب‌پذیری	تهدیدات و حملات
ارتباطات و زیرساخت	امنیت ارتباطات	استراق سمع / مسیریابی غلط/تحلیل ترافیک / دست‌کاری ترافیک/جعل هویت/ فردی در میان/ ارسال پیام منتخب/ حمله درج/حمله ack
هویت‌های مجازی	امنیت در ذخیره‌سازی امنیت در رمزنگاری	دست‌کاری داده/ تهدید حریم خصوصی / رمزگشایی و استخراج اطلاعات
خدمات	امنیت خدمات بر روی شیء امنیت دستگاه‌های پایانی امنیت در رمزنگاری	کُدک‌های مخرب/ ابزار Xmpp
سازمان‌دهی خدمات	امنیت خدمات شبکه امنیت ارتباطات	DOS / دست‌کاری ترافیک / اغتشاش در مسیر/ تهدید حریم خصوصی
مدیریت فرایندها	امنیت ارتباطات محدودیت نرم‌افزار امنیت خدمات ابری امنیت شرکت ابری	دست‌کاری دستگاه/ جایگزینی میان‌افزار/ حمله اکتشافی
امنیت مدیریت	امنیت نرم‌افزار و میان‌افزار امنیت نرم‌افزار و میان‌افزار امنیت خدمات شبکه ناهمگونی دستگاه‌ها امنیت ارتباطات محدودیت قابلیت توسعه	رمزگشایی و استخراج اطلاعات/ جعل هویت / فردی در میان تحریف ساعت Jamming/GTS بلاک کانال /برنامه تقلبی کنترل از راه دور/ ارسال پیام منتخب /DOS

۳-۳- نیازهای امنیتی خانه هوشمند

پس از بررسی تهدیدات و آسیب‌پذیری‌ها و نگاشت آن‌ها در مؤلفه‌های معماری، شناخت نیازها جهت بهبود وضعیت امنیت الزامی است. در همین راستا مطالعه و بررسی جهت شناخت نیازهای امنیتی به انجام رسید که نتیجه آن در جدول ۵ قابل مشاهده است. به‌کارگیری یا قالب مؤلفه امنیت معماری مرجع است.

بهبود عملکرد مکانیسم‌های امنیتی در هر یک از این مؤلفه‌ها موجب ارتقاء امنیت در حوزه کاربرد خانه هوشمند خواهد شد؛ بنابراین هدف اصلی این مقاله ارائه راهکارهایی جهت تأمین نیازهای امنیتی ذکرشده در قالب مؤلفه امنیت معماری مرجع است.

جدول ۵- نیازهای امنیتی خانه هوشمند

عنوان نیازمندی	مراجع
احراز هویت	[۳۱]
مدیریت هویت	[۴۱]
حریم خصوصی	[۴۱, ۳۱]
دسترس پذیری	[۴۱] [۳۱]
مقاوم بودن	[۴۲, ۴۱, ۳۱]
حفاظت اطلاعات	[۳۱]
کنترل دسترسی	[۳۱]
تفویض اختیار	[۳۱]
اعتماد	[۴۱]

سلامت از راه دور به خانه هوشمند خواهد شد. مؤلفه‌های چارچوب پیشنهادی با مؤلفه‌های چارچوب استاندارد IoT-A در جدول ۶ مقایسه شده است.

جدول ۶- مقایسه مؤلفه‌های چارچوب پیشنهادی با

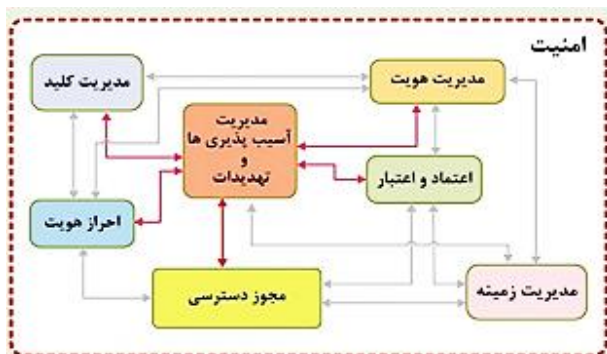
مؤلفه‌های چارچوب معماری IoT-A	
مؤلفه‌های پیشنهادی	مؤلفه‌های معماری
احراز هویت	احراز هویت
مدیریت هویت	مدیریت هویت
مجوز دسترسی توزیع شده**	مجوز دسترسی
تبادل و مدیریت کلید اعتماد و اعتبار	تبادل و مدیریت کلید اعتماد و اعتبار
مدیریت آسیب پذیری‌ها و تهدیدات**	-
مدیریت زمینه**	-

۳-۴- راهکار پیشنهادی برای ارتقاء امنیت

مدل کاربردی معماری مرجع IoT-A، مجموعه‌ای از مؤلفه‌ها را با درجه مشخصی از انتزاع به‌عنوان یک چارچوب امنیتی ارائه می‌کند. مدل مذکور به توسعه‌دهندگان این امکان را می‌دهد تا با توجه به حوزه کاربرد، رویکردهای متنوعی را در پیاده‌سازی داشته باشند. لذا در این مقاله، با توجه به الزامات امنیتی ذکرشده، مدل انتزاعی فوق به شکلی تکمیل می‌شود که درجه امنیت در حوزه کاربردی خانه هوشمند ارتقاء یابد. جهت نیل به این هدف، مؤلفه مدیریت زمینه^{۱۹} به‌منظور جمع‌آوری، به‌روزرسانی و مدیریت صحیح اطلاعات مربوط به اشیاء موجود و ارائه اطلاعات صحیح و تازه به سایر مؤلفه‌های امنیتی موجود اضافه شده است. همچنین مؤلفه مدیریت آسیب‌پذیری‌ها و تهدیدات^{۲۰} جهت پایش حداکثری، کشف و مقابله با تهدیدات و آسیب‌پذیری‌ها به ۵ مؤلفه چارچوب امنیتی معماری اضافه شده است. مؤلفه صدور مجوز به نحوی تغییر پیدا کرده تا دسترسی به منابع اطلاعاتی خانه هوشمند با رعایت هر چه بیشتر حریم خصوصی و حفظ امنیت ساکنین انجام شود. این تغییر باعث نظارت بیشتر در جهت امن‌تر شدن نحوه دسترسی سایر حوزه‌های کاربردی ازجمله حوزه

۳-۵- تشریح راهکار پیشنهادی

این بخش به تشریح مؤلفه‌های چارچوب پیشنهادی می‌پردازد که در شکل ۳ نمایش داده شده است. همان‌طور که در جدول ۵ مشاهده شد دو مؤلفه مدیریت آسیب‌پذیری و تهدیدات و مدیریت زمینه به چارچوب مرجع اضافه شده و تغییراتی در نحوه صدور مجوز دسترسی داده شده است که در ادامه توضیح داده می‌شود.



شکل ۳- مؤلفه‌های چارچوب پیشنهادی

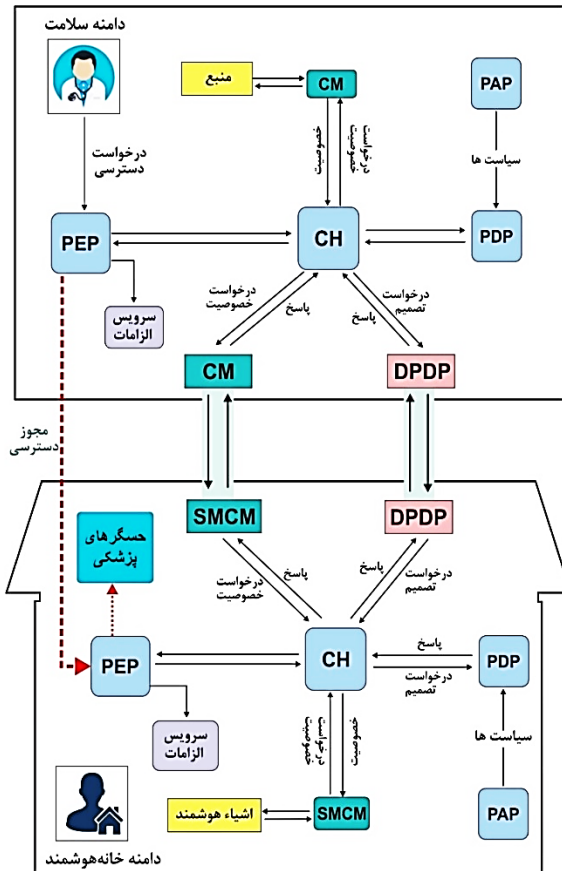
۳-۵-۱- مدیریت زمینه

این مؤلفه مسئول شناسایی و حفظ اطلاعاتی است که به‌طور مداوم توسط کاربران و دستگاه‌ها تولید و ردوبدل می‌شود. این اطلاعات شامل خصوصیات اشیاء، خدمات و موجودیت‌های موجود در حوزه کاری است. مکانیسم پیشنهادشده برای شناسایی و ثبت اشیاء هوشمند و خدمات

¹⁹ Context management

²⁰ Vulnerability & Threat Management

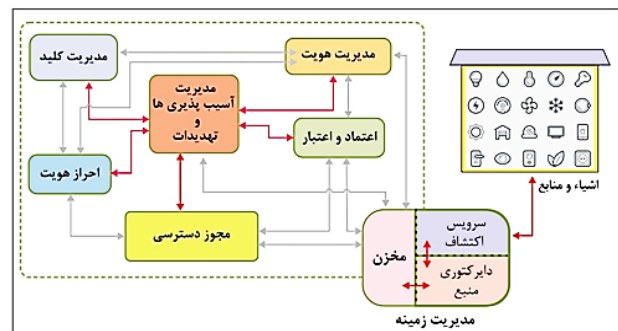
اشیاء، روش صدور مجوز توزیع‌شده در چارچوب امنیتی ارائه‌شده، مدنظر قرار گرفته است. ترکیب فرایند احراز هویت و مجوز دسترسی در شکل ۵ قابل‌مشاهده است.



شکل ۵- مکانیسم ارزیابی و صدور مجوز به روش توزیع‌شده بین دو حوزه خانه هوشمند و سلامت

با توجه به شکل، درخواست‌کننده^{۲۵}، درخواست دسترسی را به نقطه اجرای سیاست^{۲۶} ارسال می‌کند. نقطه اجرای سیاست، درخواست دریافت اطلاعات را به نگه‌دارنده محتوا^{۲۷} ارسال می‌کند. با توجه به اینکه حوزه تصمیم‌گیری در حوزه دیگری مانند خانه هوشمند است، نگه‌دارنده محتوا، جهت تکمیل اطلاعات در مورد خصوصیت^{۲۸} منبع مورد درخواست،

موجود با استفاده از سرویس اکتشاف^{۲۱} و مجموعه‌ای از مخزن‌ها^{۲۲} در سطح دامنه^{۲۳} خواهد بود. اطلاعات پس از اکتشاف در دایرکتوری منبع^{۲۴} ثبت و در مخزن ذخیره می‌شود. این سرویس‌ها به‌صورت توزیع‌شده بوده و به مراکز اصلی خود در سرویس‌دهنده اصلی مرتبط خواهند شد و اطلاعات هر دامنه را با توجه به سطح دسترسی و ضرورت به سیستم مرکزی انتقال خواهند داد. این روش امکان ادغام اشیاء هوشمند تحت فناوری‌های مختلف و پروتکل‌های گوناگون را میسر می‌سازد [۵۲]. علاوه بر آن این مؤلفه تأمین‌کننده اطلاعات بروز و تازه برای سایر مؤلفه‌های امنیتی خواهد بود. نحوه ارتباط این مؤلفه با سایر مؤلفه‌ها در شکل ۴ نمایش داده شده است.



شکل ۴- مدیریت زمینه و ارتباط آن با سایر مؤلفه‌ها

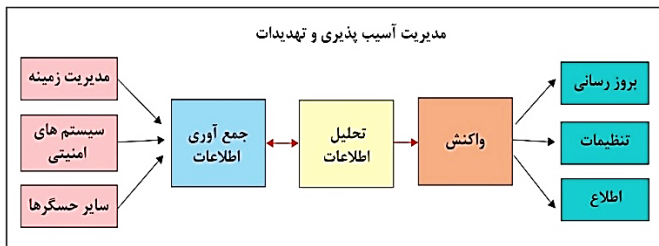
۲-۳-۵- مجوز دسترسی توزیع‌شده

اجرای سیاست‌های کنترل دسترسی، نیاز به یک مکانیسم تصمیم‌گیری فراگیر و توسعه‌پذیر دارد. این مکانیسم می‌بایست دارای خصوصیتی همچون قدرت اجرای ارزیابی‌های متنوع، سهولت در مدیریت سیستم‌ها و پشتیبانی از مفهوم الزامات باشد. همچنین قابلیت گسترش و تصمیم‌گیری در مورد کنترل دسترسی به‌صورت مشارکتی در چندین گره و یا اصطلاحاً توزیع‌شده را نیز داشته باشد. با توجه به تعامل خانه هوشمند با سایر حوزه‌های اینترنت

²⁵ Requester
²⁶ Policy Enforcement Point
²⁷ Context Handler
²⁸ Attribute

²¹ Discovery service
²² Repository
²³ Directory
²⁴ Source Directory

ارتباط بوده و به جمع‌آوری اطلاعات تازه و قابل‌اطمینان از اشیاء و سرویس‌های موجود در خانه هوشمند بپردازد. پس از تحلیل اطلاعات امنیتی، تشخیص و واکنش مناسب به تهدید احتمالی انجام خواهد شد. هم‌چنین برای رفع آسیب‌پذیری‌های موجود در اشیاء و مقاوم‌سازی^{۳۸} آن‌ها بکار می‌رود. به دلیل بالا بودن هزینه طراحی، اجرا و نگهداری این سرویس، استقرار آن در سمت سرویس ابری و ارائه‌کننده خدمات اینترنت اشیاء پیشنهاد می‌شود. نحوه فعالیت آن در شکل ۶ نمایش داده شده است.



شکل ۶- مدیریت آسیب‌پذیری و تهدیدات

۳-۶- تحلیل راهکار ارائه‌شده

در این مقاله الزامات و نیازمندی‌های امنیتی خانه هوشمند مبتنی بر اینترنت اشیاء ارائه شد. در مدل کاربردی معماری IoT-A یک چارچوب امنیتی کلی و با درجه مشخصی از انتزاع، جهت برقراری امنیت در نظر گرفته شده است. در این مقاله ضمن انجام تغییرات بر روی این مدل امنیتی، سعی شد تا چارچوبی جهت ارتقاء امنیت در حوزه کاربردی خانه هوشمند به‌عنوان راهکار جدید ارائه شود. این تغییرات شامل اضافه شدن دو مؤلفه مدیریت زمینه و مدیریت آسیب‌پذیری و تهدیدات و به‌کارگیری ارزیابی و صدور مجوز با روش توزیع‌شده و استفاده از مؤلفه جدید مدیریت زمینه بود. هدف از ارائه چارچوب جدید، پوشش حداکثری نیازهای امنیتی قیدشده، برای ارتقاء امنیت در خانه هوشمند بوده است. راهکارهای ارائه‌شده بر اساس نیازهای امنیتی در جدول ۶ نمایش داده شده است. این مقاله به‌صورت نظری و از تجمیع راهکارهای موفق تحقیقات قبلی و با درجه‌ای از

درخواستی را به مدیریت زمینه^{۲۹} ارسال می‌کند. ضمناً جهت اخذ تصمیم مقتضی، پیامی را نیز به نقطه تصمیم‌گیری توزیع‌شده^{۳۰} ارسال می‌کند. مدیریت زمینه، از نقطه متقابل خود یعنی مدیریت زمینه خانه هوشمند درخواست اطلاعات می‌نماید. نقطه تصمیم‌گیری توزیع‌شده نیز از نقطه متقابل خود در خانه هوشمند تقاضای ارائه تصمیم می‌نماید. نگه‌دارنده محتوا در خانه هوشمند کلیه درخواست‌ها را دریافت می‌نماید.

نقطه مدیریت سیاست^{۳۱}، سیاست‌ها و مجموعه سیاست‌ها^{۳۲} را در اختیار نقطه مدیریت تصمیم‌گیری^{۳۳} قرار می‌دهد. نقطه تصمیم‌گیری بر اساس سیاست‌های موجود و خصوصیات منبع مورد درخواست، پاسخ نتیجه‌گیری لازم را به نگه‌دارنده محتوا^{۳۴} ارسال می‌کند. نگه‌دارنده محتوا تصمیمات را به نقطه تصمیم‌گیری توزیع‌شده ارائه و خصوصیات مورد درخواست را نیز به مدیریت زمینه ارائه می‌کند. نگه‌دارنده محتوا اطلاعات ارسالی از خانه هوشمند را به نقطه اجرای تصمیم ارائه می‌دهد. نقطه اجرای سیاست‌ها^{۳۵} الزامات را بررسی و در صورت تأیید، مجوز دسترسی به منبع را می‌دهد، در غیر این صورت دسترسی را رد می‌کند.

۳-۳-۵- مدیریت آسیب‌پذیری و تهدیدات

این مؤلفه که به‌نوعی ایفاکننده نقش مرکز عملیات امنیت^{۳۶} را برای خانه هوشمند است، جهت پایش، کشف آسیب‌پذیری‌ها و مقابله با تهدیدات با مدیریت متمرکز پیشنهادشده که متشکل از سرویس‌های پایش^{۳۷}، جمع‌آوری اطلاعات، تحلیل و پاسخ است [۵۳]. این مؤلفه جهت عملکرد صحیح، نیاز دارد تا با مؤلفه مدیریت زمینه در

²⁹ Context Management (CM)

³⁰ Distributed decision point (DPDP)

³¹ Policy Administration Point (PAP)

³² Policy sets

³³ Policy Decision Point (PDP)

³⁴ Context Handler (CH)

³⁵ Policy Enforcement Point (PEP)

³⁶ Security operation center

³⁷ Monitoring

³⁸ Hardening

انتزاع ارائه شده است. لذا جهت ارزیابی مدل نظری ارائه شده از تحلیل و مقایسه استفاده می‌شود.

جدول ۶- نیازهای امنیتی و راهکارهای پیشنهاد شده

متناظر با آن	
عنوان نیاز امنیتی	راهکار پیشنهادی
احراز هویت	مؤلفه احراز هویت توزیع شده
مدیریت هویت	مؤلفه مدیریت هویت
حریم خصوصی	مؤلفه مجوز دسترسی / مدیریت هویت / اعتماد و اعتبار
دسترس پذیری	مؤلفه صدور مجوز
مقاوم بودن	مؤلفه مدیریت آسیب پذیری و تهدیدات
حفاظت اطلاعات	مؤلفه تبادل و مدیریت کلید / صدور مجوز توزیع شده
کنترل دسترسی	مؤلفه صدور مجوز توزیع شده
تفویض اختیار	مؤلفه صدور مجوز توزیع شده
اعتماد	مؤلفه اعتماد و اعتبار

در ادامه به تحلیل هر یک از مؤلفه‌های پیشنهادی بر اساس کاربرد و هدف امنیتی آن پرداخته می‌شود. جدول ۷ نمایشگر کاربرد مؤلفه و اهداف امنیتی موردنظر که توسط آن مؤلفه تأمین می‌شود خواهد بود.

جدول ۷- مؤلفه‌های راهکار پیشنهادی به همراه کاربرد و هدف امنیتی آن

اهداف امنیتی موردنظر	کاربرد مؤلفه	مؤلفه پیشنهادی
حریم خصوصی کاربران	مدیریت هویت، نام مستعار و خط‌مشی‌های دسترسی مرتبط	مدیریت هویت
تائید هویت مسئولیت‌پذیری	تائید هویت موجودیت‌ها	احراز هویت
کنترل دسترسی خدمات	کنترل دسترسی بر خدمات	احراز هویت
محرمانگی داده‌ها	کنترل دسترسی بر خدمات	احراز هویت
یکپارچگی داده‌ها	کنترل دسترسی بر زیرساخت	صدور مجوز
حریم خصوصی خدمات	کنترل دسترسی بر زیرساخت	صدور مجوز
دسترس پذیری خدمات	کنترل دسترسی بر زیرساخت	صدور مجوز
محرمانگی ارتباطات	مدیریت و تبادل کلیدهای رمزگذاری	مدیریت و تبادل کلید
صحت ارتباطات	مدیریت و تبادل کلیدهای رمزگذاری	مدیریت و تبادل کلید
عدم انکار	مدیریت و تبادل کلیدهای رمزگذاری	مدیریت و تبادل کلید
محرمانگی روبه‌جلو و عقب	مدیریت و تبادل کلیدهای رمزگذاری	مدیریت و تبادل کلید
محرمانگی یکپارچگی اطلاعات	مدیریت و تبادل کلیدهای رمزگذاری	مدیریت و تبادل کلید
صحت اطلاعات	مدیریت و تبادل کلیدهای رمزگذاری	مدیریت و تبادل کلید
حریم خصوصی امنیت ارتباطات	مدیریت و تبادل کلیدهای رمزگذاری	مدیریت و تبادل کلید
اعتبار خدمات	جمع‌آوری امتیاز اعتبار کاربر و محاسبه سطح اعتماد خدمت	اعتماد و اعتبار
اعتماد خدمات	جمع‌آوری امتیاز اعتبار کاربر و محاسبه سطح اعتماد خدمت	اعتماد و اعتبار
حریم خصوصی	جمع‌آوری امتیاز اعتبار کاربر و محاسبه سطح اعتماد خدمت	اعتماد و اعتبار
تازگی و صحت اطلاعات	جمع‌آوری اطلاعات مربوط به اشیاء و منابع و خدمات	مدیریت زمینه
حریم خصوصی دسترسی	جمع‌آوری اطلاعات مربوط به اشیاء و منابع و خدمات	مدیریت زمینه

تغییرات انجام‌شده در چارچوب امنیت معماری به شرح زیر است:

۱-۳-۶- مؤلفه مدیریت زمینه

به‌منظور جمع‌آوری اطلاعات اشیاء، ارتباطات و منابع خانه هوشمند، حفظ حریم خصوصی دسترسی‌پذیری بیشتر به منابع و صحت اطلاعات موردنیاز به چارچوب اضافه‌شده است. این مؤلفه در دو جایگاه، یکی خانه هوشمند و دیگری در خدمات ابری پیاده‌سازی می‌شود. این مؤلفه از چارچوب

می‌توان کمک گرفت [۲۵].

۳-۳-۶- ارزیابی و صدور مجوز دسترسی توزیع شده
به منظور کنترل دسترسی مناسب به خدمات و منابع و اشیاء به/از خانه هوشمند با حفظ حریم خصوصی و در نظر گرفتن پایین بودن توان منابع پردازشی تجهیزات خانه هوشمند ارائه گردیده است. به این جهت، پردازش‌های مهم و پیچیده به سرویس‌دهنده مستقر در خانه و یا سرویس ابری محول خواهد شد. ارزیابی و صدور مجوز توزیع شده به جهت حفظ محرمانگی اطلاعات ساکنین خانه هوشمند از اهمیت بالایی برخوردار است. به این ترتیب ارزیابی‌های مربوطه به خود دامنه محول شده و نتایج آن به سرویس ابری اعلام می‌شود. هزینه‌های مربوط به پردازش‌های پیچیده نیز بر عهده ابر سرویس‌دهنده خواهد بود. جایگاه و هدف از پیاده‌سازی هر یک از مؤلفه‌ها در جدول ۸ نمایش داده شده است.

امنیتی برای دسترسی به خدمات مبتنی بر اینترنت اشیا در ساختمان‌های هوشمند الگوبرداری شده است. این مدل توسط یکی از مراکز تحقیقاتی معتبر پیاده‌سازی شده است [۲۵].

۲-۳-۶- مدیریت آسیب‌پذیری و تهدیدات

جهت کشف آسیب‌پذیری‌ها و مقابله متمرکز با تهدیدات، حفظ محرمانگی، صحت و یکپارچگی اطلاعات و بالا بردن امنیت در ارتباطات و حفظ حریم خصوصی افزوده شده است. جایگاه این سرویس در خدمات ابری بوده و توسط ارائه‌کننده سرویس مدیریت می‌شود. از نظر هزینه پیاده‌سازی برای کاربر بار مالی نداشته و بر روی خدمات ارائه شده محاسبه خواهد شد. عملکرد این سرویس همانند یک سرویس اطلاعات و مدیریت رخدادهای امنیتی^{۳۹} [۳۱] خواهد بود. برای پیاده‌سازی این مؤلفه از مدل‌های معتبر

جدول ۸ - جایگاه و روش پیاده‌سازی هر یک از مؤلفه‌های چارچوب امنیتی

مؤلفه پیشنهادی	روش پیاده‌سازی	جایگاه پیاده‌سازی	هدف از پیاده‌سازی
مدیریت هویت	توزیع شده	سرویس ابری خانه هوشمند	مدیریت متمرکز همه دامنه‌ها حفظ حریم خصوصی - محرمانگی اطلاعات
احراز هویت	توزیع شده	سرویس ابری خانه هوشمند	دامنه‌ها - منابع مدیریت متمرکز همه زیاد حفظ حریم خصوصی - محرمانگی اطلاعات
صدور مجوز	توزیع شده	سرویس ابری خانه هوشمند	مدیریت متمرکز - منابع زیاد حفظ حریم خصوصی - محرمانگی اطلاعات
مدیریت و تبادل کلید	طبق معماری	سرویس ابری خانه هوشمند	یکپارچگی و محرمانگی ارتباطات و اطلاعات ارتباطات امن بین دامنه کاربرد و ابر
اعتماد و اعتبار	طبق معماری	سرویس ابری خانه هوشمند	اعتماد و اعتبار بین کاربران و خدمات اعتماد و اعتبار بین کاربران و خدمات
مدیریت زمینه	توزیع شده	سرویس ابری خانه هوشمند	مدیریت صدور مجوز بین دامنه‌های کاربردی محرمانگی و حفظ حریم خصوصی
مدیریت آسیب‌پذیری و تهدیدات	متمرکز	سرویس ابری	مدیریت متمرکز تهدیدات و آسیب‌پذیری‌ها

³⁹ Security Information and event management

۳-۷- مقایسه نتایج

در ادامه مدل ارائه‌شده با راهکارهای موجود مقایسه خواهد شد. در ابتدا این مقایسه با مدل کاربردی امنیت معماری پیشنهادی و سپس با چارچوب‌های موجود امنیتی در این حوزه انجام خواهد شد.

۱-۳-۷- مقایسه با چارچوب امنیتی موجود در

معماری IoT-A

چارچوب ارائه‌شده در معماری مرجع IoT-A دارای پنج مؤلفه استاندارد برای تأمین امنیت اجزاء معماری است. این مؤلفه‌ها طبق نیازهای استاندارد امنیتی طراحی‌شده و قابل پیاده‌سازی هستند. جدول ۹ مقایسه‌ای بین اهداف امنیتی تأمین‌شده توسط دو چارچوب امنیتی اولیه معماری و چارچوب پیشنهادی ارائه داده است.

جدول ۹- مقایسه مؤلفه‌های امنیتی چارچوب معماری و پیشنهادی [۲۵، ۳۲]

مؤلفه امنیتی	اهداف امنیتی موردنظر	معماری	پیشنهادی
مدیریت هویت	حریم خصوصی کاربران	✓	✓
	حریم خصوصی خدمات	✓	✓
	مسئولیت‌پذیری	✓	✓
صدور مجوز	کنترل دسترسی خدمات	✓	✓
	محرمانگی داده‌ها	✓	✓
	یکپارچگی داده‌ها	✓	✓
	حریم خصوصی خدمات	✓	✓
	دسترسی‌پذیری خدمات	✓	✓
	حریم خصوصی حوزه کاربرد	✓	✓
مدیریت و تبادل کلید	محرمانگی ارتباطات	✓	✓
	صحت ارتباطات	✓	✓
	عدم انکار	✓	✓
	محرمانگی روبه‌جلو و عقب	✓	✓
مدیریت آسیب‌پذیری و تهدیدات	مقاوم‌سازی	-	✓
	محرمانگی	-	✓
	یکپارچگی اطلاعات	-	✓
	صحت اطلاعات	-	✓
	حریم خصوصی	-	✓
	امنیت ارتباطات	-	✓
	امنیت برنامه‌های کاربردی	-	✓
اعتماد و اعتبار	اعتبار خدمات	✓	✓
	اعتماد خدمات	✓	✓
	حریم خصوصی	✓	✓
مدیریت زمینه	تازگی و صحت اطلاعات	-	✓
	محرمانگی اطلاعات حوزه کاربرد	-	✓
	دسترسی‌پذیری اطلاعات	-	✓

۲-۳-۷- مقایسه با سایر پژوهش‌ها

در مقالات متعدد به موضوع آسیب‌پذیری‌ها، تهدیدات خانه هوشمند و اینترنت اشیا پرداخته شده و یا راهکارهایی جهت امن سازی آن ارائه شده است. در این مقاله علاوه بر بررسی موضوعات فوق، به منظور ارائه راهکار استاندارد برای تأمین امنیت خانه‌های هوشمند از معماری مرجع IoT-A استفاده شده است. به کارگیری معماری مرجع اینترنت اشیا در این پژوهش موجب ایجاد یک قالب واحد برای تمامی فعالیت‌ها و فرایندهای مربوط به این دامنه کاربردی خواهد شد. به این معنا که ارائه چارچوب امنیتی نه تنها موجب امن سازی دامنه کاربردی خانه هوشمند خواهد شد، بلکه کلیه فرایندها و سرویس‌ها و ارتباطات مبتنی بر معماری اینترنت اشیا را پوشش خواهد داد.

مؤلفه مدیریت زمینه قبلاً در ساختمان‌های هوشمند بکار گرفته شده و کارایی آن آزموده شده است [۵۲]. در این مقاله با اندکی تغییر در نوع کاربرد، از مؤلفه فوق به عنوان تأمین‌کننده اصلی اطلاعات برای سایر مؤلفه‌های چارچوب امنیتی به منظور حفظ تازگی اطلاعات و جهت جلوگیری از برخی حملات استفاده شده است.

مؤلفه مدیریت آسیب‌پذیری و تهدیدات مشابه یک مرکز عملیات امنیت عمل می‌کند که به طور توزیع شده در بستر ابر و حوزه کاربرد پیاده‌سازی می‌شود. این مؤلفه با استفاده از سرویس‌های پایش، جمع‌آوری و تحلیل اطلاعات به امن سازی حداکثری حوزه کاربرد اقدام می‌کند. این روند با به کارگیری سیستم‌های مدیریت رخداد و رویدادهای امنیتی^{۴۰} قبلاً در حوزه اینترنت اشیا بررسی و آزموده شده است [۵۳].

۴- نتیجه‌گیری و پیشنهادها

این مقاله باهدف ارتقا امنیت در خانه‌های هوشمند مبتنی بر اینترنت اشیا، به ارائه یک چارچوب امنیتی از طریق انجام تغییرات و اضافه کردن مؤلفه‌های لازم به چارچوب امنیتی

معماری مرجع IoT-A پرداخته است. اضافه شدن مدیریت زمینه به مؤلفه‌های چارچوب امنیتی به شناسایی و جمع‌آوری اطلاعات منابع و اشیا هوشمند و همچنین اطلاعات مربوط به پروتکل‌های ارتباطی خانه هوشمند کمک می‌کند. در چارچوب پیشنهادی تغییراتی در نحوه کار ارزیابی و صدور مجوز کنترل داده شده است به طوری که این مکانیسم با استفاده از مدیریت زمینه به صورت توزیع شده به صورت بهینه به فعالیت خود خواهد پرداخت. همچنین مؤلفه مدیریت آسیب‌پذیری و تهدیدات به این چارچوب اضافه شده که در مدیریت متمرکز امنیت کمک شایانی خواهد نمود. مدل ارائه شده با توجه به تحقیقات پیشین و جداول مقایسه و ارزیابی این مقاله، از نظر تئوری موجب تأمین نیازهای امنیتی خانه هوشمند مبتنی بر معماری اینترنت اشیا IoT-A می‌شود.

مطالعات انجام شده در این مقاله نشان می‌دهد که فقدان یک معماری استاندارد و مشترک برای این فناوری کاملاً محسوس است. با توجه به گستردگی زمینه فعالیت و پژوهش جهت ارائه روش‌های نوین و یا استانداردسازی در این حوزه اجرای طرح‌های مطالعاتی جامع‌تر پیشنهاد می‌شود. مؤلفه مدیریت هویت و احراز هویت در چارچوب ارائه شده با استفاده مکانیسم‌های پیشنهاد شده توسط معماری مرجع پیاده‌سازی شده است. با توجه به ظهور و بروز شدن مکانیسم‌های ابری و استفاده روزافزون از آن‌ها در این زمینه، پیشنهاد می‌گردد برای تمرکز در مدیریت و ارتقاء امنیت در این زمینه و همچنین کاهش هزینه‌ها، از مدیریت هویت ابری^{۴۱} یا شناسه به عنوان خدمت^{۴۲} استفاده شود.

⁴² Identity as a service

⁴⁰ SIEM (Security information and event management)

منابع

- IEEE communications surveys & tutorials, 17(4) (2015) 2347-2376.
12. A.K. Sangaiah, G. Li, A joint resource-aware and medical data security framework for wearable healthcare systems, *Future Generation Computer Systems*, 95 (2019) 382-391.
 13. D. Vinodhan, A. Vinnarasi, IOT Based Smart Home, *International Journal of Engineering and Innovative Technology (IJEIT)*, 10 (2016).
 14. M. O'Neill, Insecurity by design: Today's IoT device security problem, *Engineering*, 21(1) (2016) 48-49.
 15. Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the Internet of Things: perspectives and challenges, *Wireless Networks*, 20(8) (2014) 2481-2501.
 16. E. Nimmermark, A. Larsson, Comparison of IoT frameworks for the smart home, (2016).
 17. G. Lobaccaro, S. Carlucci, E. Löfström, A review of systems and technologies for smart homes and smart grids, *Energies*, 9(5) (2016) 348.
 18. H.K. Jonnalagadda, Secure Communication Scheme in Smart Home Environment, (2016).
 19. F. Johari, The security of communication protocols used for Internet of Things, *LU-CS-EX 2015-42*, (2015).
 20. F. Kausar, E. Al Eisa, I. Bakhsh, Intelligent home monitoring using RSSI in wireless sensor networks, *International Journal of Computer Networks & Communications*, 4(6) (2012) 33.
 21. S. Marzano, *The new everyday: Views on ambient intelligence*, 010 Publ., 2003.
 22. A. Saad al-sumaiti, M.H. Ahmed, M.M. Salama, Smart home activities: A literature review, *Electric Power Components and Systems*, 42(3-4) (2014) 294-305.
 23. W. Granzer, W. Kastner, G. Neugschwandtner, F. Praus, A modular architecture for building automation systems, na, 2006.
 1. J. Zheng, C.D.S.R. Bisdikian, H. Mouftah, The internet of Things, *IEEE Communications Magazine*, 49(11) (2011) 30-31.
 2. T. Fan, Y. Chen, A scheme of data management in the Internet of Things, in: 2010 2nd IEEE International Conference on Network Infrastructure and Digital Content, IEEE, 2010, pp. 110-114.
 3. Y. Yu, J. Wang, G. Zhou, The exploration in the education of professionals in applied internet of things engineering, in: 2010 4th International Conference on Distance Learning and Education, IEEE, 2010, pp. 74-77.
 4. Y. Huang, G. Li, Descriptive models for Internet of Things, in: Paper presented at the Intelligent Control and Information Processing (ICICIP), 2010 International Conference on, 2010.
 5. K. Ashton, That 'internet of things' thing, *RFID journal*, 22(7) (2009) 97-114.
 6. G.T. Ferguson, Have your objects call my objects, *Harvard business review*, 80(6) (2002) 138-144.
 7. L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, *Computer networks*, 54(15) (2010) 2787-2805.
 8. G. Lawton, Machine-to-machine technology gears up for growth, *computer*, (9) (2004) 12-15.
 9. A. Gandomi, M. Haider, Beyond the hype: Big data concepts, methods, and analytics, *International journal of information management*, 35(2) (2015) 137-144.
 10. S. Zhang, S. Zhang, X. Chen, X. Huo, . Cloud computing research and development trend, in: Paper presented at the Future Networks. ICFN'10. Second International Conference on., 2010.
 11. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications,

- 33.H. Lin, N. Bergmann, IoT privacy and security challenges for smart home environments, *Information*, 7(3) (2016) 44.
- 34.Z.A. Almusaylim, N. Zaman, A review on smart home present state and challenges: linked to context-awareness internet of things (IoT), *Wireless Networks*, 25(6) (2019) 3193-3204.
- 35.I. Lee, K. Lee, The Internet of Things (IoT): Applications, investments, and challenges for enterprises, *Business Horizons*, 58(4) (2015) 431-440.
- 36.J. Bugeja, A. Jacobsson, P. Davidsson, On privacy and security challenges in smart connected homes, in: 2016 European Intelligence and Security Informatics Conference (EISIC), IEEE, 2016, pp. 172-175.
- 37.S.C. Mukhopadhyay, N. Suryadevara, Internet of things: Challenges and opportunities. In *Internet of Things* (pp. 1-17), Springer, 2014.
- 38.M. Younas, Research challenges of big data, (2019).
- 39.O. Olayemi, V. Antti, H. Keijo, T. Pekka, Security issues in smart homes and mobile health system: threat analysis, possible countermeasures and lessons learned, (2017).
- 40.R. Billure, V.M. Tayur, V. Mahesh, Internet of Things-a study on the security challenges, in: 2015 IEEE International Advance Computing Conference (IACC), IEEE, 2015, pp. 247-252.
- 41.A. Riahi, E. Natalizio, Y. Challal, N. Mitton, A. Iera, A systemic and cognitive approach for IoT security, in: 2014 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2014, pp. 183-188.
- 42.C. Lee, L. Zappaterra, K. Choi, H.-A. Choi, Securing smart home: Technologies, security challenges, and security requirements, in: 2014 IEEE Conference on Communications and Network Security, IEEE, 2014, pp. 67-72.
- 24.M.A. Al-Qutayri, J.S. Jeedella, Integrated wireless technologies for smart homes applications, in: *Smart Home Systems*, IntechOpen, 2010.
- 25.B.L.R. Stojkoska, K.V. Trivodaliev, A review of Internet of Things for smart home: Challenges and solutions, *Journal of Cleaner Production*, 140 (20.۱۴۶۴-۱۴۰۴ (۱۷
- 26.T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S.S. Kumar, K. Wehrle, Security Challenges in the IP-based Internet of Things, *Wireless Personal Communications*, 61(3) (2011) 527-542.
- 27.G. Gan, Z. Lu, J. Jiang, Internet of things security analysis, in: 2011 international conference on internet technology and applications, IEEE, 2011, pp. 1-4.
- 28.M. Katagi, S. Moriai, Lightweight cryptography for the internet of things, Sony Corporation, (2008) 7-10.
- 29.S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), IEEE, 2011, pp. 1-5.
- 30.R. Roman, P. Najera, J. Lopez, Securing the internet of things, *Computer*, (9) (2011) 51-58.
- 31.M.M. Hossain, M. Fotouhi, R. Hasan, Towards an analysis of security issues, challenges, and open problems in the internet of things, in: 2015 IEEE World Congress on Services, IEEE, 2015, pp. 21-28.
- 32.P. Sarigiannidis, E. Karapistoli, A.A. Economides, VisIoT: A threat visualisation tool for IoT systems security, in: 2015 IEEE International Conference on Communication Workshop (ICCW), IEEE, 2015, pp. 2633-2638.

- Management, Springer, 2013, pp. ۲۰۶-۲۱۷.
- 48.P. Fremantle, A reference architecture for the internet of things, WSO2 White paper, (2014).
- 49.S. Chen, H. Xu, D. Liu, B. Hu, H. Wang, A vision of IoT: Applications, challenges, and opportunities with china perspective, IEEE Internet of Things journal, 1(4) (2014) 349-359.
- 50.I. FhG, S.H. SAP, E.H. HSG, C. Jardak, A.O. CEA, A. Serbanati, J.W. Walewski, Internet of things-architecture iot-a deliverable d1. 3-updated reference model for iot v1. 5 (2012).
- 51.A. Torkaman, M.A. Seyyedi, Analyzing IoT reference architecture models, International Journal of Computer Science and Software Engineering, 5(8) (2016) 154.
- 52.J.L. Hernández-Ramos, M.V. Moreno, J.B. Bernabé, D.G. Carrillo, A.F. Skarmeta, SAFIR: Secure access framework for IoT-enabled services on smart buildings, Journal of Computer and System Sciences, 81(8) (2015) 1452-1463.
- 53.N. Miloslavskaya, A. Tolstoy, New SIEM System for the Internet of Things, in: In World Conference on Information Systems and Technologies (pp. 317-32) (V Springer, Cham. April., 2019).
- 43.H.A. Abdul-Ghani, D. Konstantas, A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective, Journal of Sensor and Actuator Networks, 8(2) (2019) 22.
- 44.D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, G. Baldini, Security and privacy issues for an IoT based smart home, in: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, 2017, pp. 1292-1297.
- 45.M. Dabbagh, A. Rayes, Internet of things security and privacy, in: Internet of Things From Hype to Reality, Springer, 2019, pp. 211-238.
- 46.I. Yaqoob, E. Ahmed, M.H. ur Rehman, A.I.A. Ahmed, M.A. Al-garadi, M. Imran, M. Guizani, The rise of ransomware and emerging security challenges in the Internet of Things, Computer Networks, 129 (20 (۱۷ . ۴۴۴-۴۵۸
- 47.T. Bhattasali, R. Chaki, N. Chaki, Study of security issues in pervasive environment of next generation internet of things, in: IFIP International Conference on Computer Information Systems and Industrial