دانشگاه صنعتی شریف
دانشکده مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد
رایانش امن

# تولید رفتار جعلی بر اساس هستی‌شناسی برای حفظ حریم خصوصی در خانه هوشمند

نگارش

بهزاد دارا

استاد راهنما

دکتر مرتضی امینی

آذر ۱۴۰۲


بسم الله الرحمن الرحیم

به نام خدا

دانشگاه صنعتی شریف

دانشکده مهندسی کامپیوتر

پایان‌نامه‌ی کارشناسی ارشد

این پایان‌نامه به عنوان تحقق بخشی از شرایط دریافت درجه‌ی کارشناسی ارشد است.

عنوان: تولید رفتار جعلی بر اساس هستی‌شناسی برای حفظ حریم خصوصی در خانه هوشمند

نگارش: بهزاد دارا

کمیته‌ی ممتحنین

استاد راهنما: دکتر مرتضی امینی امضاء:

استاد داور داخلی: دکتر ... امضاء:

استاد داور مدعو: دکتر ... امضاء:

تاریخ:

# اظهارنامه

(اصالت متن و محتوای پایان‌نامه کارشناسی ارشد)

عنوان پایان‌نامه: تولید رفتار جعلی بر اساس هستی‌شناسی برای حفظ حریم خصوصی در خانه هوشمند

استاد راهنما: دکتر مرتضی امینی  استاد مشاور: –

این‌جانب بهزاد دارا اظهار می‌دارم:

۱. متن و نتایج علمی ارائه شده در این پایان‌نامه اصیل بوده و زیر نظر استادان نام‌برده شده در بالا تهیه شده است.

۲. متن پایان‌نامه به این صورت در هیچ جای دیگری منتشر نشده است.

۳. متن و نتایج مندرج در این پایان‌نامه، حاصل تحقیقات این‌جانب به‌عنوان دانشجوی کارشناسی ارشد دانشگاه صنعتی شریف است.

۴. کلیه مطالبی که از منابع دیگر در این پایان‌نامه مورداستفاده قرار گرفته، با ذکر مرجع مشخص شده است.

نگارنده: بهزاد دارا

تاریخ:

امضا:

نتایج تحقیقات مندرج در این پایان‌نامه و دستاوردهای مادی و معنوی ناشی از آن (شامل فرمول‌ها، توابع کتابخانه‌ای، نرم‌افزارها، سخت‌افزارها و مواردی که قابلیت ثبت اختراع دارد) متعلق به دانشگاه صنعتی شریف است. هیچ شخصیت حقیقی یا حقوقی بدون کسب اجازه از دانشگاه صنعتی شریف حق فروش و ادعای مالکیت مادی یا معنوی بر آن یا ثبت اختراع از آن را ندارد. همچنین، کلیه حقوق مربوط به چاپ، تکثیر، نسخه‌برداری، ترجمه، اقتباس و نظایر آن در محیط‌های مختلف اعم از الکترونیکی، مجازی یا فیزیکی برای دانشگاه صنعتی شریف محفوظ است. نقل مطلب با ذکر مأخذ بلامانع است.

استاد راهنما: دکتر مرتضی امینی  نگارنده: بهزاد دارا

تاریخ:  تاریخ:

امضا:  امضا:

سپاس بر

پروردگار که در تمامی لحظات زندگی، حضور نعمت‌های بی‌کران او را دیده‌ام و ستایش به درگاه او که مرا در انجام این پژوهش یاری کرد تا ذره‌ای از آنچه در مکتب اساتید آموخته‌ام به عنوان ره‌آوردی مختصر ارائه نمایم.

تقدیم به

بهترین تکیه‌گاه دنیا، پدرم

بهترین حامی دنیا، مادرم

بهترین همراه دنیا، همسرم

# تقدیر و تشکر

در اینجا وظیفه خود می‌دانم از تمامی افرادی که به طریقی مرا در انجام این پایان‌نامه یاری نموده‌اند، تشکر کنم. به خصوص استاد بزرگوارم، جناب آقای دکتر مرتضی امینی که همواره با گشاده‌رویی خویش پذیرای اینجانب بودند و بادقت و حوصله اینجانب را در تهیه و تدوین این پایان‌نامه یاری نموده‌اند و از هیچ‌گونه تلاش و کوششی دریغ ننموده‌اند.

# چکیده

...

کلیدواژه‌ها: اینترنت اشیاء، حریم خصوصی، خانه‌ی هوشمند، هستی‌شناسی، سکوهای اینترنت اشیاء

# فهرست مطالب

# فهرست جداول

# فهرست تصاویر

# فصل ۱

# مقدمه

خانه‌های هوشمند[۱] نمونه‌ای از کاربردهای مبتنی بر تکنولوژی‌های نوین، برای کمک به زندگی مستقل جمعیت مسن رو به رشد در جهان و همچنین بالاتر بردن کیفیت زندگی انسانها از بعد راحتی و آسایش و امنیت[۲] هستند. با اینکه از تعریف اولیه این مفهوم بیش از ۲۰ سال می‌گذرد اما با بالاتر رفتن سرعت هوشمند شدن حسگرها[۳] و کوچکتر شدن اندازه آن‌ها و همچنین ارزانتر شدن هزینه‌های استفاده از آن‌ها در خانه‌های هوشمند، تحقیقات و پیشرفت‌های این حوزه در حال سرعت گرفتن است. خانه‌های هوشمند در کنار کاربردهای دیگر اینترنت اشیاء[۴] مانند کشاورزی هوشمند، سیستم‌های مبتنی بر سلامت هوشمند و امثالهم، باعث افزایش تعداد حسگرها و عملگرهای اینترنت اشیاء به کارگرفته شده در جهان شده‌اند. طبق برآورد صاحب نظران این حوزه تا سال ۲۰۲۵ تعداد دستگاه‌های اینترنت اشیاء در حال استفاده در جهان، به بیش از ۵۷ میلیارد خواهد رسید [؟].

عمده تحقیقات و پیشرفت‌های صورت گرفته در حوزه خانه‌های هوشمند، جدا از بهبودها و پیشرفت‌های صورت گرفته در حوزه حسگرها، در زیرحوزه‌های سلامت انسان‌ها مانند پایش اطلاعات حیاتی مرتبط با بیماران، پایش رفتار افراد مسن، خودکارسازی[۵] رفتارها، کنترل انرژی‌های مصرفی در خانه و دسترسی به سرویس‌های از راه دور صورت گرفته است که همه آن‌ها متکی بر شناسایی و کلاس‌بندی رفتار کاربران است.

با پیشرفت‌های هرچه بیشتر در این حوزه، به تدریج مشکلات بیشتری نیز مربوط به چگونگی حفظ حریم خصوصی کاربر شناسایی و معرفی می‌گردد. برای مثال با بیشتر شدن استفاده از تجهیزات هوشمند

[۱] Smart homes
[۲] Safety
[۳] Sensors
[۴] Internet of things
[۵] Automation

بی‌سیم در خانه‌های هوشمند، آسیب‌پذیری‌های ذاتی این تجهیزات و حملات مرتبط با آن‌ها از جمله حمله کانال جانبی[۶] که مربوط به شنود ترافیک ارسالی و استنتاج اطلاعات حساس به صورت غیر مستقیم از ترافیک ارسالی است، حریم خصوصی کاربر را بیشتر در معرض خطر قرار داده است [؟].

از سوی دیگر، تجهیزات اینترنت اشیاء موجود در بازار که قابل استفاده در خانه‌های هوشمند هستند همگی ساخت یک تولید کننده خاص نیستند و لذا با مشکل عدم امکان تعامل با یکدیگر روبرو هستند. این مشکل، کاربران را متمایل به استفاده از سکوهای اینترنت اشیاء می‌نماید چرا که این سکوهای اینترنت اشیاء[۷]، کاربران را قادر می‌سازند تا با اتصال دستگاه‌ها و سرویس‌های برخط گوناگون به یکدیگر، قواعد خودکارسازی دلخواه خود را اعمال کنند و از سرویس‌های متنوع ارائه شده توسط این سکوها بهره‌مند شوند برای مثال یکی از سرویس‌های مورد استقبال کاربران در این حوزه، شناسایی رفتار فعلی کاربر و ارائه پاسخ دقیق به کاربر در مقابل رفتار مشاهده شده است.

از آنجا که سکوهای اینترنت اشیاء هیچ قابلیتی برای کنترل نشت داده‌های حسگرها، در اختیار کاربران قرار نمی‌دهند، لذا حریم خصوصی کاربر را با خطر مواجه می‌نمایند. هنگامی که از امکان نقض حریم خصوصی کاربر با دسترسی غیر مجاز به داده‌های رفتاری کاربر حاصل از حسگرهای خانه‌های هوشمند صحبت می‌کنیم در واقع به این موضوع توجه داریم که تجهیزات یک خانه هوشمند همچون حسگرها و عملگرها، طیف وسیعی از داده‌های رفتاری ساکنان خانه هوشمند را به طور منظم جمع‌آوری می‌نمایند. به عبارت دیگر تجهیزات هوشمند امروزی مانند گوشی‌های تلفن همراه، ساعت‌های هوشمند، تجهیزات پوشیدنی[۸] هوشمند و بسیاری از تجهیزات الکترونیکی مدرن، قابلیت تولید داده دارند. چون این داده‌ها در قالب‌های خام و اولیه خود شامل اطلاعات حساسی درباره ساکنان خانه هوشمند هستند و همچنین با توجه به اینکه در زمانی زندگی می‌کنیم که جرایم سایبری هر روز گسترده‌تر، ویرانگرتر و پیچیده‌تر می‌شود، لذا جمع‌آوری داده‌ها بدون توجه کافی به نوع و مفهوم داده‌های ارسالی از دیدگاه مهاجمین، تبعات حتمی نقض حریم خصوصی کاربر و استفاده غیر مجاز از این داده‌ها را به دنبال خواهد داشت. به همین دلیل است که طبق مطالعات صورت گرفته اخیر، حفظ حریم خصوصی کاربران یکی از موانع بسیار اساسی در توجه و سازگار شدن عموم افراد به استفاده از تکنولوژی‌های خانه‌های هوشمند است [؟].

با توجه به مواردی که ذکر شد مشخص است که تحلیل قابل اعتماد داده‌های ارسالی حسگرها و عملگرها و به طور کلی رفتار کاربر در یک خانه هوشمند و کسب اطمینان از محافظت از این داده‌ها در مقابل دسترسی مهاجمینی که اقدام به شنود ترافیک ارسالی می‌نمایند و یا عدم ارسال داده‌های محرمانه کاربر به سکوهای اینترنت اشیاء، چالش بزرگی پیش روی ارائه کنندگان راهکارهای امنیتی در این حوزه

[۶] Side channel attack
[۷] Internet of things platforms
[۸] Bearable device

است.

در حوزه حفظ حریم خصوصی کاربر در برابر سکوهای نامعتمد اینترنت اشیاء، این سوال مطرح است که چگونه می‌توان داده‌های حسگرها را به سکوهای اینترنت اشیاء ارسال کرد و از سرویس‌های متنوع این سکوها بهره‌مند شد بدون این که به حریم خصوصی کاربر خدشه‌ای وارد شود و فعالیت‌های حساس و رفتار کاربر از دید سکو قابل شناسایی نباشد. راهکارهای ارائه شده برای پاسخ به این سوال می‌بایست توازنی در پاسخ به هر دو مسئله داشته باشند و مصالحه‌ای بین حفظ حریم خصوصی کاربر و دریافت سرویس‌های مد نظر کاربر در خانه هوشمند ایجاد نمایند. این راهکارها می‌بایست برای شناسایی رفتار کاربر در خانه هوشمند یک مدل رفتاری مناسب ایجاد نمایند و سپس قادر باشند تا با پنهان‌سازی، رفتارهای حساس کاربر را از دیدگاه سکوهای اینترنت اشیاء، مخفی نمایند.

در سال‌های اخیر، راهکارهایی در جهت حفظ حریم خصوصی کاربر در خانه‌های هوشمند در برابر سکوهای نامعتمد ارائه شده است. این راهکارها بر اساس روش، به راهکارهای مبتنی رمزنگاری، کمینه‌سازی[۹]، آشفته‌سازی[۱۰] و تولید رویداد جعلی تقسیم می‌شوند. راهکارهای مبتنی بر رمزنگاری، با استفاده از تکنیک‌های رمزنگاری، محاسبات چندجانبه امن و محیط اجرای امن داده‌های کاربر را از دید سکو پنهان می‌کنند. راهکارهای مبتنی بر کمینه‌سازی، از روش حذف داده‌هایی که در اجرای فواعد رهانا[۱۱]ـ‌کنش[۱۲] اثرگذار نیستند، اقدام به کاهش اطلاعات ارسالی به سکو و ناقص کردن دانش آن می‌کنند. راهکارهای مبتنی بر آشفته‌سازی، داده‌های کاربر را قبل از ارسال به سکو به شکل‌های مختلف تغییر می‌دهند. راهکارهای مبتنی بر رویداد جعلی، برای حفظ حریم خصوصی کاربر و اطلاعات حساس آن، از ارسال رویدادهای جعلی به سکو استفاده می‌کند؛ به نحوی که از دید سکو رویدادهای جعلی و واقعی قابل تمایز نباشند.

این پژوهش با هدف افزایش امنیت در خانه‌های هوشمند انجام شده و از هستی‌شناسی[۱۳] خانه‌های هوشمند بهره برده است. در این راستا، برای محافظت از امنیت خانه‌های هوشمند در برابر حملات مخرب و جلوگیری از نفوذ مهاجمان، اقدام به تولید سلسله رویداد جعلی شده است. این سلسله رویدادها با دقت و اصول هستی‌شناسی خانه طراحی شده‌اند به نحوی که مهاجمان قادر به تشخیص دقیق داده‌های واقعی از داده‌های جعلی نباشند و به تبع آن، نتوانند اطلاعات حساس مربوط به زندگی افراد در خانه‌های هوشمند را به دست آورند.

یکی از جوانب مهم در طراحی این راه حل این است که تنوع و تصادف در تولید سلسله رفتارها حفظ

---

[۹] Filtering
[۱۰] Randomization
[۱۱] Trigger
[۱۲] Action
[۱۳] Ontology

شده و از الگوهای قابل پیش‌بینی پرهیز گردد. برای این منظور، از عوامل تصادفی‌ساز[۱۴] بهره گرفته شده تا مهاجمین نتوانند با تحلیل تکراری بودن رفتارها به اهداف خود دست یابند. اقدام دیگری که علاوه بر تولید متنوع سلسله رفتارها برای گمراه‌سازی مهاجم انجام می‌شود، زمان انجام هر رفتار پس از رفتار دیگر است که با استفاده از عوامل تصادفی ساز، زمان انجام هر رفتار در بازه‌ای مشخص متغیر است. این پژوهش امیدوار است که با اجرای این برنامه، امنیت خانه‌های هوشمند تقویت شده و از حملات ناخواسته جلوگیری شود.

این پایان‌نامه در شش فصل ابعاد مختلف مساله را بررسی کرده و ارائه‌ی راه‌حل و ارزیابی آن را انجام می‌دهد. در فصل دوم تعاریف مفاهیم پایه‌ی مورد نیاز برای درک کامل مساله ارائه می‌شود، در فصل سوم پژوهش‌های پیشین مرتبط با این پژوهش را بررسی کرده که هر یک به بررسی یک یا چند بخش مرتبط با این پژوهش را انجام داده‌اند. در فصل چهارم راه‌حل ارائه شده برای حل این مساله را مدل‌سازی کرده و پیاده سازی کامل و جامع آن را ارائه می‌کنیم. در فصل پنجم به ارزیابی روش پیشنهادی و ارائه نتایج حاصل از ارزیابی می‌پردازیم و در فصل آخر نتیجه‌گیری این پژوهش ارائه خواهد شد.

[۱۴] Randomizing factors

# فصل ۲

# تعاریف و مفاهیم اولیه

پیش از مرور کارهای انجام شده در زمینه‌ی انتشار داده و حفظ حریم خصوصی و همچنین تشخیص فعالیت‌های کاربران در خانه های هوشمند نیاز است تا در ابتدا تعاریف و مفاهیمی پایه‌ای مورد نیاز ارائه گردد.

## ۲-۱ مفاهیم پایه

در حوزه خانه هوشمند و تشخیص فعالیت کاربران مفاهیم و اصطلاحات زیادی مطرح است که جهت شفاف‌سازی و ایجاد درک مشترک از مطالب ارائه شده، هر یک را به صورت دقیق تعریف می‌کنیم.

- همبستگی[۱]: همبستگی، ارتباط بین دو یا چند موجودیت[۲] را نشان می‌دهد که به معنی تاثیرگذاری آن‌ها روی یکدیگر است [؟].
- زمینه[۳]: با توجه به تعریف هونگ[۴] و همکاران [؟] و همچنین تعریف رودریگز[۵] و همکاران [؟]، زمینه به هرگونه اطلاعات که برای توصیف وضعیت یک موجودیت استفاده می‌شود گفته می‌شود. در این پژوهش از تعریف یسایی[۶] و همکاران [؟] استفاده شده است. این تعریف بیان می‌کند که زمینه شرایطی است که سیستم در آن کار می‌کند و آن شرایط بر نتیجه سیستم تاثیر می‌گذارد.

---

۱ Correlation
۲ Entity
۳ Context
۴ Hong
۵ Rodriguez
۶ Yasaei

- معناشناسی[۷]: شاخه‌ای از زبان‌شناسی و منطق است که تحلیل معنا و روابط بین کلمات را در خود دارد. زمانی که در سیستمی به اطلاعات معنا داده می‌شود به طوری که برای کاربران و رایانه‌ها قابل فهم و تعامل باشد، مجهز به ابزار معناشناسی است [؟].

- رخداد[۸]: داده دریافتی از حسگرها است که بیانگر حالت حسگر یا نقدار اندازه‌گیری شده توسط حسگر در لحظه‌ای از زمان است [؟].

- فعالیت[۹]: مجموعه‌ای از رخدادها که نمایانگار تاثیرات یک فعالیت انسانی، مانند ظرف شستن یا مسواک زدن، بر روی حسگرهای نصب شده در محیط باشد [؟].

- رفتار[۱۰]: در حالی که دسته‌ای از پژوهش‌ها [؟، ؟، ؟] دو واژه فعالیت و رفتار را هم‌معنی دانسته‌اند؛ در این پژوهش از تعریف دسته دیگر [؟، ؟] استفاده شده است که رفتار را یک سطح بالاتر و به عنوان مجموعه‌ای از فعالیت‌ها می‌دانند.

## ۲-۲ روش‌های داده‌محور، دانش‌محور و ترکیبی

روش‌ها در هوش مصنوعی به سه دسته‌ی داده‌محور[۱۱]، دانش‌محور[۱۲] و ترکیبی تقسیم می‌شوند [؟، ؟]:

- روش‌های داده‌محور: این روش‌ها به صورت خودکار و با استفاده از تکنیک‌های یادگیری ماشین[۱۳]، داده‌های جمع شده تا لحظه کنونی را تبدیل به مدل می‌کنند. روش‌های داده محور در محیط‌های پویا کاربردی بوده و دقت بالایی دارند اما در صورتی که نیاز به دانش با در نظر گرفتن زمینه باشد دچار مشکل می‌شود. با توجه به این مشکل امکان استفاده مجدد یک موجودیت برای موجودیت دیگر وجود ندارد و برای هر موجودیت مدلی جدا برای آموزش نیاز است. همچنین داده زیادی برای آموزش مورد نیاز است که زمانی طول می‌کشد تا به بهره‌وری برسد که اصطلاحا شروع سرد[۱۴] نام دارد. توجه شود که بعضی فعالیت‌ها به ندرت انجام شده و این فعالیت‌های مشاهده نشده نقطه ضعف این روش هستند چرا که تا زمان عدم مشاهده‌ی این فعالیت‌ها، مدل‌سازی ناقص بوده و حتی با گذشت زمان زیادی از یادگیری مدل، نمی‌توان اطمینان از کامل بودن آن داشت.

---

[۷] Semantics
[۸] Event
[۹] Activity
[۱۰] Behaviour
[۱۱] Data-driven
[۱۲] Knowledge-driven
[۱۳] Machine learning
[۱۴] Cold-start

- روش‌های دانش‌محور: در این دسته از روش‌ها فرد خبره[۱۵] با دانش پیشین از حوزه، مدل را به صورت دستی ایجاد می‌کند. این روش زمینه را در نظر می‌گیرد و قابلیت استفاده مجدد دارد. همچنین این روش مشکل شروع سرد را ندارد زیرا نیاز به داده اولیه برای آموزش ندارد و با توجه به دانش فرد خبره به خودی خود کامل است اما نیاز است تا فرد خبره دانش کامل و عمیقی داشته باشد. عیب دیگر این روش ایستا بودن آن است که تغییرات فعالیت کاربران لحاظ نمی‌شود و نیاز است به صورت دستی به‌روز شوند.

- روش‌های ترکیبی: این روش‌ها از ترکیب روش‌های داده‌محور و دانش‌محور استفاده می‌کنند تا محدودیت و نقاط ضعف این روش‌ها را برطرف نمایند و از نقاط قوت آن‌ها بهره ببرند.

## ۲-۳ هستی‌شناسی

هستی‌شناسی نمایش صوری[۱۶] دانش توسط مجموعه‌ای از مفاهیم[۱۷]، خصوصیات و محدودیتشان و همچنین روابط بین این مفاهیم است [؟]. هستی‌شناسی (تی‌باکس[۱۸]) به همراه مجموعه‌ای از نمونه‌ها[۱۹] (ای‌باکس[۲۰]) پایگاه دانش را تشکیل می‌دهند. ای باکس شامل نمونه‌هایی از عناصر تعریف شده در تی‌باکس است (به همراه روابط[۲۱]). هستی‌شناسی در حوزه‌های مختلف از جمله وب معنایی[۲۲]، موتورهای جستجو[۲۳]، تجارت الکترونیکی[۲۴]، پردازش زبان‌های طبیعی[۲۵]، مهندسی دانش[۲۶]، بازیابی اطلاعات[۲۷] و اینترنت اشیاء کاربرد دارد. از مزایای استفاده از هستی‌شناسی می‌توان به موارد زیر اشاره نمود:

- ایجاد یک فهم مشترک از ساختار اطلاعات
- امکان استفاده مجدد
- امکان تحلیل روی دانش

---

[۱۵] Expert
[۱۶] Formal
[۱۷] Concepts
[۱۸] Terminology box (TBox)
[۱۹] Instances
[۲۰] Assertion box (ABox)
[۲۱] Relations
[۲۲] Semantic web
[۲۳] Search engines
[۲۴] Electronic commerce
[۲۵] Natural Language Processing
[۲۶] Knowledge engineering
[۲۷] Data recovery

به طور کلی هستی‌شناسی شامل اجزای اصلی زیر است:

- مفاهیم: مجموعه یا کلاسی از موجودیت‌ها یا چیزهایی که درون یک حوزه وجود دارد.
- روابط: روابط یا ارتباطات برای بیان تعاملات بین مفاهیم و یا معین کردن ویژگی‌های یک مفهوم به کار می‌رود و در هستی‌شناسی دو نوع رابطه بین موجودیت‌ها وجود دارد. ارتباط رده‌بندی که سازماندهی مفاهیم در یک ساختار سلسله مراتبی را نشان می‌دهد مانند ارث‌بری کلاس‌ها در شیءگرایی و ارتباطات پیوندی که ارتباط مفاهیمی را با یکدیگر به نمایش می‌گذارد که در یک ساختار سلسله مراتبی به هم مرتبط نمی‌باشند.
- نمونه‌ها: اعضا یا نمونه‌ها همان چیزهایی هستند که توسط یک مفهوم معرفی می‌شوند مثلاً در حوزه مدارس، مدرسه‌ای با نام «مدرسه الف» عضوی از مفهوم مدرسه است. توجه باید کرد که یک هستی‌شناسی به خودی خود نمونه‌ای ندارد و صرفاً عبارت است از طراحی ساختاری از مفاهیم یک حوزه که ترکیب آن با اعضاء و نمونه‌ها، پایگاه دانش آن حوزه را ایجاد می‌نماید.
- قواعد[۲۸]: قاعده‌ها برای مقید کردن مقادیر برای کلاس‌ها یا ویژگی‌ها مورد استفاده قرار می‌گیرند. مثلاً می‌توان گفت سن یک انسان باید بیشتر از ۰ و کمتر از ۱۲۰ باشد.

تا کنون زبان‌های هستی‌شناسی زیادی توسعه یافته‌اند. این زبان‌ها عموما بر پایه زبان XML[۲۹] [؟] هستند که قابلیت تفسیر و سادگی معناشناسی برای ماشین را دارند. از این زبان‌ها می‌توان به RDF[۳۰] و RDF Schema [؟]، OIL[۳۱] + DAML[۳۲] [؟]، OWL [؟] و OWL2 [؟] اشاره کرد. یکی از پرکاربردترین آن‌ها OWL[۳۳] است که روی RDF و OIL + DAML توسعه یافته است و قدرت بیان بالایی دارد. OWL دارای سه زیرزبان OWL-Lite، OWL-Full و OWL-DL است و زبان توصیف قواعد SWRL[۳۴] [؟] امکان نوشتن قواعد را به OWL-DL اضافه کرده تا قدرت بیان آن را افزایش دهد.

---

[۲۸] Rules
[۲۹] eXtensible Markup Language
[۳۰] Resource Description Framework
[۳۱] Ontology Inference Layer
[۳۲] DARPA Agent Markup Language
[۳۳] Ontology Web Language
[۳۴] Semantic Web Rule Language

## ۲-۴ قوانین انجمنی

قوانین انجمنی[۳۵] در داده‌کاوی و یادگیری ماشین به دنبال کشف ارتباطات و تعاملات بین عناصر در مجموعه داده هستند [؟]. این نوع ارتباطها به طور معمول بر روی داده‌های تراکنشی مانند فروش‌های خرده‌فروشی یا خریدهای آنلاین کاربرد دارند. این قوانین دارای دو تعریف اساسی پشتیبانی[۳۶] و اطمینان[۳۷] هستند:

- پشتیبانی: پشتیبانی، فرکانس درست بودن یک قانون در یک مجموعه داده معین را اندازه گیری می‌کند و نشان دهنده نسبت تراکنش هایی است که هم موارد موجود در مقدمه و هم موارد موجود در نتیجه قانون را شامل می شود و کمک می‌کند تا کاربرد یک قانون مشخص شود، و از آن برای کشف قوانین رایج یا مکرر در مجموعه داده استفاده می‌شود.
- اطمینان: اطمینان، احتمال مشروط بودن موارد موجود در نتیجه یک قانون را با توجه به اینکه موارد موجود در مقدمه درست هستند، اندازه گیری می کند. در واقع قابلیت اطمینان یک قانون را نشان می‌دهد و اینکه هر چند وقت یک‌بار حضور عناصر را در نتیجه به درستی پیش‌بینی می‌کند، در حالی که عناصر مقدمه وجود دارند.

قوانین انجمنی برای کشف ارتباطات مفهومی و معنادار بین عناصر در مجموعه داده استفاده می‌شوند و در مواردی مانند تجزیه و تحلیل سبد خرید، سیستم‌های پیشنهادی، و اتخاذ تصمیمات در داده‌کاوی و تحلیل داده مورد استفاده قرار می‌گیرند.

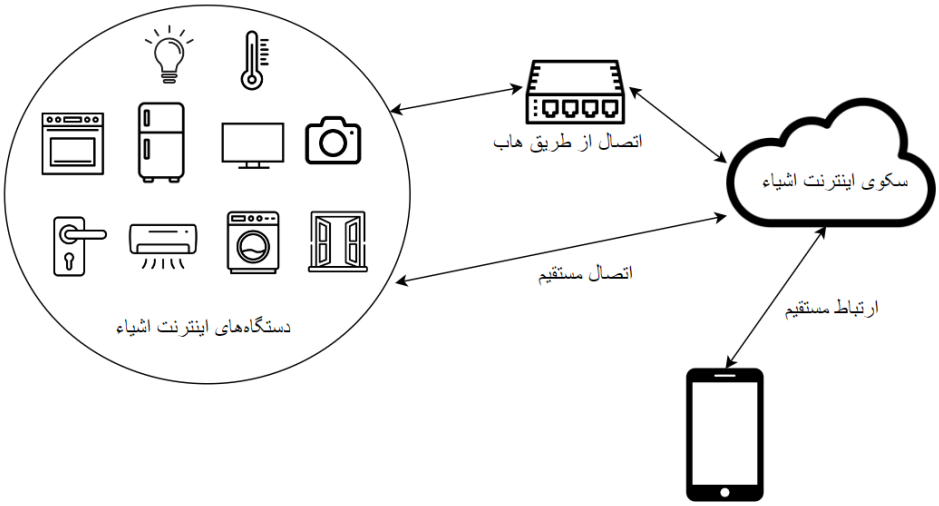
## ۲-۵ زیست‌بوم خانه‌های هوشمند

با استفاده از امکانات خانه‌های هوشمند کاربران می‌توانند دستگاه‌های اینترنت اشیاء را از راه دور کنترل کنند. ضمن این که کارهای مختلفی نیز می‌تواند به صورت خودکار برای سهولت زندگی انسان در این زیرساخت انجام شود. معماری رایج خانه‌های هوشمند در شکل ۲-۱ نشان داده شده است.

خانه های هوشمند شامل اجزای زیر هستند:

- دستگاه‌های اینترنت اشیاء: دستگاه‌های اینترنت اشیاء شامل حسگر و یا عملگرهایی[۳۸] هستند که حسگرها خصوصیتی را اندازه‌گیری می‌کنند و عملگرها کنشی را انجام می‌دهند. به عنوان مثال حسگر

[۳۵] Associative rules
[۳۶] Support
[۳۷] Confidence
[۳۸] Actuators




شکل ۲-۱: معماری رایج خانه‌های هوشمند [؟]

نور، نور محیط را اندازه‌گیری کرده و در صورت بالا بودن شدت نور، عملگر نور محیط را کم می‌کند. عملکرد یک عملگر می‌تواند به صورت خودکار یا به صورت دستی انجام شود. دستگاه‌ها در خانه هوشمند به دو دسته تقسیم می‌شوند [؟]:

- دستگاه‌های متصل به ابر[۳۹]: این دستگاه‌ها با تکنولوژی وای‌فای[۴۰] با زیرساخت ابری ارتباط برقرار می‌کنند. استفاده از وای‌فای به دلیل مصرف زیاد انرژی قابل استفاده در تمامی دستگاه‌ها نیست و اکثر دستگاه‌ها از تکنولوژی دیگری بهره می‌برند.
- دستگاه‌های متصل به هاب[۴۱]: این دستگاه‌ها دارای تکنولوژی وای‌فای نبوده و ارتباطشان با زیرساخت ابری از طریق تکنولوژی‌هایی با مصرف انرژی کم است. از این تکنولوژی‌ها می‌توان به زی‌ویو[۴۲] و زیگ‌بی[۴۳] اشاره کرد. این دستگاه‌ها از طریق هاب با زیرساخت ابری ارتباط برقرار می‌کنند.

دستگاه‌های خانه هوشمند ممکن است از یک یا هر دو نوع ذکر شده پشتیبانی کنند.

- هاب: هاب دستگاهی است که به امواج بی‌سیم با برد کم مانند زی‌ویو، زیگ‌بی و وای‌فای مجهز است. دستگاه‌های اینترنت اشیاء از طریق هاب با یکدیگر و زیرساخت ابری ارتباط برقرار می‌کنند.
- زیرساخت ابری: زیرساخت ابری پردازش‌های مربوطه را روی داده‌های دریافتی انجام می‌دهد و

[۳۹] Cloud
[۴۰] Wi-Fi
[۴۱] Hub
[۴۲] Z-Wave
[۴۳] Zigbee

امکان خودکارسازی امور را با استفاده از نرم‌افزارهای اینترنت اشیاء فراهم میکند.

- نرم‌افزار تلفن همراه: نرم‌افزار مدیریتی دستگاه‌ها و هاب که به کاربر این امکان را می‌دهد که تمامی اجزا را کنترل کند.

## ۲-۶ سکوهای اینترنت اشیاء

سکوهای اینترنت اشیاء امکان خودکارسازی ارتباطات بین دستگاه‌های اینترنت اشیاء با یکدیگر را فراهم می‌کند. این سکوها عموما از مدل رویداد_کنش استفاده می‌کنند. برنامه‌های اینترنت اشیاء می‌توانند روی این سکوها توسعه یافته و قوانین خودکارسازی خود را پیاده کنند. یعنی زمانی که رویدادی مشخص رخ دهد، سکو دستور مربوط به آن رخداد را ارسال می‌کند. امروزه سکوهای اینترنت اشیاء زیادی وجود دارد که می‌توان به IFTTT[۴۴] [؟]، اسمارت‌تینگز[۴۵] [؟]، اپن‌هاب[۴۶] [؟]، زپیر[۴۷] [؟]، اپل هوم‌کیت[۴۸] [؟] و مایکروسافت پاور اتومیت[۴۹] [؟] اشاره کرد. این سکوها از نظر زبان برنامه‌نویسی و معماری تفاوت دارند و به طور کلی همانطور که در بخش ۲-۴ اشاره شد به دو دسته ابرمحور و هاب‌محور تقسیم می‌شوند [؟]. در سکوهای ابرمحور مثل اسمارت‌تینگز که رایج‌تر هستند برنامه‌های اینترنت اشیاء روی زیرساخت ابری و در سکوهای هاب‌محور مثل اپل هوم‌کیت برنامه‌ها روی هاب اجرا می‌شوند.

---

[۴۴] If This Then That
[۴۵] SmartThings
[۴۶] OpenHAB
[۴۷] Zapier
[۴۸] Apple home kit
[۴۹] Microsoft power automate

# فصل ۳

# کارهای پیشین

تا کنون راهکارهای بسیاری برای شناسایی فعالیت کاربر و حفظ حریم خصوصی در خانه‌های هوشمند ارائه شده است که هر یک با فرضیات و دیدگاه متفاوتی اقدام به حل مساله کرده‌اند. در این فصل هستی‌شناسی‌های مختلف، روش‌های شناسایی رفتار کاربر و راهکارهای حفظ حریم خصوصی در خانه هوشمند را بررسی و دسته‌بندی کرده و به مقایسه راهکارهای ارائه شده خواهیم پرداخت.

## ۳-۱ هستی‌شناسی‌های حوزه اینترنت اشیاء

در حوزه اینترنت اشیاء هستی‌شناسی‌های متعددی تا کنون تعریف شده است که آن‌ها را از جهات مختلف می‌توان دسته‌بندی نمود. در پژوهشی که توسط باجاج[۱] و همکاران [؟] صورت گرفته است هستی‌شناسی‌های حوزه اینترنت اشیاء به چهار دسته زیر تقسیم شده است و در هر دسته نیز هستی‌شناسی‌ها بر اساس عمومی[۲] بودن و خاص‌دامنه[۳] بودن (مانند دامنه ساختمان‌های هوشمند) تفکیک شده‌اند. در این بخش به بررسی هر یک از این دسته‌ها می‌پردازیم.

---

[۱] Bajaj
[۲] Generic
[۳] Domain specific

### ۳-۱-۱ هستی‌شناسی مبتنی بر حسگر

هستی‌شناسی‌هایی که در این دسته قرار می‌گیرند مفاهیمی را در رابطه با حسگرها مانند داده‌های نمایش داده شده[۴] توسط آن‌ها، قابلیت‌های حسگرها[۵] (مانند میزان دقت و گستره پوشش آن‌ها)، توسعه‌پذیری حسگرها[۶]، نحوه به اشتراک‌گذاری داده‌ها[۷] و اکتشاف حسگرها[۸] را دربر می‌گیرند. هر یک از هستی‌شناسی‌های این دسته تنها بخشی از نیازهای موجود را پوشش داده‌اند.

در این دسته از هستی‌شناسی‌ها می‌توان به SSN[۹] اشاره نمود که یک هستی‌شناسی مبتنی بر حسگر در زیردسته کاربردهای عمومی است و توسط W3C[۱۰] پیشنهاد شده است [؟]. هدف هستی‌شناسی SSN حل مشکل ناهمگونی[۱۱] در داده‌های نمایشی و اکتشاف حسگرهاست اما مفاهیمی که پشتیبانی می‌کند محدود است. ژو[۱۲] و همکاران [؟] یک هستی‌شناسی با مفهوم نوع حسگر (عادی یا پیشرفته) و قابلیت حسگر (ایستا یا پویا) معرفی کرده‌اند که برای تعداد محدودی حسگر، توصیف معنایی ارائه می‌کند. جرارد[۱۳] و همکاران [؟] با معرفی هستی‌شناسی به نام M3 مشکل محدودیت تعداد حسگرها را برطرف کرده‌اند و با توسعه‌ی هستی‌شناسی SSN، دامنه و مشاهدات حسگرها را پشتیبانی کرده و از آن‌ها برای استنتاج روی قواعد زمینه‌ای استفاده می‌کنند.

از آنجایی که ابزار ارتباط با حسگرها ممکن است تلفن همراه باشد که به صورت پویا جابجا می‌شود، اکتشاف حسگرها چالشی مهم است که روسومانو[۱۴] و همکاران [؟] در پژوهشی یک هستی‌شناسی معرفی کرده‌اند که برای شناسایی رفتار، ارتباط، عملکرد و ابرداده‌ی حسگرها استفاده می‌شود. محدودیت این راهکار، پیچیدگی زیاد و ناتوانی در توصیف مشاهدات حسگرهاست که نیلز[۱۵] و همکاران [؟] این مشکل را با طرح یک هستی‌شناسی مرتبط با مفاهیم SSN حل کردند.

هیرمر[۱۶] و همکاران [؟] هستی‌شناسی برای ثبت حسگرهای جدید به صورت پویا معرفی کرده‌اند. در این پژوهش خصیصه‌هایی مانند نوع داده‌های حسگر مشاهده شده و با نوع داده‌های حسگر که توسط تولیدکننده‌ی حسگر اعلام شده مقایسه می‌گردد تا نوع حسگر تشخیص داده شود. در پژوهش شی[۱۷] و

[۴] Sensor data description
[۵] Sensor capabilities
[۶] Sensor extensibility
[۷] Data access & sharing
[۸] Sensor discovery
[۹] Semantic Sensor Network
[۱۰] World Wide Web Consortium
[۱۱] Heterogeneity
[۱۲] Xue
[۱۳] Gyrard
[۱۴] Russomanno
[۱۵] Niles
[۱۶] Hirmer
[۱۷] Shi

همکاران [؟] این امر خودکار شده و با توجه به محیط حسگر، زمان ارسال داده و موقعیت آن داده‌های مشاهده شده توسط حسگر دریافت شده و ماهیت حسگر تشخیص داده می‌شود.

در زیردسته کاربردهای خاص‌دامنه می‌توان به پژوهش دنیل[۱۸] و همکاران [؟] اشاره نمود که برای استفاده و مدیریت لوازم خانگی هوشمند استفاده می‌شود. در پژوهش دیگری از دنیل و همکاران [؟] توسعه‌ای روی پژوهش قبلی انجام شد که با استانداردهای مصرف انرژی خود را تطبیق داد. پژوهشی خاص‌دامنه دیگر، پژوهش دی[۱۹] و همکاران [؟] است که هستی‌شناسی روسومانو و همکاران [؟] را برای دامنه انرژی توسعه داده است. پژوهش دیگری برای دامنه مدیریت ساختمان توسط بالاجی[۲۰] و همکاران [؟] انجام شده که برای تشخیص حسگرها از برچسب استفاده می‌کنند.

هستی‌شناسی دیگری توسط هاچم[۲۱] و همکاران [؟] معرفی شده است که در حوزه خانه‌های هوشمند برای مقابله با چالش‌هایی مانند تفاوت در وضوح حسگرها که ممکن است باعث شود که چند سرویس در نهایت فعال‌کننده‌ای را در وضعیت‌هایی متضاد با یکدیگر فعال نمایند، کاربرد دارد. این هستی‌شناسی به مفاهیمی مانند حسگرها و ویژگی‌های آن‌ها، وضوح اندازه‌گیری و خطاهای مرتبط با حسگرها و جایگاه حسگرها در خانه هوشمند به همراه همه واحدهای قابل اندازه‌گیری آن‌ها می‌پردازد.

### ۳-۱-۲ هستی‌شناسی مبتنی بر زمینه

هستی‌شناسی‌های این دسته با توصیف زمینه و دسته‌بندی داخلی یا خارجی تعریف می‌شوند [؟] و عمدتا از نوع خاص‌دامنه هستند.

در زیردسته کاربردهای عمومی، هستی‌شناسی‌های مبتنی بر زمینه برای توصیف داده‌های حسگرها به کار می‌روند [؟]. بالدوف[۲۲] و همکاران [؟] هستی‌شناسی با دسته‌بندی خارجی یا داخلی معرفی کرده‌اند که زمینه‌های خارجی، با حسگر فیزیکی و زمینه‌های داخلی، با تعاملات کاربران اندازه‌گیری می‌شوند. چن[۲۳] و همکاران [؟] یک هستی‌شناسی برای محیط هوشمند ارائه کرده‌اند که هر موجودیت را با استفاده از موقعیت جغرافیایی و توضیحات آن توصیف می‌کند. هابز[۲۴] و همکاران [؟] به کمک حسگرهای فیزیکی و مجازی تلفن همراه هستی‌شناسی مبتنی بر زمینه‌ای معرفی کرده‌اند که نتایج استنتاج در این پژوهش، از اطلاعات جی‌پی‌اس[۲۵] بسیار دقیق‌تر می‌باشد.

---

[۱۸] Daniele
[۱۹] Dey
[۲۰] Balaji
[۲۱] Hachem
[۲۲] Baldauf
[۲۳] Chen
[۲۴] Hobbs
[۲۵] GPS

در زیردسته کاربردهای خاص‌دامنه می‌توان به پژوهش اوکیو[۲۶] و همکاران [؟] اشاره کرد که برای توصیف معنایی فعالیت روزانه کاربر[۲۷] به کار می‌رود و از این هستی‌شناسی برای استنتاج فعالیت‌های پیچیده استفاده می‌شود. عیب این پژوهش در نظر نگرفتن فعالیت‌های گروهی مانند جلسات و مهمانی‌هاست که باعی[۲۸] و همکاران [؟] این مشکل را حل کرده‌اند. این پژوهش با شناسایی حسگرها و و موقعیت آن‌ها توانایی استنتاج روی فعالیت‌ها و تفکیک فعالیت‌های انفرادی و گروهی را دارد.

در پژوهشی دیگر، لی[۲۹] و همکاران [؟] هستی‌شناسی فعالیت دانشگاه را معرفی کردند که فعالیت افراد داخل دانشگاه را مورد بررسی قرار می‌دهد. در این پژوهش از مدل‌سازی درختی مفاهیم استفاده شده و برای هر بخش از یک زیرهستی‌شناسی[۳۰] برای تمایز با سایر بخش‌ها استفاده شده است و هر مفهوم جدید که وارد شود، موقعیت پایین‌تری در درخت مفاهیم خواهد داشت.

پژوهش دیگری که توسط چن و همکارانش [؟] برای شناسایی رفتار کاربر در خانه هوشمند ایجاد شده است، در زیر دسته کاربرد خاص قرار می‌گیرد. در این هستی‌شناسی بر ایجاد پروفایل کاربر ناشی از انجام فعالیت تاکید شده است و در آن پروفایل کاربر دارای دو بخش اطلاعات ایستا (مانند سن، نام و نقش کاربر) و اطلاعات پویا (مانند ترجیحات کاربر در انجام فعالیت مانند طول زمان انجام فعالیت، مکان انجام فعالیت، طریقه خاص انجام فعالیت) است [؟].

### ۳-۱-۳ هستی‌شناسی مبتنی بر مکان

هستی‌شناسی مبتنی بر مکان برای توصیف زمینه‌ی فیزیکی کاربران و دستگاه‌ها استفاده می‌شود. با اینکه مکان خود نوعی زمینه می‌باشد اما می‌توان هستی‌شناسی‌هایی که صرفاً به این مفهوم پرداخته‌اند را در دسته‌بندی جداگانه‌ای قرار داد چون بسیاری از آن‌ها را در حوزه‌هایی فراتر از اینترنت اشیاء می‌توان استفاده نمود.

در این دسته از هستی‌شناسی‌ها می‌توان به هستی‌شناسی WGS84[۳۱] که توسط برکلی[۳۲] [؟] ارائه شده است، اشاره نمود که در زیردسته کاربردهای عمومی قرار دارد. این هستی‌شناسی با استفاده از طول[۳۳] و عرض[۳۴] جغرافیایی، موقعیت موجودیت‌ها را توصیف کرده و مفهوم انتزاعی برای موجودیت‌های فضایی[۳۵]

[۲۶] Okeyo
[۲۷] Activity of Daily Living (ADL)
[۲۸] Bae
[۲۹] Lee
[۳۰] sub-Ontology
[۳۱] World Geodetic System version 84
[۳۲] Brickley
[۳۳] Longitude
[۳۴] Latitude
[۳۵] SpatialThings

مانند ساختمان و موجودیت‌های موجودیت‌های زمانی[۳۶] مانند مدت زمان ارائه می‌کند. هستی‌شناسی با توصیف بهتر در پژوهش فلوری[۳۷] و همکاران [؟] معرفی شده است که با مدل ریاضی، توصیفات مختلف مکانی دسته‌بندی می‌شود. در پژوهش دیگری، کیم[۳۸] و همکاران [؟] با استفاده از داده‌ی حسگرها و استنتاج روی آن‌ها موقعیت کاربران را تخمین می‌زنند.

در زیردسته کاربردهای خاص‌دامنه می‌توان به پژوهش سزاس[۳۹] و همکاران [؟] اشاره نمود که هستی‌شناسی مبتنی بر مکان برای دامنه داخل ساختمان و موقعیت‌یابی در آن است و از مفاهیم مختلفی از هستی‌شناسی‌های دیگر بهره می‌برد. این هستی‌شناسی قابل تعمیم برای استفاده در محیط خارج از ساختمان نیز می‌باشد.

### ۳-۱-۴ هستی‌شناسی مبتنی بر زمان

زمان یک زمینه موقتی است و هستی‌شناسی‌های این دسته برای نمایش این مفهوم موقتی مورد استفاده قرار می‌گیرند.

در زیردسته کاربردهای عمومی از این هستی‌شناسی می‌توان به پژوهش فیکس[۴۰] و همکاران [؟] اشاره نمود که بر اساس خصیصه زمان، فاصله موجودیت‌ها را تعیین می‌کند. پر استفاده‌ترین هستی‌شناسی این دسته OWL-Time است که در آن مفاهیمی مانند زمان و تاریخ بر اساس موقعیت جغرافیایی تعریف شده‌اند و توسط هابز و همکاران [؟] معرفی شده‌اند.

پوستجوفستکی[۴۱] و همکاران [؟] هستی‌شناسی مبتنی بر زمان در زیردسته کاربردهای خاص‌دامنه تعریف کرداند که بر پایه مدت زمان و رویداد است از پردازش زبان طبیعی بهره می‌برد. دی و همکاران [؟] این پژوهش را توسعه داده و برای حسگرهای انرژی کاربرد دارد. در پژوهش دیگری ژانگ[۴۲] و همکاران [؟] بر اساس فرهنگ و تاریخ، رویدادها را تشخیص داده و از تقویم چینی برای تشخیص زمان‌های مهم و موقتی استفاده کرده است.

### ۳-۱-۵ جمع‌بندی

در این بخش پژوهش‌های مربوط به انواع هستی‌شناسی در حوزه اینترنت اشیاء را بر اساس دسته‌بندی باجاج و همکاران [؟] بررسی کردیم. این دسته‌بندی بر اساس دامنه و کاربرد هر یک از هستی‌شناسی‌های حوزه

[۳۶] TemporalThings
[۳۷] Flury
[۳۸] Kim
[۳۹] Szász
[۴۰] Fikes
[۴۱] Pustejovsky
[۴۲] Zhang

اینترنت اشیاء ارائه شده است. جمع‌بندی کلی این هستی‌شناسی‌ها در جدول ۳-۱ قابل مشاهده است.

جدول ۳-۱: جمع‌بندی کلی هستی‌شناسی‌های حوزه اینترنت اشیاء

| پژوهش | دسته‌بندی | کاربرد | ویژگی‌های راهکار |
|---|---|---|---|
| W3C [؟] | مبتنی بر حسگر | عمومی | حل ناهمگونی داده‌های نمایشی |
| ژو و همکاران [؟] | مبتنی بر حسگر | عمومی | توصیف معنایی تعداد محدودی حسگر |
| جرارد و همکاران [؟] | مبتنی بر حسگر | عمومی | توسعه SSN و حل مشکل محدودیت تعداد حسگر |
| روسومانو و همکاران [؟] | مبتنی بر حسگر | عمومی | شناسایی حسگرها در محیط پویا و ناتوان در توصیف مشاهدات حسگرها |
| نیلز و همکاران [؟] | مبتنی بر حسگر | عمومی | حل مشکل ناتوانی در توصیف مشاهدات حسگرها با استفاده از مفاهیم SSN |
| هیرمر و همکاران [؟] | مبتنی بر حسگر | عمومی | شناسایی حسگرها در محیط پویا با استفاده از نوع داده‌ی حسگرها |
| شی و همکاران [؟] | مبتنی بر حسگر | عمومی | خودکارسازی شناسایی حسگرها با استفاده از فواصل زمانی داده‌های ارسالی |
| دنیل و همکاران [؟] | مبتنی بر حسگر | خاص‌دامنه | مدیریت لوازم خانگی هوشمند |
| دنیل و همکاران [؟] | مبتنی بر حسگر | خاص‌دامنه | مدیریت لوازم خانگی هوشمند منطبق با استانداردهای انرژی |
| دی و همکاران [؟] | مبتنی بر حسگر | خاص‌دامنه | توسعه‌ی [؟] برای دامنه انرژی |
| بالاجی و همکاران [؟] | مبتنی بر حسگر | خاص‌دامنه | مدیریت ساختمان با برچسب‌گذاری روی حسگرها |
| هاچم و همکاران [؟] | مبتنی بر حسگر | خاص‌دامنه | مدیریت عملکرد حسگرها |
| بالدوف و همکاران [؟] | مبتنی بر زمینه | عمومی | زمینه حسگر فیزیکی و تعاملات کاربران |
| چن و همکاران [؟] | مبتنی بر زمینه | عمومی | استفاده از محیط جغرافیایی موجودیت‌ها |
| هابز و همکاران [؟] | مبتنی بر زمینه | عمومی | استفاده از حسگرهای تلفن همراه و ارائه موقعیت مکانی دقیق‌تر از جی‌پی‌اس |
| اوکیو و همکاران [؟] | مبتنی بر زمینه | خاص‌دامنه | توصیف معنایی فعالیت روزانه کاربر (بدون فعالیت‌های گروهی) |
| باعی و همکاران [؟] | مبتنی بر زمینه | خاص‌دامنه | توصیف فعالیت‌های روزانه کاربر با دسته‌بندی انفرادی و گروهی |
| لی و همکاران [؟] | مبتنی بر زمینه | خاص‌دامنه | هستی‌شناسی فعالیت‌های دانشگاه |
| چن و همکارانش [؟] | مبتنی بر زمینه | خاص‌دامنه | ایجاد پروفایل کاربر در خانه هوشمند با اطلاعات ایستا و پویا |
| برکلی [؟] | مبتنی بر مکان | عمومی | توصیف طول و عرض جغرافیایی برای موقعیت موجودیت‌ها |
| فلوری و همکاران [؟] | مبتنی بر مکان | عمومی | دسته‌بندی توصیفات مکانی با مدل ریاضی |
| کیم و همکاران [؟] | مبتنی بر مکان | عمومی | تخمین موقعیت کاربر با استفاده از داده‌های حسگرها |
| سزاس و همکاران [؟] | مبتنی بر مکان | خاص‌دامنه | موقعیت‌یابی داخل ساختمان |
| فیکس و همکاران [؟] | مبتنی بر زمان | عمومی | تعیین فاصله با استفاده از فواصل زمانی داده‌ها |
| هابز و همکاران [؟] | مبتنی بر زمان | عمومی | تعریف خصیصه‌های زمان با استفاده از موقعیت جغرافیایی |
| پوستجوفستکی و همکاران [؟] | مبتنی بر زمان | خاص‌دامنه | تعریف بر اساس رویداد و مدت زمان با استفاده از پردازش زبان طبیعی |
| دی و همکاران [؟] | مبتنی بر زمان | خاص‌دامنه | توسعه [؟] و استفاده در دامنه انرژی |
| ژانگ و همکاران [؟] | مبتنی بر زمان | خاص‌دامنه | استفاده از فرهنگ و تاریخ و تقویم چینی برای توصیف موقت رویدادهای زمانی |

## ۳-۲ تشخیص فعالیت‌های کاربران در خانه های هوشمند

فعالیت کاربر، به هرگونه اقدام، رفتار و یا حرکت از سمت انسان گفته می‌شود که این فعالیت‌ها شامل طیف وسیعی از اقداماتی است که انسان به عنوان بخشی از کارهای روزمره یا وظایف خود انجام می‌دهد.

تشخیص فعالیت کاربر[۴۳] اقدامی خودکار است که کار شناسایی و دسته‌بندی فعالیت‌های کاربر را با استفاده از اطلاعات دریافت شده از حسگرها انجام می‌دهد [؟]. به طور مثال روشن کردن لامپ خانه یک نمونه فعالیت از جانب کاربر است که حسگر تشخیص نور، افزایش نور را تشخیص می‌دهد و به صورت خودکار می‌توان متوجه روشن شدن لامپ توسط کاربر شد.

راهکارهایی که تا کنون برای مدل‌سازی و تشخیص فعالیت‌های کاربران در خانه‌های هوشمند ارائه شده است به طور کلی در سه دسته داده محور، دانش محور و ترکیبی قرار دارند که مزایا و معایب هر یک در بخش ۲-۲ شرح داده شد. در این بخش پژوهش‌های انجام شده در این زمینه را بررسی می‌کنیم تا راهکارهای مختلف مدل‌سازی فعالیت‌های کاربران را بدانیم و در راهکار پیشنهادی از مدل‌سازی مناسب استفاده کنیم.

### ۳-۲-۱ راهکارهای داده‌محور

مدت زیادی است که در بسیاری از پژوهش‌های مدل کردن قعالیت‌های کاربران در خانه‌های هوشمند، تکنیک‌های یادگیری ماشین استفاده می‌گردد. این راهکارها عموما از مدل‌های آماری و احتمالاتی مثل دسته‌بند بیز ساده[۴۴] [؟]، شبکه‌های بیزین[۴۵] [؟، ؟]، مدل پنهان مارکوف[۴۶] [؟، ؟، ؟]، خوشه‌بندی[۴۷] سلسله‌مراتبی [؟]، فرایندهای تصمیم مارکوف تا حدودی مشاهده‌پذیر[۴۸] [؟] و مدل پنهان مارکوف جفت‌شده[۴۹] [؟] استفاده می‌کنند.

راهکارهایی مبتنی بر تکنیک‌های دسته‌بندی مثل استفاده از نزدیک‌ترین همسایه[۵۰] [؟]، استفاده از ماشین بردار پشتیبان[۵۱] [؟]، استفاده از درخت‌های تصمیم[۵۲] [؟]، میدان تصادفی شرطی سلسله‌مراتبی [؟] و دسته‌بندهای استفاده از فراسطح[۵۳] که از ترکیب نتایج چندین دسته‌بند پایه استفاده می‌کنند [؟] نیز ارائه شده اند که توالی‌ای از مشاهدات حسگرها را به نزدیک‌ترین فعالیت انتساب می‌دهند.

راهکارهای دیگری نیز وجود دارند که از تکنیک‌های داده‌کاوی [؟]، استفاده از یادگیری استقرایی[۵۴]

[۴۳] Human activity recognition (HAR)
[۴۴] Naive bayes
[۴۵] Bayesian networks
[۴۶] Hidden markov model
[۴۷] Clustering
[۴۸] Partially observable
[۴۹] Coupled hidden markov model
[۵۰] Nearest neighbor
[۵۱] Support vector machine
[۵۲] Decision tree
[۵۳] Meta-level
[۵۴] Inductive learning

[؟، ؟] و استفاده از شبکه عصبی[۵۵][؟] بهره برده‌اند.

### ۳-۲-۲ راهکارهای دانش‌محور

راهکارهای دانش‌محور خود در دو دسته قرار دارند. دسته اول،راهکارهایی هستند که از منابع موجودی که مثل اسناد وب در دسترس عموم هستند استفاده می‌کنند [؟، ؟، ؟]. این راهکارها با استفاده از تکنیک‌های بازیابی اطلاعات تعاریف فعالیت‌ها را به دست می‌آورند و سپس با استخراج روابط آن‌ها فعالیت‌ها را مدل می‌کنند. دسته دوم، راهکارهایی هستند که یک فرد با دانش خبره، مدل فعالیت‌ها را به صورت دستی وارد می‌کند [؟، ؟، ؟، ؟].

راهکارهای دانش‌محور با استفاده از ابزارهای نمایش دانش برای مدل کردن فعالیت‌ها و تحلیل استفاده از استدلال منطقی[۵۶]، کار می‌کنند که هستی‌شناسی به دلیل سادگی و انعطاف بالا در ارائه فعالیت‌ها و روابطشان، استفاده بیشتری نسبت به سایر روش‌های نمایش دانش دارد [؟]. برخی از راهکارهای مبتنی بر هستی‌شناسی برای شناسایی فعالیت‌های عادی و روزمره، از عوامل زمینه‌ای بهره برده‌اند [؟، ؟، ؟] اما همبستگی زمانی را در نظر نگرفته‌اند.

در راهکار پیشنهادی توسط ریبونی[۵۷] و همکاران [؟] ویژگی‌های زمانی مثل استفاده‌ی اخیر در تعریف فعالیت‌ها آورده شده است. برخی دیگر از فعالیت‌های مبتنی بر هستی‌شناسی تمرکز روی مدل‌سازی فعالیت‌های کاربران، مستقل از شیوه‌ی انجام فعالیت توسط یک کاربر مشخص دارند [؟، ؟، ؟، ؟]. در نظر نگرفتن شیوه‌ی انجام فعالیت‌ها توسط هر کاربر باعث می‌شود تا امکان توسعه برنامه‌های مختلف با توجه به ترجیحات هر کاربر وجود نداشته باشد.

راهکار پیشنهادی توسط چن و همکاران [؟] فعالیت‌های کاربران را در دو سطح درشت‌دانه[۵۸] و ریزدانه[۵۹] به صورت انتزاعی مدل می‌کند. در مدل‌های درشت‌دانه فعالیت‌های کاربران با تعدادی ویژگی توصیف می‌شوند که این ویژگی‌ها نوع موجودیت مدنظر برای انجام یک فعالیت را توصیف می‌کنند. ولیکن در مدل‌های ریزدانه شیوه‌ی انجام فعالیت‌ها توسط هر کاربر را در نظر گرفته و توصیف می‌شود. این پژوهش با استفاده از استنتاج روابط شمول[۶۰] و استفاده از منطق توصیفی[۶۱] الگوریتمی ارائه می‌دهد که فعالیت‌ها به صورت تدریجی شناسایی می‌شوند. این راهکار ابتدا از فعالیت‌های درشت‌دانه شروع کرده و خود را به

[۵۵] Neural network
[۵۶] Logical reasoning
[۵۷] Riboni
[۵۸] Coarse-grained
[۵۹] Fine-grained
[۶۰] Subsumption reasoning
[۶۱] Description logic

فعالیت‌های ریزدانه می‌رساند و به طور کلی شناسایی فعالیت در هر دو سطح درشت‌دانه و ریزدانه انجام می‌گردد.

راهکار دیگری توسط اکیو و همکاران [؟] مطرح شده است که با استفاده از توالی زمانی بین چند فعالیت، یک فعالیت مرکب و همچنین موجودیت‌های درگیر در آن‌ها را در نظر می‌گیرد. مدیتسکوس[۶۲] و همکاران [؟] در پژوهش خود، علاوه بر فعالیت‌های مرکب، سلسله‌مراتب فعالیت‌ها را نیز در نظر گرفته‌اند.

### ۳-۲-۳ راهکارهای ترکیبی

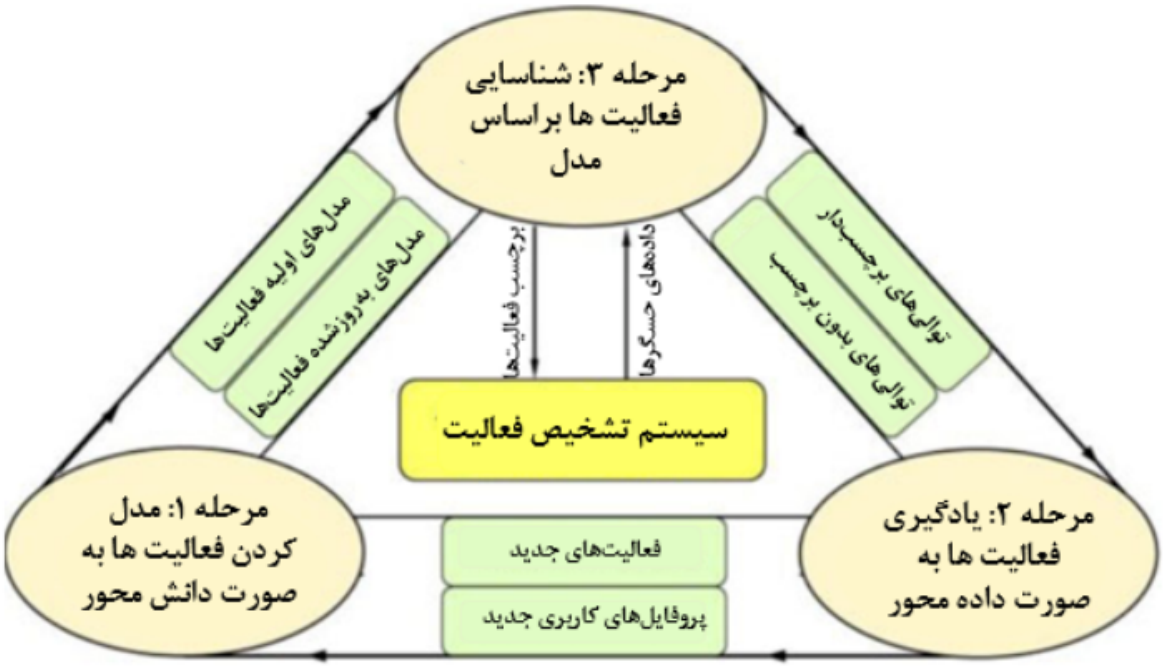
همانطور که در بخش ۲-۲ شرح داده شد هر یک از روش‌های داده‌محور و دانش‌محور معایبی دارند. یک سیستم تشخیص فعالیت باید تمامی فعالیت‌ها را با دقت بالا مدل کند. زیرا در صورت وجود فعالیتی مدل نشده، سیستم قادر به شناسایی دقیق آن فعالیت نیست. از طرفی در یک خانه هوشمند فعالیت‌های قابل انجام زیادی امکان‌پذیر است و وارد کردن تمامی آن‌ها به صورت دستی توسط فرد خبره عملا ناممکن است. همچنین دانش فرد خبره پویا نیست و تغییرات فعالیت‌ها و رفتارهای کلی کاربران را در دسترس ندارد. از طرف دیگر برای جلوگیری از شروع سرد در روند یادگیری روش‌های داده‌محور، به دانش فرد خبره نیاز است. به منظور فائق آمدن بر معایب این دو روش، راهکارهای ترکیبی ارائه شده‌اند.در جدول ۳-۲ می‌توان مقایسه‌ی کلی روش‌های ترکیبی را مشاهده کرد.

ریبونی و همکاران [؟] برای اولین بار از ترکیب روش‌های یادگیری ماشین (داده‌محور) و هستی‌شناسی (دانش‌محور) استفاده کردند. در این پژوهش با استفاده از روش‌های آماری تعدادی فعالیت به عنوان فعالیت احتمالی انجام شده انتخاب می‌شوند و سپس با استفاده از هستی‌شناسی، فعالیتی با احتمال وقوع بیشتر انتخاب می‌گردد.

چن و همکاران [؟، ؟] روش ترکیبی مطرح کردند که از یک فرایند سه مرحله‌ای تکرارشونده استفاده می‌کند. همانطور که در شکل ۳-۱ مشاهده می‌شود، در مرحله اول فرد خبره به صورت دستی دانش خود را برای ایجاد مدل‌های اولیه می‌دهد. در مرحله دوم تشخیص فعالیت‌ها با استفاده از دانش ارائه شده در مرحله اول انجام می‌گردد اما اگر فعالیتی مدل نشده باشد آن را شناسایی نمی‌کند و خروجی این مرحله سلسله داده‌هایی است که توسط حسگرها ارسال شده اما فعالیت مربوط به آن‌ها شناسایی نشده‌اند. در مرحله سوم با استفاده از روش‌های مبتنی بر داده‌کاوی، خروجی مرحله دوم را تحلیل کرده و پروفایل شخصی هر کاربر و همچنین فعالیت‌های جدید را یاد می‌گیرد. حال بر اساس شباهت سلسله داده‌های دریافتی از حسگرها، فعالیت‌ها گروه‌بندی شده و چنانچه اعضای یک گروه از تعداد مشخصی بیشتر شود،

[۶۲] Meditskos

آن فعالیت‌های شناسایی شده به بخش هستی‌شناسی سیستم اضافه می‌شوند. برچسب‌گذاری هر فعالیت و محل انجامش در سلسله فعالیت‌ها به صورت دستی انجام می‌شود.




شکل ۳-۱: فرایند سه مرحله‌ای تکرارشونده‌ی مدل کردن فعالیت‌ها در راهکار چن و همکاران [؟]

عبدالصکور[۶۳] و همکاران [؟] برای غلبه بر مشکل ناکامل بودن و به‌روز نبودن دانش فرد خبره، از ترکیب هستی‌شناسی و دسته‌بندهای بیز ساده، ماشین بردار پشتیبان و شبکه عصبی پرسپترون چند لایه[۶۴] استفاده کرده‌اند. از آنجایی که به دلیل خرابی حسگرها و یا تغییر شیوه انجام فعالیت‌ها توسط کاربران سیستم دچار خطا و عدم قطعیت می‌شود، رودریگز و همکاران [؟] یک منطق فازی[۶۵] برای نمایش فعالیت‌ها ارائه کردند که امکان مدل‌سازی دانش غیرقطعی و مبهم را دارد. به این صورت که بر خلاف منطق دودویی که در آن هر عبارت به غلط یا درست قابل ارزیابی است، از منطق فازی[۶۶] استفاده می‌کند که میزان درستی هر عبارت مقداری بین صفر تا یک است.

گایاتری[۶۷] و همکاران [؟] از ترکیب هستی‌شناسی و شبکه منطق مارکوف[۶۸] استفاده کرده‌اند. به این صورت که تی‌باکس به منطق مرتبه اول[۶۹] تبدیل می‌شود و با استفاده از نمونه‌های موجود در ای‌باکس، وزن‌ها محاسبه می‌شوند تا به فعالیت‌ها در شبکه منطق مارکوف، وزنی اختصاص یابد و توالی احتمالاتی فعالیت‌ها را داشته باشند.

---

[۶۳] A. Sukor
[۶۴] Multi-layer perceptron neural network
[۶۵] Fuzzy logic
[۶۶] Fuzzy logic
[۶۷] Gayathri
[۶۸] Markov logic network
[۶۹] First order logic

راهکار دیگری توسط ریبونی و همکاران [؟] مطرح شد که با استفاده از استنتاج روی هستی‌شناسی، همبستگی معنایی بین فعالیت‌ها و نتایج رخداد هر یک استخراج می‌شود، سپس با استفاده از اطلاعات به دست آمده، فعالیت کاندید بعدی را شناسایی می‌کند. برخی فعالیت‌ها الگوهای مشابهی دارند و سیستم‌های مطرح شده در تشخیص دقیق این فعالیت‌ها ممکن است با مشکل مواجه شوند. در راهکار دیگر که توسط بتینی[۷۰] و همکاران [؟] مطرح شده است، شناسایی فعالیت‌ها به کمک حسگرهای تلفن همراه انجام می‌شود و برای این منظور از یادگیری نیمه‌نظارتی[۷۱] و استنتاج مبتنی بر هستی‌شناسی و همچنین اطلاعات زمینه‌ای استفاده نی‌شود. در این راهکار داده‌های دریافت شده از حسگرها که با اطلاعات زمینه‌ای نظیر مکان کاربر، طبق روابط معنایی تعریف شده در هستی‌شناسی همخوانی ندارند حذف شده و در گام آخر، اگر میزان اطمینان فعالیت شناسایی شده از حد مشخصی کمتر باشد، از کاربر استعلام فعالیت کنونی را گرفته و برچسب‌گذاری انجام می‌گردد. با انجام این فرایند، مدل همواره در حال یادگیری و به‌روز شدن است.

### ۳-۲-۴ جمع‌بندی

در این بخش، پژوهش‌های انجام شده در حوزه مدل‌سازی و تشخیص فعالیت‌های کاربران در خانه‌های هوشمند بررسی و از نظر نوع رویکرد در دریافت اطلاعات مورد نیاز دسته‌بندی شدند. مقایسه‌ی کلی پژوهش‌های مطرح شده در جدول ۳-۲ قابل مشاهده است.

## ۳-۳ حفظ حریم خصوصی مبتنی بر سکوی نامعتمد

تاکنون پژوهش‌های زیادی در جهت حفظ حریم خصوصی کاربر در حوزه‌های مختلف صورت پذیرفته است. مانند تحقیقاتی که در حوزه حفظ حریم خصوصی کاربر در داده کاوی[۷۲]، انتشار اطلاعات، واکشی اطلاعات، و شبکه‌های ناامن صورت گرفته است. از منظر سکوهای اینترنت اشیاء نیز حفظ حریم خصوصی کاربر در ابعاد مختلف بررسی شده است مانند امنیت در محل ذخیره سازی داده‌ها، امنیت در واکشی، اعتبارسنجی داده‌هایی که در سکو ذخیره می‌گردد و حفظ محرمانگی داده‌های کاربران در سرویس‌دهنده و یا سکوی نامعتمد [؟]. این موضوع بیانگر جنبه‌های امنیتی گسترده‌ای است که کاربر را با تهدید مواجه می‌نماید.

راهکارهایی که در هر یک از حوزه‌های مورد اشاره ارائه شده است بعضاً قابل تعمیم به حوزه‌های دیگر هم هستند. برای مثال در حوزه داده کاوی (که بر ذخیره داده‌های کاربران در طول زمان بر روی

[۷۰] Bettini
[۷۱] Semi-supervised learning
[۷۲] Data mining

جدول ۳-۲: مقایسه کلی روش‌های ترکیبی

| پژوهش | راهکار | چالش‌ها | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | محدودیت‌های راهکارهای دانش‌محور | | | محدودیت‌های راهکارهای داده‌محور | | | پیچیدگی‌های شناسایی فعالیت | |
| | | ناکامل بودن دانش فرد خبره | عدم به روز شدن خودکار | عدم توانایی در مواجهه با عدم قطعیت | شروع سرد | عدم امکان استفاده مجدد | ناکامل بودن مدل ایجاد شده توسط روش‌های یادگیری | امکان حضور چند کاربر | شناسایی فعالیت‌های همزمان |
| چن و همکاران [؟، ؟] | یادگیری مبتنی بر داده‌کاوی | ✓ | ✓ | × | ✓ | ✓ | ✓ | × | × |
| عبدالصکور و همکاران [؟] | ماشین بردار پشتیبان و شبکه عصبی پرسپترون | ✓ | ✓ | × | ✓ | ✓ | ✓ | × | × |
| رودریگز و همکاران [؟] | منطق فازی | × | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| گایاتری و همکاران [؟] | شبکه منطق مارکوف | × | × | ✓ | ✓ | ✓ | ✓ | × | ✓ |
| ریبونی و همکاران [؟] | روش‌های آماری و شبکه منطق مارکوف | × | × | × | ✓ | ✓ | ✓ | × | ✓ |

سکوهای ابری و انجام استنتاج‌های مربوطه و کلاسه‌بندی‌های مورد نیاز، اشاره دارد) یکی از تکنیک‌های حفظ امنیت کاربران، جلوگیری از استنتاج‌های غیر ضروری با استفاده از آشفته‌سازی داده‌های ذخیره شده در سکو است. همین راهبرد در برخی از راهکارهای حفظ حریم خصوصی کاربر در انتشار داده، به کار رفته است. ضمنا باید به این نکته نیز توجه داشت که پیاده‌سازی همه راهکارها، در اختیار کاربر نیست و در برخی راهکارها مستلزم همکاری سرویس‌دهنده، سکو و یا ارائه دهنده خدمات شبکه است. به طور مثال استفاده از رمزنگاری برای حفظ حریم خصوصی نیازمند همکاری بخش‌های مختلفی در زیرساخت اینترنت اشیاء است ولیکن روشی مانند آشفته‌سازی داده‌ها می‌تواند توسط عوامل تحت اختیار کاربر انجام پذیرد.

بسیاری از پژوهش‌های حفظ حریم خصوصی، با مدل تهدید سکوی نامعتمد انجام شده است که بر اساس راهکار، به دسته‌های مبتنی بر رمزنگاری، مبتنی بر کمینه‌سازی، مبتنی بر آشفته‌سازی داده و مبتنی بر تولید رویداد جعلی تقسیم می‌شوند. در این مدل تهدید فرض می‌شود که داده‌های حساس همواره در معرض خطر قرار دارند همانطور که تعداد بسیاری حمله با استفاده از این داده‌های حساس انجام شده است [؟، ؟]. به دلیل متمرکز بودن سکوها و دسترسی به تمامی داده‌های حساس توسط سکوها، مهاجمین توجه ویژه‌ای به آن‌ها می‌کنند. ضمن این که سکوها با داشتن دسترسی به تمامی اطلاعات خانه‌هوشمند و جمع‌آوری داده‌های محرمانه کاربر (که بعضا به آن نیاز ندارند)، می‌توانند از آن‌ها برای اهدافی مانند تبلیغات یا فروش به شرکت‌های دیگر استفاده کنند [؟، ؟]. راهکارهای ارائه شده در این حوزه را می‌توان به دسته‌های مختلفی تقسیم نمود که در ادامه به معرفی راهکارهای ارائه شده در هر دسته و تحلیل آن‌ها پرداخته شده است.

### ۳-۳-۱ راهکارهای مبتنی بر رمزنگاری

یکی از روش‌های حفظ حریم خصوصی در برابر سکوی نامعتمد، استفاده از یک یا چند روش رمزنگاری روی داده‌هاست به نحوی که تمامی داده‌ها از دید سکو پنهان شود.

شوتلر[۷۳] و همکاران [؟] سکویی دو بخشی به نام والنات[۷۴] تعریف کرده‌اند که هیچ کدام دسترسی به داده‌های حساس بخش دیگر ندارند. در این روش از تلفیق محاسبه دو جانبه امن و محیط اجرای امن به ترتیب برای حفظ محرمانگی و صحت استفاده می‌شود. این پژوهش فقط مدل ارتباطی رویداد_کنش را در نظر گرفته است و مدل ارتباطی رویداد_محاسبه_کنش را در نظر نمی‌گیرد.

در پژوهش دیگری، زاوالیشن[۷۵] و همکاران [؟] از طریق معرفی یک سکوی معتمد با معماری جدید به

[۷۳] Schoettler
[۷۴] Walnut
[۷۵] Zavalyshyn

نام پاترآی‌اتی[۷۶]، سعی بر حفظ حریم خصوصی کاربر را دارند. این پژوهش مانند والنات از محیط اجرای امن استفاده کرده است. همچنین این پژوهش یک لایه محافظتی مبتنی بر خط مشی ارائه کرده است که کنترل جریان‌های داده از دستگاه‌ها تا سکو و حذف جریان‌های نامطلوب از دید کاربر را بر عهده دارد.

در پژوهش دیگری، چیانگ[۷۷] و همکاران [؟] معتقدند که سکو به کمک داده‌های دریافتی، برای هر کاربر پروفایل اختصاصی درست می‌کند. داده‌های ارسال شده توسط هر نرم‌افزار، استفاده یا عدم استفاده از دستگاهی خاص مانند دستگاه اندازه‌گیری قند خون و حتی عدم دریافت داده مورد انتظار از یک برنامه در زمان مشخص، اطلاعات حساسی هستند که سکو به آن‌ها دسترسی دارد. برای مبهم‌سازی اطلاعات در این پژوهش دو راهکار OTAP[۷۸] و ATAP[۷۹] ارائه شده است. OTAP اطلاعات وقوع یا عدم وقوع رخدادها را از سکو پنهان می‌کند. با استفاده از رمزنگاری انتها به انتها[۸۰] بین رویداد و کنش، اطلاعات را از سکو پنهان می‌کند. ATAP علاوه بر انجام راهکارهایی که OTAP ارائه می‌دهد، اطلاعات مالکیت را نیز پنهان می‌کند. با استفاده رمزنگاری متقارن بین سرویس رویداد و کنش، سعی در مخفی نگه داشتن پروفایل کاربران دارد و داده‌ای که در اختیار سکو قرار می‌گیرد تنها به سرویس کنش تحویل داده می‌شود. این پژوهش نیز مانند پژوهش ژو[۸۱] و همکاران [؟]، دستگاه‌هایی که مستقیما و بدون واسط با سکو در ارتباط هستند را در نظر نگرفته است. در این پژوهش تنها الگوی رویداد_کنش در نظر گرفته شده است در صورتی که ممکن است الگوی رویداد_محاسبه_کنش مورد استفاده باشد.

در پژوهش دیگری، چن و همکاران [؟] eTAP[۸۲] را معرفی کرده‌اند. سکوی معرفی شده محاسبات مورد نیاز را روی داده‌های رمز شده انجام داده و قابلیت استنتاج از نتیجه‌ی محاسبات را ندارد. در مدل تهدید این پژوهش مهاجم ممکن است فعال باشد. ضعف این پژوهش عدم پنهان‌سازی وقوع یا عدم وقوع رخدادهاست که علی‌رغم رمزنگاری، توسط مهاجم قابل تشخیص است.

### ۳-۳-۲ راهکارهای مبتنی بر کمینه‌سازی

در روش‌های ارائه شده مبتنی بر کمینه‌سازی، به طور کلی در خروجی سیگنال‌های سری زمانی حسگرهای یک خانه هوشمند، بخش مربوط به فعالیت‌های حساس کاربر حذف می‌گردد و به جای آشفته سازی، خروجی برش می‌خورد. برای مثال در یکی از راهکارهایی که در این دسته قرار می‌گیرد انتشار جریان زمینه کاربر برای حفظ حریم خصوصی وی به انتخاب کاربر منقطع می‌گردد و در هر زمینه جدید، در مورد انتشار و یا

[۷۶] PatrIoT
[۷۷] Chiang
[۷۸] Obfuscated Trigger-Action Platform
[۷۹] Anonymous Trigger-Action Platform
[۸۰] End-to-End
[۸۱] Xu
[۸۲] Encrypted Trigger Action Platform

عدم انتشار اطلاعات تصمیم گیری می‌شود [؟]. به عنوان مثالی در این حوزه، فرض کنید که کاربر مایل باشد که از سرویس ساکت شدن زنگ موبایل خود هنگامی که در جلسه کاری است استفاده کند اما در لحظات دیگر تمایلی نداشته باشد که سرویس دهنده از شرایط محلی که وی در آن حضور دارد مطلع شود و مثلاً متوجه نشود که کاربر در خانه است، در حال رانندگی کردن است و یا در حال قدم زدن است.

روش کمینه‌سازی شناسایی فعالیت‌های حساس کاربر را برای مهاجم دشوار می‌نماید اما همچنان فاصله‌های زمانی انجام فعالیت‌های حساس کاربر و در مواردی حتی شناسایی خود فعالیت‌ها را برای مهاجم میسر می‌نماید. مثال‌های گوناگونی در این حوزه وجود دارند که چگونگی نشت اطلاعات محرمانه از روی داده‌های غیر محرمانه را به کمک روش‌های مهندسی اجتماعی و یا مدل‌سازی رفتار کاربر در طول زمان توسط مهاجم (به کمک مدل زنجیره مارکوف) را نشان می‌دهند [؟]. در ضمن با حذف بخشی از سری زمانی مربوط به سیگنال‌ها، بخشی از اطلاعات مربوط به فعالیت‌های غیرحساس کاربر نیز ممکن است حذف شود و به این ترتیب از کارایی داده‌های ارسالی به سکوهای اینترنت اشیاء کاسته می‌شود. همچنین تکنیک‌های کمینه‌سازی که بخواهند تحلیل کاملی را روی داده قبل از ارسال آن انجام دهند ممکن است با مشکلات پردازشی و تجربه بد کاربری روبرو شوند. مشکل دیگر روش‌های کمینه‌سازی این است که برای دریافت برخی سرویس‌ها (مثلا اتوماسیون امور با استفاده از برنامه‌های اینترنت اشیاء) لازم است که داده‌هایی به سکو الزاما ارسال شود که از دید کاربر بخشی از آن‌ها حساس و محرمانه است. لذا یک تعارض بین دریافت سرویس از سکوی اینترنت اشیاء و حفظ حریم خصوصی پیش می‌آید که این دسته از روش‌ها قادر به رفع این تعارض نیستند و باید از روش‌های دیگری برای حفظ حریم خصوصی استفاده کرد.

ژو و همکاران [؟] ارتباط بین سکوی اسمارت‌تینگز و سکوهای شخص ثالث مانند ایفت را بررسی کرده‌اند و به این نتیجه رسیده‌اند که سکوی شخص ثالث به اطلاعات زیادی دسترسی دارد که به نوعی نقض حریم خصوصی کاربر محسوب می‌شود. در این پژوهش با استفاده از ماژولی به نام F&F[۸۳] برای مبهم‌سازی الگوی اطلاعات دریافتی، اطلاعات جعلی ایجاد می‌شود. همچنین در مواردی که سکو برای کنش، نیاز به اطلاعات دقیق ندارد، داده‌های تقریبی و دستکاری شده برای سکو ارسال می‌گردد. مهمترین چالش این پژوهش این است که سکوی اسمارت‌تینگز مورد اعتماد فرض شده و فقط سکوی ثالث نامعتمد است.

در پژوهشی دیگر، چی[۸۴] و همکاران [؟] سیستم کنترل جریان داده‌ای به نام پی‌فایروال[۸۵] معرفی کرده‌اند. این ابزار ابتدا کد برنامه‌ی اینترنت اشیاء در هر دستگاه را بررسی کرده و سپس داده‌ی مورد نیاز برای ارسال رویدادهای هر یک را استخراج می‌کند. با این کار تنها داده‌های مورد نیاز به سکو ارسال شده و از ارسال

[۸۳] Filter & Fuzz
[۸۴] Chi
[۸۵] PFirewall

داده‌های اضافی جلوگیری می‌شود. مزیت این ابزار آن است که نیازی به تغییر سکو، هاب و یا دستگاه‌ها نیست و ابزار پی‌ـفایروال بین هاب و سکو قرار می‌گیرد. همانطور که در بخش ۲-۴ گفته شد برخی دستگاه‌ها مستقیما با سکو در ارتباط هستند و این پژوهش این دسته از دستگاه‌ها را در نظر نگرفته است. همچنین ممکن است کد برنامه‌ی اینترنت اشیاء در تمامی دستگاه‌ها در دسترس نباشد و پی‌فایروال قادر به استخراج اطلاعات مورد نیاز نباشد.

در پژوهشی دیگر، چن و همکاران [؟] با ارائه مین‌تپ[۸۶] کارایی روش کمینه‌سازی را افزایش دادند. در این پژوهش کاربر قواعد را تعریف کرده و سپس با پردازش روی این قواعد، اطلاعات کمینه‌سازی استخراج شده و به همراه قواعد به سکو ارسال می‌شود. هنگام رخداد رویداد، خصیصه‌های آن به همراه کمینه‌ساز به سرویس‌دهنده ارسال شده و اطلاعات اضافه از رویداد حذف شده و سپس به سکو ارسال می‌گردد. این راهکار کارایی بالا و سربار قابل قبولی دارد اما نیاز به اعمال تغییرات سمت سرویس‌دهنده است.

راهکار دیگری که مبتنی بر کمینه‌سازی ارائه شده است، استفاده از نگاشت[۸۷] است که در این روش‌ها به کمک اعمال محدودیت‌ها بر روی سری‌های زمانی، سری‌های زمانی جدیدی از خروجی حسگرها ایجاد می‌گردد [؟]. و غالباً اطلاعات سری زمانی اولیه حسگرها به فضای حالتی با ابعاد کوچکتر نگاشت می‌گردد تا از میزان اطلاعاتی که به همراه دارد کاسته شود. در این روش به جای ارسال سری زمانی با ابعاد بالا (مثلا یک حسگر مربوط به سیستم تهویه مطبوع ممکن است ویژگی‌هایی مانند وضعیت عملکرد فعلی، شدت فن، و دمای محیط را ارسال نماید)، فقط بخشی از ویژگی‌های اصلی از خروجی حسگرها استخراج شده و ارسال می‌شود به نحوی که داده‌ها فقط برای استنتاج فعالیت‌های غیرحساس مفید واقع شود. در یکی از راهکارهایی که در این دسته پیشنهاد شده است، داده‌های کاربر قبل از ارسال، پیش پردازش می‌گردد تا فقط داده‌هایی که برای دریافت سرویس‌های داده کاوی خاص از سکو مورد نیاز است، ارسال شود. بدین ترتیب برای مثال اگر تجهیزی برای شناسایی حرکت در خانه استفاده می‌گردد، برای استنتاج این موضوع که آیا شخصی در خانه حضور دارد یا خیر نمی‌تواند مورداستفاده قرار گیرد. در این راهکار از یک ماژول استخراج کننده ویژگی به کمک شبکه عصبی استفاده شده است تا با کمک تکنیک‌های کاهش ابعاد، ساختار داده اصلی حفظ شود و فقط آنچه لازم نیست حذف گردد و این امر با کم کردن فاصله معنایی ویژگی‌های مربوط به هم و افزایش فاصله معنایی ویژگی‌های غیرمرتبط با هم صورت می‌گیرد. مثلا جنسیت کاربر توسط سکو شناسایی می‌شود اما تصویر وی شناسایی نمی‌گردد [؟].

قسمت دشوار استفاده از راهکار نگاشت، انتخاب بهترین مجموعه کوچک ویژگی به خصوص در روش‌های متکی بر یادگیری ماشین است که بتواند یک توازن منطقی بین کارایی داده‌های ارسالی و حفظ حریم خصوصی ایجاد نماید. در راهکار دیگری که در این دسته ارائه شده است داده‌های مربوط به سری

[۸۶] minTAP
[۸۷] Mapping

زمانی در هر مقطع از زمان طی یک فرآیند آماری به صورت تصادفی نگاشت می‌گردد و این نگاشت به نحوی صورت می‌گیرد که کاربردپذیری خروجی را به صورت حداکثری نگاه دارد. هدف از انجام این نگاشت این است که نمونه‌های داده سری زمانی در طول زمان مستقل از هم بشوند و همبستگی خود را از دید مهاجم بیرونی مخفی نمایند [؟]. چالشی که در این دسته از راهکارها وجود دارد این است که ممکن است برخی از سرویس‌های سکوها، با سیگنال‌هایی که ویژگی‌های اصلی آن‌ها تغییر یافته است نتوانند کار کنند. در ضمن در این روش اصلا نمی‌توان تضمین نمود که هر ویژگی در مجموعه‌ای که انتخاب شده است تنها حاوی اطلاعات یک فعالیت غیرحساس باشد و هیچ اطلاعی از یک فعالیت حساس را به همراه نداشته باشد.

### ۳-۳-۳ راهکارهای مبتنی بر آشفته‌سازی

در این روش هدف ارسال داده تفییریافته است به شکلی که کاربر بتواند سرویس‌های دلخواه خود را از سکو یا سرویس دهنده دریافت نماید و در عین حال عدم قطعیت داده تضمین گردد [؟]. منظور از عدم قطعیت داده این است که از روی داده‌های آشفته، ساخت اصل داده‌ها میسر نباشد.

تنوع راه‌حل‌ها و چالش‌ها در این دسته از راهکارها زیاد است و بررسی‌های متعددی در این خصوص صورت گرفته است برای مثال مطالعاتی در خصوص اعمال انواع مختلف نویز به داده‌های سری زمانی حسگرها، مانند اعمال نویز تصادفی با الگوریتم‌های مختلف [؟، ؟]، اعمال نویزی که با سری زمانی اصلی همبستگی دارد [؟]، اعمال نویز در کنار فشرده‌سازی سیگنال اولیه [؟]، و یا اعمال نویز با توجه به حفظ فاصله اقلیدسی سیگنال‌های حسگرهای مشابه از کاربران مختلف [؟] صورت گرفته است و مزایا و معایب هر روش پیشنهادی با توجه به معیارهایی که برای اندازه‌گیری حفظ حریم خصوصی کاربر و کاربردپذیری سیگنال تعریف شده اندازه‌گیری شده است.

در کنار این راهکارها، روش‌هاي متعددی نیز برای بازسازی داده‌های اولیه از روی داده‌های آشفته‌سازی‌شده پیشنهاد شده است که نقاط ضعف استفاده از این راهکارها را به چالش کشیده است [؟، ؟، ؟]. به طور خلاصه در مورد این راه‌حل‌ها می‌بایست گفت که میزان نویز اعمال شده به سیگنال اولیه، قابلیت کاربرد پذیری سیگنال (منظور امکان استفاده کاربر از سرویس‌های دلخواه) را به شدت تحت تاثیر قرار می‌دهد و حتی ممکن است اصل داده‌ها را تخریب نماید. بسیاری از راهکارهای این دسته شناسایی فعالیت‌های حساس کاربر را برای مهاجم با دشواری مواجه می‌کنند اما عدم قطعیت داده را تضمین نمی‌کنند.

راهکار دیگری برای آشفته‌سازی داده، استفاده از جایگزینی[۸۸] است. در این روش، بخش حساس سری‌های زمانی با داده‌های غیرحساس جایگزین می‌گردد. برای مثال در یکی از رویکردهایی که در این دسته

[۸۸] Replacement

ارائه شده است [؟] به کمک تکنیک‌های یادگیری ماشین، رفتارهای حساس کاربر با رفتارهای غیرحساس جایگزین می‌گردد. در این راهکار فعالیت‌های کاربر به دو گروه سفید (غیر حساس) و سیاه (حساس) تقسیم می‌گردد. منظور از رفتارهای حساس کاربر رفتارهایي هستند که برخی از حالات روانشناسی کاربر مانند وجود استرس از آن‌ها قابل استخراج است. شبکه پویای بیزین پیشنهادی در این روش، آموزش می‌بیند و در مرحله اول برای شناسایي بلاک‌های حساس کاربر در سیگنال‌های خروجی استفاده می‌گردد. سپس در مرحله بعد برای انتخاب بخش‌هایی که می‌بایست جایگزین بلاک‌های حساس گردد، استفاده می‌گردد. البته با حفظ این محدودیت که طول بلاک‌هایی که حذف می‌گردد با طول بلاک‌هایی که جایگزین می‌گردد مساوی باشد. در این راهکار توسط ماژولی سیگنال خام ورودی به سیگنالی مبتنی بر ویژگی‌های رفتاری تبدیل می‌شود و با حذف رفتارهای حساس تعدادی حفره باقی می‌مانند که می‌بایست توسط رفتارهای غیرحساس پر شوند و جایگزینی به نحوی صورت می‌گیرد که به تداوم جریان سیگنال لطمه وارد نشود. برای جایگزینی رفتارها از یک پایگاه داده نگاشت رفتاری با طول‌های زمانی مختلف استفاده می‌گردد. این راهکار به صورت برون‌ـخط عمل می‌کند یعنی قبل از تصمیم‌گیری برای جایگزینی، اطلاعات سری‌زمانی فعالیت کاربر می‌بایست در دسترس باشد.

به عنوان مثالی دیگر از راهکارهای این دسته به راهکار ارائه شده در پژوهش آقای ملک زاده [؟] می‌توان اشاره کرد که در آن یک شبکه عصبی آموزش دیده به نام خودرمزگذار[۸۹] جایگزین‌کننده، عملی مانند رفع نویز انجام می‌دهد و الگوریتم جایگزینی فعالیت‌های حساس با فعالیت‌های غیرحساس را انجام می‌دهد به نحوی که امکان تشخیص و استنتاج فعالیت‌های حساس از بین می‌رود. داده‌ها در این راهکار به سه دسته‌ی سیاه (حساس)، خاکستری (غیر حساس است و استنتاج این رفتار برای کاربر مهم نیست) و سفید (غیر حساس است و استنتاج این رفتار برای کاربر مهم و کاربردپذیر است) تقسیم می‌شوند. در هر سری زمانی و بازه‌ی دلخواه، الگوریتم مطرح شده با در نظر گرفتن کاربردپذیری از بعد دریافت سرویس‌های مد نظر کاربر از سکو، داده‌هایی از لیست سیاه را با خاکستری جایگزین می‌کند. در این راهکار اثبات می‌شود که مهاجم بدون داشتن داده‌های مورد استفاده برای تعلیم لیست خاکستری، امکان تشخیص داده‌های حساس را ندارد و از کاربردپذیری داده‌های ارسالی به سکوهای اینترنت اشیاء برای دریافت سرویس‌های دلخواه کاسته نمی‌شود.

### ۳-۳-۴ راهکارهای مبتنی بر تولید رویدادهای جعلی

در پژوهش‌های مبتنی بر تولید رویداد جعلی، برای حفظ حریم خصوصی کاربر، به جای حذف، تغییر

[۸۹] AutoEncoder

یا پنهان‌سازی داده، از اضافه کردن داده‌های جعلی برای گمراه کردن سکو استفاده می‌شود. تولید و ارسال داده‌های جعلی در این پژوهش‌ها به نحوی است که سکو امکان تمایز این داده‌ها با داده‌های واقعی را نداشته باشد و از طرفی کنش‌های سکو در جواب رویدادهای جعلی اعمال نشود.

در پژوهش ژو و همکاران [؟] الگوهای آماری باعث نقض حریم خصوصی می‌شود و برای عدم استنتاج سکو، تعدادی رویداد جعلی با برچسب مشخص ارسال می‌شود و از آن‌جایی که سکو قادر به تمایز میان رویدادهای جعلی و حقیقی نیست، کنش‌های مرتبط را ایجاد می‌کند. در آخر، با توجه به برچسب هر رویداد و وابستگی کنش‌ها به رویدادها، کنش‌های ناشی از رویدادهای جعلی تشخیص داده شده و کنار گذاشته می‌شوند.

در پژوهش چیانگ و همکاران [؟]، محرمانگی داده‌های ارسالی به سکو تضمین شده است اما در بسیاری از موارد، وقوع یا عدم وقوع یک رویداد، یک داده‌ی حساس به شمار می‌آید. برای پنهان کردن این اطلاعات، از رویکرد تولید رویداد جعلی استفاده شده است که به صورت متناوب، در بازه‌های زمانی مشخص، هر دستگاه اینترنت اشیاء، داده‌های جعلی و حقیقی را با هم به سکو ارسال می‌کند.

اقوامی‌پناه و امینی[۹۰] [؟] برای فریب مهاجمی که با استفاده از شبکه عصبی LSTM[۹۱] اقدام به استنتاج فعالیت‌های کاربر می‌کند، راهکاری بر اساس تولید رویدادهای جعلی ارائه کرده‌اند[۹۲]. در این پژوهش با استفاده از نمونه خصمانه[۹۳] و تولید رویدادهای جعلی در بازه‌های زمانی مشخص، جلوی استنتاج مهاجم گرفته می‌شود. همچنین، کنش‌هایی که در نتیجه‌ی رویدادهای جعلی دریافت می‌شود کنار گذاشته می‌شود تا کاربردپذیری خانه هوشمند کاهش پیدا نکند. هرچند این پژوهش در ابتدا فرض را بر استفاده‌ی سکو از شبکه عصبی LSTM برای استنتاج فعالیت‌های کاربر قرار داده است؛ ولیکن در ادامه با بررسی قابلیت انتقال‌پذیری، امکان موثر بودن نمونه‌های خصمانه تولید شده در به اشتباه انداختن دسته‌بندهای مبتنی بر روش‌های دیگر را با انجام آزمایش‌های عملی به اثبات رسانده است. یکی از ضعف‌های این پژوهش این است که در صورت هوشمندی بیشتر سکوی مهاجم و تجهیز آن به برخی روش‌های شناسایی ناهنجاری، امکان تشخیص و شناسایی رویدادهای جعلی تولید شده با این روش و حذف آن‌ها وجود خواهد داشت. ضعف دیگر، وجود روش‌های دفاعی [؟] در مقابل نمونه‌های خصمانه است که موجب ناکارآمد شدن این راهکار در برابر مهاجم هوشمند می‌شود.

---

[۹۰] آزمایشگاه امنیت داده و شبکه، دانشگاه صنعتی شریف

[۹۱] Long-Short Term Memory

[۹۲] مقاله پژوهش تا زمان نگارش این مطلب منتشر نشده است.

[۹۳] Adversarial example

### ۳-۳-۵ جمع‌بندی

در این بخش پژوهش‌های حفظ حریم خصوصی مبتنی بر سکوی نامعتمد بررسی شد که اکثرا نیاز به تغییر سکو و دستگاه‌ها دارند که سبب مشکل در استفاده شده است. در جدول ۳-۳ می‌توان مقایسه کلی این روش‌ها را مشاهده کرد.

جدول ۳-۳: مقایسه کلی روش‌های حفظ حریم خصوصی مبتنی بر سکوی نامعتمد

| پژوهش | راهکار | پشتیبانی از محاسبه | عدم تغییر سرویس‌ها | عدم تغییر سکو | سربار قابل قبول | حفظ کاربردپذیری | حفاظت در برابر مهاجم هوشمند |
|---|---|---|---|---|---|---|---|
| ژو و همکاران (F&F) [؟] | کمینه‌سازی، آشفته‌سازی و تولید رویدادهای جعلی | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ |
| چی و همکاران (PFirewall) [؟] | کمینه‌سازی | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| چیانگ و همکاران (OTAP) [؟] | رمزنگاری و تولید رویدادهای جعلی | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ |
| چیانگ و همکاران (ATAP) [؟] | رمزنگاری و تولید رویدادهای جعلی | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ |
| چن و همکاران (ETAP) [؟] | رمزنگاری | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ |
| چن و همکاران (minTAP) [؟] | کمینه‌سازی | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ |
| زاوالیشن و همکاران (PatrIoT) [؟] | رمزنگاری | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ |
| شوتلر و همکاران (Walnut) [؟] | رمزنگاری | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ |
| ملک‌زاده و همکاران [؟] | آشفته‌سازی | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| اقوامی‌پناه و امینی [؟] | تولید رویدادهای جعلی | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |

# فصل ۴

# راهکار پیشنهادی

همانطور که در فصل ۳ مشاهده کردیم، پژوهش‌های زیادی در زمینه حفظ حریم خصوصی در خانه هوشمند انجام شده است اما هر یک نواقصی داشتند. راهکار پیشنهادی این پژوهش، استفاده از تولید رویداد جعلی بر پایه هستی‌شناسی مبتنی بر زمینه به صورت خاص‌دامنه برای خانه‌های هوشمند است تا سکوی نامعتمد، امکان تمایز بین داده‌های حساس کاربر و داده‌های جعلی را نداشته باشد. این رویدادهای جعلی با استفاده از هستی‌شناسی که با استفاده از روش دانش‌محور توسط فرد خبره به برنامه داده شده است، تولید می‌شوند.

## ۴-۱ توصیف اجمالی

راهکار ارائه شده با توجه به دسته‌بندی بخش ۳-۱ یک هستی‌شناسی مبتنی بر زمینه ارائه می‌دهد. هستی‌شناسی در این راهکار شامل نقشه‌ی خانه هوشمند، موقعیت موجودیت‌ها (اشیاء و انسان‌ها) و حالت آن‌ها، فعالیت‌های کاربر و شروط و نتایج هر فعالیت و همچنین فعالیت‌های احتمالی آتی بعد از هر فعالیت می‌باشد. بنابراین، هستی‌شناسی در این راهکار یک هستی‌شناسی مبتنی بر زمینه بوده که به صورت خاص‌دامنه برای خانه‌های هوشمند طراحی شده است.

مدل‌سازی اطلاعات در این راهکار با توجه به دسته‌بندی در بخش ۳-۲، با استفاده از روش دانش‌محور می‌باشد زیرا فرد خبره با دانش خود اطلاعات کامل خانه، موجودیت‌ها و فعالیت کاربران را داشته و به برنامه می‌دهد. در این روش شروع سرد نخواهیم داشت و داده‌ها قابلیت استفاده مجدد دارند زیرا در صورت نیاز به استفاده مجدد، تنها بخش کمی از هستی‌شناسی نیاز به تغییر دارد. برای مثال در صورت تغییر منزل توسط کاربران، تنها بخش نقشه خانه و موقعیت موجودیت‌ها در هستی‌شناسی عوض شده و سوابق فعالیت‌های کاربر در هستی‌شناسی ثابت می‌ماند. توجه شود که این راهکار دچار مشکل ناکامل بودن دانش فرد خبره

نمی‌شود چرا که برای تولید فعالیت‌های جعلی، نیازی به آگاهی از تمامی فعالیت‌های کاربر نداریم و تنها با داشتن فعالیت‌های روزانه و پرتکرار کاربران، امکان تولید سلسله فعالیت جعلی برای برنامه فراهم است.

در این پژوهش برای حفظ حریم خصوصی در برابر سکوی نامعتمد، با توجه به دسته‌بندی در بخش ۳-۳، از راهکار مبتنی بر تولید رویداد جعلی استفاده شده است. با استفاده از هستی‌شناسی مبتنی بر زمینه که شامل سلسله فعالیت‌های کاربران و توالی احتمالی هر دو فعالیت است، برای گمراه کردن سکوی نامعتمد در این پژوهش سلسله فعالیت جعلی مبتنی بر هستی‌شناسی تولید شده که از دید سکو قابل تمایز نباشد. توجه شود که مانند پژوهش ژو و همکاران [؟]، رویدادهای جعلی با برچسب ارسال می‌شود و کنش‌های مربوط به رویدادهای جعلی کنار گذاشته می‌شوند.

## ۴-۲ مدل تهدید

در این پژوهش، سکوی اینترنت اشیاء صادق ولی کنجکاو فرض شده است و دسترسی به تمامی رویدادهای ارسال شده از حسگرهای خانه هوشمند را داشته و به طور کامل آن‌ها را به همراه زمان دریافت داده از حسگر، ذخیره می‌کند. این ذخیره‌سازی برای آن است که در صورت دریافت سلسله فعالیت جدید کاربران، داده‌های ذخیره شده را با داده‌ی دریافت شده مقایسه کرده و در صورت شباهت بیش از حد، مشکوک به جعلی بودن سلسله فعالیت دریافتی شود.

همچنین سکو به هستی‌شناسی کامل خانه دسترسی داشته و از موقعیت و حالات موجودیت‌ها، روابط و همبستگی‌های بین آن‌ها (ناشی از انواع کانال‌های ارتباط دهنده)، متغیرهای محیطی و احتمال سلسله فعالیت‌های مختلف کاربران برای تشخیص واقعی و یا جعلی بودن رویدادها استفاده می‌کند.

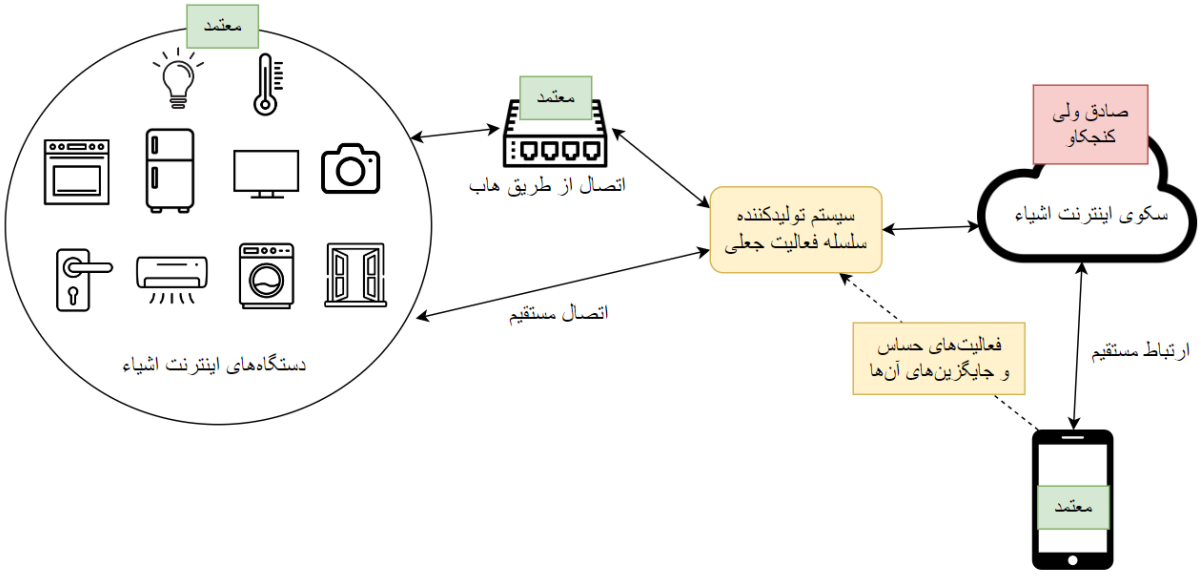
برای آن که سکو مشکوک به جعلی بودن یک سلسله فعالیت نشود، نیاز است تا تولید آن سلسله فعالیت با توجه به هستی‌شناسی خانه انجام شده و برای یکسان نبودن هر دو سلسله از فعالیت‌های جعلی، ریز فعالیت‌های انجام شده و همچنین فواصل زمانی بین انجام فعالیت‌ها، به صورت تصادفی انتخاب شده تا سکو با مقایسه‌ی سلسله فعالیت با داده‌های قبلی، متوجه شباهت زیاد بین آن‌ها نشود.

## ۴-۳ راهکار پیشنهادی

راهکار ارائه شده در این پژوهش، به حفظ حریم خصوصی کاربران در برابر سکوی نامعتمد بر اساس ترجیحات حریم خصوصی کاربر می‌پردازد. در ادامه به بررسی معماری این راهکار خواهیم پرداخت.

## ۴-۳-۱ معماری کلان

ابزار مبتنی بر راهکار پیشنهادی این پژوهش مطابق شکل ۴-۱، بین هاب و سکوی اینترنت اشیاء قرار دارد که هر کاربر، فعالیت‌های حساس خود و همچنین فعالیت‌های جعلی جایگزین را اعلام کرده است تا در صورت انجام آن فعالیت‌های حساس، سلسله فعالیت جعلی مبتنی بر نیاز کاربر تولید شود. هر فعالیت موجود در سلسله فعالیت جعلی تولید شده توسط ابزار مبتنی بر راهکار پیشنهادی، در زمان مشخص، رویداد مورد نیاز را از جانب حسگر مربوطه به سکو ارسال می‌کند.




شکل ۴-۱: محل استقرار سیستم تولیدکننده سلسله فعالیت جعلی

از طرفی، زمانی که سکو دستور کنش‌های مورد نیاز برای رویدادهای دریافتی را ارسال می‌کند؛ ابزار مبتنی بر راهکار پیشنهادی، تمامی کنش‌ها را بررسی کرده و هر کنش که در جواب رویدادی با برچسب جعلی آمده باشد را کنار می‌گذارد تا کارایی خانه هوشمند کاهش پیدا نکند.

کاربر برای تولید سلسله فعالیت جعلی دلخواهش، یکی از دو نوع ورودی مبتنی بر فعالیت و مبتنی بر نتیجه را به عنوان ورودی به ابزار مبتنی بر راهکار پیشنهادی می‌دهد. حال ابزار مبتنی بر راهکار پیشنهادی، یک سلسله فعالیت جعلی تولید می‌کند که فعالیت جعلی مدنظر کاربر در آن وجود داشته باشد.

از طرفی اگر درخواست کاربر، تولید سلسله فعالیت جعلی بر اساس نتیجه باشد، ابزار مبتنی بر راهکار پیشنهادی در ابتدا تمامی فعالیت‌های منتهی به آن نتیجه را پیدا کرده و سپس بر اساس یکی از آن فعالیت‌ها یک سلسله فعالیت جعلی تولید می‌کند که آن فعالیت را شامل باشد و نتیجه‌ی مدنظر کاربر از فعالیت مذکور گرفته شود. به عنوان مثال زمانی که ترجیح کاربر تولید سلسله فعالیت جعلی مبتنی بر نتیجه‌ی «افزایش نور محیط» است؛ نرم‌افزار ابتدا فعالیت‌های «باز کردن پنجره» (به شرط روز بودن) و «روشن کردن تلویزیون» پیدا کرده، سپس، به صورت تصادفی، یکی از آن‌ها را انتخاب کرده و بر اساس آن فعالیت، یک سلسله

فعالیت جعلی شامل فعالیت انتخاب شده تولید می‌کند.

خروجی هر بار اجرای ابزار مبتنی بر راهکار پیشنهادی، یک سلسله فعالیت جعلی بوده که هر یک در زمان خاصی باید از جانب حسگر مربوطه به سکو ارسال شوند. به طور مثال یک سلسله فعالیت جعلی شامل «باز کردن درب پذیرایی در زمان ۱۰:۴۰:۰۱:۰۰» و «روشن کردن کولر در زمان ۱۰:۴۰:۰۲:۵۰» است که بدین معناست که در زمان ۱۰:۴۰:۰۱:۰۰، کاربر درب پذیرایی را باز کرده و در زمان ۱۰:۴۰:۰۲:۵۰، کولر را روشن می‌کند. ابزار مبتنی بر راهکار پیشنهادی برای این سلسله فعالیت جعلی، در زمان ۱۰:۴۰:۰۱:۰۰، رویداد باز شدن درب پذیرایی را از جانب حسگر درب پذیرایی به سکو ارسال می‌کند؛ سپس رویداد روشن شدن کولر را در زمان ۱۰:۴۰:۰۲:۵۰، یعنی یک و نیم ثانیه پس از باز شدن درب پذیرایی، از جانب کولر به سکو ارسال می‌کند.

## ۴-۴ مدل‌سازی

برای مدل‌سازی جامع و کامل در برنامه‌ی این پژوهش، نیاز به هستی‌شناسی مبتنی بر زمینه به صورت خاص‌دامنه برای خانه هوشمند داریم و سپس با استفاده از این هستی‌شناسی اقدام به تولید سلسله فعالیت جعلی می‌نماییم.

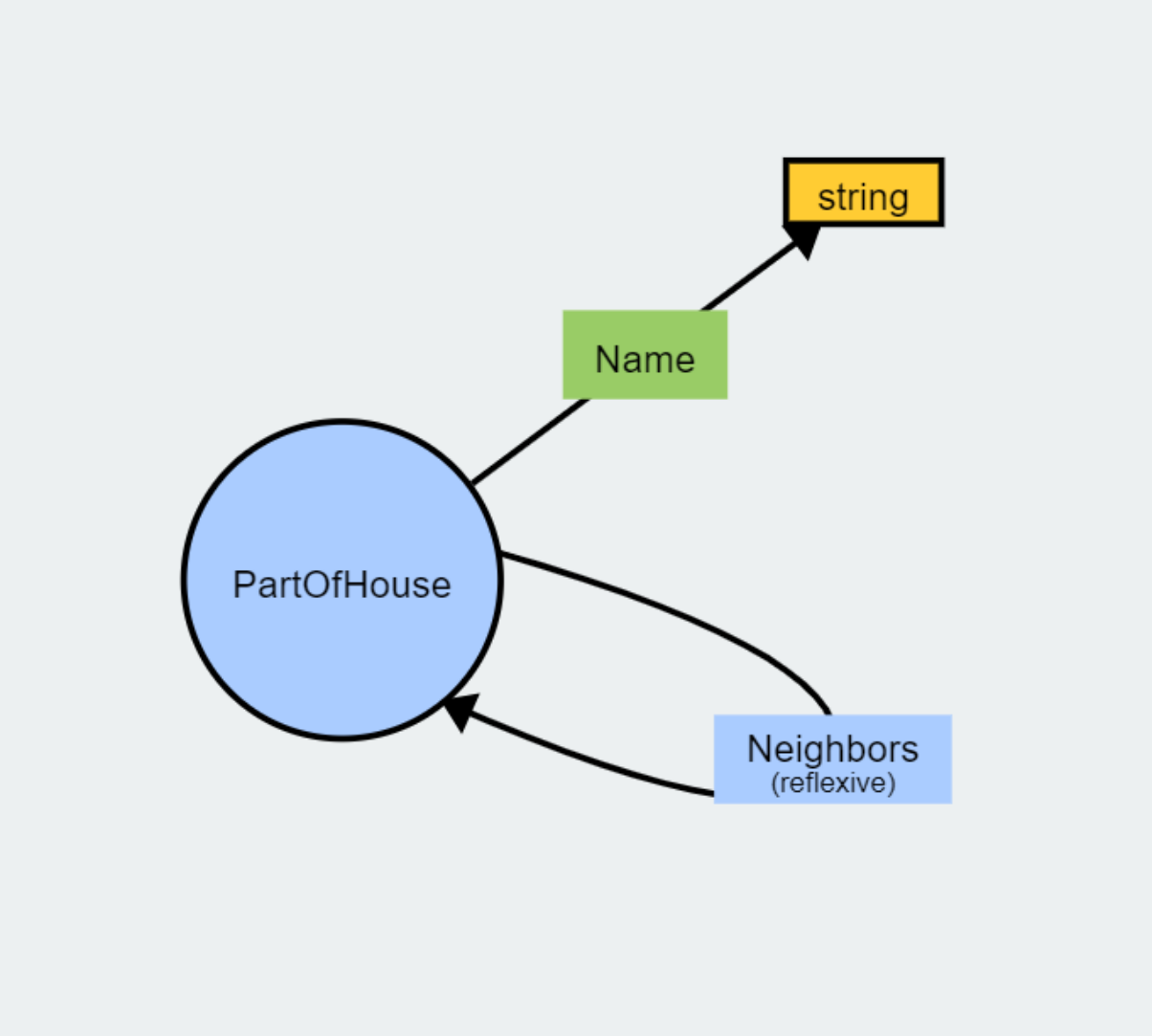
### ۴-۴-۱ هستی‌شناسی

در این پژوهش، هستی‌شناسی که با دانش فرد خبره به صورت دانش‌محور داده شده است؛ در چند بخش مختلف قرار می‌گیرد که در ادامه به توضیحات هر بخش خواهیم پرداخت.

- خانه هوشمند: همانطور که در شکل ۴-۲ قابل مشاهده است، نقشه‌ی خانه هوشمند توسط فرد خبره تعریف شده است. هر بخش شامل نام و لیست بخش‌هایی از خانه هوشمند است که به طور مستقیم به بخش مورد نظر متصل هستند (به عنوان مثال اتاق خواب، به طور مستقیم به راهرو و بالکن متصل است). استفاده از نقشه‌ی خانه در این پژوهش طوری تعریف شده است که با تغییر نقشه‌ی خانه، نیازی به تغییر دیگری در برنامه نخواهیم داشت و عملکرد برنامه تحت تاثیر قرار نخواهد گرفت.

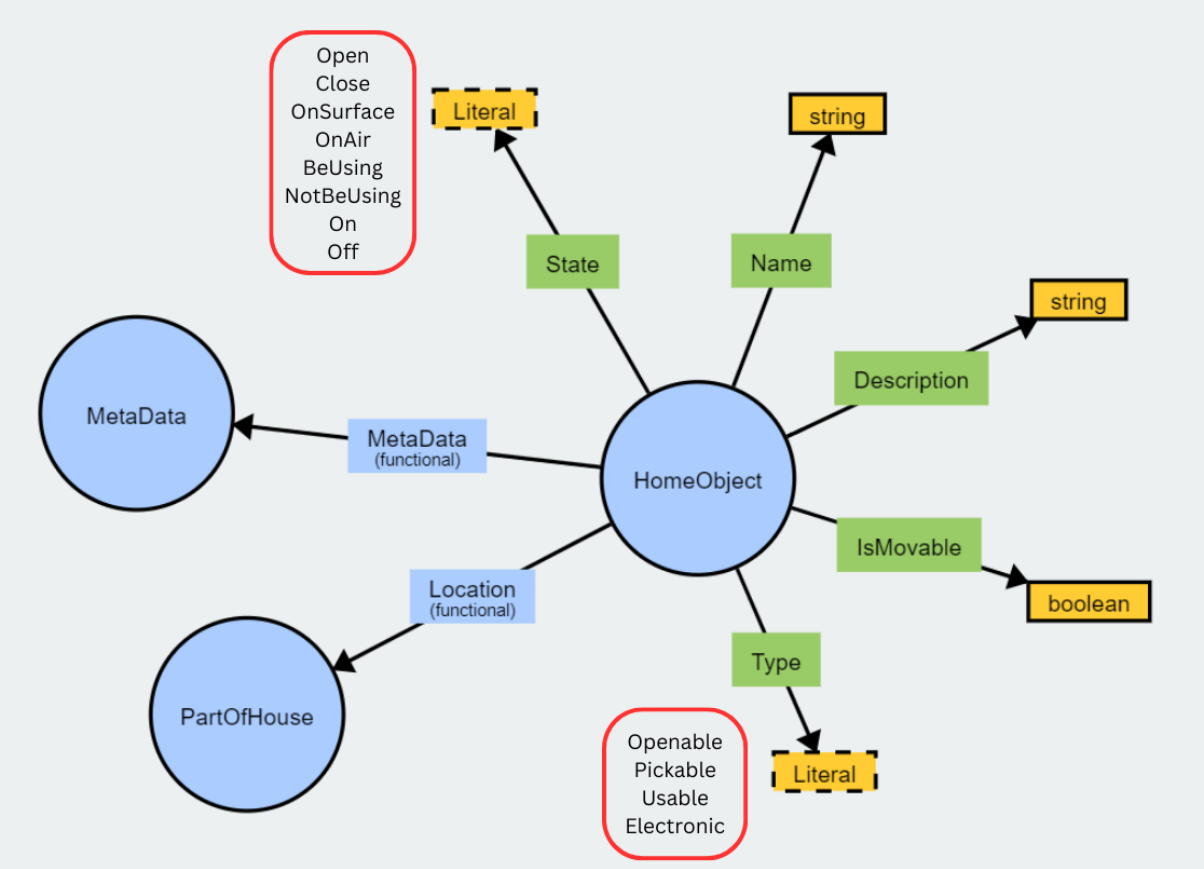
  هستی‌شناسی تعریف شده برای خانه هوشمند، در شکل ۴-۳ قابل مشاهده است. در این هستی‌شناسی هر بخش خانه هوشمند مانند آشپزخانه، راهرو، پذیرایی، بالکن، دستشویی و اتاق‌خواب‌ها و همچنین همسایگان هر کدام، توسط فرد خبره مشخص شده اند.


شکل ۴-۲: نمونه نقشه خانه هوشمند




شکل ۴-۳: هستی‌شناسی بخش‌های خانه هوشمند

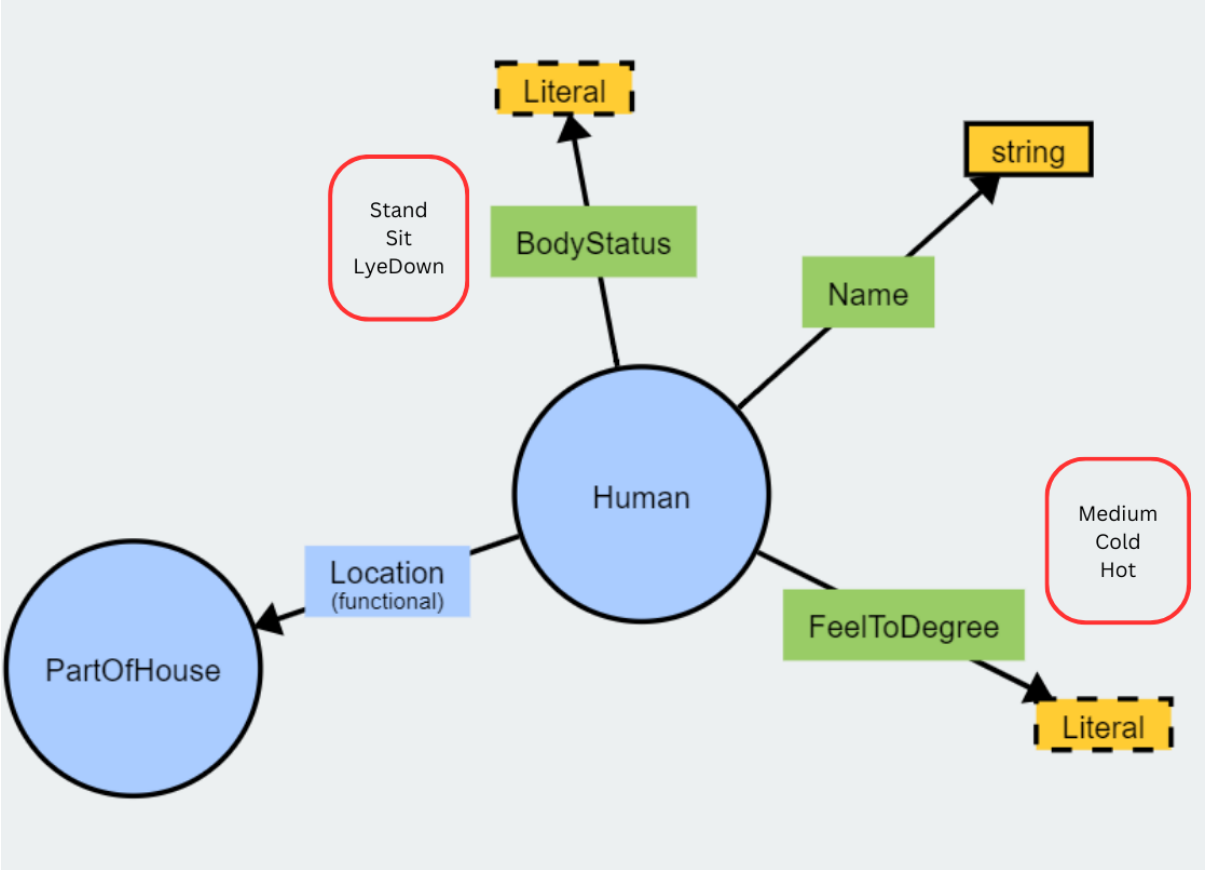
- موجودیت‌ها: در هستی‌شناسی که توسط فرد خبره به برنامه داده می‌شود، موقعیت و حالت اولیه برای تمامی موجودیت‌ها (انسان‌ها و اشیاء که حسگر دارند) فراهم می‌شود. در صورتی که در سلسله فعالیت‌های جعلی، موقعیت یا حالت یک موجودیت تغییر کند، این تغییر در پایگاه داده ذخیره می‌شود تا سلسله فعالیت‌های بعدی بر اساس اطلاعات جدید موجودیت‌ها باشد تا از دید سکوی نامعتمد، تناقضی در داده‌ها رخ ندهد اما کنش‌های مربوط به تمامی رویدادهایی که با برچسب جعلی به سکو ارسال شده‌اند، کنار گذاشته می‌شوند تا بهره‌وری خانه هوشمند کاهش پیدا نکند. هستی‌شناسی اشیاء خانه هوشمند در شکل ۴-۴ و هستی‌شناسی افراد حاضر در خانه در شکل ۴-۵ قابل مشاهده است.



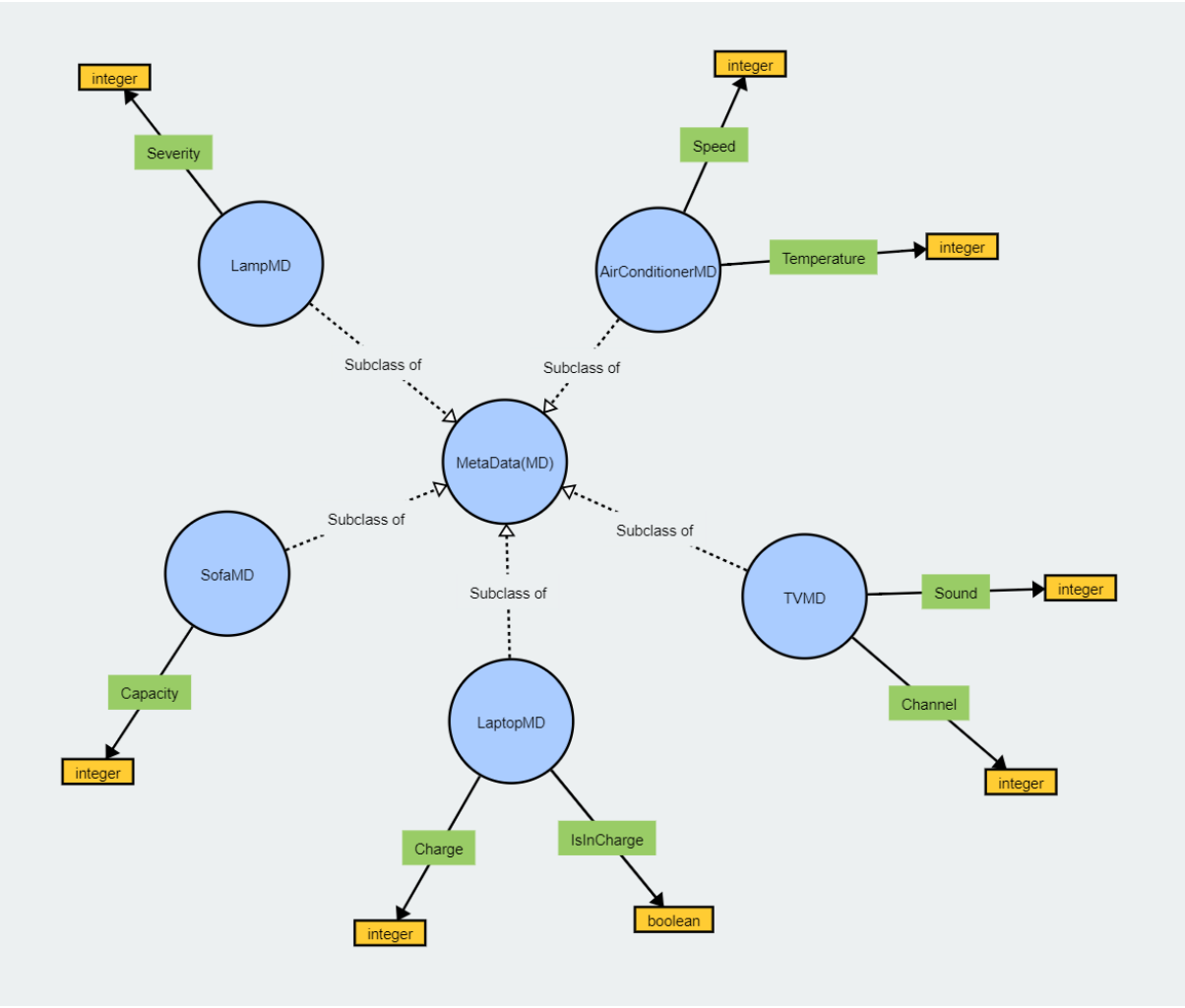

شکل ۴-۴: هستی‌شناسی اشیاء خانه هوشمند

همچنین هستی‌شناسی فرادادههای اشیاء خانه هوشمند در شکل ۴-۶ قابل مشاهده است. هر یک از اشیاء خانه هوشمند حداکثر یکی از این فرادادهها را در هستی‌شناسی خود دارند تا با استفاده از آن‌ها شروط هر یک از اشیاء به طور دقیق‌تر بررسی شود و تغییر حالت آن به طور دقیق‌تر اعمال شود.

- شرایط محیطی: برای دخیل کردن شرایط محیطی مانند میزان نور، دما، صدا و ... در تولید سلسله فعالیت‌های جعلی، مقدار اولیه برای اجزای محیط در دانش اولیه‌ی برنامه قرار دارد. توجه شود که تاریخ و ساعت به عنوان یک متغیر محیطی در تولید سلسله فعالیت جعلی دخیل بوده اما در هستی‌شناسی اولیه قرار ندارد چرا که متغیر زمان به صورت خودکار مقدار می‌گیرد. استفاده از این

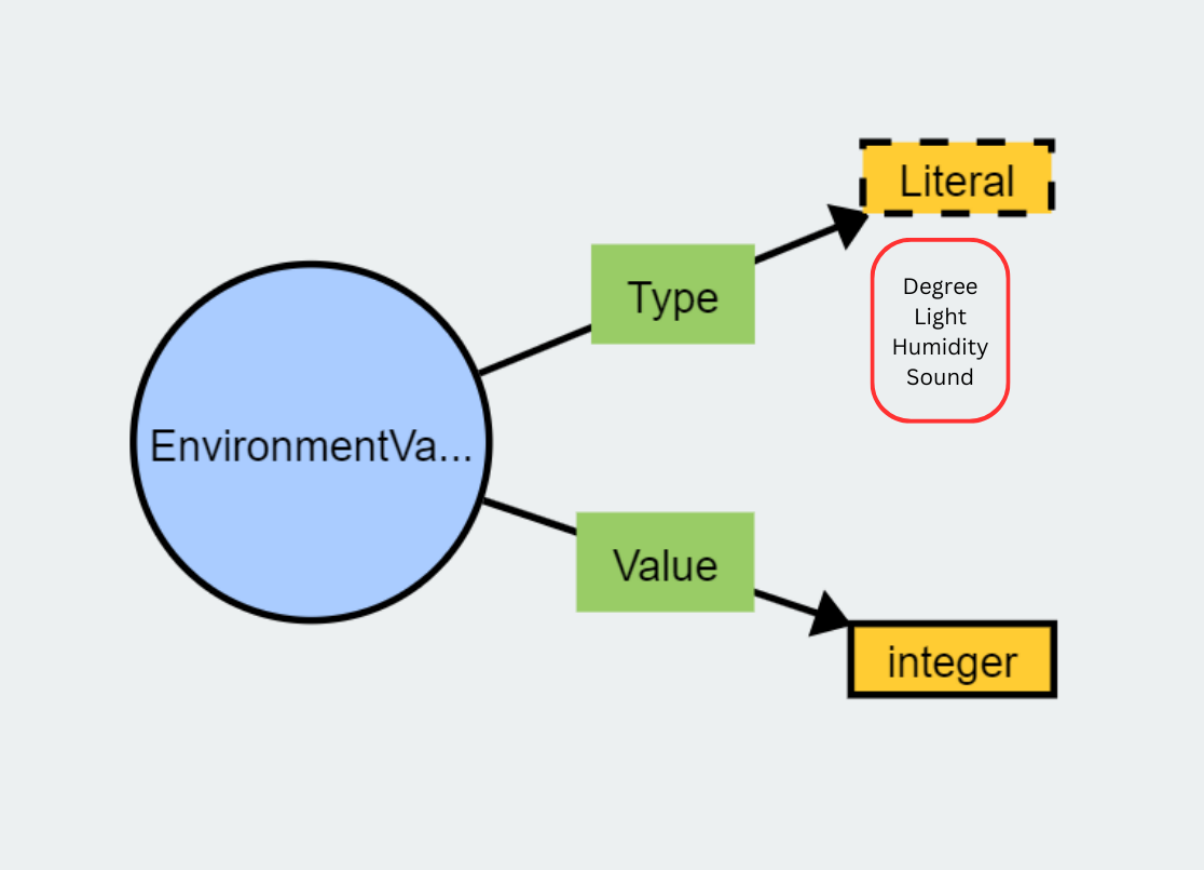



شکل ۴-۵: هستی‌شناسی افراد حاضر در خانه هوشمند




شکل ۴-۶: هستی‌شناسی فراداده‌های اشیاء خانه هوشمند

اجزای محیط کمک به واقعی به نظر رسیدن سلسله فعالیت‌های جعلی خواهد کرد. به عنوان مثال زمانی که پنجره باز می‌شود، حسگر سنجش نور محیط، در ساعاتی که خورشید در آسمان است، رویداد افزایش نور محیط را ارسال می‌کند. پس زمانی که به صورت جعلی ارسال رویداد باز شدن پنجره را به حسگر مربوطه ارسال می‌کنیم، برنامه با توجه به ساعت شبانه روز تصمیم به ارسال یا عدم ارسال رویداد افزایش نور محیط توسط حسگر سنجش نور می‌گیرد. هستی‌شناسی مربوط به اجزای محیط در شکل ۴-۷ قابل مشاهده است.

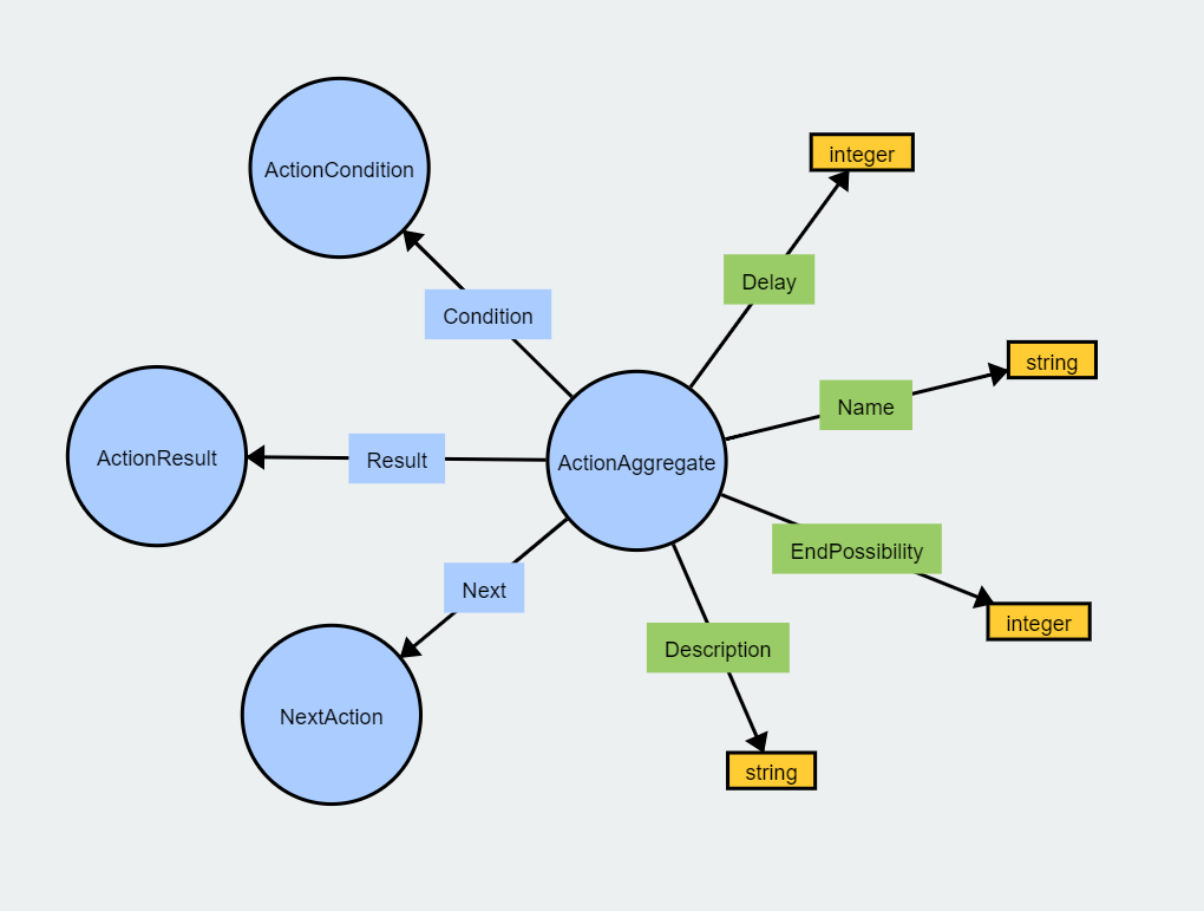



شکل ۴-۷: هستی‌شناسی اجزای محیط خانه هوشمند

- فعالیت: هر فعالیت کاربر به صورت سابقه‌ی مختص به آن کاربر در هستی‌شناسی اولیه توسط فرد خبره داده می‌شود که فعالیت‌ها شامل شروط مورد نیاز برای انجام به صورت جعلی (به عنوان مثال حضور در پذیرایی برای «روشن کردن تلویزیون»)، نتایج اعمال شده پس از ارسال رویداد جعلی یک فعالیت به سکو (به عنوان مثال کاهش دمای محیط پس از «روشن کردن کولر») و فعالیت‌های احتمالی انجام شده توسط کاربر پس از انجام یک فعالیت مشخص (به عنوان مثال پس از «ورود به پذیرایی»، «روشن کردن کولر» با احتمال ۷۰% و «نشستن روی مبل» با احتمال ۳۰% انجام می‌شود) است که نحوه مدل‌سازی احتمال توالی فعالیت‌ها را در بخش ۴-۴-۲ توضیح خواهیم داد. توجه شود که هر فعالیت با احتمالی مشخص با توجه به سوابق کاربر، می‌تواند آخرین فعالیت یک

سلسله فعالیت جعلی باشد و لزوما نیاز به ادامه در تولید سلسله فعالیت جعلی با توجه به فعالیت احتمالی بعدی نداریم. هستی‌شناسی کلی فعالیت‌ها در شکل ۴-۸ قابل مشاهده است.

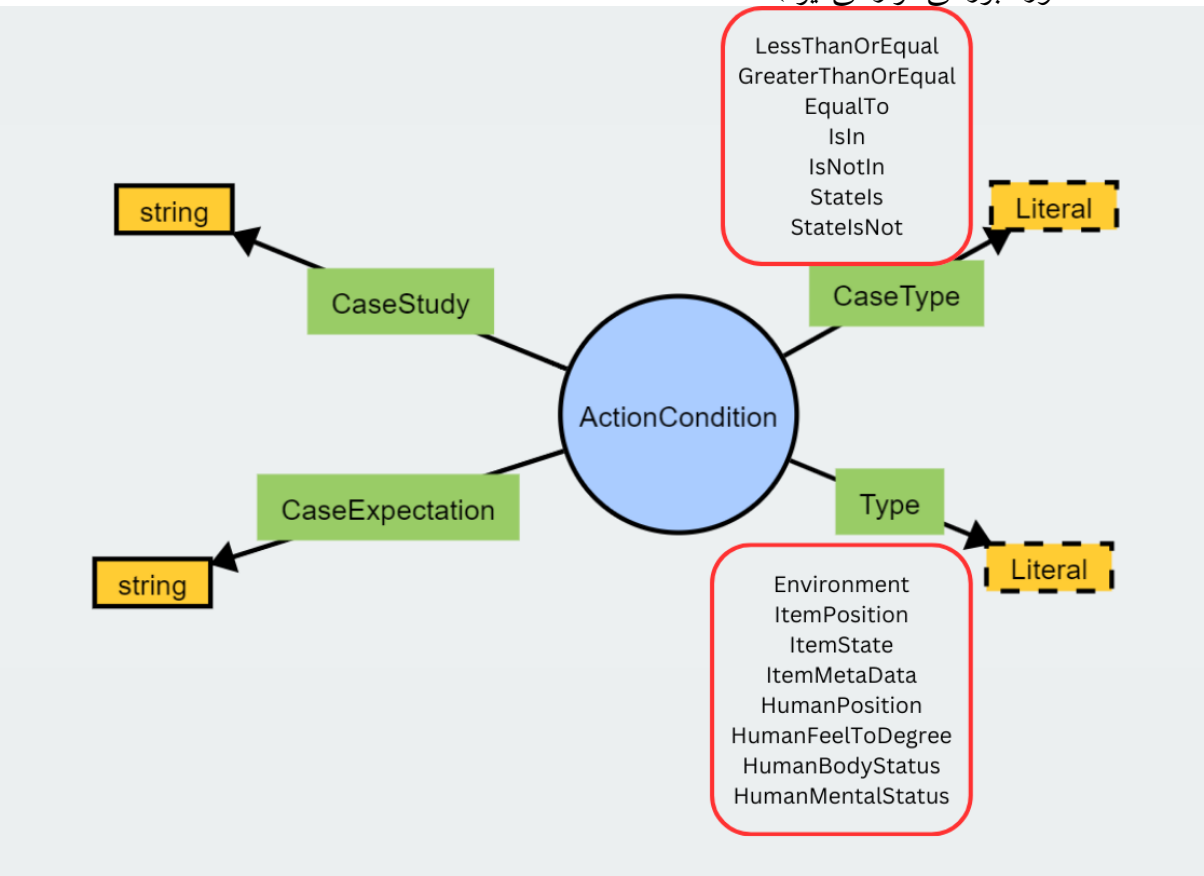
به عنوان مثال در فعالیت «روشن کردن تلویزیون» به عنوان ActionAggregate، حضور در پذیرایی یکی از شروط انجام آن (ActionCondition)، تغییر وضعیت تلویزیون به حالت روشن یکی از نتایج انجام آن (ActionResult)، افزایش یا کاهش صدای تلویزیون یکی از فعالیت‌های احتمالی بعدی (NextAction)، "روشن کردن تلیویزیون" نام آن، تاخیر برابر ۴ ثانیه، احتمال ۵۰ درصد بودن فعالیت نهایی و "روشن کردن تلویزیون به صورت دستی توسط افراد حاضر در خانه" به عنوان توضیحات بر اساس هستی‌شناسی این فعالیت داده شده است.




شکل ۴-۸: هستی‌شناسی کلی فعالیت‌های خانه هوشمند

در هستی‌شناسی شرایط انجام فعالیت که در شکل ۴-۹ قابل مشاهده است، نوع موجودیتی که شرط روی آن بررسی می‌شود(اجزای محیط، موقعیت مکانی شیء، حالت شیء، فراداده شیء، موقعیت مکانی فرد حاضر در خانه، احساس به شرایط آب و هوایی فرد حاضر در خانه و حالت بدن فرد حاضر در خانه)، نام آن موجودیت مانند تلویزیون، فرد حاضر در خانه و درب بالکن، نوع شرط مورد بررسی با توجه به موجودیت و شرط مورد بررسی مانند کمتر یا بیشتر، داخل یا خارج و برابر یا مخالف یک مقدار مشخص ذکر شده است. در هر شرط انجام فعالیت، آخرین مقادیر دریافتی از حسگرها

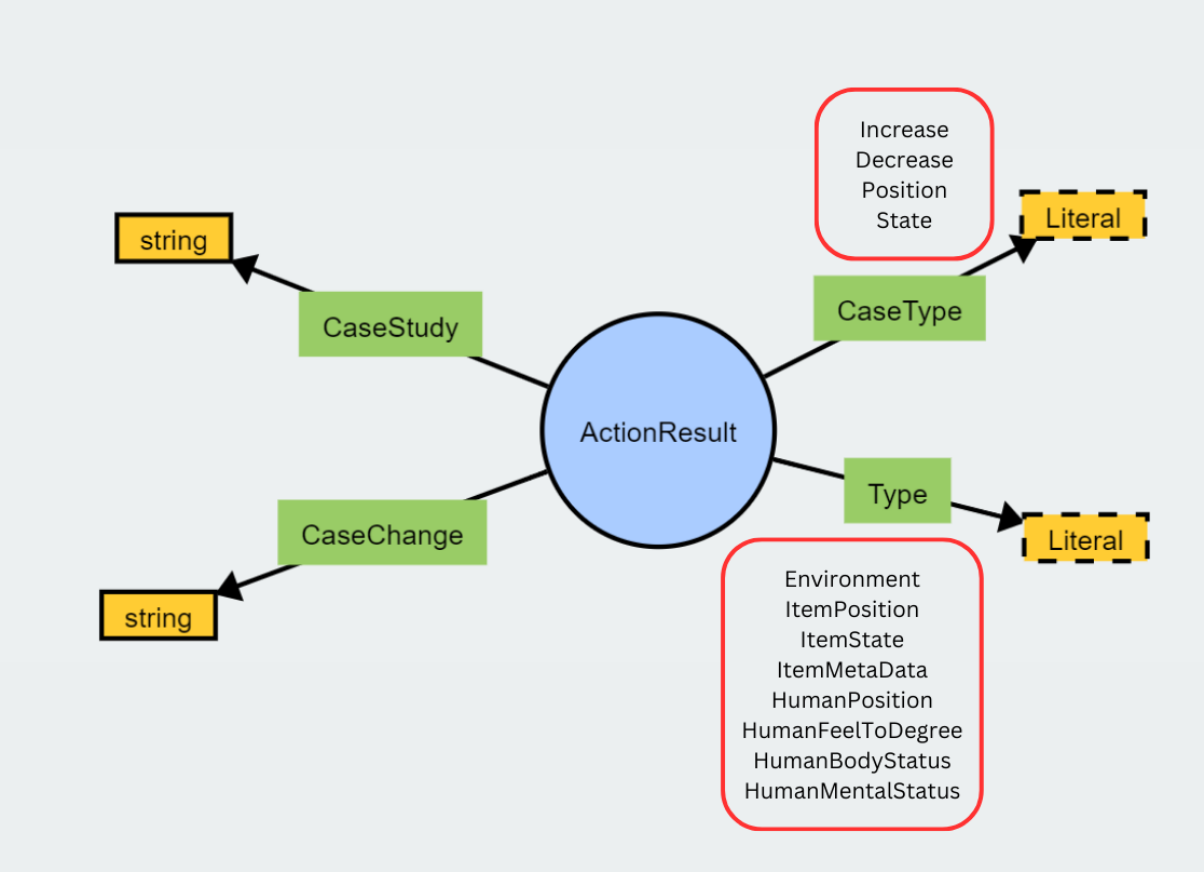
بررسی شده و بر اساس آن‌ها تصمیم گرفته می‌شود (به عنوان مثال اگر شرط انجام یک فعالیت این باشد که دمای خانه هوشمند کمتر از بیست درجه باشد، آخرین مقدار اندازه‌گیری شده توسط حسگر دما، مورد بررسی قرار می‌گیرد).



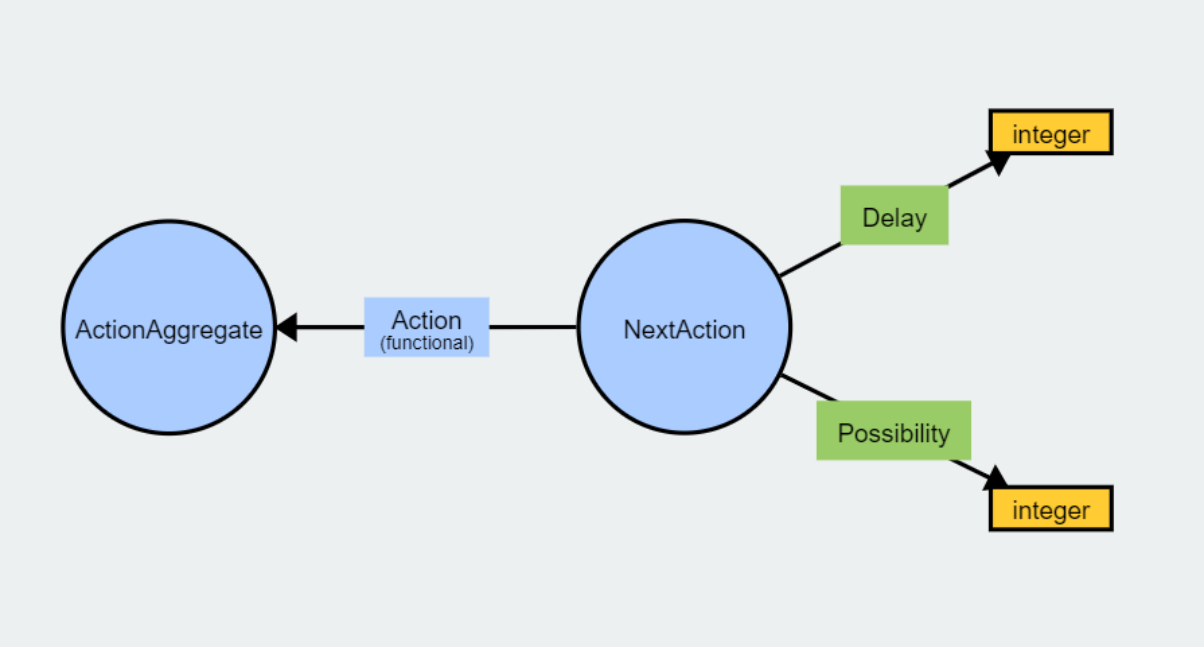

شکل ۴-۹: هستی‌شناسی شرایط فعالیت‌های خانه هوشمند

در هستی‌شناسی نتایج انجام فعالیت که در شکل ۴-۱۰ قابل مشاهده است، نوع موجودیت برای نتیجه اعمال شده، نام موجودیت، نوع نتیجه اعمال شده با توجه به موجودیت و نتیجه اعمال شده مانند افزایش یا کاهش، تغییر موقعیت مکانی و تغییر حالت به یک مقدار مشخص ذکر شده است. در هر نتیجه انجام فعالیت، آخرین مقادیر دریافتی از حسگرها تغییر می‌کند (به عنوان مثال اگر نتیجه انجام یک فعالیت این باشد که دمای خانه هوشمند پنج درجه افزایش پیدا کند، آخرین مقدار اندازه‌گیری شده توسط حسگر دما، تغییر خواهد کرد).

در هستی‌شناسی فعالیت‌های احتمالی بعدی که در شکل ۴-۱۱ قابل مشاهده است، تاخیر انجام فعالیت، احتمال انجام و خود فعالیت مشخص شده است.




شکل ۴-۱۰: هستی‌شناسی نتایج فعالیت‌های خانه هوشمند

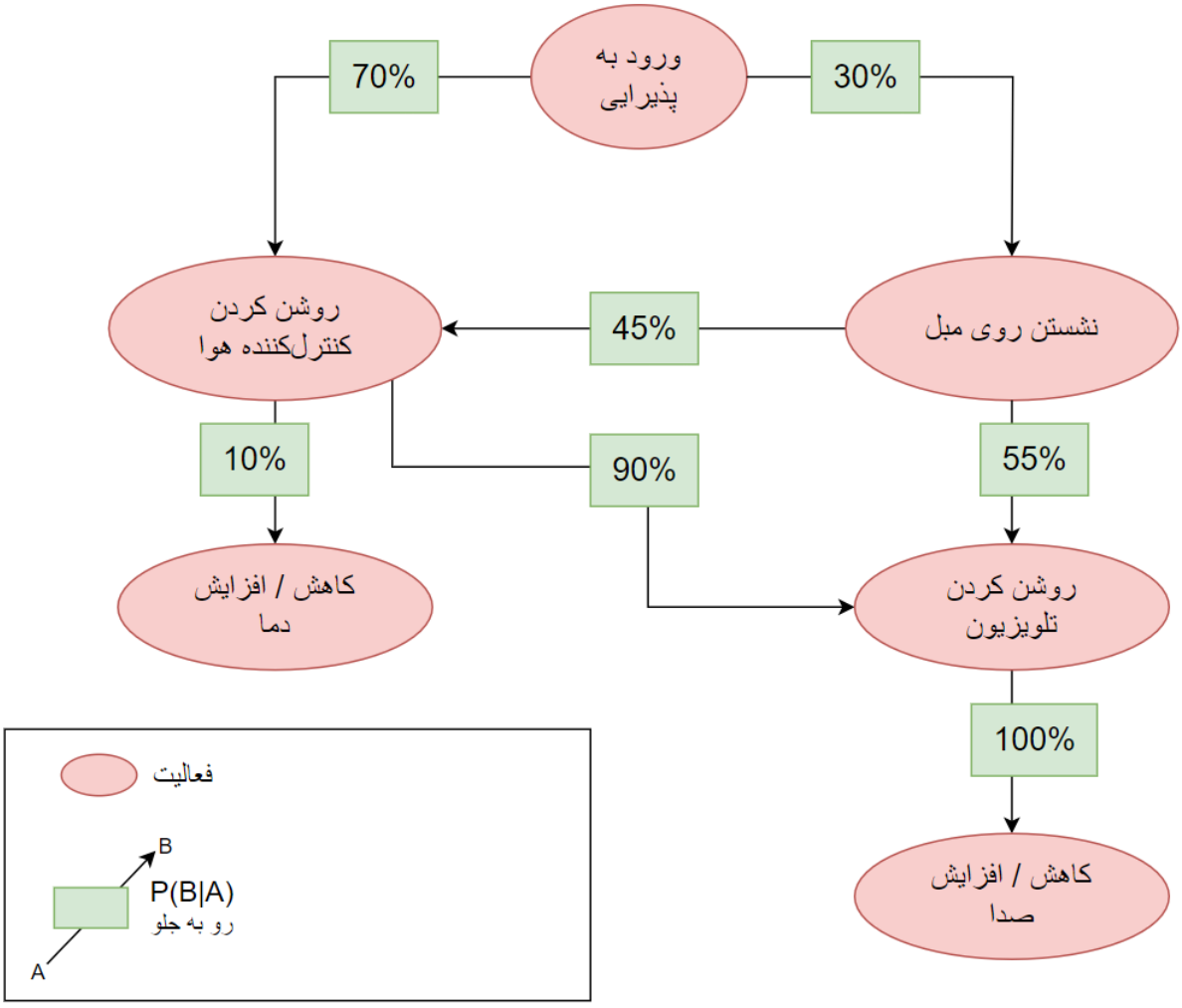



شکل ۴-۱۱: هستی‌شناسی فعالیت‌های احتمالی بعدی خانه هوشمند

## ۴-۴-۲ مدل‌سازی فعالیت کاربر با قوانین انجمنی

در این بخش به مدل‌سازی توالی فعالیت کاربر با استفاده از قوانین انجمنی خواهیم پرداخت و حرکت رو به جلو و رو به عقب سلسله فعالیت‌های کاربر را بررسی خواهیم کرد.

همانطور که در هستی‌شناسی شکل ۴-۱۱ مشاهده شد؛ هر فعالیت شامل لیستی از فعالیت‌های احتمالی بعدی است که احتمال انجام هر یک با توجه به سوابق کاربر در هستی‌شناسی فعالیت‌ها ثبت شده است. با توجه به قوانین انجمنی مطرح شده در بخش ۴-۲، احتمال انجام فعالیت Y پس از فعالیت X همان اطمینان است که بیان می‌کند در چند درصد مواقع پس از انجام فعالیت X، فعالیت Y انجام می‌شود. مثالی از نحوه مدل‌سازی احتمال توالی فعالیت‌ها با استفاده از قوانین انجمنی در شکل ۴-۱۲ قابل مشاهده است (احتمال توالی هر فعالیت پس از فعالیت دیگر به رنگ سبز نشان داده شده است).




شکل ۴-۱۲: مثالی از مدل‌سازی احتمال توالی فعالیت‌ها با استفاده از قوانین انجمنی

حال با توجه به مقدار اطمینان و با استفاده از تعریف پشتیبانی برای انجام فعالیت Y پس از فعالیت X، احتمال انجام فعالیت X قبل از فعالیت Y با فرض انجام Y را تعریف می‌کنیم. این تعریف برای حرکت

عقبگرد بین فعالیت‌ها می‌باشد تا بتوانیم انتخاب فعالیت قبل از یک فعالیت مشخص از بین فعالیت‌های ممکن را با دخیل کردن احتمال انجام هر یک انجام دهیم. این احتمال با استفاده از پشتیبانی انجام فعالیت Y پس از فعالیت X محاسبه می‌شود.

برای انجام محاسبات مربوط به احتمال انتخاب هر فعالیت در حرکت عقبگرد، در ابتدا برای هر فعالیت احتمال رخداد آن به صورت کلی را طبق فرمول زیر محاسبه می‌کنیم:

$$P(X) = \sum_{\text{Parents}} P(\text{Parent}) \cdot P(\text{Parent} \rightarrow X) \qquad (۱-۴)$$

در این فرمول، فعالیت‌هایی که به عنوان فعالیت بعدی در هستی‌شناسی هیچ فعالیت دیگری تعریف نشده‌اند، احتمال یک را دارند. برای دیگر فعالیت‌ها مانند فعالیت X، تمامی فعالیت‌هایی که پس از آن‌ها فعالیت X احتمال انجام دارد را پیدا می‌کنیم (لیست آن فعالیت‌ها را Parents می‌نامیم). سپس احتمال رخداد هر فعالیت Parent که طبق همین فرمول حساب شده را در احتمال رخداد فعالیت X به شرط رخداد فعالیت Parent ضرب کرده و در آخر مقدار به دست آمده به ازای هر فعالیت Parent را با هم جمع می‌کنیم. در ابتدای هر اجرای ابزار پیشنهادی این پژوهش، احتمال رخداد هر فعالیت به صورت کلی را محاسبه و ذخیره می‌کنیم. احتمال رخداد کلی هر فعالیت در مثال شکل ۴-۱۲، در شکل ۴-۱۳ قابل مشاهده است (احتمال کلی رخداد هر فعالیت به رنگ بنفش نشان داده شده است).

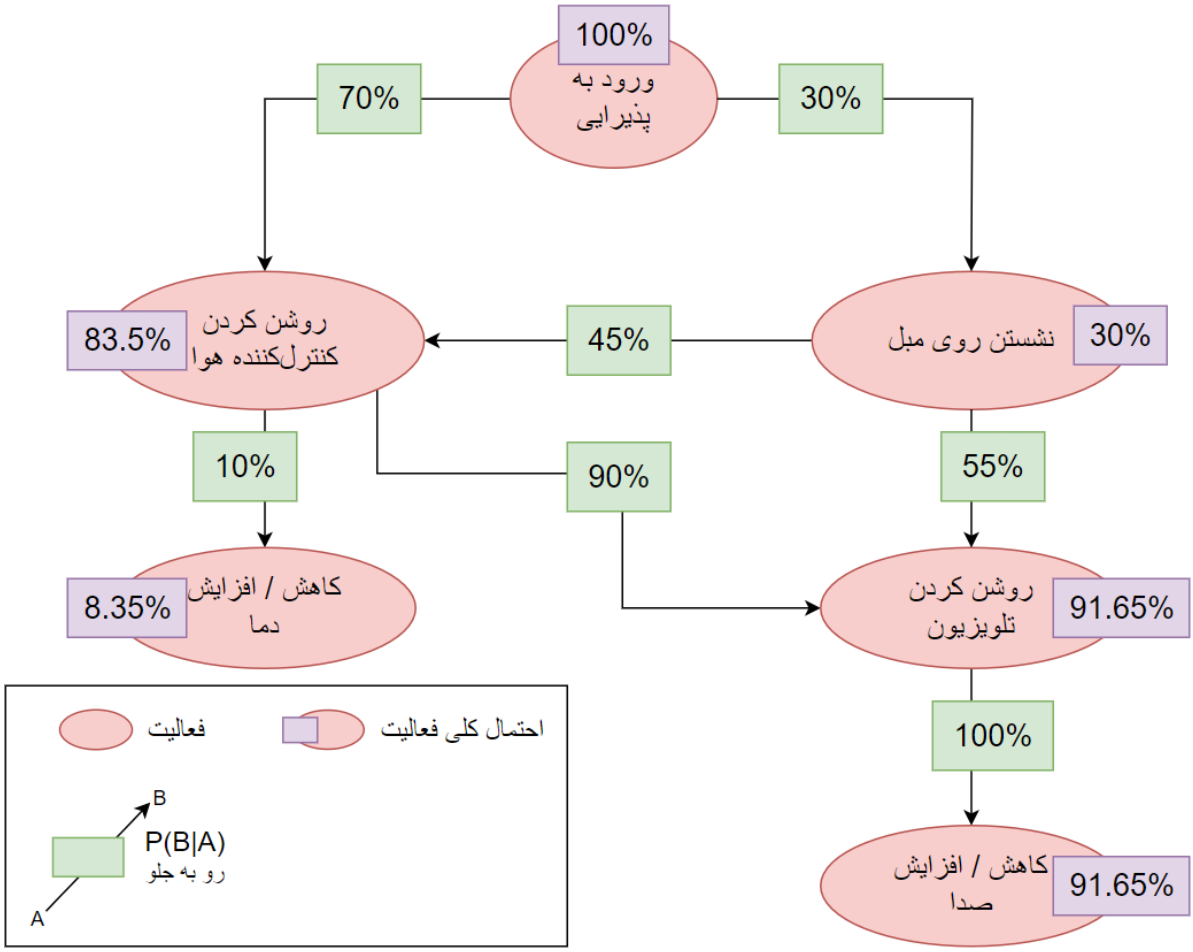
حال برای احتمال عقبگرد، از فرمول احتمالات شرطی استفاده می‌کنیم:

$$P(Y|X) = \frac{P(X|Y) \cdot P(Y)}{P(X)} \qquad (۲-۴)$$

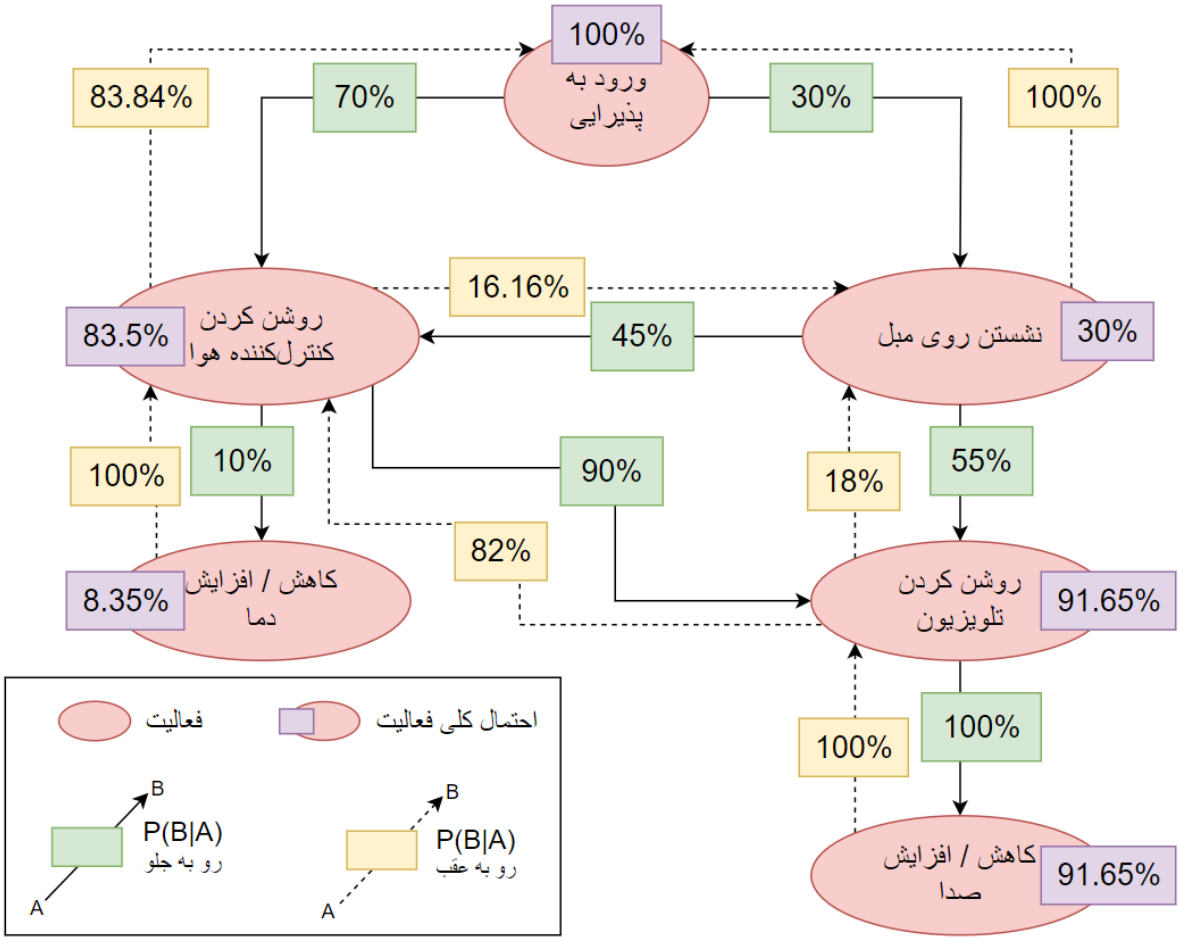
در این فرمول با استفاده از احتمال رخداد هر فعالیت مانند فعالیت X پس از هر فعالیت مانند Y و همچنین احتمال رخداد کلی فعالیت‌های X و Y که محاسبه شده است، احتمال رخداد فعالیت Y به صورت حرکت عقبگرد از فعالیت X قابل محاسبه است. احتمال انتخاب فعالیت‌ها در حرکت عقبگرد در مثال شکل ۴-۱۲، در شکل ۴-۱۴ قابل مشاهده است (احتمال انتخاب هر فعالیت برای حرکت عقبگرد از فعالیتی دیگر به رنگ زرد نشان داده شده است).

### ۴-۴-۳ الگوریتم تولید سلسله فعالیت جعلی

ابزار مبتنی بر راهکار پیشنهادی برای تولید سلسله فعالیت جعلی از الگوریتم نمایش داده شده در شکل ۴-۱۵ استفاده می‌کند. به طور کلی این فرایند به چند فاز مختلف تقسیم می‌شود که در ادامه به بررسی هر

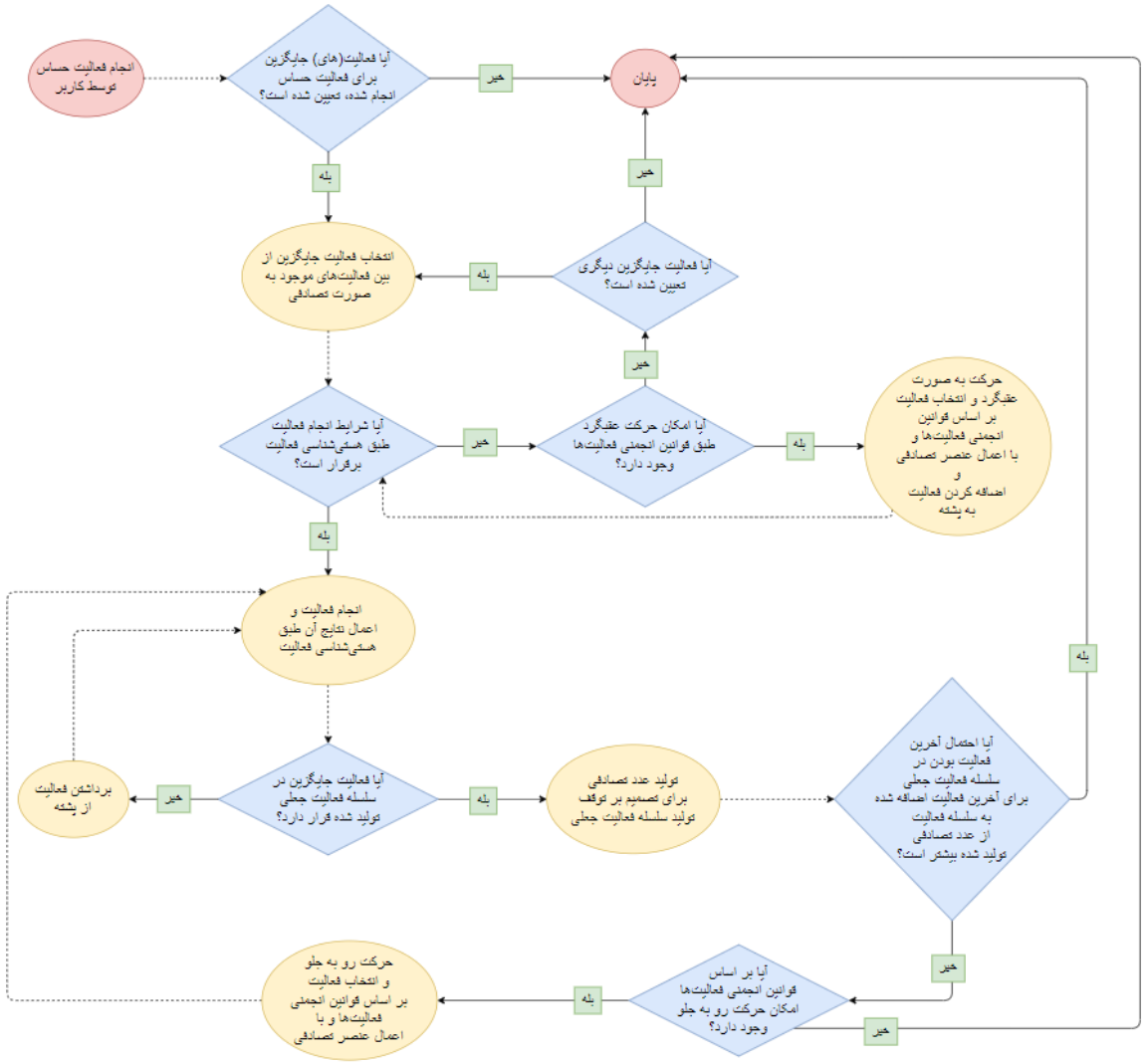



شکل ۴-۱۳: احتمال کلی فعالیت‌ها در مثال شکل ۴-۱۲




شکل ۴-۱۴: احتمال انتخاب فعالیت‌ها در حرکت عقبگرد در مثال شکل ۴-۱۲

یک خواهیم پرداخت.




شکل ۴-۱۵: الگوریتم تولید سلسله فعالیت جعلی

- انجام فعالیت حساس توسط کاربر: در اولین گام، فعالیتی حساس توسط کاربر انجام می‌شود و ابزار مبتنی بر راهکار پیشنهادی، از بین فعالیت‌های جایگزین برای این فعالیت حساس که توسط کاربر تعیین شده است، یکی را به صورت تصادفی انتخاب کرده و اقدام به تولید سلسله فعالیت جعلی می‌کند که این فعالیت جایگزین در آن حضور داشته باشد.

- حرکت عقبگرد: حال ابزار مبتنی بر راهکار پیشنهادی، با شروع از فعالیت جایگزین، حرکتی عقبگرد بر اساس قوانین انجمنی را شروع می‌کند تا جایی که به فعالیتی برسد که شرایط انجام آن طبق هستی‌شناسی فعالیت برقرار باشد. در این حرکت عقبگرد تمامی فعالیت‌ها در یک پشته ذخیره می‌شوند تا در صورت ارضا شدن شرایط یک فعالیت، آن‌ها را از پشته برداریم و به سلسله فعالیت جعلی اضافه کنیم. به طور مثال برای «روشن کردن تلویزیون»، ابتدا باید یک فرد در پذیرایی حضور

داشته باشد و برای حضور در پذیرایی باید از راهرو به آنجا وارد شد. به همین صورت حرکت عقبگرد انجام می‌دهیم تا به طور واقعی حضور فرد و ارضا شدن دیگر شرایط برای یک فعالیت را داشته باشیم؛ حال فعالیت‌های داخل پشته را برداشته و به سلسله فعالیت جعلی اضافه می‌کنیم. توجه شود که انتخاب فعالیت در حرکت عقبگرد بر اساس قوانین انجمنی و با اعمال عنصر تصادفی است که احتمال انتخاب هر فعالیت با استفاده از محاسبات مطرح شده در بخش ۴-۴-۲ انجام می‌شود.

- حرکت رو به جلو: حال که فعالیت جایگزین مورد نظر در سلسله فعالیت جعلی اضافه شده است؛ ابزار مبتنی بر راهکار پیشنهادی برای فریب سکو و یکسان نبودن سلسله فعالیت جعلی برای یک فعالیت جایگزین، حرکتی رو به جلو بر اساس قوانین انجمنی انجام می‌دهد. در ابتدا با استفاده از احتمال توقف آخرین فعالیت که در هستی‌شناسی آمده است تصمیم به ادامه تولید فعالیت جعلی یا توقف می‌گیرد؛ اگر تصمیم بر ادامه تولید فعالیت جعلی گرفته شد، با استفاده از قوانین انجمنی و با اعمال عنصر تصادفی یکی از فعالیت‌های ممکن برای کاربر با استفاده از محاسبات بخش ۴-۴-۲ را انتخاب کرده و آن را به سلسله فعالیت جعلی اضافه می‌کند.
- نقطه توقف نهایی: پس از حرکت رو به جلو جهت فریب سکو، حالت خانه هوشمند را به سمت حالت کنونی واقعی می‌بریم تا از حالات اشیاء و افراد حاضر در خانه پس از مدتی، سکو توانایی تشخیص رخداد سلسله فعالیت جعلی را نداشته باشد. برای این کار آخرین فعالیتی که تاثیر مهمی در حالات افراد حاضر در خانه و اشیاء گذاشته را از داده‌های حسگرها دریافت می‌کنیم، سپس اقدام به تولید مجدد سلسله فعالیت جعلی تا انجام آن فعالیت به عنوان فعالیت نهایی می‌کنیم. پس از تولید هر فعالیت جعلی، آخرین فعالیت با تاثیر مهم را بررسی مجدد می‌کنیم تا به صورت پویا و بدون تولید کامل سلسله فعالیت جعلی، حالت توقف را به حالت واقعی خانه هوشمند نزدیک کنیم. با استفاده از این روش همواره به حالت واقعی خانه هوشمند می‌رسیم که در بدترین حالت که تغییر سریع و مداوم حالت خانه هوشمند است، در هنگام پایان روز و زمان خوابیدن کاربران به حالت واقعی خانه هوشمند می‌رسیم.

در تولید سلسله فعالیت جعلی، جهت نزدیک بودن به واقعیت، مدت زمان میانگین انجام هر فعالیت را نیز در هستی‌شناسی لحاظ کرده‌ایم. علاوه بر آن، از آنجایی که تمامی موجودیت‌ها در خانه، هوشمند نیستند و ابزار مبتنی بر راهکار پیشنهادی از جزئیات کامل خبر ندارد؛ یک تاخیر بین فعالیت‌ها لحاظ می‌شود که زمان بین اتمام یک فعالیت و شروع فعالیت بعدی است. به طور مثال پس از «ورود به خانه»، «روشن کردن کولر» به طور میانگین پس از دو ثانیه انجام می‌شود که این زمان، حرکت کاربر از درب خانه به سمت کولر و روشن کردن آن است.

با استفاده از مدت زمان انجام هر فعالیت و فاصله زمانی آن تا فعالیت بعدی، هر فعالیتی که به سلسله فعالیت جعلی اضافه شود؛ یک زمان انجام فعالیت معینی دارد که آن زمان، زمان انجام فعالیت قبلی علاوه بر مدت زمان انجام آن و تاخیر بین فعالیت قبلی و فعالیت کنونی است. به طور مثال اگر «ورود به خانه» به مدت یک ثانیه طول می‌کشد و همچنین میانگین تاخیر بین باز کردن درب خانه و روشن کردن کولر هشت ثانیه باشد؛ زمان انجام فعالیت «روشن کردن کولر» ۱ + ۸ = ۹ ثانیه پس از «ورود به خانه» خواهد بود.

### ۴-۴-۴ عوامل تصادفی‌ساز

از آنجا که سکو قادر به ذخیره و مقایسه‌ی سلسله فعالیت‌ها و همچنین کشف شباهت بین آن‌هاست؛ در تولید سلسله فعالیت جعلی از عوامل تصادفی‌ساز استفاده می‌کنیم تا تنوع در تولید خروجی لحاظ شود. در این بخش به بررسی این عوامل خواهیم پرداخت.

- انتخاب فعالیت جایگزین: زمانی که فعالیتی حساس انجام می‌شود، فعالیت جایگزین از بین فعالیت‌های جایگزینی که ترجیح کاربر است به طور تصادفی انتخاب می‌شود.
- انتخاب فعالیت در حرکت عقبگرد: همانطور که اشاره شد، زمانی که به صورت عقبگرد حرکت می‌کنیم، احتمال انتخاب هر فعالیت به صورت تصادفی بوده اما احتمال محاسبه شده در قوانین انجمنی برای حرکت عقبگرد، به عنوان وزن در این انتخاب لحاظ می‌شود. برای این کار برای هر فعالیت سهمی برابر احتمال محاسبه شده در نظر می‌گیریم، سپس عددی تصادفی تولید کرده و با توجه به این که مقدار آن در سهم کدام فعالیت است، فعالیت مورد نیاز را انتخاب می‌کنیم. با این کار علاوه بر لحاظ کردن وزن به دست آمده با استفاده از قوانین انجمنی، از عنصر تصادفی نیز بهره بردیم.

  به عنوان مثال، سه فعالیت با احتمال محاسبه شده‌ی ۱۰، ۳۰ و ۶۰ درصد داریم، سهم فعالیت اول بازه ۰ تا ۱۰، سهم فعالیت دوم بازه ۱۰ تا ۴۰ و سهم فعالیت سوم بازه ۴۰ تا ۱۰۰ است. حال عدد تصادفی بین ۰ تا ۱۰۰ تولید می‌کنیم و فعالیت منتخب، فعالیتی خواهد بود که عدد تصادفی تولید شده متعلق به بازه‌ی آن است.
- انتخاب فعالیت در حرکت رو به جلو: با استفاده از قوانین انجمنی و هستی‌شناسی فعالیت‌ها، برای حرکت رو به جلو فعالیت بعدی در سلسله فعالیت جعلی را به صورت تصادفی انتخاب کرده اما مانند انتخاب فعالیت در حرکت عقبگرد، احتمال انجام فعالیت‌ها در تعیین فعالیت بعدی به صورت تصادفی لحاظ می‌شوند.

- تصمیم توقف: پس از آن که فعالیت جایگزین در سلسله فعالیت جعلی اضافه شد؛ امکان حرکت رو به جلو یا توقف داریم. این تصمیم با مقدار احتمال توقف که هر فعالیت در هستی‌شناسی خود آن را دارد انجام می‌پذیرد و به صورت وزن‌دار لحاظ می‌شود اما در نهایت این تصمیم به صورت تصادفی بوده و در هر بار اجرا امکان توقف یا حرکت رو به جلو داریم.
- مدت زمان انجام فعالیت و تاخیر بین فعالیت‌ها: همانطور که اشاره شد، زمان انجام هر فعالیت در سلسله فعالیت جعلی با استفاده از زمان انجام فعالیت قبلی، مدت زمان انجام آن و تاخیر بین این دو فعالیت محاسبه خواهد شد. حال برای آن که فاصله‌ی انجام بین دو فعالیت مشخص همیشه یکسان نباشد، مدت زمان انجام فعالیت‌ها و تاخیر بین انجام فعالیت‌های مختلف در سلسله فعالیت جعلی، با مقداری تصادفی بین حداقل زمان مورد نیاز تا پنج برابر حداقل زمان مورد نیاز جمع زده می‌شوند تا هر بار فاصله‌ی بین انجام فعالیت‌ها نیز متفاوت باشد.

## ۵-۴ جمع‌بندی

در این فصل به طور کامل راهکار پیشنهادی را بررسی کرده و توصیف اجمالی راه حل را ارائه کردیم. برای طراحی هر چه بهتر این نرم‌افزار مدل تهدید را بررسی کرده و بر اساس آن معماری کلان و مدل‌سازی را با جزئیات توصیف کردیم.

# فصل ۵

# پیاده‌سازی و ارزیابی

در این پژوهش تولید سلسله فعالیت جعلی به نحوی که از دید سکو قابل تمایز با سلسله فعالیت واقعی نباشد؛ نیاز به پیاده‌سازی دقیق مدل‌سازی مطرح شده در بخش ۴-۴ و ارزیابی کامل بر اساس مدل تهدید گفته شده در بخش ۴-۲ است. در این فصل به توصیف کلی پیاده‌سازی نرم‌افزار و ارزیابی کامل آن با نمونه داده‌های متنوع بر اساس مدل تهدید سکوی بدخواه خواهیم پرداخت.

## ۵-۱ پیاده‌سازی

## ۵-۲ ارزیابی

برای ارزیابی این پژوهش میزان گمراه‌سازی سکو با تولید رخدادهای جعلی بر اساس مجموعه داده‌ای از فعالیت‌های کاربر توسط ابزار پیاده‌سازی شده اندازه‌گیری شده است. بدین منظور ابتدا هستی‌شناسی متناسب با مجموعه داده تعریف شده و پس از تولید سلسله فعالیت جعلی، ترکیب آن با سلسله فعالیت واقعی به دسته‌بند داده شده و میزان کاهش دقت آن به عنوان معیار ارزیابی در نظر گرفته شده است. این معیار نشان‌دهنده قدرت راهکار پیشنهادی در گمراه‌سازی سکو است.

### ۵-۲-۱ مجموعه دادگان

مجموعه داده مورد استفاده در این پژوهش مجموعه داده Orange4Home [؟] است که شامل تقریباً ۱۸۰ ساعت فعالیت‌های روزمره یک فرد است که به مدت ۴ هفته متوالی در روزهای کاری انجام شده است.

این مجموعه داده شامل داده‌های ۲۳۶ حسگر ناهمگن است که به‌طور یکپارچه در سراسر یک آپارتمان پخش شده‌اند و ۲۰ دسته فعالیت که توسط فرد به‌طور دقیق در محل برچسب‌گذاری شده‌اند، و در مجموع ۴۹۳ نمونه از فعالیت‌ها را شامل می‌شود. این ویژگی‌ها، Orange4Home را به یک مجموعه داده مناسب برای ارزیابی الگوریتم‌های شناسایی فعالیت، ارزیابی الگوریتم‌های پیش‌بینی فعالیت و سایر مسائل پژوهشی مرتبط با الگوریتم‌ها و خانه‌های هوشمند تبدیل می‌کند.

خانه هوشمند استفاده شده در مجموعه داده Orange4Home شامل بخش‌های ورودی، آشپزخانه، دستشویی، پذیرایی و راه پله در طبقه همکف و راه پله، راهرو، دفتر کار، حمام و اتاق خواب در طبقه اول است که این نقشه در اشکال ۵-۱ و ۵-۲ قابل مشاهده است.


شکل ۵-۱: نقشه خانه مجموعه داده **Orange4Home**، طبقه همکف


شکل ۵-۲: نقشه خانه مجموعه داده **Orange4Home**، طبقه اول

در هر بخش از این خانه هوشمند، حسگرهایی با انواع دودویی[۱]، عدد صحیح[۲]، عددی[۳] و دسته‌ای[۴] وجود دارد که تعداد این حسگرها به تفکیک بخش‌های مختلف خانه هوشمند، در شکل ۵-۱ قابل مشاهده است. تعدادی از حسگرها در مجموعه داده Orange4Home سراسری و برای کل خانه است که این مقادیر رابطه مستقیم با فعالیت فعلی کاربر و داده حسگرهای مربوط به فعالیت‌ها ندارند، در نتیجه در مجموعه داده و تولید سلسله فعالیت جعلی از این داده‌ها صرف نظر شده است و به جای ۲۳۶ حسگر، در این پژوهش از ۱۹۶ حسگر (با حذف حسگرهای سراسری) استفاده شده است.

جدول ۵-۱: حسگرهای هر بخش خانه هوشمند

| محل | دودویی | عدد صحیح | عددی | دسته‌ای | مجموع |
|---|---|---|---|---|---|
| ورودی | ۳ | ۱ | ۲ | ۳ | ۹ |
| آشپزخانه | ۱۳ | ۲۱ | ۱۸ | ۰ | ۵۲ |
| پذیرایی | ۱۶ | ۶ | ۸ | ۷ | ۳۷ |
| دستشویی | ۳ | ۱ | ۱ | ۰ | ۵ |
| راه پله | ۳ | ۰ | ۰ | ۰ | ۳ |
| راهرو | ۹ | ۰ | ۱ | ۰ | ۱۰ |
| حمام | ۹ | ۶ | ۸ | ۳ | ۲۶ |
| دفتر کار | ۹ | ۳ | ۳ | ۵ | ۲۰ |
| اتاق خواب | ۱۷ | ۴ | ۶ | ۷ | ۳۴ |
| سراسری | ۱ | ۱۳ | ۲۰ | ۶ | ۴۰ |
| مجموع | ۸۳ | ۵۵ | ۶۷ | ۳۱ | ۲۳۶ |

در این مجموعه داده فعالیت‌های برچسب‌گذاری شده شامل داده‌های حسگرها می‌باشند و تمامی اطلاعات ارسالی از حسگرها بین شروع و پایان برچسب یک فعالیت است. هر فعالیت‌های برچسب‌گذاری شده متعلق به یک بخش خانه است که در ادامه لیستی از این فعالیت‌ها را داریم:

- ورودی: ورود، خروج
- آشپزخانه: آماده‌سازی، آشپزی، شستن ظروف

[۱] Binary
[۲] Integer
[۳] Real number
[۴] Categorical

- پذیرایی: خوردن، تلویزیون دیدن، کار با رایانه
- دستشویی: استفاده از دستشویی
- راه پله: بالا رفتن، پایین آمدن
- حمام: استفاده از روشویی، استفاده از دستشویی، حمام کردن
- دفتر کار: کار با رایانه، تلویزیون دیدن
- اتاق خواب: لباس عوض کردن، کتاب خواندن، خوابیدن
- تمامی بخش‌ها: تمیز کردن

همانطور که گفته شد، داده‌های حسگرها بین شروع و پایان یک فعالیت برچسب‌گذاری شده ارسال می‌شوند. در مجموعه داده Orange4Home، یک فایل csv قرار دارد که داده حسگرها با را در خود دارد. این داده‌ها شامل زمان دقیق ارسال داده توسط حسگر، نام حسگر و مقدار ارسال شده توسط آن حسگر است که نمونه داده موجود در مجموعه داده در شکل ۵-۳ قابل مشاهده است. در این شکل شروع فعالیت ورود به خانه است که در همان دقیقه ورود و باز کردن درب، داده‌های مربوط به صدای محیط، روشن شدن چراغ و ... به صورت خودکار به سکو ارسال می‌گردد.

| Time | ItemName | Value |
|---|---|---|
| 1/30/2017 7:58 | label | START:Entrance\|Entering |
| 1/30/2017 7:58 | livingroom_couch_plug_consumption | 0 |
| 1/30/2017 7:58 | office_desk_plug_consumption | 0 |
| 1/30/2017 7:58 | office_tv_plug_consumption | 0 |
| 1/30/2017 7:58 | livingroom_tv_plug_consumption | 1 |
| 1/30/2017 7:58 | livingroom_table_plug_consumption | 0 |
| 1/30/2017 7:58 | livingroom_table_noise | 0.278974 |
| 1/30/2017 7:58 | livingroom_table_noise | 0.640542 |
| 1/30/2017 7:58 | livingroom_table_noise | 2.10256 |
| 1/30/2017 7:58 | livingroom_table_noise | 0.429033 |
| 1/30/2017 7:58 | livingroom_table_noise | 0.182365 |
| 1/30/2017 7:58 | livingroom_couch_plug_consumption | 0 |
| 1/30/2017 7:58 | office_desk_plug_consumption | 0 |
| 1/30/2017 7:58 | office_tv_plug_consumption | 0 |
| 1/30/2017 7:58 | livingroom_tv_plug_consumption | 1 |
| 1/30/2017 7:58 | livingroom_table_plug_consumption | 0 |
| 1/30/2017 7:58 | livingroom_couch_noise | 0.354432 |
| 1/30/2017 7:58 | bedroom_CO2 | 490.88 |
| 1/30/2017 7:58 | entrance_door | OPEN |
| 1/30/2017 7:58 | livingroom_couch_noise | 0.165306 |
| 1/30/2017 7:58 | livingroom_couch_plug_consumption | 0 |
| 1/30/2017 7:58 | office_desk_plug_consumption | 0 |
| 1/30/2017 7:58 | office_tv_plug_consumption | 0 |
| 1/30/2017 7:58 | livingroom_tv_plug_consumption | 1 |
| 1/30/2017 7:58 | livingroom_table_plug_consumption | 0 |
| 1/30/2017 7:58 | entrance_switch_left | ON |
| 1/30/2017 7:58 | entrance_light1 | 100 |
| 1/30/2017 7:58 | entrance_switch_left | OFF |
| 1/30/2017 7:58 | staircase_light | 100 |
| 1/30/2017 7:58 | kitchen_luminosity | 20 |
| 1/30/2017 7:58 | entrance_door | CLOSED |

شکل ۵-۳: نمونه داده ارسالی از حسگرها

## ۵-۲-۲ هستی‌شناسی

برای استخراج هستی‌شناسی از مجموعه داده Orange4Home، ابتدا مجاورت بخش‌های مختلف خانه بر اساس نقشه تعریف شده است. سپس نسخه‌ای فیلتر شده از مجموعه داده که فقط دارای فعالیت‌های برچسب‌گذاری شده است را تهیه کردیم که بخشی از آن در شکل ۵-۴ قابل مشاهده است. از این مجموعه داده برای محاسبه احتمال رخداد یک فعالیت پس از دیگری استفاده شده است تا بتوانیم سلسله فعالیت جعلی غیر قابل تمایز با استفاده از قوانین انجمنی تولید کنیم (جزئیات استفاده از احتمالات در قوانین انجمنی، در بخش ۴-۴-۲ آورده شده است).

| Time | ItemName | Value |
|---|---|---|
| 1/30/2017 7:58 | label | START:Entrance\|Entering |
| 1/30/2017 8:01 | label | STOP:Entrance\|Entering |
| 1/30/2017 8:01 | label | START:Staircase\|Going_up |
| 1/30/2017 8:02 | label | STOP:Staircase\|Going_up |
| 1/30/2017 8:02 | label | START:Bathroom\|Showering |
| 1/30/2017 8:18 | label | STOP:Bathroom\|Showering |
| 1/30/2017 8:18 | label | START:Bathroom\|Using_the_sink |
| 1/30/2017 8:22 | label | STOP:Bathroom\|Using_the_sink |
| 1/30/2017 8:22 | label | START:Staircase\|Going_down |
| 1/30/2017 8:23 | label | STOP:Staircase\|Going_down |
| 1/30/2017 8:23 | label | START:Living_room\|Watching_TV |
| 1/30/2017 8:45 | label | STOP:Living_room\|Watching_TV |
| 1/30/2017 8:45 | label | START:Toilet\|Using_the_toilet |
| 1/30/2017 8:48 | label | STOP:Toilet\|Using_the_toilet |
| 1/30/2017 8:48 | label | START:Staircase\|Going_up |
| 1/30/2017 8:48 | label | STOP:Staircase\|Going_up |
| 1/30/2017 8:48 | label | START:Office\|Computing |
| 1/30/2017 11:45 | label | STOP:Office\|Computing |
| 1/30/2017 11:45 | label | START:Staircase\|Going_down |
| 1/30/2017 11:46 | label | STOP:Staircase\|Going_down |
| 1/30/2017 11:46 | label | START:Kitchen\|Preparing |
| 1/30/2017 11:48 | label | STOP:Kitchen\|Preparing |
| 1/30/2017 11:48 | label | START:Kitchen\|Cooking |
| 1/30/2017 12:02 | label | STOP:Kitchen\|Cooking |
| 1/30/2017 12:02 | label | START:Living_room\|Eating |
| 1/30/2017 12:16 | label | STOP:Living_room\|Eating |
| 1/30/2017 12:16 | label | START:Kitchen\|Washing_the_dishes |
| 1/30/2017 12:25 | label | STOP:Kitchen\|Washing_the_dishes |
| 1/30/2017 12:25 | label | START:Living_room\|Cleaning |
| 1/30/2017 12:26 | label | STOP:Living_room\|Cleaning |
| 1/30/2017 12:26 | label | START:Living_room\|Computing |

شکل ۵-۴: بخشی از مجموعه داده فیلتر شده که فقط فعالیت‌ها در آن هستند.

سپس، داده حسگرها مربوط به هر فعالیت برچسب‌گذاری شده را استخراج میکنیم و پس از تولید سلسله فعالیت جعلی بر اساس هستی‌شناسی و قوانین انجمنی فعالیت‌ها، به جای هر فعالیت یکی از سلسله داده حسگرهای موجود در مجموعه داده برای آن فعالیت را به صورت تصادفی انتخاب میکنیم و به سکو ارسال می‌کنیم. سلسله داده‌های ارسالی حسگرها به ازای هر فعالیت در هستی شناسی آن فعالیت و ارتباط

با حسگرها قرار داده شده است.

### ۵-۲-۳ دسته‌بند

همان‌طور که بیان شد، برای ارزیابی کیفیت رخدادهای جعلی تولید شده توسط ابزار پیشنهادی، میزان افت دقت تشخیص فعالیت توسط یک دسته‌بند اندازه‌گیری می‌شود. برای این منظور از دسته‌بند استفاده شده در کار پژوهشی اقوامی و همکاران به عنوان معیار ارزیابی استفاده شده است که با دقت ۹۸ درصد فعالیت متناظر با رخدادهای مجموعه‌داده Orange4Home را تشخیص می‌دهد. این دسته‌بند یک شبکه عصبی پیچشی است که معماری آن در شکل ؟؟ آورده شده است. ورودی این دسته‌بند یک بردار شامل ۱۹۶ مقدار است که هر کدام نشانگر یک سنسور در خانه است و مقدار آن بیانگر آخرین رخداد گزارش شده از سنسور است. بدین ترتیب دسته‌بند با داشتن یک وضعیت از تمام سنسورهاُفعالیت کاربر در آن زمان را تشخیص می‌دهد.

### ۵-۲-۴ نتایج

# فصل ۶

# نتیجه‌گیری

در این پژوهش راهکاری مبتنی بر تولید رویداد جعلی برای حفظ حریم خصوصی کاربر در برابر سکوی نامعتمد در خانه هوشمند ارائه شد. این راهکار برای فریب سکو و پنهان‌سازی فعالیت‌های حساس کاربر، از تولید سلسله فعالیت جعلی بنا به درخواست کاربر بهره می‌برد تا سکوی اینترنت اشیاء متوجه تفاوت بین فعالیت‌های جعلی و واقعی نشود. در ادامه ضمن جمع‌بندی، به طرح پیشنهادهایی برای پژوهش‌های آینده و تکمیل راهکار خواهیم پرداخت.

## ۶-۱ جمع‌بندی

هدف این پژوهش تولید سلسله فعالیت جعلی برای حفظ حریم خصوصی کاربر بوده که برای این هدف از روش تولید رویداد جعلی بهره برداری شده است. تولید رویداد جعلی بر اساس هستی‌شناسی خانه هوشمند بوده که دانش اولیه‌ی آن توسط فرد خبره با روش دانش‌محور فراهم شده است.

برای عدم تشخیص سکوی نامعتمد، از عوامل تصادفی‌ساز در انجام و زمان‌بندی هر رویداد جعلی استفاده شده و هر رویداد توسط نرم‌افزار، برچسب جعلی می‌خورد و به سکو ارسال می‌شود. کنش مربوط به رویدادها توسط نرم‌افزار نظارت شده و کنش‌های مربوط به رویدادهای جعلی کنار گذاشته می‌شود تا بهره‌وری خانه هوشمند پایین نیاید.

رویکرد استفاده شده در این پژوهش که بر مبنای هستی‌شناسی بوده، تا کنون کمتر مورد توجه قرار گرفته است و امید است تا حریم خصوصی کاربران در خانه هوشمند با استفاده از نتایج این پژوهش، حفظ شود.

## ۶-۲ پیشنهادهایی برای پژوهش‌های آینده

جهت تکمیل راهکار ارائه شده در این پژوهش جهت حفظ حریم خصوصی کاربر در خانه هوشمند، پیشنهادهای زیر ارائه می‌گردد:

- ذخیره‌ی وضعیت موجودیت‌ها از دیدگاه سکو: چنانچه سکوی اینترنت اشیاء، وضعیت و موقعیت موجودیت‌ها را ذخیره و روی آن‌ها استنتاج کند؛ می‌تواند متوجه جعلی بودن سلسله فعالیت شود. با استفاده از نرم‌افزار این پژوهش، بعد از مدت زمانی سکو متوجه جعلی بودن سلسله فعالیت‌های قبلی می‌شود اما امکان تشخیص این که کدام سلسله فعالیت جعلی بوده را ندارد. حتی در صورتی که بتواند با استنتاج روی کنش‌های اعمال نشده متوجه این امر شود، کماکان برای سلسله فعالیت‌های آینده امکان تشخیص در آن لحظه را ندارد زیرا هر بار سلسله فعالیتی متنوع با استفاده از عوامل تصادفی‌ساز تولید می‌شود. حال اگر نیاز به حل این مشکل باشد، نرم‌افزار باید وضعیت کامل خانه هوشمند از دید سکو را به طول کامل و با جزئیات ذخیره کند تا تولید سلسله فعالیت‌های جعلی بعدی و ترکیب آن با سلسله فعالیت‌های واقعی را بتواند انجام دهد تا تشخیص جعلی بودن یک سلسله فعالیت از دید سکو دشوارتر و حتی غیرممکن شود.
- استفاده از روش ترکیبی در ارائه دانش: برای تکمیل هستی‌شناسی خانه هوشمند، می‌توان تشخیص فعالیت کاربران را پس از ارائه دانش توسط فرد خبره، همواره کامل‌تر کرد که تکمیل تشخیص فعالیت کاربران با استفاده از روش داده‌محور است. این تکمیل هستی‌شناسی، برای تنوع در سلسله فعالیت‌های جعلی و به روز بودن نرم‌افزار از رفتار کاربران است که در تکمیل این پژوهش می‌تواند عمل کند.

# واژه‌نامه فارسی به انگلیسی

## آ

آشفته‌سازی ..... Randomization

## ا

ابر ..... Cloud
استدلال منطقی ..... Logical reasoning
اطلاعات حساس ..... Sensitive information
اطمینان ..... Confidence
امنیت ..... Safety
انتها به انتها ..... End-to-End
اینترنت اشیاء ..... Internet of things

## ب

بازیابی اطلاعات ..... Data recovery
برخط ..... Online
بیز ساده ..... Naive bayes

## پ

پایگاه دانش ..... Knowledge base
پردازش زبان طبیعی Natural Language Processing
پشتیبانی ..... Support

## ت

تا حدودی مشاهده‌پذیر ..... Partially observable
تجارت الکترونیک ..... Electronic commerce
تجهیزات پوشیدنی ..... Bearable device

## ج

جابجایی ..... Replacement

## ح

حریم خصوصی ..... Privacy
حسگر ..... Sensor
حمله کانال جانبی ..... Side channel attack

## خ

خانه هوشمند ..... Smart home
خودرمزگذار ..... AutoEncoder
خودکارسازی ..... Automation
خوشه‌بندی ..... Clustering

## د

داده کاوی ..... Data mining
داده محور ..... Data-driven
دانش محور ..... Knowledge-driven
درخت تصمیم ..... Decision tree

درشت‌دانه ..... Coarse-grained

دسته‌بند ..... Classifier

## ر

رفتار جعلی ..... Fake behavior

رفتار کاربر ..... User behavior

روابط ..... Relations

رهانا ..... Trigger

ریزدانه ..... Fine-grained

## ز

زمینه ..... Context

## س

سکوی اینترنت اشیاء . Internet of things platform

## ش

شبکه بیزین ..... Bayesian network

شبکه عصبی ..... Neural network

شبکه عصبی پرسپترون چندلایه ..... Multi-layer perceptron neural network

شبکه منطق مارکوف ..... Markov login network

شروع سرد ..... Cold-start

شناسایی ..... Recognition

## ص

صوری ..... Formal

## ط

طول جغرافیایی ..... Longitude

## ع

عرض جغرافیایی ..... Latitude

عملگر ..... Actuator

عوامل تصادفی‌ساز ..... Randomizing factors

## ف

فراداده ..... Metadata

فراسطح ..... Meta-level

فرد خبره ..... Expert

فیلترینگ ..... Filtering

## ق

قواعد ..... Rules

قوانین انجمنی ..... Associative rules

## ک

کلاس‌بندی ..... Classification

کنش ..... Action

## م

ماشین بردار پشتیبان .... Support vector machine

مدل پنهان مارکوف ..... Hidden markov model

مدل پنهان مارکوف جفت‌شده .... Coupled hidden markov model

مراقبت‌های بهداشتی ..... Health care

مشمول‌سازی ..... Subsumption reasoning

معناشناسی ..... Semantics

مفاهیم ..... Concepts

منطق توصیفی ..... Description logic

منطق دودویی ..... Binary logic

منطق فازی ..... Fuzzy logic

منطق مرتبه اول ..... First order logic

موتور جستجو ..... Search engine

موجودیت ..... Entity

موجودیت‌های زمانی ..... TemporalThings

موجودیت‌های فضایی ..... SpatialThings

مهاجم ..... Attacker

مهندسی دانش ..... Knowledge engineering

## ن

ناهمگونی ..... Heterogeneity

نزدیکترین همسایه ..... Nearest neighbor

نگاشت ..... Mapping

نمونه‌ها ..... Instances

نمونه خصمانه ..... Adversarial example

## و

وب معنایی ..... Semantic web

## ه

هاب ..... Hub

هستی‌شناسی ..... Ontology

همبستگی ..... Correlation

## ی

یادگیری استقرایی ..... Inductive learning

یادگیری ماشین ..... Machine learning

یادگیری نیمه‌نظارتی ..... Semi-supervised learning

# واژه‌نامه انگلیسی به فارسی

## A

Action ..... کنش

Actuator ..... عملگر

Adversarial example ..... نمونه خصمانه

Associative rules ..... قوانین انجمنی

Attacker ..... مهاجم

AutoEncoder ..... خودرمزگذار

Automation ..... خودکارسازی

## B

Bayesian network ..... شبکه بیزین

Bearable device ..... تجهیزات پوشیدنی

Binary logic ..... منطق دودویی

## C

Classification ..... کلاس‌بندی

Classifier ..... دسته‌بند

Cloud ..... ابر

Clustering ..... خوشه‌بندی

Coarse-grained ..... درشت‌دانه

Cold-start ..... شروع سرد

Concepts ..... مفاهیم

Confidence ..... اطمینان

Context ..... زمینه

Correlation ..... همبستگی

Coupled hidden markov model ..... مدل پنهان مارکوف جفت‌شده

## D

Data mining ..... داده کاوی

Data recovery ..... بازیابی اطلاعات

Data-driven ..... داده محور

Description logic ..... منطق توصیفی

Decision tree ..... درخت تصمیم

## E

Electronic commerce ..... تجارت الکترونیک

End-to-End ..... انتها به انتها

Entity ..... موجودیت

Expert ..... فرد خبره

## F

Fake behavior ..... رفتار جعلی

Filtering ..... فیلترینگ

Fine-grained ..... ریزدانه

First order logic ..... منطق مرتبه اول

Formal ..... صوری

Fuzzy logic ..... منطق فازی

## H

Health care ..... مراقبت‌های بهداشتی

Heterogeneity ..... ناهمگونی

Hidden markov model..... مدل پنهان مارکوف

Hub..... هاب

## I

Inductive learning ..... یادگیری استقرایی

Instances..... نمونه‌ها

Internet of things ..... اینترنت اشیاء

Internet of things platform . سکوی اینترنت اشیاء

## K

Knowledge base..... پایگاه دانش

Knowledge engineering ..... مهندسی دانش

Knowledge-driven..... دانش محور

## L

Latitude ..... عرض جغرافیایی

Logical reasoning..... استدلال منطقی

Longitude ..... طول جغرافیایی

## M

Machine learning ..... یادگیری ماشین

Mapping ..... نگاشت

Markov login network..... شبکه منطق مارکوف

Metadata ..... فراداده

Meta-level ..... فراسطح

Multi-layer..... شبکه عصبی پرسپترون چندلایه

perceptron neural network

## N

Naive bayes ..... بیز ساده

Natural Language Processing پردازش زبان طبیعی

Nearest neighbor ..... نزدیکترین همسایه

Neural network..... شبکه عصبی

## O

Online..... برخط

Ontology ..... هستی‌شناسی

## P

Privacy ..... حریم خصوصی

## R

Randomization..... آشفته‌سازی

Randomizing factors ..... عوامل تصادفی‌ساز

Recognition..... شناسایی

Relations ..... روابط

Replacement..... جابجایی

Rules..... قواعد

## S

Safety ..... امنیت

Search engine..... موتور جستجو

Semantic web ..... وب معنایی

Semantics..... معناشناسی

Semi-supervised learning.... یادگیری نیمه‌نظارتی

Sensitive information..... اطلاعات حساس

Sensor ..... حسگر

Side channel attack..... حمله کانال جانبی

## T



## U

**Abstract**

...

**Keywords**: Internet of Things, Privacy, Smart Home, Ontology, IoT Platform

Sharif University of Technology

Department of Computer Engineering

M.Sc. Thesis

# Ontology based Fake User Behavior Generation for Privacy Preservation in Smart Home

By:

**Behzad Dara**

Supervisor:

**Dr. Morteza Amini**

December 2023