دانشکده مهندسی کامپیوتر

پیشنهاد پژوهشی دکتری مهندسی کامپیوتر (گرایش نرم‌افزار)

حفظ حریم خصوصی در سکوهای اینترنت اشیاء

Privacy on IoT platforms

دانشجو: محمود اقوامی‌پناه

استاد راهنما: دکتر مرتضی امینی

بهمن‌ماه ۱۳۹۹

چکیده

سکوهای اینترنت اشیاء به کاربران کمک می‌کنند تا با اتصال دستگاه‌های هوشمند و سرویس‌های برخط به یکدیگر، فرآیند خودکارسازی محیط را اجرا نمایند. این سکوها از مدل سه‌گانه‌ی «رهانا-محاسبه-کنش» برای اجرای برنامه‌های خودکارسازی بهره می‌برند. متمرکز بودن این سکوها، موجب می‌شود، در مدل تهدیدِ سکوی بدخواه اینترنت اشیاء و یا سکویی که مورد حمله مهاجمین واقع شده، نقض حریم خصوصی کاربران صورت پذیرد.

با بررسی سکوهای اینترنت اشیاء کنونی، داده‌های ارسالی به سکوها را می‌توان در سه دسته‌ی داده‌های عمومی، داده‌های حساس، و داده‌های حساس به زمان تقسیم نمود. نشت داده‌های حساسِ کاربر نظیر موقعیت مکانی، ساعات حضور در خانه و فعالیت‌های دستگاه‌های موجود در خانه، منجر به نقض حریم‌خصوصی کاربر می‌گردد. از سویی دیگر درمورد داده‌های حساس به زمان، اطلاع سکو از زمان رخ دادن یا عدم رخداد رهانای مرتبط با این داده‌ها، امکان تحلیل آماری و ساخت پروفایل رفتاری کاربر را به سکوی بدخواه می‌دهد که می‌تواند موجب نقض حریم‌خصوصی گردد. در مسیر این پژوهش، به بررسی الگوهای نقض حریم‌خصوصی و اصل حداقل دسترسی در سکوهای اینترنت اشیاء با معماری‌های متفاوت پرداخته‌ایم. ریزدانه نبودن دریافت اطلاعات از حسگرها و داده‌های غیرصادق در شرایط برنامه، دو نمونه از الگوی نقض حریم‌خصوصی است که در سکوهای متفاوت اینترنت اشیاء دیده می‌شود.

مسئله پژوهشی مدنظر در این پیشنهاد، حفظ حریم‌خصوصی کاربران در سکوهای اینترنت اشیاء در عین حفظ کاربردپذیری آن‌هاست. رویکرد پیشنهادی در این پژوهش برای حل این مسئله، مبتنی بر این ایده است که کد برنامه‌های اینترنت اشیاء، می‌تواند مبنای تشخیص داده‌های ارسالی غیرضروری به سکو و انتخاب سازوکار حریم‌خصوصی، متناسب با عملگرهای محاسباتی و داده‌های ارسالی به سکو باشد. برای حفظ حریم‌خصوصی رهاناهای حساس به زمان نیز استفاده از مدل k-گمنامی پیشنهاد گردید. در این مدل با تجمیع داده‌های یک کاربر با k کاربر دیگر، سعی داریم تا مانع از تحلیل آماری رهاناهای حساس به زمان برای سکوی اینترنت اشیاء بدخواه گردیم.

کلمه‌های کلیدی: سکوی اینترنت اشیاء، حریم خصوصی، k-گمنامی، برنامه‌ی اینترنت اشیاء

فهرست مطالب

فهرست اشکال

فهرست جداول

فصل اول

مقدمه

در سال‌های اخیر استفاده از فناوری اینترنت اشیاء با هدف هوشمندسازی محیط‌های مختلف، گسترش یافته است. با گسترش این فناوری در حوزه‌ی خانه‌های هوشمند، سکوهای اینترنت اشیاء[۱] با استقبال قابل توجهی توسط کاربران مواجه شده‌اند. از سویی دیگر سکوهای اینترنت اشیاء به طور مستقیم به داده‌های حساس کاربران دسترسی دارند و این امر می‌تواند موجب نقض حریم خصوصی کاربر گردد. در این بخش در ابتدا مسئله‌ی پژوهشی شرح داده می شود، سپس ساختار مطالب در این نوشتار بیان می‌گردد.

۱-۱ شرح مسئله

امروزه سامانه‌های اینترنت اشیاء درکاربردهای مختلفی مورد استفاده قرار می‌گیرند. خانه‌های هوشمند، دانشگاه هوشمند ، شهر هوشمند و اینترنت اشیاء صنعتی، مواردی از کاربردهای این حوزه هستند. بنابر پیش‌بینی آماری [۱] تا سال ۲۰۲۵ بیش از ۷۵ میلیارد دستگاه اینترنت اشیاء متصل در تمام جهان وجود خواهد داشت. در کنار گسترش محیط‌های اینترنت اشیاء، دغدغه‌های جدی در زمینه‌ی امنیت و حفظ حریم خصوصی این محیط‌ها وجود دارد. محیط‌های اینترنت اشیاء به دستگاه‌هایی دسترسی دارند که قابلیت تغییر در محیط‌های فیزیکی اطراف را دارا هستند؛ سوءاستفاده و یا خطا در استفاده از این دستگاه‌ها می‌تواند منجر به نقض خط‌مشی‌های ایمنی و امنیت محیط شود. برای نمونه بازکردن درب هوشمند در زمانی که کاربر در خانه نیست می‌تواند موجب نقض ایمنی و سرقت از کاربر گردد. برخی از پژوهش‌ها به تحلیل خط‌مشی‌های امنیت و ایمنی در اینترنت اشیاء پرداخته‌اند[۲۲] [۲۴] [۲۶]. از سویی دیگر داده‌های حساسی که در اختیار سکوها و برنامه‌های اینترنت اشیاء قرار می‌گیرد قابلیت نقض حریم خصوصی را برای مهاجمین ایجاد می‌نماید. تعدادی دیگر از پژوهش‌ها به بررسی جریان اطلاعات و حفظ حریم خصوصی در برنامه‌های اینترنت اشیاء پرداخته‌اند[۲۳] [۲۵].

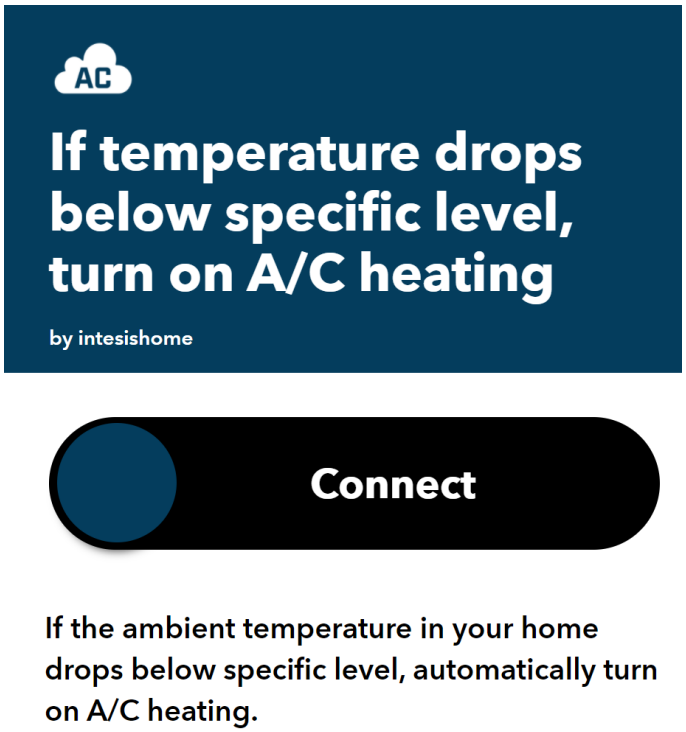
سکوهای اینترنت اشیاء مبتنی بر رهانا-کنش (TAP)[۲] نظیر IFTTT[۴] [۱]، زپیر[۵] [۲]، اسمارت‌تینگز[۷] [۳] در سال‌های اخیر توجهات ویژه‌ای را به خود جلب نموده‌اند. این سکوها با اتصال دستگاه‌های اینترنت اشیاء و سرویس‌های برخط به یکدیگر، امکان توسعه و اجرای قاعده‌های خودکارسازی[۸] را برای کاربران ایجاد نموده‌اند.

---

۱ IoT Platforms
۲ Trigger-Action Platform (TAP)
۴ If This Then That
۵ Zapier
۷ SmartThings
۸ Automation Rules

منظور از قاعده‌های خودکارسازی برنامه‌هایی است که مبتنی بر دستگاه‌های فیزیکی موجود کاربر در یک محیط اینترنت اشیاء (نظیر حسگر دما، حسگر تشخیص حرکت و درب هوشمند) و سرویس‌های برخط مورد استفاده‌ی کاربر (نظیر ایمیل و گوگل درایو[۹])، یک خدمت خودکارسازی را ارائه می‌دهند. این برنامه‌ها از یک مدل سه‌گانه‌ی «رهانا-محاسبه-کنش» استفاده می‌نمایند و درصورت رخدادن یک رهانا مشخص، با اجرای یک محاسبه‌ی مشخص، کنش موردنظر کاربر را تولید نموده و به دستگاه یا سرویس موردنظر برای کنش ارسال می‌کنند.

به عنوان نمونه‌ی ساده‌ای از این برنامه‌ها، می‌توان به برنامه‌ی «روشن نمودن تهویه‌ی هوا» اشاره نمود. شکل ۱ توصیف متنی این برنامه را در سکوی IFTTT نشان می‌دهد.

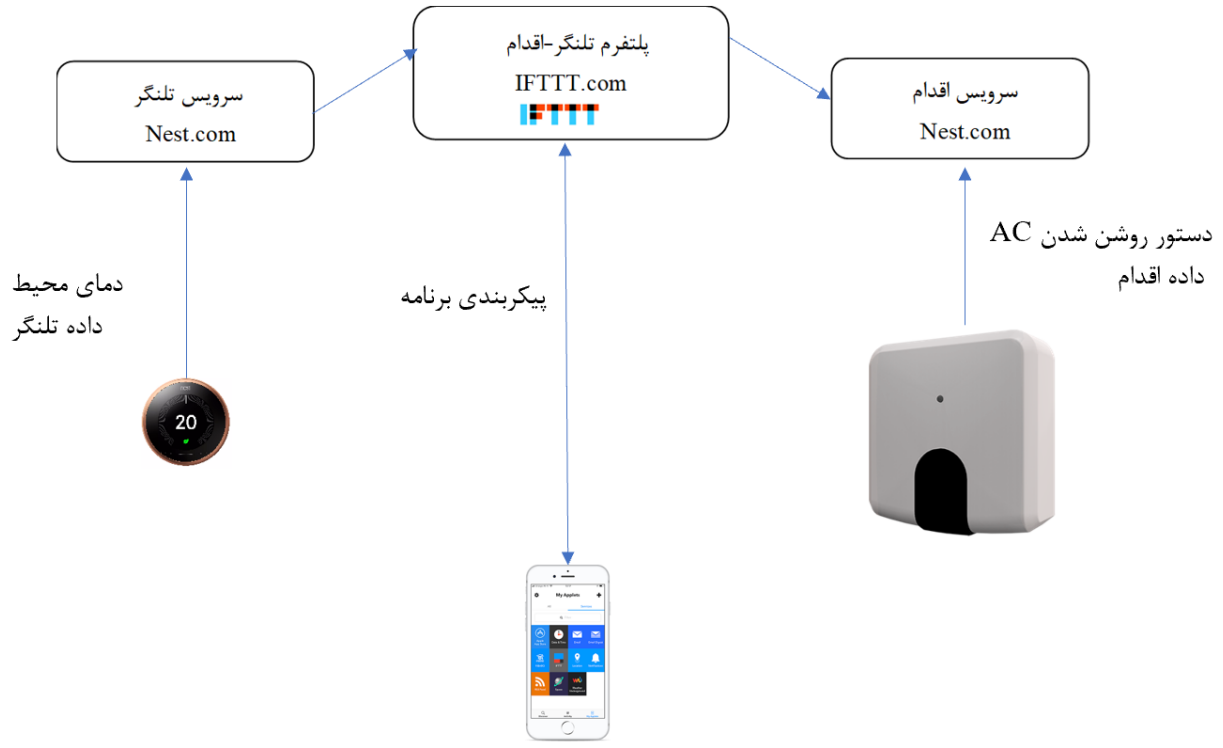


شکل ۱-توصیف برنامه روشن‌نمودن تهویه‌ی هوا در سکوی IFTTT

در این برنامه، سرویس مرتبط با حسگر دما (سرویس رهانا[۱۰]) دمای محیط را برای سکوی اینترنت اشیاء ارسال می‌کند (رهانا) و در صورت آن که دمای محیط بالاتر از مقدار معینی باشد (محاسبه)، با ارسال دستور به سرویس برخط تهویه‌ی هوا (سرویس کنش[۱۱]) دستگاه تهویه‌ی هوا را روشن می‌نماید (کنش). شکل ۲ معماری

[۹] Google Drive
[۱۰] Trigger Service
[۱۱] Action Service

کلی از این برنامه‌ی اینترنت اشیاء را در سکوی IFTTT نشان می‌دهد و جایگاه هر یک از موجودیت‌های سرویس رهانا، سکوی رهانا-کنش و سرویس کنش را مشخص می‌نماید. همان‌طور که در شکل ۲ قابل مشاهده است، سکوهای اینترنت اشیاء واسط کاربری موبایل یا وب را نیز برای ارتباط با کاربر دارند که کاربر با استفاده از آن به توسعه و تنظیم برنامه‌های اینترنت اشیاء خود می‌پردازد.



شکل ۲- معماری برنامه‌ی ساده‌ی «بازنمودن پنجره هوشمند» در سکوی IFTTT

در حال حاضر سکوهای محبوب TAP نظیر IFTTT بیش از بیست میلیون کاربر فعال و دویست‌هزار توسعه‌دهنده دارند که ماهیانه بیش از یک میلیارد برنامه خودکارسازی را با استفاده از سکوی IFTTT اجرا می‌نمایند[۴].

اگرچه سکوهای TAP فرآیند خودکارسازی و تعامل دستگاه‌های اینترنت اشیاء با یکدیگر را آسان ساخته‌اند اما دسترسی کاملی به داده‌های حساس کاربر و توکن‌ها[۱۲]ی مرتبط با سرویس‌های برخط کاربر دارند. به عنوان نمونه سکوی IFTTT می‌تواند به داده‌های حساس کاربر نظیر موقعیت مکانی، عکس‌ها، دستورات صوتی

[۱۲] منظور از توکن، Access Tokenهای کاربر است.

کاربر[۱۳]، اطلاعات سلامتی[۱۴]، فایل‌ها، وضعیت فعلی محیط زندگی نظیر حضور یا عدم حضور افراد در خانه، دما و میزان روشنایی خانه و موارد دیگر دسترسی یابد[۵].

از سویی دیگر، الگوی آماری رخداد داده‌های حساس به زمان کاربر که در اختیار سکوهای اینترنت اشیاء قرار می‌گیرد می‌تواند اطلاعات حساس و مهمی را ناخواسته به سکو منتقل نماید. درواقع سکو می‌تواند با استفاده از رهاناهای دریافتی و کنش‌های ارسالی به محیط اینترنت اشیاء، الگوی رفتاری دقیقی از کاربر را استخراج نماید. برای نمونه یک سکوی اینترنت اشیاء می‌تواند تنها با بررسی آماری ساده‌ی زمان رهاناهای ورودی از حسگرهای یک محیط، روال‌های زندگی یک کاربر(نظیر زمان ورود و خروج از خانه، زمان سفر) و فعالیت‌های فیزیکی صورت گرفته در محیط خانه (نظیر روال تهویه‌ی هوا، روال استحمام اعضای خانه با استفاده از حسگر رطوبت) را استخراج نماید.

از همین رو سکوهای TAP، هدف بسیار جذابی برای هکرها و مهاجمین سایبری هستند. یک مهاجم سایبری به جای آن که سرویس‌های مختلف یک کاربر را هک نماید، می‌تواند با نفوذ به سکوی اینترنت اشیاء کاربر، تمامی داده‌های حساس سرویس‌های مختلف و توکن‌های دسترسی این سرویس‌ها را به طور یک‌جا در اختیار بگیرد. پیش از این نمونه‌هایی از نشت داده‌ی کاربران در سامانه‌های متمرکز و یا نشت داده‌ی ناشی از خطا در سامانه‌های اینترنت اشیاء رخ داده است[۲۰][۷]. در همین راستا سال گذشته جیمیل[۱۵] به دلیل مشکلات و نگرانی‌های امنیتی و حریم خصوصی، دسترسی API خود را محدود نمود و سکوی IFTTT نیز برخی از رهاناها و کنش‌های مرتبط با جیمیل را از دست داد [۸].

از سویی دیگر در خط‌مشی حریم خصوصی سکوهای تجاری نظیر IFTTT به طور واضح ذکر شده است که داده‌های حساس کاربران از سرویس‌های مختلف جمع‌آوری می‌شود و این سکوها برای هرکاربر پروفایل شخصی را می‌سازند. براساس خط مشی حریم خصوصی موجود، این سکوها اجازه دارند تا داده‌های کاربر را با شرکت‌های شخص ثالث به دلخواه به اشتراک بگذارند[۵]. در خط‌مشی حریم خصوصی سکوی اسمارت‌تینگز نیز به طور واضح ذکر شده است که داده‌ها و پروفایل شخصی کاربران به شرکت‌های تبلیغاتی فروخته می‌شود و ممکن است کاربر، تبلیغات هدفمند براساس داده‌های شخصی خود را در سایت‌های دیگر نظیر خبرگزاری‌ها ببیند[۶].

[۱۳] دستورات صوتی که برای دستیارهای صوتی ارسال می‌شود.

[۱۴] اطلاعاتی که از حسگرهای سلامتی و مچ‌بندهای هوشمند جمع‌آوری می‌گردد، نظیر ساعت خواب کاربر.

[۱۵] Gmail

پیش از این نیز اخبار متعددی در زمینه‌ی تبلیغات هدفمند با استفاده از داده‌های حساس کاربران در سکوهای اینترنت اشیاء منتشر شده بود. برای نمونه در سال ۲۰۱۸ خبری در مورد دستگاه دستیار صوتی آمازون[۱۶] منتشر شد که نشان می‌داد آمازون با دریافت مبالغ مالی از شرکت‌های مختلف، تبلیغات هدفمند را متناسب با پروفایل کاربر صورت می‌دهد[۱۸]. هم‌چنین اخباری در زمینه نظارت و جرم‌یابی دیجیتال با استفاده از داده‌های دستگاه‌های اینترنت اشیاء نظیر مچ‌بند هوشمند دیده می‌شود[۱۹]. ما در این پژوهش به بررسی الگوهای نقض حریم‌خصوصی و اصل حداقل دسترسی در سکوهای اینترنت اشیاء پرداخته‌ایم. ریزدانه نبودن دریافت اطلاعات از حسگرها و داده‌های غیرصادق در شرایط برنامه دو نمونه از الگوی نقض حریم‌خصوصی است که در سکوهای متفاوت اینترنت اشیاء دیده می‌شود.

۱-۲ هدف پژوهش

در این پژوهش مسئله‌ی مورد بررسی ما، حفظ حریم خصوصی در سکوهای اینترنت اشیاء است. به طور معمول همواره یک مصالحه بین حفظ حریم خصوصی و استفاده از کاربردپذیری[۱۷] وجود دارد. ما در این پژوهش سعی داریم تا حفظ حریم‌خصوصی سکوهای اینترنت اشیاء را تضمین نماییم در عین حال کاربردپذیری سکوهای اینترنت اشیاء با مخاطره مواجه نشود و برنامه‌های خودکارسازی کاربران با صحت کامل قابل اجرا باشد. در فصل چهارم به طور دقیق مدل تهدید را مطرح می‌نماییم.

ایده پیشنهادی ما در این پژوهش، استفاده از کد برنامه‌های اینترنت اشیاء برای جلوگیری از ارسال داده‌های غیرضروری حساس به سکو و انتخاب سازوکار[۱۸] حریم‌خصوصی است. راه‌کار ما برای حفظ حریم‌خصوصی داده‌های حساس به زمان نیز استفاده از مدل k-گمنامی است تا امکان تحلیل آماری زمان رخداد رهاناهای حساس به زمان برای سکو ممکن نباشد.

۱-۳ ساختار مطالب پیشنهاد رساله

ساختار مطالب پیشنهاد رساله به این شرح است. در فصل دوم پیش‌زمینه‌ی لازم در حوزه‌ی اینترنت اشیاء برای طرح مسئله‌ی پژوهشی شرح داده می‌شود و مفاهیم پایه در مورد حریم خصوصی بیان می‌گردد. سپس در فصل

[۱۶] Amazon
[۱۷] Utility
[۱۸] Mechanism

سوم کارهای پژوهشی پیشین مورد بررسی قرار می‌گیرد. فرضیات، مدل تهدید و نقاط قوت و ضعف هر یک از کارهای پژوهشی در این بخش مطرح می‌گردد. در فصل چهارم با جزئیات و به طور دقیق به بیان پیشنهاد پژوهشی پرداخته‌ایم. در این فصل فرضیات، مدل تهدید و راه‌کارهای پیشنهادی اولیه برای حل مسئله را مورد بررسی قرار داده‌ایم و در نهایت در فصل ششم به جمع‌بندی این گزارش و ارایه زمانبندی فعالیت‌های آتی جهت تکمیل این پژوهش پرداخته‌ایم.

فصل دوم

پیش‌زمینه

پیش از پرداختن به موضوع حریم خصوصی در سکوهای اینترنت اشیاء، لازم است معرفی دقیقتری از این سکوها، برنامه‌های اینترنت اشیاء و معماری‌های مختلف این سکوها داشته باشیم. مفهوم حریم خصوصی نیز مفهومی قدیمی در حوزه امنیت فضای تبادل اطلاعات است که تعاریف و سازوکارهای عملیاتی مختلفی برای آن ارایه شده است. لذا لازم است مروری بر این مفهوم و شیوه‌های برقراری آن نیز پیش از پرداختن به موضوع اصلی این پژوهش داشته باشیم.

۲-۱ سکو و برنامه‌ی اینترنت اشیاء

سکوی اینترنت اشیاء[۱]، زیرساختی را فراهم می‌آورد تا برنامه‌های اینترنت اشیاء[۲] بر روی آن توسعه یابند و اجرا شوند. تا پایان سال ۲۰۱۹ میلادی تعداد سکوهای اینترنت اشیاء عرضه شده در سراسر دنیا بیش از ۶۰۰ مورد بوده است[۲۷]. در جدول ۱-۲، پنج سکوی اینترنت اشیاء خانه‌ی هوشمند و سه سکوی خودکارسازی وظیفه[۳] و ویژگی‌های آن‌ها مورد بررسی قرار گرفته است[۴۰].

جدول ۱-۲- سکوهای اینترنت اشیاء خانه‌ی هوشمند و ویژگی‌های آن‌ها[۴۰]

ردیف	سکو	پشتیبانی از محاسبه	کنش چندتایی	استفاده از داده‌ی رهانا
۱	اسمارت تینگز [۳]	✓	✓	✓
۲	IFTTT [۱]	✓	✓	✓
۳	اُپن‌هب[۴۲]	✓	✓	✓
۴	مایکروسافت پاور اتومیت[۴] [۳۰]	✓	✓	✓
۵	زپیر [۲]	×	✓	✓
۶	هوم‌کیت[۵] [۴۳]	×	×	×
۷	ایریس[۶] [۴۵]	×	×	×
۸	وینک[۷] [۴۴]	×	×	×

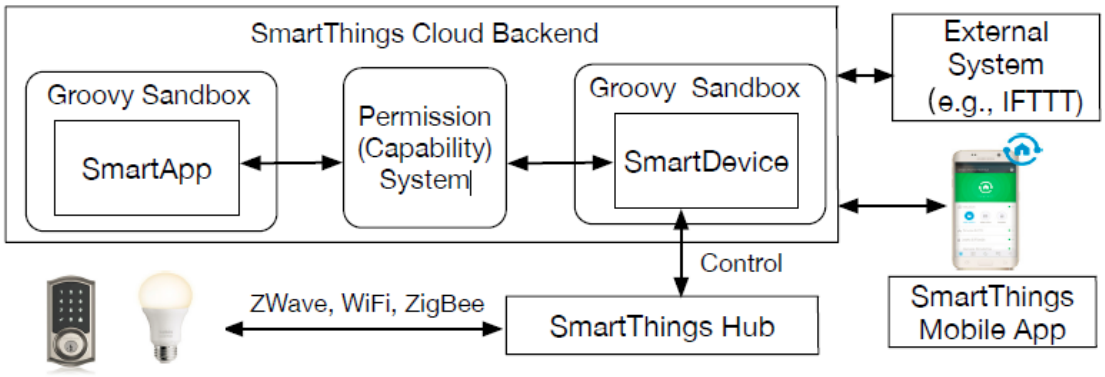
[۱] IoT platform
[۲] IoT applications
[۳] Task automation platform
[۴] Microsoft Power Automate
[۵] HomeKit
[۶] Iris
[۷] Wink

ویژگی اول پشتیبانی از محاسبه است که به توانایی سکو برای اجرای عملیات محاسباتی برروی داده‌های دریافتی از رهانا اشـاره دارد. ویژگی دوم کنش چندتایی اسـت. در برخی از سـکوها قابلیت تعریف برنامه‌هایی با چند کنش در ازای رخداد یک رهانای مشخص وجود دارد. ویژگی سوم استفاده از داده‌ی رهانا است، سکوهایی که این ویژگی را ندارند، صرفا قادر هستند برنامه‌ها را بدون ارتباط رهانا و کنش اجرا نمایند.

سکوهای اینترنت اشیاء مختلف، در معماری، واسط برنامه نویسی و ویژگی‌های مورد پشتیبانی متفاوت هستند، اما غالب آن‌ها از مدل سه‌گانه «رهانا-محاسبه-کنش» بهره می‌برند. در ادامه به عنوان نمونه، دو سکوی اسمارت‌تینگز و IFTTT و برنامه‌های آن‌ها به طور اجمالی معرفی و مورد برررسی قرار گرفته‌اند. این دو سکو، سکوهایی با تعداد قابل توجه کاربر و سکوهای رایج در پژوهش‌های این حوزه هستند.

۲-۱-۱ سکوی اسمارت‌تینگز

سکوی اینترنت اشیاء اسمارت‌تینگز، سکویی است که از سال ۲۰۱۴ مورد پیشتیبانی شرکت سامسونگ قرار گرفته است. مطابق شکل ۳، شش جزء در معماری سکوی وجود دارد[۲۸]:



شکل ۳- معماری سکوی اسمارت‌تینگز [۲۸]

۱. دستگاه‌های اینترنت اشیاء

این دستگاه‌ها حسگرها و عملگرهای[۱۲] موجود در محیط اینترنت اشیاء هستند.

[۱۲] Actuator

۲. هاب اینترنت اشیاء[۱۳]

هاب اینترنت اشـــیاء ارتباط دســـتگاه‌های اینترنت اشـــیاء موجود در محیط را با زیرســـاخت ابری برقرار می‌کند.

۳. زیرساخت ابری سکو

زیرساخت ابری سکو تمامی داده‌های محیط را جمع‌آوری نموده و پردازش‌های مربوط به برنامه‌های اینترنت اشیاء بر بستر آن صورت می‌پذیرد.

۴. برنامه‌های اسمارت‌اپ[۱۴]

برنامه‌های اسمارت‌اپ که یا توسط کاربر توسعه می‌یابد و یا از میان برنامه‌های شخص ثالث نصب می‌گردد. این برنامه‌ها در عمل، فرآیند کنترل محیط و خودکارسازی را برنامه‌ریزی می‌کنند.

۵. سرویس‌های خارج از محیط

سـرویس‌های برخط خارج از محیط اینترنت اشـیاء نظیر سـرویس آب و هوا که اطلاعاتی را به عنوان ورودی برای برنامه‌های اینترنت اشیاء ارائه می‌دهند.

۶. برنامه‌ی موبایلی سکو

برنامه‌ی موبایلی سکو که قابلیت توسعه، نصب و یا حذف برنامه‌های اینترنت اشیاء را ممکن می‌سازد.

برنامه‌های اینترنت اشـــیاء در این ســـکو، اســـمارت‌اپ نامیده می‌شـــوند. این برنامه‌ها به زبان گرووی[۱۵][۱۸] توسـعه می‌یابند و در زیرسـاخت ابری اسـمارت‌تینگز در محیط آزمون کوشـکه[۱۶][۱۹] که مربوط به زبان گرووی است اجرا می‌شوند. گرووی یک زبان برنامه‌نویسی شی‌گرا و پویا با نحو[۱۷] مشابه جاوا است. محیط آزمون کوشکه نیز یک محیط اجرایی محافظت شده را ایجاد می‌کند که صرفاً اجرای متدهای از پیش تعیین شده[۱۸] در آن مجاز

---

[۱۳] IoT Hub
[۱۴] Smartapp
[۱۵] Groovy
[۱۶] Kohsuke Sandbox
[۱۷] Syntax
[۱۸] Whitelist methods

است. مطابق شکل ۳ زیرساخت ابری سکو، برنامه‌هایی با عنوان اسمارت‌دیوایس[۱۹] را نیز درنظر می‌گیرد؛ این برنامه‌ها درواقع معادل نرم‌افزاری و انتزاعی دستگاه‌های موجود در محیط اینترنت اشیاء هستند. ارتباط یک برنامه با یک اسمارت‌دیوایس به دو صورت مقدور می‌باشد:

۱- یک برنامه کنشی را بر روی یک اسمارت‌دیوایس اجرا می‌کند که با فراخوانی متدهای آن اسمارت‌دیوایس صورت می‌پذیرد. این کنش در واقع کنشی است که بر روی محیط فیزیکی تاثیر می‌گذارد. به عنوان نمونه یک برنامه، کنش روشن شدن دستگاه تهویه‌ی هوا را با فراخوانی متد مربوط به آن صورت می‌دهد که منجر به تغییر هوای محیط فیزیکی خواهد شد.

۲- یک برنامه منتظر می‌ماند تا رخداد مشخصی از سوی یک اسمارت‌دیوایس اتفاق بیفتد. به عنوان نمونه برنامه‌ای را درنظر بگیرید که منتظر می‌ماند تا رخداد ورود یک فرد به خانه را توسط اسمارت‌دیوایس مربوط به حسگر تشخیص حرکت[۲۰] دریافت نماید.

در زمان نصب این برنامه نیز دستگاه مربوط در محیط برای هر برنامه توسط کاربر تعیین می‌گردد. دستگاه‌های اینترنت اشیاء، توانمندی‌های[۲۱] متفاوتی دارند؛ این توانمندی‌ها شامل کنش‌های قابل انجام و رخدادهای مربوط به دستگاه است. کنش‌های، اعمالی هستند که با استفاده از آن دستگاه کنترل می‌گردد و در محیط فیزیکی تغییر ایجاد می‌شود. رخدادها نیز در زمان تغییر وضعیت دستگاه فعال می‌شوند. به یک رخداد فعال‌شده رهانا می‌گوییم.

درشکل ۴ نمونه‌ای از یک برنامه‌ی اینترنت اشیاء در سکوی اسمارت‌تینگز دیده می‌شود. در بخش اول این برنامه موارد عمومی شامل نام برنامه، نویسنده‌ی برنامه و توصیف برنامه دیده می‌شود.

به طور کلی برنامه‌های اسمارت‌اپ، یک یا چند رخداد را مشترک[۲۲] می‌شوند، به این معنا که به ازای هر رهانا از این رخدادها، یک تابع رخداد[۲۳] را اجرا می‌کنند. در این جا برنامه‌ی موجود در شکل ۴ رویداد motion.active را مشترک شده است. motion.active زمانی رخ می‌دهد که حسگر حرکت، حرکت شیئ را تشخیص دهد. تابع رخداد مربوط به رخداد motion.active در این مثال motionDetectedHandle می‌باشد، که

---

[۱۹] SmartDevices

[۲۰] Motion detector

[۲۱] Capability

[۲۲] Subscribe

[۲۳] Event handeler

به ازای رهانای ورودی motion.active، سوئیچ مربوطه را روشن می‌نماید. دقت نمایید که دستگاه‌های مرتبط با برنامه در بخش preferences آمده است و توسط کاربر در زمان نصب انتخاب می‌شوند.

```
definition(
name: "MyFirstApp",
namespace: "mahmoudaghvami",
author: "Mahmoud Aghvami",
description: "Turn on light when motion detected",
category: "My Apps",
preferences {
        section("Turn on when motion detected:") {
                input "themotion", "capability.motionSensor", required: true, title: "Where?"
        }
        section("Turn on this light") {
                input "theswitch", "capability.switch", required: true
        }
}
def installed() {
        log.debug "Installed with settings: ${settings}"
        initialize()
}
def updated() {
        log.debug "Updated with settings: ${settings}"
        unsubscribe()
        initialize()
}
def initialize() {
subscribe(themotion, "motion.active", motionDetectedHandler)
}
def motionDetectedHandler(evt) {
log.debug "motionDetectedHandler called: $evt"
theswitch.on()
 }
```

شکل ۴ - نمونه کد برنامه‌ی اسمارت‌اپ

۲-۱-۲ سکوی IFTTT

سکوی IFTTT یکی از پرطرفدارترین سکوهای اینترنت اشیاء است که تعامل بین سرویس‌های برخط نظیر تقویم گوگل[۲۴] و اینستاگرام را با سرویس‌های برخط مربوط به دستگاه‌های اینترنت اشیاء نظیر ترموستات و حسگر حرکت برقرار می‌سازد. در شکل ۲ معماری کلی سکوی IFTTT را مشاهده کردیم. در این بخش جزئیات بیش‌تری از نحوه‌ی کارکرد سکوی IFTTT را مورد بررسی قرار می‌دهیم.

[۲۴] Google calender

سکوی IFTTT به طور کلی شامل پنج جزء است: سکو، سرویس رهانا، سرویس کنش، برنامه‌ی[۲۵] اینترنت اشیاء، برنامه‌ی موبایلی IFTTT. هر یک از سرویس‌های موجود در IFTTT (سرویس رهانا یا سرویس کنش) می‌توانند سرویس‌های برخط مرتبط با یک دستگاه اینترنت اشیاء نظیر سرویس برخط مچ‌بند هوشمند شیائومی[۲۶] و یا سرویس‌های کاملاً بر پایه‌ی وب نظیر سرویس اطلاع‌رسانی آب و هوا، تقویم گوگل، جیمیل و اینستاگرام باشند. این سرویس‌ها اطلاعات کاربر را در بر دارند و می‌توانند این اطلاعات را با استفاده از یک RESTful API در اختیار دیگر سرویس‌ها بگذارند. برای نمونه سرویس برخط ترموستات نِست[۲۷] می‌تواند دمای محیط را در اختیار دیگر سرویس‌ها قرار دهد. درعین حال جیمیل نیز می‌تواند امکان خواندن ایمیل‌های کاربر را برای سرویس‌های دیگر فراهم کند.

در حال حاضر سکوی IFTTT به طور متمرکز فعال است و قابلیت تعامل را بین API سرویس‌های مختلف فراهم می‌نماید. هم‌اکنون بیش از ۶۰۰ سرویس در IFTTT تعریف شده است [۴].

برنامه‌های اینترنت اشیاء در IFTTT برای تعامل بین سرویس‌ها طراحی شده است. سکوی IFTTT از یک ساختار «رهانا-محاسبه-کنش» بهره می‌برد و دو سرویس مختلف را در قالب یک برنامه به یکدیگر متصل می‌کند. درواقع هر برنامه‌ی IFTTT سعی دارد تا یک روال خودکارسازی را اجرا نماید. این کار در قالب اتصال دو سرویس به یکدیگر صورت می‌گیرد. در زمان تعریف یک برنامه IFTTT، یک سرویس به عنوان سرویس رهانا و سرویس دیگر به عنوان سرویس کنش مشخص می‌شود. اطلاعات هر سرویس رهانا شامل جزء[۲۸]های مختلفی است که برخی از آن‌ها به طور مستقیم در برنامه استفاده خواهند شد.

شکل ۵ بخش‌های مختلف را در توسعه یک برنامه IFTTT نشان می‌دهد. برنامه‌ی موجود در شکل ۵ برنامه‌ی روشن نمودن لامپ هوشمند در آزمایشگاه امنیت داده‌ی شریف، ۱۵ دقیقه مانده به زمان جلسه است. با اجرای این برنامه ۱۵ دقیقه قبل از زمان شروع یک رویداد موجود در تقویم گوگل، درصورتی که مکان برگزاری رویداد مذکور آزمایشگاه امنیت داده‌ی شریف[۲۹] و روشنایی طبیعی پایین‌تر از یک حد آستانه باشد، لامپ هوشمند سالن آزمایشگاه روشن می‌شود. در این برنامه سرویس رهانا، تقویم‌گوگل است و به ازای هر رویداد جدید، اطلاعات این رویداد برای سکوی IFTTT ارسال می‌گردد.

---

[۲۵] در سکوی IFTTT، این برنامه applet نامیده می‌شود.

[۲۶] Xiaomi

[۲۷] Nest

[۲۸] Ingredient

[۲۹] Sharif DNSL Lab

در سکوی IFTTT برنامه‌ی نوشته شده توسط کاربر شامل بخشی به نام فیلتر کد[۳۰] است که بر روی زیرساخت ابری IFTTT اجرا می‌گردد. فیلترکد، کدی به زبان تایپ‌اسکریپت[۳۱] [29] است که کاربر آن را در زمان توسعه‌ی برنامه می‌نویسد. فیلتر کد، وظیفه‌ی انجام محاسبه بر روی ورودی‌های رهانا و تبدیل آن‌ها به خروجی مورد نظر برای سرویس کنش را به عهده دارد. متن فیلترکد برنامه‌ی موجود شکل ۵، درشکل ۶ آورده شده است. در شکل ۶ با اجرای فیلترکد برنامه، عملیات محاسبه، در این‌جا عملگر مقایسه و عملگر«String.match» صورت می‌گیرد. به بیان دیگر به ازای رهاناهای ورودی از تقویم گوگل، بررسی می‌گردد که آیا مکان رویداد پیش‌رو « Sharif DNSL Lab» هست یا خیر(خط ۷). درصورت صحیح بودن شرط مکان، با استفاده از داده‌های ارسالی از سرویس تِمپستوِدِر[۳۲] که مربوط به یک حسگر هوشمند محیطی است، میزان روشنایی محیط نیز سنجیده می‌شود. (خط ۸) درصورتی که محیط به اندازه‌ی کافی روشن نباشد، ۱۵ دقیقه قبل از شروع جلسه در آزمایشگاه، خروجی متناسب برای سرویس کنش که در این‌جا سرویس برخط لامپ هوشمند است، تولید می‌گردد و لامپ مذکور روشن می‌شود.

در فرآیند توسعه‌ی برنامه IFTTT، کاربر می‌بایست سرویس رهانا و کنش را مشخص نماید و اطلاعات هویتی مورد نظر برای اتصال به این سرویس‌ها را در اختیار IFTTT بگذارد. پس از آن سکو با دریافت توکن‌های دسترسی سرویس‌ها بدون نیاز به اجازه‌ی مجدد از کاربر، اطلاعات سرویس‌ها را دریافت و یا دستورات لازم را به آن‌ها ارسال می‌نماید.

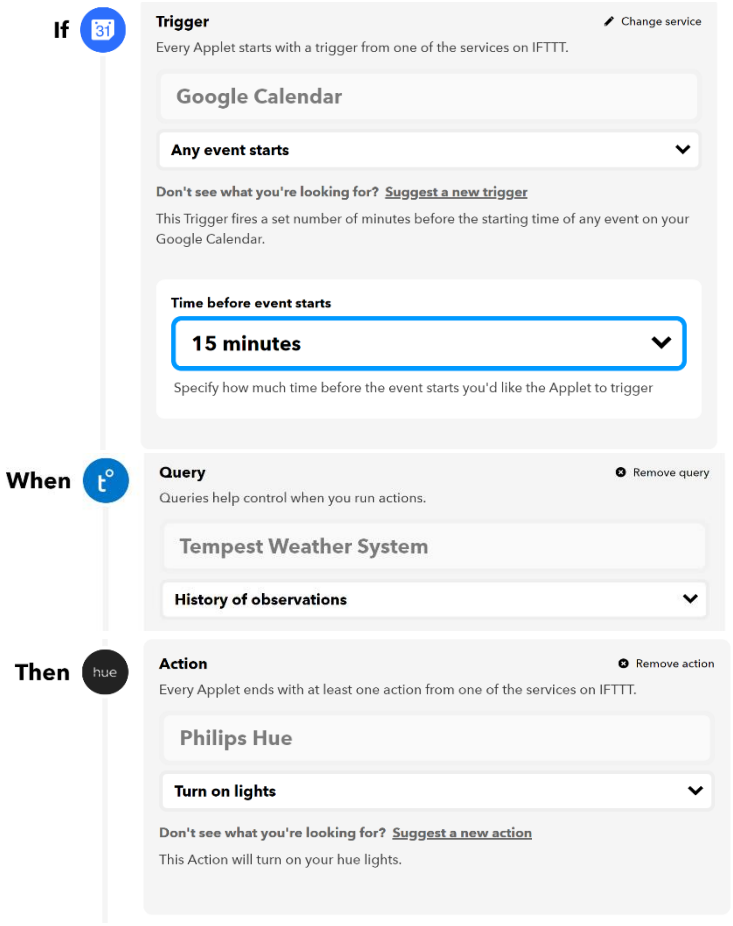
۲-۱-۳ تفاوت در سکوها

اگرچه تقریباً تمامی سکوهای اینترنت اشیاء خانه هوشمند از مدل واحد «رهانا-محاسبه-کنش» پیروی می‌کنند اما تفاوت‌های محسوسی را در معماری و واسط‌های برنامه‌نویسی دارند.

۲-۱-۳-۱ تفاوت در معماری سکوها

یکی از تفاوت‌های قابل توجه در سکوهای مختلف اینترنت اشیاء، تفاوت در معماری این سکوها است. به طور کلی می‌توان دو دسته معماری کلی را برای این سکوها ذکر نمود:

[۳۰] Filter code
[۳۱] TypeScript
[۳۲] Tempest Weather



شکل ۵- بخش‌های مختلف توسعه‌ی برنامه‌ی IFTTT

```
1.  let location = GoogleCalendar.eventFromSearchStarts.Where
2.  let aboveThreshold = 100
3.  let currentLum = Number(Weatherflow.historyOfObservations[0].Brightness)
4.  let meetingTime =GoogleCalendar.eventFromSearchStarts.Starts
5.
6.
7.  if(location.match("Sharif DNSL Lab") == null ||
8.  currentLum > aboveThreshold
9.  )
10. {
11.  Hue.turnOnAllHue.skip()
12. }
```

شکل ۶- فیلتر کد برنامه‌ی IFTTT موجود در شکل ۵

۱- سکوهایی با وجود هاب اینترنت اشیاء

بسیاری از دستگاه‌های اینترنت اشیاء، دارای محدودیت منابع[۳۳] هستند به این معنا که با توجه به طول عمر مورد انتظار برای این دستگاه‌ها، صرفاً از پروتکل‌های ارتباطی مشخص و کم‌مصرفی نظیر ZigBee و Zwawe استفاده می‌کنند. درواقع این دستگاه‌های اینترنت اشیاء، از پروتکل HTTP پشتیبانی نمی‌کنند و زیرساخت ابری پشتیبان ندارند.

برای ارتباط با این دستگاه‌ها، برخی از سکوهای اینترنت اشیاء الزاماً از هاب اینترنت اشیاء بهره می‌برند. برای مثال سکو پرطرفدار اسمارت‌تینگز برای فعالیت الزاماً نیاز به یک هاب اسمارت‌تینگز دارد. البته هاب اسمارت‌تینگز، از پروتکل ارتباط بی‌سیم[۳۴] نیز پشتیبانی می‌نماید. هم‌چنین هاب اسمارت‌تینگز این قابلیت را دارد تا تعداد معدودی از محاسبات و فرآیندهای خودکارسازی را به صورت محلی[۳۵] در خود هاب و نه با ارسال به زیرساخت ابری سکو صورت دهد.

۲- سکوهایی کاملاً مرتبط با سرویس‌های برخط

برخی دیگر از سکوهای اینترنت اشیاء، تنها از تجهیزاتی پشتیبانی می‌نمایند که سرویس ابری برخط داشته باشند. برای نمونه سکوهای IFTTT، زپیر، مایکروسافت‌پاوراتومیت [۲۹] معماری مشابه شکل ۲ دارند. در این معماری سکو الزاماً با سرویس‌های تحت وب رهانا و کنش ارتباط دارد. در صورتی که دستگاهی پروتکل HTTPS را پشتیبانی نکند و زیرساخت ابری نداشته باشد امکان تعریف آن در این سکوها موجود نیست.

۲-۱-۳-۲ تفاوت در زبان برنامه‌نویسی سکوها

زبان برنامه‌نویسی برای سکوهای مختلف اینترنت اشیاء، متفاوت است. همان طور که پیش از این ذکر شد

[۳۳] Resource constrained
[۳۴] Wifi
[۳۵] Local

سکوی اسمارت‌تینگز مبتنی بر زبان برنامه‌نویسی گرووی است. زبان برنامه‌نویسی سکوی IFTTT، زپیر و نود-رِد[۳۶] [۳۱] جاوا اسکریپت است. البته سکوی نود-رِد قابلیت توسعه با استفاده از پایتون[۳۷] را نیز دارد[۳۲].

۲-۲ حریم خصوصی

حریم خصوصی به عنوان «حق یک فرد برای حفظ کنترل و حفظ محرمانگی اطلاعات شخصی خود» تعریف می‌شود [۳۳]. در سال‌های اخیر، با افزایش حجم داده‌های تولیدی، نگرانی‌ها درمورد حفظ حریم خصوصی توسط سکوهای دارنده داده‌های کلان[۳۸] افزایش یافته است. شکل ۷ فرآیند عمومی نگه‌داری و انتشار و تحلیل داده را نشان می‌دهد[۴۶]. به طور معمول در کاربردهای مختلف، سه موجودیت در ارتباط با داده‌ها تعریف می‌شوند:

۱- مالک داده[۳۹]

مالک داده، موجودیتی است که داده ذاتاً متعلق به اوست. در محیط اینترنت اشیاء، داده‌ها توسط حسگرها تولید می‌شوند و این داده‌ها ذاتاً متعلق به کاربر هستند. البته در سکوهای بدون هاب که در بخش ۲-۱-۳-۱ به آن اشاره شد، می‌توان زیرساخت ابری دستگاه‌های اینترنت اشیاء را نیز مالک داده در نظر گرفت.

۲- نگه‌دارنده‌ی داده[۴۰]

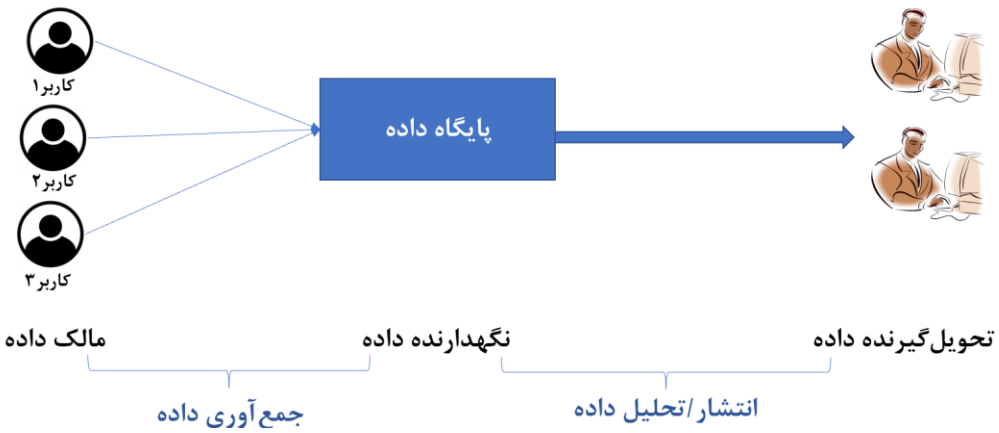
نگه‌دارنده‌ی داده، موجودیتی است که داده‌های مالکین داده را نگه‌داری می‌کند. در محیط اینترنت اشیاء، سکوی اینترنت اشیاء این نقش را دارد. تمامی داده‌های کاربر در سکو جمع‌آوری می‌شوند.

۳- تحویل‌گیرنده‌ی داده[۴۱]

تحویل‌گیرنده‌ی داده موجودیتی است که از داده‌های منتشر شده استفاده می‌کند. در محیط اینترنت اشیاء، سکوی اینترنت اشیاء با اجرای برنامه‌های اینترنت اشیاء از داده‌ها بهره می‌برد. علاوه بر آن منطبق با خط‌مشی حریم خصوصی سکوهای تجاری[۶] [۵] ، سکوها با استفاده از الگوریتم‌های یادگیری ماشین، پروفایل رفتاری کاربر را تشکیل می‌دهند و از آن برای تبلیغات هدفمند یا مقاصد دیگر استفاده می‌نمایند.

---

[۳۶] Node-RED
[۳۷] Python
[۳۸] Big data
[۳۹] Data owner
[۴۰] Data curator
[۴۱] Data recipient



شکل ۷ -حفظ حریم خصوصی در نگهداری و تحلیل اطلاعات

مطابق شکل ۷ دو مرحله‌ی اصلی در فرآیند تحلیل و انتشار داده وجود دارد.

۱- مرحله‌ی جمع‌آوری داده

در این مرحله، اشخاص داده‌های شخصی خود را در پایگاه‌داده قرار می‌دهند.

۲- مرحله‌ی انتشار/تحلیل داده

مرحله‌ی دوم، مرحله‌ی انتشار داده یا تحلیل آن است. در این مرحله، افرادِ تحویل‌گیرنده‌ی داده می‌توانند پرس‌وجوهایی[۴۲] را مطرح نمایند و نگهدارنده‌ی داده پاسخ می‌دهد (تحلیل داده). حالت دیگر آن است که نگهدارنده‌ی داده، کل پایگاه داده را برای تحلیل منتشر می‌کند (انتشار داده).

در دو حالت ممکن است نقض حریم خصوصی صورت گیرد. اگر نگهدارنده‌ی داده، مورد اعتماد نباشد، نقض حریم خصوصی در مرحله‌ی جمع‌آوری داده رخ خواهد داد و اطلاعات شخصی کاربران مستقیماً در اختیار نگهدارنده‌ی داده قرار می‌گیرد. در صورتی که نگه‌دارنده‌ی داده مورد اعتماد باشد، نقض حریم خصوصی ممکن است در مرحله‌ی انتشار داده صورت پذیرد [۴۶]. در این پژوهش فرض ما آن است که در محیط اینترنت اشیاء، سکوی اینترنت اشیاء که نگه‌دارنده‌ی داده است، مورد اعتماد نمی‌باشد.

در سال‌های اخیر روش‌های متعددی برای حفظ حریم‌خصوصی پیشنهاد داده شده است. در زیر دو دسته اصلی از روش‌های حفظ حریم خصوصی و مدل‌های مرتبط با آن‌ها را بررسی می‌نماییم. دسته اول روش‌های مبتنی

[۴۲] Query

بر افراز کاربران به گروه‌های هم‌ارزی است؛ به‌گونه‌ای که اطلاعات یک شخص خاص از میان گروه هم‌ارزی قابل تشخیص نباشد[۴۷]. دسته دوم روش‌ها، مبتنی بر تصادفی‌سازی داده‌ها است. لازم به ذکر است که در محیط اینترنت اشیاء که مورد پژوهش ماست، فرض بر عدم اعتماد به سکوی اینترنت اشیاء است، بنابراین روشهای حفظ حریم‌خصوصی مورد بحث، می‌بایست بین حسگرهای اینترنت اشیاء و سکوی اینترنت اشیاء اعمال گردد.

۲-۲-۱ حفظ حریم‌خصوصی مبتنی بر افراز

به طور کلی در یک جدول داده، چهار نوع ستون داده وجود دارد:

۱- شناسه‌های صریح[۴۳]

شناسه‌هایی که به طور آشکار و صریح منجر به شناسایی فرد می‌شوند.

۲- شبه‌شناسه‌ها[۴۴]

شناسه‌هایی که به تنهایی منجر به شناسایی یک فرد نمی‌شوند اما کنار هم قراردادن این شناسه‌ها و اطلاعات خارجی، منجر به شناسایی یک فرد می‌شود.

۳- ستون داده‌های حساس

ستون‌داده‌هایی که حساس هستند و برای تحویل‌گیرنده‌ی داده نیز کار با این داده‌ها حائز اهمیت است.

۴- ستون داده‌های غیرحساس

در فاز انتشار داده، شناسه‌های صریح حذف می‌شوند و باقی ستون‌ها منتشر می‌شوند. انتشار باقی ستون‌ها موجب می‌شود تا سطرهایی با شبه‌شناسه‌های (QI) یکسان به وجود بیاید. مجموعه‌ی این رکوردها با شبه‌شناسه‌ی یکسان تشکیل کلاس هم‌ارزی[۴۵] می‌دهند.

۲-۲-۱-۱ مدل k-گمنامی

یکی از شناخته‌شده‌ترین مدل‌های حفظ حریم خصوصی مدل k-گمنامی است. به طور ساده این مدل بیان می‌دارد که داده‌های یک شخص نباید از میان یک گروه هم‌ارزی با کم‌تر از k نفر، قابل تشخیص باشد[۴۸]. درواقع حداقل تعداد رکوردها در یک گروه هم‌ارزی می‌بایست k باشد.

---

[۴۳] Explicit identifiers

[۴۴] Quasi identifiers

[۴۵] Equivalence class

k- گمنامی دارای نقاط ضعفی است که بر روی آن حملاتی صورت گرفته است. یکی ازحملات اصلی بر روی k- گمنامی ، حمله همگنی[۴۶] است. این حمله زمانی اتفاق می افتد که ویژگی حساس فاقد تنوع باشد. به این معنا که مقادیر ستون‌های حساس در یک کلاس هم ارزی یکسان باشد.

حمله‌ی دیگر، حمله‌ی پس‌زمینه[۴۷] است. در این حمله با استفاده از اطلاعات پس‌زمینه‌ی افراد، که در جدول اصلی موجود نیست توانایی تشخیص یک فرد از یک کلاس هم‌ارزی فراهم می‌شود [۵۱].

۲-۲-۱-۲ مدل l-تنوع

در راستای مقابله با حمله‌ی همگنی، مدل l-تنوع ارائه شده است. طبق تعریف [۴۹] ، یک جدول خاصیت l-تنوع دارد اگر تمامی کلاس‌های هم‌ارزی آن l-تنوع باشد. یک کلاس هم‌ارزی خاصیت l -تنوع دارد اگر دارای تعداد l مقدار خوش‌نمایش[۴۸] برای هر ستون حساس S باشد.

مفاهیم متعددی برای عبارت «خوش نمایش» به کار می‌رود. برای نمونه:

l-تنوع متمایز[۴۹]: مقادیر حساس متمایز به ازای هر ستون حساس در هر کلاس هم‌ارزی.

l-تنوع آنتروپی[۵۰]: یک مقدار حساس در یک کلاس هم‌ارزی حداکثر $1/l$ بار تکرار شده باشد.

۲-۲-۱-۳ مدل t-نزدیکی

در پژوهش[۵۰] ، مدل t -نزدیکی ارائه شده است. در این مدل به یک کلاس هم‌ارزی دارای t -نزدیکی گفته می‌شود اگر توزیع احتمال مقادیر حساس در آن کلاس با توزیع احتمال مقادیر حساس در کل جدول حداکثر به اندازه t فاصله داشته باشد. یک جدول دارای t-نزدیکی است اگر تمام کلاس‌های هم‌ارزی آن t -نزدیکی باشند.

هر جدول با ویژگی t-نزدیکی، شامل ویژگی k-گمنامی و l-تنوع نیز هست. پارامترt درواقع نشان دهنده‌ی مصالحه‌ی بین حریم خصوصی و سودمندی است. ایده‌ی اصلی t -نزدیکی میزان اطلاع کسب‌شده[۵۱] است. میزان

---

[۴۶] Homogeneity attack

[۴۷] Background attack

[۴۸] Well represented

[۴۹] Distinct

[۵۰] Entropy

[۵۱] Information gain

اطلاع کسب‌شده‌ی یک مهاجم، در مورد ویژگی حساس یک جدول قبل از انتشار و پس از انتشار آن فاصله t را می‌سازد.

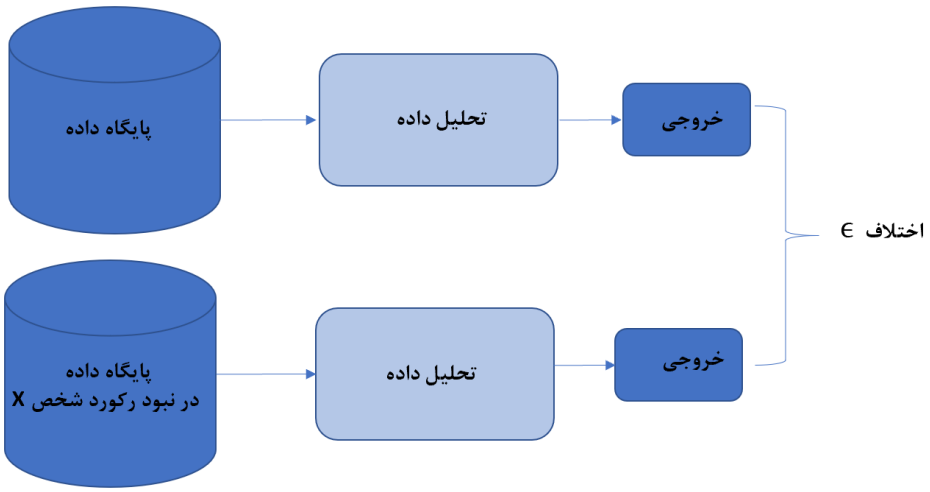
۲-۲-۲ حفظ حریم‌خصوصی مبتنی بر تصادفی‌سازی

در روش‌های حفظ حریم‌خصوصی مبتنی بر تصادفی‌سازی، داده‌ها تصادفی می‌شوند تا مقادیر حساس پنهان بماند. تصادفی‌سازی می‌تواند در بخش جمع‌آوری داده‌ها و یا در بخش تحلیل/انتشار داده‌ها صورت پذیرد.

۲-۲-۲-۱ حریم‌خصوصی تفاضلی[۵۲]

مدل حریم خصوصی تفاضلی برای پایگاه‌داده‌های آماری تعریف می‌گردد. ایده اصلی آن است که پژوهشگران (تحویل‌گیرنده‌های داده در شکل ۷) باید بتوانند پرس‌وجوهای آماری خود نظیر میانه، میانگین، واریانس و موارد دیگر را اجرا نمایند، در عین حال ، شرکت یا عدم شرکت یک فرد در این پژوهش نباید در میزان اطلاعات پژوهشگر و یا مهاجم در مورد یک شخص خاص موثر باشد. مدل حریم خصوصی تفاضلی به صورت زیر تعریف می‌گردد[۶۲]: سازوکار تصادفی M، ϵ-خصوصی تفاضلی است اگر برای هر دو پایگاه‌داده همسایه D_1 و D_2 که در یک رکورد باهم تفاوت دارند و هر $S \subseteq Range(M)$ رابطه زیر برقرار باشد:

$$Pr[M(D_1) \in S] \leq e^{\epsilon} * Pr[M(D_2) \in S]$$



شکل ۸- حریم خصوصی تفاضلی در حضور و نبود شخص X

[۵۲] Differential privacy

مطابق با شکل ۸، حریم خصوصی تفاضلی بیان می‌دارد که شرکت یا عدم شرکت فردی خاص در پژوهش، در اعتقاد مهاجم نسبت به پایگاه‌داده آماری تغییر چندانی ایجاد نمی‌کند(تغییر به میزانϵ)

۲-۲-۲-۲ پاسخ تصادفی‌سازی شده[۵۳]

در پژوهش [۶۱] روش حفظ حریم‌خصوصیِ پاسخ تصادفی شده در ارتباط با تقسیم جمعیتی یک گروه از افراد شرح داده شده است. مسئله حفظ حریم‌خصوصی افراد، در طی یک مصاحبه جمعیتی برای انتساب افراد حاضر به گروه A و B است. در این روش، ایده اصلی آن است که مصاحبه‌شونده، با احتمال مشخصی (احتمال P) حقیقت را بگوید و به احتمال (1-P) به صورت تصادفی پاسخ دهد. در پاسخ تصادفی نیز در پاسخ به سوال«آیا شما عضو گروه A هستید؟» به احتمال P، «بله» پاسخ دهد و به احتمال (1-P)، «خیر» پاسخ دهد. بنابراین درصورتی که فرد در واقعیت عضو گروه A باشد، به احتمال$P+(1-P)*P$ ، پاسخ «بله» داده است و به احتمال $(1-P)*(1-P)$ پاسخ «خیر» داده است. به‌بیان دیگر پاسخ تصادفی‌داده شده قابل انکار است. در بخش بعد چالش احتمال نقض خط‌مشی ایمنی را برای اعمال این روش در سکوهای اینترنت اشیاء مطرح خواهیم نمود.

۲-۲-۲-۳ چالش‌های روش تصادفی‌سازی داده‌ها

در مورد اعمال روش‌های حفظ حریم‌خصوصی مبتنی بر تصادفی‌سازی را در سکوهای اینترنت اشیاء، دو چالش اصلی وجود دارد:

۱. احتمال نقض خط‌مشی ایمنی در ازای تصادفی‌سازی داده‌ها

داده‌های اینترنت اشیاء در فرآیند اجرای برنامه‌ها و تغییر محیط فیزیکی نقش دارند. از این رو در بسیاری از موارد، تصادفی‌کردن نامطئن داده‌های اینترنت اشیاء، ممکن است به یک تغییر ناخواسته در محیط فیزیکی و نقض خط‌مشی ایمنی محیط منجر شود. در حقیقت در بسیاری از موردکاربردهای[۵۴] حفظ حریم‌خصوصی مبتنی بر تصادفی‌سازی داده‌ها، بخشی از کاربردپذیری[۵۵] محیط از دست می‌رود که مخاطره‌ای[۵۶] ایجاد نمی‌کند. برای نمونه پرس‌وجوی[۵۷] یک کاربر در یک موتور جست‌وجو با قابلیت

[۵۳] Randomized Response
[۵۴] Usecase
[۵۵] Utility
[۵۶] Risk
[۵۷] Query

شخصی‌سازی پرس‌وجوها را درنظر بگیرید؛ تصادفی‌سازی پرس‌جوی کاربر با هدف حفظ حریم‌خصوصی تنها موجب می‌شود قابلیت شخصی‌سازی موتور جست‌وجو به طور دقیق عمل نکند و پاسخ پرس‌وجوی کاربر به طور تخمینی با اندکی اختلاف ارائه شود. این درحالی است که تصادفی‌سازی ناآگاهانه داده‌های اینترنت اشیاء ممکن است موجب نقض خط‌مشی ایمنی در محیط فیزیکی گردد. برای نمونه ممکن است تصادفی‌سازی داده‌ی یک دستگاه اینترنت اشیاء منجر به بازماندن ناخواسته درب خانه و یا روشن‌ماندن دستگاه گرمایشی گردد.

۲. عدم وجود پایگاه داده آماری[۵۸] در سکوها

به طور خاص روش حریم‌خصوصی تفاضلی برای محیط‌هایی با پایگاه‌داده‌های آماری کاربرد دارد. پایگاه‌داده‌های آماری، پایگاه‌داده‌هایی هستند که برای اهداف آماری و اجرای توابع آماری نظیر میانگین، میانه، واریانس و موارد دیگر استفاده می‌شوند. در اغلب سکوهای اینترنت اشیاء، اجرای محاسبات برروی هریک از داده‌های ورودی به طور جداگانه و بدون درنظرگرفتن وضعیت قبلی[۵۹] صورت می‌پذیرد و هیچ تابع آماری برروی مجموعه‌ی داده‌های ذخیره‌شده در سکو فراخوانی نمی‌گردد. از سویی دیگر سکوی اینترنت اشیاء به عنوان نگه‌دارنده‌ی داده‌ها نیز مورد اعتماد نیست. بنابراین اعمال روش حریم‌خصوصی تفاضلی برای سکوهای اینترنت اشیاء امکان‌پذیر نیست.

[۵۸] Statistical database

[۵۹] Stateless

فصل سوم

کارهای پژوهشی پیشین

تحقیقات متعدد و متنوعی در حوزه‌ی حفظ حریم خصوصی در محیط‌های اینترنت اشیاء خانه هوشمند صورت گرفته است. بررسی‌ها و نظرسنجی‌ها نشان می‌دهد، بسیاری از کاربران تمایل ندارند که الگوهای رفتاری آن‌ها، لیست تجهیزات و داده‌های حساس اندازه‌گیری شده توسط حسگرها در محیط اینترنت اشیاء آن‌ها در اختیار سرویس‌های شخص ثالث قرار بگیرد[۳۹]. به طور کلی می‌توان پژوهش‌های انجام‌شده در زمینه‌ی حفظ حریم خصوصی در اینترنت اشیاء را به چهار دسته‌ی کلی زیر تقسیم نمود:

۱- حفظ حریم خصوصی نسبت به تحلیل محیط فیزیکی
۲- حفظ حریم خصوصی نسبت به حملات تحلیل ترافیک
۳- حفظ حریم خصوصی نسبت به بدخواهانه[۱] بودن برنامه
۴- حفظ حریم خصوصی نسبت به بدخواهانه بودن سکو

در ادامه ما به شرح مختصر پژوهش‌های انجام شده در سه دسته‌ی اول می‌پردازیم. سپس در ادامه به طور مفصل پژوهش‌های مرتبط با بدخواهانه بودن سکوی اینترنت اشیاء را که مستقیماً با موضوع رساله مرتبط هستند مورد بررسی و نقد قرار می‌دهیم.

۳-۱ حفظ حریم خصوصی نسبت به تحلیل محیط فیزیکی

در این پژوهش‌ها حملاتی مورد بررسی قرار گرفته‌اند که با تحلیل ویژگی‌های محیط فیزیکی نظیر دما، رطوبت، میزان روشنایی، میزان مصرف برق و شدت صوت، رفتار کاربر را در محیط اینترنت اشیاء تشخیص می‌دهند و حریم خصوصی کاربر را نقض می‌نمایند. در واقع این‌حملات مشابه حملات کانال جانبی برای دستگاه‌های اینترنت اشیاء هستند.

پژوهش [۳۴] به بررسی محیط خانه‌ی هوشمند با وجود کنتورهای هوشمند برق پرداخته است. در کنتورهای هوشمند برخلاف کنتورهای قدیمی، میزان مصرف برق در بازه‌های زمانی کوتاه برای شرکت تامین‌کننده‌ی برق ارسال می‌شود. از این رو، تامین‌کنندگان برق می‌توانند با تحلیل میزان مصرف برق، الگوی رفتار کاربر در هر بازه‌ی زمانی و دستگاه‌های متصل در محیط را تشخیص دهند و موجب نقض حریم خصوصی کاربر شوند. در این پژوهش راه‌کاری برای اضافه نمودن نویز و حفظ حریم خصوصی کاربر پیشنهاد داده شده است.

[۱] Malicous

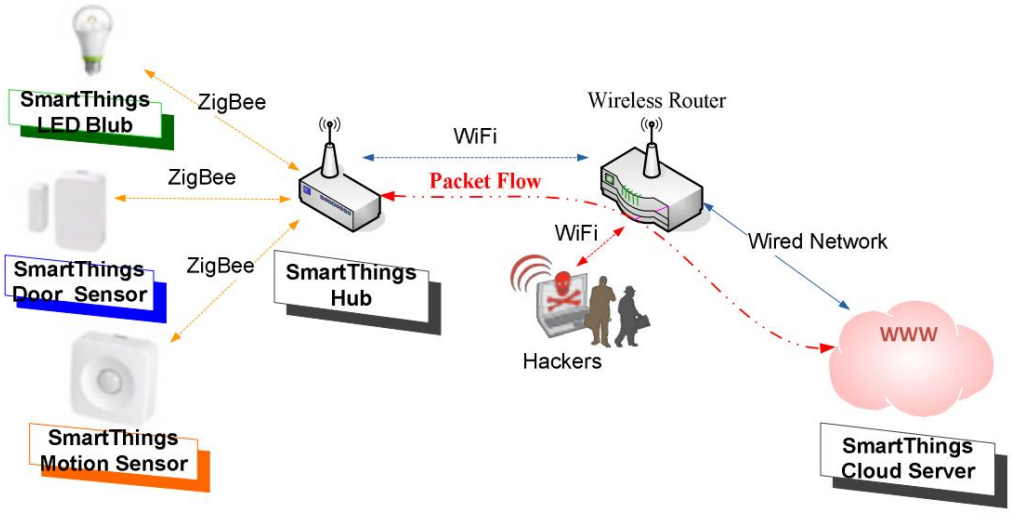
پژوهش [۳۵] حمله‌ای را طراحی نموده است که با بررسی تغییرات روشنایی دیده شده از خارج محیط خانه هوشمند (از فاصله‌ی ۷۰ متری) در هنگام تماشای تلویزیون، می‌توان با دقت بسیار بالایی محتوای در حال پخش تلویزیون را تشخیص داد.

۳-۲ حفظ حریم خصوصی نسبت به حملات تحلیل ترافیک

در سال‌های اخیر، تحلیل ترافیک رمزشده یکی از مسیرهای پژوهشی مطرح برای حملات نقض حریم خصوصی بوده است. درواقع اگرچه با استفاده از پروتکل SSL، ترافیک از دستگاه‌های اینترنت اشیاء تا زیرساخت ابری رمزشده است اما، الگوی ترافیک بسیاری از دستگاه‌های اینترنت اشیاء ثابت و قابل تشخیص است.

در پژوهش[۳۶] ، کوپس و همکاران با بررسی ترافیک رمزشده‌ی دو دستگاه اینترنت اشیاء (ترموستات شرکت نِست و دستگاه تشخیص دود شرکت نِست) نشان داده‌اند که می‌توان حضور یا عدم حضور افراد خانه و فعالیت‌های دیگر کاربران محیط اینترنت اشیاء را تشخیص داد.

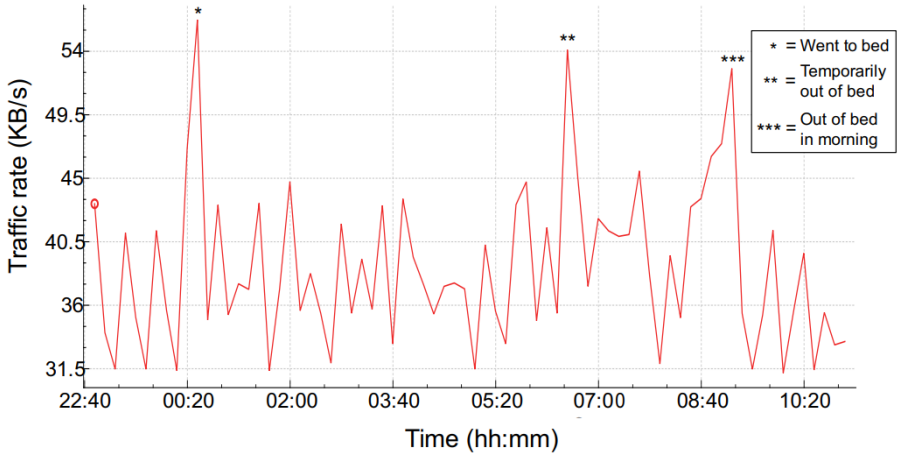
در پژوهش[۳۷] ، یوشیگو و همکاران، با بررسی ترافیک دستگاه‌های موجود در یک سکوی اسمارت‌تینگز نشان داده‌اند که الگو و خصیصه‌های دستگاه‌های مختلف مورد پشتیبانی اسمارت‌تینگز کاملاً متمایز و قابل تشخیص هستند. ، مدل تهدید بررسی شده در این پژوهش را نشان می‌دهد که مهاجمین در بین ارتباط هاب اسمارت‌تینگز و زیرساخت ابری آن حضور دارند و به تحلیل ترافیک رمزشده می‌پردازند.



شکل ۹ - تحلیل ترافیک در محیط اینترنت اشیاء سکوی اسمارت‌تینگز[۳۷]

درواقع مهاجم می‌تواند تامین‌کننده‌ی اینترنت کاربر[۲] باشد و از جزئیات دستورات اجرا شده در محیط اینترنت اشیاء کاربر اطلاع یابد. در این پژوهش، طراحی جدیدی از هاب اسمارت‌تینگز ارائه شده است که علاوه بر ترافیک نرمال، ترافیک تولیدی را نیز برای حفظ حریم خصوصی کاربر به شبکه می‌افزاید.

در پژوهش[۳۸] ، آپتورت و همکاران در ابتدا به بررسی مخاطرات حریم خصوصی ناشی از تحلیل ترافیک رمزشده‌ی محیط اینترنت اشیاء توسط شرکت تامین‌کننده‌ی اینترنت و یا هر ناظر شبکه‌ای دیگری پرداخته‌اند. مطابق شکل ۱۰ آن‌ها نشان داده‌اند که تنها با داشتن نرخ بسته‌های جابه‌جا شده ترافیک توسط حسگر خواب در محیط اینترنت اشیاء، می‌توان جزئیات قابل‌توجهی از الگوی خواب کاربر را تشخیص داد.



شکل ۱۰- نرخ ترافیک ورودی و خروجی از یک حسگر خواب[۳۸]

نویسندگان این پژوهش سپس راهکارهای پیشنهادی متنوعی را مورد بررسی قرار داده‌اند. این راه‌کارها شامل راه‌کار تونل‌سازی[۳] ترافیک و شکل‌دهی به ترافیک[۴] می‌شود.در نهایت ارزیابی نشان می‌دهد که ایده‌ی شکل‌دهی به ترافیک می‌تواند تنها با افزودن ۴۰ KB/s پهنای باند بیش‌تر از چنین حملاتی جلوگیری نماید.

[۲] ISP (Internet Service Provider)
[۳] Tunneling
[۴] Traffic shaping

۳-۳ حفظ حریم خصوصی نسبت به بدخواهانه بودن برنامه

بخش دیگری از تحقیقات مرتبط با حریم خصوصی در اینترنت اشیاء، مربوط به نقض حریم خصوصی توسط برنامه‌های اینترنت اشیاء می‌باشد.

راه‌کارهای مختلفی برای تحلیل جریان اطلاعات[۵] در برنامه‌های اینترنت اشیاء ارائه شده است[۱۷][۲۳] [۴۱]. باستیس و همکاران[۱۷] نشان دادند که برنامه‌های بدخواه در سکوهای IFTTT، زپیر و مایکروسافت‌پاوراتومیت قابلیت نشت داده‌های حساس کاربر، شامل تصاویر، موقعیت مکانی کاربر و دستورات صوتی کاربر را دارند. در این پژوهش به عنوان نمونه‌ی موردی سرویس‌های رهانا و کنش سکوی IFTTT را از منظر محرمانه‌بودن دسته‌بندی نمودند و نشان دادند که ۳۰ درصد از برنامه‌های IFTTT قابلیت نشت داده‌های حساس به سرویس‌های شخص ثالث مهاجم را دارند.

در پژوهش سِینت[۶][۲۳] از تحلیل ایستای کد برنامه‌های اسمارت‌تینگز برای یافتن جریان داده‌های حساس استفاده شده است. سِینت سه فاز کلی را برای این راه‌کار اجرا می‌نماید:

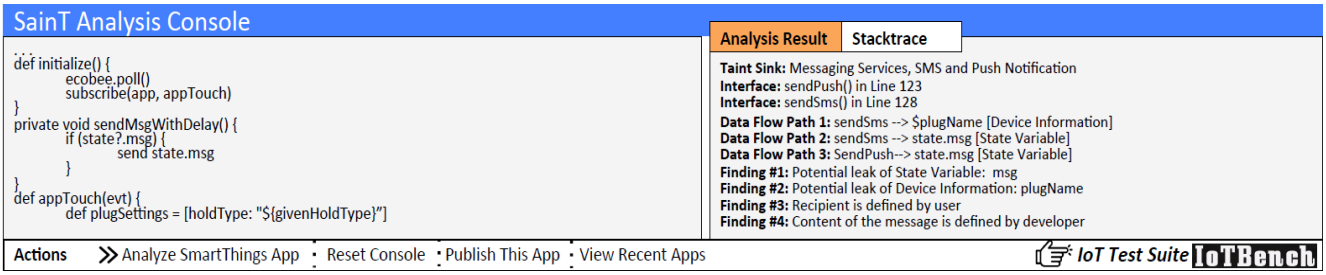
۱- تبدیل کد منبع برنامه‌ی اسمارت‌تینگز به یک کد میانی
۲- تشخیص منبع[۷] و چاه[۸] حساس
۳- تحلیل ایستا برای تشخیص جریان داده‌های حساس

در شکل ۱۱، ابزار سِینت دیده می‌شود که کد منبع برنامه‌ی اسمارت‌تینگز به عنوان ورودی و جریان داده‌های حساس برنامه به عنوان خروجی ارائه شده است. به طور طبیعی با توجه به آن که رویکرد ابزار سِینت تحلیل ایستا است، توانایی شناسایی جریان داده‌های غیرمجاز را در زمان اجرا ندارد.

در پژوهش فلوفِنس[۹][۲۵] ، از استفاده‌کنندگان داده‌های حساس درخواست می‌شود تا الگوهای جریان داده مورد نیاز خود را برای استفاده از داده‌های حساس ارائه نمایند. این جریان‌های داده در واقع جریان‌های مجاز داده هستند. فلوفِنس تمامی جریان داده‌های غیر از موارد ذکر شده را برای داده‌های حساس مسدود می‌سازد تا از عدم

[۵] Information Flow Analysis (IFA)
[۶] SAINT
[۷] Source
[۸] Sink
[۹] FlowFence

نشت داده‌ها در برنامه‌های اینترنت اشیاء مطمئن شود. البته لازم به ذکر است که رویکرد فلوفِنس تا حدی سخت‌گیرانه است و برخی از موارد را به اشتباه به عنوان جریان داده‌ی غیرمجاز مسدود می‌نماید.



شکل ۱۱- نمایی از ابزار تحلیل ایستا سِینت [۲۳]

سمت راست: کد منبع برنامه به عنوان ورودی، سمت چپ: جریان داده‌های حساس در خروجی ابزار

در پژوهش آی‌رولر[۱۱] [۴۰] ، خطرات ناشی از ارتباطات بین برنامه‌ای در یک سکوی اینترنت اشیاء مورد بررسی قرار گرفته است. راهکار پیشنهادی آی‌رولر مبتنی بر تحلیل زبان طبیعی توصیف برنامه‌ها است تا آسیب‌پذیری‌های بین‌برنامه‌ای را تشخیص دهد.

پژوهش آی‌اُتی‌واچ[۱۲] [۳۹] یک راه‌کار تحلیل پویا در زمان‌اجرا[۱۳] را برای بررسی نقض حریم‌خصوصی توسط برنامه‌های اینترنت اشیاء ارائه نموده است. این پژوهش در ابتدا یک نظرسنجی میان کاربران محیط‌های اینترنت اشیاء خانگی داشته است تا نیازها و دغدغه‌های کاربران در زمینه حریم خصوصی داده‌های حساس‌شان را استخراج نماید.

راهکار ، با استفاده از یک واسط در زمان نصب برنامه، ترجیحات حریم خصوصی[۱۴] کاربر را در مورد داده‌های مورد استفاده در یک برنامه اینترنت اشیاء دریافت می‌نماید. سپس آی‌اُتی‌واچ به کد منبع برنامه‌های اینترنت اشیاء، خطوطی را اضافه می‌کند تا در زمان اجرا اطلاعات مربوط به برنامه را جمع نماید. با استفاده از داده‌های جمع‌آوری‌شده، داده‌های ورودی و خروجی از برنامه‌ی اینترنت اشیاء چک می‌گردد و خواسته‌های حریم خصوصی کاربر اعمال می‌شود.

[۱۱] iRuler
[۱۲] IoTWatch
[۱۳] Runtime
[۱۴] Privacy Preferences

۳-۴ حفظ حریم خصوصی نسبت به بدخواهانه بودن سکو

بخش دیگری از تحقیقات در زمینه حفظ حریم خصوصی در اینترنت اشیاء، مدل تهدید مبتنی بر سکوی بدخواه را درنظر گرفته‌اند. در این مدل تهدید، دو حالت در نظر گرفته شده است:

۱- با توجه به متمرکز بودن سکوهای اینترنت اشیاء و خط‌مشی حریم خصوصی منتشرشده توسط آن‌ها [۵] [۶]، این سکوها به داده‌های حساس قابل توجهی از کاربر دسترسی دارند و از این داده‌ها برای ساخت پروفایل کاربر در راستای تبلیغات هدفمند و فروش پروفایل کاربر به شرکت‌های شخص ثالث استفاده می‌کنند.
۲- متمرکز بودن سکوها و تجمیع داده‌های حساس و توکن‌های دسترسی در این سکوها موجب شده است تا هدف جذابی برای مهاجمین سایبری و هکرها باشند. از این رو مدل تهدید مبتنی بر حضور یک مهاجم در سکو، فرض دور از ذهنی نیست.

پژوهش‌های مبتنی بر سکوی بدخواه را می‌توان به چهار دسته تقسیم نمود:

۱- پژوهش‌هایی با هدف تضمین صحت اجرای برنامه
۲- پژوهش‌های مبتنی بر رمزنگاری
۳- پژوهش‌های مبتنی بر تولید رهاناهای جعلی
۴- پژوهش‌های مبتنی بر سخت افزار امن

در ادامه هر یک از این چهار دسته و پژوهش‌های مرتبط با آن‌ها شرح داده شده و مورد نقد قرار گرفته‌اند.

۳-۴-۱ پژوهش‌هایی با هدف تضمین صحت اجرای برنامه

پژوهش DTAP

پژوهش DTAP[۱۵] [۱۰] اولین پژوهشی است که مدل تهدید سکوی بدخواه را در محیط اینترنت اشیاء خانه‌ی هوشمند مطرح نمود. اگر چه مسئله‌ی این پژوهش، نقض صحت در برنامه‌های اینترنت اشیاء است اما از منظر بدخواه بودن سکو و مدل تهدید مشابهت‌هایی با مسئله‌ی پژوهشی نقض حریم خصوصی کاربر در سکوی

[۱۵] Decentralised Trigger Action Platform

بدخواه دارد. هدف دقیق پژوهش DTAP آن است که سکوی بدخواه یا مهاجمی که موفق به دسترسی کامل به سکو شده، نتواند از توکن‌های[۱۶]دسترسی سرویس‌های مختلف کاربر سوءاستفاده نماید. علاوه بر آن، سکوی بدخواه نتواند، صحت[۱۷] داده‌های دریافتی از سرویس رهانا را نقض نماید تا مسیر اجرای برنامه‌ی اینترنت اشیاء را تغییر دهد.

فرضیات:

۱. سکو، بدخواهانه[۱۸] رفتار می‌کند. ممکن است رفتار بدخواهانه سکو ناشی از این باشد که مورد حمله مهاجمین قرار گرفته و مهاجمین دسترسی کاملی بر روی سکو داشته باشند.
۲. سکو/ مهاجم به توکن‌های OAuth کاربر دسترسی دارد و سعی دارد تا از آن‌ها سوءاستفاده نماید.
۳. سکو/مهاجم می‌تواند داده‌های دریافتی از یک سرویس رهانا را دستکاری نماید و در واقع مسیر اجرای برنامه را با تغییر ورودی عوض نماید.
۴. سرویس‌های رهانا و کنش مورد اعتماد هستند و مورد حمله قرار نگرفته‌اند.
۵. نشت داده‌های حساس کاربر (حریم خصوصی) و حملات منع سرویس مسئله‌ی این مقاله نیست.

راه‌کار پیشنهادی DTAP درواقع ماهیت واحد یک سکوی اینترنت اشیاء را به دو قسمت تقسیم می‌نماید.

۱- ابر DTAP[۱۹] که مورد اعتماد نیست.
۲- کارگزار DTAP[۲۰] که مورد اعتماد است و به صورت توزیع‌شده در اختیار هرکاربر قرار دارد (هرکاربر به کارگزار مربوط به خود اعتماد دارد).

دسترسی کاربر به سرویس‌های برخط توسط کارگزار مدیریت می‌شود. پیاده‌سازی کارگزار باید به صورت متن‌باز و مستقل از توسعه‌دهنده‌ی سکوی ابری باشد. این راه‌کار هم‌چنین از یک نسخه‌ی گسترش‌یافته از OAuth توکن با نام XToken بهره می‌برد که در واقع یک توکن مختص به برنامه[۲۱] است. دسترسی هر XToken صرفاً به یک متد خاص محدود شده است (و متد دیگری از همین سرویس قابلیت اجرا با این توکن را ندارد). به عنوان

[۱۶] OAuth Tokens
[۱۷] Integrity
[۱۸] malicious
[۱۹] DTAP Cloud
[۲۰] Client
[۲۱] Rule specific token

نمونه اگر یک برنامه اینترنت اشیاء اجازه‌ی دسترسی برای ارسال ایمیل از سرویس ایمیل کاربر را دریافت نموده باشد، با استفاده از XToken مربوطه صرفاً می‌توان ایمیل ارسال نمود و نمی‌توان کنش دیگری نظیر خواندن ایمیل کاربر را صورت داد. این درحالی است که توکن‌های دسترسی OAuth که به طور معمول در سکوهای کنونی استفاده می‌شوند ریزدانگی کافی را ندارند و در همین مثال به سکو/ مهاجم بدخواه اجازه می‌دهند بدون اجازه بتواند ایمیل‌های کاربر را نیز بخواند.

توکن‌های پیشنهادی XToken با متصل کردن دسترسی توکن برای اجرای یک کنش به رخدادن یک رهانای مشخص[۲۲]، موجب می‌شوند تا در صورت مورد حمله واقع شدن سکو، مهاجم هیچ دسترسی بیش از دسترسی لازم برای اجرای یک کنش خاص را نداشته باشد.

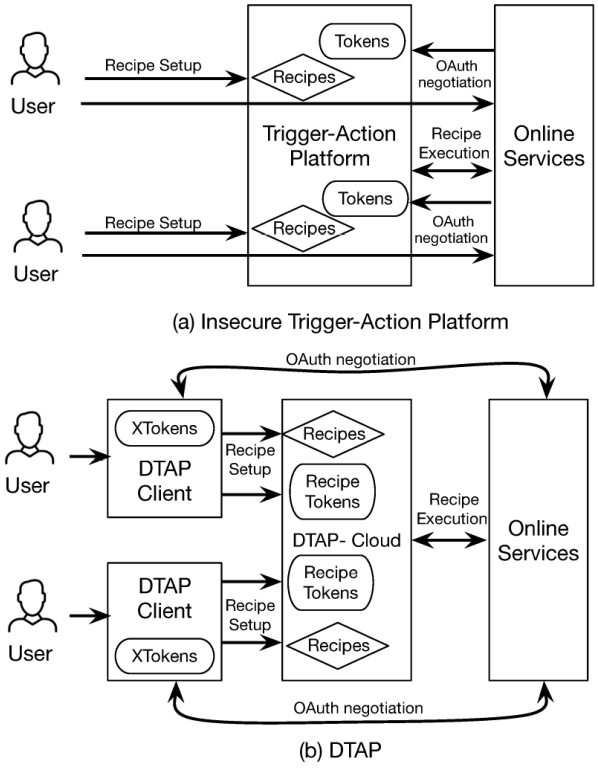
ایده‌ی اصلی راه‌کار DTAP بر دو اصل استوار است:

۱- توکن پیشنهادی XToken را داشته باشیم، به گونه‌ای که به اندازه‌ی کافی ریزدانه و مرتبط با مشخصات برنامه‌ی اینترنت اشیاء باشد.
۲- توکن‌های دسترسی تعریف‌شده را در اختیار سکوی اینترنت اشیاء قرار ندهیم؛ بلکه XToken را به صورت توزیع‌شده در کارگزارهای مورد اعتماد کاربران قرار دهیم و پس از نهایی شدن برنامه اینترنت اشیاء (تعیین رهانا و کنش مربوط به یک برنامه)، توکن رهانا[۲۳] و توکن کنش[۲۴] مربوط به یک برنامه را در اختیار سکو قرار دهیم.

چالش‌ها:

۱- درنظر نگرفتن امکان نقض حریم خصوصی در سکوی بدخواه
۲- محدودیت‌های پیاده‌سازی سرویس رهانا و کنش: سرویس رهانا و کنش باید کتابخانه لازم برای پشتیبانی از XToken و امضای دیجیتال را به خود اضافه نمایند.
۳- محدودیت‌های درنظر گرفتن کارگزار به عنوان دستگاه مورد اعتماد

[۲۲] این رهانا در زمان تعریف برنامه اینترنت اشیاء تعیین شده است.
[۲۳] Trigger Token
[۲۴] Action Token



شکل ۱۲- تفاوت ساختار توکن دسترسی در سکوهای ناامن کنونی و سکوی پیشنهادی امن DTAP [۱۰]

۳-۴-۲ پژوهش‌های مبتنی بر تولید رهانای جعلی

راه‌کار OTAP

در پژوهش [۱۲] ، چیانگ و همکاران راه‌کار OTAP[۲۵]را ارائه داده‌اند. در OTAP سعی می‌شود تا الگوی رخ دادن رهاناها با اضافه کردن تعداد زیادی رهانای جعلی[۲۶]، از دید سکوی بدخواه پنهان بماند. از سویی دیگر OTAP با استفاده از رمزنگاری انتها به انتها[۲۷]، کل بسته‌ی داده‌ی رهانا را به صورت رمزشده از سکو عبور می‌دهد تا محتوای رهانا و کنش از دید سکو پنهان بماند؛ البته این موضوع موجب می‌شود تا قابلیت محاسبه بر روی داده‌ی رهانا امکان‌پذیر نباشد.

[۲۵] Obfuscated Trigger Action Platform

[۲۶] Fake trigger

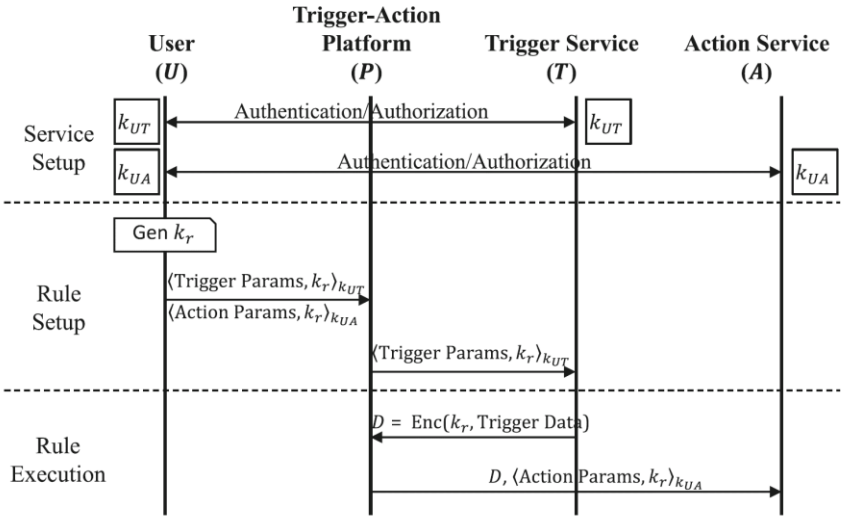
[۲۷] رمزنگاری انتها به انتها بین سرویس رهانا و سرویس کنش

فرضیات:

سکو، بدخواهانه رفتار می‌کند. ممکن است رفتار بدخواهانه‌ی سکو ناشی از حمله‌ی مهاجمین باشد.

۱. داده‌های حساس کاربر در سکوی اینترنت اشیاء عبارت است از:
   - داده‌ی رهانا (نظیر دمای محیط خانه) و پارامترهای برنامه
   - رخداد یا عدم رخداد رهانا (نظیر رخداد رهانای «ترک خانه» با استفاده از حسگر حرکت)
   - وجود دستگاه‌های اینترنت اشیاء (نظیر وجود سمعک هوشمند برای کاربر که می‌تواند نشانگر کم‌شنوایی کاربر باشد)
۲. در مدل تهدید این پژوهش، بازخورد یک کنش در نظر گرفته نشده است و در واقع فرض بر آن است که هیچ بازخوردی از اجرا یا عدم اجرای یک کنش به سکو بازگردانده نمی‌شود.
۳. سرویس‌های رهانا و کنش مورد اعتماد هستند و با سکو تبانی نکرده‌اند.
۴. تضمین صحت اجرای برنامه و مقابله با حملات منع سرویس، مسئله‌ی این مقاله نیست.

مطابق شکل ۱۳ در پروتکل OTAP، کاربر با تولید یک کلید تصادفی و ارسال آن به صورت رمزشده برای سرویس‌های رهانا و کنش، مقدمات لازم برای رمزنگاری انتها به انتها بین سرویس رهانا و سرویس کنش را فراهم می‌نماید. از این رو محتوای رهانای ارسالی برای سکو از دید سکوی بدخواه پنهان می‌ماند.
برای پنهان‌سازی الگوی رخ دادن رهاناها نیز به صورت متناوب در بازه‌های زمانی t ثانیه‌ای به ازای هر دستگاه اینترنت اشیاء، رهاناهای حقیقی (در صورت وجود) و رهاناهای جعلی برای سکو ارسال می‌شود.



شکل ۱۳- پروتکل OTAP [۱۲]

چالش‌ها:

۱- درنظر نگرفتن امکان محاسبه بر روی داده‌های رهانا

در تمامی سکوهای اینترنت اشیاء، این امکان وجود دارد تا کد منبع برنامه‌ی اینترنت اشیاء توسعه یابد و امکان تغییر و اعمال محاسباتی را برروی داده‌های ورودی رهانا فراهم آورد. با انجام محاسبه بر روی داده‌های رهانا، دستورات کنش به عنوان خروجی حاصل می‌گردد. پژوهش OTAP فرض مسئله‌ی خود را صرفاً برای تعدادی از برنامه‌های اینترنت اشیاء قرار داده است که بدون نیاز به محاسبه بر روی رهاناهای ورودی، دستورات کنش را صادر می‌نمایند. فرض مذکور کاملاً محدودکننده است و موجب می‌شود تا ویژگی رایج محاسبه در سکوهای اینترنت اشیاء درنظر گرفته نشود.

۲- سربار ارتباطی بسیار زیاد برای تولید رهاناهای جعلی (بنابر ارزیابی انجام شده در این پژوهش، سربار ناشی از راهکار بیش از ۸ برابر حالت عادی سکو است).

۳- عدم ارایه راهکار عملی مناسب برای تولید رهاناهای جعلی متناسب با رهاناهای حقیقی

۴- عدم درنظر گرفتن رخداد کنش در مدل تهدید

در مدل پیشنهادی OTAP فرض بر آن است که هیچ بازخوردی از کنش به سوی سکو نمی‌رود. این در حالی است که با توجه به همبستگی معنایی بین وقوع یک رخداد با داده‌های ورودی از حسگرهای دیگر، قابلیت نقض حریم خصوصی و تشخیص رهاناهای جعلی برای سکو وجود دارد.

به بیان دیگر در بسیاری از موارد دستگاه اینترنت اشیاء پس از انجام یک کنش، تغییر وضعیت می‌دهد و وضعیت جدید را برای سکو ارسال می‌نماید. این موضوع می‌تواند راه‌کار پیشنهادی OTAP را با مشکل جدی مواجه نماید.

پژوهش F&F

در پژوهش [۱۱]، ژو و همکاران ارتباط بین سکوی اسمارت‌تینگز با سکوهای شخص ثالثی مانند IFTTT و وب‌کُر[۲۸][۱۶] را که برنامه‌های آن‌ها برروی واسط برنامه‌نویسی[۲۹] سکوی توسعه می‌یابند، مورد بررسی قرار داده‌اند. این سکوهای شخص ثالث، امکان توسعه‌ی برنامه‌های متنوع‌تری را نسبت به برنامه‌های سکوی اسمارت‌تینگز ارائه می‌دهند. مثلا IFTTT امکان اتصال سرویس‌های مربوط به دستگاه‌های اینترنت اشیاء به سرویس‌های برخط را فراهم می‌نماید.

[۲۸] WebCore

[۲۹] API

در این پژوهش نشان داده شده است که IFTTT به اطلاعات حساس بیش‌تری از آن چه برای اجرای برنامه‌های اینترنت اشیاء نیاز است، دسترسی دارد. به عنوان نمونه سکوی IFTTT پس از دریافت اطلاعات هویتی واسط برنامه‌نویسی اسمارت‌تینگز ، به اطلاعات رهاناهای ورودی از دستگاه‌هایی که برای آن‌ها برنامه‌ای تعریف نشده است نیز دسترسی دارد که این دسترسی کاملاً غیرضروری است.

فرضیات:

۱- سکوی اسمارت‌تینگز امن و مورد اعتماد است.
۲- سکوی IFTTT، وب‌کُر یا هر سکوی شخص ثالث دیگری متصل به اسمارت‌تینگز بدخواه است و یا مورد حمله‌ی مهاجم واقع شده است.
۳- سکوی شخص ثالث قصد دارد با استفاده از تحلیل آماری و استفاده از داده‌های خامی که از کاربر در اختیار دارد پروفایل رفتاری کاربر را تهیه نماید که این موجب نقض حریم خصوصی کاربر خواهد شد.
۴- مسئله‌ی این پژوهش تضمین صحت اجرای برنامه‌ها و مقابله با حملات دیگر نظیر حمله‌ی منع‌سرویس نمی‌باشد.

این پژوهش یک ماژول با نام F&F[۳۰] را پیشنهاد می‌نماید که با استفاده از توصیف[۳۱] برنامه‌های IFTTT، داده‌های اضافی نظیر داده‌های مربوط به دستگاه‌هایی که هیچ برنامه‌ای برای آن‌ها وجود ندارد را فیلتر می‌نماید. این فیلتر کردن رهاناهای ورودی شامل داده‌های وضعیت دستگاه‌های کنش (که عملاً هیچ تاثیری در روند فعال‌کردن برنامه‌های اینترنت اشیاء ندارند) و رهاناهای اضافه (که منجر به کنش جدیدی در محیط اینترنت اشیاء نمی‌شوند) نیز می‌شود.

از سوی دیگر برای داده‌های باقی‌مانده‌ی ورودی، سکو با تولید رهاناهای جعلی سعی می‌نماید تا الگوی آماری رهاناها را گمنام[۳۲] سازد و از توانایی سکو برای استخراج الگوی آماری رفتار کاربر جلوگیری نماید. این کار با اضافه نمودن رهاناهای جعلی تا رسیدن به یک توزیع ایده‌آل[۳۳] و یا یک توزیع گوسی[۳۴] ادامه می‌یابد.

چالش‌ها:

۱- در نظر گرفتن سکوی اسمارت‌تینگز به عنوان سکوی امن و مورد اعتماد

---

۳۰ Filter & Fuzz
۳۱ Description
۳۲ Anonymous
۳۳ Ideal distribution
۳۴ distribution Gaussian

در واقع در این پژوهش مدل ساده شده‌ای فرض شده است تا راه‌کار حفظ حریم خصوصی و اعمال آن ساده‌تر گردد. این در حالی است که بررسی خط‌مشی حریم خصوصی اسمارت‌تینگز ، تعداد کاربران و متمرکزبودن سرویس آن، نشان می‌دهد که این فرض قابل‌قبول نیست.

۲- شفاف نبودن نحوه‌ی استخراج منطق برنامه براساس توضیحات متنی مختصر در ارتباط با برنامه

در این پژوهش فرض شده که با استفاده از یک افزونه‌ی مرورگر از سایت https://ifttt.com/my_applets متن توصیف برنامه[۳۵] دریافت می‌شود. این پیش‌فرض می‌تواند عملی باشد اما چالش اصلی آن است که توصیف متنی برنامه لزوماً شامل فیلترکد[۳۶] برنامه نیست و فرض آن که بتوان منطق برنامه را از توضیح متنی آن استخراج نمود، فرض نامعتبری است.

علاوه بر آن در فرآیند تولید رهاناهای جعلی، فرض شده که پس از تولید این رهاناها و پاسخ سکو به آن‌ها ماژول F&F خروجی‌های مرتبط با رهاناهای جعلی را تشخیص می‌دهد و از روال اجرا خارج می‌نماید؛ این در حالی است که عدم دسترسی به منطق دقیق برنامه می‌تواند حالاتی را رقم بزند که یک برنامه‌ی اینترنت اشیاء با عطف چند رهانا فعال گردد و یک یا چند مورد از این رهاناها جعلی و باقی رهاناها واقعی باشند. در این صورت نیز راه‌کار F&F با مشکل جدی در تشخیص و از دسترس خارج کردن نتایج رهاناهای غیرواقعی مواجه خواهد بود.

۳- مشکل بودن پیاده‌سازی این ماژول در تعامل با سکوی اسمارت‌تینگز

پیاده‌سازی ماژول F&F نیازمند همکاری و تغییر وسیع در سکوی اسمارت‌تینگز است که در عمل فرآیندی مشکل است.

۴- ساده بودن حسگرها و سناریوهای انتخاب‌شده

موارد بررسی‌شده در این مقاله، مبتنی بر داده‌های آزمون تعداد محدودی حسگر دما، حسگر حرکت و سوئیچ است و برنامه‌های درنظر گرفته شده بر روی این حسگرها، برنامه‌های بسیار ساده‌ای هستند. به بیان دیگر در بخش بررسی این مقاله دو برنامه‌ی ساده «روشن شدن سوئیچ در ازای حسگر حرکت» و «روشن شدن سوئیچ در ازای دمای بالاتر از ۳۰ درجه» در نظر گرفته شده است. در نقد این پژوهش می‌توان برنامه‌های پرطرفداری از سکوهای اسمارت‌تینگز ، IFTTT و نود-رِد را نشان داد که در این پژوهش مورد بررسی قرار نگرفته‌اند.

[۳۵] App description

[۳۶] Filter Code

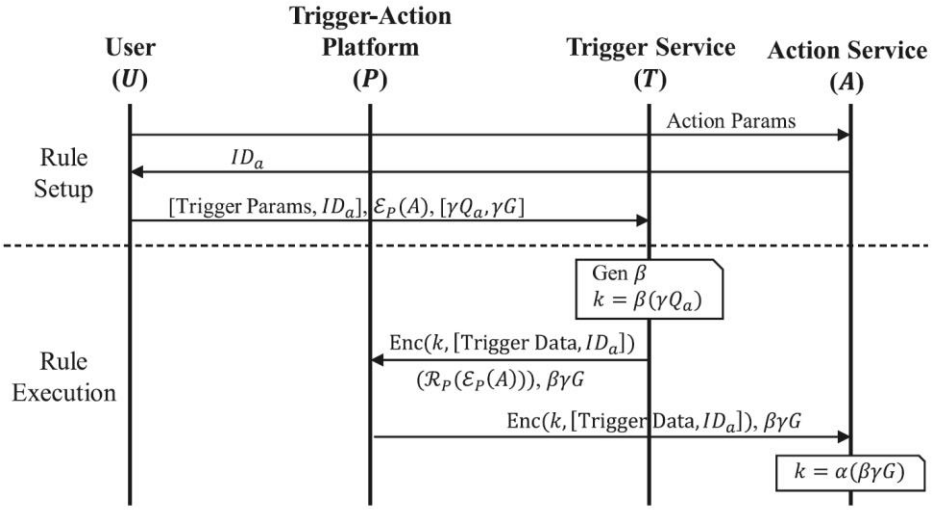
۳-۴-۳ پژوهش‌های مبتنی بر رمزنگاری

راه‌کار ATAP

در پژوهش [۱۲] ، چیانگ و همکاران راه‌کار دیگری را نیز ارائه داده‌اند که ATAP [۳۷] نام دارد. فرضیات این راه‌کار دقیقاً مشابه موارد ذکرشده در مورد OTAP است. راه‌کار ATAP سعی دارد تا حریم خصوصی را در هر سه سطح داده‌رها و پارامترهای برنامه، رخداد یا عدم رخداد رها و لیست دستگاه‌های موجود در محیط حفظ نماید. البته راه‌کار پیشنهادی ATAP نیازمند تغییرات وسیع در سکو و سرویس‌های رها و کنش است.

در راه‌کار ATAP، برنامه‌های اینترنت اشیاء در سکو ذخیره نمی‌شوند بلکه اطلاعات مربوط به این برنامه ها در سرویس‌های رها و کنش ذخیره می‌گردد.

مطابق شکل ۱۴ پروتکل ATAP سعی دارد تا با ایجاد یک زیرساخت رمزنگاری متقارن مبتنی بر توافق کلید ECDH [۳۸] بین سرویس رها و کنش، هویت کاربر را از دید سکو مخفی کند. در واقع بسته‌های رمزشده‌ای که در اختیار سکو قرار می‌گیرد، صرفاً نشان‌دهنده‌ی این است که رها از کدام سرویس دریافت شده و باید به کدام سرویس کنش ارسال شود. این موضوع موجب می‌شود تا هویت کاربر بین تمامی کاربرانی که از این سرویس رها و کنش استفاده می‌کنند گمنام بماند.



شکل ۱۴- پروتکل ATAP [۱۲]

[۳۷] Ananymous Trigger Action Platform

[۳۸] Elliptic-curve Diffie–Hellman

چالش‌ها:

۱- نیاز به تغییرات عمده در سطح سکوی اینترنت اشیاء

در این پژوهش تغییر سکو تا حدی است که نقش سکوی ATAP صرفاً به یک فرستنده‌ی[۳۹] پیام‌های کاملاً رمزشده تغییر می‌یابد. هم‌چنین برنامه‌های اینترنت اشیاء برروی سکو ثبت نمی‌شوند. به بیان دیگر فلسفه‌ی وجودی سکوی اینترنت اشیاء که ساده‌سازی ارتباط بین سرویس‌های رهانا و کنش است به طور کامل از بین می‌رود و بخش عمده‌ای از کارکرد سکو نیز از دست رفته است.

۲- نیاز به تغییرات عمده در سرویس‌های رهانا و کنش

تغییرات لازم در سرویس‌های رهانا و کنش نیز تغییرات قابل‌توجهی است. در بخشی از پروتکل ATAP، الگوریتم توافق کلید ECDH بین سرویس رهانا و سرویس کنش در نظر گرفته شده است. پیاده‌سازی این موضوع در سطح تمامی سرویس‌های رهانا و کنش، امری مشکل و بعید به نظر می‌رسد. با فرض آن که سرویس رهانا و کنش بتوانند به صورت رمزشده و با یک کلید توافق‌شده با یکدیگر گفت‌وگو کنند، با اندکی تغییر می‌توان به طور کامل سکوی اینترنت اشیاء را از پروتکل کنار گذاشت که مطلوب نیست.

۳- نیاز به تغییر کارگزار کاربر

باتوجه به نیاز به زیرساخت رمزنگاری سمت کاربر، لازم است تا کارگزار کاربر نیز تغییر یابد.

۴- عدم پشتیبانی از محاسبه بر روی داده‌های رهانا

پژوهش ATAP فرض مسئله‌ی خود را صرفاً برای تعدادی از برنامه‌های اینترنت اشیاء قرار داده است که بدون نیاز به محاسبه بر روی رهاناهای ورودی، دستورات کنش را صادر می‌نمایند. فرض مذکور کاملاً محدودکننده است و موجب می‌شود تا ویژگی رایج محاسبه در بین سکوهای اینترنت اشیاء در نظر گرفته نشود.

پژوهش ETAP (منتشر نشده)

در پژوهش[۱۵] ، چن و همکاران سکوی ETAP[۴۰] را به عنوان یک سکوی کاملاً رمزنگاری شده پیشنهاد نموده اند. این سکو قابلیت این را دارد تا محاسبات مورد نیاز برنامه‌های اینترنت اشیاء را برروی داده‌های رمزنگاری‌شده انجام دهد و خروجی این محاسبات نیز به صورت رمزشده بر روی سکو حاصل شود.

[۳۹] Forwarder

[۴۰] Encrypted Trigger Action Platform

فرضیات:

۱. سکو، بدخواهانه رفتار می‌کند؛ به طور مشخص مهاجم مسلط به سکو، دسترسی های زیر را دارد:
   - مشاهده کردن کامل ارتباطات بین سکو و سرویس‌های رهانا و کنش
   - انحراف از انجام پروتکل و تغییر، ایجاد تاخیر یا از بین بردن پیام ورودی از سرویس رهانا
   - تغییر حافظه و کد موجود در سکو
   - مشاهده‌ی منطق محاسبه‌ی انجام‌شده در هر برنامه‌ی اینترنت اشیاء
۲. سرویس‌های رهانا و کنش موجود صادق ولی کنجکاو[۴۱] هستند؛ به این معنا که از پروتکل موجود پیروی می‌کنند اما ممکن است اطلاعاتی بیش از اطلاعات مورد نیاز را جمع‌آوری کنند.
۳. سکو با هیچ یک از سرویس‌های رهانا و کنش تبانی ندارد.
۴. کاربر به کارگزار خود اعتماد دارد.
۵. مسئله‌ی این پژوهش حفظ حریم خصوصی و تضمین صحت برنامه‌های اینترنت اشیاء است.
۶. مقابله با حملات دیگر نظیر حمله منع سرویس و حملات کانال جانبی خارج از حیطه این پژوهش است.

مطابق شکل ۱۵، در این سکو از ایده‌ی پروتکل مدار درهم[۴۲] استفاده شده است. در ابتدا کارگزار مورد اعتماد کاربر به عنوان یک تولیدکننده‌ی امن مدار درهم درنظر گرفته می‌شود. کارگزار کاربر در طول زمان به صورت دوره‌ای مدار درهم را تولید می‌کند و در اختیار سکوی ناامن قرار می‌دهد. سرویس رهانا در هنگام ورود داده‌ی رهانا، آن را درهم‌سازی می‌کند و در اختیار سکو قرار می‌دهد. سپس سکو با استفاده از مدار درهم، بر روی داده‌ی درهم‌شده‌ی رهانای ورودی، مدار درهم را اجرا نموده و خروجی درهم‌شده را در اختیار سرویس کنش قرار می‌دهد. سرویس کنش در ابتدا چک امنیتی خود را صورت می‌دهد، سپس به اجرای کنش مربوطه می‌پردازد. با اجرای این پروتکل، سکو به هیچ یک از داده‌های حساس کاربر دسترسی نمی‌یابد در عین حال قادر است تا محاسبات لازم برای برنامه‌های اینترنت اشیاء را به صورت رمزشده انجام دهد.

چالش‌ها:

۱- وابسته بودن به معماری سکوهای شبه IFTTT

با توجه به آن که پروتکل مدار درهم نیازمند ساختار پیشنهاد شده با چهار موجودیت سرویس رهانا، سرویس کنش، کارگزار کاربر و سکو می‌باشد، در معماری سکوهای متفاوت از IFTTT که دارای

[۴۱] honest but curious
[۴۲] Garbled Circuit

سرویس رهانا و کنش نیستند قابل پیاده‌سازی نیست.

۲- نیاز به آپلود روزانه‌ی داده‌های مربوط به مدار درهم توسط کاربر

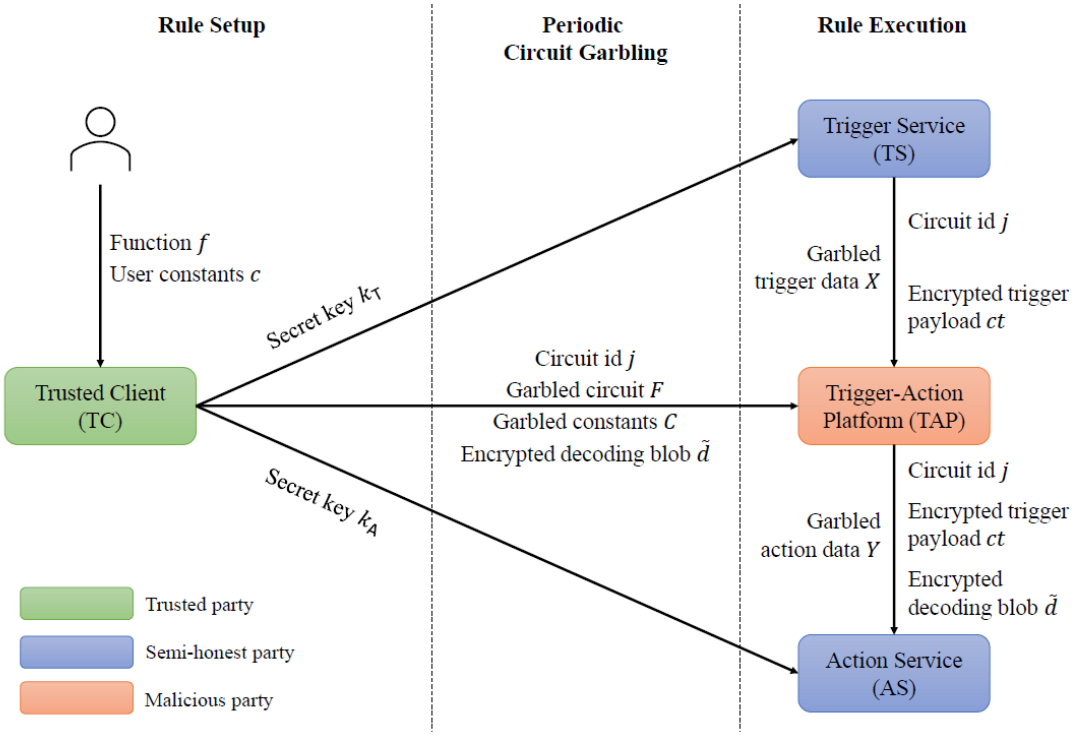
برای اجرای این پروتکل نیاز است تا کاربر روزانه حدود ۷۰ مگابایت داده مربوط به مدار درهم را آپلود نماید. این میزان در مقایسه با داده‌ی آپلود شده توسط کاربر در سکوهای عادی قابل‌توجه است.

۳- عدم پشتیبانی از حریم خصوصی در سطح رخداد یا عدم رخداد رهانا

پژوهش پیشنهادی، داده‌ها و پارامترهای رهانا و برنامه‌ی اینترنت اشیاء را محرمانه نگه می‌دارد. اما هیچ ایده‌ای در زمینه‌ی حریم خصوصی ناشی از رخداد یا عدم رخداد رهانا ندارد. در حقیقت در سکوی ETAP هم‌چنان بررسی‌های آماری و استخراج الگوی آماری رفتار کاربر برای سکوی ناامن قابل انجام است.

۴- نیاز به تغییر سکو، کارگزار کاربر، سرویس‌های رهانا و کنش

برای اجرای پروتکل مدار درهم لازم است تا تمامی چهار موجودیت سکو، زیرساخت رمزنگاری لازم برای پروتکل مدار درهم را پشتیبانی نمایند. اعمال این تغییر برای تعداد زیاد سرویس‌های رهانا و کنش دور از ذهن به نظر می‌رسد.



شکل ۱۵- معماری سکوی ETAP [۱۵]

۳-۴-۴ پژوهش‌های مبتنی بر سخت افزار امن

یکی از مسیرهای پژوهشی در مدل تهدید سکوی بدخواه، استفاده از بسترهای مورد اعتماد سخت‌افزاری است. در این میان برخی از پژوهش‌ها با استفاده از محیط اجرای قابل اعتماد (TEE)[۴۳] به این موضوع پرداخته‌اند. این محیط‌های سخت‌افزاری به آن‌ها اجازه می‌دهد تا محاسبه بر روی داده‌ی رهانا را با حفظ محرمانگی و صحت انجام دهند.

پژوهش Walnut (منتشرنشده)

در پژوهش[۱۴] ، شوتلر و همکاران، سکوی Walnut را ارائه نموده اند. Walnut سکویی است که کاربر با اعتماد اندک به آن می‌تواند تمامی کارکردهای مشابه سکوی IFTTT را داشته باشد.

فرضیات:

۱- سکو، بدخواهانه رفتار می‌کند.

۲- هدف این پژوهش حفظ حریم خصوصی و صحت برنامه‌ها به طور همزمان است.

مطابق شکل ۱۶، سکوی Walnut در ابتدا به دو بخش مستقل فیزیکی با نام‌های S1 و S0 تقسیم شده است. هر یک از این دو بخش بر روی محیط‌های جداگانه ای در IBM و Azure مستقر هستند. ایده‌ی Walnut آن است که پروتکل مدار درهم YAO را که یک پروتکل 2PC[۴۴] است بین S1 و S0 اجرا نماید. با این روش هیچ‌یک از دو بخش S0 و S1 به داده‌های حساس دسترسی نخواهند داشت. از سویی دیگر Walnut با هدف حفظ صحت، اجرای پروتکل را بر روی سخت‌افزارهای مورد اعتماد الزامی می‌داند. این سخت‌افزارها یک محیط اجرای قابل اعتماد (TEE) را ارائه می‌دهند که قادر به محاسبه به گونه‌ای است که هیچ موجودیت بیرونی نتواند صحت آن را خدشه‌دار نماید. البته با توجه به حملات فیزیکی که بر روی این سخت افزارها محتمل است، Walnut مجبور به استفاده از چند TEE از چند فروشنده‌ی مختلف شده است.

چالش‌ها:

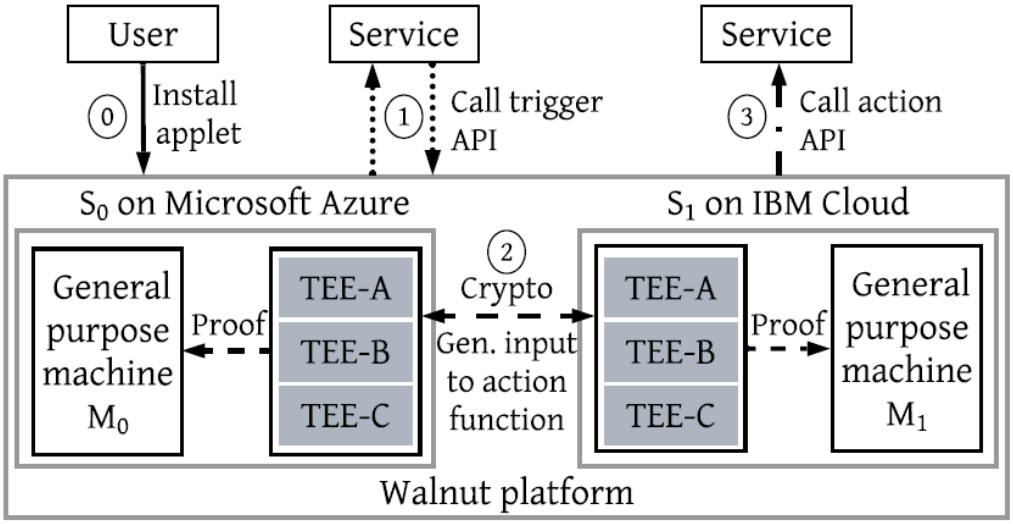
۱- قابلیت تبانی کارخواه‌های[۴۵] S1 و S0

[۴۳] Trusted Execution Environment

[۴۴] 2 Party Computation

[۴۵] Server

فرض Walnut بر آن است که جدا بودن کارخواهها موجب می‌شود تا با استفاده از 2PC امنیت حاصل گردد. این درحالی است که با تبانی کارخواه S1 و S0 تمامی تمهیدات اندیشیده شده از دست خواهد رفت.



شکل ۱۶- معماری سکوی Walnut [۱۴]

۲- سختی پیاده‌سازی سکوی Walnut

پیاده‌سازی مدل Walnut، نیازمند تغییرات فیزیکی در سطح کارخواهها، تبدیل سکو به دو کارخواه در دو محل فیزیکی و استفاده از سخت‌افزار مورد اعتماد است.

۳- نیاز به تغییر در سرویس‌های رهانا و کنش

سرویس‌های رهانا و کنش می‌بایست قابلیت‌های پشتیبانی از مدار درهم را داشته باشند که این موضوع نیازمند تغییر این سرویس‌ها است.

۴- وجود حملات بر روی زیرساخت‌های TEE [۲۱]

پژوهش PatrIoT

در پژوهش[۱۳] ، زاوالیشن و همکاران با درنظر گرفتن خطرات مرتبط با حریم خصوصی در سکوهای اینترنت اشیاء مدلی را با نام PatrIoT ارائه داده‌اند. ایده‌ی اصلی PatrIoT استفاده از پردازنده‌های SGX[۴۷] اینتل می‌باشد.

[۴۷] Software Guard Extensions

این مجموعه از پردازنده‌های اینتل می‌توانند، دسترسی غیرمجاز به داده‌های حساس کاربران را توسط تامین‌کنندگان ابری سکوهای اینترنت اشیاء محدود سازند. درواقع PatrIoT سعی دارد تا مالکیت کاربران بر روی داده‌های تولیدشده‌ی اینترنت اشیاء را به طور کامل تضمین نماید.

هم‌چنین این سکو تلاش می‌کند تا به کاربران این امکان را بدهد که خط‌مشی مشخصی را در سطح دستگاه‌های اینترنت اشیاء برای اشتراک‌گذاری داده‌های حساس خود، تعریف نمایند. در واقع PatrIoT جریان اطلاعات را پایش می‌نماید تا از نحوه‌ی استفاده‌ی داده‌های حساس توسط برنامه‌های اینترنت اشیاء مطمئن شود.

فرضیات:

۱- سکو، بدخواهانه رفتار می‌کند و سعی دارد تا حریم خصوصی کاربر را نقض نماید.

۲- توسعه‌دهندگان برنامه اینترنت اشیاء نیز بدخواهانه رفتار می‌کنند و سعی دارند تا حریم خصوصی کاربر را نقض نمایند.

مطابق شکل ۱۷، بخش اصلی سکوی پیشنهادی محیط حفاظت‌شده‌ی اجرای برنامه(TSAR[۴۸]) است که دستگاه‌های اینترنت اشیاء و برنامه موبایلی سکو به آن اتصال می‌یابند. حفاظت شده بودن TSAR به دو علت است:

۱- TSAR برروی یک بستر TEE درحال اجراست و زیرساخت نرم‌افزاری سکو را تامین می‌نماید. از این رو پردازه‌های خاص سیستم‌عامل[۴۹] نمی‌توانند به حافظه TSAR دست یابند و داده‌ی حسگرهای محیط را مشاهده کنند.

۲- دسترسی به سرویس TSAR صرفاً برای برنامه موبایلی سکو و دستگاه‌های هوشمند، محدود شده است.

باتوجه به توضیحات بالا در مورد حفاظت‌شده بودن TSAR، کاربر تنها می‌بایست به پیاده‌سازی نرم‌افزاری TSAR اطمینان یابد و از استقرار درست این پیاده‌سازی نرم‌افزاری بر روی بستر TEE مطمئن شود. این موضوع با متن‌باز بودن کد TSAR و نگه‌داری نسخه‌ای از آن بر بستر امن و مورداعتماد تضمین شده است.

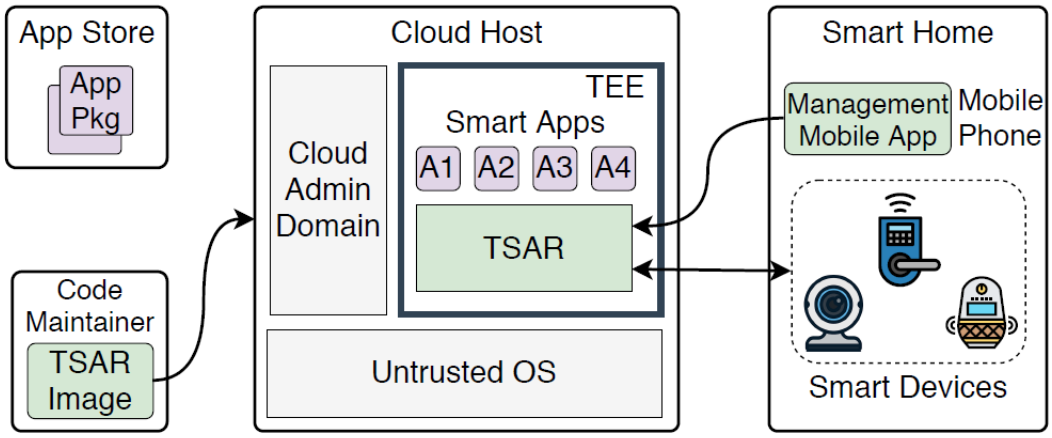
چالش‌ها:

۱- وجود حملات بر روی زیرساخت‌های TEE [۲۱]

[۴۸] TEE-protected Smart App Runtime (TSAR)

[۴۹] Privileged OS processes

۲- نیاز به تغییر سخت‌افزاری کارخواه سکو



شکل ۱۷- مدل پیشنهادی PatrIoT [۱۳]

۳-۵ جمع‌بندی

در

جدول ۱-۳ پژوهش‌های مرتبط با موضوع پیشنهاد رساله را می‌توان به صورت خلاصه مشاهده کرد. باتوجه به بررسی انجام‌شده، برخی از این پژوهش‌ها، از قابلیت محاسبه در سکو پشتیبانی نمی‌نمایند، این درحالی است که تعداد زیادی برنامه‌های اینترنت اشیاء با شرط محاسبه وجود دارد و هم‌اکنون در سکوها در حال استفاده است. برخی دیگر از پژوهش‌ها، تغییرات عمده‌ای در سرویس‌های برخط یا خود سکوی اینترنت اشیاء داده‌اند که اعمال این تغییرات فاصله قابل‌توجهی با اجرا در محیط واقعی دارد. از سویی دیگر برخی از راه‌کارهای پیشنهاد شده نیز سربار اجرایی قابل توجهی دارند که در عمل کارکرد سکوی اینترنت اشیاء را با اشکال مواجه می‌نماید. در فصل بعد با اشاره جزئی‌تر به برخی از نقاط ضعف موجود در راه‌کارهای پیشین، به بیان مسئله پژوهشی خود می‌پردازیم.

جدول ۱-۳ مقایسه‌ی پژوهش‌های مرتبط با رساله

ردیف	مقاله	مساله	روش	پشتیبانی از محاسبه	عدم تغییر در سرویس‌ها	عدم تغییر در سکو	سربار قابل قبول
1	F&F [11]	حفظ حریم خصوصی نسبت به سکوهای شخص ثالث متصل به اسمارت‌تینگز	فیلتر نمودن رخدادهای غیرضروری برای IFTTT تغییر داده خام به صورت تصادفی تا رسیدن به توزیع نرمال	✓	✓	×	✓
2	OTAP [12]	حفظ حریم خصوصی در سکوی IFTTT	ارسال رهاناهای جعلی به سکو و استفاده از رمزنگاری	×	×	✓	×
3	ATAP [12]	حفظ حریم خصوصی در سکوی IFTTT	استفاده از رمزنگاری و توافق کلید بین سرویس رهانا و کنش	×	×	×	✓
4	PatrIoT [13]	حفظ حریم خصوصی در سکوی IFTTT	مبتنی بر محیط سخت افزاری TEE	✓	✓	×	×
5	Walnut [14]	حفظ حریم خصوصی و جامعیت در سکوی FTTT	مبتنی بر محیط سخت افزاری TEE استفاده از الگوریتم‌های ۲PC استقرار دو سرور مستقل به صورت فیزیکی	✓	×	×	×
6	ETAP [15]	حفظ حریم خصوصی در سکوی IFTTT	اسفاده از مدار درهم	✓	×	×	×

فصل چهارم

پیشنهاد رساله

در سال‌های اخیر سکوهای رهانا-کنش اینترنت اشیاء کاربردهای متنوع و کاربران گسترده‌ای یافته اند. سکو IFTTT با دارا بودن بیش از ۲۰ میلیون کاربر، میزبان بیش از ۶۰۰ عدد سرویس مختلف برای خودکارسازی در محیط‌های متنوع است [۴]. سکوهای دیگر نظیر نود-رِد علاوه بر کاربرد در محیط‌های هوشمند خانگی، کاربرد گسترده‌ای در محیط‌های اینترنت اشیاء صنعتی[۱] نیز یافته‌اند[۵۲]. کاربرد نود-رِد در محیط‌های اینترنت اشیاء شامل راه‌کارهای تجاری این محیط نظیر مالتی‌تک[۲][۵۳] ، OPT22[۵۴] و آی‌اِکانکت[۳][۵۵] نیز شده است.

علی‌رغم استفاده گسترده و کاربردهای متنوع سکوهای رهانا-کنش، این سکوها کم‌تر مورد ارزیابی امنیتی قرار گرفته‌اند. یکی از نقاط ضعف جدی در طراحی این سکوها، امکان نقض حریم خصوصی گسترده برروی داده‌های حساس کاربران، در صورت وقوع رخداد حمله و یا بدخواه‌بودن خود این سکوها است. در این فصل ابتدا به شرح ساختار، شاکله و مشخصات برنامه اینترنت اشیاء و سکوی اینترنت اشیاء می‌پردازیم. سپس مسئله پژوهشی را با ذکر دو نمونه الگوی نقض حریم خصوصی در سکوهای اینترنت اشیاء شرح می‌دهیم. در ادامه با بیان راه‌کار پیشنهادی خود مبتنی بر تحلیل کد برنامه و بررسی مدل حریم‌خصوصی k-گمنامی، به بیان چالش‌های پیش‌رو و اهداف پژوهشی این رساله می‌پردازیم.

۴-۱ ساختار برنامه و سکوی اینترنت اشیاء

۴-۱-۱ ساختار برنامه در سکوهای اینترنت اشیاء

سکوهای رهانا-کنش این قابلیت را به کاربر می‌دهند تا به توسعه‌ی برنامه‌های خودکارسازی محیط اینترنت اشیاء بپردازند. ما با بررسی ساختار برنامه‌های اینترنت اشیاء در سکوهای مختلف، سه عنصر را در این برنامه‌ها شناسایی کردیم. این سه عنصر مستقل از معماری سکوها و زبان برنامه‌نویسی، در ساختار برنامه‌ها حضور دارند.

۱- رهانای برنامه

در هربرنامه اینترنت اشیا، رویداد مشخصی به عنوان رهانای برنامه تعریف می‌شود. مستقل از این که رویداد توسط خود دستگاه اینترنت اشیاء، هاب و یا سرویس برخط مرتبط با دستگاه ارسال شده باشد، رویداد دریافتی و داده‌های آن، ورودی برنامه اینترنت اشیاء خواهند بود. برای مثال شکل ۴ را که نمونه‌ای از کد یک برنامه

[۱] IIoT
[۲] MultiTech
[۳] Iaconnects

اسمارت‌اپ است درنظر بگیرید در این برنامه دستگاهی با توانمندی تشخیص حرکت توسط کاربر تعریف می‌گردد (خط ۸-۱۰). سپس رهانای این برنامه که رویداد تشخیص یک حرکت توسط حسگر است با استفاده از تابع زیر تعریف شده است (خط ۲۴-۲۶):

Subscribe(themotion, “motion.active”, motionDetectedHandler)

به طور مشابه مثال موجود در شکل ۵ را که یک برنامه در سکوی IFTTT است، درنظر بگیرید. در این برنامه در بخش رهانا، سرویس تقویم گوگل انتخاب شده است که به ازای هر رویداد در حال آغاز، داده‌های آن را برای سکو ارسال می‌نماید. مطابق شکل ۱۸، داده‌های رهانای مربوط به تقویم گوگل دیده می‌شود، این داده‌ها در پنل توسعه برنامه‌ی سکو لیست شده‌اند تا بتوان با استفاده از آن‌ها بخش محاسبه برنامه را توسعه داد.

Trigger data

```
GoogleCalendar.anyEventStarts.Title
GoogleCalendar.anyEventStarts.Description
GoogleCalendar.anyEventStarts.Where
GoogleCalendar.anyEventStarts.Starts
GoogleCalendar.anyEventStarts.Ends
GoogleCalendar.anyEventStarts.EventUrl
GoogleCalendar.anyEventStarts.VideoCallUrl
```

شکل ۱۸- لیست داده‌های رهانای برنامه اینترنت اشیاء شکل ۵

۲- محاسبه برنامه

به طور معمول منطق برنامه‌های اینترنت اشیاء شامل دو بخش است. بخش اول شرط محاسباتی است. در این بخش یک یا چند عبارت منطقی که شرایط اجرای برنامه هستند، بررسی می‌گردد. در صورت صادق بودن این شرایط براساس داده‌های دریافتی از رهانا، برنامه اجرا می‌گردد. بخش دوم ، بخش مرتبط با کنش برنامه است، در این بخش براساس داده‌های رهانا، دستور کنش مربوطه ساخته می‌شود و به سرویس کنش یا دستگاه اینترنت اشیاء ارسال می‌گردد.

این نکته نیز لازم به ذکر است که برخی از برنامه‌های اینترنت اشیاء به طور کلی منطق و شرط محاسباتی ندارند و به طور کاملا ساده صرفا در ازای رخ دادن یک رهانای مشخص، یک کنش مشخص و از پیش تعیین شده را مستقل از داده‌های ورودی رهانا اجرا می‌نمایند.

در شکل ۱۹، نمونه ای از فیلتر کد یک برنامه IFTTT را مشاهده می‌نمایید. در این فیلتر کد بخش اول مربوط به شرایط محاسباتی لازم برای اجرای برنامه است (خط ۱۱). در این بخش میزان روشنایی محیط به عنوان شرط اجرای برنامه بررسی می‌گردد. در صورت آن که محیط بیش از حد آستانه روشن باشد و نیازی به روشن نمودن لامپ هوشمند نباشد، کنشی در ارتباط با لامپ هوشمند رخ نمی‌دهد و پیامی با ساختار مشخص (خط ۵-۹)، برای کاربر در سکوی اینترنت اشیاء ذخیره می‌شود. بخش دوم کد، بخش مرتبط با کنش برنامه است.

```
1.  let location = GoogleCalendar.eventFromSearchStarts.Where
2.  let aboveThreshold = 100;
3.  let currentLum = Number(Weatherflow.historyOfObservations[0].Brightness);
4.
5.  let time_unlocked = moment(Smartthings.unlockedSmartthings.UnlockedAt,'MMMM D, YYYY at
6.  h:mmA').format("HH:mm");
7.
8.  var msg = 'Door unlocked at ' + time_unlocked + ' and it is currently ' + currentLum + 'lum above the ' +
9.  aboveThreshold + 'lum threshold.';
10.
11. if (currentLum > aboveThreshold){
12.    Smartthings.turnOnSmartthings.skip(msg)
13. }
```

شکل ۱۹-شرط محاسباتی و بخش مرتبط با کنش در فیلتر کد یک برنامه سکوی IFTTT

۳- کنش برنامه

هر برنامه اینترنت اشیاء دارای یک کنش است که خروجی اجرای برنامه را به صورت تغییر در محیط فیزیکی یا سرویس برخط منعکس می‌نماید. کنش برنامه‌های اینترنت اشیاء می‌تواند روشن/خاموش شدن یک دستگاه (به عنوان نمونه لامپ هوشمند)، تغییر پارامتر تنظیم‌کننده یک دستگاه (به عنوان نمونه پارامتر دمای ایده‌آل برای دستگاه تهویه هوا)، کنشی در یک سرویس برخط (به عنوان نمونه ارسال یک ایمیل) و یا اعلان شرایط محیط به کاربر باشد.

۴-۱-۲ داده‌های حساس موجود در سکوهای اینترنت اشیاء

ما داده‌های موجود در سکوهای اینترنت اشیاء را مورد بررسی قرار دادیم. مطابق انواع مختلف داده‌ها در سکوی اسمارت‌تینگز پشتیبانی می‌شوند. از منظر حساسیت داده‌ها، می‌توان این داده‌ها را در سه دسته تقسیم

نمود [۱۵]:

۱- داده‌های عمومی

داده‌هایی نظیر وضعیت آب و هوا، زمان طلوع و غروب خورشید و داده‌های عمومی که از سرویس‌های برخط قابل دریافت هستند و در برخی از برنامه‌های اینترنت اشیاء در بخش شرط محاسباتی استفاده می‌شوند.

۲- داده‌های حساس

بخش عمده‌ای از داده‌ی حسگرها، داده‌ی سرویس‌های برخط کاربر نظیر ایمیل و تقویم داده‌های حساس کاربر محسوب می‌شوند.

۳- داده‌های حساس به زمان

منظور از این داده‌ها، داده‌هایی است که زمان وقوع آن‌ها دارای حساسیت است. برای مثال رویداد عدم حضور[۴] در یک خانه را درنظر بگیرید. زمانی که حسگر حضور[۵] وضعیت عدم حضور برای یک محیط فیزیکی را به سکو ارسال می‌نماید، زمان رخ دادن این رویداد خود دارای حساسیت است.

جدول ۱-۴ - انواع داده‌های مورد پذیرش در سکوی اسمارت‌تینگز [۵۹]

Data Type	Example	Description
STRING	"This is a String"	Represents character strings
NUMBER	`5`, `10.67`	The Number data type is a guideline indicating that a number should be expected, and not a specific type. Device Handlers contain the implementation of what kind of number object is actually returned.
VECTOR3	`(x,y,z)`	This Data Type is a representation of x,y,z coordinates in space. Device Handlers contain the implementation of the actual data structure, but it is usually as a Map: `[x: 0, y: 0, z: 0]`.
ENUM	"one", "two", "three"	The Enum Data Type is a static set of predefined String values that an Attribute can have, or that a Command can accept as an argument.
DYNAMIC_ENUM	"Any", "value"	Much like the Enum Data Type, Dynamic Enum is a set of String values. However, the set is not static or predefined.
COLOR_MAP	`[hue: 50, saturation: 75]`	The Color Map is a Map specifically for the use of color control. As such, the Map should contain a Hue and a Saturation value.
JSON_OBJECT		A standard JSON object. Device Handlers contain the implementation and thus should be consulted when looking for the JSON object structure.
DATE		A Date, usually represented as a java.util.Date object.
BOOLEAN	true, false	A boolean data type with a value of true or false.

[۴] معادل وضعیت Sensor.presence= Unpresent

[۵] Presence Sensor نوعی از حسگرهای محیطی هستند که دقت بالاتری از حسگرهای تشخیص حرکت دارند و حضور یا عدم حضور افراد را تشخیص می‌دهند.

۴-۱-۳ عملگرهای محاسباتی موجود در سکوهای اینترنت اشیاء

عملگرهای محاسباتی، در بخش شرط محاسباتی برنامه‌های اینترنت اشیاء کاربرد دارند. در سکوی IFTTT در فیلتر کد یک برنامه، می‌توان یک کد تایپ‌اسکریپت نوشت که محدودیتی در تعریف عملگرهای محاسباتی ندارد. در سکوی اسمارت‌تینگز نیز می‌توان کد گرووی نوشت که محدودیتی در تعریف عملگرهای محاسباتی ندارد. پژوهش[۱۵] با بررسی مجموعه‌ای از برنامه‌های پرطرفدار سکوی IFTTT و زپیر، جدول ۲-۴ را، که نمایانگر عملگرهای محاسباتی این برنامه‌هاست، ارائه نموده است. عملگرهای منطقی، عملگرهای پایه ریاضی و عملگرهای مربوط به پردازش رشته در این برنامه‌ها استفاده شده‌اند.

جدول ۲-۴- عملگرهای استفاده شده در مجموعه برنامه‌های IFTTT و زپیر [۱۵]

Type	Operation	Description
Bool	`x | a`	x OR y
	`x & a`	x AND y
	`! x`	NOT x
Num	`x < n`	Is x *less than* n?
	`x > n`	Is x *greater than* n?
	`x.mathop(n)`	Basic math ops. $(+, -, \times, \div)$
	`x.format()`	Format x into a string
Str	`x == s`	Does x *exactly match* the string s
	`x.contain(s)`	Does x *contain* the string s
	`x.startwith(s)`	Does x *start with* the string s
	`x.endwith(s)`	Does x *end with* the string s
	`x.split(d, i)`	Split x using delimiter string d and select the i-th substring
	`x.replace(s, t)`	Replace all occurrences of s in x with t
	`x.to_lowercase()`	Convert all characters in x to lowercase
	`x.truncate(n)`	Truncate x to size n
	`x.extract_phone()`	Extract the first phone number found in x
	`x.extract_email()`	Extract the first email address found in x
	`x.strip_html()`	Remove all HTML tags in x
	`x.html2markdown()`	Convert all HTML tags in x to Markdown
	`m.lookup(x)`	Look up the value for the key x in a user-provided map m
Any	`x == null`	Does x *exist*?
	`x.default(y)`	Set value of x to y if it does not exist

۴-۲ شرح مسئله پژوهشی

در این بخش باتوجه به ساختار و مشخصات سکوهای اینترنت اشیاء و برنامه‌های اینترنت اشیاء که پیش از این شرح داده شد، نشان می‌دهیم که ساختارهای کنونی دارای نقاط ضعفی هستند که الگوهای نقض حریم‌خصوصی

را در سکوها به وجود می‌آورند. هم‌چنین با بررسی نقاط ضعف پژوهش‌های پیشین، چالش‌های باز این حوزه را بررسی می‌نماییم. درنهایت اهداف پژوهشی این پیشنهاد رساله را بیان می‌نماییم.

۴-۲-۱ نقض حریم‌خصوصی در سکوهای اینترنت اشیا

ما به عنوان نمونه مطالعاتی با بررسی سکوی اسمارت‌تینگز و IFTTT، دو مورد از الگوهای نقض حریم‌خصوصی و نقض اصل حداقل دسترسی[۶] [۵۸] را در این سکوها به نمایش گذاشته‌ایم:

۱- ریزدانه‌نبودن دسترسی دریافت اطلاعات از حسگرها
۲- داده‌های غیرصادق در شرط برنامه

این الگوهای مطرح‌شده، در سکوهای دیگر اینترنت اشیاء نیز قابل تعریف هستند. شکل ۲۰، یک نمونه از برنامه‌های اینترنت اشیاء در سکوی اسمارت‌تینگز است. این برنامه، برنامه‌ای مرتبط با خودکارسازی یک پارکینگ هوشمند است که با تشخیص باز ماندن درب پارکینگ با استفاده از حسگر چندمنظوره‌ی[۷] موجود بر درب، پیامک یا اعلانی[۸] را برای کاربر ارسال می‌نماید. در شکل ۲۰ بخشی از این برنامه آورده شده است؛ کدمنبع کامل این برنامه در [۵۶] موجود است.

۴-۲-۱-۱ ریزدانه‌نبودن دریافت اطلاعات از حسگرها

منظور از ریزدانه نبودن دریافت اطلاعات از حسگرها آن است که سکوی اسمارت‌تینگز، پس از طی فرآیند اتصال یک دستگاه جدید اینترنت اشیاء، تمامی اطلاعات قابل دریافت از آن دستگاه را به طور کامل و مستقل از نیاز برنامه‌های اینترنت اشیاء کاربر دریافت می‌نماید.

به عنوان نمونه حسگرهای چندمنظوره اینترنت اشیاء توانمندی‌های متنوعی نظیر اندازه‌گیری دما، تشخیص حرکت، رطوبت و موقعیت مکانی را دارند [۵۷]. محیط اینترنت اشیاء را فرض نمایید که شامل یک حسگر چندمنظوره است. کاربر این محیط اینترنت اشیاء، تنها برنامه شکل ۲۰ را در سکوی اسمارت‌تینگز فعال کرده است. در این برنامه، تنها از توانمندی[۹] موقعیت مکانی(threeAxis) این حسگر چندمنظوره برای خودکارسازی

[۶] Least Priviledge
[۷] Multipurpose Sensor
[۸] Notification
[۹] Capability

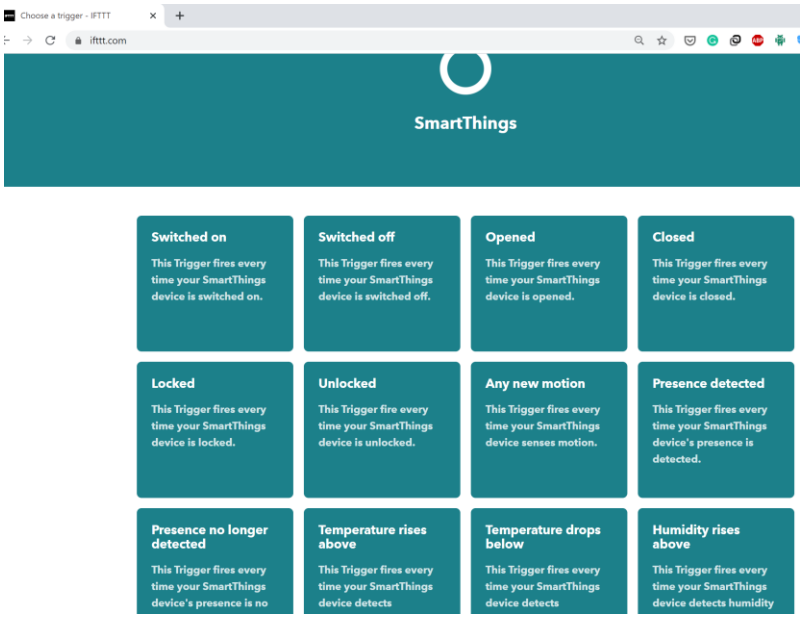
محیط استفاده شده است (خط۳). این درحالی است که تمامی داده‌های حسگر چندمنظوره به طور متناوب به سکوی اسمارت‌تینگز انتقال می‌یابد. ما برای اطمینان از این موضوع، با اتصال سکوی اسمارت‌تینگز به سکوی IFTTT مشاهده کردیم که تمامی اطلاعات این حسگر چندگانه در سکوی IFTTT نیز قابل دسترس خواهد بود؛ این موضوع در شکل ۲۱ قابل مشاهده است. به‌بیان دیگر حسگر چندمنظوره تمامی اطلاعات حساس کاربر نظیر تشخیص حرکت، دما و رطوبت را فارغ از نیاز و ارتباط به برنامه‌های اینترنت اشیاء موجود در اختیار سکوی اسمارت‌تینگز قرار می‌دهد.

```
1.  preferences {
2.                  section("When the garage door is open...") {
3.                  input "multisensor", "capability.threeAxis", title: "Which?"
4.          }
5.          section("For too long...") {
6.                  input "maxOpenTime", "number", title: "Minutes?"
7.          }
8.          section("Text me at (optional, sends a push notification if not specified)...") {
9.      input("recipients", "contact", title: "Notify", description: "Send notifications to") {
10.       input "phone", "phone", title: "Phone number?", required: false
11.     }
12.         }
13. }
14. .
15. .
16. .
17. .
18. def accelerationHandler(evt) {
19.         def latestThreeAxisState = multisensor.threeAxisState // e.g.: 0,0,-1000
20.         if (latestThreeAxisState) {
21.                 def isOpen = Math.abs(latestThreeAxisState.xyzValue.z) > 250
```

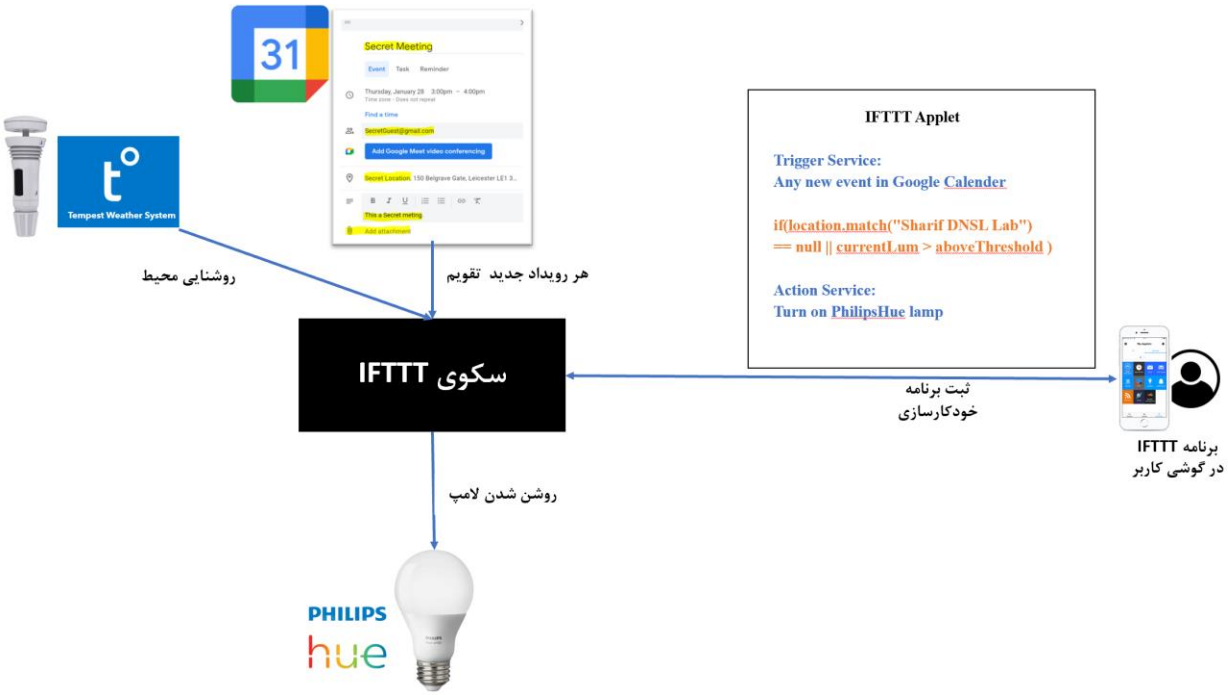
شکل ۲۰-بخش از برنامه اعلام بازبودن درب پارکینگ با استفاده از حسگرچندگانه

برای بررسی این الگوی نقض حریم خصوصی در سکوی IFTTT، برنامه اینترنت اشیاء موجود در شکل ۲۲ را درنظر بگیرید. توسعه این برنامه پیش از این در شکل ۵ و فیلترکد آن در شکل ۶ معرفی شده بود. این برنامه برای رویدادهای موجود در تقویم گوگل که مکان رویداد موردنظر «Sharif DNSL Lab» باشد و در همان زمان که محیط آزمایشگاه امنیت داده شریف به اندازه کافی روشن نباشد، لامپ هوشمند محیط را روشن می‌نماید. منطبق بر، تمامی اطلاعات مربوط به رویدادهای موجود در تقویم گوگل کاربر برای سکوی IFTTT ارسال می‌شود، این درحالی است که سکوی IFTTT برای اجرای این برنامه خودکارسازی تنها به مکان برگزاری رویداد نیاز دارد. به بیان دیگر مطابق شکل ۲۲، داده‌های حساس دیگر موجود در یک رویداد، شامل عنوان رویداد، زمان رویداد،

شرکت‌کنندگان رویداد، توصیف رویداد و ضمیمه رویداد که حاوی داده‌های حساس کاربر است بدون دلیل در اختیار سکوی IFTTT قرار می‌گیرد و موجب نقض حریم‌خصوصی کاربر می‌گردد.



شکل ۲۱- دسترسی‌های موجود در سکوی IFTTT پس از اتصال به سکوی اسمارت تینگز



شکل ۲۲ - ساختار برنامه IFTTT شکل ۵ و داده‌های حساس ارسالی به آن

۴-۲-۱-۲ داده‌های غیرصادق در شرایط برنامه

به طور معمول، بسیاری از برنامه‌های توسعه‌یافته در سکوهای اینترنت اشیاء، دارای یک یا چند شرط محاسباتی هستند. این شرایط محاسباتی، تعیین‌کننده اجرا یا عدم اجرای برنامه است. به عنوان نمونه شرط محاسباتی برای برنامه شکل ۲۲ عبارت منطقی زیر است:

If (location.match("Sharif DNSL Lab") == null|| currentLum > aboveThreshold)

سکوهای اینترنت اشیاء نسبت به حسگرهای متفاوت، دو حالت کاری متفاوت دارند [15]. حالت کاری اول، حالت نمونه‌برداری[۱۰] است در این حالت سکوی اینترنت اشیا، داده‌ی حسگر را به طور متناوب در بازه‌های از پیش‌تعیین شده، دریافت می‌کند. برای نمونه سکوی اینترنت اشیاء برای حسگرهای دما، رطوبت و روشنایی در حالت نمونه‌برداری است و داده‌های این حسگرها در بازه‌های زمانی کوتاه، به طور متناوب دریافت می‌شود.

حالت دوم، حالت پیشران[۱۱] است. در این حالت به ازای رخ دادن یک رویداد، داده‌ی جدید توسط دستگاه اینترنت اشیاء برای سکو ارسال می‌شود. برای نمونه سکوی اینترنت اشیاء برای حسگرهای تشخیص حرکت در حالت پیشران است و به ازای هربار تشخیص حرکت، رخداد مربوطه را برای سکو ارسال می‌نماید.

در حالت اول که سکو دریافت‌کننده متوالی داده‌های حسگر است. تنها داده‌هایی برای سکو ارزش اجرایی دارند که در شرط محاسباتی برنامه‌های مربوطه صدق کنند. به عنوان نمونه در مورد برنامه شکل ۲۲ ممکن است، در طول یک ماه، فقط یک رویداد با مکان آزمایشگاه امنیت داده شریف وجود داشته باشد و یا تنها یک بار در ماه رویدادی در آزمایشگاه برقرار و هم‌زمان میزان روشنایی محیط نیز کم‌تر از حد آستانه باشد؛ با این‌حال در سکوهای اینترنت اشیاء کنونی برای برنامه شکل ۲۲، در طول ماه تمامی رویدادهای موجود در تقویم کاربر و میزان روشنایی آزمایشگاه به طور متناوب با دوره زمانی کوتاه به سکو ارسال می‌شود. این داده‌های ارسالی، می‌تواند زمینه‌ساز نقض حریم‌خصوصی و تشکیل پروفایل رفتاری کاربر باشد، برای نمونه میزان روشنایی محیط که به طور متناوب توسط سکو دریافت می‌شود، می‌تواند الگوی حضور یا عدم حضور افراد را در محیط آزمایشگاه مشخص نماید.

موارد ذکر شده در بالا، الگوهای موردی از نقض حریم‌خصوصی در سکوهای اینترنت اشیاء می‌باشد. به طورکلی، تجمیع داده‌های کاربر در سکوهای اینترنت اشیاء، امکان ساخت پروفایل رفتاری کاربر و نقض حریم

[۱۰] Polling

[۱۱] Push mode

خصوصی را برای سکوی بدخواه اینترنت اشیاء موجب می‌شود. از سویی دیگر، تجمیع این داده‌ها در یک سکوی اینترنت اشیاء به طور متمرکز، هدف جذابی برای مهاجمین سایبری خواهد بود.

۴-۲-۲ مسائل مرتبط با سکوهای اینترنت اشیا

علاوه بر حفظ حریم خصوصی، سه دغدغه جدی دیگر نیز در ارتباط با سکوهای اینترنت اشیاء وجود دارد:

۱- صحت داده‌ی دریافتی از حسگرها

برنامه‌های اینترنت اشیاء بر مبنای داده‌های دریافتی از حسگرها اجرا می‌شوند و تغییراتی را در محیط فیزیکی ایجاد می‌کنند. درصورتی که داده‌ی دریافتی، داده غیرواقعی باشد و یا بنابر خرابی دستگاه ، نوسان برق یا هر علت دیگری داده‌ی ارسالی توسط حسگر اینترنت اشیاء ناهنجاری تلقی شود، منجر به اجرای اشتباه برنامه اینترنت اشیاء می‌گردد و می‌تواند نقض ایمنی را در محیط فیزیکی موجب شود.

۲- صحت اجرای برنامه

منظور از صحت اجرای برنامه آن است که با فرض بدخواه بودن سکوی اینترنت اشیاء و یا نفوذ یک مهاجم بدخواه به سکو، هم‌چنان اجرای برنامه تحت شرایط درست، صورت پذیرد. نقض صحت اجرای برنامه زمانی رخ می‌دهد که مهاجم بدخواه بتواند از توکن‌های دسترسی کاربر سواستفاده نماید و بدون وجود یک رهانای معتبر، کنش مربوطه را با توکن دسترسی فراخوانی نماید. از سویی دیگر در مدلِ تهدید سکوی بدخواه، سکو می‌تواند با تغییر در داده‌ی رهانای ورودی، مسیر اجرای برنامه را تحت تاثیر قرار دهد و صحت اجرای برنامه را نقض نماید.

۳- قابلیت اطمینان[۱۲] اجرای برنامه در محیط فیزیکی

منظور از قابلیت اطمینان اجرای برنامه در محیط فیزیکی آن است که کنش‌های یک برنامه اینترنت اشیاء به درستی در محیط فیزیکی اجرا شود. اجرای واقعی کنش‌های برنامه در محیط فیزیکی ممکن است بنابر عوامل متعددی نظیر قطع اینترنت، خرابی دستگاه و تداخل با کنش‌های برنامه‌های دیگر دچار اختلال گردد. از آن‌جا که برنامه‌های اینترنت اشیاء با محیط فیزیکی تعامل دارند، اختلال در اجرای برنامه‌ها ممکن است موجب نقض خسارت‌بار ایمنی و امنیت گردد.

[۱۲] Reliability

۴-۲-۳ ضعف راه‌کارهای حفظ حریم خصوصی کنونی

۴-۲-۳-۱ درنظر نگرفتن برنامه اینترنت اشیاء

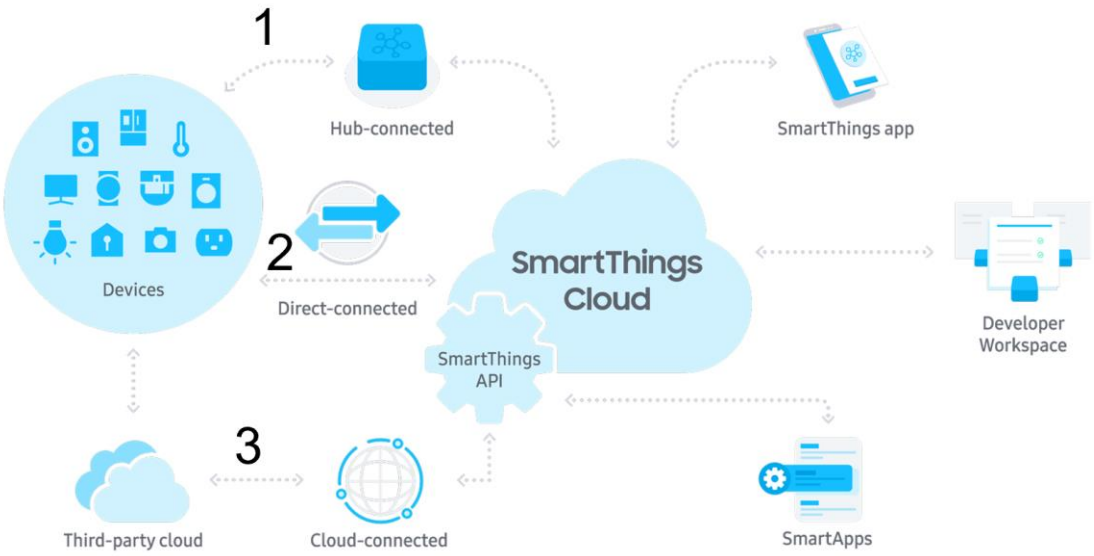
مطابق با پژوهش‌های پیشین که در فصل سوم مورد بررسی قرار گرفت، راه‌کارهای مختلفی برای حریم خصوصی در سکوهای اینترنت اشیاء پیشنهاد داده شده است. هریک از این راه‌کارها، چالش‌ها و سربار مشخصی دارند و برای دسته‌ای خاص از داده‌های موجود در برنامه‌ها مناسب‌تر هستند. به عنوان نمونه، ایده‌ی راهکار OTAP [۱۲]، با ایجاد رهاناهای جعلی، سعی دارد تا وجود یا عدم وجود رهاناهای واقعی را پنهان‌سازد و امکان نقض حریم خصوصی کاربر با استفاده از تحلیل آماری رهاناهای ورودی را از سکوی اینترنت اشیاء بگیرد. راه‌کارOTAP به طور مشخص برای داده‌ی حسگرهایی مناسب است که در حالت کاری پیشران با سکو در ارتباط هستند و صرفا با رخ دادن یک رویداد جدید داده‌ی خود را برای سکو ارسال می‌کنند. به بیان دیگر برای دستگاه‌های اینترنت اشیاء در حالت پیشران، راهکار OTAP معنادار است و برای حسگرهایی که در حالت نمونه برداری با سکو تعامل دارند و به طور متناوب داده‌های خود را به سکو ارسال می‌کنند کاربردی ندارد.

به طور مشابه راه‌کار ETAP [۱۵]، با اضافه کردن زیرساخت رمزنگاری و پروتکل مدار درهم، سعی نموده تا تمام داده‌های ارسالی به سکوی اینترنت اشیاء را رمز نماید. این درحالی است که برای حسگرهایی نظیر حسگر تشخیص حضور، صرفا رخداد یا عدم رخداد حضور اهمیت دارد و رمزشده بودن یا نبودن آن کمکی به حفظ حریم خصوصی در حضور سکوی بدخواه نمی‌کند.

از این رو راه‌کارهای ارائه شده پیش از این، به طور کلی و بدون درنظر گرفتن برنامه اینترنت اشیاء سعی داشته‌اند تا تغییر کلی را در سکوی اینترنت اشیاء ایجاد نمایند و حریم خصوصی کاربر را حفظ کنند که به نظر فاصله قابل‌توجهی با یک طرح قابل قبول و عملی داشته‌اند. ما در راهکار پیشنهادی خود برنامه اینترنت اشیاء را مبنا قرار داده‌ایم و با بررسی محتوای برنامه، راه‌کارهای حفظ حریم خصوصی متفاوتی را پیشنهاد می‌دهیم.

۴-۲-۳-۲ معماری متفاوت سکوهای اینترنت اشیاء

چالش دیگری در این حوزه که تاکنون به آن پرداخته نشده است، معماری‌های متفاوت سکوهای اینترنت اشیاء است. شکل ۲۳، مسیرهای ارتباطی دستگاه‌های اینترنت اشیاء در سکوی اسمارت‌تینگز را نشان می‌دهد. در این شکل سه مسیر متفاوت برای ارتباط دستگاه‌ها با سکو در نظر گرفته شده است.



شکل ۲۳- مسیر های ارتباطی دستگاه‌های اینترنت اشیاء در سکوی اسمارت‌تینگز [۵۹]

۱- مسیر ارتباط با هاب متصل به سکو

این مسیر ارتباطی، به طور خاص برای دستگاه‌هایی طراحی شده است که دارای محدودیت منابع هستند و می‌خواهند با پروتکل‌های کم‌مصرف‌تر ارتباطی نظیر Zigbee و Z-wawe فعالیت کنند. البته هاب اینترنت اشیاء اسمارت‌تینگز از پروتکل Wifi نیز پشتیبانی می‌نماید و قابلیت اجرای برخی از محاسبات را به صورت محلی در خود دارد.

۲- مسیر ارتباط مستقیم دستگاه اینترنت اشیاء با سکو

در این مسیر ارتباطی، دستگاه اینترنت اشیاء به طور مستقل به سکو متصل شده و داده‌های خود را برای سکو ارسال می‌نماید و دستورات مربوط به کنش‌ها را نیز از سکو دریافت می‌کند.

۳- مسیر ارتباط با سرویس ابری متصل به سکو

در این مسیر ارتباطی دستگاه اینترنت اشیا، صرفا با سرویس ابری خود ارتباط دارد و تعامل با سکوی اینترنت اشیاء به طور کامل مبتنی بر سرویس ابری دستگاه پیش‌خواهد رفت.

مطابق شکل ۲ معماری سکوی اینترنت اشیاء IFTTT کاملا متفاوت است و مشابه مسیر ارتباطی سوم در شکل ۲۳ است. تفاوت در معماری و مسیرهای ارتباطی سکوها، نیازمند درنظر گرفتن جزئیات در راه‌کارهای حفظ حریم

خصوصی برای این سکوهاست. تاکنون تمامی پژوهش‌های ارائه شده، راه‌کار خود را برای معماری سکوهای اینترنت اشیاء نظیر IFTTT ارائه داده‌اند که صرفا با سرویس‌های برخط ابری ارتباط دارد.

۴-۲-۳-۳ درنظر نگرفتن خط‌مشی حریم‌خصوصی کاربر

مطابق با بررسی‌های انجام شده در فصل سوم، پژوهش‌های پیشین، خط‌مشی حریم خصوصیِ کاربر را در تعامل با سکوهای اینترنت اشیاء درنظر نگرفته‌اند. تنها پژوهش PatrIoT [۱۳] ترجیحات حریم‌خصوصی[۱۳] کاربر را دریافت می‌نماید که البته این پژوهش نیز ترجیحات حریم‌خصوصی را در ارتباط با حفظ حریم‌خصوصی نسبت به برنامه‌های اینترنت اشیاء و نه نسبت به سکوی اینترنت اشیاء درنظرگرفته است.

۴-۲-۳-۴ حمله پیش‌زمینه[۱۴]

یکی از حملات شناخته‌شده در حفظ حریم‌خصوصی حمله پیش‌زمینه است[۶۳]. در این حمله مهاجم برروی جداول اطلاعات موجود تحلیلی را صورت می‌دهد و اطلاعات جدیدی را استخراج می‌کند که منجر به نقض حریم‌خصوصی می‌گردد. برای نمونه سکوی بدخواه می‌تواند از همبستگی[۱۵] موجود بین دستگاه‌های اینترنت اشیاء در یک محیط واحد استفاده نماید و درحالی که به داده‌ی یک حسگر خاص دسترسی ندارد، داده‌ی آن حسگر را استنتاج نماید مثلا از همبستگی حسگر شدت روشنایی می‌توان وضعیت لامپ هوشمند موجود در همان محیط را استنتاج نمود. مطابق با بررسی‌های انجام شده در فصل سوم، پژوهش‌های پیشین نظیرOTAP [۱۲] ، حمله پیش‌زمینه را درنظر نگرفته‌اند.

۴-۲-۴ اهداف پژوهشی

باتوجه به مواردی که در ارتباط با مسئله پژوهشی ذکر شد، اهداف رساله به صورت زیر تعریف می‌شود:

- ارائه راه‌کار حافظ حریم‌خصوصی داده‌های حساس کاربر در سکوهای اینترنت اشیاء غیرقابل‌اعتماد با شرایط زیر:
  - حفظ حریم‌خصوصی مبتنی بر خط‌مشی/ترجیحات حریم‌خصوصی کاربر
  - اختصاصی‌سازی سازوکار حریم خصوصی مبتنی بر تحلیل کد برنامه

[۱۳] Privacy Preference
[۱۴] Foreground attack
[۱۵] Corrolation

- حفظ کاربردپذیری سکوی اینترنت اشیاء
- پشتیبانی از معماری‌های متفاوت سکوهای اینترنت اشیا
- عدم تغییر در سرویس‌های رهانا و کنش برخط
- مقاوم نسبت به حمله پس‌زمینه در نقض حریم‌خصوصی

- تحلیل کد برنامه‌های اینترنت اشیا با هدف جلوگیری از ارسال داده‌های حساس غیرضروری به سکوها
- ارائه راه‌کار حفظ حریم‌خصوصی برای داده‌های حساس به زمان کاربر

۴-۳ مدل تهدید مسئله

شکل ۲۴، نمای کلی مدل تهدید مسئله پژوهشی را نشان می‌دهد. ما در این پژوهش مدل تهدید زیر را در نظر گرفته ایم.

۱- سکوی اینترنت اشیاء غیرقابل اعتماد است و ممکن است مورد حمله واقع شده باشد و بخواهد از داده‌های خصوصی کاربران سواستفاده نماید. سکوی غیرقابل اعتماد و یا مهاجمی که به سکو دسترسی دارد، داده‌های زیر را از یک کاربر در اختیار دارند:

- پارامترهای برنامه اینترنت اشیاء (پارامترهای رهانا و کنش): این پارامترها در هنگام توسعه‌ی برنامه تعیین می‌شوند. برای نمونه در برنامه شکل ۶ حدآستانه روشنایی محیط، پارامتر رهانای برنامه است.
- داده‌های رهانا
- زمان رخداد رهانا
- توکن‌های دسترسی کاربر به سرویس‌های برخط
- لیست دستگاه‌های مورد استفاده کاربر

۲- باتوجه به معماری متفاوت سکوهای اینترنت اشیاء به طور کلی سه حالت را درنظر گرفته ایم:

- اگر رهانا و کنش متصل به سرویس برخط هستند:

سرویس‌های رهانا و کنش را صادق ولی کنجکاو[۱۶] در نظر گرفته‌ایم. به این معنا که این سرویس‌ها از پروتکل‌های موجود پیروی می‌کنند اما ممکن است اطلاعاتی را به دست بیاورند.

[۱۶] Honest but Curious

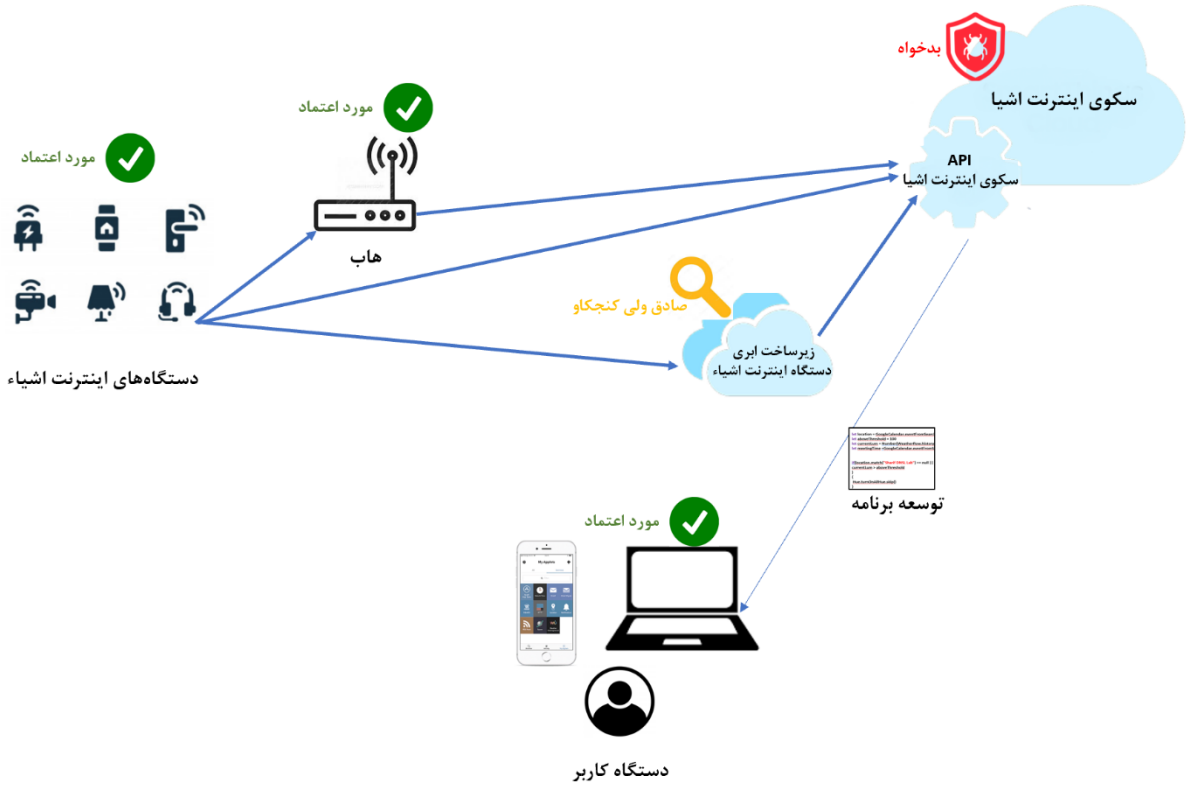
- اگر رهانا و کنش متصل به هاب هستند:

باتوجه به آن هاب در شبکه تحت کنترل کاربر قرار دارد، هاب اینترنت اشیاء را مورد اعتماد در نظر گرفته‌ایم.

- اگر رهانا و کنش مستقیما به سکو متصل هستند:

دستگاه‌های اینترنت اشیاء را مورد اعتماد درنظر گرفته‌ایم. علت آن است که خود این دستگاه‌ها در محیط قرار می‌گیرند و به داده‌های حساس کاربر دسترسی دارند.

۳- دستگاه کاربر (موبایل، تبلت یا لپ‌تاپ) که با استفاده از آن به سکوی اینترنت اشیاء متصل می‌گردد و به توسعه برنامه اینترنت اشیاء و تنظیمات مربوط به سکو می‌پردازد را مورد اعتماد درنظر گرفته‌ایم. فرض ما آن است که هر شخص به دستگاه خود اعتماد دارد.



شکل ۲۴- نمای کلیِ مدلِ تهدید مسئله‌ی پژوهشی

این نکته نیز قابل ذکر است که مورد اعتماد نبودن سکوی اینترنت اشیاء و مورداعتماد بودن دستگاه شخصی افراد بر مبنای این ایده درنظرگرفته شده است که سکوی اینترنت اشیاء با دارا بودن داده‌های حساس کاربران متعدد جذابیت بیش‌تری برای نفوذ مهاجمین سایبری به نسبت دستگاه شخصی یک فرد دارد.

۴- فرض را بر آن گذاشته ایم که سکو با هیچ‌یک از سرویس‌های برخط رهانا و کنش یا هاب اینترنت اشیاء تبانی ندارد و به طور مستقل از یکدیگر عمل می‌نمایند.
۵- ارتباطات بین موجودیت‌های مختلف در محیط اینترنت اشیاء، از جمله ارتباطات بین سکو با سرویس‌های برخط با استفاده از کانال امن (به عنوان نمونه HTTPS) صورت می‌پذیرد. لذا فرض بر این است که محرمانگی و صحت داده‌های در حال انتقال محفوظ است.
۶- مسائل مربوط به صحت اجرای یک برنامه، نظیر ارسال مجدد رهاناهای قدیمی و اجرای بدخواهانه یک کنش بدون رخ دادن رهانای مربوط به آن مدنظر این پژوهش نیست.
۷- مسائل مربوط به صحت داده‌های دریافتی از حسگرها مدنظر این پژوهش نیست.
۸- حملات منع سرویس برروی سکو اینترنت اشیاء مدنظر این پژوهش نیست.

۴-۴ راهکار پیشنهادی

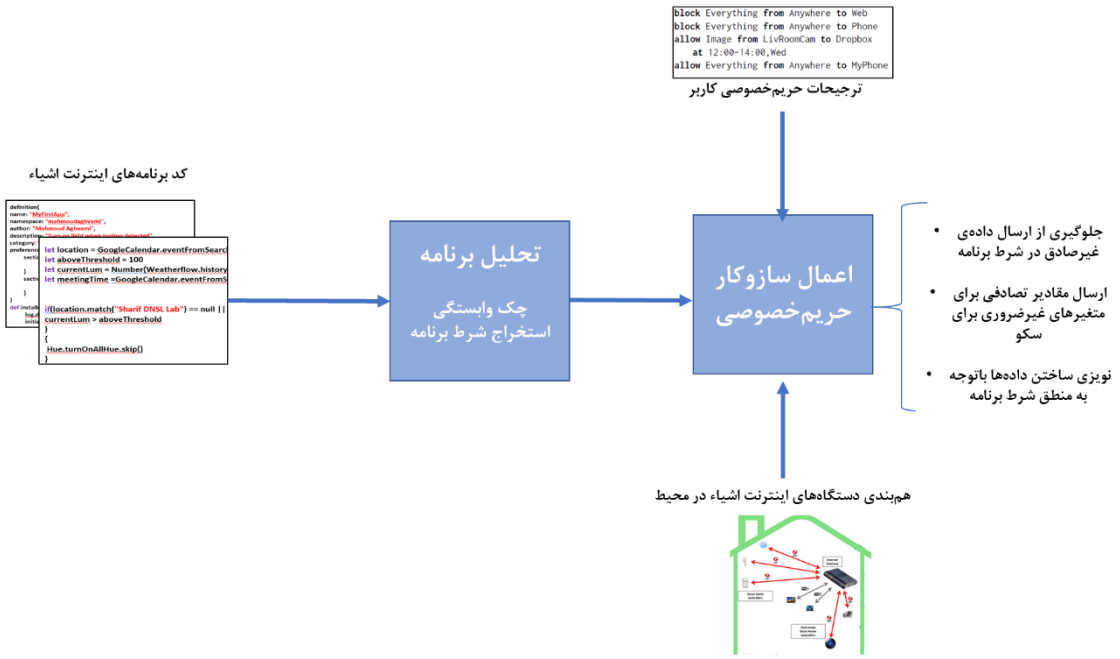
همان‌طور که در فصل سوم بیان شد، پژوهش‌های پیشین نقاط ضعف جدی را دربردارند. برخی از روش‌های پیشین از دیدگاه کارایی قابل قبول نیستند و یا حملاتی در راستای نقض حریم خصوصی برروی آن‌ها قابل اعمال است. برخی دیگر از روش‌ها نیز فرضیاتی نظیر تغییر همه‌ی سرویس‌های رهانا و کنش را در نظر گرفته اند، که فاصله قابل توجهی با اجرا دارد.

ما در راه‌کار پیشنهادی خود چهار هدف را دنبال می‌نماییم:

۱- از کد و منطق برنامه‌های اینترنت اشیاء، برای انتخاب سازوکار حفظ حریم خصوصی استفاده نماییم.
۲- تا حد امکان تغییر عمده و غیرقابل اجرایی را برروی سرویس‌های خارج از اختیار کاربر نداشته باشیم.
۳- حریم‌خصوصی را در ارتباط با رهاناهای حساس به زمان حفظ نماییم. رخداد یا عدم رخداد این رهاناها، فارغ از محتوای آن ممکن است توسط سکوی بدخواه برای تحلیل آماری رهاناهای کاربر و نقض حریم خصوصی او استفاده گردد.

۴- راه‌کار پیشنهادی ما مستقل از معماری یک سکوی خاص اینترنت اشیاء باشد و قابلیت اعمال را برای تمامی سکوها دارا باشد.

ایده اصلی ما در این راه‌کار استفاده از کد برنامه برای انتخاب سازوکار حفظ حریم‌خصوصی است. مطابق شکل ۲۶، کدبرنامه‌های اینترنت اشیاء به عنوان ورودی دراختیار راه‌کار ما قرار می‌گیرد. در بلوک اول تحلیل کدبرنامه شامل تحلیل وابستگی و استخراج شرط برنامه صورت می‌پذیرد. سپس خروجی تحلیل برنامه، به همراه ترجیحات حریم‌خصوصی کاربر و هم‌بندی[۱۷] دستگاه‌های موجود در محیط فیزیکی در اختیار بلوک دوم قرار می‌گیرد. در بلوک دوم، سازوکار حریم‌خصوصی متناسب با برنامه‌ی اینترنت اشیاء موردنظر، دستگاه مورد استفاده در این برنامه و هم‌بندی دستگاه‌ها در محیط تعیین و اعمال می‌گردد.



شکل ۲۵ - روال کلی راه‌کار پیشنهادی

شکل ۲۷ نمودار استقرار راه‌کار پیشنهادی را نشان می‌دهد. در این راهکار، ما دستگاه (موبایل یا لپ‌تاپ) کاربر اینترنت اشیاء را مورد اعتماد درنظر گرفته‌ایم و کارگزار تغییریافته و متن‌باز[۱۸] سکوی اینترنت اشیاء را برروی آن فرض کرده‌ایم. مطابق روال کلی راه‌کار پیشنهادی که در شکل ۲۵ شرح داده شد. کارگزار تغییریافته‌ی کاربر، در

[۱۷] Topology
[۱۸] Open source

زمان توسعه‌ی برنامه، تحلیل کدبرنامه را صورت می‌دهد. هم‌چنین واسطی را برای بیان ترجیحات حریم‌خصوصی در اختیار کاربر می‌گذارد.

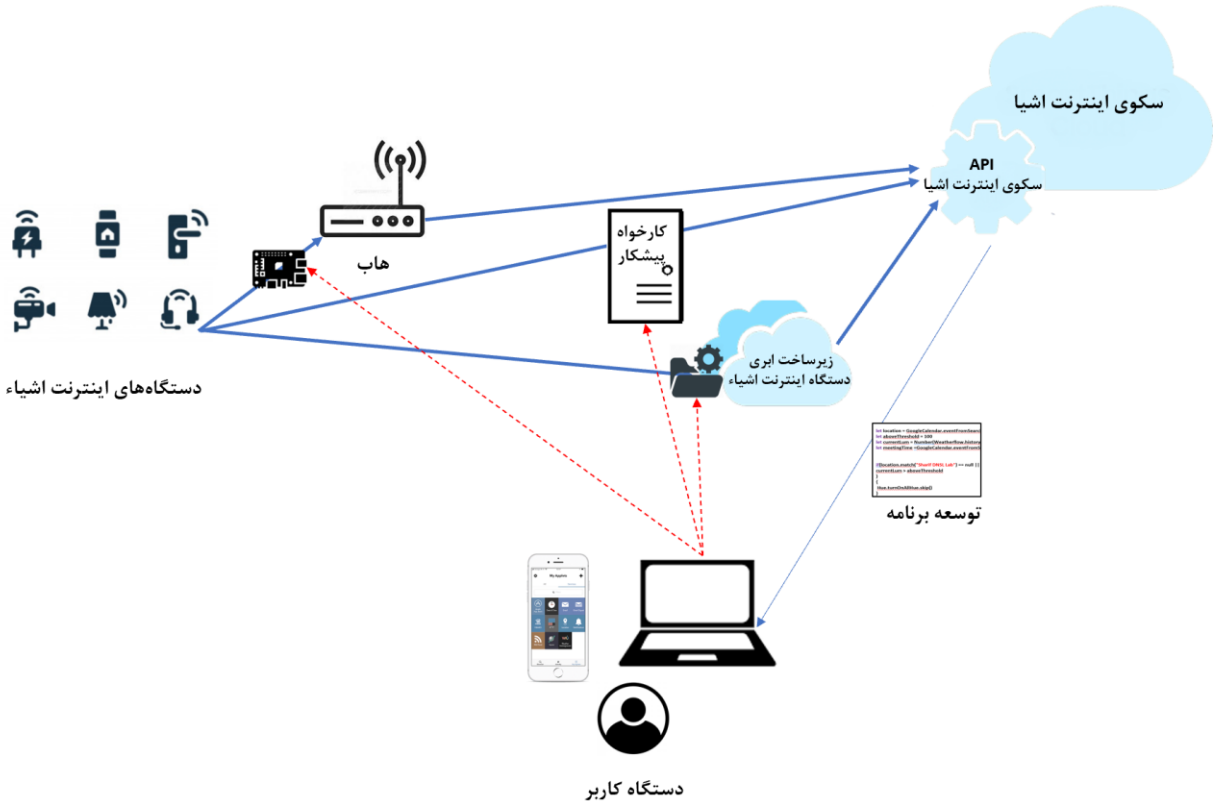
برای انتخاب مکانیزم حریم‌خصوصی و اعمال آن در زمان اجرای برنامه‌های اینترنت اشیاء، متناسب با معماری سکو، سه حالت را درنظر گرفته‌ایم:

۱. وجود یک کارخواه پیشکار[۱۹] را در ارتباط مستقیم دستگاه‌های اینترنت اشیاء با سکو
۲. وجود یک واسط سخت‌افزاری در ارتباط با هاب اینترنت اشیاء
۳. وجود کتابخانه‌ی نرم‌افزاری در زیرساخت ابری دستگاه‌های اینترنت اشیاء

مطابق شکل ۲۷ کارگزار تغییریافته‌ی کاربر پس از انجام تحلیل کد و دریافت ترجیحات حریم‌خصوصی کاربر، اطلاعات مربوطه را در اختیار یکی از سه موجودیت ذکرشده در بالا می‌گذارد(خطوط قرمز خط‌چین در شکل). کارخواه پیشکار، واسط سخت‌افزاری و یا کتابخانه نرم‌افزاری درنظر گرفته شده، وظیفه‌ی انتخاب سازوکار حریم‌خصوصی و اعمال آن را برعهده دارند.

لازم به ذکر است مدل حریم‌خصوصی k-گمنامی را برای رهاناهای حساس به زمان پیشنهاد داده‌ایم، پیاده‌سازی این مدل نیز برعهده‌ی کارگزار تغییریافته‌ی کاربر است. در ادامه با جزئیات بیش‌تری به شرح تحلیل برنامه اینترنت اشیا و پیاده‌سازی مدل حریم‌خصوصی k-گمنامی پرداخته می‌شود.

[۱۹] Proxy



شکل ۲۷-نمودار استقرار راه‌کار پیشنهادی

۴-۴-۱ تحلیل برنامه اینترنت اشیا

کاربر سکوی اینترنت اشیا، برنامه‌ی موردنظر خود را در کارگزار سکو توسعه می‌دهد. پس از توسعه کاربر، کارگزار جدید قادر است تا برنامه اینترنت اشیاء را در اختیار کارخواه پیشکار قرار دهد. برای حفظ حریم‌خصوصی کاربر، کد منبع این کارخواه پیشکار به صورت متن‌باز منتشر می‌شود و هر کاربر می‌تواند خود کارخواه پیشکار خود را راه‌اندازی نماید. تحلیل برنامه‌های اینترنت اشیاء و اعمال تغییر این تحلیل موارد زیر را شامل می‌شود:

۱- بررسی وابستگی[۲۱] خروجی برنامه به داده‌های دریافتی از رهانای برنامه

همان‌طور که در بخش ۴-۲ شرح داده شد، در بسیاری از برنامه‌ها تنها بخشی از داده‌های دریافتی از رهانا برای اجرای برنامه کافی است. با تحلیل وابستگی برنامه، داده‌های غیرضروری برای ارسال به سکو مشخص می‌شوند

[۲۱] Dependency check

و از ارسال آن‌ها جلوگیری می‌شود. تشخیص این داده‌ها در مرحله توسعه برنامه برعهده کارگزار سکو و اعمال جایگزینی این داده‌ها با مقادیر تصادفی برعهده‌ی کارخواه پیشکار می‌باشد.

۲- بررسی شرط محاسباتی اجرای برنامه

برای جلوگیری از الگوی نقض حریم‌خصوصی مبتنی بر ارسال داده‌های غیرصادق در شرط برنامه، عبارت منطقی شرط برنامه استخراج می‌شود. از شرط برنامه می‌توان برای دومنظور کمک گرفت:

الف) عدم ارسال داده‌هایی که در شرط برنامه صادق نیستند.

ب) داده‌های صادق در شرط برنامه را به صورت نویزی به سکوی اینترت اشیاء ارسال نماییم.

برای نمونه برنامه‌ی اینترنت اشیاء را درنظر بگیرید که به ازای دمای محیط بالاتر از ۲۸ درجه سانتی‌گراد دستگاه تهویه هوا را روشن می‌نماید. شرط محاسباتی برنامه دمای فعلی محیط را با حد آستانه ۲۸ درجه چک می‌نماید. با دانستن شرط محاسباتی و حدآستانه شرط، تفاوتی وجود ندارد که مقدار دقیق دمای واقعی محیط برای نمونه ۳۲ درجه را برای سکوی اینترنت اشیاء ارسال نماییم. در این مثال کافی است داده‌ی نویزی بالاتر از ۲۸ درجه(مثلاً ۴۰ درجه) برای سکو ارسال شود، هم‌چنان عملکرد برنامه به درستی صورت خواهد گرفت.

پ)بررسی نیاز به تولید رهانای جعلی

همان‌طور که در فصل سوم اشاره شد، راه‌کار ارائه شده پیشین در زمینه تولید رهانای جعلی (راه‌کار OTAP [۱۲]) دارای نقاط ضعف مشخصی است. در این راهکار رهاناهای جعلی، به صورت متناوب و در بازه‌های زمانی کوتاه (حدود ۱۵ دقیقه) برای تمامی دستگاه‌های اینترنت اشیاء تولید می‌شوند. این تولید متناوب راه‌کار جعلی علاوه بر سربار شدیدی که به سکو تحمیل می‌کند، نمی‌تواند از وقوع حمله‌ی پیوند[۲۲] برای نقض حریم‌خصوصی جلوگیری نماید. مشکل راه‌کار OTAP آن است که بدون درنظر گرفتن برنامه‌های اینترنت اشیاء و بدون بررسی دستگاه مورد استفاده اینترنت اشیاء به طور کلی به تولید رهانای جعلی می‌پردازد. ما در پژوهش خود با تحلیل کد برنامه، صرفا در مورد دستگاه‌هایی مشخص و تحت شرایط مشخصی اقدام به تولید رهانای جعلی می‌نماییم.

[۲۲] Link

۴-۴-۲ پیاده‌سازی k-گمنامی

همان‌طور که در فصل سوم بررسی شد یکی از نقاط ضعف جدی راه‌کارهای پیشین، عدم ارائه راه‌حلی برای حفظ حریم‌خصوصی در ارتباط با رهاناهای حساس به زمان بود. درواقع راه‌کارهای مبتنی بر رمزنگاری نظیر راه‌کار ETAP [۱۵] پاسخ‌گوی این نیاز نبودند. از سویی دیگر راه‌کارهای مبتنی بر رهانای جعلی نیز چالش‌های قابل توجهی داشتند و در عمل قابل اجرا نبودند.

ما برای حفظ حریم‌خصوصی رهاناهای حساس به زمان و جلوگیری از تحلیل آماری رخداد یا عدم رخداد رهاناها که منجر به استخراج پروفایل یک کاربر مشخص و تبلیغات هدفمند و نقض حریم‌خصوصی او می‌گردد، راه‌کاری را مبتنی بر مدل k-گمنامی پیشنهاد می‌نماییم. در این راه‌کار ایده ما استفاده از کارخواه پیشکار مطرح شده پیش از این، برای تجمیع اطلاعات k کاربر یک سکوی اینترنت اشیاء است. فرضیه ما بر این است که داده‌های تجمیع شده‌ی دریافتی از k کاربر (اگر رفتار این کاربران به اندازه کافی متنوع باشند)، قابلیت تحلیل آماری و ساخت پروفایل مشخص را ندارد. با بررسی مدل k-گمنامی با دو چالش مواجه هستیم.

۱- چالش کنترل دسترسی برروی دستگاه‌ها

فرض ما بر آن است از دید سکوی اینترنت اشیا، k کاربر مشارکت کننده در کارخواه پیشکار، یک کاربر واحد دیده می‌شوند که به تعداد مجموع دستگاه‌های اینترنت اشیا، دستگاه دارند. لازم است تا کنترل دسترسی برای دستگاه‌های کاربران صورت گیرد و قابلیت تعریف برنامه برای هرکاربر به دستگاه‌های خود او محدود شود. از تداخل احتمالی درصورت وجود دستگاه‌های مشابه نیز باید جلوگیری گردد.

۲- چالش تعیین پارامتر k و انتخاب k کاربر

مسئله اصلی در این مدل پیشنهادی، حفظ حریم‌خصوصی است. از این رو، لازم است تا پارامتر k به گونه‌ای تعیین شود که مطمئن باشیم تحلیل آماری رهاناهای دریافتی برای سکو مقدور نیست و یا منجر به نتیجه قابل توجهی نمی‌شود. از این رو تعیین پارامتر k یکی از چالش‌های موجود است.

چالش دیگر انتخاب k کاربر از میان همه‌ی کاربران سکو است. یک ایده دسته‌بندی کاربران براساس معیار نزدیکی مکانی است. مثلا کاربران سکوی اسمارت‌تینگز موجود در یک مجتمع ساختمانی با یکدیگر یک کلاس هم‌ارزی را تشکیل دهند. ایده دیگر دسته‌بندی کاربران براساس لیست دستگاه‌هایی که دارا هستند می‌باشد.

۴-۵ ارزیابی

برای ارزیابی راه‌کار پیشنهادی ارائه شده، دو بخش را درنظر داریم:

۱- ارزیابی مبتنی بر تحلیل صوری و اثبات

در ارزیابی تحلیلی بررسی می‌کنیم که روش پیشنهادی چه ویژگی‌هایی را در زمینه حفظ حریم خصوصی تضمین می‌نماید. برای اثبات این ویژگی‌ها، از توصیف و اثبات صوری بهره خواهیم برد.

۲- ارزیابی مبتنی بر پیاده‌سازی روش

ما یک نمونه آزمایشگاهی از راه‌کار پیشنهادی خود را پیاده‌سازی خواهیم نمود. پس از آن سوالات پژوهشی زیر را در ارتباط با نمونه پیاده‌سازی‌شده پاسخ خواهیم داد:

- سکوی پیشنهادی چه میزان سربار محاسباتی بیش‌تر از سکوی مشابه بدون حفظ حریم خصوصی (برای مثال سکوی اسمارت‌تینگز) دارد؟
- سکوی پیشنهادی توانایی پشتیبانی از چه نوع برنامه‌هایی را دارد؟
- سکوی پیشنهادی چه تاثیری بر عملکرد زیرساخت و کاربردپذیری آن دارد؟

برای مقایسه نمونه پیاده‌سازی شده و سکوی تجاری اینترنت اشیا، لازم است تا عملکرد یکی از سکوهای تجاری را بازنویسی کنیم. سپس به مقایسه‌ی عملکرد سکوی تجاری و سکوی پیشنهادی برروی مجموعه داده‌ی آزمون بپزدازیم. مجموعه‌داده ی آزمون دو بخش خواهد داشت:

۱- مجموعه برنامه‌های اینترنت اشیاء
۲- مجموعه داده‌های دریافتی از دستگاه‌های اینترنت اشیاء

مجموعه‌ی برنامه‌های اینترنت اشیاء مورد آزمون می‌بایست شامل برنامه‌هایی دارای شرط محاسباتی متنوع (انواع حالات شرط‌های منطقی قابل توسعه)، رهاناهای متفاوت (انواع ساختارداده‌های گسسته و پیوسته قابل پشتیبانی برای رهانا) و کنش‌هایی با ساختارهای مختلف باشد.

درمورد مجموعه‌ی داده‌های دریافتی از دستگاه‌های اینترنت اشیا موارد زیر را باید درنظر گرفت:

۱- تنوع زمان رخداد رهاناهای دریافتی از دستگاه‌ها
۲- وجود انواع دستگاه‌های متنوع اینترنت اشیاء
۳- تنوع در هم‌بندی دستگاه‌های اینترنت اشیاء در محیط فیزیکی

لازم به ذکر است در پژوهش‌های پیشین نظیر پژوهش [۱۱] از مجموعه داده آزمون CASAS [۶۱] (داده‌های hh104, hh105, hh110, hh111) نیز به عنوان داده‌ی تولیدی دستگاه‌های اینترنت اشیاء استفاده شده است. این داده‌ها، داده‌های واقعی ثبت شده از دستگاه‌های اینترنت اشیا (دستگاه‌های تشخیص حرکت، حسگر تماس، حسگر دما، کلیدها و میزان باتری دستگاه‌ها) برای افراد مختلف است که در بازه‌های زمانی یک و دوماهه ذخیره شده اند. بررسی مجموعه آزمونCASAS نشان می‌دهد، تنوع دستگاه‌ها وحالات مختلف رهاناهای دریافتی متناسب با نیازمندی‌های آزمون پژوهش ما کافی نیست و باتوجه به دغدغه‌های موجود، لازم است تا مجموعه‌ی دادهای آزمون اختصاصی خودمان را طراحی نماییم.

۴-۶ زمان‌بندی فعالیت‌ها

در جدول ۳-۴ زمان‌بندی تخمینی انجام پیشنهاد رساله آمده است.

جدول ۳-۴- زمان‌بندی اجرای فعالیت‌های رساله پیشنهادی

شماره فعالیت	فعالیت‌ها	مدت زمان (برحسب ماه)
۱	بررسی ساختار برنامه‌ها و تفاوت‌های موجود آن‌ها در سکوهای مختلف اینترنت اشیاء	۱
۲	ارائه مدل صوری برای برنامه‌های اینترنت اشیاء در سکوهای مختلف	۱
۳	توسعه‌ی فرآیند تحلیل برنامه‌های اینترنت اشیاء برای دوسکوی نمونه (تحلیل وابستگی، استخراج شرط برنامه)	۴
۴	ارائه مدل اختصاصی‌سازی خودکار سازوکار حریم‌خصوصی متناسب با برنامه اینترنت اشیا	۴
۵	ارائه مدل حریم‌خصوصی k-گمنامی در سکوی اینترنت اشیاء، ارائه راه‌کار برای چالش‌های موجود آن	۶
۶	طراحی مجموعه داده‌ی آزمون شامل مجموعه برنامه‌های اینترنت اشیاء و مجموعه داده‌های دریافتی از دستگاه‌های اینترنت اشیاء	۲
۷	پیاده‌سازی نمونه‌ی آزمایشگاهی و ارزیابی با داده‌ی آزمون	۴
۸	تدوین رساله	۲
۹	مطالعه کارهای پژوهشی مرتبط جدید	۲۴

۴-۷ جمع‌بندی

ما در این پیشنهاد پژوهشی، الگوهای نقض حریم‌خصوصی در سکوهای اینترنت اشیاء را مورد بررسی قرار دادیم. راه‌کارهای پیشین این حوزه را نیز بررسی نموده و نقاط ضعف هریک از آن‌ها را بیان نمودیم. سپس به شرح مسئله‌ی پژوهشی خود در راستای حفظ حریم‌خصوصی سکوهای اینترنت اشیاء با حفظ کاربردپذیری آن‌ها پرداختیم. در ادامه راه‌کار پیشنهادی خود را بر مبنای تحلیل برنامه‌های اینترنت اشیا با هدف انتخاب سازوکار حریم‌خصوصی و اعمال آن مطرح نموده و زمان‌بندی فعالیت‌های پیش‌رو را بیان کردیم.

مراجع

[1] IFTTT. IFTTT (if this, then that). https://ifttt.com/. [Online; accessed 4-May-2020].

[2] Zapier. https://zapier.com/.[Online; accessed 4-May-2020].

[3] SmartThings. SmartThings Community Forum for Third-party Apps. https://community.smartthings.com/.[Online; accessed 4-May-2020].

[4] IFTTT. IFTTT: Number of Users and Online Services. https://platform:ifttt:com/plans, 2020.

[5] IFTTT Terms and Privacy Policy. https://ifttt.com/terms. [Online; accessed 4-May-2020].

[5] SmartThings Privacy Policy. https://www.smartthings.com/privacy. [Online; accessed 4-May-2020].

[7] The 15 biggest data breaches of the 21st century, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html[Online; accessed 4-May-2020].

[8] Important update about the Gmail service. https://help.ifttt.com/hc/en-us/articles/360020249393-Important-update-about-the-Gmail-service[Online; accessed 4-May-2020].

[9] Internet of Things - number of connected devices worldwide 2015-2025 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/[Online; accessed 4-May-2020].

[10] Fernandes, E., Rahmati, A., Jung, J., & Prakash, A. (2018, February). Decentralized action integrity for trigger-action IoT platforms. In Proceedings 2018 Network and Distributed System Security Symposium.

[11] Xu, R., Zeng, Q., Zhu, L., Chi, H., Du, X., & Guizani, M. (2019). Privacy leakage in smart homes and its mitigation: IFTTT as a case study. IEEE Access, 7, 63457-63471.

[12] Chiang, Y. H., Hsiao, H. C., Yu, C. M., & Kim, T. H. J. (2020, September). On the privacy risks of compromised trigger-action platforms. In European Symposium on Research in Computer Security (pp. 251-271). Springer, Cham.

[13] Zavalyshyn, I., Santos, N., Sadre, R., & Legay, A. (2020). My House, My Rules: A Private-by-Design Smart Home Platform. In EAI MobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services.

[14] Schoettler, S., Thompson, A., Gopalakrishna, R., & Gupta, T. (2020). Walnut: A low-trust trigger-action platform. arXiv preprint arXiv:2009.12447.

[15] Chen, Y., Chowdhury, A. R., Wang, R., Sabelfeld, A., Chatterjee, R., & Fernandes, E. (2020). Data Privacy in Trigger-Action IoT Systems. arXiv preprint arXiv:2012.05749.

[16] WebCoRE WiKi_Web-enabled Community's own Rule Engine. https://wiki.webcore.co/ [Online; accessed 4-May-2020].

[17] Bastys, I., Balliu, M., & Sabelfeld, A. (2018, January). If this then what? Controlling flows in IoT apps. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1102-1119).

[18] Yes, Your Amazon Echo Is an Ad Machine. https://gizmodo.com/yes-your-amazon-echo-is-an-ad-machine-1821712916 [Online; accessed 4-May-2020].

[19] Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing. https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html.[Online; accessed 4-May-2020].

[20] Amazon Sends 1,700 Alexa Voice Recordings to a Random Person. https://threatpost.com/amazon-1700-alexa-voice-recordings/140201/.[Online; accessed 4-May-2020].

[21] Chen, G., Chen, S., Xiao, Y., Zhang, Y., Lin, Z., & Lai, T. H. (2019, June). SgxPectre: Stealing Intel secrets from SGX enclaves via speculative execution. In 2019 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 142-157). IEEE.

[22] Celik, Z. B., McDaniel, P., & Tan, G. (2018). Soteria: Automated iot safety and security analysis. In 2018 {USENIX} Annual Technical Conference ({USENIX}{ATC} 18) (pp. 147-158).

[23] Celik, Z. B., Babun, L., Sikder, A. K., Aksu, H., Tan, G., McDaniel, P., & Uluagac, A. S. (2018). Sensitive information tracking in commodity IoT. In 27th {USENIX} Security Symposium ({USENIX} Security 18) (pp. 1687-1704).

[24] Celik, Z. B., Tan, G., & McDaniel, P. D. (2019, February). IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT. In NDSS.

[25] Fernandes, E., Paupore, J., Rahmati, A., Simionato, D., Conti, M., & Prakash, A. (2016). فلوفِنس: Practical data protection for emerging iot application frameworks. In 25th {USENIX} Security Symposium ({USENIX} Security 16) (pp. 531-548).

[26] Jia, Y. J., Chen, Q. A., Wang, S., Rahmati, A., Fernandes, E., Mao, Z. M., ... & Unviersity, S. J. (2017, February). ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms. In NDSS.

[27] IoT Platform Companies Landscape 2019/2020: 620 IoT Platforms globally. https://iot-analytics.com/iot-platform-companies-landscape-2020. [Online accessed 4-May-2020].
[28] SmartThings Overview. https://docs.smartthings.com/en/latest/getting-started/overview.html. [Online accessed 4-May-2020].
[29] Typed JavaScript at Any Scale. https://www.typescriptlang.org. [Online accessed 4-May-2020].
[30] Microsoft Power Automate. https://flow.microsoft.com/en-us. [Online accessed 4-May-2020].
[31] Node-RED platform https://nodered.org/docs. [Online accessed 4-May-2020].
[32] node-red-contrib-python-function https://flows.nodered.org/node/node-red-contrib-python-function. [Online accessed 4-May-2020].
[33] Oldehoeft, A. E. (1992). Foundations of a Security Policy for Use of the National Research and Educational Network. US Department of Commerce, National Institute of Standards and Technology.
[34] Barbosa, P., Brito, A., & Almeida, H. (2015, April). Defending against load monitoring in smart metering data through noise addition. In Proceedings of the 30th Annual ACM Symposium on Applied Computing (pp. 2218-2224).
[35] Xu, Y., Frahm, J. M., & Monrose, F. (2014, November). Watching the watchers: Automatically inferring tv content from outdoor light effusions. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 418-428).
[36] Copos, B., Levitt, K., Bishop, M., & Rowe, J. (2016, May). Is anybody home? Inferring activity from smart home network traffic. In 2016 IEEE Security and Privacy Workshops (SPW) (pp. 245-251). IEEE.
[37] Yoshigoe, K., Dai, W., Abramson, M., & Jacobs, A. (2015, December). Overcoming invasion of privacy in smart home environment with synthetic packet injection. In 2015 TRON Symposium (TRONSHOW) (pp. 1-7). IEEE.
[38] Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017). Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. arXiv preprint arXiv:1708.05044.
[39] Babun, L., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2019). Real-time analysis of privacy-(un) aware iot applications. arXiv preprint arXiv:1911.10461.
[40] Wang, Q., Datta, P., Yang, W., Liu, S., Bates, A., & Gunter, C. A. (2019, November). Charting the attack surface of trigger-action iot platforms. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 1439-1453).
[41] Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In 2016 IEEE symposium on security and privacy (SP) (pp. 636-654). IEEE.
[42] OpenHAB platfrom. https://www.openhab.org. [Online accessed 4-May-2020].

[43] Apple HomeKit. http://www.apple.com/ios/home. [Online accessed 4-May-2020].
[44] Wink. https://www.wink.com/. [Online accessed 4-May-2020].
[45] Iris. https://www.irisbylowes.com/. [Online accessed 4-May-2020].
[46] Zhu, T., Li, G., Zhou, W., & Philip, S. Y. (2017). Differential privacy and applications. Cham, Switzerland: Springer International Publishing.
[47] Ganta, S. R., Kasiviswanathan, S. P., & Smith, A. (2008, August). Composition attacks and auxiliary information in data privacy. In Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 265-273).
[48] Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05), 557-570.
[49] Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). l-diversity: Privacy beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1), 3-es.
[50] Li, N., Li, T., & Venkatasubramanian, S. (2007, April). t-closeness: Privacy beyond k-anonymity and l-diversity. In 2007 IEEE 23rd International Conference on Data Engineering (pp. 106-115). IEEE.
[51] Wong, R. C. W., Fu, A. W. C., Wang, K., & Pei, J. (2007, September). Minimality attack in privacy preserving data publishing. In Proceedings of the 33rd international conference on Very large data bases (pp. 543-554).
[52] Ferencz, K., & Domokos, J. Using Node-RED platform in an industrial environment.
[53] MultiTech Industrial IoT solutions. https://www.multitech.com. [Online accessed 4-May-2020].
[54] Opto 22. https://www.opto22.com/ https://www.opto22.com. [Online accessed 4-May-2020].
[55] Advanced Control and Commissioning for the Internet of Things. https://www.iaconnects.co.uk. [Online accessed 4-May-2020].
[56] Garage-door-monitor application. https://github.com/SmartThingsCommunity/SmartThingsPublic/blob/36d37c1b431eb81c2722202c66dd07d38f3bd3dd/smartapps/smartthings/garage-door-monitor.src/garage-door-monitor.groovy. [Online accessed 4-May-2020].
[57] TriSensor. https://aeotec.com/z-wave-motion-sensor. [Online accessed 4-May-2020].
[58] Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63(9), 1278-1308.
[59] SmartThings Data types.https://smartthings.developer.samsung.com/docs/api-ref/capabilities.html. [Online accessed 4-May-2020].
[60] CASAS. (2015). Datasets for Advanced Studies in Adaptive Systems of WSU. http://casas.wsu.edu/datasets. [Online accessed 4-May-2020].

[61] Warner, S. L. (1965). Randomized response: A survey technique for eliminating evasive answer bias. Journal of the American Statistical Association, 60(309), 63-69.

[62] Dwork, C. (2008, April). Differential privacy: A survey of results. In International conference on theory and applications of models of computation (pp. 1-19). Springer, Berlin, Heidelberg.

[63] Wong, R. C. W., Fu, A. W. C., Wang, K., Yu, P. S., & Pei, J. (2011). Can the utility of anonymized data be used for privacy breaches?. ACM Transactions on Knowledge Discovery from Data (TKDD), 5(3), 1-24.