امنیت و حریم خصوصی در اینترنت اشیا

حمیدرضا ارکیان*، عاطفه پورخلیلی و حمیدرضا خوش‌اخلاق

گروه رمز و امنیت اطلاعات، پژوهشکده افتا، پژوهشگاه توسعه فناوری‌های پیشرفته خواجه نصیرالدین طوسی، تهران، ایران
{arkian; pourkhalili; khoshakhlagh}@rcdat.ir

چکیده

با ظهور اینترنت نحوه ارتباط انسان‌ها با یکدیگر دست‌خوش انقلابی بنیادین شد. موج دوم توسعهٔ اینترنت دیگر در مورد انسان‌ها نیست؛ بلکه در مورد دستگاه‌های به هم متصل هوشمند خواهد بود. با اینکه بیش از یک دهه از مطرح‌شدن مفهوم "اینترنت اشیا" می‌گذرد؛ اما به دلایل مختلفی همچون عدم توسعه فناوری‌های مورد نیاز و وجود چالش امنیت، توسعه این مفهوم با کندی مواجه بوده است. هنگامی‌که ما در محیط‌های هوشمند و فناوری‌هایی مثل اینترنت اشیا درحال تحقیق هستیم، باید زمان و انرژی مضاعفی را صرف شناخت چالش‌های امنیتی و راه‌کارهای موجود کنیم. در این مقاله تلاش می‌شود با رویکردی نظام‌مند به بررسی تهدیدات و مخاطرات موجود در حوزه امنیت و حریم خصوصی اینترنت اشیا پرداخته و همچنین مروری بر راه‌حل‌های پیشنهادشده در منابع و مقالات علمی ارائه شود. در انتها نیز فرصت-های پژوهشی باقیمانده در این حوزه بررسی می‌شود.

واژگان کلیدی:اینترنت اشیا، IoT، امنیت، حفظ حریم خصوصی، حملات امنیتی.

۱- مقدّمه

اینترنت اشیا[1] یا IoT بخشی از اینترنت آینده است که شامل اینترنت موجود و در حال رشد و همچنین توسعه‌های آینده شبکه می‌شود. IoT به‌طور مفهومی می‌تواند به‌عنوان یک زیرساخت شبکهٔ سراسری پویا با قابلیت‌های خودپیکره‌بندی و مبتنی بر استانداردها و پروتکل‌های ارتباط جمعی و مشارکتی تعریف شود که در آن "اشیا" فیزیکی و مجازی دارای شناسه‌ها، صفات فیزیکی و مشخصه‌های مجازی، از واسط‌های هوشمند استفاده کرده و به‌طور یکنواخت و مستمر در یک شبکه اطلاعات مجتمع شده‌اند [۱]. اینترنت اشیا می‌تواند جهان را تغییر دهد؛ شاید بسیار عمیق‌تر از آنچه امروز اینترنت مردم‌محور تغییر داده است. با این وجود، اینترنت اشیا نیز مشابه اینترنت فعلی از ابهام و بی‌نظمی در تعریف رنج می‌برد.

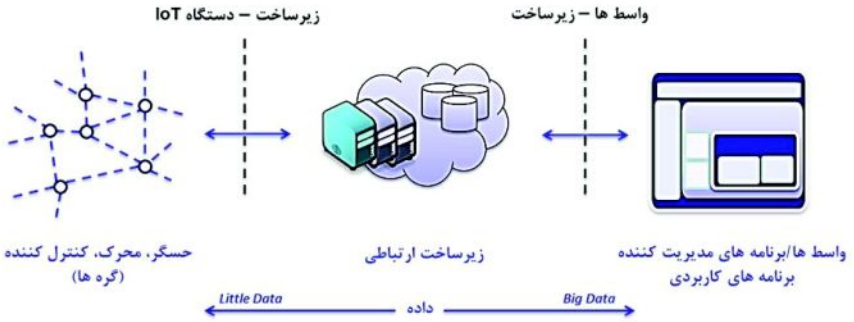
مجموعه‌های بزرگی در حوزهٔ فناوری اطلاعات سعی در تعریف IoT بر اساس آینده‌های قابل پیش‌بینی، داشته‌اند. CisCo آن را اینترنت همه چیز[2] می‌نامد و می‌گوید این "آخرین موج از اینترنت متصل‌کنندهٔ اشیا با هدف ایمنی، راحتی و بهره‌وری بیشتر" خواهد بود. IBM آن را به‌عنوان "یک وب جهانی به‌طورکامل جدید که در آن دستگاه‌ها قادرند پیامی را به دستگاهی دیگر ارسال کنند"، تعبیر می‌کند. جنرال الکتریک می‌گوید "اینترنت صنعتی" شاید جذاب‌ترین تعریف باشد، چون تصور کاربردهای جدید را امکان‌پذیر می‌سازد [۲]. هرکس به طریقی آینده را تشریح می‌کند؛ اما همه موافقند که IoT و سامانه‌های هوشمند قادر خواهند بود جهان ما را به‌طور بنیادین تغییر دهند.

در IoT، اشیاء هوشمند می‌توانند به‌عنوان شرکت‌کنندگان فعال در فعالیت‌های تجاری، اطلاعاتی و اجتماعی محسوب شوند. در این فعالیت‌ها، اشیا با یکدیگر و همچنین با محیط اطراف خود از طریق تبادل داده‌ها و

[1] Internet of Things

[2] Internet of EveryThings

* نویسندهٔ عهده‌دار مکاتبات



(شکل- ۱): یک مدل ساده از یک سیستم IoT

اطلاعات جمع‌آوری‌شده، تعامل داشته و ارتباط برقرار می‌کنند. علاوه‌براین می‌توانند به‌طور خودکار به رویدادهای دنیای واقعی واکنش نشان داده و با اجرای پردازش‌هایی که منجر به فعالیتی خاص شده و یا سرویسی را راه‌اندازی می‌کنند، محیط را تحت تأثیر قرار دهند. این کارها می‌توانند با یا بدون دخالت مستقیم انسان صورت پذیرد [۳].

سرویس‌ها نیز قادر خواهند بود با این اشیای هوشمند از طریق واسط‌های استاندارد که اتصالات لازم را از طریق اینترنت فراهم می‌کند، تعامل داشته تا به این ترتیب وضعیت خود را تغییر داده و اطلاعات مورد نیاز خود را با درنظرگرفتن مسائل امنیت و حریم خصوصی بازیابی کنند. به طور کلی نوآوری IoT در دو موضوع است: مقدار افزودهٔ اطلاعاتی که توسط اتصالات داخلی بین اشیا تولید می‌شود و همچنین انتقال اطلاعات پردازش‌شده به پایگاه دانش[1] جهت استفاده انسان‌ها و جامعه.

یک سامانهٔ IoT شباهت‌های زیادی با دیگر سامانه‌ها و فناوری‌های موجود دارد که موجب می‌شود بعضی از ویژگی‌ها و خصوصیات آن‌ها را به ارث ببرد. به‌طور کلی می‌توان اینترنت اشیای فعلی را مشتمل بر سه مؤلفهٔ مستقل دانست که مجموعهٔ سامانه IoT درحقیقت برقرارکنندهٔ ارتباط بین این سه مؤلفه خواهند بود شکل (۱). این سه مولفه عبارتند از:

۱. دستگاه‌های IoT یا گره‌های شبکه که می‌توانند شامل تمام دستگاه‌ها، حس‌گرها، سامانه‌ها و تجهیزاتی شوند که قابلیت متصل‌شدن به یک ساختار IoT را دارند.
۲. زیرساخت؛ که درحقیقت در حال حاضر مجموعهٔ ابر[2] مورد استفاده در یک سامانه IoT را تشکیل داده و جهت یک‌پارچه‌سازی داده‌ها، ذخیرهٔ داده و انجام محاسبات مختلف مورد استفاده قرار می‌گیرد.
۳. واسط‌ها یا برنامه‌های کاربردی؛ که شامل تمامی ابزارهای نرم‌افزاری و مدیریتی مورد استفاده در یک سامانه IoT می‌گردد و ارتباط تنگاتنگی با زیرساخت ابر خواهند داشت [۴].

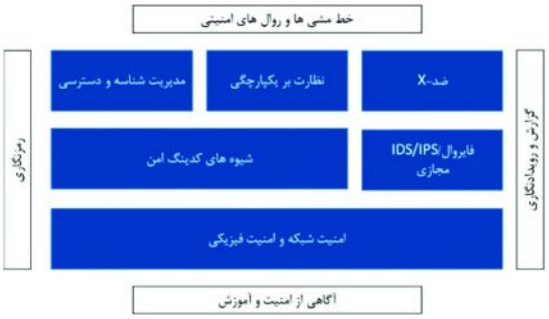
به‌تازگی، برخلاف پژوهش‌های صورت‌گرفته مرتبط با IoT و امنیت آن، حملات مختلفی معرفی می‌شود که فضای این مفهوم و فناوری‌های مرتبط با آن را درگیر کرده است. معرفی این حملات بیشتر در کنفرانس‌هایی مثل BlackHat و دیگر انجمن‌های غیرامنیتی صورت می‌گیرد. این نشان می‌دهد که فناوری به پرتگاه بسیار پیچیده‌ای نزدیک شده و اقدامات متقابل اغلب، فقط واکنشی است [۵]؛ بنابراین نیاز است اندکی به عقب بازگردیم –زمانی‌که آن فناوری‌های مؤثر بر زندگی، در حال توسعه بودند و به سمت ابعاد خوبی از فناوری تمایل داشتند– و امنیت را در هرسطحی بازتعریف کنیم. اگرچه این مسائل به خاطر اجبارهای نظارتی در حال تغییر است، اما با این حال تأیید مراکز دولتی به معنای امنیت نخواهد بود.

مسألهٔ امنیت در IoT را می‌توان مهم‌ترین چالش توسعه این فناوری در نظر گرفت. در این رابطه استانداردهای مختلفی در حال توسعه است؛ ولی همچنان نیازمندی‌های امنیتی IoT و حتی مخاطرات آن به‌خوبی شناسایی و تحلیل نشده است [۶].

با بررسی مقالات و کتاب‌هایی که در حوزهٔ امنیت اینترنت اشیاء ارائه شده‌اند، می‌توان دریافت که امنیت باید در تمام سطوح بسته‌ها و سرویس‌ها نیز در نظر گرفته شود؛ بنابراین در تمام مراحل توسعهٔ سیستم، ویژگی‌های امنیتی

[1] Knowledge base
[2] Cloud

وجود خواهند داشت. در شکل(۲) امکان مشاهده رویکرد "دفاع- در-عمق" در توسعهٔ امنیت، قابل مشاهده است.



(شکل-۲): استراتژی دفاع-در-عمق فراگیر

این رویکرد، امنیت را در دل شبکه IoT گنجانده و به سازمان‌ها و شرکت‌ها اجازه می‌دهد تا با درگیرکردن مهاجمان به‌صورت لایه‌به‌لایه، زمان بیشتری برای دفاع از منابع خود داشته باشند [۷].

این مطالعه به یک مرور کلی از مباحث مختلف در حوزهٔ امنیت و حریم خصوصی اینترنت اشیا می‌پردازد. بخش بعد با بررسی انواع رویکردهای تحلیل تهدیدات امنیتی IoT آغاز شده و پیش‌فرض‌ها، مقدمات و همچنین محدوده تحلیل صورت گرفته مرور می‌شود. در قسمت انتهایی این بخش نیز تهدیدات مربوطه بررسی خواهد شد. در بخش سوم تلاش می‌شود تا جمع‌آوری مناسبی از راه‌حل‌های مختلف پیشنهادشده ارائه شود. در بخش انتهایی این مقاله نیز با هدف کمک به پژوهش‌گران جهت ادامه پژوهش‌ها در این حوزه، به بیان فرصت‌های پژوهشی و مسائل باز در امنیت و حریم خصوصی اینترنت اشیا می‌پردازیم.

۲- تحلیل و بررسی تهدیدات امنیتی IoT

در این بخش، مجموعه‌ای از تهدیدات موجود را مورد بررسی و تحلیل قرار می‌دهیم. هدف از این بخش، تحلیل سامانه‌ای است که در حال حاضر تحت طراحی است نه در حال پیاده‌سازی عملیاتی. ایده اصلی پشت این تحلیل مخاطرات و تهدیدها، در سه مورد خلاصه می‌شود: ۱) مسائل بنیادین امنیت و حریم خصوصی در گسترش IoT چیست؟ ۲) کدام موجودیت‌ها نیاز به حفاظت دارند؟ ۳) در چنین توسعه‌ای چه انواعی از حملات قابلیت اجرایی شدن دارند؟ این تحلیل تهدیدات، الزامی کلیدی جهت رسیدن به نیازمندی‌های معماری سامانه IoT با درنظر گرفتن مفاهیم امنیت، حریم خصوصی[1] و قابلیت اطمینان[2] از طریق طراحی خواهد بود [۸]. به‌طوراساسی حداقل سه رویکرد متفاوت جهت فهمیدن و درک سامانه‌ای تهدیدات و دسته‌بندی آن‌ها وجود دارد:

۱. مهاجم‌محور[3]
۲. نرم‌افزارمحور[4]
۳. دارایی‌محور[5].

رویکرد نرم‌افزارمحور زمانی استفاده می‌شود که نرم‌افزاری جهت اعمال آزمایش‌های نفوذ[6]، تحلیل ایستا، تحلیل پویا و مانند آن وجود دارد. از آن‌جایی که هنوز چنین نرم‌افزارهایی با تمرکز بر IoT توسعه داده نشده‌اند، یک رویکرد نرم‌افزارمحور در قالب این مقاله نمی‌گنجد.

مدل‌کردن تهدیدات به روش دارایی‌محور با ایجاد یک "فهرست دارایی" از دارایی‌ها و کالاهای IT یک سامانه آغاز می‌شود که این دارایی‌ها می‌توانند سخت‌افزار، نرم‌افزار، فرآیندها و داده‌ها باشند. در کاربردهای تجاری این مفهوم اطلاعات تجاری وابسته به کاربر، مشتری‌ها، نقشه‌های تولید، استراتژی و مانند آن را شامل می‌شود. در سامانه‌های ارتباطی نیز جداول مسیریابی، فرآیندهای نظارت بر کارایی، داده‌های زیرساخت و پردازش‌ها را در بر می‌گیرد. در کاربردهای IoT تمام داده‌های مربوط به فراهم‌سازی سرویس‌ها و به‌خصوص اطلاعات شخصی حساس مربوط به کاربران را می‌توان به عنوان دارایی[7] در نظر گرفت.

تحلیل‌های مهاجم‌محور نیز بر روی تهدیدات ممکن که یک مهاجم از آن‌ها استفاده می‌کند و همین‌طور مجموعه فعالیت‌های آن مهاجم تمرکز دارد. ما نگاه خود را به بحث در مورد تهدیداتی محدود می‌کنیم که می‌توان با مفاهیم IT به آن‌ها پرداخت. این به آن معناست که به‌عنوان‌مثال حفاظت فیزیکی از دارایی‌های سخت‌افزاری در چارچوب تمرکز ما نمی‌گنجد. به‌طورکلی فراهم‌کردن سازوکارهای امنیت IT برای کمک به حفاظت سخت‌افزار کار مشکلی است. این مساله زمانی پررنگ می‌شود که به‌عنوان‌مثال یک قطعه از سخت‌افزار دارای دستگاهی تعبیه‌شده باشد که امکان ردیابی آن بعد از دزدیده‌شدن وجود دارد. اگر یک مهاجم به‌صورت فیزیکی یک سخت‌افزار را بشکند تا کلیدهای رمزنگاری یا

[1] Privacy
[2] Reliability
[3] Attacker-centric
[4] Software-centric
[5] Asset-centric
[6] Penetration testing
[7] Assests

اطلاعات سطح بالای مدیریتی را سرقت کند، آنگاه موجودیتی که باید امن نگه داشته شود، سخت‌افزار نخواهد بود؛ بلکه کلیدها یا داده‌هایی که مهاجم به دنبال آن‌هاست، دارایی حساس ما محسوب می‌شوند. اطلاعات ممکن است، گاهی با استفاده از ترکیبی از امنیت فیزیکی و امنیت IT، امن شوند (مانند: ماژول محاسباتی قابل اعتماد یا رمزنگاری داده و ذخیره‌سازی کلیدهای رمزنگاری در یک دستگاه مقاوم در برابر دست‌کاری و نفوذ) [۹].

تحلیل تهدیدات ما از یک رویکرد سه گامی پیروی می‌کند. ما با یک رویکرد دارایی‌محور آغاز می‌کنیم، که در آن تحلیل‌های محرمانگی[1]، یک‌پارچگی[2] و دسترس‌پذیری[3] (C-I-A) را بر روی دارایی‌های شناسایی‌شده اعمال می‌کنیم. پس از آن به تحلیلی مهاجم‌محور پرداخته و تهدیدات خاص مربوط به احراز اصالت[4]، مجازشناسی[5]، حسابرسی[6] (AAA) را مورد بررسی قرار می‌دهیم. در آخر نیز نگاهی بر تهدیدات وابسته به حریم خصوصی خواهیم داشت. از آنجایی که ما درحال تحلیل تهدیدات سامانه‌ای هستیم که خود در حال طراحی است، ارزیابی ریسک‌های آن به‌تنهایی بسیار مشکل و احتمالی خواهد بود. بنابراین تحلیل ریسک[7] در این بررسی جای ندارد.

۲-۱- پیش‌فرض‌ها و محدودهٔ تحلیل تهدیدات

در این بخش ما محدوده تحلیل تهدیدات را براساس منابع ریسک مورد توجه قرار می‌دهیم. علاوه‌براین چند نوع ترافیک دادهٔ درون‌شبکه را نیز تعریف می‌کنیم. این مفاهیم در بخش بعدی مورد استفاده قرار خواهد گرفت.

۲-۱-۱- منابع ریسک

ما مجموعهٔ منابع ریسکی را که در مفاهیم IT برای دارایی‌های IT قابل پیش‌بینی است، به‌صورت زیر دسته‌بندی می‌کنیم:

- منابع ریسک بشری؛ مثل دزدی، گم‌شدن، تصادف، خطاهای کاربری و حملاتی که توسط کاربران بداندیش آغاز می‌شود. در میان این منابع ریسک، تحلیل تهدیدات صورت‌گرفته، تنها قصد دارد حملات ارادی را شناسایی کند.
- منابع ریسک غیربشری؛ که می‌تواند حاصل پدیده‌های طبیعی مثل سیل یا آتش یا خراب‌شدن دستگاه‌ها باشد. منابع ریسک غیربشری نیز خارج از محدوده مورد نظر تحلیل صورت گرفته است.

با وجود این‌که برخی از منابع ریسک آورده‌شده در بالا در محدوده این تحلیل نمی‌گنجند، اما باز هم امکان تعریف سازوکارهای محافظتی IT جهت کم‌کردن تأثیر آن ریسک‌ها وجود خواهد داشت. برای مثال: ذخیره‌سازی امن کلیدهای رمزنگاری و داده‌های کاربر اثرات منفی دزدیده‌شدن دستگاه را که در محدوده تعریف‌شدهٔ تحلیل تهدیدات قرار ندارد، پوشش داده و این اثرات را کاهش می‌دهد.

۲-۱-۲- انواع ترافیک داده درون شبکه

دو نوع ترافیک شبکه را می‌توان در یک شبکه IoT درنظر گرفت که در ادامه به تشریح آن‌ها می‌پردازیم:

۲-۱-۲-۱- تبادل داده سطح کنترل[8]

ترافیک داده‌ای وجود دارد که برای نظارت و کنترل رفتار کاربرد خاصی که برای آن طراحی شده است، استفاده می‌شود. این نوع جریان می‌تواند شامل داده‌های مدیریت شبکه (در استاندارد سنتی ISO-FCAPS [۱۰])، پیام‌های کنترل مسیریابی، پیام‌های اکتشاف همسایگی، اتحادهای لایهٔ اتصال[9]، دست‌تکانی‌های نشست‌های TCP، درخواست و پاسخ‌های مدیریت شبکه (مثل ورود به مود خواب یا تغییر کانال ارتباطی)، باشد. ترافیک داده سطح کنترل به‌طور معمول برای کاربران نهایی نامعلوم و مخفی بوده و از طرف آن‌ها نیز علاقه‌ای به این نوع داده‌ها وجود ندارد.

۲-۱-۲-۲- تبادل داده سطح داده

این نوع ترافیک داده، در لایهٔ کاربرد مورد استفاده قرار می‌گیرد که برای کاربر نهایی قابل رؤیت بوده و به آن علاقه‌مند است. ما در ادامه از مفاهیم "ترافیک برنامهٔ کاربردی" یا "ترافیک کاربر" برای ارجاع به این نوع ترافیک استفاده می‌کنیم. مثال‌هایی از این نوع داده شامل: داده‌های دمایی انتقال داده شده از گره‌های حس‌گر، گزارش وضعیت یک‌محرک که توسط کاربر به یک گره ارسال شده و پاسخ متناسب با آن، درخواست‌های تغییر وضعیت محرک‌ها و مانند آن است.

[1] Confidentiality
[2] Integrity
[3] Availibility
[4] Authentication
[5] Authorization
[6] Acounting
[7] Risk Assessment
[8] Control Plane Data Exchanges
[9] Link Layer

در سراسر این مقاله تمایزی بین "دادهٔ در حال گذر[1]" و "دادهٔ ساکن[2]" قائل شده‌ایم. دادهٔ در حال گذر برای تشریح داده‌ای استفاده می‌شود که بر روی شبکه در حال انتقال است و دادهٔ ساکن نیز بر داده‌ای اشاره دارد که در یک دستگاه ذخیره شده است. در مورد داده‌های در حال گذر، سازوکارهای جهت افزایش امنیت و حریم خصوصی در ارتباطات انتهابه‌انتها فراهم می‌شود. بخشی از این ارتباطات در زیرساخت‌های شبکه، مثل اینترنت و ISPها رخ می‌دهد که بحث درمورد تهدیدات مربوط به این زیرساخت‌ها خارج از محدوده این مقاله است.

۲-۲- مدل مهاجم

در این بخش دارایی‌های مختلفی از دستگاه‌ها و واحدها را مشخص خواهیم کرد که می‌توانند انواع گوناگونی از خطاها و تهدیدات را به سامانه تحمیل کنند. امنیت IT در مورد حفاظت در برابر موجودیت‌ها و نهادهای بداندیش مورد توجه قرار می‌گیرد و نه در برابر کاربران و سامانه‌های که به‌صورت غیر ارادی و سهوی یک‌پارچگی داده‌ها و فرآیندها را به مخاطره می‌اندازند و همچنین نه در برابر خطاهای حاصل از نوفه‌های کانال که در هنگام ارسال پیام از مبدأ به مقصد به وجود می‌آید [۱۱]. برای این موارد روش‌های مشخصی وجود دارد که نه‌تنها این وضعیت‌ها را شناسایی می‌کند، بلکه از این قبیل مشکلات جلوگیری می‌کند.

ما این موجودیت‌های بداندیش را مهاجم[3] می‌نامیم که قصد دارند به داده‌های محرمانه دستیابی پیدا کرده و یا تلاش کنند تا داده‌های مربوط به یک سرویس صحیح را دست‌کاری کنند. انواع مختلفی از مهاجمان وجود دارد که براساس توانایی بالقوهٔشان در بازیابی اطلاعات، موقعیتشان نسبت به سامانه (به‌عنوان مثال در بیرون یا درون شبکه)، انگیزه‌هایشان و همچنین این‌که به کدام لایه از پروتکل‌های شبکه دسترسی دارند و این‌که از چه چیزی برای سوءاستفاده و راه نفوذ استفاده کرده‌اند، از هم متمایز می‌شوند.

به‌منظور ساده‌سازی تحلیل و دست‌یابی به مدلی کاربردی از مهاجمان، معیار "بدترین حالت[4]" یک وضعیت، در نظر گرفته شده است:

- بدترین حالت، به مهاجمی اشاره دارد که با انگیزهٔ بسیار بالا، به همهٔ جریان‌های داده و رمزگذاری‌نشده شبکه و به اطلاعات شناخته‌شده و عمومی دسترسی داشته و همچنین به همه کانال‌های ارتباطی میان گره‌های مختلف، در تمام لایه‌های شبکه نیز، دسترسی فیزیکی دارد. اساس و منطق انتخاب یک مهاجم قوی به دو قسمت تقسیم می‌شود: از یک سو، داشتن همچنین مهاجمی با شرایط بالا، به‌طوراساسی غیرمنطقی نیست؛ یا حداقل هر مهاجم ضعیفی نیز به‌احتمال بیش از حد محدودکننده است. از سوی دیگر این حالت شامل همهٔ مهاجمان در شبکه می‌شود. این حمله به‌عنوان مهاجم Dolev-Yao شناخته شده است [۱۲].
- از طرفی دیگر؛ نیازمند برخی محدودیت‌ها برابر مهاجم هستیم. اگر مهاجم مورد نظر بتواند رمز سامانه رمزنگاری‌شده را بشکند، پس از آن به‌هیچ‌وجه هیچ حفاظتی در برابر آن وجود ندارد. او قادر خواهد بود اسرار کاربران و دارایی‌ها را بازیابی کند و از این رو سازوکارهای احراز اصالت را دور بزند. در این حالت او می‌تواند خود را یک کاربر جا بزند و داده‌ها را در حین انتقال به هر طریقی که خودش انتخاب می‌کند، تغییر دهد. بنابراین، به‌طور معمول فرض می‌کنیم که رمزنگاری استفاده‌شده، امن و به‌درستی پیاده‌سازی شده است. به‌طور مشابه در این مرحله از طراحی، فرض می‌کنیم که سازوکارهای امنیتی طرح‌ریزی شده، به طور ایمن پیاده‌سازی خواهند شد. این فرض درست است؛ زیرا در این مرحله سازوکارهای پیاده‌سازی‌شده‌ای وجود ندارد که کسی بتواند کارایی آن‌ها را ارزیابی کند.

برای جزئیات بیشتر، براساس پیشنهاد ارائه‌شده توسط Pfitzmann و Fedarrath [۱۳]، ما فرض دیگری علاوه‌بر توانمندی و علاقه‌مندی مهاجم، در نظر می‌گیریم: مقاومت[5] مهاجم در برابر سازوکارهای امنیتی و حریم خصوصی و همین‌طور خود سازوکارهای مورد استفاده:

۱. پیاده‌سازی بی‌عیب و نقص سازوکارهای امنیتی. این فرضیه در بیشتر اوقات غیر واقعی است. پیاده‌سازی امنیتی به‌طورمعمول عیوب و نواقصی دارد؛ اما این پیاده‌سازی‌ها می‌تواند از لحاظ قابلیت‌های امنیتی و نمایش به‌اصطلاح "آسیب‌پذیری‌های معمول[6]" که مهاجمان بدون نیاز به تلاش خیلی زیاد می‌توانند آن‌ها را شناسایی کنند، آزمایش شوند. فرضیه مذکور می‌تواند به روش ضعیف‌تری نیز تنظیم شود: مهاجم

[1] Data in transit
[2] Data at rest
[3] Attacker
[4] Worst-case
[5] Strength
[6] Common Vulnerabilities

قادر به پیداکردن نواقص پیاده‌سازی سازوکارهای امنیتی که امکان دسترسی را به دارایی‌های حفاظت‌شده توسط آن‌ها می‌دهد، نباشد.

۲. مهاجم قادر به حدس‌زدن یا شکستن پروتکل‌های رمزنگاری (که توسط سازمان‌های استانداردسازی امن درنظر گرفته شده‌اند)، نیست.

۳. پروتکل‌های رمزنگاری به‌صورت عمومی در نظر گرفته شده و بنابراین هدف قرار دادن یک دارایی محافظت‌شده برای مهاجم، آسان و امکان‌پذیر خواهد بود. این حالت به این معنی است که دارایی‌ها نمی‌توانند توسط روش‌های رمزنگاری اختصاصی و مخفی حفاظت شوند.

۴. طرح‌های امضا[1] نیز، در پروتکل‌های رمزنگاری در نظر گرفته می‌شوند. آن‌ها بدون عیب و نقص پیاده‌سازی شده و به‌صورت عمومی شناخته شده هستند.

۵. مهاجم قادر به نفوذ به مکانیزم‌های امنیتی فیزیکی نخواهد بود.

مهاجم به‌طور کلی یا یک موجودیت خارجی برای سامانه محسوب می‌شود و یا یکی از اعضای قانونی سامانه در نظر گرفته می‌شود. او قادر است که به‌صورت فعال آغاز به کار کرده و یا به‌صورت منفعل به ارتباطات و جریان‌های داده در کاربردهای مختلف گوش کند.

علاوه‌براین فرض می‌کنیم که مهاجم از وجود دارایی‌ها در سامانه آگاه است. او قادر است اطلاعات را از سامانه جمع‌آوری کرده و با ترکیب‌کردن این اطلاعات پیام‌های ردوبدل‌شده را بسازد. اطلاعاتی از سامانه که او می‌تواند جمع‌آوری کند، شامل موارد زیر است:

۱) اطلاعات عمومی؛

۲) اطلاعاتی که او مجاز به دانستن آن‌هاست، اگر او عضو سامانه باشد؛

۳) پیام‌هایی که او می‌تواند از شبکه شنود یا استراق سمع کند؛

۴) پاسخ‌های مربوط به درخواست‌هایی که او می‌تواند ایجاد کند.

همان‌طور که در بالا اشاره شد، او توسط محدودیت‌هایی که از طریق سازوکارهای امنیتی یا رمزنگاشتی ایجاد شده، محدود خواهد بود.

به این ترتیب، مهاجمانی را که ما در نظر می‌گیریم، کاربران نهایی یا اشخاص بیرونی هستند که به جزئیات داخلی سامانه و یا کانال‌های ارتباطی دسترسی دارند. این شامل شهروندان و همچنین در مورد یک موقعیت مشخص، مراجع ذی‌صلاح محلی، مجموعه‌های عمومی کارکنان و کارمندان آن مجموعه‌ها، می‌شود. البته، مراجع ذی‌صلاح شهر نیز می‌توانند از داده‌های جمع‌آوری‌شده توسط برنامه‌های کاربردی، سوءاستفاده کنند؛ اما باید مورد اعتمادبودن آن‌ها مورد توجه قرار گیرد که شامل موارد زیر می‌شوند:

- توسعه‌دهندگان و فروشندگان حس‌گرها، و توسعه‌دهندگان نرم‌افزارهایی که بر روی اشیای هوشمند و دروازه‌ها اجرا می‌شوند.
- یک‌پارچه‌سازها/فراهم‌کنندگان راه‌حل.
- نصب‌کنندگان تجهیزات و پشتیبانی‌کنندگان.
- فراهم‌کنندگان شبکه.
- توسعه‌دهندگان کاربردها و فراهم‌کنندگان راه‌حل‌های شخص ثالث.

این اشخاص، به‌طوراساسی می‌توانند در قسمت‌های مختلف درب‌پشتی[2] و یا دیگر سازوکارهای بداندیش را قرار داده تا به این طریق از داده‌ها یا قابلیت‌های سامانه سوءاستفاده کنند. اگرچه روش‌هایی جهت مقابله با این‌گونه حملات و یا حداقل‌کردن احتمال یا تأئید آن‌ها وجود دارد، این نوع از حملات را نیز خارج از حوزه بررسی خود قرار می‌دهیم. تمام فروشندگان، دارندگان و تأمین‌کنندگان محصول فرض می‌شود که قابل اعتماد بوده و سازوکارهای مجزایی خارج از موارد موجود در حوزهٔ مورد بررسی ما، جهت مدیریت ریسک مربوط به آن نوع تهدیدات لازم خواهد بود [۱۴].

به‌طورکلی مهاجم مورد توجه ما می‌تواند فعال[3] یا منفعل[4] باشد. یک مهاجم فعال قادر خواهد بود هر نوع جریان داده‌ای را ایجاد کند. بنابراین او قادر است بسته‌های داده و بلوک‌های قابل انتقال را دست‌کاری کرده، پیام‌هایی را از طرف خود یا دیگر شرکت‌کنندگان دوباره ارسال کرده و همین‌طور به‌عنوان یک عضو معتبر از آن دسته رازهای رمزنگاری که برای او در دسترس است، رمزگشایی و بهره‌برداری کند. در نقش یک منفعل، مهاجم مورد نظر

[1] Signature schemes

[2] Backdoor
[3] active
[4] passive

می‌تواند به جریان‌های ارتباطی گوش داده و یا آن‌ها را ضبط کند [۱۵]. بنابراین او قادر است هر نوع اطلاعات ردوبدل‌شده را به‌دست آورده و به‌صورت برخط آن‌ها را تحلیل کند. به این ترتیب یک مهاجم منفعل نمی‌خواهد یا نمی‌تواند آن اطلاعات را به‌صورت فعال مورد استفاده قرار دهد. علاوه‌براین در نظر گرفته می‌شود که مهاجم مورد نظر قابلیت‌های محاسباتی بالا و زمان دسترسی بالایی دارد؛ اما نه به‌اندازه‌ای که بتواند رمزنگاری سامانه را شکسته و یا رازها یا گواهی‌نامه‌های یک سامانه یا موجودیت را حدس بزند. همچنین فرض می‌شود که مهاجم منابع مالی میانه یا بالایی دارد و قادر است درصورت نیاز دستگاه‌های خاصی را نیز تهیه کند؛ اما نه به‌اندازه‌ای که بتواند به‌عنوان‌مثال یک ایستگاه GSM یا امنیت استاندارد مربوط به 3G یا 4G را به خطر بیاندازد.

۲-۳- شناسایی دارایی‌های IT

از آن‌جایی که طراحی یک سامانه کامل هنوز به پایان نرسیده، برخی دارایی‌های IT وابسته به زیرساخت و تعیین‌کننده، فراداده‌ها[1] و همچنین داده‌های مدیریت و راهبری هنوز تعریف نشده‌اند. این شامل داده‌ها و پردازش‌های وابسته به زیرساخت یا سازوکارهای امنیتی که ما قصد پیاده‌سازی آن‌ها را داریم نیز می‌شود. این اطلاعات نیز می‌تواند وابسته به طراحی، شاخص‌ها، جداول مسیریابی، اطلاعات وضعیت کانال، کلیدهای رمزنگاری، جداول پیکره‌بندی، داده‌های مدیریتی، مدل‌های معنایی و مانند آن باشد. دست‌کاری یا خواندن این اطلاعات می‌تواند منجر به تهدیدات و مخاطرات جدی شود که آسیب‌های فراوانی را به‌همراه خواهد داشت.

۲-۳-۱- اعتبارنامه‌های احراز اصالت[2]

اعتبارنامه‌های احراز اصالت، داده‌هایی است که برای شناسایی موجودیت‌های مشارکت‌کننده مثل کلیدهای سری که بین مدیران و کاربران محدودشده، تمایز ایجاد می‌کند، مورد استفاده قرار می‌گیرند. اعتبارنامه‌های احراز اصالت، بخشی از تبادل داده سطح کنترل محسوب می‌شوند.

۲-۳-۲- داده‌های کاربر[3] (U-DATA)

داده‌های کاربر را می‌توان به سه دستهٔ کوچک‌تر تقسیم کرد:

- داده‌های حس‌شده[4] (S-DATA)
- داده‌های تحریک[5] (A-DATA)
- داده‌های برنامه‌های سطح بالا[6] (H-DATA)

تمام داده‌های کاربری، بخشی از تبادلات دادهٔ سطح داده که در بخش ترافیک داده بحث شده، هستند. دسته‌بندی‌های بالا شامل ردوبدل داده‌های واقعی خوانده‌شده و درخواست‌های کاربر که موجب ارسال این داده‌ها شده، است. برای مثال انتقال دادهٔ دمای محیطی خوانده‌شده، به‌عنوان U-DATA در نظر گرفته می‌شود. درخواست کاربر که موجب ارسال داده‌های خوانده‌شده می‌شود، نیز U-DATA در نظر گرفته می‌شود. مثال‌های دیگر از انواع داده‌های کاربر در ادامه بیان می‌شود:

- اندازه‌گیری‌های مصرف انرژی (S-DATA)
- وضعیت محرک‌ها (A-DATA)
- اندازه‌گیری کیفیت هوا (S-DATA)
- درخواست تحریک مثل خاموش‌کردن چراغ (A-DATA)

داده‌های برنامه‌های سطح بالا نیز به‌طورمعمول براساس درخواست‌های کاربر نهایی ارسال می‌شود؛ اما محتوایی مثل فراداده در مورد کاربر و یا پارامترهای الزامی برنامه‌ها مثل موقعیت کاربر، مقصد او و یا مانند آن خواهد داشت. این نوع داده‌ها در بعضی موارد اهمیت بیشتری نسبت به دو نوع دادهٔ دیگر دارد. بنابراین سازوکارهای جداگانه‌ای برای اطمینان از حریم خصوصی و تحویل امن آن‌ها لازم است.

۲-۳-۳- داده‌های فرمان و کنترلی[7] (C&C-DATA)

داده‌های فرمان و کنترلی، داده‌ها و فراداده‌هایی هستند که جهت کنترل، نظارت و مدیریت وضعیت کلی سامانه با هدف اطمینان از صحت عملکرد سامانه، مورد استفاده قرار می‌گیرند. به‌طورکلی، ما مجموعه C&C-DATAهای زیر را در نظر می‌گیریم:

- شناسه‌های EUI-64 [۱۶] برای واسط‌های شبکه بر روی گره‌های حس‌گر و دروازه‌ها؛
- اطلاعات پیشوندی 6LoWPAN که برای ارتباط از طریق یک مش[8] استفاده می‌شود؛
- جداول مسیریابی IPv6.
- اطلاعات تاریخچه استفاده از کانال/طیف؛

[1] Metadata
[2] Authentication Credentials
[3] User Data

[4] Sensed Data
[5] Actuation Data
[6] High-level Application Data
[7] Command and Control Data
[8] Mesh

- مخازن اکتشاف همسایه[1]؛
- داده‌های پیکره‌بندی برنامه‌ها؛
- به‌روزرسانی‌های نسخهٔ برنامه.

۲-۳-۴- نرم‌افزار[2] (S/W)

تمام نرم‌افزارهایی که ما در نظر می‌گیریم، چه در اشیای هوشمند و چه در دروازه‌ها، همگی در حال اجرا هستند. بررسی ما بر روی مؤلفه‌های نرم‌افزاری که بر روی اشیای هوشمند در حال اجرا هستند، تمرکز دارد؛ اما یک استثنا به نام زیرساخت نرم‌افزاری فراهم‌کننده‌های سرویس شبکه نیز وجود دارد. مثال‌هایی از نرم‌افزارهایی که باید مورد محافظت قرار گیرند عبارتند از:

- پیاده‌سازی نرم‌افزاری سازوکارهای امنیت و حریم خصوصی؛
- سیستم‌های عامل (به خصوص در کاربران نهایی ضعیف‌تر، مثل گره‌های حسگر)؛
- پیاده‌سازی نرم‌افزاری پشته پروتکل شبکه؛
- نرم‌افزار گزارش‌دهی و تولید داده؛
- نرم‌افزار تحریک (نرم‌افزاری که وظیفه‌اش دریافت، تأیید و اجرای تحریک‌ها است).

۲-۴- تحلیل و بررسی جریان‌های داده

در این بخش به تشریح جریان‌های داده‌ای که بین اجزای سامانه برقرار است، می‌پردازیم. در بسیاری از کاربردهای IoT اشیای هوشمند و دروازه‌های استفاده شده برای پیاده‌سازی سامانه، یک شبکهٔ مش 6LoWPAN بر روی IEEE 802.15.4 تشکیل می‌دهند. دروازه نیز دارای یک اتصال به اینترنت بوده و از طریق آن با یک سرور در ارتباط است. با درنظرگرفتن این پیش‌فرض‌ها، جریان‌های داده موجود در ادامه بررسی می‌شوند.

۲-۴-۱- جریان‌های U-DATA

از دریچهٔ لایهٔ شبکه از پشته TCP/IP، جریان‌های داده به‌طوراساسی چندجهشی[3] هستند. در طول مقدمات توسعه، جریان‌های U-DATA چندین شیء هوشمند[4] (SO) را در طول مسیر می‌پیمایند که هریک از آن‌ها نقش یک مسیریاب میانی را در شبکهٔ مش 6LoWPAN ایفا می‌کنند. اگر جریان مورد نظر از سرور برنامه کاربردی آغاز و یا به آن ختم شود، آنگاه دروازه نیز به‌عنوان یک مسیریاب عمل کرده و U-DATA بین دروازه و سرور از طریق یک شبکه عمومی (مثل اینترنت) جابه‌جا می‌شود. از داده‌ها هنگام گذرکردن بین دروازه و سرور محافظت خواهد شد؛ اما تحلیل تهدیدات شبکه‌های مورد استفاده در این بین، در حوزهٔ این بخش قرار نمی‌گیرد. همان‌طورکه بیان شد، جریان‌های U-DATA در بین اشیای هوشمند و بین یک شیء هوشمند (SO) و دروازه (ازدریچهٔ لایهٔ اتصال) از طریق اتصالات بی‌سیم IEEE 802.15.4 در محل مورد نظارت، صورت می‌گیرد.

۲-۴-۱-۱- جریان S-DATA: SO به SO؛ SO به دروازه؛ دروازه به سرور

دریچه‌های لایهٔ شبکه و لایهٔ اتصال از جریان‌های S-DATA در قسمت قبل توضیح داده شد؛ اما از دریچهٔ لایهٔ کاربرد، اندازه‌گیری‌های مربوط به حس‌گرها، یکی از دو مقصد زیر را خواهند داشت:

۱. سرور برنامه کاربرد؛
۲. دروازه.

در هر دو مورد، U-DATA اصلاحات مربوط به افزایش امنیت و حریم خصوصی را در اشیای هوشمند میانی، متحمل خواهد شد.

زمانی‌که U-DATA به سرور ارسال می‌شود، از دریچهٔ یک لایهٔ کاربرد، این انتقال می‌تواند:

- به‌طورمستقیم از شیء هوشمند به سرور باشد.
- به سرور از طریق دروازه باشد. در این مورد ممکن است اطلاعات وابسته به امنیت بیشتری (مثل تجمیع یا گمنام‌سازی) اعمال شود.

۲-۴-۱-۲- جریان A-DATA: سرور برنامه کاربردی به SO (دوطرفه)؛ دروازه به SO (دوطرفه)

ابعاد لایهٔ شبکه و لایهٔ اتصال که در بخش قبل مورد بررسی قرار گرفت. اما از لحاظ لایهٔ کاربرد، جریان‌های A-DATA یا از دروازه سرچشمه می‌گیرند و یا از سرور ناشی می‌شوند. در مورد نخست، A-DATA به موقعیت تحت نظارت محدود می‌شود؛ اما در مورد دوم جریان داده می‌تواند در جاهای مختلف ایجاد شود:

- به‌طورمستقیم از سرور به یک یا بیشتر SO؛
- از سرور به SOها از طریق دروازه؛ در این مورد نیز دروازه ممکن است اصلاحات وابسته به امنیت بیشتری (مثل احراز اصالت یا مجازشناسی) را اعمال کند.

[1] Neighbor Discovery
[2] Software
[3] Multihop
[4] Smart Object

۲-۴-۲- جریان‌های C&C-DATA

این جریان‌های داده به عملکرد صحیح پروتکل‌ها و الگوریتم‌های شبکه در کاربردهای مختلف، مربوط می‌شود. برای مثال توسعهٔ یک سامانهٔ نظارتی براساس موارد مختلفی صورت خواهد پذیرفت:IEEE 802.15.4 در لایهٔ اتصال، IPV6، RPL، اکتشاف همسایه و 6LoWPAN در لایهٔ شبکه و همین‌طور در TCP/IP در لایهٔ چهار. تمام پیام‌های کنترلی که توسط آن پروتکل‌ها رد و بدل می‌شوند، یک جریان C&C-DATA را تشکیل می‌دهند. براساس تبادلات بین مبدأ و مقصد از مش C&C-DATA، ما جریان‌های زیر را مشخص می‌کنیم:

۲-۴-۲-۱- جریان C&C-DATA: از SO به SO یا دروازه (دوطرفه)

- دیتاگرام‌های کنترل مسیریابی جهت تشکیل مش 6LoWPAN.
- پیام‌های اکتشاف همسایه IPV6 یا 6LoWPAN-ND [۱۷] برای نگهداری از مخازن ND در SOها و دروازه.
- برقراری نشست TCP و از بین بردن آن.
- مدیریت پیکره‌بندی خواندن و تغییر دادن درخواست‌ها و پاسخ‌ها.

۲-۴-۲-۲- جریان C&C-DATA: از SO به دروازه به سرور (دوطرفه)

- برقراری نشست TCP و ازبین‌بردن آن؛
- مدیریت پیکره‌بندی خواندن و تغییردادن درخواست‌ها و پاسخ‌ها.

۲-۵- تهدیدات و مخاطرات محرمانگی، یکپارچگی و دسترسی پذیری (C-I-A)

در این بخش به قسمت نخست تحلیل مخاطرات با فهرست‌کردن تهدیدات در برابر محرمانگی، یک‌پارچگی و دسترسی‌پذیری می‌پردازیم. مجموعه تهدیدات و مخاطرات مطرح‌شده در شکل۳ قابل مشاهده است.

۲-۵-۱- از دست رفتن محرمانگی اعتبارنامه‌های احراز اصالت (تهدید ۱)

نقض محرمانگی اعتبارنامه می‌تواند جهت آغاز حملات جعل هویت بعدی مورد استفاده قرار گیرد که به‌احتمال منجر به از بین رفتن محرمانگی U-DATA (تهدید ۲) می‌شود.

۲-۵-۲- از دست رفتن محرمانگی U-DATA (تهدید ۲)

بر اساس کاربردی که در آن از شبکه IoT استفاده می‌شود، U-DATA می‌تواند داده‌های خصوصی بوده و بنابراین افشای آن‌ها می‌تواند موجبات نقض حریم خصوصی را فراهم کند.

۲-۵-۳- از دست رفتن محرمانگی C&C-DATA (تهدید ۳)

از دست رفتن محرمانگی C&C-DATA باعث فاش‌شدن اطلاعات توپولوژی شبکهٔ توسعه‌یافته می‌شود. یک کاربر بداندیش یا مخرب می‌تواند متعاقباً از این اطلاعات استفاده کرده و حملات مشخصی را بر روی U-DATA مربوط به یک SO خاص وارد کند.

۲-۵-۴- ازدست‌رفتن محرمانگی نرم‌افزار (تهدید ۴)

ازدست‌رفتن محرمانگی نرم‌افزار می‌تواند تأثیر منفی بر روی توسعه‌دهندگان آن داشته باشد. برای مثال، این ممکن است رازهای تجاری آن‌ها را فاش کند. علاوه‌براین، نرم‌افزار در معرض تلاش‌های مهندسی معکوس قرار می‌گیرد، که این خود موجبات حملات و مخاطرات بیشتر و بدتر را فراهم می‌کند.

۲-۵-۵- ازدست‌رفتن یک‌پارچگی U-DATA (تهدید ۵)

اگر یک حملهٔ موفق صورت گیرد، برنامه شروع به فراهم‌کردن مقادیر نادرست S-DATA خواهد کرد. به‌صورت سخت‌گیرانه‌تر، این حتی یک مورد از نقض یک‌پارچگی A-DATA است که از طریق آن یک کاربر بداندیش و مخرب می‌تواند تحریک‌های نامطلوب و حتی ناقض حریم خصوصی (مثل: باز کردن یک پنجره) را صورت دهد. این حمله می‌تواند به‌عنوان فراهم‌کنندهٔ شرایط اجرای حملات دیگر به محرمانگی و یکپارچگی نرم‌افزار مورد استفاده قرار گیرد. بنابراین بسیار سخت‌گیرانه‌تر باید مورد ملاحظه قرار گیرد.

۲-۵-۶- ازدست‌رفتن یک‌پارچگی C&C-DATA (تهدید ۶)

ازدست‌رفتن یک‌پارچگی C&C-DATA می‌تواند زمانی‌که داده در حالت مستقر یا گذر است، رخ دهد. به‌طور خاص، دست‌کاری اطلاعات مسیریابی، می‌تواند منجر به افت شدید کارایی یا سرویس شده و یا منجر به قطعه‌قطعه‌شدن و دردسترس‌نبودن شبکه از طریق محدودکردن مسیریاب‌هایی که وظیفه نگهداری از ارتباطات را دارند، شود. حمله

ضعیف‌تر دیگر افشای اطلاعات مسیریابی برای یک مهاجم است. در این حالت، مهاجم از اطلاعات مسیریابی، توپولوژی شبکه و یا اطلاعات مربوط به پیکره‌بندی و برقراری اتصال در شبکه، مطلع می‌شود. به این طریق از گره‌های کلیدی و یا اتصال‌هایی که می‌تواند هدف حملات بعدی باشند، آگاهی کسب می‌کند. به‌طور مشابه، یک مهاجم می‌تواند طیف مربوط به اطلاعات حس‌شده را که بین گره‌ها تبادل می‌شود، تغییر داده و نتایج را با هدف بهره‌برداری از حفره‌های طیف در دسترس، دست‌کاری کند (این به‌عنوان "تحریف طیف داده‌های حس‌شده[1]" (SSDF) در شبکه‌های رادیوشناختی[2] شناخته شده است).

ازدست‌رفتن یک‌پارچگی C&C-DATA، به‌احتمال بر روی محرمانگی و دسترس‌پذیری U-DATA تاثیر می‌گذارد. همچنین ممکن است، بر روی محرمانگی، یک‌پارچگی و دسترس‌پذیری نرم‌افزار تأثیر منفی بگذارد. این تهدید ممکن است، به‌عنوان یک تسهیل‌کننده برای حملات بعدی استفاده شود و باید بسیار سخت‌گیرانه مورد ملاحظه قرار گیرد. به‌عنوان مثال، یک حمله SSDF ممکن است به حالتی ختم شود که SOها یک فرکانس پرازدحام را انتخاب کرده و به طبع آن دچار عدم دسترسی به رسانهٔ بی‌سیم شده، که نتیجه‌اش عدم توانایی انتقال داده است. بنابراین نتیجه یک حملهٔ SSDF می‌تواند باعث ازبین‌رفتن دسترس‌پذیری U-DATA (تهدید ۸) شود.

۲-۵-۷- ازبین‌رفتن یک‌پارچگی نرم‌افزار (تهدید ۷)

نقض یک‌پارچگی نرم‌افزار، اثر منفی روی عملکرد آن داشته و ممکن است، نرم‌افزاری غیرکاربردی را ارائه دهد. این حمله ممکن است، برای انجام حملات بعدی از دسته‌بندی‌های مختلف به سامانه استفاده شود. نقض یک‌پارچگی نرم‌افزار می‌تواند اثرات منفی بیشتری بر روی ارزش نرم‌افزار از لحاظ شهرت، بازنگری‌های بد، کاهش تعداد کاربران و کاهش نصب اولیه برنامه شود.

۲-۵-۸- ازبین‌رفتن دسترس‌پذیری U-DATA (تهدید ۸)

این تهدید ممکن است به‌طور همزمان با ازدست‌رفتن محرمانگی رخ دهد؛ که در بعضی موارد احتمال نقض حریم خصوصی و درنتیجه افزایش شدت حمله وجود دارد (به‌عنوان مثال، یک حمله خون‌آشام[3] با هدف تخلیهٔ منبع انرژی از یک دستگاه مبتنی بر باتری). اگر یک SO هدف حملهٔ خون‌آشام موفق قرار گیرد، باتری‌هایش خالی می‌شود و آن SO از دسترس خارج می‌شود. این به منزله یک حملهٔ موفق به دسترس‌پذیری U-DATA است؛ اما محرمانگی U-DATA به خطر نمی‌افتد. از طرفی، حملات جلورانی انتخابی[4] یا حملات Sinkhole نیز قابلیت جلورانی شبکه را به خطر می‌اندازد و این به منزلهٔ نقض دسترس‌پذیری است؛ اما حملات مشابه می‌تواند محرمانگی را نیز به خطر بیاندازد.

۲-۵-۹- ازدست‌رفتن دسترس‌پذیری C&C-DATA (تهدید ۹)

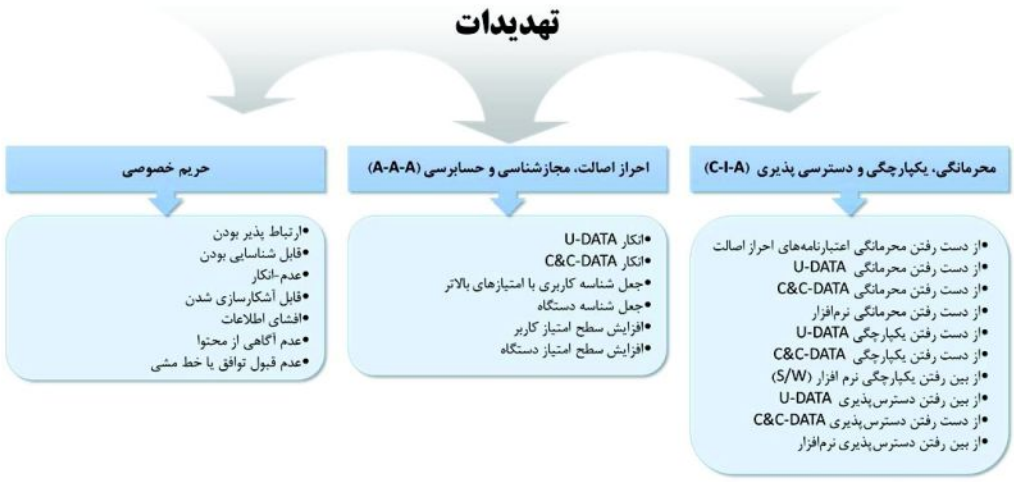
ازبین‌رفتن دسترس‌پذیری C&C-DATA بسیار محتمل است که در برخی SOها منجر به قطعی اتصال از شبکه گسترش یافته شود و از این رو تأثیر منفی بر روی دسترس‌پذیری U-DATA خواهد داشت.

۲-۵-۱۰- ازبین‌رفتن دسترس‌پذیری نرم‌افزار (تهدید ۱۰)

از بین رفتن دسترس‌پذیری نرم‌افزار زمانی رخ می‌دهد که سفت‌افزار[5] نصب‌شده بر روی یک SO یا دروازه قادر به اجرا شدن نباشد. در این حالت سفت‌افزار مورد نظر به‌طور معمول خود را به‌عنوان نرم‌افزار متوقف‌شده، دستگاه‌های غیرپاسخ‌گو یا دستگاه‌های دچار راه‌اندازی مجدد شده، معرفی می‌کند که می‌تواند نتیجه دست‌کاری غیرمجاز باشد. اگر یک کاربر غیرمجاز با اجرای کدهای مخرب بر روی یک SO یا دروازه، حذف یا تغییری در نرم‌افزار ایجاد و یا به یکی از آن‌ها از طریق جعل موفق یک شناسه، دسترسی از راه دور پیدا کند، این تهدید رخ می‌دهد. همچنین ممکن است با تخلیهٔ باتری که توسط حملهٔ خون‌آشام اعمال می‌شود، این تهدید رخ دهد.

ازبین‌رفتن دسترس‌پذیری نرم‌افزار در برخی موارد به‌صورت مستقل رخ خواهد داد؛ اما به‌طور معمول ناشی از نقض یک‌پارچگی نرم‌افزار، یا یک‌پارچگی U-DATA یا یک‌پارچگی C&C-DATA خواهد بود. ازبین‌رفتن دسترس‌پذیری نرم‌افزار همچنین می‌تواند ناشی از طراحی و پیاده‌سازی اشتباه باشد؛ اما از آنجا که این‌ها نتیجه فعالیت‌های بدخواهانهٔ عمدی نبوده است، جزء محدودهٔ این تحلیل قرار نمی‌گیرد.

[1] Spectrum Sensing Data Falsification
[2] Cognitive Radio
[3] Vampire
[4] Selective Forwarding
[5] Firmware



(شکل-۳): دسته‌بندی انواع تهدیدات بر اینترنت اشیا

۲-۶- تهدیدات بر روی احراز اصالت، مجازشناسی و حسابرسی (AAA)

در این بخش به تهدیدات احراز اصالت، مجازشناسی و حسابرسی می‌پردازیم. همان‌طور که در بخش‌های قبل گفته شد، این تهدیدها اغلب به انجام مرحلهٔ دوم حملات منتهی می‌شود که این مسئله باعث نقض محرمانگی، دسترس‌پذیری و یک‌پارچگی دارایی‌های IT خواهد شد.

۲-۶-۱- انکار[1] U-DATA (تهدید ۱۱)

این تهدید زمانی رخ می‌دهد که منبع U-DATA بعدها ادعا می‌کند که U-DATA توسط منشأ دیگری تولید شده است. در مورد S-DATA، منشأ یک SO است و باید امکان این وجود داشته باشد که SOها برای تولید S-DATA پاسخ‌گو باشند. فرمان‌های A-DATA نیز می‌توانند به‌طور مستقیم توسط یک کاربر داده شود، یا این فرمان‌ها می‌توانند به‌صورت خودکار و مبتنی بر برنامه‌ریزی یا رویداد که توسط کاربر مشخص شده، داده شود. در هر دو مورد، سامانه باید قادر باشد تا کاربران را نسبت به تحریک دستی و همچنین تعریف یک زمان‌بندی یا رویداد، پاسخ‌گو نگه دارد.

۲-۶-۲- انکار C&C-DATA (تهدید ۱۲)

این تهدید زمانی رخ می‌دهد که یک مهاجم قادر است بعدها موجودیت دیگری را متقاعد کند که مهاجم، منبع C&C-DATA نبوده یا حتی قادر باشد موجودیت دیگری را متقاعد کند که داده در جای دیگری تولید شده است. C&C-DATA توسط SOها یا دروازه تولید می‌شود؛ که در این صورت سامانه باید قادر باشد دستگاه‌ها را نسبت به تولید C&C-DATA پاسخ‌گو نگه دارد. از آنجا که این حالت نیازمند روشی برای شناسایی منحصربه‌فرد دستگاه‌ها خواهد بود، سازوکارهای عدم انکار مفاهیم حریم خصوصی را می‌توان در برداشته باشد.

۲-۶-۳- جعل شناسه کاربری[2] با امتیازهای بالاتر (تهدید ۱۳)

این تهدید زمانی رخ می‌دهد که کاربران بداندیش با تظاهر به این‌که مدیر یا سرپرست سامانه هستند، دستورهایی را ارسال کنند. در انجام این کار، آن‌ها ممکن است قادر به خواندن و تغییر در پیکره‌بندی سامانه شوند و درنهایت منجر به کاهش محرمانگی، یک‌پارچگی و دسترس‌پذیری دارایی‌ها شوند [۱۸].

۲-۶-۴- جعل شناسه دستگاه (تهدید ۱۴)

این تهدید زمانی رخ می‌دهد که یک دستگاه با تظاهر به این‌که دستگاه یا گره دیگری است، به شبکه بپیوندد. اگر یک مهاجم بتواند بدون احراز اصالت به زیرساخت شبکه بپیوندد و یا هویت خود را جعل و یا از هویت گره‌های دیگر به‌عنوان

[1] Repudiation

[2] Identity Spoofing

هویت خود استفاده کند، بنابراین می‌تواند نقش یک گره مشروع و قانونی را که درقبل در شبکه بوده، ایفا کند. این نفوذگر ممکن است، قادر باشد تا داده‌های خوانده‌شدهٔ گزارش‌شده یا پیام‌های کنترلی نادرست را ارائه دهد. مهاجم همچنین می‌تواند به‌منظور حملات بیشتر، ترافیک داده‌ای را به سمت خود هدایت کند. اگر او به‌طور مداوم گره‌های جعلی را اضافه کند، منابع زیرساخت (مثل فضای در دسترس و قدرت‌های محاسباتی برای مدیریت شناسه و جداول مسیریابی بزرگ) کاهش یافته و منجر به از دسترس خارج‌شدن سامانه می‌شود. این حالت باعث نقض محرمانگی، یک‌پارچگی و دسترس‌پذیری U-DATA و همچنین C&C-DATA در حالت گذر می‌شود [۱۹].

۲-۶-۵- افزایش سطح امتیاز کاربر[1] (تهدید ۱۵)

این تهدید زمانی رخ می‌دهد که کاربر دسترسی سطح بالاتری از سطح دسترسی موجود خود به سامانه را به‌دست آورد. درنتیجه، کاربر بداندیش پس از آن می‌تواند U-DATA را بخواند و یا A-DATA را بدون داشتن مجوز این کار در سامانه، ارسال کند. این حالت منجر به نقض محرمانگی، یک‌پارچگی و دسترس‌پذیری U-DATA و همچنین C&C-DATA در حالت گذر می‌شود.

۲-۶-۶- افزایش سطح امتیاز دستگاه (تهدید ۱۶)

این تهدید زمانی رخ می‌دهد که دستگاه، نقش دستگاه‌های دیگر با امتیاز بالاتر را برعهده بگیرد. به‌عنوان مثال، اگر یک SO نقش دروازه را بر عهده بگیرد. در تمام موارد، یک حملهٔ موفق از این طبقه‌بندی می‌تواند محرمانگی، یکپارچگی و دسترس‌پذیری U-DATA و همچنین C&C-DATA را در حالت گذر نقض کند.

۲-۷- تهدیدات حریم خصوصی

روش استنباط حریم خصوصی که در این بخش استفاده شده است، از روش LINDDUN که توسط Deng در [۲۰] پیشنهاد شده، پیروی می‌کند، که این روش نیز هم‌ارز با چرخه حیات امنیت[2] معرفی‌شده توسط مایکروسافت (STRIDE) می‌باشد. هر حرف از کلمهٔ LINDDUN مربوط به یک تهدید حریم خصوصی است که در ادامه به تشریح این تهدیدات می‌پردازیم.

[1] User Privilege Elevation
[2] Security lifecycle

۲-۷-۱- ارتباط‌پذیربودن[3] (تهدید ۱۷)

ارتباط‌پذیربودن قابلیت تعیین مناسب تفاوت‌های دو یا چند مورد از بخش‌های مورد علاقه[4] (IOI) (مانند: موضوعات، پیام‌ها و واکنش‌ها) است. به‌عنوان مثال، نمونه حمل‌ونقل هوشمند را در نظر بگیرید. داده‌های ترافیکی جمع‌آوری‌شده توسط خودروهای دارای GPS می‌تواند به‌طور کامل گمنام باشند. با این حال، اگر درخواست برای این نوع داده‌ها (داده‌های C&C-DATA) از یک سرور به خودرو بتواند هر دفعه به یک خودروی خاص متصل شود، آن‌گاه داده‌های ترافیکی نمی‌توانند همچنان گمنام بمانند.

۲-۷-۲- قابل شناسایی‌بودن[5] (تهدید ۱۸)

قابلیت شناسایی به مجموعه‌ای از موضوعات یا IOIها اشاره دارد. این توانایی بدین معنی است که مهاجم به اندازه‌ی کافی قادر به شناسایی موضوعات در این مجموعه باشد. این می‌تواند زمانی رخ دهد که U-DATA به اندازه کافی تجمیع نشده باشد و مجموعه‌ی مشخصی از U-DATAها بتواند به عنوان موضوع مرتبط به یک کاربر خاص شناسایی شود.

۲-۷-۳- عدم-انکار[6] (تهدید ۱۹)

عدم انکار، عدم توانایی زیر سؤال‌بردن اعتبار یک وضعیت تأیید شده را توصیف می‌کند. این برای حفظ امنیت ضروری است؛ اما به‌عنوان یک تهدید برای حریم خصوصی نیز باید در نظر گرفته شود. Deng در [۲۰] عدم انکار را به‌عنوان "قابلیتی از یک مهاجم توصیف می‌کند که شواهد و مدارک را برای مقابله با ادعاهای طرف انکارکننده جمع‌آوری و ثابت می‌کند که یک کاربر می‌داند کاری را انجام داده یا چیزی را گفته است". این ممکن است دوباره در موضوع حمل‌ونقل هوشمند اتفاق بیافتد، زمانی‌که یک کاربر به‌طور ناشناس داده‌ای را برای موقعیت X گزارش دهد که در زندگی شخصی یا موقعیتش مشکل‌ساز است و یک مهاجم می‌تواند ثابت کند که داده باید توسط آن شخص، در آن موقعیت و در یک نقطهٔ زمانی خاص جمع‌آوری شده باشد (به‌عنوان‌مثال گزارش یک تصادف). کاربر نیز قادر نخواهد بود که نقش خودش را به‌عنوان منبع H-DATA مربوطه انکار کند.

[3] Linkability
[4] Items Of Interest
[5] Identifiability
[6] Non-repudiation

۲-۷-۴- قابل آشکارسازی‌شدن[1] (تهدید ۲۰)

آیا یک مهاجم توانایی این را دارد که تشخیص دهد یک موضوع یا یک IOI وجود دارد یا نه؟ Deng در [۲۰] نمونه‌ای از پیام‌ها را به‌عنوان IOIها نشان داده است: اگر پیام‌ها قابل آشکارسازی باشند، بنابراین به اندازهٔ کافی قابل تشخیص هستند. به‌عنوان مثال نوفه‌های تصادفی. این می‌تواند در مورد مدیریت انرژی در خانه مورد استفاده قرار گیرد. C&C-DATA زمانی را که یک کاربر خارج از خانه است، ارسال می‌کند. یک مهاجم ممکن است به پیام‌های تصادفی C&C-DATAکه از سمت کاربر در فواصل زمانی تصادفی ارسال شده است، اطلاع یابد. اگر آن مهاجم هنوز هم بتواند بین پیام‌های تصادفی و پیام‌های واقعی تمایز قائل شود، مهاجم از قابلیت آشکارسازی بهره برده است.

۲-۷-۵- افشای اطلاعات[2] (تهدید ۲۱)

افشای اطلاعات بسیار نزدیک به هدف امنیتی محرمانگی است. عنوان این تهدید، افشای اطلاعات شخصی به افرادی که مجوز دسترسی به این اطلاعات را ندارند، است. محرمانگی به‌عنوان یک هدف امنیتی، IOIها را به یک روش دو وجهی قابل خواندنی و غیر قابل خواندنی برای شخصی خاص طبقه‌بندی کرده است. به غیر از طرف‌های دارای دسترسی و مجاز، افشای اطلاعات در مورد این‌که چه نوع اطلاعاتی افشا شده است، نیز، تعریف می‌شود. اگر سازوکارهای امنیتی مناسب اعمال نشود، افشای U-DATA ممکن است در هر موردی اتفاق بیافتد. علاوه‌براین، اجرای سیاست‌های حفظ حریم خصوصی الزامی است. U-DATA ممکن است در بازهٔ زمانی خاصی در دسترس قرار گیرد؛ اما پس از آن از دسترسی به آن ممانعت شود.

۲-۷-۶- عدم آگاهی از محتوا[3] (تهدید ۲۲)

این مخاطره، تهدید مربوط به عدم آگاهی از اطلاعات افشاشده برای سامانه در مورد یک موضوع خاص را توصیف می‌کند. عدم آگاهی از این‌که چه مقدار اطلاعات افشا شده و این‌که این اطلاعات به یک مهاجم اجازه بازیابی شناسهٔ آن موضوع را می‌دهد و یا چگونه اطلاعات نادقیق و نادرست می‌تواند موجب تصمیمات و واکنش‌های غلط شود. برای مثال می‌توان به‌اندازه‌گیری نوفهٔ محیط اشاره کرد. مساله این است که آیا مهاجم با افشای مقادیر نوفهٔ محیط قادر به شناسایی گفتار و افشای هر کلمه که گفته شده، است؟

[1] Detectability
[2] Information Disclosure
[3] Content Unawareness

۲-۷-۷- عدم تعهد به توافق یا خط‌مشی[4] (تهدید ۲۳)

این تهدید عدم تعهد یک سامانه به خط مشی‌های اعلام‌شده و یا تعهدات او نسبت به توافق صورت‌گرفته با نهادهای مرتبط با داده را تعریف می‌کند. بدون هیچ ضمانتی از سیستم، داده‌های موجودیتی خاص، ممکن است علی‌رغم توافق او افشا شده و یا مورد استفاده قرار گیرد و یا حتی توافقات یا خط مشی‌های متفاوتی تعریف شود.

۳- فناوری‌های توانمندساز و راه‌حل‌های طراحی

هدف از این بخش معرفی رویکردها و راه‌حل‌های پیشنهادشده برای چیره‌شدن بر چالش‌های امنیت و حریم خصوصی است که در بخش قبل به آن‌ها اشاره شد. بر اساس آنچه در [۲۱] بیان شده، راه‌حل‌های موجود را می‌توان به دو قسمت تقسیم کرد: قسمت نخست راه‌حل‌ها و رویکردهایی که فقط برای شبکه‌های IoT پیشنهاد شده است و قسمت دوم نیز راه‌حل‌ها و رویکردهایی که به طور کلی مطرح شده‌اند؛ اما قابلیت استفاده از آن‌ها در IoT نیز وجود دارد. در ادامه ما به همین ترتیب به بیان راه‌حل‌ها می‌پردازیم. نکته قابل ذکر این‌که، برخی از راه‌حل‌های پیشنهادشده ممکن است شبیه به هم بوده و یا بخش‌هایی از آن‌ها برهم انطباق داشته باشند.

۳-۱- راه‌حل‌های پیشنهادشده برای شبکه IoT

۳-۱-۱- ابزار کنترل مصرف

سیاست‌های کنترل مصرف مشخص‌شده در [۲۲] شامل مجازشناسی‌ها و الزاماتی است که به‌عنوان قواعد اجرای رویداد-شرط-عمل[5] (ECA) تصریح شده‌اند. این قواعد به‌عنوان مرجعی برای مجموعه مدل‌های طراحی که ابعاد مختلف سامانه‌های IoT را نشان می‌دهد، استفاده می‌شود. این راه‌حل که نظارت بر قواعد ECA و چگونگی اجرای اصول امنیتی را شامل می‌شود، به‌عنوان ابزار امنیتی مدل‌محور یا Seckit نامیده می‌شود [۲۳؛ ۲۴]. Seckit شامل مجموعه‌ای از فرامدل‌ها جهت توصیف ساختار، اطلاعات، رفتار، زمینه‌ها، شناسه‌ها، قواعد سازمانی و قواعد امنیتی یک سامانه رایانه‌ای می‌شود. این فرامدل‌ها حداقل‌های مورد نیاز برای مهندسی امنیت را تأمین کرده و به این صورت نیازمندی‌های امنیت و حریم خصوصی را فراهم می‌کند.

[4] Policy and consent Noncompliance
[5] Event-Condition-Action

۳-۱-۲- سیاست‌های جریان چسبنده

سیاست‌های الصاق به جریان، سیاست‌های چسبندگی برای داده را با سیاست‌های جریان داده ترکیب می‌کند. به این معنا که یک بخش داده در یک سامانه که از این فناوری استفاده می‌کند با یک خط‌مشی امنیتی همراه خواهد بود که چگونه یک داده می‌تواند مورد استفاده قرار گیرد و این‌که کدام شرایط را قبل از این‌که یک داده به موجودیت دیگر منتقل شود، باید فراهم شود، تشریح می‌کند. معماری امنیتی پیشنهادشده در [۲۵] به‌شدت وابسته به سیاست‌های جریان چسبنده است.

۳-۱-۳- میان‌افزار امن مبتنی بر مدیریت خط‌مشی

از آن‌جاکه بسیاری از کاربردهای آتی IoT نیازمند به اشتراک‌گذاری خودکار زمینه‌ها[1] که به‌صورت خودکار توسط حس‌گرها جمع‌آوری شده است، خواهد بود؛ حفظ حریم خصوصی زمینه‌ها نیز یک مفهوم جدایی‌ناپذیر است. حریم خصوصی در [۲۶] بر سه نکتهٔ زیر تمرکز دارد:

۱) حفظ حریم خصوصی طراحی و پیاده‌سازی سازوکارهای و پروتکل‌های به اشتراک‌گذاری اطلاعات زمینه‌ها.

۲) توسعه ابزارهای استخراج که خط‌مشی‌های حریم خصوصی را به‌طور خودکار از مجموعه‌ای از سرویس‌های تحت وب جمع‌آوری و تولید می‌کند.

۳) یک‌پارچه‌سازی این سازوکارها، پروتکل‌ها و ابزارها، در یک بستر کشف دادهٔ تطبیقی که در [۲۶] توسعه داده شده است. به‌اشتراک‌گذاری زمینه‌ها، اشیا را قادر می‌سازد تا به این سؤال که چه اطلاعاتی باید با چه کسی به اشتراک گذاشته شود، پاسخ‌دهند. به این ترتیب، این مسأله که شیء یک خط‌مشی حریم خصوصی خوب تعریف‌شده داشته باشد که شامل اشیای قابل اعتماد و مشخصات زمینه‌های قابل به اشتراک‌گذاری شود، به‌صورت خودکار پاسخ داده خواهد شد.

۳-۱-۴- مدیریت خط‌مشی مبتنی بر توانمندی

مدیریت خط‌مشی مبتنی بر توانمندی در حوزه مدیریت امنیت، مانند سازوکار کنترل دسترسی (و سازوکارهای مبتنی بر توانمندی) که در [۲۷] انجام شده، ارزشمند خواهد بود؛ چراکه جداکردن مسائل تضمین امنیت را در بین طرفین درگیر (مثل اشیای هوشمند و سرویس‌ها) امکان‌پذیر ساخته و به این ترتیب نیاز به میان‌افزار پیچیده را کاهش می‌دهد. علاوه‌براین سازوکار پیشنهادشده در [۲۷] کنترل دسترسی را از مدیریت شناسه جدا کرده و به این صورت تلاش امنیتی و پیچیدگی میان‌افزار قابل اعتماد را به‌شدت کاهش می‌دهد.

۳-۱-۵- قراردادها

جهت تحلیل بهینهٔ سرویس‌ها و ترکیب آن‌ها و همین‌طور جهت تشریح فعالیت‌های مربوط به امنیت سرویس‌های امنیتی، [۲۵] مفهوم فرادادهای امنیتی را نیز مطرح کرده است. قراردادها تعهد یک سرویس نسبت به بستر را در مورد رفتارکردن براساس یک اصول مشخص توصیف می‌کنند. قراردادهای تعریف‌شده در [۲۵] متعهد می‌شوند که وضعیت امنیت داده‌ها و موجودیت‌های سامانه را در یک مسیر ازپیش‌تعیین‌شده تغییر داده، پیش‌شرط‌هایی را که باید قبل از اجرا برآورده شوند، تعیین کرده و جریان داده را در طول اجرا تشریح کنند.

۳-۱-۶- مدل‌های راستی‌آزمایی[2] و آزمایش

تکنیک‌ها و فناوری‌هایی که در [۲۸] توسعه داده شده‌اند، بیشتر تلاش‌های مربوط به مدل‌کردن، راستی‌آزمایی و آزمایش سرویس‌های تحت وب را پوشش می‌دهد. این گام به‌طورمعمول انتظار می‌رود که در طول فرآیند توسعهٔ سرویس اتفاق بیافتد. بنابراین، ابزارهایی که توسط [۲۸] پیاده‌سازی شده‌اند، باید با محیط‌های توسعهٔ سرویس (SPE) یک‌پارچه شوند. در این مورد این پروژه از بستر Eclipse استفاده کرده است. ابزار طراحی‌شده در [۲۸] فناوری‌های بسیار جدیدی را برای آزمایش نفوذ، آزمایش امنیت، یادگیری خودکار، وارسی‌کردن مدل و همچنین تکنیک‌های نتیجه‌گیری خودکار، با یکدیگر ترکیب می‌کند.

۳-۱-۷- احراز اصالت/صدور مجوز

سرور صدور مجوز پیشنهادشده توسط [۲۹] مرکزی جهت مدیریت امنیت محسوب می‌شود. همهٔ طرف‌های ارتباط می‌بایست مدیریت صدور مجوز و مدیریت کاربر را به سرور صدور مجوز بسپارند. سرور صدور مجوز جداکردن ایجاد اعتماد و امنیت داده‌ای را که بین مصرف‌کننده منبع (برنامه کاربردی) و فراهم‌کننده سرویس ردوبدل می‌شود امکان‌پذیر

[1] Context

[2] Verification

می‌سازد. توانمندساز اعتماد در انتقال داده درگیر نمی‌شود؛ این جدایی امکان پیاده‌سازی نیازمندی‌های حریم خصوصی را فراهم می‌کند. پروتکل امنیتی نیز امکان امنیت انتها به انتها بین مصرف‌کننده منبع و فراهم‌کننده منبع را فراهم می‌کند. به این ترتیب برنامه کاربردی با مصرف‌کننده بر اساس قواعد تعیین‌شده توسط کاربر به منابع سمت کاربر دسترسی پیدا می‌کند.

در این مورد، [۳۰] نیز سازوکارهای را برای ارتباطات شیء با شیء و شیء با اینترنت پیاده‌سازی کرده تا اطمینان یابد که متجاوزان یا کاربران/ اشیای غیرمجاز به سامانه دسترسی پیدا نخواهند کرد.

۳-۱-۸- صدور مجوز و ترکیب سرویس با استفاده از HANDLE

در [۳۱] با استفاده از سامانه HANDLE ایده بخش قبل را گسترش داده تا به مسأله صدور مجوز امکان گسترش به چندین حوزه مدیریتی را بدهد. بخش قبلی که از [۲۹] مطرح شده بود بر سامانه مدیریت صدور مجوز مرکزی تاکید داشت. با کمک سامانه HANDLE درحقیقت یک دامنهٔ HANDLE اصلی وجود دارد. با این وجود، ساختار سامانه به‌گونه‌ای است که هنگامی‌که یک موجودیت در سرویس سراسری HANDLE ثبت می‌شود، آن موجودیت مجاز به راه‌اندازی، ثبت و مدیریت عمدهٔ شناسه‌های فضای بعد از خودش (پسوندی)، خواهد بود. در حال حاضر این مسأله حاکمیتی است که CNRI[1] اجازهٔ دو نوع از پذیره‌نویسی[2] را می‌دهد: یکی نرخ خیلی پایین، اگر کسی تنها جهت ثبت‌نام شناسه‌ای دیگر در یک دامنه، مجاز شناخته شده باشد؛ و یا نرخی که هزار برابر بالاتر بخواهد مجاز شناخته شود تا یک طور کامل یک فضای شناسه پسوندی را مدیریت کند.

۳-۱-۹- رمزنگاری در IoT

در این بخش سامانه‌های رمزنگاری مختلفی را که توسط مراجع مختلف معرفی شده‌اند، تشریح می‌کنیم:

۳-۱-۹-۱- طرح‌های امضای منعطف[3]

طرح‌های امضای منعطف (MSS) در [۳۲] پیشنهاد شده است. MSS شبیه امضاهای دیجیتال کلاسیک بوده و تلاش می‌کند، داده‌های امضاشده را در برابر تغییرات بدخواهانهٔ شناسایی‌نشده محافظت کند. مفهوم امضاهای منعطف به یک طرف مشخصی که پیوسته گندزدا[4] را صدا زده است، اجازه می‌دهد تا توسط امضاکننده مجاز شناخته شده و بتواند از یک راه مجاز، پیام ازقبل امضاشده را تغییر دهد. برای تمام فعالیت‌هایی که مجاز نباشند و تمام طرف‌هایی که به‌عنوان گندزدا تعریف نشده باشند، هرگونه تغییر منجر به شکست تصدیق امضا خواهد شد. به این ترتیب، MSS می‌تواند تنها به دروازه‌های حریم خصوصی[5] مشخصی اجازه فعالیت بدهد تا به‌عنوان گندزدا تغییراتی را در حریم خصوصی اطلاعاتی که از لحاظ تمامیت محافظت شده‌اند، ایجاد کند. این کار یک‌پارچگی را در مقایسه با مقدار اصلی تغییرنیافته کاهش می‌دهد. با این وجود در رویکرد MSS این تعادل می‌تواند برای کاربردهایی که سطحی از حفاظت از یک‌پارچگی و سطحی از حریم خصوصی را نیاز دارند، به‌طوری مناسب تنظیم شود.

۳-۱-۹-۲- حس‌کردن فشرده[6]

حس‌کردن فشرده (CS) که توسط [۳۳] پیشنهاد شده است، امکان کسب رمزنگاری خیلی سطح بالا را در کنار بهره‌وری مصرف انرژی که دو نیاز اساسی کاربردهای IoT محسوب می‌شوند، فراهم می‌کند. این تکنیک به بالابردن امنیت و حریم خصوصی در IoT کمک خواهد کرد.

۳-۱-۹-۳- تمامیت و اصالت رمزنگاری

جهت اطمینان از این‌که متجاوزان و کاربران/اشیای غیرمجاز به سامانه دسترسی نخواهند یافت، [۳۲] بر روی احراز اصالت گام‌به‌گام، انتها‌به‌انتها و مبتنی بر PKI و با درنظرگرفتن محدودیت منابع در اشیای هوشمند، تحقیق کرده است. در [۳۴] نیز به رمزنگاری و احراز اصالت برای اشیای هوشمند دارای محدودیت، پرداخته شده است که برای این‌کار یک پروتکل احراز اصالت دوطرفهٔ امن و بهینه و همین‌طور یک طرح توافق کلید معرفی کرده که مبتنی بر رمزنگاری خم بیضوی (ECC) هستند [۳۵]. این رویکرد امکان برقراری ارتباط امن را با منبع محاسباتی ضعیف بر روی اشیای هوشمند فراهم می‌کند. این رویکرد یک روال "انتصاب کلید خارج ازخط" معرفی می‌کند که برای احراز اصالت هر گره از طریق تولید زوج‌کلید عمومی/خصوصی برای رمزنگاری و رمزگشایی، مورد استفاده قرار می‌گیرد. احراز اصالت با تولید یک کلید خصوصی مبتنی بر عدد نخست ذخیره‌شده درون گره امکان‌پذیر می‌شود.

[1] Corporation for National Research Initiatives
[2] Subscription
[3] Malleable Signature Schemes
[4] Sanitizer
[5] Privacy Gateways
[6] Compressed Sensing

۳-۱-۹-۴- مولد عدد تصادفی حقیقی سبک‌وزن

پروژه BUTLER [۳۴] که توسط مجموعه‌ای از چندین دانشگاه در اتحادیه اروپا انجام شده است، تجربیات مختلفی را در ابعاد مختلف سنجش مجموعه‌هایی از داده‌های حس‌گرهای فیزیکی تعبیه‌شده در گره‌ها و ویژگی‌های رادیویی آن‌ها کسب کرده است. BUTLER آنتروپی را که در هر منبع وجود دارد، توسط تخمین زننده‌های آنتروپی-حداقل[1] که توسط NIST در آخرین مستند خودش در سال ۲۰۱۲ منتشر کرده، تحلیل کرده است. نوآوری این تحلیل‌ها درحقیقت یک تحلیل آماری است که بر روی نمونه‌های منبع داده انجام می‌شود، نه بر روی خروجی‌های مولدهای تصادفی.

BUTLER چندین حس‌گر مرتبط را مورد ارزیابی قرار داده است تا آنتروپی آن‌ها را در مودهای غیرواقعی بررسی کند. اما هنگامی‌که گره‌ها در حالت بیکار[2] هستند، حس‌گرها نیز فعالیت نداشته و بنابراین آنتروپی کاهش می‌یابد. با مشاهده این حقیقت که همهٔ گره‌ها قادر به دریافت یک سیگنال رادیویی هستند، BUTLER بر روی تحلیل آمارهای رادیویی تمرکز کرد: RSSI (نمایشگر قدرت سیگنال دریافتی[3])، LQI (نمایش‌گر کیفیت اتصال[4]) و همین‌طور بسته‌های نادرست دریافت‌شده توسط گره‌ها که به‌عنوان خطاهای افت کانال محسوب می‌شوند برای یک اتصال نظیر به نظیر، یکتا محسوب می‌شوند. در نتیجه، LQI و بسته‌های نادرست، منابع آنتروپی مربوطه هستند. بنابراین BUTLER شروع به طراحی یک مولد عدد تصادفی حقیقی سبک‌وزن کرده که می‌تواند در گره‌های خیلی کوچک که با سیستم‌عامل Contiki کار می‌کنند، تعبیه شود. چندین آزمایش سلامت نیز جهت پویش سلامت منبع آنتروپی تعبیه‌شده در دستگاه در حین اجرا، نیز توسعه داده شده است. یک مولد عدد تصادفی حقیقی نمی‌تواند تنها بر یک منبع استوار باشد. در نتیجه، چندین منبع همراه با آزمایش سلامتشان مورد توجه قرار گرفته‌اند. BUTLER علاوه بر طراحی نهایی TRNG مورد نظر، یک فرآیند پیش‌پردازش را نیز تعریف کرده است.

مطالعاتی که منجر به طراحی یک مولد عدد تصادفی حقیقی تعبیه‌شده گردید، گره‌ها را قادر می‌سازد تا مشخصه‌های رمزنگاشتی مخصوص خود را تولید کنند. با این وجود، یک گره قادر به مدیریت گواهی X.509 نخواهد بود. بنابراین یک سازوکار دست‌تکانی مبتنی بر فرضیه انتشار کاهش‌یافتهٔ کلید عمومی یک دروازه، پرکاربرد خواهد بود.

۳-۱-۹-۵- سرور صدور مجوز محلی

در [۲۹]، استفادهٔ هم‌زمان از سرور صدور مجوز در لایهٔ کاربرد و سازوکار خودراه‌اندازی در لایهٔ حس‌گرهای بی‌سیم، شبکه را قادر خواهد ساخت که مساله امنیت انتهابه‌انتها و گام‌به‌گام را بین یک گره حس‌گر مربوط به حوزه IoT و یک برنامه کاربر نهایی متصل به اینترنت، حل کند. دروازهٔ قرارگرفته در مرز بین دنیای اینترنت و محدوده حس‌گرهای بی‌سیم، ارتباطات استاندارد را برای قابلیت عملیات مشارکتی تضمین می‌کند. جهت سازوکار امنیتی گام‌به‌گام، دروازه برای سرور صدور مجوز در فضای اینترنت، احراز اصالت شده؛ همچنین گره حس‌گر نیز برای دروازه در همان محدوده حس‌گرهای بی‌سیم احراز اصالت می‌شود. اعتبارنامه‌های امنیتی تولیدشده توسط سرور صدور مجوز می‌تواند توسط دروازه مورد استفاده قرار گیرد. این سازوکار برای سناریوهای سیار نیز مفید خواهد بود. برای سازوکار امنیتی انتهابه‌انتها نیز گره حس‌گر برای سرور صدور مجوز جهت بازیابی اعتبارنامه‌های امنیتی، احراز اصالت خواهد شد.

۳-۱-۹-۶- تولید کلید محرمانه[5] مبتنی بر تئوری اطلاعات

در انتها، [۳۶] طرح‌های پویا و مبتنی بر تئوری اطلاعات تولید کلید محرمانه (SKG) را برای ارتباطات برد کوتاه[6] (SRC) پیشنهاد داده است. هدف، ایجاد امکان ارتباط طرفین تبادل، جهت تولید محلی کلیدهای محرمانه و مقداردهی به سامانه‌های رمزنگاری تعبیه‌شدهٔ آن‌ها بدون استفاده از رمزنگاری کلاسیک و محاسباتی مطرح‌شده در بالا است. طرح‌های تبادل کلید فعلی، در چارچوب محرمانگی حاصل از تئوری اطلاعات از آنتروپی کانال ارتباطی بهره برده تا بیت‌های محرمانه را استخراج کند. با این وجود، برای سناریوی مورد توجه، که ویژگی اصلی آن اتصال‌های LOS[7] و خیلی کوتاه بین دستگاه‌ها است، فرضیات قبلی دیگر معتبر نیستند؛ بنابراین طرح‌های SKG جدید پیشنهادشده، از شرایط AWGN[8] مواجه‌شده توسط سیستم‌های SRC

[1] Min-entropy
[2] Idle
[3] Received Signal Strength Indicator
[4] Link Quality Indicator

[5] Secret key generation
[6] Short range communication
[7] Line-of-Sight
[8] Additive White Gaussian Noise

استفاده کرده تا نواحی محرمانه جغرافیایی را ایجاد کند که استراق سمع‌کنندگان نتوانند فازهای تبادل‌شده بین یک زوج قانونی را به‌دست آورند.

۳-۱-۱۰- توابع مدیریتی

در [۳۲] سازوکارهای خودمدیریت و خودنظارت توزیع‌شده‌ای پیشنهاد می‌شود که برای شناسایی خطاها در شبکه و در نظارت وضعیت اشیای هوشمند استفاده می‌شوند. آمار کلیدی که باید نظارت شوند شامل: انرژی، وضعیت (روشن یا خاموش)، وضعیت اتصال، تعداد گم‌شدن بسته‌ها و مانند آن است. از آن طریق، هر شیء یا اتصال خراب به‌صورت خودکار شناسایی شده و الگوریتم‌های خوددرمانی[1] بهینه‌ای برای حل این مسائل اعمال خواهد شد. برای نظارت و مدیریت رویدادهای امنیتی، در [۳۲] ایده "بستری جهت بازپیکره‌بندی بلادرنگ امنیت[2]" (PRRS) را پیشنهاد داده است که مؤلفه‌ای از هستهٔ معماری "اینترنت آینده" محسوب می‌شود. PRRS به یک برنامه، کاربر نهایی یا سرویس اجازه می‌دهد تا یک درخواست را به چارچوب PRRS ارسال کند که نیازمندی‌های منحصر به فرد امنیتی خودش را تشریح کرده و توسط سرویس‌های دردسترس قابل پیاده‌سازی است. PRRS همچنین تخلفات را در طول زمان اجرا، از طریق جمع‌آوری شواهد در فرآیند نظارت در زمان اجرا، در یک راه‌حل امنیتی مبتنی بر شواهد کنترل می‌کند.

۳-۱-۱۱- نصب و پیکره‌بندی امن

جهت افزایش امنیت و کاهش حملات، [۳۲] اقدام به باز طراحی مشخصه‌های خود-X پایه، برای اشیای هوشمند کرده است تا سازوکارهای امنیت و حریم خصوصی را در آنها تعبیه کند. مکانیزم‌های خود-پیکره‌بندی و پیکره‌بندی خودکار نیز با امنیت تعبیه شده و آگاهی از زمینه، توسعه یافته است که تبادل‌های امن را درون شبکه امکان‌پذیر می‌سازد.

به‌کارگیری فناوری رادیوشناختی[3] (CR) نیز می‌تواند به‌عنوان بخشی از یک سازوکار پیکره‌بندی خودکار امن جهت کاهش اختلال و تداخل در اتصالات بین اشیای هوشمند، مورد توجه قرار گیرد [۳۷].

[1] Self-healing
[2] Platform for Run-time Reconfigurability of Security
[3] Cognitive Radio

۳-۱-۱۲- استفاده از مستعارسازی[4]

توانایی مشابه یک شخص سوم جهت دانستن این‌که دو موجودیت در حال تبادل داده هستند، می‌تواند نقض حریم خصوصی محسوب شود. هر دو کاربر و سرویس ممکن است نیاز داشته باشند که پردازش را تحت سناریویی مشخص انجام دهند، بدون اینکه طرف دیگر اطلاعاتی در مورد احراز هویت، نشانی‌دهی و یا دیگر اطلاعات حساس آن‌ها کسب کند. این می‌تواند با برخی نیازمندی‌های مربوط به احراز اصالت، مجازشناسی و عدم انکار در تضاد باشد.

با به‌کارگیری یک سرویس زیرساخت مستعارسازی قابل اعتماد در [۳۸] که شناسه‌های موقتی ساختگی با اعتبارنامه‌های مربوطه و خط‌مشی‌های مجازشناسی مربوطه را فراهم می‌کند، یک سامانه IoT می‌تواند هم‌زمان نیازمندی‌های حریم خصوصی و عدم انکار را تأمین کند.

۳-۱-۱۳- سامانه‌های اعتماد و شهرت

مفهوم اعتماد در مراجع و منابع، به‌طور واضح تعریف نشده و تعاریف مختلفی برای آن دردسترس است. یکی از آن تعاریف این است که "اعتماد" سطح احتمالی است که به‌واسطهٔ آن شخص A انتظار دارد که شخص B کاری را انجام دهد که سلامت و سعادت شخص A به آن وابسته است. شهرت نیز به اعتماد وابسته است و به‌عنوان یک سنجش از اعتماد تعریف می‌شود؛ هر موجودیت اطلاعات شهرت و اعتبار دیگر موجودیت‌ها را نگهداری کرده و به این ترتیب یک "وب" ساخته می‌شود که شبکه‌ای از اعتماد نامیده می‌شود [۳۹؛ ۴۰].

در این مورد از IoT و شبکه‌بندی ماشین‌به‌ماشین، درک اعتماد مسئله اصلی محسوب می‌شود. [۳۲]، اعتماد را به‌عنوان مؤلفه‌ای که نقش کلیدی را در پذیرش IoT دارد، در نظر گرفته و بر روی بالابودن سطح قابلیت اعتماد به سامانه هم برای کاربران و هم فراهم‌کنندگان سرویس، تمرکز کرده است. اعتماد در تنظیمات معماری پیشنهادی [۳۲] به‌عنوان انتظاری که از یک شیء می‌توان داشت تا به‌صورتی‌که از ابتدا برنامه‌ریزی‌شده عمل کند، ترسیم شده است. برای پرداختن به اعتماد، مفهوم "هستهٔ سامانه" در [۳۲] برای تمام لایه‌هایش و با تمرکز ویژه به اشیای هوشمند معرفی کرده است. مفهوم کلیدی این است که تنها اشیای هوشمند قابل اعتماد، اجازهٔ تبادل داده‌های حساس کاربر را خواهند داشت و فقط داده‌هایی که توسط اشیای

[4] Pseudonymization

هوشمند قابل اعتماد تولید شده‌اند، در تصمیمات سامانه مورد توجه قرار می‌گیرند. جهت سنجش قابلیت اعتماد به شیء هوشمند یک مدل وزن‌دهی مورد استفاده قرار می‌گیرد. وزن مربوطه نه تنها توسط ورودی که توسط کاربران فراهم شده تعیین می‌شود، بلکه در زمانی‌که آخرین بار به‌روز شده است و با تأثیر واقعی که آن پارامترها بر سرویس مربوطه دارد، مشخص می‌شود.

۳-۲- راه‌حل‌های عمومی دیگر

هدف از این بخش، مرور کلی فناوری‌ها و رویکردهای بالقوه‌ای است که در حوزهٔ اینترنت اشیا مطرح نشده‌اند؛ اما می‌توانند در این حوزه نیز پیاده‌سازی شده و جهت کمک به امنیت و حریم خصوصی IoT مورد استفاده قرار گیرند. لازم به ذکر است که بررسی‌های صورت‌گرفته در این مقاله یک بررسی جامع نیست؛ چون موضوعات پژوهشی در این حوزه بسیار گسترده است.

۳-۲-۱- مدیریت شناسه

مدیریت شناسه، به شناسهٔ کاربر یا اشیا اشاره دارد. در دنیای دیجیتال، کاربر باید یک یا چند شناسه داشته باشد. به‌طورکلی یک شناسه توسط "فراهم‌کنندهٔ شناسه[1]" مدیریت می‌شود. نقش اصلی فراهم‌کنندهٔ شناسه، تأمین مشخصه‌های شناسایی قابل تأیید برای فراهم‌کنندهٔ سرویس است. مثال‌هایی از فناوری‌های مدیریت شناسه شامل موارد زیر است:

- FaceBook-Connect API [۴۱]: اعضای فیسبوک را قادر می‌سازد تا به سایت‌های بیرونی متصل شوند.
- Google IM: مدیریت شناسه گوگل از استاندارد OAuth-2.0 استفاده می‌کند تا به منابع محافظت شده دسترسی داشته و برای کاربران نیز مبتنی بر OpenID [۴۲] کار می‌کند.
- Microsoft Cardspace [۴۳]: Cardspace براساس مفهوم کارت‌های اطلاعاتی کار می‌کند که در آن فراهم‌کننده‌های سرویس، طرف‌های رله‌کننده[2] بوده و فراهم‌کنندهٔ شناسه[3] نیز STS نامیده می‌شود.

۳-۲-۲- محاسبات خودمختار[4]

محاسبات خودمختار مفهوم پیاده‌سازی خودمدیریت در سامانه‌های توزیع شده است که برای اعمال تغییرات مربوط به شرایط درونی و بیرونی، بدون یا با حداقل مداخلهٔ انسان استفاده می‌شود. محاسبات خودمختار نخستین‌بار در سال ۲۰۰۱ مطرح شد. مفاهیم محاسبات خودمختار می‌تواند جهت پشتیبانی از سامانه‌های فیزیکی–سایبری (CPS) منعطف و بهبود امنیت سراسری آن‌ها مانند آنچه در [۴۴] تشریح شده، مورد استفاده قرار گیرد؛ اما همچنان کمبود پژوهش بر روی چگونگی تطبیق پژوهش‌های موجود بر روی محاسبات خودمختار با ویژگی‌های منحصربه‌فرد CPS مثل پویایی بالا، توزیع‌شدگی، طبیعت بلادرنگ‌بودن، منابع محدود و محیط پراتلاف، وجود دارد.

۳-۲-۳- گمنام‌سازی ترافیک در شبکه‌ها

هدف شبکه‌های گمنام‌سازی، فراهم‌کردن گمنامی کاربرانشان در حین برقراری ارتباط در اینترنت، است. دلایل زیادی وجود دارد که کاربران را به سمت مخفی‌کردن خودشان و یا شناسهٔشان می‌کشاند؛ از آزادی بیان در کشورهای سرکوب‌کننده تا اجرای فعالیت‌های غیرقانونی. سیستم‌های گمنام‌سازی مختلفی نیز وجود دارد که بعضی از آن‌ها فقط ارتباطات گمنام (TOR [۴۵]، I2P [۴۶]) و بعضی دیگر امکاناتی نظیر ذخیره‌سازی گمنام را نیز فراهم می‌کنند (Freenet [۴۷]، GNUnet [۴۸]). جهت مخفی‌کردن صادرکنندهٔ پیام، اکثر شبکه‌های گمنام‌سازی فعلی مبتنی بر مسیریابی پیازی[5] [۴۵] و رمزنگاری لایه‌بندی‌شده هستند.

۳-۲-۴- فناوری‌های افزایش حریم خصوصی (اعتبارنامه‌های گمنام)

U-Prove [۴۹] یک فناوری بالابردن حریم خصوصی است که صدور و نمایش درخواست‌های محافظت‌شده را با کمک رمزنگاری امکان‌پذیر می‌سازد. یک توکن U-Prove مجموعه‌ای از مشخصه‌ها[6] است که به یک کاربر مربوط می‌شود. درحقیقت U-Prove یک فناوری کاربرمحور است که هدف آن بهبود حریم خصوصی کاربر با استفاده از توکن‌های مبتنی بر "امضای کور" به‌جای امضای استاندارد PKI است.

Identity Mixer (Idemix) [۵۰] نیز یک فناوری افزایش حریم خصوصی است که در پژوهش‌های IBM توسعه داده شده و صدور نمایش درخواست‌های محافظت‌شده با کمک

[1] Identity Provider
[2] Relying Party
[3] Security Token Service
[4] Autonomic Computing
[5] Onion Routing
[6] Attributes

رمزنگاری را امکان‌پذیر می‌سازد. Idemix یک کتابخانه متن‌باز است که توسط IBM در پروژه اروپایی ABC_4Trust پیشنهاد شده و هدف آن بهبود حریم خصوصی کاربران با استفاده از توکن‌های مبتنی بر "امضای گروهی" به جای امضای استاندارد است.

۳-۲-۵- مذاکرات اعتماد[1]

مذاکرات اعتماد در اصل برای محیط‌های محاسبات توزیع‌شدهٔ بازطراحی‌شده است [۵۱]، که هدف آن اجازه‌دادن به طرف‌های ناشناخته جهت دسترسی به سرویس‌ها و منابع است. مذاکرات اعتماد براساس درخواست‌های مکرر و افشاهای اعتبارنامه‌ها در بین طرف‌های ارتباط جهت کسب سطح قابل قبولی از اعتماد است که اجازهٔ دسترسی به منابع را می‌دهد. همان‌طور که در [۵۲] مشخص شده، یک پیاده‌سازی عملی از تکنیک‌های مذاکرات اعتماد می‌تواند از لحاظ فاکتورهای مختلفی متفاوت باشد: تنوع دستگاه‌های محاسباتی، کانال مورد استفاده برای انتقال اعتبارنامه‌ها و قدرت محاسباتی دستگاه‌ها.

۳-۲-۶- توابع غیرقابل مشابه‌سازی فیزیکی

توابع غیرقابل مشابه‌سازی فیزیکی[2] (PUF) به مفهوم استفاده از مشخصه‌های فیزیکی ذاتی یک دستگاه برای احراز هویت است. در [۵۳] این مفهوم را برای RFID اعمال کرده‌اند تا مقاومت احراز اصالت PUF را بهبود بخشند. به‌طوراساسی PUF تابعی است که مجموعه‌ای از چالش‌ها را به مجموعه‌ای از پاسخ بر مبنای یک سامانه فیزیکی پیچیده نگاشت می‌کند. تابع مذکور تنها می‌تواند با یک سامانه فیزیکی خاص سنجیده شود که برای آن نمونه‌ی فیزیکی یکتا است.

۳-۳- نگاشت راه‌حل‌ها به چارچوب معماری

در این بخش می‌خواهیم به این مسأله بپردازیم که چگونه راه‌حل‌های معرفی‌شده می‌توانند در یک چارچوب معماری مشخص از IoT مجتمع شوند. جهت نمایش بهتر راه‌حل‌ها، آن‌ها را به معماری معرفی‌شده توسط پروژه IoT-A [۵۴] که به‌عنوان یک مدل پذیرفته‌شده محسوب می‌شود، نگاشت می‌کنیم. در شکل(۴) راه‌حل‌های شناسایی‌شده در بخش قبل به‌صورت بخش‌های بر روی معماری مرجع پیشنهادی قرار گرفته‌اند که راه‌حل‌های پیشنهاد شده برای شبکه IoT تیره‌تر و دیگر راه‌حل‌ها روشن‌تر نمایش داده شده‌اند.

[1] Trust Negotiation
[2] Physical Unclonable Functions

۴- فرصت‌های پژوهشی در امنیت اینترنت اشیا

با تمرکز بر فاصله‌های موجود بین چالش‌ها و راه‌حل‌های بررسی‌شده در حوزه امنیت و حریم خصوصی در IoT، فرصت‌های پژوهشی مختلفی قابل تعریف است، که در ادامه به بیان آن‌ها می‌پردازیم.

۴-۱- قابلیت استفاده درمبحث احراز اصالت

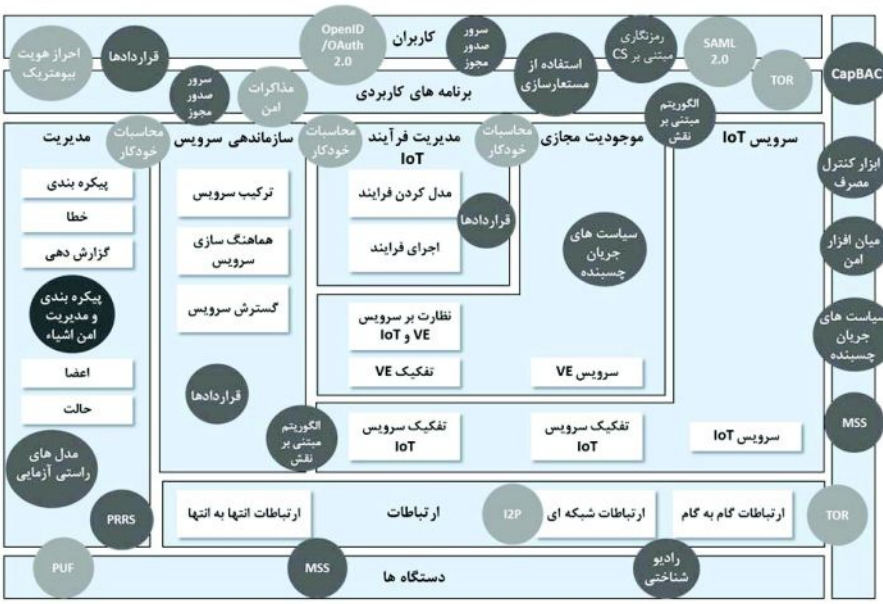
شکاف قابل توجهی بین امنیت و قابل استفاده بودن فرم‌های فعلی احراز اصالت وجود دارد. سازوکارهای قدرتمندی برای احراز اصالت پیشنهاد شده است، اما یک کاربر عام به احتمال زیاد با به کارگیری آن‌ها مشکل خواهد داشت؛ چون پیاده‌سازی و اعمال آن روش‌ها مشکل است. از طرف دیگر، سازوکارهای امنیتی رمزهای متنی و PINهای چهار رقمی که جهت استفاده آسان‌تر هستند، تضمین امنیتی کمتری را نیز فراهم می‌کنند. بنابراین یکی از چالش‌های پژوهشی ابداع سازوکارهای احراز اصالت جدیدی است که از روش‌های فعلی متفاوت بوده و یا ترکیبی از آن‌ها بوده و به نحو بهتری بتواند بدون قربانی کردن قابلیت استفاده، امنیت بیشتری را تأمین کند.

۴-۲- کنترل دسترسی با مدیریت خط‌مشی

کنترل دسترسی همراه با مدیریت خط‌مشی توسط منابع مختلفی با نام‌های مختلف پیشنهاد شده است. بنابراین دانش کافی برای توسعهٔ یک چهارچوب کامل و استاندارد وجود دارد. چارچوب موردنظر باید بتواند جهت پشتیبانی از امنیت تلفن همراه و توسعه بر روی بسترهای تلفن همراه مورد استفاده قرار گیرد تا از امنیت و حریم خصوصی کاربران حتی در برابر دستگاه‌های تلفن همراه آن‌ها حمایت کند. تعریف این کنترل دسترسی چالش کلیدی را هدف قرار می‌دهد: توانایی فراهم‌کردن کنترل بر کاربر و داده‌های او و توانایی اجرای قوانین و مقررات براساس سیاست‌ها و خط‌مشی‌ها.

۴-۳- تصدیق سرویس‌های IoT

همانطور که درقبل بیان شد، باید راهی وجود داشته باشد تا سطحی از اطمینان برای موجودیت‌هایی که سرویس‌های IoT را برای کاربران فراهم می‌کنند، وجود داشته باشد.



(شکل-۴): راه‌حل‌های امنیتی پیشنهادشده و معماری IoT-A

درحالی‌که سازمان‌ها و مراجع قانون‌گذاری می‌توانند بهترین گزینه برای تأیید یک سرویس IoT باشند؛ اما راه‌حل‌های فنی نیز می‌تواند جهت پشتیبانی از فرآیند تصدیق و تأیید فراهم شوند. چارچوب‌های اعتماد، شهرت و مدیریت شناسه وجود چارچوب‌های اعتماد، شهرت و مدیریت شناسه که بتواند یک سازوکار منسجم و کامل را برای کاربر فراهم کند، ضروری است. با این‌که راه‌حل‌های مشخصی برای این موارد پیشنهاد شده است، اما باید کارهای بیشتری برای یک چارچوب منسجم انجام شود. تلاش‌های پژوهشی جدید باید به مسائل قابلیت تعامل[1] بین فراهم‌کنندگان سرویس بپردازند. ارتباط بین یک کاربر و دستگاه‌های IoT او باید به‌طورعمیق مورد توجه قرار گیرد تا شهروندان بتوانند بر رفتار و فعالیت‌های دستگاه‌هایی که تحت نام آن‌ها کار می‌کنند، کنترل داشته باشند. کنترل جریان اطلاعات IoT و حریم خصوصی فراگیرشدن IoT در آیندهٔ نزدیک به‌طورکامل قابل پیش‌بینی است. حس‌گرها و دستگاه‌های هوشمند حجم عظیمی از داده‌ها را جمع‌آوری و منتقل خواهند کرد. در بیشتر موارد داده‌های جمع‌آوری‌شده توسط یک دستگاه IoT آسیب زیادی را به حریم خصوصی کاربر وارد نمی‌کند. با این وجود، تجمیع زیاد داده‌هایی که از موقعیت مشخص می‌آیند، می‌تواند حریم خصوصی شهروندان را به مخاطره بیاندازد. چارچوب‌هایی شامل مجموعه‌ای از خط‌مشی‌ها جهت جمع‌آوری داده و داده‌کاوی نیاز است تا هم از قابلیت بالقوه این حجم از داده‌ها استفاده و هم از حقوق حریم خصوصی افراد حفاظت کند.

۴-۴- احراز اصالت و تمامیت ارتباط در IoT

احراز اصالت و محرمانگی به‌طور طبیعی از طریق سامانه‌های رمزنگاری سنتی و براساس ساختارهای مبتنی بر PKI قابل دست یافتن است. با این حال، IoT به‌طوراساسی با سامانه‌های به‌طورکامل توزیع‌شده، با دردسترس‌بودن غیرپیوسته و در برخی واقع محدودیت‌های منابع انرژی و محاسباتی ترکیب شده است. در این شرایط، چارچوب‌های توزیع‌شده و سبک‌وزن احراز اصالت و تمامیت باید طراحی شود که بر این مشخصه‌های منحصربه‌فرد IoT غلبه کند.

۴-۵- امنیت در سامانه‌های سایبری-فیزیکی

در حوزهٔ سامانه‌های سایبری-فیزیکی نیز همچنان به تعریف راه‌حل‌های امنیتی جدید جهت رفع تهدیدات امنیتی موجود، نیاز است. در این مورد استانداردهایی از ابعاد فنی و حاکمیتی لازم است.

[1] Interoperability

۴-۶- توسعه و اعتبارسنجی نرم‌افزارهای IoT

نرم‌افزارها در IoT اغلب، بدون درنظرگرفتن مفاهیم امنیتی توسعه داده می‌شوند؛ مانند دیگر فناوری‌های ICT در IoT نیز از ابتدای گسترش باید استانداردهایی جهت تعیین فرصت مشترک و معماری توسعه مشترک، جهت توسعه نرم‌افزارها تعیین شود.

۴-۷- کنترل دسترسی افقی/عمودی

کنترل دسترسی و مجازشناسی ابعاد مهمی از بسیاری سناریوهای M2M هستند. یک چارچوب مجازشناسی و کنترل دسترسی عام باید طراحی شود که مفاهیم کنترل دسترسی نامتغیر کمی را درگیر کند. چنین سازوکاری به اعتبارنامه‌های امنیتی و شناسایی دستگاه‌ها نیاز دارد. با این وجود، در دنیای واقعی کاربردهای IoT مشکلات زیادی برای اتصال به یک اپراتور مشخص دارند. درنتیجه استفاده از این دستگاه‌ها با موارد کاربرد افقی یا عمودی امن به مفهومی جهت تجمیع‌کردن دستگاه در چارچوب امنیتی نیز دارند که این با راه‌اندازی شناسه‌های دستگاه و اعتبارنامه‌های امنیتی امکان‌پذیر می‌شود. پروژه‌های پژوهشی باید برچگونگی وابسته‌بودن به محیط اجرای پویای دستگاه جهت استخراج و افشای امن داده‌های نامتغیر برای یک بازهٔ زمانی قابل قبول که براساس آن امکان راه‌اندازی اعتبارنامه‌های امنیتی و خوداراه‌اندازی سازوکاری امنیتی توسط کاربر فراهم می‌شود، تمرکز داشته باشند.

۵- نتیجه‌گیری

در این مقاله قصد داشتیم به این موضوع بپردازیم که چه نیازمندی‌های امنیتی در حوزهٔ اینترنت اشیا باید در نظر گرفته شود. بدون شک این یک مساله پیچیده بوده و باید از زمان طراحی راه‌حل‌های مختلف IoT به آن توجه کرد. مشخص شد که امنیت از اهمیت ویژه‌ای در توسعه IoT برخوردار است و موارد بسیاری از محرمانگی و یک‌پارچگی تا محافظت از اطلاعات و حریم خصوصی برای حفظ ایمنی و امنیت انسان‌ها نیاز به بررسی دارند. بنابراین در این مقاله تلاش شد تا مبتنی بر یک روش استاندارد به تحلیل تهدیدات و چالش‌های امنیت و حریم خصوصی در اینترنت اشیا پرداخته شود و راه‌حل‌ها و پیشنهادهای مختلفی که در مورد بخش‌های مختلف امنیت IoT مطرح شده است، مرور گردند. در انتها نیز با هدف کمک به اشخاص و مجموعه‌های پژوهشی که قصد رفع موانع امنیتی توسعه اینترنت اشیا را دارند، به فرصت‌های پژوهشی و نیازمندی‌های باقیمانده امنیت اینترنت اشیا پرداختیم.

آنچه در مورد اینترنت اشیا مشخص است، این است که فناوری IoT یک زمینه پژوهشی جذاب بوده و با اطمینان می‌توان گفت که اگر مسائل و چالش‌های امنیت و حریم خصوصی آن مرتفع شوند، توسعه‌های بیشتری را در سال‌های آینده تجربه خواهد کرد.

۶- مراجع

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2016.

[2] Ed. Höller, "From machine-to-machine to the Internet of things: introduction to a new age of intelligence", Amsterdam: Elsevier Academic Press, 2014.

[3] L. Belli, S. Cirani, L. Davoli, "Applying Security to a Big Stream Cloud Architecture for the Internet of Things", International Journal of Distributed Systems and Technologies (IJDST), 7(1), 37-58, 2016.

[4] A. Botta, W. Donato, V. Persico, "Integration of Cloud computing and Internet of Things: A survey", Future Generation Computer Systems, Volume 56, Pages 684-700, March 2016.

[5] O. Arias, J. Wurm, K. Hoang, "Privacy and Security in Internet of Things and Wearable Devices", IEEE Transactions on Multi-Scale Computing Systems, vol.1, no.2, pp.99-109, June 2015.

[6] T. Borgohain, U. Kumar, S. Sanyal, "Survey of Security and Privacy Issues of Internet of Things", International Journal of Advanced Networking and Applications, vol. 6, pp. 2372–2378, 2015.

[7] S. Sicari, A. Rizzardi, D. Miorandi, "A secure and quality-aware prototypical architecture for the Internet of Things", Information Systems, Available online 18 February 2016.

[8] T. Mouroutis, A. Lioumpas, "Use-cases definition and threat analysis", RERUM Project-Deliverable D2.1, December 2014.

[9] J. S. Kumar, "A Survey on Internet of Things : Security and Privacy Issues", International Journal of Computer Applications, vol. 90, no. 11, pp. 20–26, 2014.

[10] ISO/IEC 10040, "Information technology - Open Systems Interconnection - Systems management overview - Part 4: Management framework", 1998.

[11] R. Venkatakrishnan, M. A. Vouk, "Using Redundancy to Detect Security Anomalies: Towards IoT security attack detectors", The

Internet of Things (Ubiquity symposium), January 2016.
[12] D. Dolev, A. C. Yao, "On the Security of Public Key Protocols", IEEE Transactions on Information Theory, vol. it - 29, no. 2, March 1983.
[13] H. Federrath, A. Pfitzmann, Originally published in German language in: 2.1 Technische Grundlagen. In: Alexander Rossnagel (Hg.): Handbuch des Datenschutzrechts, TU Dresden, Beck Verlag, 2002.
[14] A. Sadeghi, C. Wachsmann, M. Waidner, "Security and privacy challenges in industrial internet of things", In Proceedings of the 52nd Annual Design Automation Conference (DAC '15). ACM, USA, 2015.
[15] S. Sicari, A. Rizzardi, L.A. Grieco, "Security, privacy and trust in Internet of Things: The road ahead", Computer Networks, Volume 76, Pages 146-164, 2015.
[16] IEEE Standards Association, Guidelines for 64-bit Global Identifier (EUI-64TM).
[17] Z. Shelby, S. Chakrabarti, E. Nordmark, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, 2012.
[18] S. Raza, L. Seitz, D. Sitenkov, "S3K: Scalable Security With Symmetric Keys-DTLS Key Establishment for the Internet of Things", IEEE Transactions on Automation Science and Engineering, pp. 1–11, 2016.
[19] H. Ning, H. Liu, L. T. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things", IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 3, pp. 657–667, Mar. 2015.
[20] M. Deng, K. Wuyts, R. Scandariato, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements", Requirements Engineering, vol. 16, pp. 3-32, 2011.
[21] G. Baldini, T. Peirce, "IoT Governance, Privacy and Security Issues", European Research Cluster on the Internet of Things, January 2015.
[22] G. Baldini, N. Dumont, M. Etelapera, "Security requirements for the iCore cognitive management and control framework", iCore Project- Deliverable 2.2, May 2012.
[23] R. Neisse, A. Pretschner, V. Di Giacomo. "A Trustworthy Usage Control Enforcement Framework", International Journal of Mobile Computing and Multimedia Communications (IJMCMC), 2013.
[24] R. Neisse, J. Doerr, "Model-based specification and refinement of usage control policies", Privacy, Security and Trust (PST), Eleventh Annual International Conference on, pp.169,176, July 2013.
[25] D. Schreckling, "Security requirements and architecture for COMPOSE", COMPOSE Project- Deliverable 5.1.1, 2013.
[26] M. Handte, W. Apolinarski, "Privacy Preservation Specification", GAMBAS Project-Deliverable 2.2, September 2012.
[27] J. Imtiaz, L. Dürkop, H. Trsek, "Integrated secure Plug&Work framework", IoT@Work Project- Deliverable 2.5, 2013.
[28] L. Viganò, "Methodology and technology for vulnerability-driven security testing", SPaCIoS Project-Deliverable D3.3.2, 2014.
[29] S. Vuppala, A. Andrushevich, "Requirements, Specifications and Security Technologies for IoT Context-Aware Networks", BUTLER Project- Deliverable 2.1, October 2012.
[30] D. Ruiz, "Enhancing the autonomous smart objects and the overall system security of IoT based Smart Cities", RERUM Project-Deliverable 3.1, 2015.
[31] IoT6 D3.1, "Look-up/discovery, context-awareness, and resource/services directory".
[32] H. C. Pöhls, R. C. Staudemeyer, "Privacy enhancing techniques in the Smart City applications", RERUM Project- Deliverable 3.2, September 2015.
[33] A. Fragkiadakis, I. Askoxylakis, E. Tragos, "Joint compressed-sensing and matrix-completion for efficient data collection in WSNs", in Proc. of the IEEE CAMAD2013, Berlin, Germany, September 2013.
[34] F. Sottile, M. Franceschinis, Zh. Xiong, "IoT Enabling Technologies and Future Developments", BUTLER Project- Deliverable 2.5, October 2014.
[35] S. Ullah Khan, C. Pastrone, L. Lavagno, "An Authentication and Key Establishment Scheme for the IP-Based Wireless Sensor Networks", Procedia Computer Science, Vol. 10, Pp. 1039-1045, 2012.
[36] S. Severi, G. Pasolini, D. Dardari, "A Secret Key Exchange Scheme For Near Field Communication", Proc. IEEE Wireless Communications and Networking Conference (WCNC), 2014.
[37] E. Tragos, V. Angelakis, "Cognitive Radio Inspired M2M Communications (Invited Paper)", in IEEE Global Wireless Summit, 2013.
[38] M. R. Palattella, L. Ladid, S. Ziegler, “IoT - IPv6 integration handbook for SMEs”, IoT6 Project-Handbook, May 2014.
[39] J. Golbeck, J. Hendler, "Accuracy of metrics for inferring trust and reputation", Proceedings of the 14th International Conference on Knowledge Engineering and Knowledge Management, 2004.
[40] J. Golbeck, J. Hendler, "Inferring reputation on the semantic web", Proceedings of the 13th International World Wide Web Conference, 2004.
[41] FaceBook-Connect API - http://developers.facebook.com/docs/guides/web/.
[42] OpenID 2.0 http://openid.net/specs/openid-authentication-2_0.html.

[43] Windows Microsoft CardSpace, http://msdn.microsoft.com/enus/library/aa480189.aspx.
[44] L. Gurgen, O. Gunalp, Y. Benazzouz, "Self-aware cyber-physical systems and applications in smart buildings and cities", Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013.
[45] R. Dingledine, N. Mathewson, P. Syverson, "Tor: The second-generation onion router", in roceedings of the 13th USENIX Security Symposium, 2004.
[46] J.P. Timpanaro, I. Chrisment, O. Festor, "Monitoring the I2P network", Research Report RR - 7844, INRIA, December 2011.
[47] I. Clarke, T. W. Hong, S. G. Miller, "Protecting Freedom of Information with a", in IEEE Internet Computing, 2002.
[48] K. Bennett, C. Grothoff, "gap - Practical Anonymous Networking", in Designing Privacy Enhancing Technologies. Springer-Verlag, 2003.
[49] C. Paquin, G. Thompson, "U-Prove CTP White Paper", Microsoft Corporation, 2010.
[50] Idemix - Camenisch & Van Herreweghen, Design and Implementation of the Idemix Anonymous Credential System, 2002.
[51] A. Lee, K. Seamons, M. Winslett, "Automated Trust Negotiation in Open Systems Secure Data Management in Decentralized Systems", Advances in Information Security, Volume 33, Part III, 217-258, 2007.
[52] G. Yajun, W. Yulin, "Establishing Trust Relationship in Mobile Ad-Hoc Network", Wireless Communications, Networking and Mobile Computing (WiCom), 2007.
[53] S. Devadas, E. Suh, S. Paral, "Design and Implementation of PUF-Based "Unclonable", RFID ICs for Anti-Counterfeiting and Security Applications", IEEE International Conference on RFID, pp.58,64, 2008.
[54] M. Bauer, M. Boussard, N. Bui, "Final Architectural Reference Model for the IoT", IoT-A Project-Deliverable D1.5, 2013.

حمیدرضا ارکیان کارشناسی ارشد خود را از دانشگاه گیلان در رشتهٔ مهندسی فناوری اطلاعات گرایش شبکه‌های رایانه‌ای دریافت کرد. ایشان از سال ۱۳۸۶ با پژوهشگاه توسعهٔ فناوری‌های پیشرفته همکاری داشته و در پروژه‌های پژوهشی مختلفی در حوزهٔ امنیت شبکه و فضای سایبر مشارکت کرده است. از ایشان تاکنون بیش از پانزده مقاله در مجلات و کنفرانس‌های ملی و بین‌المللی به چاپ رسیده است. زمینهٔ پژوهشی مورد علاقهٔ وی رمزنگاری، امنیت شبکه، شبکه‌های بی‌سیم و اینترنت اشیا است.

عاطفه پورخلیلی کارشناسی ارشد خود را در سال ۱۳۹۳ از دانشگاه گیلان در رشته مهندسی فناوری اطلاعات گرایش شبکه‌های رایانه‌ای دریافت کرد. زمینهٔ پژوهشی مورد علاقهٔ ایشان امنیت شبکه در فناوری‌های نوظهور بوده و دارای مقالات متعددی در مجلات و کنفرانس‌های ملی و بین‌المللی است و همچنین در پروژه‌های پژوهشی مختلفی در همین حوزه‌ها، همکاری داشته است.

حمیدرضا خوش‌اخلاق دارای مدرک کارشناسی در رشتهٔ ریاضی کاربردی از دانشگاه صنعتی خواجه نصیرالدین طوسی در سال ۱۳۹۱ و کارشناسی ارشد در رشته علوم کامپیوتر گرایش نظریه محاسبات از دانشگاه صنعتی شریف در سال ۱۳۹۳ است. زمینه‌های پژوهشی مورد علاقهٔ وی مباحث نظری رمزنگاری و امنیت اطلاعات است.