بررسی تهدیدات و چالش های امنیتی در حوزه اینترنت اشیاء و ارائه یک مدل

پریسا سلمانی نژاد
دانشگاه آموزش عالی مهرالبرز _ تهران

چکیده

اینترنت اشیا [۱](IoT) توسط فن آوری ناهمگن ایجاد می شود که موفق به تأمین خدمات نوآورانه در حوزه های مختلف نرم افزار است. در این سناریو، رضایت از امنیت و حریم خصوصی نقش اساسی مورد نیاز بازی می کند. همچنین شامل محرمانه بودن اطلاعات و احراز هویت، کنترل دسترسی در شبکه اینترنت اشیا، حفظ حریم خصوصی و اعتماد در میان کاربران و ... می شود. در این مقاله با توجه به اهمیتی که حفظ امنیت در این شبکه دارد بر آن شدیم تا با شناسایی چالش ها و تهدیدات حول این حوزه بتوانیم از بروز مشکلات بعدی جلوگیری کرده و به نحوی امنیت را در سطح این شبکه برقرار کنیم. در این مقاله با بررسی و تائید برخی از چالش ها و تهدیدات اساسی موجود در این حوزه توسط خبرگان از جمله حریم خصوصی، اعتماد، تصدیق هویت، کنترل دسترسی، معماری IOT و ناهمگونی بین اشیاء درون شبکه مدلی را ارائه شد که طبق مدل ارائه شده و بررسی نتایج بدست آمده از نرم افزار SPSS و آزمون اسپیرمن و رگرسیون خطی چندگانه نتیجه شد با توجه به بالا بودن مقدار sig در دو فرضیه ناهمگونی و تصدیق هویت، این دو فرضیه رد شدند و نتیجه شد دیگر فرضیات با مقدار sig کمتر از ۰,۰۵ تائید شدند و سپس بوسیله آزمون رگرسیون رابطه خطی و مستقیم آنها با مدل ارائه شده، تائید شد. لازم به ذکر است که روایی و پایایی پرسش نامه توسط خبرگان در این حیطه تائید شد و با پخش پرسش نامه با ۱۹ سوال بین ۲۲ خبره از نتایج پرسش نامه ها جهت استفاده در نرم افزار بکار گرفته شد.

واژگان کلیدی :تهدیدات اینترنت اشیاء، چالش های اینترنت اشیاء، امنیت اینترنت اشیاء، اینترنت اشیاء

[۱] Internet Of Thing

۱- مقدمه

۲-۱- بیان مساله:

از آنجایی که در اینترنت اشیاء، حفظ امنیت یک مساله کلیدی محسوب می شود لازم دیده شد که تهدیدات و چالش های حول این محور بررسی شوند و با حفظ سازوکارهای مربوطه در هر چالش بتوان از بروز حملات امنیتی جلوگیری کرد. مساله اصلی این تحقیق ارائه مدل برای تحقیق در مورد اینکه چه موارد کلیدی بر روی چالش ها و تهدیدات شبکه IOT اثر گذار هستند.

۲-۲- اهمیت موضوع:

با بررسی های لازم در حیطه برقراری امنیت در شبکه IOT می توان متوجه شد که تا چه اندازه برقراری امنیت در این شبکه می تواند بر روی حفظ حریم خصوصی، اعتماد، کنترل دسترسی، تصدیق هویت و ...؛ اشیاء و یا کاربران فعال در این می تواند اثر گذار باشد. با برقراری امنیت می توان این تاکید را کرد که کاربران و یا سیستم های متصل به شبکه با خیالی آسوده تر می توانند به انجام تراکنش های فعال در این شبکه پرداخته و از همه مهمتر اینکه حریم خصوصی آنان نیز تضمین می شود. در صورتی که این شبکه با تهدیدات و آسیب پذیری هایی رو به رو باشد، امکان وقوع حمله در لایه های ارتباطی معماری شبکه IOT و در نتیجه با نقض برقراری ارتباط به صورت امن رو به رو خواهیم بود. چه بسا افرادی که بخاطر عدم تائید برقراری امنیت در این شبکه از استفاده از این فناوری خودداری کرده تا مهاجمان به حریم خصوصی آنان تجاوز نکنند، لذا با وجود اشد برقراری ارتباط امن بر آن شدیم تا با شناسایی نقاط تهدیدآمیز و مطالعه برخی از راهکارها، مدلی را ارائه دهیم تا کلیدی ترین چالش ها و تهدیدات را در حوزه شبکه IOT شناسایی و مورد بررسی قرار دهیم.

۲-۳- ادبیات و پیشینه تحقیق:

اینترنت اشیاء (IOT) فناوری مدرنی است که در آن برای هر موجودی (انسان، حیوان و یا اشیاء) قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت، فراهم می‌گردد. معماری اینترنت اشیا قرار است به مقابله با میلیاردها شی، که با یکدیگر و با اشخاص دیگر در تعامل هستند، می پردازد. مانند تعامل انسان و یا اشخاص مجازی و همه این فعل و انفعالات باید به نحوی امن، با حفاظت از اطلاعات و تأمین خدمات تمامی اشیاء مربوطه باشد و باید تعداد حوادث مربوط به کل اینترنت اشیا را محدود کرد. بنابراین حفاظت از اینترنت اشیاء در یک مجموعه کار دشواری است. تعداد حملات در دسترس، (دسترسی هر شی، در هر حال، در هر زمان) پایه های اصلی اینترنت اشیا می باشد. تهدیداتی که می تواند تحت تاثیر نهادهای اینترنت اشیا باشد، مانند حملاتی که با هدف کانال های ارتباطی متنوع و فیزیکی، محرومیت از خدمات مجاز، ساخت هویت غیرمجاز و ... (Babar et al, 2011) قرار بگیرد. در نهایت، پیچیدگی ذاتی اینترنت اشیا، که در آن نهادهای ناهمگن متعدد در زمینه های مختلف که با یکدیگر اطلاعات را مبادله می کنند، طراحی پیچیده و بکارگیری کارآمد اشیاء و

مکانیسم های امنیتی و سازگار در آنها مقیاس پذیر است.

۱) چالش های موجود در اینترنت اشیاء:

برخی از چالش هایی که در کنار مکانیزم های امنیتی که باید با اینترنت اشیاء یکپارچه شوند توسط جامعه پژوهش (Vermesan et al, 2011) (Torner and Polka, 2011)، (Roman et al, 2011) معرفی شدند عبارتند از:

۱-۱) ناهمگونی؛ نفوذ زیادی از پروتکل و خدمات امنیت شبکه دارد که باید در اینترنت اشیا اجرا شود. با دستگاه های محدود، مختلف و ناهمگن به طور مستقیم یا از طریق دروازه ارتباط برقرار خواهد کرد (به عنوان مثال دیگر محدودیت ها شامل دستگاه ها و وب سرورها می شود).

راهکار:

برای حل این مشکل در این سناریو، نه تنها ضروری است که الگوریتم های رمزنگاری کارآمد پیاده سازی شود بلکه می توان برای انطباق و یا ایجاد وزن پروتکل های امنیتی سبک که ارتباط امنی را برای کانال ارائه دهد. این پروتکل نیاز به اعتباردهی دارد، در نتیجه سیستم های مدیریت، به کلید بهینه ای برای اجرای توزیع این اعتبار و کمک به ایجاد کلید جلسه لازم بین همسالان، نیاز دارد.

۱-۲) وجود میلیاردها شیء ناهمگن نیز در مدیریت هویت تاثیر می گذارد. فراتر از تعریف دامنه واقعی از «هویت» در این زمینه (به عنوان مثال هویت اساسی غیرمجاز در مقابل هویت واقعی، هویت هسته ای در مقابل هویت موقت)، ما نیز نیاز به ارائه برخی مکانیزم هایی برای دستیابی به احراز هویت جهانی داریم. بدون احراز هویت، این عمل برای اطمینان از اینکه داده های جریان تولید شده توسط یک نهاد خاص و آنچه که قرار است باشد، ممکن نخواهد بود. یک جنبه مهم دیگر مربوط به احراز هویت مجوز است. پس در واقع اگر هیچ دسترسی وجود نداشته باشد، کنترل دسترسی هرکس (انسان یا سیستم) باید انجام شود.

۱-۳) در واقع، داده های ایجاد شده توسط میلیاردها شیء باعث ایجاد اطلاعات بسیار زیادی بعنوان یک تهدید بزرگ به حریم خصوصی است.

راهکار:

ابزارها اجازه می دهند که کاربران با حفظ محرمانگی خود به این جهان فوق العاده متصل شوند. در واقع، اینترنت اشیاء، باید به طور جدی به اجرای حریم خصوصی و اصول طراحی آن بپردازد (Kawokian, 2009)، ارائه پشتیبانی کاربر محور برای امنیت و حریم خصوصی از پایه های اصلی اینترنت اشیاء است.

۴-۱) اندازه و ناهمگونی از اینترنت اشیا نیز بر اعتماد و حکومت آن تاثیر می گذارد. در واقع دو بعد برای حفظ اعتماد وجود دارد: (الف) اعتماد به تعامل بین اشخاص، که در آن ما باید برای مقابله با عدم اطمینان در مورد اقدامات آینده از تمام نهادهای همکاری استفاده کنیم، و (ب) اعتماد در سیستم از نقطه نظر کاربر، به طوری که باید کاربران قادر به مدیریت همه اشیاء ناشناخته باشند.

راهکار:

راجع به حکومت آن نیز به یک شمشیر دو لبه نیاز است که باید با مراقبت از یک طرف، ثبات آن ارائه دهد، از تصمیم گیری های سیاسی پشتیبانی کرده و این امکان را می دهد که یک چارچوب مشترک و مکانیسم قابلیت همکاری را ارائه دهد. از سوی دیگر، به راحتی می توانید حکومت را بیش از حد کنترل کرده و به کنترل بیش از حد محیط بپردازیم.

۵-۱) تعداد سیستم های آسیب پذیر و حملات برداری مطمئنا در زمینه اینترنت اشیا افزایش می یابد، در نتیجه آن تحمل تهدیدات ضروری است.

راهکار:

برای حل این مشکل ما نه تنها باید در تلاش برای پیاده سازی امنیت به طور پیش فرض (پیاده سازی قوی و قابل استفاده سیستم و ...) در اینترنت اشیا بپردازیم، بلکه ما نیاز به توسعه مکانیزم های آگاهی برای کاربران هستیم که می تواند مورد استفاده برای ایجاد پایه های تشخیص نفوذ و مکانیزم های پیشگیری قرار گیرد و کمک خواهد کرد که نهادهای اینترنت اشیا از آن محافظت کرده و یا حتی کاهش خدمات را داشته باشند. در نهایت، خدمات بازیابی باید قادر به ایجاد مناطق امن شود (به عنوان مثال مناطق تحت تاثیر حملات را مشخص کرده و برای رفع آنها چاره ای بیاندیشد) و در نتیجه مسیر عملکرد سیستم را به دیگر مناطق مورد اعتماد تغییر دهد.

۲) تجزیه و تحلیل مدل های مهاجم و تهدیدات مربوطه:

مفهوم محیط در اینترنت اشیاء یعنی اینکه: یک مهاجم می تواند بخشی از شبکه را کنترل کرده باشد، اما با توجه به طبیعت ذاتی توزیع اینترنت اشیاء تقریبا این عمل برای یک مهاجم برای کنترل کامل طیف سیستم غیر ممکن است. به عنوان یک نتیجه ارزیابی شده، یک مهاجم می تواند در هر دو موقعیت "داخلی" و "خارجی" و در همان زمان وجود داشته باشد.

۲-۱) محرومیت از خدمات (DOS):

تعداد گسترده ای از این حملات وجود دارد، که می توان آنها را در برابر اینترنت اشیا راه اندازی کرد. فراتر از حملات داس که ارائه دهنده خدمات منابع داده ای، پهنای باند شبکه بی سیم و همچنین زیرساخت های ارتباطی بسیاری از اکتساب داده های شبکه می تواند مورد هدف قرار گیرد (به عنوان مثال تراکم کانال).

۲-۲) آسیب فیزیکی:

این تهدید می تواند به عنوان یک زیر مجموعه از تهدید DOS[۲] مورد استفاده قرار گیرد. در این مدل مهاجم یک حمله فعال معمولا همراه با فاقد دانش فنی انجام می دهد و تنها می تواند مانع ارائه مجوز به خدمات اینترنت اشیا با از بین بردن اشیاء واقعی شود. این یک حمله واقعی در زمینه اینترنت اشیا است، چرا که همه چیز ممکن است به راحتی در دسترس هر کسی قرار گیرد. در صورتی که مهاجم نمی تواند به سادگی می توانید ماژول های سخت افزاری را هدف قرار دهد.

۲-۳) استراق سمع:

حمله منفعلانه ای که می تواند ارتباط های مختلفی را هدف قرار دهد. کانال هایی مثل شبکه های بی سیم، شبکه سیمی محلی، اینترنت به منظور استخراج داده ها از جریان اطلاعات استفاده می شود. بدیهی است، یک مهاجم داخلی دسترسی به زیرساخت های خاص دارد و به استخراج اطلاعات موجود در زیرساخت شبکه می پردازد.

۲-۴) ضبط گره:

همه چیز (برای مثال خانه لوازم خانگی، چراغ های خیابانی) از نظر فیزیکی در یک محیط خاص قرار گرفته است. به جای از بین بردن آنها، مهاجم می تواند اطلاعات آنها را استخراج کند. مهاجمان فعال می توانند زیرساخت های دیگری که اطلاعات هدف را ذخیره کنند، مانند پردازش داده ها و یا ذخیره سازی داده های اشیاء.

۲-۵) کنترل:

تا زمانی که یک مسیر حمله وجود دارد، مهاجمان فعال می توانند سعی کنند کنترل جزئی یا کاملی را از بیش از یک نهاد اینترنت اشیا به دست آورد. دامنه آسیب های ناشی از این حمله بستگی دارد به (الف) اهمیت مدیریت اطلاعات آن نهاد خاص، (ب) خدماتی که توسط آن نهاد خاص ارائه شده است.

راهکار:

در حالی که هر دو روش متمرکز باشند و توزیعی برای به اشتراک گذاری مدل های مهاجم وجود داشته باشد، تفاوت های ظریفی وجود دارد که ناشی از ویژگی های توزیع اینترنت اشیا و اصول مربوط به آن است. برای حل این مشکل جنبه های مختلفی از زیرساخت های اساسی را باید تغییر دهید، مانند استراتژی های استقرار مختلف نهادهای اینترنت اشیا، جریان اطلاعات واقعی و در دسترس بودن رابط ها و خدمات. این تغییرات می تواند تهدیدات جدیدی را ایجاد کرده و حمله را تسهیل کند، اما می تواند اثر بخشی بردارهای حمله را کاهش دهند.

۳) جنبه هایی که ویژگی های اینترنت اشیا را تحت تاثیر قرار می دهد و اصولی که آنها را تهدید می کند و مهاجم را تحت تاثیر مدل ها قرار می دهد، عبارتند از:

[۲] Denial of Service attack

۳-۱) یکی از جنبه های مهم آن تمرکز در منابع است. مهاجمان سیستم های بزرگ را مورد هدف قرار می دهند که نهادهای مرکزی تحت نظر این دسته قرار می گیرند، در آنها ذخیره، مدیریت و پردازش مقدار زیادی از اطلاعات همواره مورد استفاده قرار می گیرد. از لحاظ تئوری، این اشیاء مرکزی مکانیسم بهتر حفاظت را در بر دارند، اما هرگونه آسیب پذیری می تواند سقوط کل سیستم را در بر داشته باشد.

راهکار:

اگر از اینترنت اشیاء که توزیع شده است، اطلاعاتی ایجاد شود و پردازش شود که در آن اشیاء مختلف قرار داشته باشد، بنابراین مهاجمان نیاز دارند همان مقدار از منابع را کنترل کنند. اگر دشمن تنها به یک قطعه خاص از اطلاعات علاقه مند باشد، می تواند مدیریت خاصی از اطلاعات سیستم را هدف قرار دهد.

۳-۲) حملات تبدیل ضبط گره خطرناک تر است، در واقع، دشمن می تواند از یک استراتژی جنگ استفاده کرده و به کنترل تدریجی از قطعات کوچک شبکه می پردازد.

۳-۳) یکی دیگر از جنبه ها مربوط به تمرکز منابع و ماهیت جریان اطلاعات است. در اینترنت اشیا بر یک الگوی سلسله مراتبی که به عنوان یک نهاد مرکزی، اطلاعات را از آن دریافت خواهد کرد، متمرکز است. از سوی دیگر، در روش توزیعی، جریان اطلاعات بین سیستم ها در حال تبادل است. در این مورد خاص، مهاجمی که در شبکه استراق سمع می کند، قادر نیست که به اطلاعات کل سیستم دسترسی داشته باشد. یک نکته مهم در اینجا وجود دارد:

اگر مهاجم اینترانت اشیاء را در یک سناریوی توزیع شده مورد حمله قرار دهد، او ممکن است قادر به بازیابی اطلاعات پردازش شده به جای داده های خام باشد. با توجه به اتصال به کل شبکه، در این روش انتظار می رود که به طور مستقیم و بوسیله آدرس دهی از طریق اینترنت بتواند قادر باشد که اتصالات را از نهادهای خارجی پذیرا باشد. این موقعیت اجازه می دهد تا مهاجمان برای راه اندازی حملات مخرب به راحتی منابع خود را مصرف کنند. در نهایت، ما نیز باید در پیکربندی مکانیزم های امنیتی بعنوان یک کاربر تلاش کنیم. کارشناسان امنیت بر این باورند که، اگر اشتباهات امنیتی اتفاق بیافتد هیچ مکانیزمی به اندازه کافی قابل استفاده نیست.

۴) چالش های خاص و راه حل های امیدوار کننده مربوط به هر چالش:

۴-۱) هویت و تصدیق هویت:

برای بررسی چگونگی مدیریت هویت و احراز هویت در اینترنت اشیاء که به عنوان قلمروهای مختلف (به عنوان مثال منابع داده، ارائه دهندگان خدمات، سیستم پردازش اطلاعات) نیاز به تأیید هویت یکدیگر به منظور ایجاد خدمات قابل اعتماد است

(Mahaleh et al, 2011). هنگام تعریف مکانیسم امنیت، به عنوان فعل و انفعالات کاملا پویا، اشیاء شبکه ممکن است در پیشبرد دائمی که شرکا می توانند یک سرویس خاص را استفاده کنند، بکار روند. اگر میلیاردها شیء در حال تبادل اطلاعات باشند، لازم است هویت خود را در راه مقیاس پذیر مدیریت کنند. در این رویکرد خاص، منطق برنامه این است که عمدتا یک نهاد مرکزی (به عنوان مثال اینترنت اشیا، پلت فرم نرم افزار مبتنی بر ابر) را فراهم کند که مجموعه ای از نقاط ورودی شناخته شده (به عنوان مثال رابط های برنامه کاربردی) انجام شود. هر دو ارائه دهندگان داده ها مانند حسگرها، و مصرف کنندگان اطلاعات مانند برنامه های کاربردی کاربران و مشتریان دیگر، به این نهاد مرکزی متصل هستند. به عنوان یک نتیجه، تمام احراز هویت منطقه را می توان در این نهاد و یا در یک هویت متمرکز ارائه دهنده با آن انجام داد. در صورتی که ارائه دهندگان داده هویت خود را ارائه ندهند، هیچ مقیاس پذیری وجود ندارد، در این زمینه سناریو ما پویا و N به N بوده که در آن ارائه دهندگان داده دیگر غیر فعال هستند و قادر به بدست آوردن و پردازش اطلاعات از منابع یکدیگر نیستند. علاوه بر این، کاربران محلی می توانند از ارائه دهندگان اطلاعات محلی به طور مستقیم پرس و جو کرده و بدون دخالت از نهادهای خارجی فعالیت کنند.

نتیجه گیری:

در برخی از مناطق احراز هویت باید وجود داشته باشد ولی در صورتی که ارائه دهنده خدمات از جمله اجزاء با تعداد اشیاء کم باشند اما باید توجه داشته باشید که با این حال، همه چیز در خلاء وجود ندارد: آنها معمولا به یک گروه خاص تعلق دارند، در واقع مخصوص نهادهای خاصی هستند که برای این جنبه باید راهکار زیر در نظر گرفته شود.

راهکار:

دو راهکار در زیر با شرایط مختلف ارائه شده اند:

- ✓ برای مدیریت هویت اشیاء که در یک مسیر مقیاس پذیر است. از سال ۲۰۱۲، مکانیسم های مختلفی وجود دارد که می تواند مورد استفاده برای شناسایی اشیای منحصر به فرد شود، از جمله به عنوان EPC[۳] (کد استانداردهای برچسب) و ucode (li Zoodoor et al. 2011). بنابراین، انتظار می رود که در سیستم های مختلف آینده نه تنها در سطح جهانی بلکه در مقیاس محلی نیز از آنها استفاده شود (Takalo matilla et al, 2010). به عنوان یک نتیجه، همه چیز باید قادر به شناسایی باشد. ویژگی ها و زمینه با توجه به اشیاء احراز هویت، ما باید در نظر بگیریم که در بسیاری از حالات شیء متعلق به یک گروه خاص (به عنوان مثال شبکه های داخلی از همه چیز، شبکه های شخصی) در واقع منطقه مکانی (مثلا بیمارستان، تعمیرگاه و وسایل منزل و ...) است. در چنین محیطی، ارائه دهندگان هویت محلی می توانند مدیریت هویت از آن اشیاء و همچنین می توانند یک دایره اعتماد را برای ارائه دهندگان منابع خارجی مربوطه ایجاد کنند. در نتیجه، نهادهای محلی نه تنها قادر به تصدیق به یکدیگر در داخل یک گروه هستند بلکه می توانند یک سند هویت مربوط به تعامل با نهادهای خارجی را بوجود آورند. همچنین، موجودیتهای خارجی می توانند یک شخصیت موقت را دریافت کرده و از هویت محلی ارائه دهنده در صورت لزوم با خبر باشند. این گروه بر اساس استراتژی هایی انجام شده است که در

[۳] Electronic Product Code

واقع، تا حدی تعاملات بین جزایر WSN را در نظر گرفته اندکه در آن همکاری از طریق مدیریت هویت فدرال ممکن است ترجمه و نشانه های دسترسی وجود داشته باشند (boag, 2011).

- ✓ اگر شی در واقع یک انسان باشد، می توان از مکانیسم های تأیید هویت های موجود (به عنوان مثال اعتبار وب، کارت شناسایی الکترونیکی، استفاده از توکن و یا امضای دیجیتال) استفاده کرد. به عنوان مثال، (Joinard et al, 2010) با پیشنهاد یک زیرساخت دروازه هوشمند (مثل کنترل دسترسی اجتماعی و یا SAC) که اجازه می دهد تا کاربران برای بازیابی داده ها از سنسور محلی با استفاده از شبکه های اجتماعی خود (مانند فیس بوک یا توییتر و ...) اعتباردهی هویت را انجام دهند. توجه داشته باشید که این روش ممکن است در مورد ارتباط مستقیم انسان به با سایر موجودیت ها صدق نداشته باشد. در چنین مواردی، لازم است به جایگزین مکانیسم هایی بپردازیم که می تواند به نمایندگی از دیگر کاربران اشیاء عمل کنند که یکی از نمونه های موجود (Weber et al, 2010) شامل یک دستگاه که هویت دیجیتال از فروشگاه های کاربران است و به عنوان نماینده خود در دنیای مجازی عمل می کند. نه تنها یک ارتباط امن را فراهم می کند، بلکه اجازه می دهد آن شیء با یک نام مستعار فعالیت خود را انجام دهد.

۲-۴) کنترل دسترسی:

در اینترنت اشیاء، چالش های مربوط به کنترل دسترسی از نزدیک به کسانی که در هر سیستم توزیع شده وجود دارند. یک سرویس خاص است با چندین خدمات و منابع داده از مکان ها و زمینه های مختلف (به عنوان مثال بازیابی اطلاعات از صفحه اصلی بیماران و آمبولانس یک بیمارستان).

همه این ارائه دهندگان اطلاعات، سیاست های کنترل دسترسی و مجوز خود را که چرخه عمر (ایجاد، اجرا، تعمیر و نگهداری، ترجمه) باید مدیریت شود را در نظر می گیرد. همچنین برخی از مسائل خاص که باید در زمینه اینترنت اشیا انجام شود، وجود دارد. محل (به عنوان مثال چک کردن اینکه آیا کاربران دسترسی به خدمات از یک چیز به صورت محلی و یا از راه دور) وجود دارد و همچنین تبدیل عناصر مهمی از سیاست های کنترل دسترسی در سناریوهای خاص همواره باید وجود داشته باشد. همچنین، هر زمان که مکانیسم های کنترل دسترسی در حال اجرا باشند در سطح شیء، لازم است میزان منابع محاسباتی که در دسترس هستند، به عنوان دستگاه های محدود شده برای آن فضای کافی همواره وجود داشته باشد و در نتیجه پیاده سازی یک مکانیزم کنترل دسترسی پیچیده است. در نهایت، به عنوان بسیاری از کارهایی که توسط کاربران انجام می شود (یا به طور دائم و یا به طور موقت) و ممکن است به یک گروه (به عنوان مثال شبکه شخصی) تعلق داشته باشد، لازم است یک مکانیسم مهم در نظر گرفته شود، به عنوان مثال یکی از اشیاء ممکن است در عمل نام کاربر / گروه مد نظر قرار گیرد. همانطور که با احراز هویت، سیاست های کنترل دسترسی راحت تری برای مدیریت در معماری اینترنت اشیا متمرکز است.

نتیجه:

باید تمام کنترل دسترسی سیاست ها ذخیره شده و مدیریت در یک مرکز انجام و بررسی شود. بنابراین، ارائه دهندگان داده لازم نیست به پیاده سازی هر نوع از منطق کنترل دسترسی بپردازند، آنها تمام اطلاعات خود را به کسانی که به آنها اعتماد

دارند (به عنوان مثال نهاد مرکزی) ارسال می کنند و از این پیکربندی، هر دو ارائه دهندگان داده ها و اطلاعات مصرف کنندگان باید به طور کامل به نهاد مرکزی اعتماد داشته باشند و آن را به عنوان اطلاعات تولید شده توسط همه موجودیت های موجود در شبکه در نظر بگیرند.

راهکار:

- ✓ صرفا معماری اینترنت اشیا توزیع شده باید برای مقابله با تمامی چالش ها مورد استفاده قرار گیرد. اجرا و مدیریت سیاست های ناهمگن در اشیاء مختلف درون و برون یک شبکه یکی از راهکارهای موثر است.
- ✓ یک راه حل ارائه شده در (علی و همکاران)، که یک فرمت از پیشنهاد الگوریتم رمزنگاری RC4 برای غلبه بر رمزگشایی می تواند به علت مشکلات هماهنگ سازی بوجود آید.
- ✓ برای محافظت در برابر دسترسی غیر مجاز به جریان اطلاعات بررسی شده است. روشی که در (lindner and mear, 2006) پیشنهاد شده یک مدل RBAC برای گسترش و حفاظت از داده های با دسترسی غیرمجاز است. ایده اصلی این است که با درخواست طراحی شده ی اپراتور در جریان، ناشی از ارزیابی یک پرس و جو برای فیلتر کردن تاپل خروجی که از سیاست های کنترل دسترسی راضی نیست. اشکال اصلی این روش این است که چارچوب پیشنهاد شده قادر نیست که سیاست های کنترل در نمایش داده ها از جریانهای چندگانه را که در اینترنت اشیا رخ می دهد را کنترل کند.
- ✓ یکی دیگر از کارهای مربوطه که در (Nehme et al, 2008) ارائه شده این است که در آن نویسنده پیشنهاد می کند که سیاستهای دسترسی به داده ها توسط کاربران در تعریف داده های خود جریان است. این باعث می شود که کاربران قادر باشند تا به سیستم مدیریت جریان داده و اطلاعات شخصی دسترسی داشته باشند. به این ترتیب، این یک راه حل مناسب تر برای پرداختن به مسائل حریم خصوصی، به جای کنترل دسترسی عمومی است. راه حل کلی تر آن مربوط به بهترین دانش ما در (Carminati et al, 2008) است، که با گسترش کار (Carminati et al, 2007) و ارائه یک چارچوب کلی برای حفاظت از جریان داده ها به صورت مستقل است.
- ✓ یک روش جایگزین، استفاده از رمزنگاری کلید با عمومی است (Mikelton et al, 2008)، اما در این مورد این اشکال توسط هزینه های محاسباتی مرتبط باید ارائه شود. این راه حل در پایین لایه مسائل امنیتی متمرکز است، به عنوان مثال، در مورد تصویب رمزگذاری تکنیک ها و طرح های توزیع کلیدها (Eschenauer and gelijer, 2002) (Pitro et al, 2009) در حوزه اینترنت اشیا، با استفاده از داده های جمع آوری شده نیاز به رسیدگی به دو چالش تحقیقات بنیادی است. اولین مورد، نیاز به کنترل دسترسی داده های جمع آوری شده در جریان داده است که در صورت تجمع داده ها با ویژگی های مربوط به اینترنت اشیاء یک راه حل برای ایجاد ویژگی دسترسی به داده های جمع آوری شده نیاز است. دومین مورد، نیاز مربوط به مقدمه ای از اپراتورهای مناسب برای حصول اطمینان از امکان بازیابی جریان خام از داده های تجمیع شده است.
- ✓ به منظور جلوگیری از دسترسی های غیر مجاز، به خصوص با توجه به استفاده از ارتباطات بی سیم در لایه های پایین تر،

مکانیسم های کنترل دسترسی باید با تکنیک حفاظت از داده ها صورت گیرد. نمونه های معمولی تکنیک های ناشناس هستند که بر اساس داده ها (Milikin, 2004) (Narayan and smetikoo,2005) ، و یا مکانیسم پنهان داده های دیگر، غیر قابل تشخیص است.

۳-۴) حریم خصوصی:

حفظ حریم خصوصی کلی شبکه بوسیله چیزهایی که می توانید به طور مستقیم آنها را کنترل کنید تا دسترسی به اطلاعات خود را محدود کنید. سازوکارهای اضافی باید اجرا شوند که در هر زمان اصل همکاری معماری متمرکز اینترنت اشیا اعمال شود. همچنین توجه داشته باشید که ما به صورت دستی نیز نیاز به پیکربندی و ارتباط مستقیم بین شبکه های داخلی و موجودیت های خارجی در شبکه ها را داریم.

راهکار:

پیشرفت کمی در مدیریت سیاست های کنترل دسترسی برای اینترنت اشیاء وجود داشته است اما در واقع، درخواست کنترل دسترسی موجود به محیط توزیع شده کاملا نزدیک است.

- ✓ مقیاس پذیری و سازگاری از جمله مسائل مهم در هنگام ذخیره لیستی از کاربران و مرتبط با حقوق دسترسی در لیست کنترل دسترسی آنها است(ACL) .
- ✓ دسترسی مبتنی بر نقش:

کنترل (RBAC) یک مکانیزمی است که نیاز به تعریف های مختلف نقش کاربران دارد که ممکن است در زمینه های مختلف حتی اگر آنها به همان نوع از نهاد مراجعه کرده باشند. در نهایت، سیاست RBAC که (Wey and Minel, 2004) نیاز به یک زیرساختی دارد که اجازه می دهد تا به گواهی مربوط به این زیرساخت در یک محیط اعتبار ببخشد. توجه داشته باشید، با این حال، که با توجه به ویژگی های خاص اینترنت اشیاء که ممکن است از نظر برخی از عوامل مانند شبکه اشیاء و به عنوان بخشی از مدل کنترل دسترسی با پشتیبانی از فن آوری مناسب و سیاست های خاص (به عنوان مثال فقط کاربران تصدیق وقایع در طول ساعات کاری می تواند گزارش دسترسی کاربران امروز را ارائه دهد) به راحتی اجرا شود.

- ✓ در روش دیگر، کنترل دسترسی منطقی را می توان در کارهای خود اجرا کرد، اما تنها تکیه بر روی نقش کاربر بصورت محلی دارد (به عنوان مثال یک دکتر از یک بیمارستان باید نقش محلی خود را قبل از ترک بیمارستان با اشیاء محلی بیمارستان بازیابی کند.)
- ✓ راه حل های مرسوم برای حصول اطمینان از محرمانه بودن اطلاعات ممکن است به دلیل به دو عامل عمده محدود کننده باشد. یکی از این عوامل مربوط به مقدار مطلق از اطلاعات تولید شده توسط این سیستم ها و مربوط به مسائل مقیاس پذیری است. دیگری مربوط به کنترل دسترسی به داده های برخط و راه حل انعطاف پذیر، با حقوق دسترسی به تغییرات در زمان اجرا با جریان داده های پویا است.

- ✓ تهدید وارده به این استراتژی این است که کاربران ابتدا باید قبل از دسترسی به اعتماد، نیاز خود را به اطلاعات همه اشیاء مشخص کند.

۴-۴) پروتکل های امنیتی شبکه:

یک کانال ارتباطی امن در اکثر موارد، یک محصول جانبی از احراز هویت موفق است. (به عنوان مثال سرور احراز هویت و یا تصدیق دو جانبه با استفاده از پروتکل هایی مانند TLS / DTLS) که در این فرآیند استفاده از برخی از موارد مانند اعتبار کاربر، کلید به اشتراک گذاشته و یا گواهی X.509 توصیه می شود.

در صورتی که برای مجموعه ای محدود از برنامه های متمرکز شده هر شی می تواند با هر شی دیگری در هر زمانی متصل شود، اشیاء ممکن است از پیش یکدیگر را بشناسند و همچنین با دستگاه های محدود می توانید اطلاعات را با دیگر دستگاه های محدود تبادل کنید. بنابراین، در این سناریو مدیریت کلید یک مشکل مهم است.

چالش های موجود در پروتکل های امنیتی:

- ✓ برخی از چالش های اضافی مربوط به منابع در دسترس محاسباتی وجود دارد مثل وجود کانال امن، دستگاه باید قادر به مذاکره واقعی پارامترهای این کانال باشد، مانند الگوریتم به عنوان مثال RSA تنها صداقت در مقابل محرمانه بودن و تمامیت ارضاء نمی شود بدلیل اینکه دستگاه ها محدود نمی شوند و قادر به اجرای تنظیمات خاص هستند و از طرفی سازگاری میان آنها هم وجود ندارد. بسته به عوامل مختلف مانند سطح بحرانی داده ها، آن را نمی توان با درخواست مکانیسم های محافظت قوی به یک جریان اطلاعاتی خاص محدود کرد.
- ✓ چالش دیگر نیاز به تجزیه و تحلیل تعداد پروتکل های امنیتی که می تواند در درون یک دستگاه محدود می شود، دارد. در واقع، لازم است به دقت مطالعه شود که آیا پروتکل اینترنت موجود باید به این زمینه اقتباس شود یا خیر؟
- ✓ در نهایت، چیزهایی که می توان آنها را به طور مستقیم دید (به عنوان مثال در روش اینترنت اشیا توزیع شده) باید مراقب باشید در مورد سربار ناشی از اتصالات ورودی (به عنوان مثال اتصالات ورودی های متعدد که نیاز به استفاده از رمزنگاری کلید عمومی دارد.) به موقع شناسایی شود.

راهکار:

- ✓ به عنوان اینترنت اشیاء ساکن اکوسیستم، مهم است که به ارائه پشتیبانی از پروتکل های امنیتی موجود پرداخته شود. در واقع، امنیت در طراحی پروتکل های انتقال وب، مانند COAP محدود به پروتکل کاربردی است و تا حد زیادی وابسته به اجرای این پروتکل های امنیتی است (Brachmann et al, 2012). برخی از پروتکل های آن می توانند بدون هیچ تغییر عمده ای اجرا شوند. مثلاً پیاده سازی تجاری از DTLS برای دستگاه های محدود موجود است . با این حال، پروتکل های دیگر نیاز به توجه به پیچیدگی طراحی خود دارند. چنین پروتکل هایی باید یک معاوضه بین رسیدن به

سادگی و سازگاری داشته باشند. برای مثال، یک رویکرد به دنبال اعمال IPsec برای محیط های محدود، با موازنه لایه امنیتی و امنیت IPsec را دارا است. (رضا و همکاران). همانطور که برای توزیع اعتبار، استراتژی های مختلفی وجود دارد که می تواند مورد استفاده قرار گیرد برای مقابله با این مشکل است. به همین دلیل در هر زمان که یک شی متعلق به یک گروه خاص محلی باشد، ممکن است دارای یک یا نهادهای مختلف مسئول مدیریت و توزیع اعتبار باشد.

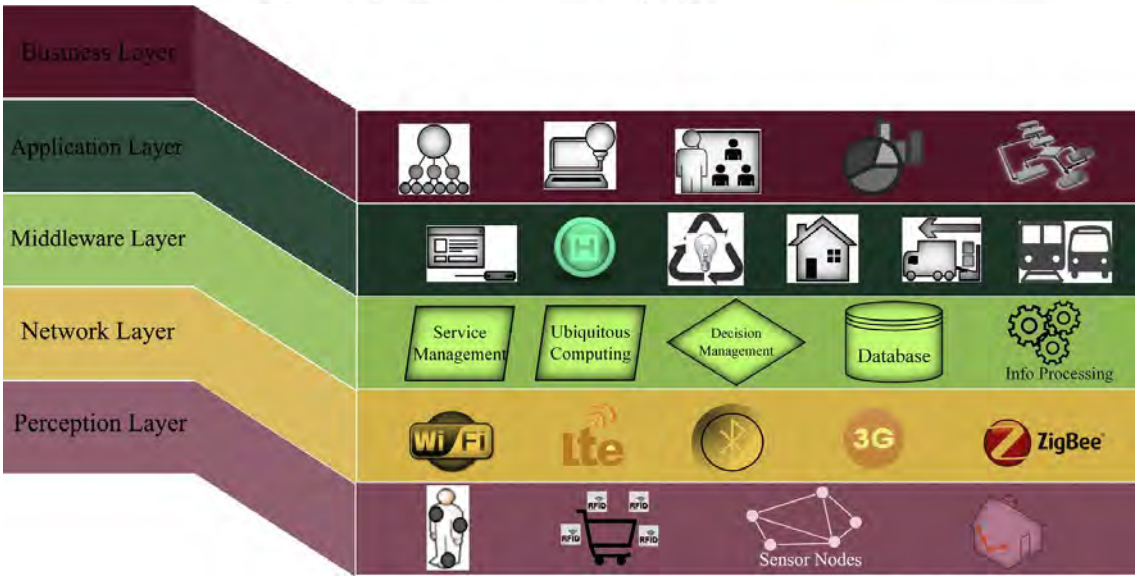
- ✓ در حالاتی که در آن مشتریان و سرور از پیش یکدیگر را می شناسند نیز ممکن استفاده از برخی پروتکل های مبتنی بر کلید متقارن، که می تواند انعطاف پذیری بالایی را به حملات داشته باشد تجویز می شود (Roman et al, 2011).
- ✓ در نهایت، فراتر از بهینه سازی این امنیت پروتکل های هستند. محققان به دنبال اجرای الگوریتم های رمزنگاری سریع و جمع و جور هستند. مناطق تحقیقاتی مختلفی که وجود دارد متقابلا منحصر به فرد نیست، از طراحی توابع هش گرفته تا الگوریتم های متقارن را نیز شامل می شود. می توان به بهینه سازی شکلهای هندسی اولیه موجود نیز پرداخت (Verbauwhede and Fan, 2012).

۵) برخی چالش های مربوط به آینده:

I / W / SW-OT پارادایم های مختلفی هستند. از جمله ویژگی های آنها در مقیاس بزرگ، غیر متمرکز و توزیع شده است، علاوه بر چالش های سنتی ای که از WSN به ارث برده چهره I / W / SW-OT (Yen Kuang, 2012) چالش های مختلفی را در بر دارد. این چالش ها را می توان به سه سطح طبقه بندی کرد: سطح فن آوری، سطح ارتباطات و شبکه، سطح هوش. سطح فناوری به چالش یکپارچه سازی هوشمند اشیاء می پردازد. سطح ارتباطات و شبکه چالش معاملات درون شبکه و ارائه خدمات در همه جا را شامل می شوئد. سطح هوش معاملات با چالش های همجوشی داده های عظیم و کشف سرویس . برخی از چالش های منحصر بفرد اینترنت اشیاء در بخش ذیل ذکر شده است.

۵-۱) معماری:

در طول مراحل اولیه اینترنت اشیا، بسیاری از پروژه ها و تحقیقات تلاش کرده اند برای ساخت معماری های مختلف که یک موضوع کلیدی و حیاتی برای توسعه اینترنت اشیا است، فعالیت کنند. بدون معماری خوب تعریف شده اینترنت اشیا نمی تواند در سطح جهانی مستقر شود. در حال حاضر، اینترنت اشیا با هدف ایجاد یک معماری مرجع که اجازه می دهد بدون درز فن آوری های ناهمگن و تسهیل فدراسیون، خود را با سیستم های دیگر ادغام کند. به منظور رسیدن به این هدف، اینترنت اشیا یک سری از مکانیسم های علمی و تکنولوژیکی مانند مقیاس پذیری، نگاه کردن و مکانیسم کشف شیء هوشمند را شناسایی کرده است. در اینجا یک نمونه معماری به تصویر کشیده شده است:



شکل ۱- معماری اینترنت اشیاء

۵-۲) عدم تجانس:

پارادایم I / W / SW-OT استقرار مشخص تعداد زیادی از دستگاه ها و اشیاء متفاوت را نشان می دهد. اینها اشیاء ناهمگن از نظر قابلیت محاسبه هستند: روش های ارتباطی، قابلیت ذخیره سازی با قدرت، در دسترس بودن انرژی، سازگاری. علاوه بر این، برنامه های کاربردی و خدمات از نظر پهنای باند نیاز متنوعی دارند، زمان تاخیر، قابلیت اطمینان، و غیره تعدادی از SWOTهای برنامه های کاربردی ارائه شده به جای ناهمگنی در اشیاء است. با این حال، مدیریت چنین سیستم های ناهمگنی بسیار چالش برانگیز است.

۵-۳) مقیاس پذیری:

هنگامی که اشیاء با منابع محدود مجهز به وب سرورها هستند، امکان استفاده از منابع را در وب فعال کنید. به عنوان تعدادی از اشیاء مبتنی بر وب بسیار گسترده می شود، مقیاس پذیری یک مسئله حیاتی است که در دو مرحله انجام می شود .در مرحله اول، اشیاء دارای فضای حافظه محدود برای رسیدگی به تعداد زیادی از درخواستها هستند و در مرحله دوم، قابلیت های خدمات وب سیستم عامل ها ممکن است در حضور هزاران میلیارد اشیاء هوشمند مقیاس پذیر باشد. یک پاسخ بصری به منظور بهبود مقیاس پذیری سرورهای وب پیشرفته تر است. ضروری است که یک مکانیسمی را ایجاد کرده و مختصات اشیاء هوشمند را برای ارائه راه حل های موثر برای مقیاس پذیری موضوع در یک سیستم اینترنت اشیا در مقیاس بزرگ بوجود آوریم.

۴-۵) گرین کارت آمریکا:

پیدا کردن اشیاء فیزیکی و توصیف خدماتی که از جمله قابلیت های اساسی در هر سیستم I / W / SW-OT هستند پس به طور کامل برای بهره برداری از این ویژگی های سیستم، اشیاء باید به طور موثر پیدا شده و توسط هر انسان و دیگر اشیاء استفاده شود. مکانیسم گرین کارت آمریکا اجازه می دهد تا اشیاء را در معرض ویژگی ها و پیدا کردن بهترین شی برای ارائه خدمات مورد نیاز ارائه دهد (nitti et al, 2014). با این حال، در یک سیستم I / W / SW-OT موجود مکانیزم خدمات گرین کارت آمریکا برای سیستم ها با تعداد کمی از اشیاء طراحی شده و بنابراین ممکن است در یک محیط حاوی تعداد بزرگی از اشیاء انجام نشود. یک روش جایگزین، به بهره برداری از موتورهای جستجو وب موجود برای سیستم I / W / SW-OT وجود دارد اما اجرای تکنیک جستجو در وب در یک سیستم I / W / SWOT چالش جدیدی است (Prera et al, 2014) و نمی توان به گرفتن ویژگی مهم اشیاء هوشمند مانند قابلیت اطمینان، محل، عمر باتری و ... اکتفا کرد. بنابراین، برای گسترش موتورهای جستجو وب سایت شامل اشیاء هوشمند امکان استفاده از گرین کارت آمریکا مورد نیاز است. چالش دیگر در استفاده از وب سیستم جستجوی بر روی یک سیستم I / W / SW-OT دست زدن به حجم زیادی از اطلاعات تولید شده توسط اشیاء در زمان واقعی است. وب کنونی از جمله روش های نمایه سازی هستند که مسئولیت رسیدگی داده های تولید شده به صورت پویا هستند، که به شدت می تواند اندازه شاخص عملکرد جستجو موتور را افزایش دهند. بنابراین، لازم است که برای طراحی تکنیک های جدید جستجو و مکانیزم هایی مانند نمایه سازی و پرس و جو، برای مقابله با این چالش ها و ویژگی های مورد نیاز ضبط از I / W / SW-OT استفاده کرد.

۵-۵) ترکیب پویا:

درSWOT ، ترکیب ها بصورت ایستا هستند آنها به عنوان یک مجموعه ای از خدمات پیش تعریف شده موجود می شود. با این حال، در طول زمان اجرا، برخی از خدمات می توانند به صورت پویا با سایر خدمات ایجاد شوند. کاربران می توانند با پیروی از قوانین و آگاهی از خدمات به رفع نیازهای خود بپردازند.

۵-۶) حریم خصوصی:

در اینترنت اشیا، اشیاء فیزیکی به تعداد زیادی از حملات آسیب پذیر هستند، در نتیجه برای اطمینان از امنیت آن در سطوح مختلف، با شروع از حفظ امنیت در سطح جسم از طریق پروتکل ارتباطی به سطح برنامه و حریم خصوصی کاربران از اهمیت زیادی در RFID برخوردار است (های و همکاران، ۲۰۱۲) . این مکانیزم در I / W / SW-OT می تواند برای افراد مورد استفاده قرار گیرد. برای هر راه حل امنیتی باید اطمینان حاصل شود تمامیت داده های رمزگذاری شده و احراز هویت در سطح امنیتی تائید شود. برای حفظ امنیت از جدیدترین پروتکل ارتباطی مثل 6LoWPAN انتظار می رود برای پیروزی در شبکه های آینده استفاده شود. این پروتکل یک حفاظ مناسب در برابر حملات می باشد. به طور مشابه، دارای چندین COAP امنیتی است که انتظار می رود به عنوان مکانیسم تحقیقاتی فعال در چند سال آینده استفاده شود.

طراحی پروتکل های ارتباطی یک چالش مهم برای I / W / SW-OT است. از آنجا که اکثر اشیاء به طور مستقیم نمی توانند این پروتکل را پشتیبانی کنند از آدرس IP به منظور حصول اطمینان سیستم برای تعداد زیادی از اشیاء و ارتباط بین آنها بعنوان پروتکل های ارتباطی استفاده می شود.

راهکار:

- ✓ در (Cavakli et al 2014) که در واقع، نشان دهنده یک روش مهندسی مورد نیاز برای حفظ الزامات حریم خصوصی به روند طراحی سیستم است. روشی را فراهم می کند که مجموعه ای از مفاهیم و الزامات به مدل حریم خصوصی و مجموعه ای از قوانین برای تبدیل و پیاده سازی این الزامات است.
- ✓ در (Coen et al, 2010)، هدف، تعریف UML[۴] عمومی است که مدل برای حفظ سیاست حریم خصوصی است. مدل مشخص شامل مجموعه ای از ماژول های تابعی مورد نیاز یک نرم افزار به منظور اجرای این سیاست ها و معرفی تمام عناصر مورد نیاز برای تعریف سیستم های آگاه حریم خصوصی است. به عنوان مثال آن را در سطح بسیار بالایی از انتزاع اجرا کرده و برای استفاده از اینترنت اشیا، که با درجه بالایی از عدم تجانس در شرایط الزامات حریم خصوصی پیاده سازی می شود.
- ✓ ارائه چند راهکار برای چالش تحقیقاتی باز از نظر حفظ حریم خصوصی بعنوان یک مکانیزم برای اینترنت اشیا شامل موارد ذیل است:
  - تعریف یک مدل کلی برای حفظ حریم خصوصی در اینترنت اشیا.
  - توسعه روش های اجرائی نوآورانه که قادر به پشتیبانی از مقیاس پذیری و ناهمگنی مشخص در سناریوهای اینترنت اشیا است.
  - توسعه راه حل هایی که نیاز به ناشناس ماندن توسط برخی از برنامه های محلی سازی دارند و الزامات برخی از آنهایی که نیازمند ردیابی هستند که این امر مستلزم تعریف سیاست حفظ حریم خصوصی است که تحت آن شرایط ممکن است لازم باشد به شناسایی و ترجمه و بومی سازی یک شیء هوشمند بپردازیم، علاوه بر این، نیاز دارد که به اطلاعات حساس دسترسی داشته باشیم.

۷-۶) شناسایی شبکه های اجتماعی:

متاسفانه، SWOT از جمله چالش های جدید است. موضوع شناسایی شبکه های اجتماعی نیز یک موضوع مهم است. ایجاد یک هویت برای شبکه های اجتماعی برای هر شی هوشمند با توجه به دخالت کاربر غیر ممکن است. بنابراین، ترکیب برخی از شبکه های اجتماعی به منظور رسیدگی به تعداد زیادی از اشیاء با حداقل هویت شبکه های اجتماعی امکان پذیر است.

[۴] Unified Modeling Language

۶-۶) اعتماد:

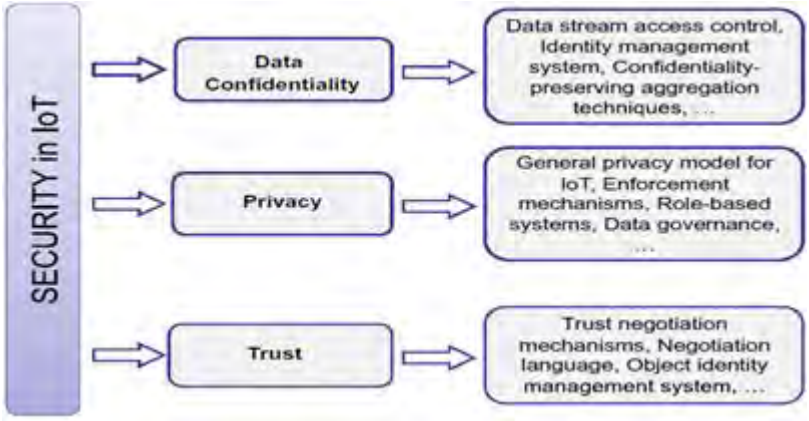
مدیریت اعتماد برای ساخت سیستم با قابلیت اعتماد بر اساس رفتار کاربران در I / W / SW-OT قابل استفاده است.

راهکار:

- ✓ در راه حل های پیشنهادی برای ساخت مدل ذهنی برای مدیریت اعتماد از روش هایی مثل نظیر به نظیر (P2P)[۵] و شبکه های اجتماعی (Nitti et al, 2012) استفاده می شود، که در آن هر گره به تعیین اعتماد از دوستان بر اساس تجربه خود را دارد و در نظر دوستان مشترک هستند. نویسندگان در (Nitti et al, 2013) یک مدل هدفی را پیشنهاد داده اند که در آن اطلاعات در مورد هر گره توزیع و ذخیره شده به طوری که هر گره می تواند از همان اطلاعات استفاده کند.
- ✓ معرفی یک زبان ساده مذاکره برای حمایت از الزامات قابلیت همکاری معنایی اینترنت اشیا.
- ✓ تعریف یک مکانیزم مذاکره اعتماد بر اساس کنترل دسترسی جریان داده.
- ✓ توسعه مدیریت هویت اشیاء کافی سیستم.
- ✓ طراحی یک مدیریت اعتماد کلی و قابل انعطاف برای چارچوب موارد فوق.

۷) راهکارهای چالش اصلی برای حصول اطمینان از محرمانه بودن اطلاعات در یک سناریوی اینترنت اشیا، همانطور که در شکل ۲ نشان داده شده است عبارتست از:

- ✓ تعریف مکانیزم مناسب برای کنترل دسترسی جریان اطلاعات تولید شده توسط دستگاه های اینترنت اشیا.
- ✓ تعریف زبان پرس و جوی مناسب برای فعال کردن برنامه های بازیابی اطلاعات مورد نظر از یک جریان داده.
- ✓ تعریف مدیریت هویت مناسب اشیاء هوشمند سیستم.



شکل۲- سناریوی اینترنت اشیا

۲-۴- اهداف و فرضیه های پژوهش:

[۵] Peer to Peer

هدف اصلی تحقیق:

ارائه مدل برای شناسایی چالش ها و تهدیدات کلیدی در حوزه اینترنت اشیاء

اهداف فرعی:

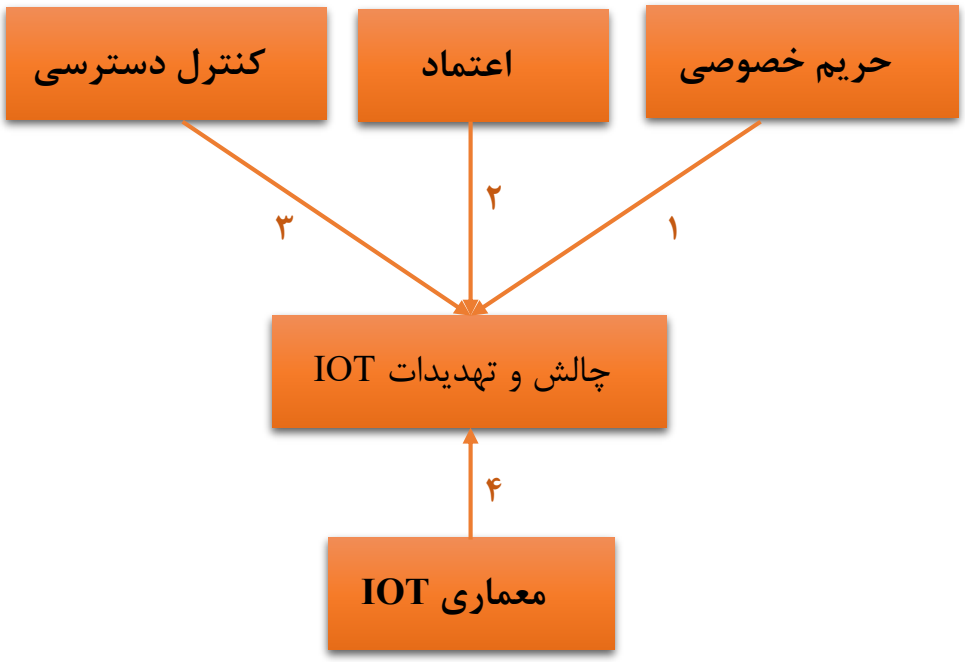
- ✓ بررسی و تحلیل چالش ها و تهدیدات در حوزه اینترنت اشیاء
- ✓ بررسی و تحلیل راهکارهای ارائه شده در حیطه هر یک از چالش ها و تهدیدات در حوزه اینترنت اشیاء
- ✓ شناسایی بیشترین تهدیدات در حوزه اینترنت اشیاء
- ✓ بررسی و تحلیل بروزترین راهکارهای ارائه شده توسط خبرگان در زمینه اینترنت اشیاء

۳-روش تحقیق:

پژوهش حاضر از نظر هدف کاربردی و از نظر روش کار تحلیلی _ پیمایشی است. با توجه به مطالعات انجام شده در بخش ادبیات تحقیق، با تهیه فهرستی از چالش ها و تهدیدات حول اینترنت اشیاء و بررسی راهکارهای ارائه شده مربوط به برخی از آنها، عواملی را که در تهدیدات و چالش های اینترنت اشیاء اثر گذارند شناسایی شد و با بررسی این عوامل طبق نظر خبرگان در این حوزه، برترین آنها شناسایی شد و پرسش نامه ای حاوی ۱۹ سوال که در پیوست قرار داده شده است جهت ارزیابی این عوامل بین خبرگان موجود در این حیطه بصورت تصادفی پخش شد. لازم به ذکر است سوالات پرسش نامه نیز طبق نظر خبرگان امر، ویرایش و اصلاح شده اند و همه سازه ها با طیف لیکرت (۱=خیلی کم، ۵=خیلی زیاد) مورد سنجش قرار گرفتند. سپس با بررسی و حذف عواملی که تاثیر مثبت و مستقیمی بر روی مدل نداشتند این مدل در شکل ۴ به تصویر کشیده شده است.

۳-۱- مدل ارائه شده در تحقیق:

طبق آزمون های انجام شده باتوجه به اینکه مقدار sig بیشتر از ۰,۰۵ بود متغیرهای اعتماد و ناهمگونی از مدل حذف شدند و مدل نهایی در شکل ۴ به تصویر کشیده شده است.



شکل۴- مدل پژوهش

۳-۲- فرضیات تحقیق:

۱: بین حریم خصوصی افراد موجود در شبکه IOT و چالش ها و تهدیدات IOT رابطه مثبت و مستقیم وجود دارد.

۲: بین اعتماد افراد مصرف کننده گان شبکه IOT و چالش ها و تهدیدات IOT رابطه مثبت و مستقیم وجود دارد.

۳: بین کنترل دسترسی اشیاء و یا کاربران موجود در شبکه IOT و چالش ها و تهدیدات IOT رابطه مثبت و مستقیم وجود دارد.

۴: بین معماری های معرفی شده برای IOT و چالش ها و تهدیدات IOT رابطه مثبت و مستقیم وجود دارد.

۴-یافته ها:

جدول۱_ سابقه کاری خبرگان در زمینه اینترنت اشیاء

تعداد	کمترین سابقه	بیشترین سابقه	میانگین	چولگی
۲۲	۳	۱۹	۱۳,۴۴	۰,۱۱۰

جدول۲_ تحصیلات مربوط به خبرگان در زمینه اینترنت اشیاء

تعداد	کارشناسی ارشد	دکترا
۲۲	۲	۲۰

جدول۳_ میانگین دسته بندی پرسشنامه

	حریم خصوصی	معماری IOT	کنترل دسترسی	اعتماد
مینیمم	۲	۲	۲	۲
ماکسیمم	۱۰	۲	۵	۲
میانگین	۶	۲	۳,۵	۲

جدول۴_ روایی و پایایی پرسش نامه

سوالات پرسشنامه	
دسته بندی سوالات بر اساس مدل ارائه شده	آلفای کرونباخ
حریم خصوصی	۰,۰۴
اعتماد	۰,۰۵
کنترل دسترسی	۰,۰۱۲
معماری IOT	۰ .۰۳
ناهمگونی	۱,۰۰
تصدیق هویت	۰,۰۷
کل پرسشنامه	۰,۸۲

از آنجایی که میزان آلفای کرونباخ برای تمامی فرضیات (بجز دو مورد) کمتر از ۰,۰۵ است پس این فرضیات تائید شده و دو فرضیه دیگر (ناهمگونی و تصدیق هویت) که مقادیر آلفای کرونباخ آنها بیش از ۰,۰۵ است رد شده اند.

جدول۵_ نتایج مربوط به آزمون اسپیرمن

فرضیات	آزمون اسپیرمن	
	sig	درجه
۱	۰,۰۲۹	۰,۲۷۰
۲	۰,۰۳۱	۰,۳۷۰
۳	۰,۰۳۹	۰,۳۵۶
۴	۰,۰۴۸	۰,۳۲۰

از آنجایی که مقدار sig در تمامی فرضیات کمتر از ۰,۰۵ است پس تمامی فرضیات تائید شده اند. لازم به ذکر است که فرضیات ناهمگونی و تصدیق هویت به ترتیب با مقدار sig، ۱ و ۰,۰۷ رد شدند.

جدول۶_ نتیاج آزمون رگرسیون چندگانه

متغیر وابسته	متغیرهای مستقل	میزان شدن رابطه	sig	نتیجه
حریم	اعتماد و کنترل	۰,۷۵	۰,۰۰۶	رابطه خطی وجود

خصوصی	دسترسی			دارد
اعتماد	کنترل دسترسی و معماری	۰,۶۴	۰,۰۰۹	رابطه خطی وجود دارد
کنترل دسترسی	معماری و حریم خصوصی	۰,۱۲	۰,۰۲۲	رابطه خطی وجود دارد
معماری IOT	حریم خصوصی و کنترل دسترسی	۰,۴۴	۰,۰۱۲	رابطه خطی وجود دارد

از آنجایی که مقدار sig کمتر از ۰,۰۵ است و با توجه به متغییرهای وابسته و مستقل نتایج مثبت بدست آمده است و نتیجه شد که رابطه خطی بین متغیرها وجود دارد.

۵-بحث و نتیجه گیری:

پژوهش حاضر یکی از مطالعات انجام شده در حوزه بررسی و تحلیل حول تهدیدات IOT است که با ارائه مدلی از تهدیدات IOT سعی شده کلیدی ترین عوامل تاثیر گذار شامل حریم خصوصی، معماری IOT، کنترل دسترسی و اعتماد؛ شناسایی شده و با جلوگیری از این تهدیدات از بروز مسائل و مشکلات بعدی نیز جلوگیری به عمل آید. در این پژوهش ۶ فرضیه در نظر گرفته شد. دو فرضیه ناهمگونی و تصدیق هویت با میزان sig بیشتر از ۰,۰۵ رد شدند و چهار فرضیه دیگر با عناوین حریم خصوصی، معماری IOT، کنترل دسترسی و اعتماد با مقادیر sig کمتر از ۰,۰۵ پذیرفته شدند. فرضیه با متغیر وابسته حریم خصوصی و متغیرهای مستقل اعتماد و کنترل دسترسی با میزان رابط ۰,۷۵ و مقدار sig، ۰,۰۰۶ تائید شده و ثابت شد که میان آنها رابطه خطی و مستقیم وجود دارد. فرضیه با متغیر وابسته اعتماد و متغیرهای مستقل معماری و کنترل دسترسی با میزان رابط ۰,۶۴ و مقدار sig، ۰,۰۰۹ تائید شده و ثابت شد که میان آنها رابطه خطی و مستقیم وجود دارد. فرضیه با متغیر وابسته کنترل دسترسی و متغیرهای مستقل معماری و حریم خصوصی با میزان رابط ۰,۱۲ و مقدار sig، ۰,۰۲۲ تائید شده و ثابت شد که میان آنها رابطه خطی و مستقیم وجود دارد. فرضیه با متغیر وابسته معماری و متغیرهای مستقل حریم خصوصی و کنترل دسترسی با میزان رابط ۰,۴۴ و مقدار sig، ۰,۰۱۲ تائید شده و ثابت شد که میان آنها رابطه خطی و مستقیم وجود دارد. یافته های تحقیقات پیشین طبق آنچه که در پیشینه تحقیق ذکر شد ارائه فهرست وار تهدیدات و چالش های حول IOT و ارائه راهکار در مورد برخی از تهدیدات جهت جلوگیری از مشکلات امنیتی و برقراری فضای امن بوده است. در واقع هدف این پژوهش بررسی این موارد و ارائه یک مدل براساس مهمترین و کلیدی ترین تهدیدات IOT بوده است که با تائیدیه فرضیات این تحقیق طبق نظر خبرگان به نتایج مناسبی دست یافته شد. طبق آنچه که لازم بود باید بروزترین مقالات در حیطه IOT انتخاب و مطالعه می شدند و از طرفی هم پیدا کردن خبرگان در این حیطه جهت شناسایی و بررسی کلیدی ترین تهدیدات از

جمله محدودیت هایی بود که حول این پژوهش وجود داشت.

ما امیدواریم که این بررسی برای محققان و پژوهشگران در حوزه شناخت امنیت در اینترنت اشیاء مفید باشد و به کاربران در این زمینه کمک کند که به درک پتانسیل عظیمی از اینترنت اشیاء پرداخته و مسائل مربوط به تهدیدات، چالش ها، آسیب پذیری ها و از همه مهمتر برقراری شرایط امن را حل کنند، ابداع راه حل های نوآورانه فنی به نوبه خود قادر است اینترنت اشیا را از یک چشم انداز تحقیقی به واقعیت تبدیل کند. حوزه پژوهشی پیشنهادی آینده در خصوص امنیت اینترنت اشیا در دستگاه های تلفن همراه است. تلاش های بسیاری توسط جامعه علمی در سراسر جهان به پرداختن به موضوعات فوق الذکر شده است، اما هنوز بسیاری از مسائل روشن نشده است. ما امیدواریم که این پژوهش در مسیر سایر پژوهش های مشابه به منظور استفاده گسترده سیستم های اینترنت اشیا در جهان واقعی باشد.

۶- منابع:

1. B. Carminati, E. Ferrari, K. Tan, J. Cao, A framework to enforce access control over data streams, ACM Trans. Inform. Syst. Sec. (TISSEC) 13 (3) (2008) 1–31.
2. B. Carminati, E. Ferrari, K. Tan, Enforcing access control policies on data streams, in: Proceedings of the 12th ACM Symposium on Access Control Models and Technologies (SACMAT'07), Sophia Antipolis, France, 2007, pp. 21–30.
3. B. Carminati, E. Ferrari, K. Tan, Specifying access control policies on data streams, in: Proceedings of the 12th International Conference on Database System for Advanced Applications, Lecture Notes in Computer Science, Springer, Bangkok, Thailand, 2007, pp. 410 421.
4. Bechini, F. Marcelloni, A. Segatori, Low-effort support to efficient urban parking in a smart city perspective, in: S. Gaglio, G. Lo Re (Eds.), Advances onto the Internet of Things, Springer International Publishing, 2014, pp. 233–252, http://dx.doi.org/10.1007/978-3- 319-03992-3_17.
5. CASAGRAS, RFID and the Inclusive Model for the Internet of Things, EU Project Number 216803, 2011, pp. 16–23.
6. Clark, D. (2014, January 5). 'Internet of Things' in reach: Com-panies rush into devices like smart door locks, appliances, but limitations exist. The Wall Street Journal. Retrieved April 3, 2015, from http://www.wsj.com/articles/SB10001424052702303640604579296580892973264.
7. Cavoukian, Privacy by Design. . . Take the Challenge, Information and Privacy Commissioner of Ontario, Canada, 2009.
8. C. Gao, Z. Ling, Y. Yuan, The research and implement of smart home system based on Internet of Things, in: 2011 International Conference on Electronics, Communications and Control (ICECC),Ningbo, China, 2011, pp. 2944–2947. http://dx.doi.org/10.1109/ICECC.2011.6066672.

9. Coen-Porisini, P. Colombo, S. Sicari, Privacy aware systems: from models to patterns, in: Software Engineering for Secure Systems: Industrial and Research Perspectives, IGI Global, 2010.
10. C. Perera, A. Zaslavsky, C.H. Liu, M. Compton, P. Christen, D. Georgakopoulos, Sensor search techniques for sensing as a service architecture for the internet of things, IEEE Sensors J. 14 (2014) 406–420, http://dx.doi.org/10.1109/JSEN.2013.2282292.
11. C. Yen-Kuang, Challenges and opportunities of internet of things, in: 2012 17th Asia and South Pacific, Design Automation Conference (ASP-DAC), 2012, pp. 383–388. http://dx.doi.org/10.1109/ASPDAC. 2012.6164978.
12. D. Guinard, M. Fischer, V. Trifa, Sharing using social networks in a composable web of things, in: 1st International Workshop on the Web of Things (WoT'10), Mannheim, Germany, 2010, pp. 702_707.
13. D. Minoli, Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications, Wiley, 2013.
14. D. Viehland, F. Zhao, The future of personal area networks in a ubiquitous computing world, International Journal of Advanced Pervasive and Ubiquitous Computing 2 (2) (2010) 30–44.
15. European Network of Excellence in Cryptology II. <http:// www.ecrypt.eu.org/> (accessed 11.12).
16. E. Ilie-Zudor, Z. Kemeny, F. van Blommestein, L. Monostori, A. vander Meulen, A survey of applications and requirements of unique identification systems and RFID techniques, Computers in Industry 62 (3) (2011) 227–252.
17. E. Kavakli, C. Kalloniatis, P. Loucopoulos, S. Gritzalis, Addressing privacy requirements in system design: the pris method, J. Requirements Eng. 13 (3) (2008) 241–255.
18. E. Mykletun, J. Girao, D. Westhoff, Public key based cryptoschemes for data concealment in wireless sensor networks, in: Proceedings of IEEE ICC, Istanbul, Turkey, 2006, pp. 2288–2295.
19. E. Theodoridis, G. Mylonas, I. Chatzigiannakis, Developing an IoT smart city framework, in: 2013 Fourth International Conference on Information, Intelligence, Systems and Applications (IISA), Piraeus, Greece, 2013, pp. 1–6. http://dx.doi.org/10.1109/IISA.2013. 6623710.
20. F. Shifeng, X. Lida, P. Huan, L. Yongqiang, L. Zhihui, Z. Yunqiang, Y. Jianwu, Z. Huifang, An integrated approach to snowmelt flood forecasting in water resource management, IEEE Trans. Ind. Inform. 10 (2014) 548–558, http://dx.doi.org/10.1109/TII.2013.2257807.
21. INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in co-operation with the Working group RFID of the ETP EPOSS, Internet of things in 2020: Roadmap for the future, 27 May 2008.
22. J. Takalo-Mattila, J. Kiljander, M. Etelapera, J.-P. Soininen, Ubiquitous computing by utilizing semantic interoperability with item-level object identification, in: Second

International ICST Conference on Mobile Networks and Management (MONAMI'10), Santander, Spain, 2010, pp. 198–209.
23. L.D. Xu, C. Wang, Z. Bi, J. Yu, Object-oriented templates for automated assembly planning of complex products, IEEE Trans. Automat. Sci. Eng. (2013) 1–12, http://dxdoi.org/10.1109/ TASE.2012.2232652.
24. L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of ACM CCS, Washington, DC, USA, 2002, pp. 41–47.
25. L. Tan, N. Wang, Future internet: the internet of things, in: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE, Chengdu, China, 2010, pp. 376–380, http://dx.doi.org/10.1109/ICACTE.2010.5579543.
26. M. Nitti, R. Girau, L. Atzori, A. Iera, G. Morabito, A subjective model for trustworthiness evaluation in the social Internet of Things, in: 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), IEEE, Sydney, Australia, 2012, pp. 18–23, http://dx.doi.org/10.1109/PIMRC.2012. 6362662.
27. M. Ali, M. ElTabakh, C. Nita-Rotaru, Ft-Rc4: A Robust Security Mechanism for Data Stream Systems, Purdue University, Technical Report, TR-05-024.
28. M. Brachmann, S.L. Keoh, O.G. Morchon, S.S. Kumar, End-to-end transport security in the IP-based internet of things, in: 21st International Conference on Computer Communications and Networks (ICCCN'12), Munich, Germany, 2012, pp. 1–5.
29. M.C. Domingo, An overview of the internet of things for people with disabilities, J. Netw. Comput. Appl. 35 (2012) 584–596, http:// dx.doi.org/10.1016/j.jnca.2011.10.015.
30. M. Nitti, R. Girau, L. Atzori, Trustworthiness management in the social internet of things, IEEE Trans. Knowl. Data Eng. 26 (2013) 1253–1266, http://dx.doi.org/10.1109/TKDE.2013.105 .
31. M. Nitti, L. Atzori, I.P. Cvijikj, Network navigability in the social Internet of Things, in: 2014 IEEE World Forum on Internet of Things (WF-IoT) Seoul, Korea, 2014, pp. 405–410. doi:10.1109/WFIoT. 2014.6803200.
32. Mocana – NanoDTLS. https://mocana.com/products.html (accessed 11.12).
33. W. Lindner, J. Meier, Securing the borealis data stream engine, in: Proceedings of the International Database Engineering and Application Symposium (IDEAS'06), Delhi, India, 2006, pp. 137– 147.
34. Narayanan, V. Shmatikov, Obfuscated databases and group privacy, in: Proceedings of ACM International Conference on Computer and Communications Security (CCS), ACM Press, New York, USA, 2005, pp. 102–111.
35. O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I.S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, P. Doody, Internet of Things Strategic Research Roadmap, Cluster of European Research Projects on the Internet of Things, CERP-IoT, 2011.
36. P. Mahalle, S. Babar, N.R. Prasad, R. Prasad, Identity management framework towards Internet of Things (IoT): roadmap and key challenges, in: N. Meghanathan, S.

Boumerdassi, N. Chaki, D. Nagamalai (Eds.), Recent Trends in Network Security and Applications, Communications in Computer and Information Science, vol. 89, Springer, Berlin Heidelberg, 2010, pp. 430–439.

37. R. Nehme, E. Rundesteiner, E. Bertino, A security punctuation framework for enforcing access control on streaming data, in: Proceedings of the 24th International Conference on Data Engineering (ICDE'08), Cancun, Mexico, 2008, pp. 406–415.
38. R.D. Pietro, C. Soriente, A. Spognardi, G. Tsudik, Collaborative authentication in unattended WSNs, in: Proceedings of ACN WiSec, Zurich, Switzerland, 2009, pp. 237–244.
39. R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in the context of the internet of things, Computers & Electrical Engineering 37 (2011) 147–159.
40. R. Roman, P. Najera, J. Lopez, Securing the internet of things, IEEE Computer 44 (9) (2011) 51–58.
41. Sarma, J.a. Girم٥, Identities in the future internet of things, Wireless Personal Communications 49 (3) (2009) 353–363.
42. S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad, Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT), in: 3rd International Conference on Recent Trends in Network Security and Applications (CNSA'10), Chennai, India, 2010, pp. 420–429.
43. S. Eberle, Adaptive internet integration of field bus systems, IEEE Trans. Ind. Inform. 3 (2007) 12–20, http://dx.doi.org/10.1109/ TII.2006.890525.
44. S.G. Weber, L.A. Martucci, S. Ries, M. Mühlhنuser, Towards trustworthy identity and access management for the future internet, in: 4th International Workshop on Trustworthy Internet of People, Things & Services (Trustworthy IoPTS'10), 2010.
45. S. Fang, L. Xu, Y. Zhu, J. Ahati, H. Pei, J. Yan, Z. Liu, An integrated system for regional environmental monitoring and management based on internet of things, IEEE Trans. Ind. Inform. (2014) 1596– 1605, http://dxdoi.org/10.1109/TII.2014.2302638.
46. S. Hui, W. Jiafu, Z. Caifeng, L. Jianqi, Security in the internet of things: a review, in: 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, China, 2012, pp. 648–651. http://dx.doi.org/10.1109/ICCSEE.2012. 373.
47. S. Raza, S. Duquennoy, J. Hglund, U. Roedig, T. Voigt, Secure communication for the internet of things – a comparison of linklayer security and IPsec for 6LoWPAN, Security and Communication Networks (in press). http://dx.doi.org/10.1002/sec.406/abstract.
48. S. Turner, T. Polk, Security Challenges For the Internet of Things, in: IAB Interconnecting Smart Objects with the Internet Workshop, Prague, Czech Republic, 2011.
49. T. Bauge (Ed.), D3.5 – Global and Pluggable Sensor and Actuator Networking Framework, SENSEI Project, 2011. <http://www.senseiproject. eu/>.

50. T. Mielikinen, Privacy problems with anonymized transaction databases, in: Proceedings of international Conference on Discovery Science (DS 2004), Lecture Notes in Computer Science, vol. 3245, Springer, 2004.
51. Verbauwhede, J. Fan, Light-weight public key implementations for constrained devices, in: Workshop on Cryptography for the Internet of Things, Antwerp, Belgium, 2012.
52. Y. Chen, J. Guo, X. Hu, The research of internet of things' supporting technologies which face the logistics industry, in: 2010 International Conference on Computational Intelligence and Security (CIS), China, 2010, pp. 659–663. http://dx.doi.org/10.1109/CIS.2010.148.
53. Y. Fan, Y. Yin, L. Xu, Y. Zeng, F. Wu, IoT based smart rehabilitation system, IEEE Trans. Ind. Inform. (2014) 1568–1577, http:// dxdoi.org/10.1109/TII.2014.2302583.
54. Z. Bi, L. Xu, C. Wang, Internet of things for enterprise systems of modern manufacturing, IEEE Trans. Ind. Inform. (2014) 1, http:// dxdoi.org/10.1109/TII.2014.2300338.
55. Z. Ji-chun, Z. Ju-feng, F. Yu, G. Jian-xin, The study and application of the IOT technology in agriculture, in: 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), Chengdu, China, 2010, pp. 462–465. http://dx.doi.org/10. 1109/ICCSIT.2010.5565120.
56. Z. Pang, L. Zheng, J. Tian, S. Kao-Walter, E. Dubrova, Q. Chen, Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things, Enterprise Inform. Syst. (2013) 1–31, http://dxdoi.org/10.1080/17517575.2013.776118.
57. Z. Tao, Q. Yajuan, G. Deyun, D. Junqi, Z. Hongke, A practical deployment of Intelligent building wireless sensor network for environmental monitoring and air-conditioning control, in: 2010 2nd IEEE International Conference on Network Infrastructure and Digital Content, Beijing, China, 2010, pp. 624-628. http://dx.doi.org/10.1109/ICNIDC.2010.5657858.
58. Z. Wei, C. Meinel, Implement role based access control with attribute certificates, in: 6th International Conference on Advanced Communication Technology (ICACT'04), Phoenix Park, Korea, 2004, pp. 536–540.