# مدیریت هویت و حفاظت از تمامیت در اینترنت اشیاء


## چکیده

احراز هویت و مدیریت هویت به حفاظت از منابع و توجیه کردن اعتماد به عملیات اصلی توسط مشتری سرویس و فراهم کننده ی سرویس کمک می کند. بعلاوه، مدیریت هویت می تواند سخت افزار کمک کننده به حفظت از تمامیت را پشتیبانی کند. در اینترنت اشیاء (IOT)، تعداد بالای دستگاه های سبگ وزن نیازمند راه حل های مقیاس پذیر و سبک وزن برای اطمینان به مدیریت است. مقاله چارچوبی برای احراز هویت و حفاظت از تمامیت مناسب برای یک محیط IOT ارائه می دهد.


## 1. دیباچه

عبارت "اینرنت اشیاء" به یک قرارداد در دنیا که "همه چیز" به صورت منحصر به فرد از طریق نوعی دستگاه ارتباطی قابل شناسایی و نشانی پذیر هستند و بتوان اشیاء را برای هدف های مختلف موقعیت یابی کرد، به کار گرفت،حفظ و نگهداری کرد و مورد بازرسی قرار داد.

"اشیاء" چه به عنوان ارزش مادی یا چه در حالت سویسی که رائه می دهند، منابع ارزشمندی هستند (ارائه می کنند). منابع نیاز دارند تا از طریق چرخه ی زندگیشان مدیریت شوند، و دسترسی به منابع نیاز دارند تا کنترل و حسابرسی شوند. هویت منابع و مشتری هایشان (در جایی که قابل اطلاق باشد) باید توسط یک سیستم مدیریت هویت مدیریت، محافظت و نگهداری شود، و باید مکانیزم هایی در محل برای احراز هویت ها، کنترل دسترسی به منابع و حفاظت از کاربرد اطلاعات به خاطر حفاظت از حریم خصوصی وجود داشته باشد (۱).

در حوزه ی مدیریت هویت (IDM)، مفهوم تضمین هویت به عنوان یک وسیله ی مهم برای کنترل منبع در نظر گرفته شده است. یک IDM سرویس هایی برای احراز هویت که به معنی نوعی مکانیزم برای تشخیص ماهیت (به عنوان مثال یک شخص) که بر روی منبع فعالیت می کند، است ارائه می کند. احراز هویت یک شیء لزوما به معنی اطمینان از هویت نیست بلکه اطمینان از اصالت یا تمامیت آن است. احراز هویت پیش نیازی برای حسابرسی ، حسابداری و کنترل دسترسی همانند پرونده های کاربری شخصی و دیگر سرویس های نامرتبط به امنیت و مسئولیت است.

قوانین IDM به خوبی درک شده اند اما سیستم های IDM پیچیده هستند و اکثرا در محیط های نسبتا همگنی یافت می شوند که استانداردهای فراگیر برای ارائه ی اطلاعات و پروتوکل های شبکه بتوانند اجرا شوند. اینترنت اشیاء مشخصاتی ذاتی دارد که برای گسترش یک IDM چالش هایی ارائه می کند:

• مقیاس مطلق سیستم، به صورت بالقوه میلیارد ها شیء با چرخه ی زندگی کوتاه و "نرخ تولد" بالا

• عدم تجانس واحد ها، که از چیپ های RFID با حداقل توان پردازش، قابلیت های ارتباطی و حافظه ی داخلی تا کامپیوتر های مقیاس بزرگ با منابع زیاد تغییر می کند. هیچ استاندارد رایجی برای ارائه یا اانتقال بر روی این محدوده ی تجهیزات نمی تواند اجرا شود و چندین استاندارد مختلف به احتمال زیاد همزیستی می کنند.

• تعداد بالای حوزه های مدیریت. دستگاه های IOT توسط اجتماع بزرگی ار فراهم کننده های سرویس ها و سرمایه گذاران مدیریت و به کار گرفته می شوند. آنها به احتمال زیاد سیاست های نمگذاری بسیار مختلف ، چارچوب های امنیتی، نیازمندی های پروتوکلی و کنترل های دسترسی را به کار می برند. به منظور اتصال دادن این تفاوت ها، ممکن است که نقاط درگاهی سنتی نیاز به جایگزینی توسط پردازنده های معنا شناختی داشته باشند.

در ادامه ی مقاله، برخی مسائل و اهداف تحقیق مرتبط با IdM در اینترنت اشیاء بحث خواهد شد. مجموعه ای از مکانیزم های ارائه شده برای کنترل اصالت ارائه خواهد شد مشخصات ضروری مکانیزم ها، سادگی، احتیاط و وفق پذیریشان خواهد بود.

## 2. مشخصات ضروری سیستم

انتظار می رود تا اینترنت اشیاء به مقیاسی که قبلا هرگز مشاهده نشده و با محدوده ی گسترده تری از تجهیزات با منابع و توانایی مختلف بیشتر دست یابد. بعلاوه، قطعا کاربردهای آینده ی IOT به صورت شگفتی می آیند و نگاه کنونی ما بر اینکه چطور دستگاه های IOT می توانند به ساخت تجارت کمک کنند را به چالش می کشد.

بنابراین، گسترش تکنولوژی برای اهداف IOT باید قوانین شناخته شده از محاسبه ی مقیاس بزرگ را دنبال کند (2).

### A. گرایش خدمت

ممکن است که "اشیاء" به شکل اهداف خنثی به نظر برسند اما ممکن است که به عنوان فراهم کننده های سرویس به خوبی در نظر گرفته شوند. ساده ترین سرویس ممکن، معلوم کردن هویت یک فرد است که حتی یک دستگاه ساده ی RFID قادر به انجام دادن آن است. بنابراین قرار دادن اینترنت اشیاء در چشم انداز جهت دار سرویس که در آن تمام تراکنش ها یک آغازگر و یک پاسخ دهنده دارند، مفید است.

اتصال سست میان مشتری و سرویس، و جدایی واضح خط اتصال از پیاده سازی، شانس های قابلیت همکاری بین اشیاء در آینده را افزایش می دهد.

### B. مدیریت هویت

رمزنگاری ساده است اما مدیریت کلمه ی عبور سخت است. اکثر مکانیزم های امنیتی به برخی الگوریتم های رمزی متکی هستند، و همه ی آنها از مواد کلمه ی عبور گذاری که باید به طور ایمن در بخش ها مستقر شوند، استفاده می کنند. مدیریت کلمه ی عبور شامل تولید، گسترش، به روز رسانی و برداشت کلمه ی عبور وکمک به کلمه ی عبور ها توسط هویت ها به روشی که بتواند توسط هر کسی تایید شود، می شود . همچنین مدیریت هویت، ویژگی مدیریت را به شکل مشخصاتی که به روشی معتبر، به صورتی ایمن به هویتی مقید هستند ارائه می کند.

برای عملیات مقیاس بزرگ IOT، سرویس های مدیریت هویت سبک و موثر، ضروری هستند. به عنوان مثال، ممکن است که ارتباط گسترده با سرورهای مرکزی، مانع باشند و ممکن است که دسترسی پذیری کتابخانه های برنامه نویسی رمزنگاری محدود شود.

مشارکت این مقاله براساس یک سیستم مدیریت هویت موجود که در ذهن با سیستم های موبایل در ذهن توسعه یافته و برای گوشی های هوشمند انروید کاملا قابل انتقال می باشد، است. بنا به دانش نویسنده، تعداد بسیار کمی از محصول های گران IdMs ( روش احراز هویت، عملیات حوزه ی متقابل و غیره) چنین سطحی از احتمال را ارائه می کنند. این موضوع همچنین با تغییرات ارائه شده می تواند شامل واحد های سبک وزن مانند آنهایی که در یک IOT یافت می شوند، شود.

## 3. احراز هویت و اینترنت اشیاء

معنی مرسوم دنیای احراز هویت "استقرار هویت"است. این اتفاق وقتی که انسان ها هدف عملیات هستند: اطمینانی از این که عملگر سیستم یک فرد است و در غیر اینصورت وفادار و شایسته شناسایی شده است، بسیار منطقی به نظر می رسد. به فرد رمز عبوری یا سخت افزاری به عنوان نشانه برای کمک به احراز هویت برای احراز هویت داده شده است، و احراز هویت اگر این موارد گم شوند و یا کشف رمز رخ دهد ممکن است که غلط باشد.

وقتی که سرویسی احراز می شود، ما به هویت کامپیوتر سرویس علاقه مند نیستیم اما برای خود سرویس، بدون در نظر گرفتن اینکه اگر سرور بر روی یک کامپیوتر، یک گروه کامپیوتر یا ابر عمومی اجرا می شود، علاقه مندیم. سازمانی که این کامپیوتر ها را فعال می کند، اطمینان می دهد که تنها سرویس داده شده می تواند اعتبارنامه ی مورد نیاز در هنگام احراز هویت را ارائه کند و ابنکه آنها همچنین تمامیت عملیات را تضمین می کنند.

مشترک این دو نوع، اطمینان از عملیات "واجد شرایط" است که که بخش ها همدیگر را گمراه نمی کنند. یک سرویس و یا مشتری که توسط نرم افزارهای مخرب و غیره، در معرض خطر قرار گرفته، از طریق عملیات احراز هویت معمولی یافته نخواهد شد.

### A. احراز هویت ضدرشوه

یک عملیات احراز هویت یک فرد ممکن است که اگر نشانه دزدیه و یا گم شود،یا اگر رمز عبور برای دیگران فاش شود (داوطلبانه یا به زور)، برانداخته شود. این ریسک، نیاز برای باطل سازی نشانه را ایجاد می کند، برای مثال اینکه نشانه ها غیر معتبر فرض شده و بلا استفاده تولید شده. از تحقیق بر روی زیرساخت کلمه ی عبور عمومی (PKI) می دانیم که مکانیزم لغو در حالت مقیاس پذیر، گران و مشکل برای اجرا کردن است.

از سوی دیگر، احراز هویت برای اشیاء ممکن است که در هنگام فرایند تولید ضد رشوه تولید شوند. نشانه ها ممکن است که در دستگاه های سخت افزار ذخیره شوند و اگر جدا شده اند، در چنین شرایطی که نشانه یا شیء از بین رفته است، قرنطینه شوند . پس به منظور احراز هویت یک ساعت رولکس تقلبی، ساعت اصلی باید نابود شود که مدل تجارتی قابل دوام برای مجرمین نیست. تمامیت یک کانتینر وسایل یا یک جعبه ی کامپیوتر ممکن است که توسط یک نشانه ی احراز هویت مهر و موم شود به طوریکه اگر کانتینر باز شود، نشانه نابود شده باشد.

در مفاد سیستم مدیریت هویت، وجود یک مکانیزم احراز هویت ضدرشوه می تواند برخی هزینه های مرتبط به لغو نشانه ها را کم کند. اینکه عملیات احراز هویت بر مبنای مکانیزم ضد رشوه می تواند با تضمین کمتر تایید اعتبار شود و اینکه تمثال لغو مواد کلمه ی عبور گذاری می تواند کمتر ارزیابی شود، فرضی منطقی است. این مبحث در زمانی که ظرفیت شبکه سازی مورد نیاز در نزدیکی اشیاء برنامه ریزی شده است، مهم می شود.

### B. مدیریت هویت بدون لیست های ابطال

IdM عملی که در (4) و (5) تشریح شد، براساس این فرضیه که اعتبارنامه ها نباید مضمون ابطال باشد اما بلکه مکررا با طول عمر کوتاه خارج شود، ساخته شده است(6). در حال حاضر این مورد نه تنها به داخل کردن اعتبار سنجی هویت بلکه همچنین به تمامیت سرویس گسترش یافته است. مفهومی که بعدا در مقاله تشریح خواهد شد.

### 4. اطمینان از طریق گواهی اصالت

احراز هویت از این فرضیه که یک تبادل براساس توقعات و توافقات و در سبکی "اصیل" اتفاق می افتد، پشتیبانی می کند. پیزی که مشتری هم نیاز دارد، اطمینان از تمامیت سرویس است، برای مثال اینکه از بدافزار یا دیگر تغییرات متخاصم، مبرا است.

چندین رویکرد برای پشتیبانی از تمامیت سرویس وجود دارد رویکرد مرسوم، به کار بردن سیستمی در حال کار با جدایی صلب میان فرایند ها به طوریکه بدافزار در یک فرایند نتواند بر روی دیگر فرایندها اثر بگذارد، است. این جدایی اموال درسیستم هایی فعال امنیتی چند سطحی (MLS) یافت می شود اما هنوز نیازمند نرم افزار نگهداری پیچیده برای جلوگیری از آسیب پذیری در اجرای کد، در فرایند های خاص هستند. در ضمن، سیستم های MLS کم،گران و در مقایسه با نرم افزار COTS نامناسب است.

فرایندی متفاوت که تنها تحت شرایطی خاص عملی می باشد، مهر و موم کردن پیکربندی با مقداری درهم که به طور امنی در مخزنی خارجی ذخیره شده است، می باشد. در طول عملیات مقدار درهم تولید و با مقدار "استریل" به منظور یافتن هر گونه آلودگی، مقایسه می شود. تولید و کنترل کردن وقدار درهم باید غیر قابل کنارگذاشتن، ضدرشوه، محافظت شده از حملات مکرر و به صورت مستقل تصدیق شده، باشد.

یک کنترل موفق تمامیت باید توسط قسمت سومی که در داخل یک IdM که "فراهم کننده ی هویت" (IdP) نامیده می شود، تایید شود. یک IdP اعتبارنامه ها برای احراز هویت و کنترل دسترسی را عنوان می کند و ممکن است که همچنین مقدار درهم معتبر شده ی داده شده از دستگاه کنترل تمامیت را تایید کند. مشتری چنین سرویسی باید قادر به اعتبار سنجی گواهی قبل از قبول پاسخ سرویس باشد.

### A. مدول پلتفرم مورد اعتماد

محدوده ی واحد های سخت افزار برای احراز هویت و کنترل تمامیت ممکن است که برای این کاربرد در نظر گرفته شود. واحدهای ساده که برای چالش های بنیادی وجود دارند به احراز هویت های موجود پاسخ می دهند، آنها یا از

کلمه های عبور متقارن یا کلمه های عبور نامتقارن استفاده می کنند. برای سخت افزار کنترل کمک تمامیت، تناه واحد شناخته شده برای نویسنده مدول پلتفرم مورد اعتماد (TPM) است که توسط کنسرسیوم گروه محاسبه ی مورد اعتماد طراحی شده است(۷). یک TPM پردازنده ی رمزی قادر به اجرای عملیات های متنوع ذخیره ی کلمه ی عبور ، عملیات های رمزی و کنترل کردن پیکربندی است. در حالیکه فضا، اجازه ی تعریفی با جزییات از عملیات های TPM را نمی دهد، کفایت می کند تا بگوییم که به خوبی با یک سیستم مدیریت هویت به منظور تایید یک پیکربندی معتبر همکاری می کند، اما اثربخشی مکانیزم متکی به همکاری کاملا با جزییات با سیستم در حال کار است. جزییات بیشتر در (8) یافته می شود.

**B. واحدهای محافظت ساده**

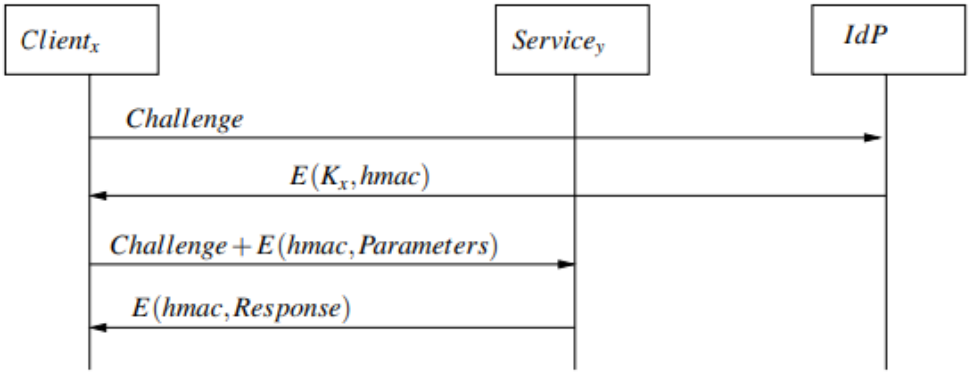
در حالیکه TPM دستگاهی برای PC ها است، ممکن است فراهم کننده های سرویس کار شده ی باتری و چیپ، دستگاهی ساده تر با هزینه و مصرفی مناسب را ترجیح دهند. این دستگاه ها ممکن است با یک مکانیزم پاسخ-چالش ساده که شامل تابع HMAC بر روی کلمه ی عبور سری، می شود، و یک واحد حفاظت تمامیت که از تنظیم مجدد بردار پردازنده جلوگیری کند، کار کنند، حافظه را برای تابع درهم کردن اسکن کنند و شامل مقدار درهم به عنوان بخشی از پارامترهای تابع HMAC شوند.

$$hmac = f(K, h(mem), challenge) \qquad (1)$$

تابع درهم ریختن h برای هر بار احضار f ارزیابی نمی شود، بلکه در هنگام خود راه اندازی و بعدا در هنگام احساس ضرورت ترزیابی می شود. نتیجه برای استفاده به عنوان پارامتری در تابع f دریافت شده است. امری ضروری است که کلمه ی عبور سری K هیچوقت در هیچ عملیاتی به غیر از f که h (mem) همیشه یک پارامتر است، استفاده نشود. پارامتر چالش، عرضه-مشتری است.

قرارداد نشان داده شده در معادله ی 1، سخت افزار واحد ضدرشوه را برای اطمینان از اینکه پاسخ hmac از یک چالش، وابسته به مقدار حافظه است، و اینکه اعتبارسنجی مقدار، درستی کلمه ی عبور سری را همانند مقدار حافظه تضمین می کند. طراحی پردازش گر باید اجرای موقعیت های حافظه ی پوشیده نشده با تابع h را منع کند.

احراز هویت بر مبنای HMAC ، ترافیک پاسخ متعاقب از حمله ی یک من در میدان را تضمین نمی کند اما تابع HMAC ممکن است که برای ایجاد کردن یک راز مشترک میان مشتری و سرویس که بتواند برای رمزنگاری پیغام به منظور حل آن مشکل مورد استفاده قرار گیرد. بخش بعدی پروتوکل را که از طریق یک بخش سوم مورد اعتماد (یک فراهم کننده ی هویت) که می تواند کلمه های عبور و اطلاعات هویتی را مدیریت کند و با واحد سخت افزار برای تصدیق اصالت سرویس همکاری کند، تشریح می کند.




شکل 1: پروتوکل حفاظت از اصالت بر مبنای کلمه های عبور رمزی متقارن و تابع HMAC داده شده در معادله ی12

**C. پروتوکل ها برای تایید اصالت**

۱) کلمه های عبور متقارن: نشان داده خواهد شد که چطور تابع HMAC ضد رشوه که در بخش IV-B توصیف شد می تواند پروتوکلی که به مشتری جهت اعتماد به اصالت سرویس اجازه می دهد را پشتیبانی کند. پروتوکل این مشخصات را خواهد داشت:

• تنها فراهم کننده ی هویت (IdP) کلمه ی عبور سری و مقدار درهم حافظه ی معتبر سرویس را می داند.

• هیچ اتصالی بین سرویس و IdP لازم نیست.

• کنترل اصالت و احضار سرویس در همان پروتوکل رفت و برگشتی جهت ذخیره ی منابع شبکه ای اتفاق می افتد.

• مشتری و سرویس به کتابخانه های نرم افزاری برای عملیات رمزی متقارن نیاز دارند.

شکل ۱ تعاملات این پروتوکل را نشان می دهد. فرض می شود که تابع در معادله ی ۱ و کلمه ی عبور سری Ky در IdP و سرویس ها دسترسی پذیر هستند.همچنین وجود عملیات های رمزی C=E(K,P) . و P=D(K,C) فرض می شود. به یاد داشته باشید که مقدار hamc به سرویس انتقال پیدا نمی کند بلکه در سرویس محاسبه می شود و به عنوان کلمه ی عبور برای انتقال پیام بعدی استفاده می شود. مشتری مقدار hamc که از IdP فرستاده شده و با کلمه ی عبور سری اش E(Kx,hmac) رمزگشایی شده را نیاز دارد. پارامتر ها برای درخواست سرویس شامل چالش در حالت رمزنگاری شده است و سرویس تنها قادر به رمزگشایی ان با یک کلمه ی عبور سری صحیح و مقدار H(mem) صحیح می باشد.

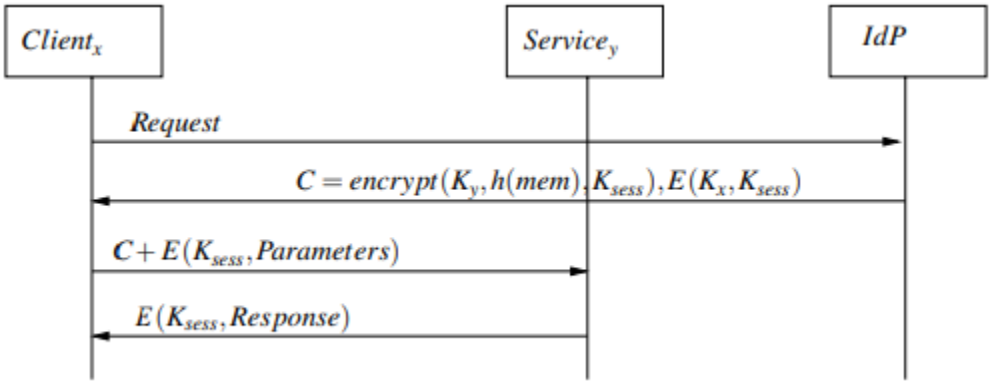
وجود کلمه ی عبور سری مشتری Kx نشان می دهد که مشتری باید خودش را برای IdP معرفی کند و IdP می تواند از کنترل دسترسی جهت تصمیم گیری بر اینکه آیا عملیات ها باید کامل شوند، استفاده کند. همچنین IdP می تواند از حدود وسط برای تشخیص درخواست های تکرار شده به عنوان حمله ی متن انتخاب شده بر روی تابع HMAC استفاده کند.

2) کلمه های عبور نامتقارن: به عنوان یک جایگزین، یک واحد سخت افزاری می تواند برای اداره ی عملیاتها بر روی کلمه های عبور نامتقارن سیم کشی شود، چیزی که مدیریت کلمه ی عبور امن تر و ساده تری ایجاد می کند. سخت افزار یک تابع رمزگشایی مرتبط به معادله ی 1 در حالت پیش رو ارائه می دهد:

$$K_{sess} = decrypt(K'_y, h(mem), C) \qquad (2)$$

که در آن

$$C = encrypt(K_y, h(mem), K_{sess}) \qquad (3)$$




شکل 2: پروتوکل حفاظت از اصالت بر مبنای کلمه های عبور رمزی متقارن و تابع رمزگشایی داده شده در معادله ی 2

و $(K'_y, K_y)$ جفت کلمه ی عبور متعلق به سرویس y هستند، و Ksess یک کلمه ی عبور دوره ای که توسط IdP انتخاب شده است. مشتری کلمه ی عبور دوره ای که توسط یکی از کلمه های عبور متقارن یا نامتقارنش رمزنگاری شده را دریافت می کند که به این برنامه ی متقارن اجازه می دهد تا بدون در نظر گرفتن توانایی های مشتری به کار گرفته شود.

تنها راهی که سرویس می تواند کلمه ی عبور دوره ای را بازیابی کند، به کار بردن تابع رمزگشایی با مواد کلمه ی عبور گذاری صحیح و محتوای حافظه ی صحیح است. اگر عملیات شکست بخورد، سرویس قادر به مشارکت در ارتباط بعدی با مشتری نیست. ممکن است که این موضوع به عنوان خروجی غیرمرسوم برای یک احراز هویت شکست خورده به نظر برسد اما این موضوع عملیات اضافی رفت و برگشت پروتوکل را حذف می کند که منابع را حفظ و زمان را ذخیره می کند. شکل 2 جزئیات دوره ای پیام را فراهم می کند.

مزیت اصلی برای برنامه ی متقارن این است که هیچ کلمه ی عبور سری برای ذخیره شدن در IdP مورد نیاز نیست. این موضوع به حفاظت راحت تر برای نقاط انتهایی سرویس Idp همانند عملیات IdP متقابل که در آن مشتری و سرویس متکی به نمونه های مختلف IdP هستند، اجازه می دهد.

### D. کنترل دسترسی

دسترسی مشتری به سرویس باید تابع کنترل دسترسی باشد. سرویس می تواند کنترل دسترسی خودش را انجام دهد که نیازمند دسترسی مکرر به یک IdP برای تایید اعتبارنامه است. انتخاب این مقاله واگذار کردن کنترل به IdP بوده است که می تواند تصمیمات لازم را بر مبنای اطلاعات هویتی که در IdP (یا از دیگر منابع مورد اعتماد مطرح شده) نگهداری شده اند بگیرد. مشتری که دسترسی برایش رد شده، اطلاعات مورد نیاز برای فراخوانی سرویس را دریافت نخواهد کرد.

در ابعاد بزرگ، اجتماع چند حوزه ای، کنترل دسترسی باید براساس نقش باشد (RBAC). روش RBAC با اجازه دادن به "کنترل اکثریت" گروه های کاربر و همجنین در راستای حوزه های مدیریت، مزایا را به نقش ها و نقش ها را به هویت ها مرتبط می کند.

## 5. تحقیق مرتبط

تحقیق مرتبط شامل کارهایی توسط گیلبرت و دیگران (9) و سارو و دیگران (10) می شود، که هر دو سعی بر حفاظت از تمامیت خواندن سنسورها از طریق یک مکانیزم امضاکردن ضدرشوه ی وابسته به یک TPM داشتند. این نویسنده اعتقاد دارد که حفاظت از تمام نقاط سنسوری مورد نیاز است. یک سنسور "محافظت شده" میتواند مقادیر خواندن سنسور را تضمین کند اما به موقع بودنش را نمی تواند و حفاظت در برابر حمله های تکرار شده بدون اعتماد به پشتوانه ی ارتباط سرویس، عملی نیست. همچنین مقاله ها نادیده گرفتن پیچیدگی توزیع کلمه ی عبور در یک شبکه با تعداد زیادی گره را ذکر کرده اند. مشارکت ماف لزوم سیستم مقیاس پذیر برای هویت و مدیریت کلمه ی عبور را پی ریزی می کند.

## 6. نتایج

تدارک احراز هویت کافی و سرویس مدیریت هویت در یم اجتماع واحدهای سبک وزن هدف این مقاله ی موقعیت بوده است. این کنترل اهراز هویت و تمامیت سرویس ترکیب شده، توسط یک واحد سخت افزار ساده و عملیات های رمزنگاری ساده ارائه شده اند.

محدودیت رویکرد، نگاه ایستا ی حافظه ی برنامه در سرویس است. این رویکرد در سیستم های حافظه ی مجازی که کد برنامه بر روی موقعیت های فیزیکی تصادفی قرار داده شده اند و کتابخانه های برنامه بر اساس تقاضا بر روی حافظه بارگذاری شده اند، کمتر قابل استفاده خواهد بود. در این موارد یک OS پیچیده تر به برنامه خدمت می کند و واحد سخت افزار TPM انتخاب بهتری خواهد بود.

### References


[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] L. Tan and N. Wang, "Future internet: The internet of things," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 5, aug. 2010, pp. V5–376 –V5–380.

[3] A. Fongen, "Federated identity management for android," in *SECURWARE 2011*. Nice, France: IARIA, July 2011.

[4] ——, "Identity management without revocation," in *SECURWARE 2010*. Mestre, Italy: IARIA, July 2010.

[5] ——, "Architecture patterns for a ubiquitous identity management system," in *ICONS 2011*. Saint Maartens: IARIA, Jan. 2011.

[6] ——, "Optimization of a public key infrastructure," in *MILCOM 2011*. Baltimore, MD: IEEE/MILCOM, Nov 2011.

[7] Trusted Computing Group, "TPM Main Specification," http://www.trustedcomputinggroup.org/resources/tpm_main_specification, online, Accessed Mars 2012.

[8] A. Fongen and F. Mancini, "Identity management and integrity protection in publish-subscribe systems," in *Under review for MILCOM 2012*. Orlando, FL, USA: IEEE/MILCOM, Oct 2012.

[9] P. Gilbert, L. P. Cox, J. Jung, and D. Wetherall, "Toward trustworthy mobile sensing," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, ser. HotMobile '10. ACM, 2010, pp. 31–36.

[10] S. Saroiu and A. Wolman, "I am a sensor, and i approve this message," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, ser. HotMobile '10. ACM, 2010, pp. 37–42.