چارچوب امنیت هوشمند برای دستگاه های اینترنت مبتنی بر اشیا

معماری امنیتی انتها-به-انتها بر پایه رمزنگاری

چکیده

اینترنت مبتنی اشیا با لینک کردن دستگاه های سکوهای مختلف ، خدمات ارائه می دهد. اینترنت اشیا محدودیت هایی در ارائه خدمات هوشمند دارد. دستگاه های اینترنت مبتنی بر اشیا ناهمگون هستند که حس گرهای بی سیم تا دستگاه هایی با محدودیت منبعی کمتر، را شامل می‌شود. این دستگاه ها در معرض حمله های نرم افزاری/سخت افزاری و شبکه قرار دارند. در صورت عدم امنیت متناسب، ممکن است مسائل امنیتی مانند حریم خصوصی و قابلیت اعتماد مطرح شود. برای حل مسئله ذکر شده، در این مقاله یک چارچوب امنیت هوشمند برای دستگاه های اینترنت مبتنی بر اشیا پیشنهاد شده است. روش پیشنهادی از 1) رمزنگاری نامتقارن سبک وزن برای تامین امنیت دستگاه های انتها به انتها که از درگاه خدمات اینترنت مبتنی بر اشیا و گره های حس گر دارای قدرت کم محافظت می کند، تشکیل شده و 2) از رمزنگاری شبکه بنیان برای تامین امنیت درگاه/دستگاه های کارگزار و خدمات ابر استفاده می کند. معماری پیشنهادی از رمزنگاری کلید نامتقارن برای به اشتراک گذاشتن کلید جلسه بین گره ها استفاده می کند و سپس این کلید جلسه را برای انتقال پیام استفاده می کند. این امر سبب محافظت سیستم از حملات انکار سرویس توزیع شده، حملات استراق سمع و حملات الگوریتم کوانتمی جلوگیری می کند. پروتکل پیشنهادی از شناسه دستگاه منحصربفرد حس گرها برای تعمیم جفت کلید جهت احراز هویت متقابل بین دستگاه ها و خدمات استفاده می کند. در نهایت، سازو کار احراز هویت متقابل در درگاه، بکار رفت.

کلید واژه ها: امنیت اینترنت مبتنی بر اشیا، اینترنت مبتنی بر اشیا، رمزنگاری، حمله کوانتوم، احراز هویت، رمزنگاری نامتقارن، رمزنگاری متقارن، رمزنگاری، حملات انکار سرویس توزیع شده

مقدمه

در (3) یک چارچوب امنیتی اینترنت مبتنی بر اشیا برای تضمین امنیت انتها به انتها از یک برنامه اینترنت مبتنی بر اشیا به دستگاه های اینترنت مبتنی بر اشیا، پیشنهاد شده است. ترکیب محاسبات ابر و اینترنت مبتنی بر اشیا، دستگاه های حس

گر همه جا حاضر و پردازش قدرتمندانه جریان داده حس گر را ممکن می سازد (13). اینترنت مبتنی بر اشیا معمولا یک معماری سه لایه متشکل از درک (حس دامنه دستگاه)، شبکه (دامنه شبکه) و لایه های برنامه (دامنه ابر) دارد. هر لایه اینترنت مبتنی بر اشیا در معرض تهدیدها و حملات فعال و منفعل از منبع بیرونی یا شبکه داخلی، قراردارد. اینترنت مبتنی بر اشیا از یک ساختار متمرکز به سمت شبکه پیچیده ای از دستگاه های هوشمند متمرکز زدایی شده حرکت می کند. در (12) و (14)، دستگاه ها و خدمات اینترنت مبتنی بر اشیا در معرض حملات انکار سرویس توزیع شده قراردارند. تبانی استراق سمع کننده ها یکی از تهدیدهای مهم نسبت به امنیت ارتباط بیسیم است. امنیت باید در کل چرخه زندگی دستگاه از اولین طراحی تا محیط اجرایی در نظر گرفته شود. چالشهای جدی ای که راه حل های اینترنت اشیا با آن مواجه هستند به چگونگی کسب بیت بیشتر از طول عمر باتری برای راه حل های نوآورانه اینترنت مبتنی بر اشیا و محدودیت های نیرو در ارتباط مربوط می شود. اولا، چارچوب امنیت هوشمند برای امنیت انتها به انتها را پیشنهاد می کنیم (16). دوما، مروری بر روش رمزنگاری مربوطه انجام می شود.

الف. رمزنگاری کلید متقارن و نامتقارن

سیستم های رمزنگاری نامتقارن مخارج کلی بالایی دارند، نمی توانند امنیت تمام وقت و واقعی را فراهم کنند. در طول روند آشنایی اولیه کلید عمومی برای رمزنگاری و کلید خصوصی برای رمزگشایی استفاده می شود که به دو طرف اجازه می دهد تا با اعتماد یک کلید مشترک جدید را تنظیم و تبادل کنند. کلیدهای مشترک برای ارتباط امن استفاده می شوند و برای جلسه کنونی ارتباط ارزشمند هستند. این کار گره اینترنت مبتنی بر اشیا و هزینه کلی انتقال کلید درگاه دستگاه ها را کاهش می دهد.

ادامه مطالب مقاله به این صورت ارائه می شود. در بخش 2 مطالعات انجام شده در پیشینه مطالعاتی مرور می شود. بخش سوم به پروتکل پیشنهادی و مشخصات آن می پردازد. بخش چهارم نتیجه گیری است.

مروری بر مطالعات پیشین

ارتباط و اتصال درونی انواع مختلف دستگاه های اینترنت مبتنی بر اشیا و ناهمگونی منجر به تهدید داده ها می شود. در این پژوهش، امنیت اینترنت مبتنی بر اشیا و پروتکل های احراز هویت مربوطه را بطور کلی با آسیب پذیری های آنان نسبت به حملات در طول مسیریابی، بررسی می کنیم.

ب. پروتکل ثبت کارگزار اینترنت مبتنی بر اشیا (1)

در (1)، سکوی خدمات معمول اینترنت مبتنی بر اشیا هوشمند و ثبت کارگزار اینترنت مبتنی بر اشیا را پیشنهاد کرده اند. در این مدل، کارگزار اینترنت مبتنی بر اشیا، دستگاه های جدید را با استفاده از مدل دستگاه، محل و آدرس IP آن ثبت می کند. بعد از ایجاد هدف دستگاه، در مدل داده های عمومی که یک پایگاه داده است، ثبت می شود. مدیریت دستگاه درخواستی را برای مجوز دستگاه به تابع مجوز در چارچوب امنیت می فرستد. تابع مجوز نشانه دستگاه را ایجاد کرده و آن را به مدیریت دستگاه می فرستد و به این ترتیب ثبت کامل می شود.

ج. پروتکل مسیریابی و مشخصات امنیتی آن (2)

در این مقاله، پروتکل های مسیریابی مختلف و تهدید نسبت به آنها دسته بندی شده است. پروتکل ها بر اساس مدیریت کلید، رمزنگاری و چارچوب های مدیریت اعتماد امن اینترنت مبتنی بر اشیا دسته بندی شده اند تا امنیت انتها به انتها تضمین شود.

د. پروتکل مبتنی بر امنیت انتها به انتها (3)

در این مقاله، محیط امن را با استفاده از دستگاه اینترنت مبتنی بر اشیا، کارگزار اینترنت مبتنی بر اشیا و برنامه اینترنت مبتنی بر اشیا پیشنهاد کرده اند. پروتکل برنامه های محدود شده [1]و پروتکل های انتقال صف پیام تله متری[2] برای ایجاد ارتباط بین کارگزار اینترنت مبتنی بر اشیا و دستگاه های اینترنت مبتنی بر اشیا استفاده شده است. استاندارد رمزنگاری پیشرفته[3] و رمزنگاری مبتنی بر مشخصه[4] برای ایجاد متن صفر استفاده شده اند.

ه. مدیریت و حذف تکرار در محاسبات ابر (4)

در این مقاله، رمزنگاری مبتنی بر مشخصه برای حذف تکرار داده های رمزنگاری شده ذخیره شده و کنترل دسترسی امن به داده ها پیشنهاد شده است. شناسه کاربران داده برای ایجاد کلید عمومی استفاده می شوند. کلید تعمیم یافته برای احراز هویت دستگاه برای کارگزار اینترنت مبتنی بر اشیا استفاده می شود.

و. پروتکل مبتنی بر تکرار ماشین مجازی

در این مقاله، استفاده از تکرار ماشین مجازی برای بهبود قابلیت بقا برنامه های ماموریت بحرانی در سیستم های ابر از طریق یک رویکرد تکرار ماشین مجازی چندسطحی، پیشنهاد شده است.

ز. پروتکل تبادل کلید بر مبنای شخص ثالث معتمد (6)

در این مقاله، استفاده از شخص ثالث معتمد را برای تعمیم کلید پیشنهاد شده است. این پروتکل 40 جلسه کلید را بطور همزمان ایجاد می کند. در مقابل حمله های کلید شناخته شده، جعل هویت، بازپخش، استراق سمع و جعل مقاوم است.

ح. پروتکل تبادل کلید ماشین به ماشین (7)

در این مقاله، ماشین به ماشین و تهدیدهایی که ارتباط ماشین به ماشین باید با آنها مقابله کند، بررسی شده است.

ط. مقدمه آموزشی (8)

[1] Constrained Application Protocol (CoAP)
[2] Message Queue Telemetry Transport (MQTT) Protocols
[3] Advanced Encryption Standard (AES)
[4] Attribute-Based Encryption (ABE)

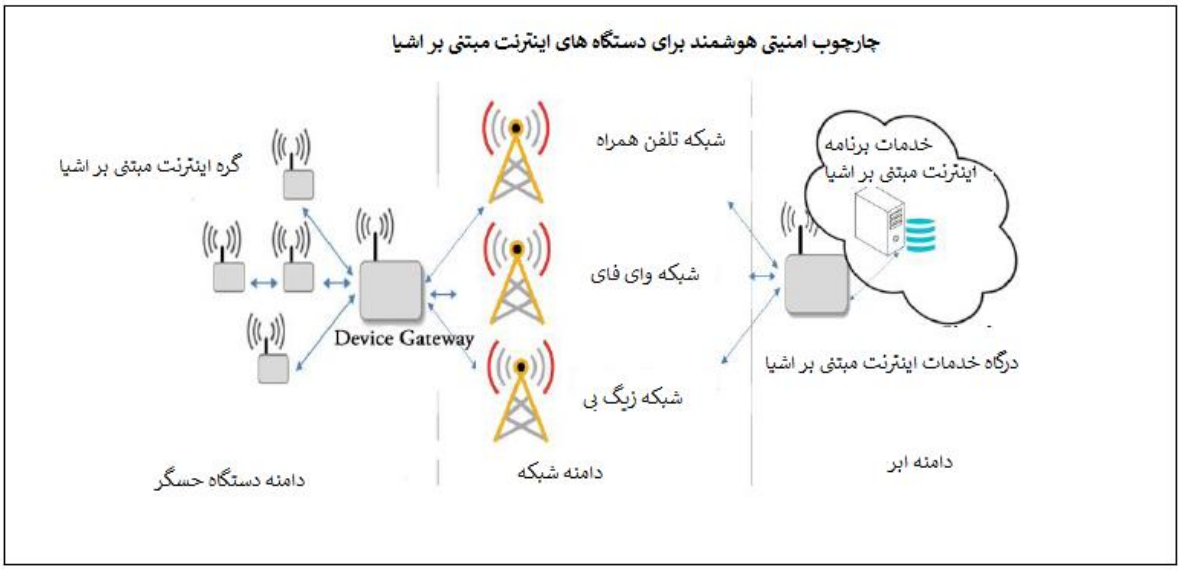
در این مقاله، یک مقدمه آموزشی برای اکوسیستم اینترنت مبتنی بر اشیا ارائه شده است. دو چالش ویژه پژوهشی در اینترنت مبتنی بر اشیا، امنیت و کارایی انرژی، عمیقا بررسی شده است.

ی. پروتکل تبادل کلید بر مبنای شخص ثالث مورد اعتماد

در این مقاله، مجموعه ای از آزمونهای یکپارچه در تمام دستگاه های اینترنت مبتنی بر اشیا همیشه روشن انجام شده و نتایج در چهار حوزه سازماندهی شده اند: خدمات ابر در مواجه با کاربر، رابط برنامه های تلفن همراه، خدمات ابر پشتیبان انتها، و رابط های اشکال زدایی دستگاه.

ک. پروتکل تبادل کلید بر مبنای شخص ثالث مورد اعتماد (11)

در این مقاله، به ملاحظات امنیتی از اینترنت مبتنی بر اشیا از دیدگاه کاربران نهایی، کاربران ابر، و تامین کنندگان ابر، که در بازه ای از فناوریهای اینترنت اشیا فعال هستند توجه شده است.



شکل 1. چارچوب امنیت هوشمند برای دستگاه های اینترنت مبتنی بر اشیا

ل. حمله به سیستم های اینترنت مبتنی بر اشیا (15)

در این مقاله، به ملاحظات امنیتی، حملات و اقدامات متقابل آنها توجه شده است. حمله های فیزیکی، حملات به کانال جانبی، حمله های محیطی، حمله های تحلیل رمزگشایی، حملات نرم افزاری و حملات شبکه ای دسته بندی شده اند.

م. امنیت، حریم خصوصی و اعتماد (16)

در این مقاله، به برآورده کردن نیازهای امنیتی و حریم خصوصی توجه شده است که شامل محرمانگی و احراز هویت، کنترل دسترسی، شبکه اینترنت مبتنی بر اشیا، حریم خصوصی و اعتماد میان کاربر و اشیا، و اجرای سیاست گذاریهای امنیتی و حریم خصوصی می شود.

چارچوب امنیت هوشمند

تحلیل رمزگشایی به معنی استفاده از کدها و صفرها برای محافظت از ارتباط خصوصی است و ارتباط را از همه بجز دریافت کننده مورد نظر محفوظ نگه می دارد. اعمال توابع رمزنگاری کافی روی دستگاه های دارای محدودیت به دلیل محدودیت منابع دشوار است. این سیستم پیشنهادی از احراز هویت دو سویه دوگانه استفاده می کند.

ابتدا، تحلیل رمزنگاری کلیدی نامتقارن سبک وزن برای ارائه احراز هویت بین گره حسگر و درگاه دستگاه استفاده می شود. شناسه منحصربفرد گره حسگر و شناسه منحصربفرد درگاه دستگاه برای ایجاد تاییدیه کلیدی/دیجیتال با استفاده از الگوریتم AES استفاده می شود. سپس، درگاه دستگاه و خدمات ابر بصورت مشترک با استفاده از امضا دیجیتال رمزنگاری کلید عمومی احراز هویت می شود.

الف. رمزنگاری کلید نامتقارن

رمزنگاری سبک وزن یک الگوریتم رمزنگاری بکاربرده شده در محیط های محدود شامل تگ های RFID ، حس گرها، کارتهای هوشمند بدون تماس و غیره می شود.

میتوان از نشت اطلاعات فردی و کارهای خطرناک با استفاده از احراز هویت همسان و امن کردن انتقال داده ها جلوگیری کرد. ما یک معماری نمایندگی جدید را برای احراز هویت مبتنی بر گواهی یک سویه را معرفی کرده ایم.

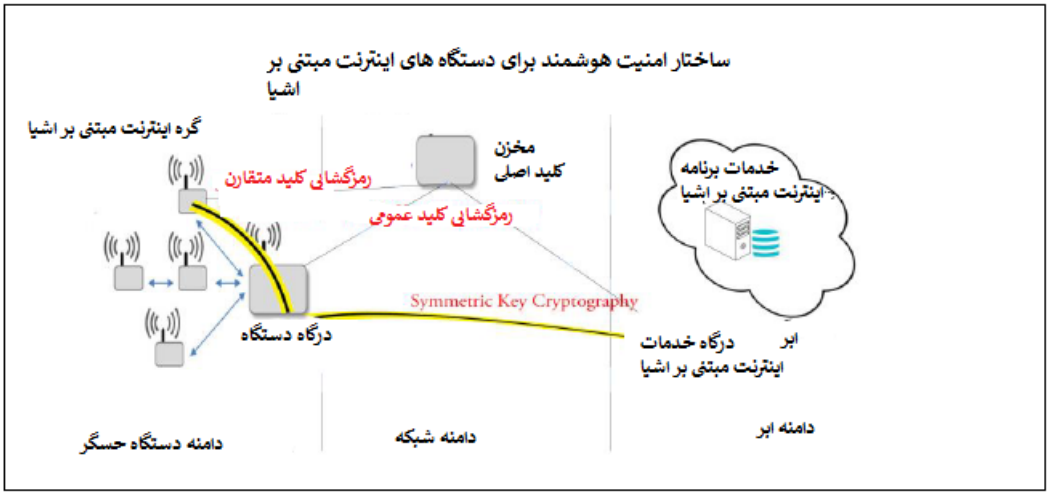
یکبار معرفی بین گره های حس گر و درگاه دستگاه با استفاده از شناسه واحد دستگاه انجام شد. پیام گره حس گر با استفاده از تاییدیه دیجیتال رمزگشایی می شود و درگاه دستگاه پیام را رمزگشایی کرده و شناسه هویت مالک را ارزیابی می کند و در صورت نقض پیام نادیده گرفته می شود.

یک الگوریتم موثر در درگاه برای محدود کردن ترافیک ناخواسته در شبکه و دستگاه های ابر بکار می رود.

ب. رمزگشایی مبتنی بر شبکه

یک کلید عمومی با استفاده از عدد اتفاقی و شناسه واحد درگاه تعمیم داده می شود. این کلید برای انتقال پیام بین ابر و درگاه استفاده می شود. شناسه واحد دستگاه های حس گر با استفاده از دیدار اولیه تسهیم می شود، هنگام ورود دستگاه جدید/تقلبی، درگاه دستگاه شناسه منحصربفرد را ارزیابی می کند و گره اطلاعات برای خدمات ابر بروزرسانی می شود.

درگاه دستگاه پیام را با استفاده از کلید عمومی خدمات ابر رمزنگاری می کند. هنگام دریافت پیام، خدمات ابر پیام را با استفاده از کلید خصوصی آن رمزگشایی کرده و شناسه منحصربفرد را در مخزن خود بررسی می کند. اگر هر نوع عدم تطابقی دیده شد، پیام نادیده گرفته می شود.



شکل 2. رمزگشایی متقارن و رمزگشایی کلید عمومی

ج. چارچوب امنیت هوشمند یک الگوریتم پیشنهادی

مرحله 1: پیش نیازها

1.1 مخزن کلید اصلی جزییات شناسه منحصربفرد گره های اینترنت مبتنی بر اشیا ،درگاه دستگاه، درگاه خدمات اینترنت مبتنی بر اشیا و خدمات ابر را حفظ می کند و جفت کلید را با استفاده از یادگیری با رمزگشایی خطا تعمیم می دهد.

کلید پنهان= $\overleftarrow{Z^n_q}$

1.2. کلید عمومی مخزن کلید اصلی از طریق تماس یکباره بین واحدهای مرتبط ایجاد می شود و تمام ارتباطات بین آنها با رمزگشایی پیام توسط کلید عمومی مخزن کلید اصلی که کسب شده/تعمیم یافته انجام می شود.

مرحله 2: تعمیم جفت کلیدهای گره های اینترنت مبتنی بر اشیا

2.1. گره اینترنت مبتنی بر اشیا مخزن کلید اصلی را به شکل آفلاین/آنلاین به اشتراک می گذارد و کلید عمومی مخزن کلید اصلی را کسب می کند.

2.2. گره اینترنت مبتنی بر اشیا شناسه منحصربفرد خود و مهر زمانی با کلید عمومی مخزن کلید اصلی را رمزگشایی می کند.

کلید عمومی مخزن کلید اصلی (شناسه واحد گره ها + زمان)

2.3. مخزن کلید اصلی شناسه واحد و مهر زمانی را ارزیابی می کند. مخزن کلید اصلی یک جفت کلید را تعمیم داده و آن را با کلید خصوصی رمزگشایی کرده ، آن را به گره اینترنت مبتنی بر اشیا ارسال کرده و کلید عمومی درگاه دستگاه را به گره اینترنت مبتنی بر اشیا می فرستد.

کلید عمومی مخزن کلید اصلی (جفت کلید گره ها)

مرحله 3: تعمیم کلید جلسه دستگاه پنهان

3.1. گره های اینترنت مبتنی بر اشیا شناسه منحصر بفرد آن و مهر زمانی را با کلید خصوصی رمزگشایی می کد و با کلید عمومی مخزن جلسه کلید اصلی دوباره رمزگشایی کرده و به مخزن کلید اصلی می فرستد.

مخزن کلید اصلی عمومی (گره های اینترنت مبتنی بر اشیا (شناسه منحصربفرد+ زمان))

3.2. مخزن ملید اصلی با کلید خصوصی خود و کلید عمومی گره اینترنت مبتنی بر اشیا رمزگشایی می کند. کلید جلسه دستگاه پنهان برای این شناسه منحصربفرد خاص و مهرزمانی تعمیم می دهد.

کلید جلسه دستگاه پنهان ← (شناسه منحصربفرد+زمان)

3.3. مخزن کلید اصلی کلید جلسه دستگاه پنهان و کلید عمومی درگاه دستگاه را با کلید خصوصی آن رمزگشایی کرده و آن را به گره اینترنت مبتنی بر اشیا می فرستد.

کلید خصوصی مخزن کلید اصلی (کلید جلسه دستگاه پنهان + درگاه دستگاه عمومی)

3.4. مخزن کلید اصلی کلید جلسه دستگاه پنهان و کلید عمومی گره های اینترنت مبتنی بر اشیا را رمزگشایی کرده و آن را به درگاه دستگاه می فرستد.

کلید خصوصی مخزن کلید اصلی (کلید جلسه دستگاه پنهان+ گره اینترنت مبتنی بر اشیا عمومی)

نکته: کلید جلسه دستگاه پنهان برای هر جلسه کسب می شود.

مرحله 4: تعمیم کلید جلسه دستگاه پنهان

4.1. درگاه دستگاه شناسه واحد خود و مهر زمان را با کلید خصوصی آن رمزگشایی کرده و با کلید عمومی مخزن کلید اصلی دوباره رمزگشایی کرده و به مخزن کلید اصلی می فرستد.

کلید عمومی مخزن کلید اصلی (کلید خصوصی درگاه دستگاه (شناسه واحد+ زمان))

4.2. مخزن کلید اصلی با کلید خصوصی آن و با کلید عمومی درگاه دستگاه رمزگشایی می کند. کلید جلسه خدمات پنهان برای این شناسه منحصربفرد و مهر زمانی خاص تعمیم پیدا می کند.

کلید جلسه خدمات پنهان (شناسه منحصربفرد+زمان)

4.3. مخزن کلید اصلی ؛ کلید جلسه خدمات پنهان و کلید عمومی درگاه خدمات اینترنت مبتنی بر اشیا را با کلید خصوصی آن رمزگشایی کرده و به درگاه دستگاه میفرستد.

کلید خصوصی مخزن کلید اصلی (کلید جلسه خدمات پنهان + درگاه خدمات اینترنت مبتنی بر اشیا عمومی)

4.4. مخزن کلید اصلی ، کلید جلسه خدمات پنهان و کلید عمومی درگاه دستگاه را با کلید خصوصی خود رمزگشایی کرده و آنر ا به درگاه خدمات اینترنت مبتنی بر اشیا میفرستد.

کلید خصوصی مخزن کلید اصلی (کلید جلسه خدمات پنهان+ درگاه دستگاه عمومی)

نکته: کلید جلسه خدمات پنهان برای هر جلسه کسب می شود.

مرحله 5: انتقال داده از گره های اینترنت مبتنی بر خدمات و درگاه دستگاه پس از کسب کلید جلسه دستگاه پنهان

5.1. گره پیام و مهر زمانی را با استفاده از کلید جلسه دستگاه پنهان رمزگشایی می کند

کلید جلسه دستگاه پنهان (زمان + پیام)

5.2. درگاه گره پیام را با استفاده از جلید جلسه دستگاه پنهان رمزگشایی کرده و سپس مهرزمانی را بررسی می کند.

5.3. پیام بعد از تایید کلید جلسه بازیابی می شود و دستورالعمل محلی بروزرسانی می شود.

نکته:

اگر کلید جلسه دستگاه پنهان ارائه نشود (بعد از دریافت درخواست های متعدد از یک گره) در درگاه دستگاه، جلسه ای را با مخزن کلید اصلی ایجاد کرده و کلید عمومی گره را می فرستد. مخزن کلید اصلی مجددا برای بررسی شناسه منحصربفرد تایید می کند، اگر بروزرسانی شده باشد، کلید عمومی و کلید جلسه خدمات پنهان گره به درگاه دستگاه بروزرسانی می شود ، در غیر اینصورت اعلامیه نادیده گرفتن پیام القا شده و بسته می افتد.

مرحله 6: انتقال داده از درگاه دستگاه و درگاه خدمات اینترنت مبتنی بر اشیا بعد از کلید جلسه خدمات پنهان

6.1 پیام درگاه دستگاه و مهر زمانی با استفاده از کلید جلسه خدمات پنهان

کلید جلسه خدمات پنهان (زمان +پیام)

6.2. درگاه خدمات اینترنت مبتنی بر اشیا پیام را با استفاده از کلید جلسه خدمات پنهان رمزگشایی کرده و سپس مهر زمانی را بررسی می کند.

6.3. پیام بعد از تایید کلید جلسه بازیابی کرده و دستورالعمل های محلی بروزرسانی می شوند.

نکته:

اگر کلید جلسه خدمات (بعد از دریافت درخواست های متعدد از یک گره) به درگاه خدمات اینترنت مبتنی بر اشیا ارائه نشود، جلسه ای را با مخزن کلید اصلی ایجاد کرده و کلید عمومی درگاه دستگاه را می فرستاد. مخزن کلید اصلی مجددا ارزیابی می شود تا شناسه منحصربفرد بررسی شود، اگر بروزرسانی شده بود، کلید عمومی و کلید جلسه خدمات پنهان درگاه دستگاه به درگاه خدمات اینترنت مبتنی بر اشیا بروزرسانی می شود و در غیر اینصورت اعلام نادیده گرفتن پیام القا شده و بسته می افتد.

مرحله 7: تبادل امن انتها به انتها

7.1. گره پیام و کلید جلسه دستگاه مرموز را فرستاده و دوباره آن را با استفاده از کلید خصوصی و کلید عمومی درگاه دستگاه رمزگشایی می کند.

درگاه دستگاه عمومی (کلید خصوصی گره اینترنت اشیا (کلید جلسه دستگاه پنهان))

7.2. درگاه دستگاه پیام را با استفاده از کلید خصوصی آن رمزگشایی کرده و سپس با کلید عمومی گره ها رمزگشایی کرده و کلید جلسه دستگاه پنهان را ارزیابی می کند.

7.3. درگاه دستگاه کلید جلسه دستگاه پنهان را از میان برداشته و پیام را با کلید جلسه خدمات پنهان در نظر گرفته و آنر ا با کلید خصوصی رمزگشایی می کند و با کلید عمومی گرده درگاه خدمات اینترنت اشیا رمزگشایی می کند.

درگاه خدمات اینترنت مبتنی بر اشیا عمومی (درگاه دستگاه خصوصی (کلید جلسه خدمات پنهان +پیام))

7.4. درگاه خدمات اینترنت مبتنی بر اشیا پیام را با استفاده از کلید خصوصی آن رمزگشایی کرده و سپس با کلید عمومی درگاه دستگاه رمزگشایی کرده و کلید جلسه دستگاه پنهان را تایید کرده و پیام اصلی را می خواند.

نکته: اگر دم تطابقی در مهر زمانی وجود داشته باشد، بسته ها نادیده گرفته می شود.

شکل 1 و 2، معماری اصلی و سیستم های رمزگشایی را نشان می دهد. این طرح ، حمله استراق سمع، حمله مردی در میانه و حملات انکار سرویس توزیع شده، (9) را حذف می کند. رمزگشایی کلید شبکه امنیت را فراهم کرده و حملات الگوریتم کوانتوم را حذف می کند.

نتیجه گیری

در این مقاله، طرح های احراز هویت دو سویه و دوبل را پیشنهاد کردیم که ترافیک را با حذف بسته های خطا و تقلبی حذف می کند. این سیستم امنیت در مقابل حمله های کوانتوم را فراهم کرده ، عملکرد را بهبود بخشیده و مصرف پهنای باند را کاهش می دهد.