نشریه مطالعات برق آپادانا
دوره ۱، شماره ۱، زمستان ۱٤۰۲، ٤٦-٦۱
ajes.apadana.ac.ir

بررسی و تحلیل افزایش حریم امنیتی و شخصی اینترنت اشیاء به وسیلهٔ ادغام یک رابط امن بلاک‌چینی

امیر شاطری *

فارغ التحصیل مقطع کارشناسی پیوسته مهندسی برق، موسسه آموزش عالی آپادانا شیراز؛ ایران

تاریخ دریافت: ۱۴۰۲/۱۰/۰۶
تاریخ پذیرش: ۱۴۰۲/۱۱/۳۰

چکیده

در این تحقیق و مقاله، اینترنت اشیاء و بلاک‌چین دو فناوری اصلی در نظر گرفته می‌شوند. تأخیر کمتر و تعداد سیستم پیوندی بالاتر، انعطاف‌پذیری بیشتری را برای اجرای برنامه‌های اینترنت اشیا (IoT) از راه دور فراهم می‌کند. بر کسی پوشیده نیست که دستگاه‌های اینترنت اشیاء اغلب ظرفیت محاسباتی کافی (هم از نظر قدرت پردازش و هم نیازهای ذخیره‌سازی) برای پشتیبانی از الگوریتم‌های حفاظت و رمزگذاری قوی ندارند. اینترنت اشیاء با چالش‌های زیادی مانند قابلیت همکاری ضعیف، آسیب‌پذیری‌های امنیتی، حریم خصوصی و فقدان استانداردهای صنعتی مواجه است. حملات سایبری به دستگاه‌های اینترنت اشیاء می‌تواند بر حریم خصوصی و امنیت تجارت انرژی تأثیر بگذارد. این تحقیق و مقاله روشی را برای معرفی یک رابط پایه به معماری دروازهٔ امنیتی دستگاه اینترنت اشیاء همراه با بلاک‌چین برای ارائهٔ تمرکززدایی و احراز هویت پیشنهاد می‌کند. ناشناس‌بودن و تطبیق‌پذیری بسیار مورد نیاز را به زیرساخت اینترنت اشیاء اضافه می‌کند که در حال حاضر فاقد آن است. این راه‌حل، قابلیت اطمینان داده‌های ارسال‌شده به سرویس‌های راه دور را با اعمال الگوریتم های رمزنگاری سازگار قبل از ارسال، افزایش می‌دهد. مزایای این راه‌حل شامل سازگاری با همهٔ محصولات اینترنت اشیاء و توانایی اجرای هر الگوریتم رمزنگاری بر روی داده‌هایی است که می‌تواند برای تجارت ریزشبکه استفاده شود و می‌تواند به‌صورت اولیه و ایمن از طریق زیرساخت‌های شبکهٔ ۵G یا ۶G منتقل شود. به‌عنوان بخشی از این کار، یک رویهٔ امنیتی ایجاد شده است که از هر الگوریتم رمزنگاری برای همهٔ دستگاه‌های اینترنت اشیا در شبکه، پشتیبانی می‌کند. علاوه بر این، این رابط توسط فناوری بلاک‌چین محافظت می‌شود که اختیار کنترل واحد را حذف می‌کند، تراکنش‌های تاریخی انجام شده توسط دستگاه‌های اینترنت اشیاء را ثبت می‌کند و اعتماد بین دستگاه‌ها را ایجاد می‌کند.

کلیدواژه‌ها: امنیت، اینترنت اشیا، بلاک چین، دروازه امنیتی، حریم خصوصی

* نویسندهٔ مسئول: amir.sh197799@gmail.com

مقدمه

دستگاه‌های اینترنت اشیاء برای تبادل داده‌ها نیاز به اتصال دائمی به اینترنت دارند، که شبکهٔ ۵G را به انتخابی عالی از نظر تأخیر کم و سرعت پیک داده بالا، تبدیل می‌کند (Neves et al., 2017). شبکه‌های ۵G کنونی می‌توانند ۱۰۶ دستگاه را در هر کیلومتر مربع با حداکثر سرعت ۱۰ مگابیت بر ثانیه در هر کیلومتر مربع و ۱ میلی‌ثانیه تأخیر رفت و برگشت اولیه، پشتیبانی کنند. اینترنت اشیاء با استفاده از شبکه‌های سیمی و بی‌سیم به چندین رایانه و دستگاه متصل می‌شود. از نظر در دسترس بودن، این ویژگی‌های شبکه‌های ۵G فعلی، آن‌ها را به گزینه‌ای عالی برای برنامه‌های اینترنت اشیاء تبدیل می‌کند، اما خطرات باید به درستی در نظر گرفته شوند و با آن‌ها برخورد شود. مفهوم اینترنت اشیاء و اینترنت انرژی (IoE) هر روز بیشتر و بیشتر در زندگی روزمره جاسازی می‌شود. این بدان معناست که اینترنت اشیاء و اینترنت انرژی به راه‌حل‌های امنیتی قوی در تمام بخش‌های زیرساخت خود نیاز دارند. یکی از مهم‌ترین چالش‌ها در اینترنت اشیاء، اجرای حفاظت است. این تحقیق و مقاله به بحث در مورد وضعیت امنیت اینترنت اشیاء و مسائلی که آن را مطرح می‌کند، ادامه می‌دهد. هرچند تحقیقات دانشمندان در این حوزه، تأثیر قابل‌توجهی داشت و آگاهی در مورد دستگاه‌های اینترنت اشیاء پایدارتر را افزایش داد (Pavlović et al., 2021). اما دستگاه‌ها نیز مرتبط هستند. در نتیجه، اینترنت اشیاء ممکن است به اتصال دستگاه‌های الکترونیکی رایج اشاره داشته باشد (Zunino et al., 2020) پتانسیل اینترنت اشیاء برای ارائهٔ خدمات متنوع، آن را به سریع‌ترین فناوری در حال رشد تبدیل کرده است. تأثیر زیادی بر محیط زیست و جامعه داشته است. هدف اینترنت اشیاء (IoT) با اجازه دادن به ابزارهای هوشمند برای انجام کارهای روزانه با حداقل مشارکت انسانی، تغییر نحوهٔ زندگی امروز ما است. شهرهای هوشمند، خانه‌های هوشمند، حمل‌ونقل و زیرساخت‌های هوشمند و اصطلاحات دیگر برای توصیف اینترنت اشیاء استفاده می‌شود.

سهم اصلی در این کار:

۱. توسعهٔ یک رابط امنیتی برای دستگاه‌های اینترنت اشیاء.
۲. اضافه کردن نقشهٔ پروتکل اینترنت برای همهٔ دستگاه‌ها در رابط امنیتی.
۳. افزودن بلاک‌چین برای جلوگیری از دسترسی اشخاص ثالث به رابط، ایجاد اعتماد بین دستگاه‌ها و افزایش قابلیت اطمینان به دلیل قرارگرفتن در شبکهٔ غیرمتمرکز بسته.
۴. توسعهٔ راه‌حل در Node.js و استفاده از حافظهٔ آزمایشی برای AES، DES، Triple DES.

چندین گروه کاری و رهبران کسب‌وکار، استانداردسازی دستگاه‌های اینترنت اشیاء را پیشنهاد کرده‌اند، اما هیچ راه حلی پیدا نشده است (Palattella et al., 2013). اینترنت اشیاء به دلیل افزایش تقاضا برای دستگاه‌ها و خدمات متصل در سراسر جهان، به محافظت بیشتر نیاز دارد. برای اینکه اینترنت اشیاء به پتانسیل کامل خود برسد، باید در برابر اشکالات و مهاجمان بالقوه محافظت شود. انواع حملات و تهدیدها که هر روز بر تعداد و پیچیدگی آن‌ها افزوده می‌شود یا به‌عنوان یک مهاجم انجام می‌شود یا به عنوان یک مصرف‌کننده از بین می‌رود. برای ارائهٔ عملکرد مفید به کاربران، اینترنت اشیاء باید از مناسب بودن و قابل اعتماد بودن داده‌های پردازش‌شده اطمینان حاصل کند. برای اطمینان از استحکام و قابلیت اطمینان در سطح خدمات و همچنین حمایت از حفاظت، به چنین سیستم‌هایی نیاز اساسی وجود دارد. نگرانی‌های مشتریان در مورد امنیت و حریم خصوصی با حرکت به سمت اینترنت اشیاء افزایش می‌یابد. ادغام اینترنت اشیاء در خانه و محل کار نگرانی‌های امنیتی جدیدی را ایجاد می‌کند. مشتریان و تأمین‌کنندگان باید از چالش‌ها آگاه باشند و در برخورد با مسائل حفاظتی و حریم خصوصی احتیاط کنند. چالش‌های امنیتی به شکل شیوه‌های طراحی، فقدان استانداردها و مقررات است. بسیاری از مسائل مربوط به حریم خصوصی ناشی از موافقت کاربر برای اجازه دادن به فروشندگان برای جمع‌آوری فعالیت‌های خود در دستگاه‌های هوشمند است. اینجاست که بلاک‌چین

به‌کار گرفته می‌شود. فناوری بلاک‌چین سروری را که مرکز زیرساخت اینترنت اشیاء است حذف می‌کند. با بررسی تدریجی هر تراکنش یا درخواست شبکه، بلاک‌چین به دستگاه‌ها اجازه می‌دهد تا جریان دادهٔ فعلی را حفظ کنند و در عین حال امنیت و حریم خصوصی را نیز بهبود بخشند.

معرفی بلاک‌چین به زیرساخت اینترنت اشیاء، مزایای زیر را به همراه دارد:

۱. هیچ مرجع کنترلی واحدی وجود ندارد.
۲. بین دستگاه‌های اینترنت اشیاء اعتماد ایجاد کرده‌اند.
۳. تمام اقدامات انجام‌شده توسط دستگاه‌های اینترنت اشیاء ثبت می‌شود.
۴. داده‌های به اشتراک گذاشته‌شده توسط دستگاه‌ها خصوصی است.

نگرانی‌های زیر به دلیل معرفی بلاک‌چین به زیرساخت اینترنت اشیاء ایجاد می‌شود:

۱. محدودیت ذخیره‌سازی.
۲. مقیاس‌پذیری.
۳. زمان پردازش.

محدودیت ذخیره‌سازی به دفتر کل توزیع‌شده گره خورده است که برای ذخیرهٔ تمام تراکنش‌های بلاک‌چین لازم است. مسائل مقیاس‌پذیری با افزودن دستگاه‌های اینترنت اشیا بیشتر به شبکه‌های غیرمتمرکز مرتبط است که زمان پردازش فعالیت‌های انجام‌شده توسط دستگاه‌ها را نیز افزایش می‌دهد.

فناوری بلاک‌چین بر چهار مفهوم استوار است:

۱. یک شبکهٔ همتا به همتا، همهٔ شرکت‌کنندگان از کلیدهای خصوصی/عمومی برای تعامل با شبکه استفاده می‌کنند. کلید خصوصی برای امضای تراکنش‌ها و کلید عمومی به‌عنوان آدرس در شبکه استفاده می‌شود.
۲. دفتر کل باز و توزیع‌شده، پایگاه داده همهٔ تراکنش‌ها، که برای همه باز است.
۳. همگام‌سازی کپی‌های لجر، راهی برای همگام‌سازی دفتر کل بین همهٔ شرکت‌کنندگان.
۴. ماینینگ، راهی برای جلوگیری از افزودن گره‌ها بر روی یک زنجیره، زیرا زنجیره باید معتبر و منظم باشد.

پیشینهٔ پژوهش

اینترنت اشیاء (IoT) دستگاه‌هایی با حسگرها، توانایی پردازش، نرم‌افزار و سایر فناوری‌ها را توصیف می‌کند که داده‌ها را با دستگاه‌ها و سیستم‌های دیگر از طریق اینترنت یا سایر شبکه‌های ارتباطی متصل و مبادله می‌کنند. اینترنت اشیا شامل الکترونیک، ارتباطات و مهندسی علوم کامپیوتر است. "اینترنت اشیاء" به‌عنوان یک نام اشتباه در نظر گرفته شده است، زیرا دستگاه‌ها نیازی به اتصال به اینترنت عمومی ندارند. آن‌ها فقط باید به یک شبکه متصل باشند و به‌صورت جداگانه قابل آدرس‌دهی باشند. این زمینه به دلیل همگرایی چندین فناوری، از جمله محاسبات فراگیر، حسگرهای کالا و سیستم‌های جاسازی شده قدرتمندتر و همچنین یادگیری ماشین، تکامل یافته است. زمینه‌های قدیمی‌تر سیستم‌های تعبیه‌شده، شبکه‌های حسگر بی‌سیم، سیستم‌های کنترل، اتوماسیون (از جمله اتوماسیون خانه و ساختمان)، به‌طور مستقل و جمعی اینترنت اشیاء را فعال می‌کنند. در بازار مصرف، فناوری اینترنت اشیاء مترادف با محصولات «خانهٔ هوشمند» است، از جمله دستگاه‌ها و لوازم خانگی (لوازم روشنایی، ترموستات، سیستم‌های امنیتی خانه، دوربین‌ها و سایر لوازم خانگی) که از یک یا چند اکوسیستم رایج پشتیبانی می‌کنند [توضیحات لازم] و می توان از طریق دستگاه‌های مرتبط با آن اکوسیستم، مانند گوشی‌های هوشمند و بلندگوهای هوشمند، کنترل کرد. اینترنت اشیا در سیستم های مراقبت های بهداشتی نیز استفاده می شود. نگرانی‌های زیادی در مورد خطرات رشد فناوری‌ها و

محصولات اینترنت اشیاء، به‌ویژه در حوزه‌های حفظ حریم خصوصی و امنیت وجود دارد و در نتیجه، صنایع و دولت‌ها برای رسیدگی به این نگرانی‌ها، از جمله توسعهٔ استانداردهای بین‌المللی و محلی، اقداماتی انجام داده‌اند که شامل دستورالعمل‌ها و چارچوب‌های نظارتی است. مفهوم اصلی شبکه‌ای از دستگاه‌های هوشمند در اوایل سال ۱۹۸۲ مورد بحث قرار گرفت و یک دستگاه خودکار کوکاکولا تغییر یافته در دانشگاه کارنگی ملون به اولین دستگاه متصل به شبکهٔ آژانس پروژه‌های تحقیقاتی پیشرفته تبدیل شد که می‌توانست موجودی خود را گزارش دهد و اینکه آیا نوشیدنی‌های تازه بارگذاری‌شده سرد هستند یا نه. مقالهٔ مارک ویزر در سال ۱۹۹۱ در مورد محاسبات فراگیر، "کامپیوتر قرن ۲۱" و همچنین مکان‌های دانشگاهی، مانند UbiComp و PerCom چشم‌انداز معاصر اینترنت اشیاء را ایجاد کرد. در سال ۱۹۹۴، رضا راجی مفهوم را در مجلهٔ مؤسسه مهندسان برق و الکترونیک اینگونه توصیف کرد: "[انتقال] بسته‌های کوچک داده به مجموعهٔ بزرگی از گره‌ها، به‌طوری که همه چیز از لوازم خانگی گرفته تا کل کارخانه‌ها را یکپارچه و خودکار کند". بین سال‌های ۱۹۹۳ و ۱۹۹۷، چندین شرکت راه‌حل‌هایی مانند مایکروسافت در محل کار یا Novell's NEST را پیشنهاد کردند. زمانی که بیل جوی ارتباط دستگاه با دستگاه را به‌عنوان بخشی از چارچوب «شش وب» خود که در مجمع جهانی اقتصاد در داووس در سال ۱۹۹۹ ارائه شد، در نظر گرفت، این زمینه شتاب بیشتری گرفت. مفهوم "اینترنت اشیاء" و خود این اصطلاح، اولین بار در سخنرانی پیتر تی لوئیس، در پانزدهمین آخر هفتهٔ قانونگذاری سالانهٔ بنیاد سیاه‌پوستان کنگره در واشنگتن دی سی، منتشر شده در سپتامبر ۱۹۸۵ ظاهر شد. به گفته لوئیس، "اینترنت اشیاء، ادغام افراد، فرایندها و فناوری با دستگاه‌ها و حسگرهای قابل اتصال است تا امکان نظارت از راه دور، وضعیت، دستکاری و ارزیابی روند چنین دستگاه‌هایی را فراهم کند.

کار مرتبط با آخرین هنر

تحقیق برای کار مرتبط در ادامه شرح داده شده است. سایر محققان رایج‌ترین مسائل امنیتی در هاب‌های اینترنت اشیا و همچنین محبوب‌ترین حملات و استراتژی‌های مورد استفاده علیه دستگاه‌های اینترنت اشیاء را کشف کرده‌اند. ما انسان‌ها یک آزمایش در دنیای واقعی انجام می‌دهیم تا ببینیم آیا کار بعد از ایجاد راه‌حل توصیه شده امنیت بیشتری می‌دهد یا خیر. ارزیابی با خلاصه‌ای از آنچه انجام شده و توصیه‌هایی برای کار بیشتر به پایان می‌رسد (Nawir et al., 2016). عناصر کلیدی مرتبط با سیستم‌های اینترنت اشیا، روابط آن‌ها، مسائل امنیتی فزاینده را در محیط‌های مختلفی که در آن‌ها یکپارچه شده اند توضیح می دهد. این دستگاه‌ها عمدتاً در خانه، پزشکی و حمل و نقل استفاده می‌شوند. برای پشتیبانی از میلیاردها دستگاه اینترنت اشیاء در سراسر جهان، زیرساخت‌های جامعهٔ بی‌سیم باید از نظر ظرفیت حداقل راحتی را داشته باشند و به‌طور استثنایی قابل گسترش باشند، اما در مناطق مختلف اینترنت اشیاء را با توجه به نیازهای ارائه‌دهندهٔ منحصر به فرد خود مدیریت بهینه کنید (Anon, 2015). اینترنت موبایل و اینترنت اشیاء دو پیوند اصلی با شبکهٔ سلولی سرنوشت‌ساز هستند که نمای وسیعی از ۵G را ارائه می‌دهند. نسل ۵G به‌عنوان اولین جامعه‌ای است که توسعه‌پذیر، همه‌کاره و هوشمندانه برای دومین جهان متصل اینترنت اشیاء طراحی شده است (Chvez-Santiago et al., 2015). به گفته آنون[1] (۲۰۱۴)، ۵G بسیاری از عناصر سبک زندگی آینده مانند خانه، محل کار و حمل‌ونقل را کنترل می‌کند و می‌تواند با تراکم محدودهٔ بازدیدکنندهٔ بالا، تراکم اتصال بالا و تحرک بیش از حد، محیط زیست اینترنت اشیاء مشخص شود. توابع اساسی سیستم را تنظیم کنید (Mavromoustakis et al., 2016). این دستگاه هنگام استفاده در خانه باید ایمن و در برابر دسترسی غیرمجاز مقاوم باشد. متداول‌ترین حملات و تکنیک‌های حملات شبکه به دستگاه‌های اینترنت اشیاء عبارت‌اند از: حملهٔ انکار سرویس (DoS)، (Thakur,

1. Anon

2015; Goyal & Dutta, 2018)، جعل، تغییر یا پخش مجدد درخواست شبکه (Rong et al., 2013)، سیبل (Buford et al., 2008). حملات به دستگاه‌های اینترنت اشیا را می‌توان در سطوح مختلف شبکه انجام داد. در بخش بعدی این تحقیق و مقاله، حملات بر اساس لایه مدل اتصال سامانه‌های باز شبکه‌ای که روی آن اجرا می‌شوند مرتب شده و شرح داده شده‌اند. در لایهٔ فیزیکی، دستگاه‌های اینترنت اشیا می‌توانند تحت تأثیر پارازیت یا دستکاری قرار گیرند که باعث ایجاد تداخل رادیویی و خستگی در دستگاه‌های اینترنت اشیاء می‌شود که می‌تواند منجر به ایجاد گره‌های در معرض خطر شود. دو گره می‌توانند در فرکانس یکسان ارسال کنند که می‌تواند منجر به برخورد در پیوند داده شود. مهاجمان لایه برنامه می توانند مانند کاربر عادی در سیستم اینترنت اشیاء عمل کنند. مهاجمان می‌توانند فعالیت‌های مخربی را در سیستم اینترنت اشیاء انجام دهند که می‌تواند منجر به حمله به قابلیت اطمینان (تغییر ساعت، ارسال انتخابی داده‌ها و اغراق داده‌ها) شود. سعی شد که به درک بهتر تهدید کمک شود. می‌توان توضیح داد که چرا دستگاه‌های اینترنت اشیاء برای مهاجمان بسیار مفید هستند. اکثر دستگاه‌های اینترنت اشیا بدون تعامل انسانی کار می‌کنند و به‌طور فیزیکی به راحتی در دسترس مهاجمان قرار می‌گیرند. این دستگاه‌ها همچنین با استفاده از شبکه‌های بی‌سیم کار می‌کنند تا مهاجمان بتوانند حملات متوسط را انجام دهند و به راحتی اطلاعات حساس را به‌دست آورند. اکثر دستگاه‌ها به دلیل محدودیت‌های سخت‌افزاری قادر به پشتیبانی از الگوریتم‌های امنیتی پیچیده نیستند. این تحقیق و مقاله بر چالش‌های پیرامون دستگاه‌ها و خدمات متمرکز شده و مهم‌ترین مسائل امنیتی اینترنت اشیاء را تشریح می‌کند. دانشمندان به این نتیجه رسیدند که هم کاربران نهایی و هم فروشندگان باید کارهای زیادی انجام دهند. تعریف استانداردهایی که کاستی‌های مکانیسم‌های امنیتی فعلی اینترنت اشیاء را برطرف می‌کنند، مهم است (Abomhara & Køien., 2015; Mahmoud et al., 2015) یک نمای کلی جامع از حملات به تمام لایه‌های شبکه ارائه می‌دهد. پروتکل‌های شبکهٔ جدید (مانند IPv۶ و ۵G) باید برای هدایت دستگاه‌های امنیتی برای دستیابی به ترکیبات توپولوژی پویا اینترنت اشیاء پیاده‌سازی شوند. بیشتر حملات در لایه درک، لایهٔ شبکه و لایهٔ برنامه اتفاق می‌افتد. بیشتر سیگنال‌های ارسال‌شده بین دستگاه‌های اینترنت اشیاء ممکن است تداخل داشته باشند و در نتیجه تحت تأثیر قرار گیرند. حملات رله از این لایهٔ محرمانه بهره خواهند برد. حملات رله را می‌توان با تغییر، کپی یا جعل اطلاعات هویتی ارائه‌شده توسط دستگاه انجام داد. نوع دیگری از حملاتی که می‌توان بر روی این لایه انجام داد، حملهٔ زمانی است. حملات زمان‌بندی را با تجزیه و تحلیل زمان مورد نیاز برای انجام رمزگذاری انجام دهید. نتیجه این حمله این است که مهاجم می‌تواند به کلید رمزگذاری دسترسی پیدا کند. مهاجم می‌تواند به گره دسترسی فیزیکی پیدا کند و تمام اطلاعات و داده‌ها را بگیرد. به این حمله گرفتن گره می‌گویند. در لایهٔ شبکه، محبوب‌ترین حملات؛ حملات انکار سرویس (DoS) و حملات انسان در وسط است. به دلیل عدم وجود استانداردها یا سیاست‌های امنیتی در اینترنت اشیاء، تعداد زیادی از دستگاه‌ها می‌توانند در برابر حملات در لایهٔ برنامه مقاومت کنند. برنامه‌های مختلف دارای الگوریتم‌های امنیتی متفاوت یا بدون الگوریتم امنیتی هستند. بزرگ‌ترین مشکل در اینجا این است که دستگاه‌های مختلف اینترنت اشیاء باید با یکدیگر سازگار باشند. در این تحقیق و مقاله می‌توان نتیجه گرفت که تجهیزات باید از استاندارد شبکهٔ جدیدتری استفاده کنند. می‌توان اجرای یک چارچوب هوشمند دستگاه هوشمند با امنیت سرتاسر را پیشنهاد کرد. سخت‌افزار، نرم‌افزار، فناوری‌های بی سیم و شناسایی جدید برای غلبه بر چالش‌های اینترنت اشیاء مورد نیاز است. بدافزار بریکربات (Souran et al., 2019) در سال ۲۰۱۷ کشف شد اما دوباره در سال ۲۰۱۹ ظاهر شد. نرم‌افزار دسترسی به اینترنت عمومی را اسکن می‌کند و سعی می‌کند دستگاه‌های اینترنت اشیاء را در آن پیدا کند. اگر دستگاه اینترنت اشیاء قابل کشف باشد، سعی می‌کند با استفاده از رایج ترین ترکیبات لاگین ضعیف به آن دسترسی پیدا کند. اگر دسترسی پیدا کند، تمام داده‌های شبکه موجود در دستگاه هوشمند را حذف می‌کند که

آن را غیرقابل استفاده می‌کند، مگر اینکه شخصی به‌طور فیزیکی به دستگاه دسترسی پیدا کند تا آن را به حالت پیش‌فرض کارخانه راه‌اندازی مجدد کند. این بدافزار هدف دیگری جز هدف مخرب ندارد و دستگاه را غیرقابل استفاده می کند. در سال ۲۰۱۶ میرای بات نت (Kambourakis et al., 2017) بیش از ۸.۴ میلیون دستگاه اینترنت اشیاء را تصاحب کرد. این دستگاه‌ها برای انجام حملات انکار سرویس توزیع‌شده (DDoS) مورد استفاده قرار گرفتند. برخی از اقدامات برای یافتن کدهای مخرب در دستگاه ها حتی امروزه نیز انجام می شود. مشکل اینجاست که هیچ سابقهٔ ثبت‌شده‌ای از اقدامات انجام شده توسط دستگاه‌ها وجود ندارد که پیدا کردن یک دستگاه مخرب در شبکه را حتی سخت‌تر می‌کند. کومار و مالیک[1] (۲۰۱۸) تحقیق کردند که زیرساخت‌های فعلی اینترنت اشیاء با چه چالش هایی روبه‌رو هستند. در این تحقیق و مقاله با چالش‌های حریم خصوصی و امنیتی سروکار داریم. می‌توان گفت که بزرگ‌ترین مشکلات زیرساخت‌های فعلی شناسایی شدند و یک نمای کلی از همهٔ آن‌ها ارائه شد. با مرور کلیِ ارائه‌شده در این تحقیق و مقاله، دلیل نیاز به بلاک‌چین در اینترنت اشیاء ارائه شد. برخی از بخش‌هایی که بلاک‌چین و اینترنت اشیاء را می‌توان ادغام کرد و مزایای خوبی ارائه کرد عبارت‌اند از کشاورزی، تجارت، توزیع، انرژی (Yuvaraj et al., 2017)، غذا، مالی، مراقبت‌های بهداشتی، حمل‌ونقل و تدارکات و شهر هوشمند. صاحب‌نظران در تحقیقات قبلی فهرستی از مزایایی مانند داده‌های ضد دستکاری، حذف مرجع کنترل واحد، داده‌های قوی، ثبت تراکنش‌های قدیمی در دستگاه‌های هوشمند و موارد دیگر ارائه کردند. انگیزهٔ این کار ناشی از مشکلات مشاهده شده است که در همه دستگاه‌های اینترنت اشیاء وجود دارد. هاب اینترنت اشیاء ارائه‌شده توسط سازنده (در صورت وجود) ویژگی‌های امنیتی کمی را ارائه می‌دهد یا اصلاً وجود ندارد. این هاب‌ها عمدتاً دستگاه‌های مختلف اینترنت اشیاء با همان برند را ادغام می‌کنند. سایر مراکز اینترنت اشیاء عمدتاً برای مشاهدهٔ دستگاه‌های اینترنت اشیاء (دوربین‌های هوشمند، واکی تاکی و غیره) در خانهٔ هوشمند و نمایش داده‌هایی که آن‌ها در رایانهٔ شخصی ارائه می‌دهند استفاده می‌شود. راه‌حل یک رابط ساده مناسب برای هر دستگاه اینترنت اشیاء و زیرساخت شبکه است. استفاده از بلاک‌چین به‌عنوان یک لایهٔ اضافی مانع از دسترسی سایر مهاجمان به دستگاه‌های هوشمند می‌شود. ویژگی اصلی این کار این است که از هر الگوریتم رمزگذاری استفاده‌شده توسط سرورهای راه دور برای ارائهٔ داده به دستگاه‌های اینترنت اشیا پشتیبانی می‌کند.

راه‌حل پیشنهادی

از نظر تئوری، مقاله راه‌حلی را ارائه می‌دهد که تا پیاده‌سازی واقعی و ارزیابی امنیتی توسعه یافته است. این راه‌حل بر اساس محیط زیر است:

۱. سرور خانگی سفارشی (هاب) برای همهٔ دستگاه‌های هوشمند متصل.
۲. استفاده از اتصالات سیمی بین دستگاه هوشمند و سرورهای خانگی.
۳. افزودن یک لایهٔ امنیتی به فایروال سرور خانگی، سریال‌سازی داده‌ها، فشرده‌سازی داده‌ها، رمزگذاری.
۴. استفاده از یک زبان برنامه‌نویسی تا سرور بتواند روی هر دستگاهی اجرا شود.
۵. از برقراری ارتباط مستقیم دستگاه هوشمند با اینترنت یا اینترنت برای ارتباط مستقیم با دستگاه هوشمند جلوگیری می‌کند. تمام ارتباطات باید از طریق سرور خانگی انجام شود.

1. Kumar & Mallick

۶. افزودن فناوری بلاک‌چین و غیرمتمرکز کردن شبکه. دفتر کل توزیع‌شده را برای نظارت بر همهٔ درخواست‌ها اضافه کنید و با استفاده از احراز هویت بلاک‌چین یک لایه امنیتی اضافی اضافه کنید و از هرگونه درخواستی که توسط دستگاه انجام می‌شود جلوگیری کنید.

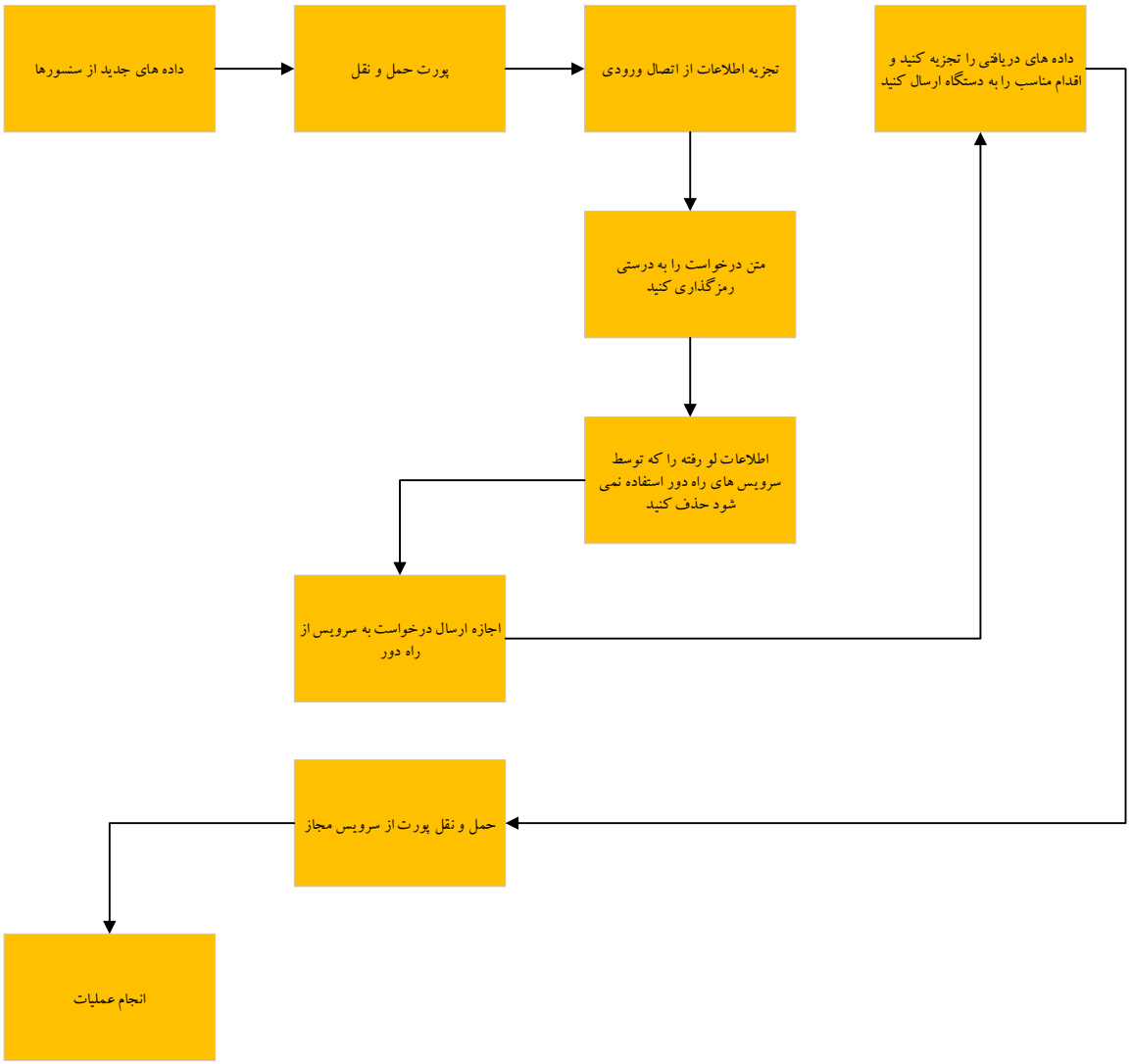
در شکل ۱ منطق بلاک‌چین در سرور خانگی گنجانده شده است. هنگام تجزیهٔ داده‌های ورودی، بلاک‌چین داده‌ها را تأیید می‌کند، بلوک‌های جدید ایجاد می‌کند و آن‌ها را به دفتر کل توزیع می‌کند. امنیت دستگاه‌های هوشمند، مانند امنیت شبکه‌های بی‌سیم است (Kavianpour & Anderson, 2017). سوءاستفاده از دستگاه هاب مانند سوءاستفاده از هر دستگاه متصل است. این هاب دستگاه‌های هوشمند را به شبکهٔ پروتکل اینترنت متصل می‌کند و یک رابطه اعتماد از پیش ایجادشده دارد. این همان امنیت شبکهٔ بی‌سیم است که امنیت هاب به آن متصل است. از آنجایی‌که برخی از دستگاه‌های هوشمند از هاب پشتیبانی نمی‌کنند، این امنیت مبتنی بر امنیت شبکه است. برای بهبود امنیت این دستگاه‌ها، ما یک راه‌حل مبتنی بر سرور خانگی (هاب) سفارشی برای همهٔ دستگاه‌های هوشمند بدون توجه به پشتیبانی هاب پیشنهاد کرده‌ایم. این راه حل شامل سرور خانگی، اتصال سیمی یا بی سیم به یک دستگاه هوشمند و فناوری بلاک‌چین است. تمام داده‌های ارسال شده از دستگاه‌های هوشمند به سرویس‌های راه دور آن‌ها توسط سرور رهگیری و تجزیه می‌شود. این بدان معنی است که اطلاعات لو رفتهٔ غیرضروری را می‌توان در مورد دستگاه حذف کرد و بسته را قبل از ارسال به سرویس به درستی رمزگذاری کرد. داده‌های دستگاه هوشمند باید با فرمت صحیح تجزیه و برای سرویس راه دور آماده شوند. برای رهگیری این داده‌ها، ما از فناوری بلاک‌چین برای نظارت بر هر درخواست شبکه انجام شده توسط گره، دستگاه اینترنت اشیاء استفاده می‌کنیم. با استفاده از یک برنامهٔ حملهٔ بویش، مانند یک تحلیل‌کنندهٔ نرم‌افزار آزاد و متن باز (Iqbal & Naaz, 2019) می‌توانیم تشخیص دهیم که کدام دستگاه در حال ارسال درخواست به کدام سرویس، آدرس پروتکل اینترنت و پورت آن است، به این ترتیب می‌توانیم مطمئن شویم که داده‌های نوشته‌شده در دفتر کل توزیع‌شده صحیح است. تمام درخواست‌های داخل یک شبکهٔ خصوصی تراکنش هستند و هیچ راهی برای ساختگی یا تغییر آن‌ها وجود ندارد. هر تراکنش در دفتر کل توزیع‌شده ذخیره می‌شود، پایگاه داده‌ای که می‌تواند در رابط بلاک‌چین باشد. یک رابط بلاک‌چین می‌تواند بر روی هر رایانه‌ای میزبانی شود و دفتر کل توزیع‌شده را می‌توان در دستگاه و سرور شبکهٔ محلی ذخیره کرد یا در صورت استفاده در خانه‌های هوشمند که در آن سرور محلی وجود ندارد، پایگاه دادهٔ راه دور که می‌تواند با الگوریتم رمزگذاری قوی رمزگذاری شود، درخواست شود. برای این سرور می‌توان با استفاده از الگوریتم رمزنگاری به روش کلید عمومی، رمزگذاری انجام داد.

سرور خانگی عملکردهای زیر را انجام می‌دهد:

دریافت اطلاعات از دستگاه هوشمند. داده‌ها باید تجزیه شوند. تعیین کنید که این داده‌ها به درستی رمزگذاری شده و به سرویس راه دور منتقل شده‌اند (با استفاده از پروتکل Http(s)). ویژگی‌های اضافی که در سرور خانگی می‌خواهیم:

۱. نظارت بر داده‌های دستگاه هوشمند برای هرگونه درخواست مشکوک.
۲. در صورت امکان، از یک الگوریتم رمزگذاری قوی استفاده کنید (فقط در صورتی امکان‌پذیر است که سرویس از راه دور از استانداردهای رمزگذاری مختلف پشتیبانی کند). این باید برای هر دستگاه هوشمند در شبکهٔ خانگی فعال شود (Faheem Mushtaq et al., 2017).
۳. از فناوری بلاک‌چین برای جلوگیری از هرگونه دستکاری در درخواست‌های شبکه توسط اشخاص ثالث استفاده کنید.

۴. برای ایجاد اعتماد بین دستگاه‌های اینترنت اشیا در همان شبکه، احراز هویت اضافی را از طریق بلاک‌چین اضافه کنید.



شکل ۱. راه‌حل پیشنهادی در فلودیاگرام فعالیت.

رابط سرور خانگی باید به زبان برنامه‌نویسی نوشته شود که در اکثر دستگاه‌ها قابل‌اجرا باشد. در حل، Node.js (Sun et al., 2018) به‌عنوان یک زبان برنامه‌نویسی استفاده می‌شود. Node.js از اکثر دستگاه‌ها پشتیبانی خوبی دارد. برخی از مدیران فرایند برای Node.js مانند PM2 از رویکرد کانتینر پشتیبانی خوبی دارند. این بدان معناست که سرور خانگی در یک کانتینر است و هر مهاجمی برای اتصال به آن مشکل خواهد داشت. PM2 از حالت کلاستر نیز پشتیبانی می‌کند. از آنجایی که Node.js یک حالت کلاستر زبان تک‌رشته‌ای است به برنامه‌ها اجازه می‌دهد از تمام هسته‌های واحد پردازش مرکزی استفاده کنند که به برنامه‌ها امکان مقیاس‌پذیری را می‌دهد. این کار عملکرد سرور را بسته به تعداد واحدهای پردازش مرکزی اصلی بسیار افزایش می‌دهد. هر فرایند بر روی یک خوشه جدید ایجاد می‌شود. اگر یک مهاجم سعی کند از هر فرایندی در سرور سوءاستفاده کند، خوشه پس از مدت زمان معینی فرایند را از بین می‌برد تا مطمئن شود که سرور همان‌طور که در نظر گرفته شده است کار می‌کند. با استفاده از سرور خانگی، از حملات زیر جلوگیری می‌کند:

۱. هیچ راهی برای مهاجمان وجود نخواهد داشت که مستقیماً داده‌ها را از دستگاه‌های هوشمند استشمام کنند. تنها داده‌ای که آن‌ها می‌توانند دریافت کنند، از روتر به اینترنت است. اگر به درستی رمزگذاری شود، شانس بسیار کمی برای انجام هرگونه بهره‌برداری وجود خواهد داشت.
۲. اتصال مستقیم به یک دستگاه هوشمند و انجام هرگونه سوءاستفاده بر روی آن. تمام اتصالات از راه دور به یک دستگاه هوشمند به سرور خانگی ارسال می‌شود و سپس بررسی می‌شود که آیا درخواست از منابع تأییدشده است یا خیر.
۳. دستگاه‌هایی در شبکه‌های محلی که احراز هویت ندارند، یک لایهٔ امنیتی جدید بر اساس احراز هویت در سرور خانگی خواهند داشت. برای دسترسی به هر دستگاه خانهٔ هوشمند، احراز هویت و مجوز در سرور خانگی مورد نیاز است.

این راه‌حل پیشنهادی را می‌توان با افزودن موارد زیر بهبود بخشید:

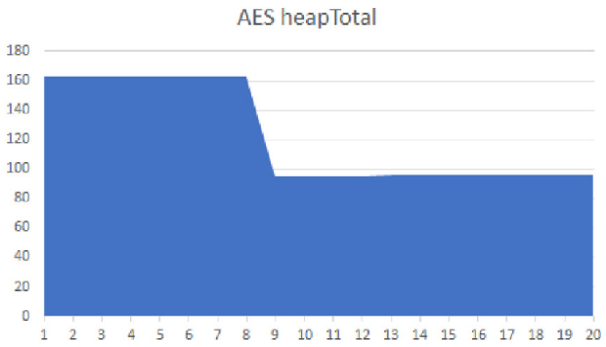
۱. فیلتر کردن به سرویس‌های ابری اجازه می‌دهد تا به شبکهٔ بلاک‌چین دسترسی داشته باشند، با اجازه دادن به آدرس‌های پروتکل اینترنت خاص یا محدوده‌ای از آدرس‌هایی که می‌توانند دسترسی داشته باشند.
۲. افزودن یک لایهٔ امنیتی اضافی با پیاده‌سازی رابطی که داده‌هایی را که از شبکهٔ بلاک‌چین خارج می‌شوند رمزگذاری/رمزگشایی می‌کند.
۳. برای جلوگیری از خروج درخواست‌ها از شبکه بلاک‌چین، فرمی از پاسخ ذخیره‌سازی را از ابر اضافه کنید. اگر همان درخواست به ابر ارسال شود، می‌توانیم از یک دفتر کل توزیع‌شده برای ارائهٔ یک دستگاه هوشمند با پاسخ قبلی از ابر استفاده کنیم.

امنیت، اعتماد و محدودیت‌های راه‌حل

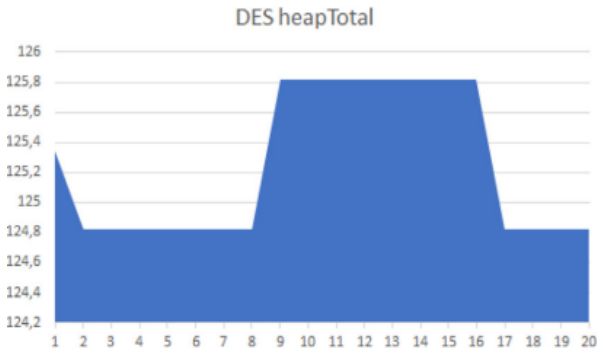
همانطور که در شکل ۱ نشان داده شده است، راه‌حل پیشنهادی دارای چهار نگرانی است. اولین تمرکز بر روی دستگاه‌های هوشمند است. دستگاه‌های هوشمند از حسگرها برای جمع‌آوری داده‌ها و پردازش داده‌های لازم برای ارسال آن به یک سرور راه دور استفاده می‌کنند. به دلیل قدرت پردازش پایین این دستگاه، داده‌های جمع‌آوری‌شده از منابع خارجی رمزگذاری ضعیفی دارند یا اصلاً رمزگذاری نمی‌شوند. برای اطمینان از امنیت این داده‌ها در اینترنت، راه حل پیشنهادی باید آن را رهگیری کند. شنود داده‌ها از نقطه دوم مورد علاقه شروع می‌شود. دومین نکتهٔ مورد توجه، رابط بلاک‌چین است. رابط بلاک‌چین به دنبال هر درخواست شبکه به‌عنوان یک تراکنش جدید است. هر تراکنش در دفتر کل توزیع‌شده ذخیره می‌شود. پس از ذخیرهٔ تراکنش جدید، درخواست به سرور راه دور ارسال می شود. برای پردازش این داده‌ها از روتر، سرور در حال گرفتن آن به‌صورت محلی است. داده‌هایی که از دستگاه می‌آیند دارای سرصفحه درخواست و بدنهٔ درخواست هستند. هدر درخواست دارای اطلاعاتی مانند مکان‌یاب منبع یکسان درخواست، روش درخواست، کد وضعیت، نسخهٔ درخواست (HTTP/۱.۱ یا HTTP/۲)، اطلاعات رمزگذاری، اطلاعات عامل کاربر، اطلاعات مجوز و اطلاعات نوع محتوا است. برخی از هاب‌های اینترنت اشیاء (Cirani et al., 2015) برای درست کار کردن، اطلاعات اضافی را در مورد هاب در هدر ارسال می‌کنند. بیشتر داده‌های موجود در سرصفحه‌های درخواست توسط سرویس راه دور استفاده نمی‌شوند، بنابراین می‌توان آن‌ها را حذف کرد. بدنهٔ درخواست دارای داده‌هایی است که برای تجزیهٔ سرویس از راه دور لازم است. برای جلوگیری از نشت داده‌ها، سرور داده‌های استفاده نشده را از هر درخواست به سرویس راه دور حذف می‌کند. تمام درخواست‌های ارائه‌شده از سرور به اینترنت از نسخهٔ HTTP/۲ پروتکل استفاده می‌کنند. برای بهبود بیشتر امنیت هر درخواست، امکان افزودن یک لایهٔ

رمزگذاری برای بدنهٔ درخواست وجود دارد. این بدان معناست که اگر یک سرویس راه دور قابلیت استفاده از الگوریتم‌های رمزگذاری مختلف را داشته باشد، سرور می‌تواند آن را در اینجا اضافه کند. به‌عنوان مثال، سرور می‌تواند یک جفت کلید ریوست–شمیر–ادلمن تولید کند (Zhou & Tang, 2011) و یک کلید عمومی در سرویس راه دور اضافه کند یا هر کلید متقارن را برای استفاده با AES، DES، یا DES سه‌گانه تولید کند (Bhat et al., 2015). اکنون می‌توان درخواست‌های جدید آماده شده را پردازش و به سرویس از راه دور ارسال کرد. درخواست از سرور به رابط بلاک‌چین ارسال می‌شود و سپس آن را به اینترنت ارسال می‌کند. تنها نقطهٔ ورود برای هر دستگاه اینترنت اشیاء در شبکهٔ خانگی از طریق درخواست‌های رابط بلاک‌چین است که به سرور خانگی ارائه می‌شود. همین امر در مورد راه دیگری نیز صدق می‌کند. سرویس راه دور داده‌های ارسال شده توسط سرور را تجزیه می‌کند و اقدام مربوطه را برای دستگاه برمی‌گرداند. دوباره، رابط بلاک‌چین این درخواست را به سرور ارسال می کند. هر درخواستی برای دستگاه اینترنت اشیاء به سرور ارسال می‌شود. اعتبار درخواست در سرور بررسی می‌شود. سپس سرور به سؤالات زیر پاسخ می‌دهد:

۱. آیا سرورهای خانگی انتظار دارند که سرویس از راه دور، درخواستی را به دستگاه اینترنت اشیاء ارسال کند؟
۲. آیا بدنه و هدر درخواست حاوی داده‌های مشکوکی است؟



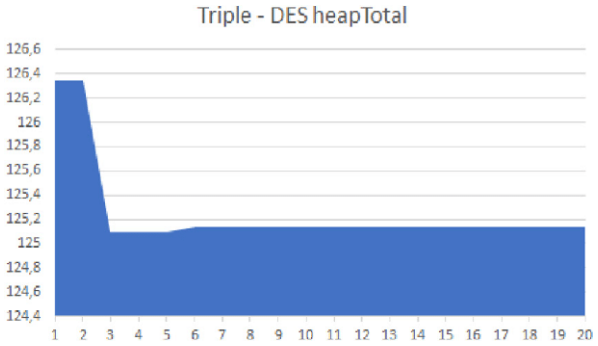
شکل ۲. حافظهٔ HeapTotal AES از ۲۰ پردازش در مگابایت.



شکل ۳. حافظهٔ DES heapTotal از ۲۰ پردازش در مگابایت بر ثانیه.

اگر سرور به این نتیجه برسد که درخواست معتبر است، به یک دستگاه اینترنت اشیاء در شبکهٔ محلی ارسال می‌شود. پس از این دستگاه اینترنت اشیاء، اقدام خاص درخواست شده توسط سرویس راه دور را به‌عنوان اقدام قانونی انجام می دهد. استفاده از حافظه با استفاده از AES، DES و Triple DES ارزیابی شده و در اینجا نتایج آمده است. اندازه‌گیری‌ها بر حسب مگابایت نمایش داده می‌شوند. Heap یک بخش حافظه است که به ذخیرهٔ انواع مرجع مانند اشیاء، رشته‌ها و بسته‌ها اختصاص داده شده است. Heap total نشان‌دهندهٔ اندازه کل هیپ مورد استفاده توسط سرور

است (نگاه کنید به شکل ۲). سرور خانگی با توجه به اندازه‌گیری‌های حافظه، برای انجام رمزگذاری/رمزگشایی روی داده‌های دستگاه هوشمند به بیش از ۲۰۰ مگابایت حافظه دسترسی تصادفی نیاز ندارد. این بدان معناست که ساخت سرور خانگی برای تولید انبوه ارزان خواهد بود. کمترین میزان استفاده از حافظه در الگوریتم استاندارد رمزنگاری پیشرفته است. DES و Triple DES دارای حافظهٔ پایداری هستند اما بالاتر از استاندارد رمزنگاری پیشرفته هستند (شکل ۳ را ببینید). راه‌حل به یک پایگاه داده برای ذخیرهٔ کلیدهای دستگاه‌های مختلف برای اهداف رمزگذاری/رمزگشایی نیاز دارد. این بدان معناست که اگر اتفاقی برای پایگاه داده بیفتد، راه‌حل را غیرقابل استفاده می‌کند. این را می‌توان با استفاده از پایگاه دادهٔ حافظه حل کرد. هنگامی که راه‌حل پیشنهادی منتظر پاسخ از سرویس راه دور است و پاسخ نمی‌دهد، فرایند را در سرور متوقف می‌کند (شکل ۴ را ببینید). مشکل دیگر در اینجا به رابط بلاک‌چین مرتبط است. با افزودن بلاک‌چین به زیرساخت فعلی اینترنت اشیاء، مشکل مقیاس‌پذیری را معرفی کرده‌ایم. با افزودن دستگاه‌های هوشمند بیشتر به شبکه، سرعت پردازش کاهش می‌یابد. مصرف انرژی را می توان با افزودن کنتورهای هوشمند با اینورتر متصل به شبکه (Shabalov et al., 2021) بهبود بخشید تا عملکرد خوبی با هزینهٔ مصرف انرژی پایین در هنگام ارتقاء مقیاس شبکه ارائه دهد. مهم‌ترین محدودیت این است که بیشتر کدهای در حال اجرا در دستگاه‌های هوشمند منبع باز نیستند، بنابراین دریافت داده‌ها از دستگاه هوشمند، تجزیه و ارسال رمزگذاری شده به سرویس راه دور بدون تماس مستقیم با سازنده امکان‌پذیر نیست. با این حال، برخی از تولیدکنندگان اسنادی را برای توسعه‌دهندگان و داشبوردها ارائه می‌کنند که در آن داده‌ها را می‌توان تغییر داد، بهبود داد و در قالب‌های متفاوتی به سرویس از راه دور ارائه کرد.

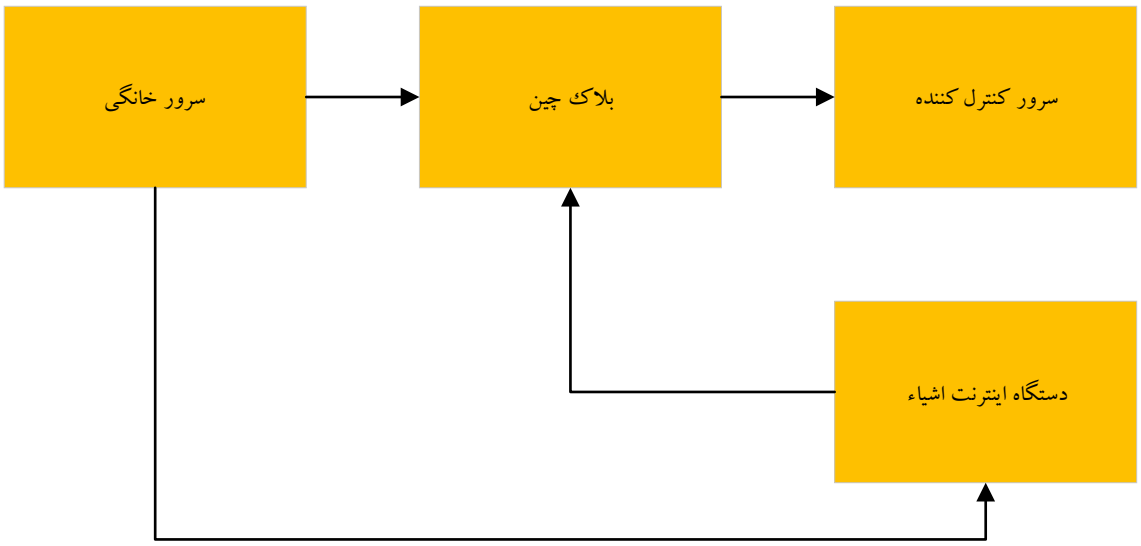


شکل ٤. حافظهٔ سه‌گانه DES HeapTotal از ۲۰ پردازش در مگابایت.

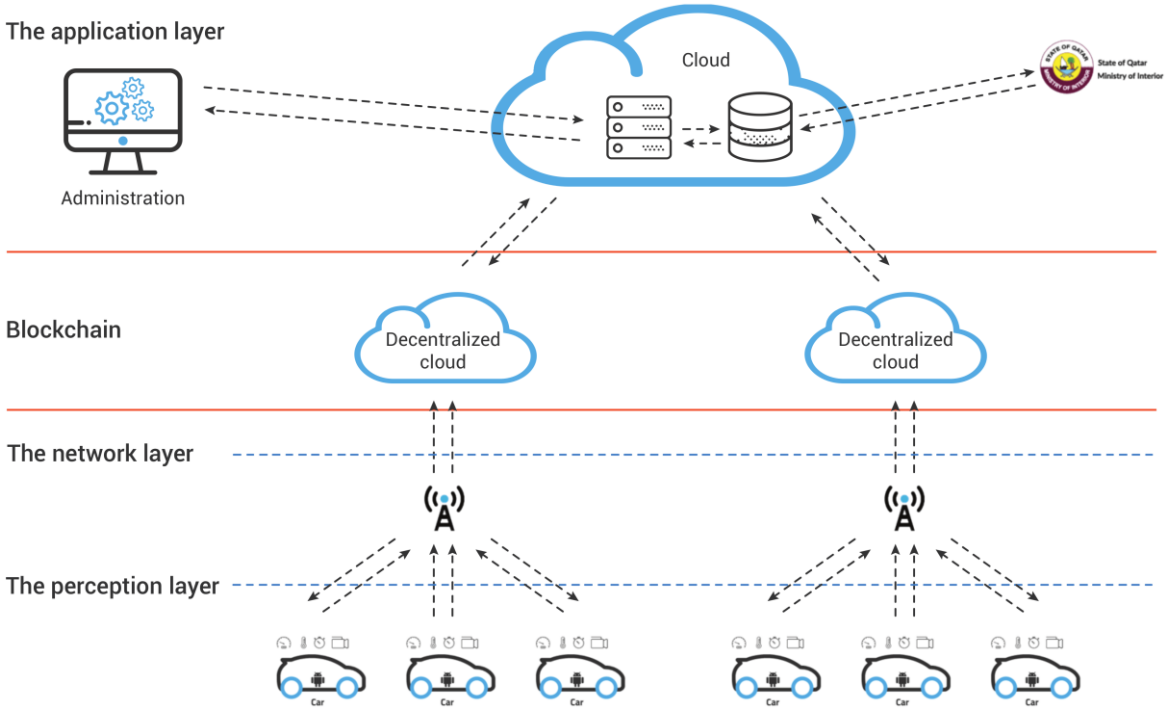
ارزیابی امنیتی

یک نمودار کلاسیک برای راه‌حل پیشنهادی در شکل ۵ ارائه شده است. دستگاه‌های اینترنت اشیاء داده‌ها را به یک ناظر ارسال می‌کنند. این داده‌ها می‌توانند هر چیزی باشند. در این کار از آردوینو (Andriansyah et al., 2017) با سنسورهای دما و رطوبت استفاده شده است. دما و رطوبت اندازه‌گیری شده و این داده‌ها به اینترنت ارسال می‌شود. قبل از ارسال مستقیم آن به اینترنت، رابط بلاک‌چین این داده‌ها را به (سرور خانگی) ارسال می‌کند. ناظر در حال تجزیه داده‌ها، انجام رمزگذاری و ارسال آن به سرویس از راه دور است. سرویس از راه دور تجزیه و تحلیل داده‌ها، رمزگشایی در آن فرایند است و بر اساس داده‌ها، یک اعلان به دستگاه‌های اینترنت اشیاء ارسال می کند تا اقدامات خاصی را انجام دهند. پس از احراز هویت درخواست، ایجاد یک تراکنش جدید و ثبت آن در دفتر کل توزیع‌شده، رابط بلاک‌چین درخواست را به ناظر ارسال می‌کند، که داده‌ها را رمزگشایی می‌کند و برای انجام اقدامات مورد نیاز به دستگاه اینترنت اشیاء ارسال می‌کند. در نمودار کلاس ۰ و ۱ برای تعداد بسیار زیاد استفاده می شود. این بدان معنی

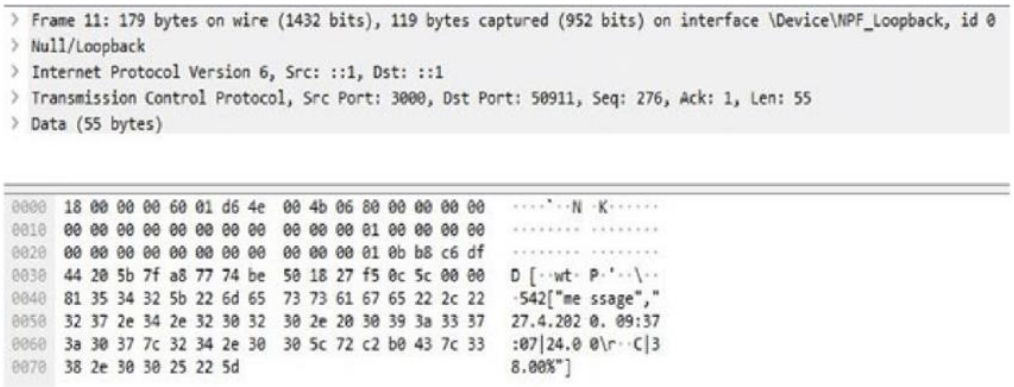
است که سرور خانگی در مورد ما بخشی اختیاری از آن را دارد. ارسال به سرور راه دور قابل انجام است یا خیر. ساختار شبکهٔ راه‌حل پیشنهادی در شکل ۶ نشان داده شده است. شامل دستگاه‌های اینترنت اشیاء، حسگرها، سرور خانگی، رابط بلاک‌چین، ارائه‌دهندهٔ شبکه و سرور خدمات راه دور است. در شکل ۶ ساختار راه‌حل پیشنهادی را نشان می دهد. هر دستگاه اینترنت اشیاء به زیرساخت بلاک‌چین متصل است و هر درخواست شبکه یک تراکنش است. همان‌طور که قبلاً ذکر شد، رابط امنیتی بین رابط بلاک‌چین است و روتر و آن هر درخواستی که به اینترنت ارسال می‌شود را نظارت می کند. در شکل ۷ یک تحلیل‌کنندهٔ نرم‌افزار متن باز برای دریافت درخواست‌های شبکه که از یک دستگاه اینترنت اشیاء به اینترنت می‌آیند استفاده می‌شود. همانطور که در تصویر نشان داده شده است، بدنهٔ درخواست شبکه به‌صورت متن ساده است. با استفاده از راه‌حل پیشنهادی می‌توان امنیت بدنهٔ درخواست شبکه را بسیار بهبود بخشید. یک تحلیل‌کنندهٔ نرم‌افزار متن باز برای درخواست ضبط شبکه به‌عنوان یک استاندارد واقعی برای بازرسی بسته‌های شبکه استفاده شده است. تکامل زیرساخت‌های شبکه ۵G و ۶G یک بلوک ساختمانی مهم برای ادغام دستگاه‌های اینترنت اشیاء در نظر گرفته می‌شود. ما می‌توانیم در سال‌های آینده منتظر راه‌حل‌های بیشتری برای اینترنت اشیاء با این زیرساخت باشیم. با این حال، پذیرش دستگاه‌های اینترنت اشیاء در شبکه‌های ۵G و ۶G مطمئناً چالش‌های امنیتی جدید و انواع جدیدی از حملات به داده‌های شخصی جمع‌آوری‌شده توسط حسگرها و دستگاه‌های اینترنت اشیا را ارائه می کند. این مقاله استفادهٔ انعطاف‌پذیر از هر دستگاه اینترنت اشیاء را بدون نگرانی در مورد امنیت ارائه‌شده توسط دستگاه اینترنت اشیاء پیشنهاد می کند. این راه‌حل یک رابط ساده ارائه می‌دهد که بالاترین سازگاری امنیتی را با سرویس راه دوری که دستگاه اینترنت اشیاء به آن متصل است، اضافه می کند. این راه‌حل به منظور ارائهٔ امنیت سازگار با خدمات از راه دور است. الگوریتم رمزگذاری از دستگاه اینترنت اشیاء به سرور میزبان منتقل می‌شود.



شکل ۵. راه‌حل پیشنهادی در نمودار (فلودیاگرام) ارائه شده است.



شکل ٦. نمودار مبتنی بر بلاک‌چین و فضای ابری برای بهترین راه‌حل پیشنهادی.



شکل ۷. یک تحلیل‌کنندهٔ دقیق نرم‌افزار آزاد و متن‌باز برای عیب‌یابی شبکه و گرفتن بسته منفرد از راه‌حل پیشنهادی.

سرورها محرمانه‌بودن، یکپارچگی و در دسترس‌بودن را به‌گونه‌ای ارائه می‌کنند که توسط شبکهٔ تولید تأمین می‌شود. این کار با استفاده از الگوریتم‌های رمزنگاری موجود انجام می‌شود. این اثر موارد زیر را ارائه می‌دهد:

۱. انعطاف‌پذیری برای استفاده از همهٔ الگوریتم‌های رمزگذاری.
۲. امنیت قوی که از دستگاه اینترنت اشیاء به لایه و دستگاه شبکه منتقل می‌شود.
۳. امنیت دستگاه اینترنت اشیاء همان امنیت شبکهٔ محلی است، سرور در شبکه کار می‌کند.
۴. جلوگیری از نفوذ، تمام درخواست‌های دریافتی برای دستگاه‌های اینترنت اشیاء در شبکهٔ محلی را بررسی کنید.
۵. ادغام زیرساخت‌های فعلی اینترنت اشیاء با فناوری بلاک‌چین.

آنچه باید مورد توجه قرار گیرد این است:

۱. به منظور بهبود امنیت هر دستگاه اینترنت اشیاء در شبکه محلی، سازندگان دستگاه‌های اینترنت اشیا باید یک رابط انعطاف‌پذیر ارائه دهند که دستگاه به آن متصل می‌شود. این بدان معنی است که داده‌های دستگاه اینترنت اشیاء ارسال‌شده به سرور را می‌توان با استفاده از یکی از بسیاری از الگوریتم‌های رمزگذاری مدرن رمزگذاری کرد.
۲. سازندگان دستگاه‌های اینترنت اشیاء باید فهرستی از آدرس‌های پروتکل اینترنت که دستگاه‌های اینترنت اشیاء به آن‌ها متصل هستند ارائه کنند. به این ترتیب، می‌توانیم از تلاش سایر آدرس‌های پروتکل اینترنت برای اتصال به دستگاه اینترنت اشیاء ما در شبکهٔ محلی خود جلوگیری کنیم.

این راه‌حل یک رابط کاربری ساده ارائه می‌دهد که سازندگان دستگاه‌های اینترنت اشیاء می‌توانند از آن برای بهبود امنیت کلی دستگاه‌های خود استفاده کنند. دستگاه‌ها را می‌توان همانطور که هست، بدون توجه به محیط شبکه (اپتیکال، ۵G، ۶G) مورد استفاده قرار داد. از این طریق امنیت دستگاه‌های هوشمند به میزان قابل‌توجهی افزایش می‌یابد. امروزه دستگاه‌های هوشمند در برابر حملات مختلف آسیب‌پذیر هستند و اکثر دستگاه‌های هوشمند سیاست امنیتی اجباری کمی دارند یا اصلاً وجود ندارند. امنیت به لایهٔ شبکه منتقل می‌شود و کل فرایند تبادل داده توسط رمزگذاری سرتاسر سرور به سرور اعمال می‌شود. نتایج راه‌حل‌های پیشنهادی این است که همهٔ درخواست‌ها به درستی رمزگذاری شده‌اند. دستگاه‌های هوشمند جدید را می‌توان بدون هیچ تغییر اضافی به شبکه اضافه کرد. بلاک‌چین با اعتبارسنجی تمام داده‌هایی که از دستگاه‌ها و به آن‌ها می‌آیند، لایهٔ امنیتی بیشتری را فراهم می‌کند.

بحث و نتیجه‌گیری

این تحقیق و مقاله پیشنهاد می‌کند که امنیت دستگاه‌های هوشمند با محدودکردن درخواست‌های مستقیم اینترنتی بهبود یابد. تمام درخواست‌ها باید از طریق رابط بلاک‌چین احراز هویت شوند و در صورت صحت، می‌توانند تأیید شوند. با پیاده‌سازی یک رابط ساده به‌عنوان یک دروازهٔ امنیتی، سازندگان دستگاه می‌توانند لایهٔ دیگری از حفاظت امنیتی برای ارتباطات اینترنتی اضافه کنند. این رابط همچنین می‌تواند دستگاه را از دسترسی شخص ثالث به شبکهٔ محلی که توسط قوانین شبکه مجاز نیست، محافظت کند. در آینده، سرور به گونه‌ای بهینه‌سازی می‌شود که با انواع الگوریتم‌های رمزنگاری سازگار باشد، بنابراین می‌تواند با طیف وسیع‌تری از دستگاه‌های اینترنت اشیاء استفاده شود. با ادغام پیشنهادی راه‌حل، می‌توان به امنیت شبکهٔ محلی یا داخلی و درخواست‌های راه دور دست یافت. بنابراین نه تنها می‌توان امنیت را بهبود بخشید، بلکه یک پایگاه داده (دفتر کل توزیع‌شده) با لیستی از تمام درخواست‌های نوشته‌شده در آن دریافت کرد. بنابراین، اگر حمله‌ای رخ داد، می‌توان آن را از پایگاه داده اشکال‌زدایی کرد و یک لایهٔ حفاظتی اضافی به معماری موجود اضافه کرد و حفره‌های زیرساخت را به‌روزرسانی کرد. در ادامهٔ این تحقیق و مقاله به طور دقیق به مخاطب گفته شد که چه حملاتی به زیرساخت‌های فعلی اینترنت اشیا امکان‌پذیر است و راه‌حل پیشنهادی در برابر آن‌ها چقدر قوی است.

منابع

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.

Andriansyah, M., Subali, M., Purwanto, I., Irianto, S. A., & Pramono, R. A. (2017). E-KTP as the basis of home security system using arduino UNO. In *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)* (pp. 1-5). IEEE.

Anon. (2014). IMT: 5G Vision and Requirements. *Technical report, International Mobile Telecommunications*.

Anon. (2015). Group 4G Americas: 5G Spectrum Recommendations. *Technical report, 4G Americas*.

Bhat, B., Ali, A. W., & Gupta, A. (2015). DES and AES performance evaluation. In *International Conference on Computing, Communication & Automation* (pp. 887-890). IEEE.

Buford, J., Yu, H., & Keong Lua, E. (2008). *P2P networking and applications*. San Francisco: CA.

Chávez-Santiago, R., Szydełko, M., Kliks, A., Foukalas, F., Haddad, Y., Nolan, K. E., ... & Balasingham, I. (2015). 5G: The convergence of wireless communications. *Wireless Personal Communications*, *83*, 1617-1642.

Cirani, S., Ferrari, G., Iotti, N., & Picone, M. (2015). The IoT hub: A fog node for seamless management of heterogeneous connected smart objects. In *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking-Workshops (SECON Workshops)* (pp. 1-6). IEEE.

Goyal, M., & Dutta, M. (2018). Intrusion detection of wormhole attack in IoT: A review. In *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)* (pp. 1-5). IEEE.

Iqbal, H., & Naaz, S. (2019). Wireshark as a tool for detection of various LAN attacks. *Int. J. Comput. Sci. Eng*, *7*(5), 833-837.

Kaliaperumal Rukmani, D., Thangaraj, Y., Subramaniam, U., Ramachandran, S., Madurai Elavarasan, R., Das, N., ... & Imran Abdul Rasheed, M. (2020). A new approach to optimal location and sizing of DSTATCOM in radial distribution networks using bio-inspired cuckoo search algorithm. *Energies*, *13*(18), 4615.

Kambourakis, G., Kolias, C., & Stavrou, A. (2017). The mirai botnet and the iot zombie armies. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)* (pp. 267-272). IEEE.

Kavianpour, A., & Anderson, M. C. (2017). An overview of wireless network security. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 306-309). IEEE.

Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia computer science*, *132*, 1815-1823.

Lu, Q., Zhang, Z., & Lü, S. (2020). Home energy management in smart households: Optimal appliance scheduling model with photovoltaic energy storage system. *Energy Reports*, *6*, 2450-2462.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th international conference for internet technology and secured transactions (ICITST)* (pp. 336-341). IEEE.

Mavromoustakis, C. X., Mastorakis, G., & Batalla, J. M. (Eds.). (2016). *Internet of Things (IoT) in 5G mobile technologies* (Vol. 8). Springer.

Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., & Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. *International Journal of Advanced Computer Science and Applications*, *8*(11).

Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016). Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd international conference on electronic design (ICED)* (pp. 321-326). IEEE.

Neves, P., Calé, R., Costa, M., Gaspar, G., Alcaraz-Calero, J., Wang, Q., ... & Preto, R. (2017). Future mode of operations for 5G–The SELFNET approach enabled by SDN/NFV. *Computer Standards & Interfaces*, *54*, 229-246.

Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., & Dohler, M. (2013). Standardized protocol stack for the internet of (important) things. *IEEE communications surveys & tutorials*, *15*(3), 1389-1406.

Pavlović, N., Šarac, M., Adamović, S., Saračević, M., Ahmad, K., Maček, N., & Sharma, D. K. (2021). An approach to adding simple interface as security gateway architecture for IoT device. *Multimedia Tools and Applications*, *81*(26), 36931-36946.

Rong, C., Zhao, G., Yan, L., Cayirci, E., & Cheng, H. (2013). Computer and information security handbook (2nd ed.). Morgan Kaufmann.

Sarma, R., & Barbhuiya, F. A. (2019). Internet of Things: attacks and defences. In *2019 7th International Conference on Smart Computing & Communications (ICSCC)* (pp. 1-5). IEEE.

Shabalov, M. Y., Zhukovskiy, Y. L., Buldysko, A. D., Gil, B., & Starshaia, V. V. (2021). The influence of technological changes in energy efficiency on the infrastructure deterioration in the energy sector. *Energy Reports*, *7*, 2664-2680.

Shouran, Z., Ashari, A., & Priyambodo, T. (2019). Internet of things (IoT) of smart home: privacy and security. *International Journal of Computer Applications*, *182*(39), 3-8.

Sun, H., Bonetta, D., Humer, C., & Binder, W. (2018, February). Efficient dynamic analysis for Node. js. In *Proceedings of the 27th International Conference on Compiler Construction* (pp. 196-206).

Thakur, K. (2015). Analysis of denial of services (DOS) attacks and prevention techniques. *International journal of engineering research and technology*, *4*.

Yuvaraj, T., Ravi, K., & Devabalaji, K. R. (2017). Optimal allocation of DG and DSTATCOM in radial distribution system using cuckoo search optimization algorithm. *Modelling and Simulation in Engineering*, *2017*.

Zhou, X., & Tang, X. (2011). Research and implementation of RSA algorithm for encryption and decryption. In *Proceedings of 2011 6th international forum on strategic technology* (Vol. 2, pp. 1118-1121). IEEE.

Zunino, C., Valenzano, A., Obermaisser, R., & Petersen, S. (2020). Factory communications at the dawn of the fourth industrial revolution. *Computer Standards & Interfaces*, *71*, 103433.

استناد به این مقاله: شاطری، امیر. (۱۴۰۲). بررسی و تحلیل افزایش حریم امنیتی و شخصی اینترنت اشیاء به وسیلهٔ ادغام یک رابط امن بلاک‌چینی. *نشریه مطالعات برق آپادانا*، ۱(۱)، ۴۶-۶۱.