یازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
11th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

سیستم غیر متمرکز بر پایه بلاکچین برای حفظ حریم خصوصی در خانه هوشمند

رویا زارع فرخادی[1]

[1]هیئت علمی گروه نرم افزار، موسسه آموزش عالی و غیرانتفاعی رشدیه ،تبریز،roya.farkhady@gmail.com

چکیده

کاهش سربار گزاری و سبک سازی فناوری بلاکچینبرای بالا بردن امنیت و حفظ حریم شخصی در اینترنت اشیا در خانه های هوشمند یکی از چالش های روز است. هدف از این مقاله کاهش این سربارگذاری است بطوری که هر موجودیت در یک خانه هوشمند قادر به تبادل داده با کمترین میزان مصرف داده با بالاترین امنیت باشد. این مقاله از نوع کاربردی – تحلیلی می باشد که با استفاده ازمعماری مبتنی بر بلاک چین امنیت و حریم خصوصی غیرمتمرکز را فراهم می کند، ولی بدلیل استفاده از انرژی ، تأخیر و سربار محاسباتی که برای اکثر دستگاه های اینترنت اشیا مناسب نیستند ما یک نوع سبک از بلاک چین برای استفاده در اینترنت اشیا را با اصلاح اثبات کار و استفاده از الگوریتم LSB به جای الگوریتم های منابع فشرده تر مانند PoW و PoS که به طور معمول در بلاک چین استفاده می شوند، الگوریتم استنتاج مبتنی بر زمان را جایگزین کردیم. مدل پیشنهادی ما از ترکیب تکنیک تحلیل همبستگی چند متغیره برای تحلیل ترافیک شبکه و شناسایی همبستگی بین ویژگی های ترافیکی و ادغام الگوریتم های LSB که مقیاس پذیر و متناسب با اینترنت اشیا است طراحی شده سپس ضمن مقایسه با روش های موجود، عملکرد معماری پیشنهادی خود را با استفاده از پارامترهای مختلف مانند توان عملیاتی و سرعت پردازش ارزیابی کردیم.

واژه‌های کلیدی

بلک چین، الگوریتم استنتاج مبتنی بر زمان، LSB.

۱. مقدمه

اینترنت اشیا کاربردهای وسیعی از جمله شبکه‌های هوشمند، شهرهای هوشمند، و مدیریت سلامت دارد. با این حال، جمع‌آوری و انتشار گسترده، متراکم و فراگیر، پردازش و انتشار داده‌ها در زندگی خصوصی افراد باعث افزایش نگرانی‌های امنیتی و حریم خصوصی می‌شود. چندین ویژگی ذاتی اینترنت اشیا چالش‌های امنیتی و حریم خصوصی آن را تقویت می‌کنند از جمله: فقدان کنترل مرکزی، ناهمگونی در منابع دستگاه ها، سطوح حمله چندگانه، خطرات خاص محتوا، و مقیاس پذیری[1] .

امنیت و حفظ حریم خصوصی اینترنت اشیا یکی از مهمترین چالش ها است که عمدتاً به دلیل گسترده بودن ماهیت و توزیع شبکه ای است. رویکردهای مبتنی بر بلاک چین امنیت و حریم خصوصی غیرمتمرکز را فراهم می کند اما آنها دارای انرژی، تأخیر و سربار محاسباتی هستند که برای اکثر دستگاه های اینترنت اشیا مناسب نیست.

هر خانه هوشمند با یک دستگاه همیشه آنلاین و با منبع بالا، مجهز به ماینر که مسئولیت رسیدگی به کلیه ارتباطات داخل و خارج از خانه را دارد مجهز است. این ماینر همچنین حفظ امنیت بلاک چین را برای کنترل ارتباطات مورد استفاده قرار می دهد. ما نشان می دهیم که چارچوب توسعه یافته مبتنی بر بلاک چین ما با تجزیه و تحلیل امنیت به اهداف اساسی مقاله دست میابد. سرانجام نتیجه شبیه سازی را ارائه می دهیم که نشان می دهد که هزینه های اصلی (تراکنش، زمان پردازش و مصرف انرژی) که با رویکرد ما معرفی شده اند بهبود یافته اند.

تکنولوژی بلاک چین که پشتیبان بیت‌کوین (بیت‌کوین اولین سیستم ارز رمزنگاری که در سال ۲۰۰۸ راه‌اندازی شد) است [2]، می‌تواند یک راه‌حل موثر برای امنیت و حریم خصوصی اینترنت اشیا فراهم کند. امنیت بلاک چین به طور عمده از یک معمای رمزنگاری شناخته‌شده به نام اثبات کار (POW) استفاده می کند که برای افزودن (استخراج) بلوک‌های جدید به بلاک چین به کار می‌رود. بلاک چین نیز با استفاده از کلید عمومی قابل تغییر به عنوان هویت کاربران، سطح بالایی از حریم خصوصی را ارایه می‌دهد. بلاک چین برای تعدادی از کاربردهای غیر مالی بکار گرفته شده‌است، به عنوان مثال اثبات موقعیت، سیستم‌های ذخیره‌سازی توزیعی، و داده‌های مراقبت بهداشتی.

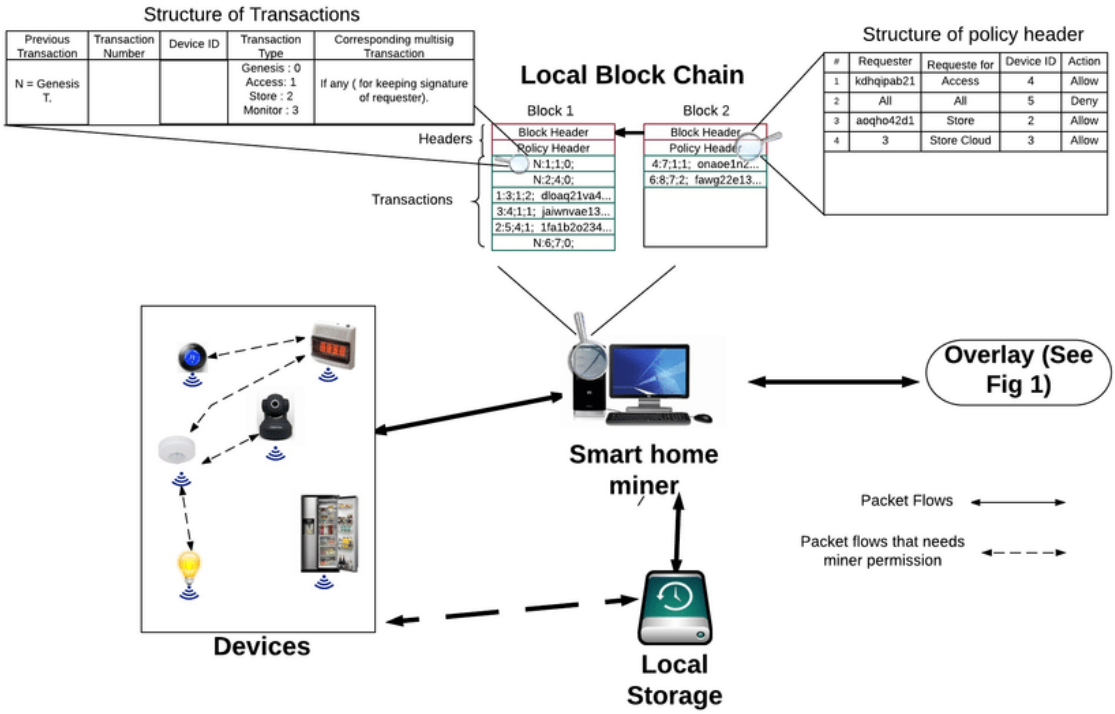
این ویژگی‌های برجسته بلاک چین برای ارایه حریم خصوصی و امنیت توزیع شده در اینترنت اشیا جذاب می‌سازد. امنیت و حفظ حریم شخصی در اینترنت اشیا همچنان یک چالش اساسی است و بدلیل مقیاس گسترده و ماهیت شبکه (توزیع شدگی) اینترنت اشیا رویکرد های مبتنی بر بلاک چین امنیت و حریم شخصی را به طور قابل توجهی بالا برده است اما مصرف انرژی بالا، تاخیر و سربار محاسباتی که در این فناوری است برای دستگاه های اینترنت اشیا مناسب نیست. بلاک چین از لحاظ محاسباتی بسیار ارزان است و به دلیل ماهیت تغییر ناپذیر آن و امنیت بالا توانایی غلبه بر چالشهای امنیتی و حریم خصوصی اینترنت اشیا را دارد. با این حال از نظر محاسبات پرخرج، مقیاس پذیری محدود و سربار و تاخیر بسیاری در پهنای باند ایجاد می کند که در تناقض با ماهیت اینترنت اشیا است. اشیا بی شماری که هر بار از آنها استفاده می کنیم به دستگاه های الکترونیکی و مجموعه های پروتکل هایی مجهز شده اند تا ضمن اتصال بهم به اینترنت نیز متصل شوند. در اینترنت اشیا تبادل و پردازش اطلاعات بدون دخالت انسان انجام میگیرد بنابراین به دلیل این استقلال کامل این اشیا باید یکدیگر را شناسایی و تأیید کنند و همچنین از صحت اطلاعات مبادله شده خود اطمینان حاصل کنند در غیر این صورت هدف کاربران مخرب قرار خواهند گرفت و با توجه به اندازه و سایر ویژگی های اینترنت اشیا ایجاد یک سیستم تأیید متمرکز کارآمد تقریباً غیرممکن است[1] .برای اصلاح این محدودیت ما یک معماری سبک وزن، مقیاس پذیر و غیر متمرکز را پیشنهاد می کنیم تا با شناسایی و احراز هویت دستگاه ها از یکپارچگی داده ها و در دسترس بودن محافظت می کند.

۲. خانه هوشمند بر پایه بلاک چین

در اینترنت اشیا تبادل و پردازش اطلاعات بدون دخالت انسان انجام میگیرد. بنابراین به دلیل این استقلال کامل این اشیا باید یکدیگر را شناسایی و تأیید کنند و همچنین از صحت اطلاعات مبادله شده خود اطمینان حاصل کنند در غیر این صورت هدف کاربران مخرب قرار

خواهند گرفت. با توجه به اندازه و سایر ویژگی های اینترنت اشیا ایجاد یک سیستم تأیید متمرکز کارآمد تقریبا غیرممکن است. برای اصلاح این محدودیت ما یک سیستم سبک وزن، مقیاس پذیر و غیر متمرکز را پیشنهاد می کنیم تا با شناسایی و احراز هویت دستگاه ها از یکپارچگی داده ها و در دسترس بودن محافظت می کند. مدل پیشنهادی ما از ترکیب تکنیک تحلیل همبستگی چند متغیره برای تحلیل ترافیک شبکه و شناسایی همبستگی بین ویژگی های ترافیکی و ادغام الگوریتم های LSB که مقیاس پذیر و متناسب با اینترنت اشیا است طراحی شده، سپس ضمن مقایسه با روش های موجود، عملکرد معماری پیشنهادی خود را با استفاده از پارامترهای مختلف مانند توان عملیاتی ارزیابی کرده و به یک راه حل امنیتی کارآمد برای آینده اینترنت اشیا با فناوری بلاک چین پی بردیم.

در هر خانه هوشمند یک بلاک چین خصوصی محلی وجود دارد که مانع تراکنش های خارجی می شود و یک سرفصل سیاست برای اجرای دستور کاربران برای تراکنش ورودی و خروجی دارد. با شروع از تراکنش پیدایش تراکنش هر دستگاه به عنوان یک دفترچه تغییرناپذیر در بلاک چین زنجیر شده است. هر بلوک در موقعیت محلی بلاک چین شامل دو هدر است که همانطور که در شکل بالا نشان داده شده است دارای سربرگ block و header می باشد. سرصفحه بلوک برای جلوگیری از تغییر ناپذیری بلاک چین هش بلوک قبلی را دارد. هدر The policy برای مجوز دستگاهها و اجرای سیاست کنترل صاحب خانه بر سر خانه خود استفاده می شود. همانطور که در گوشه سمت چپ شکل ۲ نشان داده شده است هدر خط مشی دارای چهار پارامتر است.



شکل ۱: ساختار خانه هوشمند

پارامتر "درخواست کننده" به درخواست کننده PK در تراکنش overlay از این رو اشاره دارد. برای دستگاه های محلی این اصل با "شناسه دستگاه" مطابق شکل در ردیف چهارم عنوان سیاست پیشنهادی نشان داده شده است. ستون دوم در هدر پولی عملکرد درخواست شده در تراکنش را نشان می دهد که عبارتند از: ذخیره سازی داده ها را به صورت محلی بر روی ابر ذخیره میکند و دسترسی به داده های ذخیره شده در یک دستگاه دسترسی داشته باشد و همچنین با نظارت به داده های زمان واقعی نیز دسترسی داشته باشید. ستون سوم به عنوان خط مشی شناسه یک دستگاه داخلی در خانه هوشمند است و بطور کلی آخرین ستون کاری را که باید برای

تراکنش انجام شود با ویژگی های قبلی انجام می دهد. بلوک دارای تعدادی تراکنش است و برای هر پارامتر تراکنش در بلاک چین محلی که در گوشه بالا سمت چپ شکل ۱ نشان داده شده است ذخیره می شود. دو پارامتر اول برای زنجیره تراکنش های یک دستگاه مشابه به یکدیگر و شناسایی هر تراکنش در بلاک چین استفاده می شود. "نوع تراکنش" به تراکنشی اطلاق می شود که می تواند تراکنش پیدایش، دسترسی، ذخیره و فروشنده باشد. این تراکنش در نسخه اصلی آن که از شبکه پوشش حاصل می شود ذخیره می شود.

برای افزودن دستگاه به smart home ماینر با به اشتراک گذاشتن کلید دستگاه یک تراکنش اولیه ایجاد می کند. کلید اشتراک گذاری شده بین ماینر و دستگاه در تراکنش ذخیره می شود. در رابطه با تعیین خط مشی صاحب خانه سیاست های خود را مطابق ساختار پیشنهادی ما در شکل ۲ ایجاد می کند و عنوان سیاست را به اولین بلوک اضافه می کند. ماینر از آخرین خط مشی بلاکچین به عنوان سیاست استفاده می کند. هر یک از دستگاه های موجود در منزل ممکن است از داده های داخلی دیگری بخواهد خدمات خاصی را ارائه دهد به عنوان مثال، لامپ چراغ از سنسور حرکتی درخواست می کند تا چراغ ها را به طور خودکار هنگام ورود کسی به خانه روشن کند. برای دستیابی به کنترل کاربری در انجام تراکنش خانه یک کلید مشترک باید از طریق ماینر به دستگاههایی که نیاز به ارتباط مستقیم با یکدیگر دارند، اختصاص یابد. برای تخصیص این کلید ماینر هدر را چک می کند یا از صاحب اجازه درخواست می کند و یک کلید مشترک بین دستگاه ها توزیع می کند. دستگاه ها پس از دریافت کلید مستقیماً تا زمانی که کلید آنها معتبر باشد ارتباط برقرار می کنند. برای اجازه ماینر با ارسال یک پیام کنترل به دستگاه ها کلید توزیع را به عنوان نامعتبر علامت گذاری می کند. کارآیی این روش به دو صورت است: از یک طرف ماینر (مالک) لیستی از دستگاه هایی که داده ها را به اشتراک می گذارند و از سوی دیگر ارتباطات بین دستگاه ها با یک کلید مشترک تأمین می شود. داده های ذخیره شده در ذخیره سازی محلی توسط دستگاه ها تراکنش دیگر ممکن است در داخل خانه باشد. برای ذخیره سازی داده ها به صورت محلی هر دستگاه باید با استفاده از یک کلید اشتراکی به فضای ذخیره شده موجود در آن تأیید شود. برای اعطای کلید دستگاه نیاز به درخواست ماینر دارد و در صورت داشتن مجوز ذخیره ماینر یک کلید مشترک را تولید می کند و کلید را برای مشاوره و ذخیره سازی ارسال می کند. با دریافت کلید حافظه محلی نقطه شروع را ایجاد می کند که شامل کلید مشترک است. با داشتن کلید اشتراکی دستگاه می تواند داده ها را به طور مستقیم در فضای محلی ذخیره کند. دستگاهها ممکن است خواستار ذخیره داده ها در فضای ذخیره سازی ابری باشند که به عنوان ذخیره تراکنش شناخته می شود. ذخیره داده ها در clouds یک فرآیند ناشناس است. برای ذخیره سازی داده ها درخواست کننده به یک نقطه شروع نیاز دارد که حاوی شماره یک بلاک و یک هش است که برای تأیید اعتبار ناشناس برای اهداف خود استفاده می شود. فضای ذخیره‌سازی ابری ممکن است متعلق به SP باشد و تحت مدیریتSP باشد یا توسط صاحب خانه مثلاً Dropbox هزینه و مدیریت شود.

تراکنش احتمالی دیگر "دسترسی" و "مانیتور" تراکنش است که این تراکنش عمدتا توسط صاحب خانه ایجاد می شود تا خانه را هنگامی که او در خارج و یا از SP برای نظارت بر داده های دستگاه ها برای خدمات شخصی مانیتور کند. با استفاده از تراکنش دسترسی از گره های موجود در پوشش این برنامه مشخص می کند که آیا داده های درخواست شده در فضای ذخیره سازی ابر قشر محلی وجود دارد یا خیر. اگر داده ها در محل ذخیره محلی ذخیره شوند ماینر داده ها را از محل ذخیره محلی درخواست کرده و آن را به درخواست کننده ارسال می کند. از طرف دیگر ، اگر داده ها در فضای ابر ذخیره شده باشند ماینر یا داده هایی را از فضای ذخیره ابر درخواست می کند و آن را به درخواست کننده می فرستد یا آخرین هش شماره بلوک و شماره را به درخواست کننده می فرستد.

هنگامی که یک فرد بیش از یک خانه دارد به ماینر مجزا و انبار برای هر یک از خانه ها احتیاج دارد. برای کاهش هزینه و مدیریت هزینه در این مثال، یک توزیع مشترک تعریف شده است. پوشش مشترک شامل حداقل دو خانه هوشمند است که توسط یک ماینر مشترک به طور مرکزی به عنوان یک خانه واحد اداره می شود. پوشش مشترک به یک خانه هوشمند مشابه است با این حال ساختار مشترک بلاک چین قبل از خانه یک خانه هوشمند متفاوت نیست. در بلاکچین مشترک هرکدام دارای یک تراکنش پیدایش است و تراکنش پیدایش همه دستگاه ها به تراکنش پیدایش منزل خود از طریق معدن پوشاننده مشترک زنجیر شده است.

۳.الگوریتم LSB

الگوریتم LSB شامل دو مولفه تراکنش و مدیر بلاک هست. تراکنش،ا رتباط اولیه پایه برای کنترل مبادله اطلاعات در بین هر موجودیت است و مدیر بلاک موجودیتی است برای مدیریت بلوک ها که شامل تولید، تأیید و ذخیره سازی تراکنش شخصی و بلوک تراکنش است.
در LSB الگوریتم های منابع فشرده تر مانند Pow و PoS که به طور معمول در بلاک چین استفاده می شوند را بهینه می کنیم و الگوریتم استنتاج مبتنی بر زمان را پیشنهاد می کنیم. الگوریتم اجماع باید از یک ژنراتور بلوک که به طور تصادفی در بین گره ها انتخاب شده باشد اطمینان حاصل کند و همچنین تعداد بلوک هایی که می تواند تولید کند محدود است. برای معرفی ژنراتورهای بلوک تصادفی هر OBM باید قبل از تولید یک بلاک جدید، منتظر یک زمان تصادفی معروف به دوره انتظار باشد. از آنجایی که مدت انتظار برای هر OBM متفاوت است، ممکن است یک OBM بلوک جدید ایجاد شده توسط آن OBM دیگر شامل یا تراکنش هایی باشد که بطور تصادفی در حوالی تراکنش OBM انجام می شود. در این شرایط این OBM باید این تراکنش را از همان زمان که توسط OBM دیگری در بلاک چین ذخیره می شود از آن خارج کند. نیاز به OBM ها برای انتظار برای زمان تصادفی و تعداد بلوک های تکراری که می توانند همزمان تولید شوند را نیز کاهش می دهد. حداکثر زمان انتظار در دو برابر حداکثر تأخیر تا پایان شبکه روی هم قرار گرفته است. هنگامی که یک بلوک جدید تولید می شود آن را به همه گره های پوشش دیگر پخش می کند تا بتواند به بلاک چین اضافه شود.
فرض می کنیم که هر گره در لایه های باز توسط یک کلید عمومی (PK) شناخته شده است. گره ها از PK جدید برای ایجاد اطمینان از ناشناس بودن استفاده می کنند. روکش ، همانطور که در شکل ۱ نشان داده شده است شامل اشخاص مختلفی است که به عنوان overlay nodes شناخته می شوند از جمله خانه هوشمند توسط LocalBM (LBM) که در بخش بعدی معرفی خواهد شد (تلفن های همراه، سرویس دهنده های ارائه دهنده خدمات (SP) و فضای ذخیره سازی ابری (توسط دستگاه های خانگی هوشمند برای ذخیره داده ها استفاده می شود). شبکه روی هم می تواند به طور بالقوه از تعداد گره ها تشکیل شود. بنابراین برای اطمینان از مقیاس پذیری فرض می کنیم که کلید عمومی بلاکچین با زیر مجموعه ای از لایه های اضافه اداره می شود. ما فرض می کنیم که از یک الگوریتم خوشه بندی برای گروه بندی گره ها در خوشه ها استفاده می شود که با هر یک از اقلیم ها یک سر خوشه (CH) را انتخاب می کنند CH ها مسئول مدیریت بلاکچین هستند و از این رو به آنها Overlay Block Mangers (OBMs) گفته می شود. علاوه بر این CHs تراکنش ها ورودی و خروجی را که از اعضای آنها جمع می شوند یا پردازش می کنند. انتظار می رود گره انتخاب شده به عنوان CH برای مدت زمان طولانی به صورت آنلاین و منابع مناسب برای پردازش بلوک ها و تراکنش ها ادامه یابد. از آنجا که پایه های بنیادی توسط CH ها انجام می شوند LSB تحت تأثیر دینامیک IoTdevice یعنی پیوستن و ترک دستگاهها قرار نمی گیرد. تراکنش ها موجود در این طریق را می توان بیشتر به "اقدامات مربوط به امضاهای منفرد طبقه بندی کرد که فقط حاوی امضای تراکنش گر و تراکنش ها چند منظوره" هستند که با ایجاد کننده تراکنش ها (درخواست کننده) و گیرنده (درخواست کننده) امضا می شوند. بیشتر تراکنش ها در LSB چند چهره ای هستند. به عنوان مثال در جایی که از تراکنش ها یک امضا استفاده می شود. نخستین شناسه برای تراکنش در حالی که تراکنش دومین شناسه قبلی گره درخواست کننده است. بنابراین تمام تراکنش ها ایجاد شده توسط یک درخواست کننده با هم زنجیر شده اند. این کار پس از پیگیری و امضای درخواست کننده و درخواست کننده انجام می شود. وقتی که تراکنش توسط گیرنده دریافت می شود Latter signature اضافه می شود. هفتمین شناسه تراکنش های خروجی توسط درخواست کننده تعیین و ثبت می شود. شماره خروجی شامل ۳ مورد زیر است:

- تعداد کل تراکنش ها ایجاد شده توسط درخواست کننده که توسط شخص پذیرفته شده پذیرفته شده است
- تعداد کل تراکنش ها رد شده توسط فرد متقاضی
- هش از PK که درخواست کننده برای آن استفاده می کند

تراکنش بعدی اولین دو شناسه اول اطلاعاتی را ارائه می دهند که برای محاسبه ی ورود به سیستم درخواست کننده ضروری است که در الگوریتم توزیع شده به شرح در بخش بعدی استفاده می شود. آخرین خروجی لازم برای تأیید آینده درخواست کننده ضروری است، زیرا گره های روی هم باعث تغییر PK مورد استفاده برای تراکنش ها جدید می شوند. شخص ثالث در یک انتقال داده چند منظوره یعنی "ابرداده" اطلاعاتی راجع به مورد نظر و دستگاه هوشمندسازی که هدف این عمل است که ارائه می دهد. یک تراکنش منفرد دارای

ساختار مشابهی است ، اما PK و امضا فوق داده و خروجی [۰] و [۱] را به عنوان تنها یک گره رویه درگیر می کند. توجه داشته باشید که تراکنش ها چندرسانه ای و تک امضا به صورت جداگانه سازماندهی می شوند زیرا خروجی های مربوطه متفاوت هستند.

تراکنش ها اصلی در پوشش به شرح زیر است:

پیدایش: هر گره رویه ابتدا نباید یک توزیع پراکندگی را ایجاد کند که به عنوان نقطه شروع کاربری پیشگامان در بلاکچین باشد.

مخزن ذخیره: یک گره رویه یک تراکنش مخزن ذخیره ایجاد می کند تا داده ها را در فضای ذخیره ابری ذخیره کند.

دسترسی: یک تراکنش دسترسی توسط یک گره an overlay ایجاد می شود تا درخواست داده های ذخیره شده از یک دستگاه به عنوان مثال (درخواست کننده) ممکن است تمام داده های ذخیره شده توسط یک دستگاه (درخواست کننده) را برای هفته گذشته درخواست کند.

در LBS جریان داده ها از جریان تراکنش ها جدا می شود. بنابراین در پاسخ به دسترسی یا مانیتور انتقال دستگاه متقاضی داده ها را پس از تأیید اینکه دسترسی به داده ها مجاز به داده ها است یک بسته (داده) جداگانه به درخواست کننده ارسال می کند. به طور مشابه برای تراکنش ها مبادله داده های ایجاد شده توسط درخواست کننده از تراکنش بطور کامل مشخص می شوند. بسته های داده ای که پخش می شوند بسته های داده یکپارچه هستند و می توانند مسیرهای بهینه را از طریق شبکه پوشش با استفاده از پروتکل های استفاده از مسیریابی مانند OSPF مسیریابی کنند. تراکنش ها لایه باز در عمومی ذخیره می شوند و هر بلوک در بلاکچین شامل دو بخش اصلی یعنی تراکنش ها و هدر بلوک است. هدر بلوک شامل موارد زیر است: هش بلوک قبلی ، شناسه بلوک ژنراتور و امضاهای تأییدکننده. هش بلوک قبلی در بلاکچین عمومی امکان تغییرپذیری وجود دارد. اگر یک مهاجم سعی کند یک تراکنش قبلی را ذخیره کند هش بلوک مربوطه که در بلوک بعدی ذخیره شده است دیگر سازگار نخواهد بود و بدین ترتیب این حمله را افشا می کند. "شناسه مولد بلوک" و "امضاهای تأییدکنندگان" در این بخش به بحث و گفتگو خواهد پرداخت. مشابه بیت کوین ، چندین تراکنش با هم گروه بندی شده و سپس به عنوان یک بلوک پردازش می شوند AdBlock .می تواند حداکثر تراکنش ها T max را ذخیره کند. مقدار t max حداکثر بر کارایی بلاکچین تأثیر می گذارد به گونه ای که با استفاده از حداکثر بزرگتر تراکنش ها بیشتری را می توان در یک بلوک واحد ذخیره کرد.

هنگامی که OBM تراکنش Y را دریافت می کند اولین بار بررسی می کند که آیا فرد متقاضی این تراکنش شامل خوشه درون ذات باشد. OBM یک لیست کلیدی (اساساً یک لیست کنترل دسترسی ساده شده) متشکل از Pairs PK درخواست کننده دارد که از درخواست کننده هایی که مجاز به ارسال تراکنش ها به متقاضیان خاص هستند نشان می دهد. این لیست کلیدی توسط یک عضو خوشه به روز می شود تا به سایر لایه های اضافه اجازه ارسال تراکنش ها به آن را بدهد. یک فرد متقاضی ممکن است ارزش لیست پایینتر را در لیست کلید OBM به عنوان "پخش" قرار دهد و این توجیه می کند که کلیه تراکنشی را که حاوی PPK آن به عنوان PK درخواست کننده باشد دریافت می کند. اگر متقاضی و متقاضی تراکنش ورودی Y با ورود به لیست کلیدها مطابقت داشته باشند OBM تراکنش را به متقاضی ارسال می کند (که در خوشه آن است و بنابراین مستقیماً با OBM متصل می شود). اگر فرد گیرنده در Y متعلق به حساب OBM نباشد آن تراکنش به تمام OBM های دیگر پخش می شود. کلیه تراکنش ها در انتظار هر OBM در یک استخر تراکنش ذخیره می شوند. وقتی اندازه استخر در حال تبدیل شدن به T max می شود OBM روند ایجاد بلوک جدید را با استفاده از الگوریتم اجماع شروع می کند.

۴.الگوریتم اجماع

همانطور که در LSB گفته شد ما به جای گزینه های فشرده تر مانند PoW و PoS که بطور معمول دربلاکچین استفاده می شوند، الگوریتم محوریت مبتنی بر زمان را پیشنهاد می کنیم. در LSB الگوریتم های منابع فشرده تر مانند Pow و PoS که به طور معمول در بلاک چین استفاده می شوند را بهینه می کنیم و الگوریتم استنتاج مبتنی بر زمان را پیشنهاد می کنیم. الگوریتم اجماع باید از یک ژنراتور بلوک که به طور تصادفی در بین گره ها انتخاب شده باشد اطمینان حاصل کند و همچنین تعداد بلوک هایی که می تواند تولید

کند محدود است. برای معرفی ژنراتورهای بلوک تصادفی هر OBM باید قبل از تولید یک بلاک جدید، منتظر یک زمان تصادفی معروف به دوره انتظار باشد. از آنجایی که مدت انتظار برای هر OBM متفاوت است، ممکن است یک OBM بلوک جدید ایجاد شده توسط آن OBM دیگر شامل یا تراکنش هایی باشد که بطور تصادفی در حوالی تراکنش OBM انجام می شود. در این شرایط این OBM باید این تراکنش را از همان زمان که توسط OBM دیگری در بلاک چین ذخیره می شود از آن خارج کند. نیاز به OBM ها برای انتظار برای زمان تصادفی و تعداد بلوک های تکراری که می توانند همزمان تولید شوند را نیز کاهش می دهد. حداکثر زمان انتظار در دو برابر حداکثر تأخیر تا پایان شبکه روی هم قرار گرفته است. هنگامی که یک بلوک جدید تولید می شود آن را به همه گره های پوشش دیگر پخش می کند تا بتواند به بلاک چین اضافه شود.

برای محافظت از پوشش در برابر OBM مخرب که به طور بالقوه می تواند تعداد زیادی از بلوک های بدون تراکنش ها را که منجر به حمله ضمائم می شود تولید کند. دوره ای که بلوک های سازنده OBM آن محدود می شود به گونه ای است که فقط یک بلوک از طریق یک بازه ایجاد می شود. دوره اجماع تنظیم شده توسط دوره مدیریت توزیع شده (DTM) تنظیم می شود. برای جلوگیری از اینکه همیشه ادعا شود OBM یک دوره انتظار کوتاه دارد OBM همسایه مرتباً تحت نظارت قرار می گیرد که OBM باعث ایجاد بلوک های جدید در ایجاد دوره انتظار می شود. اگر تعداد چنین بلاکچین از آستانه ای فراتر رود که براساس برنامه های طراحان بلاکچین مشخص شده است OBM ها بلوک ایجاد شده توسط همسایه خود را رها می کنند.

۵. ارزیابی سیستم

در این بخش ما امنیت کیفی و خصوصی سازی و همچنین ارزیابی عملکرد کمی را ارائه می دهیم و با مقایسه جدولی حملات احتمالی الگوریتم LSB را در سیستم پیشنهادی بررسی خواهیم کرد. همانطور که قبلا گفتیم چارچوب ما بلاک‌چین را برای اینترنت اشیا با ارائه سطوح مختلف بلاک‌چین بهینه سازی می کند. هر لایه دارای ویژگی های منحصر به فرد است که باعث می شود با لایه های دیگر و بلاک‌چین تفاوت داشته باشد که تفاوت های کلیدی بین بلاک‌چین و سیستم پیشنهادی مورد بحث است.

۵,۱تجزیه و تحلیل امنیت و حفظ حریم خصوصی

در این بخش درباره امنیت حریم خصوصی و تحمل LSB بحث می کنیم. فرض بر این است که طرف مقابل می تواند OBM وسیله ای در خانه هوشمند در شبکه باشد. خرابکاران می توانند ارتباطات را خراب کنند، تراکنش ها را خراب کند، تراکنش ها و بلوک های کاذب ایجاد کنند، داده ها را در ذخیره سازی تغییر دهند یا حذف کنند، تراکنش ها چندگانه را در تلاش برای شناسایی نام یک گره انجام دهند و تراکنش ها جعلی را امضا کنند تا گره های تقلبی را قانونی کنند و همچنین فرض می کنیم که از روشهای استاندارد تأیید رمزنگاری در خانه هوشمند و پوشش بالایی استفاده می شود که توسط مهاجمان به خطر نمی افتد.

جدول ۱ خلاصه سازوکارهای مختلفی را برای سیستم پیشنهادی فراهم می کند تا الزامات اصلی امنیتی را برآورده سازند. در جدول ۲ ما ۱۲ حمله امنیتی ویژه را که شبکه های IoT یا بلاکچین ها به ویژه آسیب پذیر هستند را تشریح می کنند و چگونگی محافظت از LSB در برابر آنها را بیان می کنند. این معیارها هر حمله را بر اساس معیارهای زیر ارزیابی می کنند:

- زمان: زمان تجمعی برای حمله کننده برای اولین بار آسیب پذیری را شناسایی می کند و متعاقبا برنامه ریزی می کند که حمله موفقی را انجام دهد.
- خبرگی: این امر به طور کلی بیانگر آن است که مهاجم باید در مورد آن باشد. اصول زیربنایی برای برپایی حمله می باشد.
- دانش: اطلاعات ویژه ای که در مورد سیستم هدف در دسترس است، به عنوان مثال ، تضمین امنیتی
- فرصت: مدت زمان ماندگاری (به طور مداوم یا متناوب) دسترسی به سیستم های مورد نیاز برای تجهیزات حمله
- تجهیزات: نرم افزار و یا سخت افزار لازم برای انجام حمله LSB در مقایسه با مقاومت بالا در برابر هفت حمله و مقاومت بالا به سه حمله قرار دارد که این نشان می دهد که LSB بسیار مطمئن است.

جدول ۱- بحث الزامات امنیتی

۵,۲حریم خصوصی

سیستم پیشنهادی از ناشناسی و کنترل کاربر برای محافظت از حریم شخصی کاربران در پوشش خانه هوشمند و فضای ذخیره سازی Cloud استفاده می کند. با استفاده از PK های قابل تغییر به عنوان گره های متغیر سطح مشابهی از ناشناس بودن و حریم خصوصی را که در سایر سیستم های مبتنی بر BC (مانند بیت کوین) تجربه می شود، معرفی می کند. در برخی از برنامه های IoT، دو نقطه پایانی که در حال برقراری ارتباط هستند ممکن است نیاز به شناخت هویت واقعی دیگری داشته باشد. به عنوان مثال، یک شرکت بیمه خانه نیاز به هویت واقعی صاحب خانه هوشمند که بیمه می کند می داند. در این موارد ژنراتور مربوط به انتقال از یک PK منحصر به فرد برای ارتباط با هر گره پوشش استفاده می کند. تراکنش های ذخیره شده در عمومی بلاکچین با استفاده از درخواست کننده PK برای محافظت از حریم خصوصی گره های پوشش در برابر مهاجمین که سعی در خواندن داده ها در فوق داده یک تراکنش مالتی دارند رمزگذاری شده اند.

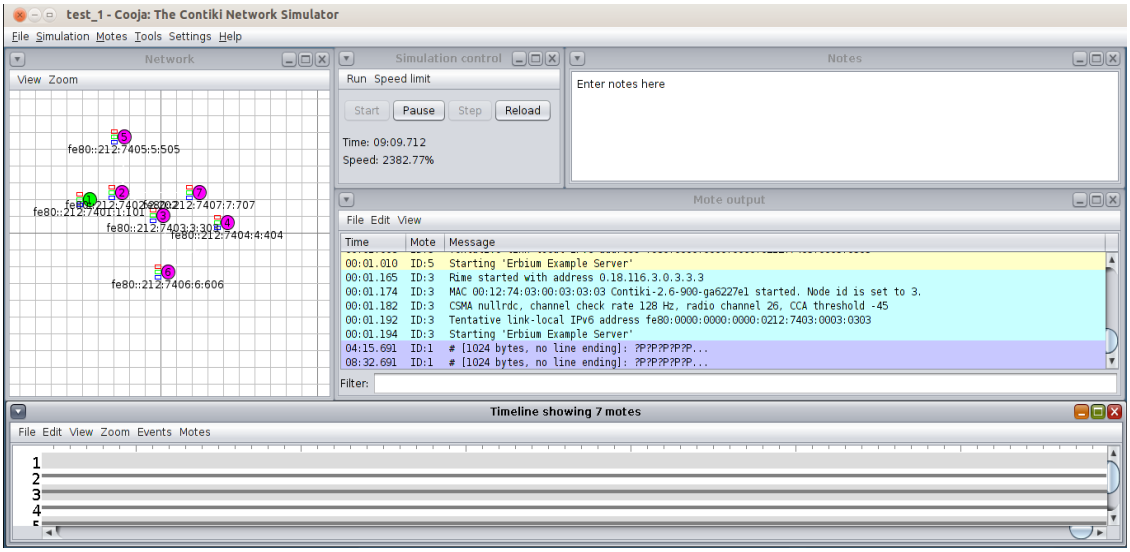
در خانه هوشمند LBM به سیاست های صاحب خانه برای اطمینان از کنترل داده های مبادله شده از این رو از حریم خصوصی محافظت می کند. حافظه ابری قادر به استفاده از داده های مختلف یک گره پوششی برای شناسایی هویت واقعی خود است. این ناشناسی دستگاه ها گره پوشش از اعتبارهای مختلفی برای ذخیره داده های دستگاه های خود استفاده می کند. این مانع از شناسایی ابر دستگاه های مختلف گره روی هم می شود.

۵,۳تحمل خطا

تحمل خطا اندازه گیری چگونگی مقاومت در برابر معماری برای خرابی گره ها است. از بخش قبلی بدیهی است که LBM و OBM عملکردهای مختلفی را اجرا می کنند و عدم موفقیت این گره ها به طور احتمالی می تواند بر عملکرد طبیعی LSB تأثیر بگذارد. عدم موفقیت LBM می تواند خانه هوشمند مربوطه و دستگاههای مرتبط را از روی اتصال جدا کند. این دستگاه هوشمند می تواند داده ها را به صورت محلی به اشتراک بگذارد اما قادر به ذخیره داده ها در فضای ابری یا ارتباط با سایر دستگاه های پوشش نخواهد بود. در صورتی OBM پوشش را ترک می کند که اعضای خوشه با این OBM در ارتباط باشند که هیچ خدمتی را دریافت نمی کنند و حتی می توانید به راحتی یک OBM جدید را برای همکاری انتخاب کنیم. عزیمت OBM همچنین ممکن است روی خروجی تأثیر بگذارد زیرا OBM های کمتری برای تولید بلوک وجود دارد. با این وجود مکانیسم DTM که در فصل گذشته بیان شده است می تواند وضعیت دستکاری را انجام دهد. خروج چندین OBM ممکن است به دلیل اقدامات مربوط به ساز و کار اعتماد سازشده ، امنیت را نیز تحت تأثیر قرار دهد.

۶.سنجش عملکرد

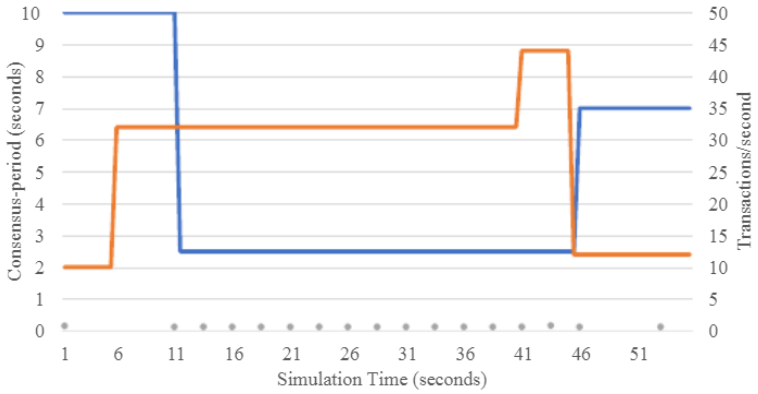
در این بخش ، ما ارزیابی های گسترده ای از جنبه های مختلف عملکرد LSB ارائه می دهیم. سنجش عملکرد ما از طریق پیاده سازی الگوریتم LSB در پایتون و همچنین پیاده سازی خانه هوشمند بر پایه پروتکل 6LowPan در لینوکس اجرا می شود.از Cooja برای بررسی عملکرد ردیف خانه هوشمند استفاده می کنیم. Cooja برای ارزیابی وسایل کم مصرف مناسب است و در دسترس بودن اجرای پروتکل های مختلف آگاهی IoT را مناسب می کند. همچنین برای ارزیابی عملکرد پوشش استفاده می کنیم زیرا برای تجزیه و تحلیل شبکه های همتا به هم استفاده می شود. برای شبیه سازی Cooja شبکه ای را متشکل از ۶ گره روی هم در نظر می گیریم. ما فرض می کنیم که T max حداکثر ۱۰ باشد. ما فرض می کنیم که درخواست کنندگان چهار تراکنش را ایجاد می کنند. به تنظیمات فوق به عنوان پیش فرض اصطلاحات گفته می شود و در شبیه سازی ها مورد استفاده قرار می گیرد مگر اینکه در غیر این صورت صریحاً یادداشت شود.



شکل۲– پیاده سازی و شبیه سازی در Cooja

در بقیه این بخش ما زمان پردازش POW را در بخش بعدی ارزیابی می کنیم. عملکرد ردیف خانه هوشمند در بخش بعدی ارزیابی می شود. در مرحله بعدی ما زمان تعیین شده را که گره رویه در هنگام درخواست داده های خانه در بخش بعدی به نمایش می گذارد را ارزیابی می کنیم. اعتماد توزیع شده و تأثیرات آن بر امنیت و عملکرد پوشش در بخش بعدی بررسی شده است.

شکل ۳- ارزیابی سربار زمان در LBM



شکل ۴– ارزیابی زمان در شبیه سازی Cooja

شبیه سازی هایی را با استفاده از Cooja برای ارزیابی میزان مصرف انرژی و سربار زمان LBM انجام می دهیم. این امر به این دلیل است که LBM پرمصرف ترین وسیله مصرف کننده در این شهر است زیرا همه تراکنش ها را انجام می دهد و بسیاری از عملیات هش کردن و رمزگذاری (هم متقارن و هم نامتقارن) را انجام می دهد. در مقابل دستگاه های IoT باید وظایف بسیار ساده ای را انجام دهند که بیشترین محاسبات مربوط به رمزگذاری متقارن است. نشان داده شده است که بیشتر دستگاه های IoT از قابلیت های مناسب برای انجام این کار برخوردار هستند. ارزیابی کاملی از ردیف خانه هوشمند از کارهای قبلی ما ارائه شده است.

ما از IPv6 بیش از LowPower بی سیم شبکه های ناحیه شخصی شخصی (6LoWPAN) به عنوان پروتکل ارتباطی در شبیه سازی استفاده می کنیم از آنجا که برای یک محیط خانه هوشمند به محدودیت های منبع دسترسی پیدا می کند. ما در هر ۱۰ ثانیه سه حسگر حرکتی z1 (که دستگاه های smart home را تقلید می کنند) شبیه سازی می کنیم (شکل ۲)که داده ها را مستقیماً به LBM (شبیه سازی شده به عنوان یک موتور z1) ارسال می کنند. هر یک از شبیه سازی ها به مدت ۳ دقیقه انجام می شود و نتایج در طول این مدت به طور متوسط انجام می شود. حافظه ابری برای ذخیره سازی داده ها به طور مستقیم به LBM متصل است. برای ارائه یک ارزیابی جامع ما تراکنش ها ذخیره و دسترسی را شبیه سازی می کنیم. برای تراکنش ذخیره سازی دو الگوی متفاوت و واقع گرایانه ترافیک مختلف را شبیه سازی کردیم:

- تناوبی: در این تنظیم دستگاه ها بطور دوره ای داده ها را در فضای ذخیره سازی ابر ذخیره می کنند (مشابه یک ترموستات هوشمند که به طور دوره ای در ابر می خواند دمای خواندن دما).
- مبتنی بر پرس و جو: در دستگاه ها هنگامی که یک پرس و جو از کاربر دریافت کردند داده ها را ذخیره می کنند که به عنوان مثال یک نمایشگر صاحب خانه دوربین امنیتی را متصل کرد تا بررسی کند آیا کسی به درب نزدیک شده است یا خیر

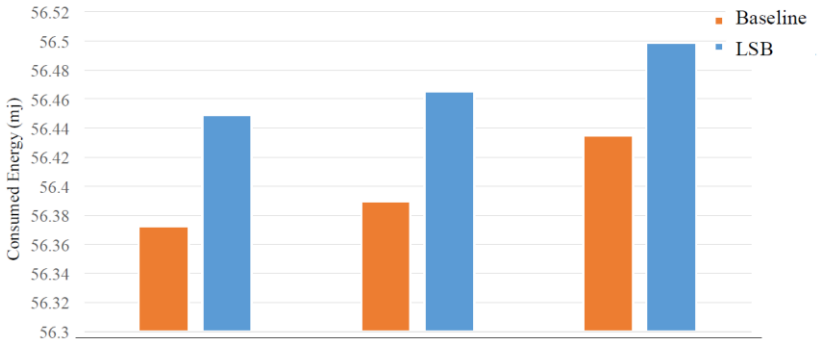
معیارهای زیر را ارزیابی می کنیم:

- سربار زمان: به زمان پردازش برای هر تراکنش در LBM اشاره دارد و از زمانی که تراکنش در LBM دریافت می شود اندازه گیری می شود تا اینکه پاسخ مناسب به درخواست کننده ارسال شود.
- مصرف انرژی: به انرژی مصرف شده توسط LBM برای پردازش تراکنش ها اشاره دارد.

شکل ۴ نتایج مربوط به سربار زمان را نشان می دهد. LSB زمان بیشتری را برای پردازش بسته ها نسبت به خط پایه مصرف می کند که می تواند به عملیات رمزگذاری و هشدار اضافی نسبت داد. در بدترین حالت تراکنش مبتنی بر پرس و جو اضافه کار اضافی تولید شده توسط LSB 20ms است.

شکل ۵ نتایج مصرف انرژی را تشریح می کند. همانطور که مشهود است LSB مصرف انرژی را ۰,۰۷ (میلی متر) افزایش می دهد. جدول در پایین شکل ۵ خط مصرف انرژی برای ۳ وظیفه اصلی انجام شده توسط LBM را نشان می دهد یعنی: CPU ، انتقال (Tx) و گوش دادن (Lx). مصرف انرژی توسط CPU به دلیل رمزگذاری و هشدار در LSB تقریباً ۰,۰۰۲ (mj) در LSB افزایش می یابد. LSB

منجر به بسته های طولانی تر (به دلیل رمزگذاری و هشدار) می شود و این باعث می شود که میزان مصرف انرژی انتقال در مقایسه با پایه دو برابر شود. لازم به ذکر است که ما در ارزیابی های خود چرخه وظیفه رادیویی ۱۰۰٪ را در نظر گرفتیم (یعنی رادیو همیشه روشن است). اگر رادیو بصورت بی وقفه برای صرفه جویی در انرژی روشن شود آنگاه صدای بالای ناشی از شنوایی LSB بیشتر می شود. با این حال حتی با فرض یک چرخه وظیفه بسیار با شدت ۱ درصد افزایش نسبی شنوایی فقط ۶۰ درصد خواهد بود.



	Access			Store-Query			Store-Period		
	CPU	Tx	Lx	CPU	Tx	Lx	CPU	Tx	Lx
Baseline	0.0103	0.0102	56.3489	0.0117	0.0357	56.3393	0.0121	0.0549	56.3645
LSB	0.0127	0.0834	56.3496	0.0132	0.1106	56.3379	0.0133	0.1166	56.3657

شکل ۵- ارزیابی مصرف انرژی

۶. نتیجه گیری

اگرچه بلاکچین یک فناوری موثر برای تأمین امنیت و حفظ حریم خصوصی IoT است و کاربرد آن در زمینه IoT چالش های ویژه ای مانند پیچیدگی، سرریز پهنای باند، سرعت و مقیاس پذیری را شامل می شود. راه حلهای امنیتی موجود لزوماً برای IoT به دلیل مصرف انرژی بالا و پردازش بالای سربار مناسب نیستند. در این مقاله ما به تشریح اجزای اصلی مختلف ردیف خانه هوشمند پرداخته و در مورد تراکنش های مختلف و روشهای مرتبط با آن بحث کرده ایم. ما همچنین تجزیه و تحلیل همه جانبه ای را در مورد امنیت و حریم خصوصی آن ارائه کردیم. نتایج شبیه سازی نشان می دهد که هزینه های اصلی ناشی از روش ما برای devices IoT با منابع کم و قابل کنترل هستند. ما استدلال می کنیم که این سربارها ارزش سنگین بودن آنها به منافع قابل توجه امنیت و حفظ حریم خصوصی را دارند. این تحقیق با هدف بهینه سازی بلاکچین در زمینه خانه های هوشمند است که با استفاده ازمعماری مبتنی بر بلاکچین امنیت و حریم خصوصی غیرمتمرکز را فراهم می کند ولی بدلیل استفاده از انرژی تأخیر و سربار محاسباتی که برای اکثر دستگاه های اینترنت اشیا مناسب نیستند ما یک نوع سبک از بلاکچین برای استفاده در اینترنت اشیا را با بهینه سازی کار اثبات (POW) و با استفاده از الگوریتم LSBبه جای الگوریتم های منابع فشرده تر مانندPoW و PoS که به طور معمول در بلاک چین استفاده می شوند، الگوریتم استنتاج مبتنی بر زمان را جایگزین کردیم. مدل پیشنهادی ما از ترکیب تکنیک تحلیل همبستگی چند متغیره برای تحلیل ترافیک شبکه و شناسایی همبستگی بین ویژگی های ترافیکی و ادغام الگوریتم های LSB که مقیاس پذیر و متناسب با اینترنت اشیا است طراحی شده است. نتایج شبیه سازی نشان می دهد که معماری پیشنهادی ما پهنای باند و زمان پردازش را در مقایسه با بلاکچین های کلاسیک کاهش می دهد. علاوه بر این صاحبان smart home خدمات بدون تأخیر اضافی تراکنش ها جابجایی (یعنی ارتباطات منازل هوشمند) دریافت می کنند و با تأخیر قابل درک اندک برای تراکنش ها امنیت و حریم خصوصی بالایی را برای کاربران IoT به ارمغان می آورد.

منابع

[1] S. S. K. R. J. Ali Dorri, "Towards an Optimized BlockChain for IoT," *IoTDI,* 2017.

[2] S. S. K. R. J. Ali Dorri, "Blockchain in internet of things: Challenges and Solutions," *Computers and Society,* 2016.

[3] S. S. a. A. Bilami, "Compressed and distributed hostidentity protocol for end-to-end security in the iot," *International Conference on Next Generation Networks and Services(NGNS),* 2014.

[4] Y. X. a. C. L. P. C. J. Liu, "Authentication and accesscontrol in the internet of things," *International Conferenceon Distributed Computing Systems Workshops,* 2012.

[5] M. S. H. H. G. V. S. a. R. B. S. Notra, "An experimental study of security and privacy risks with emerginghousehold appliances," *Communications and Network Security (CNS),* 2014.

[6] D. C. D. E. a. R. B. V. Sivaraman, "Smart-phones attackingsmart-homes," *in Proceedings of the 9th ACM Conference on Security &Privacy in Wireless and Mobile Networks. ACM,* 2016.