دوفصلنامه محاسبات و سامانه‌های توزیع شده
www.jdcs.ir

ارائه یک مدل امنیتی مبتنی بر قراردادهای هوشمند بلاک چین جهت بهبود احراز هویت در اینترنت اشیا

محمد سعید صفایی صادق [۱]، شمس اله قنبری [۲]
دانشگاه آزاد اسلامی واحد آشتیان [۱و۲]

چکیده

اینترنت اشیا[۱] برای اولین بار در سال ۱۹۹۹ توسط کوین اشتون[۲] مورداستفاده قرار گرفت و بر اساس آمار منتشرشده از موسسه تحقیقاتی و پژوهشی IDC به‌عنوان یکی از پردرآمدترین پروژه‌هایی است که از سال ۲۰۰۶ به بعد ظهور کرد. یکی از مهم‌ترین مسائل در اینترنت اشیا مسئله امنیت ، تحقیقات حاکی از آن است که معماری اینترنت اشیا دارای مدلی سه لایه است. این تحقیق با استفاده قراردادهای هوشمند بلاک چین یک مدل ۵ لایه را برای اینترنت اشیا ارائه می‌دهد و با تحلیل و بررسی مدل پیشنهادی نشان می‌دهد که معماری ۵ لایه، نسبت به مدل ۳ لایه در راستای بهبود مقاومت در برابر مداخله خارجی و همچنین اعتمادپذیری غیرمتمرکز، یک سرویس امن احراز هویت و صلاحیت را فراهم خواهد کرد. نتایج این تحقیق نشان می‌دهد روش مبتنی بر بلاک چین برای افزایش امنیت حریم خصوصی و قابلیت کنترل، راه‌حلی عملی برای مسئله امنیت اینترنت اشیا خواهد بود.

کلیدواژه‌ها: اینترنت اشیا، بلاک چین، امنیت، احراز هویت، معماری اینترنت اشیا، قراردادهای هوشمند بلاک چین

Email: myrshg@Gmail.com

[۱] IOT (Internet of Things)
[۲] Kevin Ashton

تاریخچه مقاله:
تاریخ ارسال:۹۷/۶/۱
تاریخ اصلاحات:۹۷/۱۰/۱
تاریخ پذیرش:۹۷/۱۲/۱۰
تاریخ انتشار:۹۷/۱۲/۲۲

A Security Model Based on Block Chain Smart Contracts for Improve Authentication on Internet of Things

Mohammad Saeid Safaei Sadegh[۱] and Shamsollah Ghanbari[۲]

[1,2] Islamic Azad University Branch of Ashtian

Abstract

The internet has been developed for the first time in ۱۹۹۹ by Kevin Ashton, based on statistics published by research and research institute IDC as one of the highest - earning projects since ۲۰۰۶. One of the most important issues on the internet research indicates that the architecture of the internet has a three - layer model.This study presents a five - layer model for the internet by analyzing the proposed model, and by analyzing and examining the proposed model, the proposed model will provide a secure authentication service relative to the three layer models in order to improve the resistance against external intervention as well as Distributed confidentiality. The results of this study show that the blockchain - based method for increasing privacy security and capability of control will be a practical solution to the issue of internet security.

Keywords:
IOT
Block chain
Security
Smart contract distributed ledger

روش ارجاع به مقاله: م. صـــفایی صـــادق، ش. قنبری، ارائه یک مدل امنیتی مبتنی بر قراردادهای هوشمند بلاک چین جهت بهبود احراز هویت در اینترنت اشیاء، دوفصلنامه محاسبات و سامانه های توزیع شده، سال دوم، شماره اول، شماره پیاپی ۳، سال ۱۳۹۸، ص ۱-۱۶

۱- مقدمه

اینترنت اشیا مفهومی است که در آن اشیای فیزیکی به اینترنت وصل می‌شوند و با اشیای دیگر در ارتباط قرار می‌گیرند و بدین ترتیب از دستگاه‌های ساده به دستگاه‌های هوشمند تبدیل می‌گردند.

رشد فعلی جوامع و تحول سریع در فناوری ارتباطات، موجب افزایش تعداد دستگاه‌های الکترونیکی مناسب در بسیاری از حوزه‌ها گشته است. اینترنت اشیا، به‌صورت مجموعه‌ای از فناوری‌ها از جمله شبکه‌های حسگر بی‌سیم (WSN) و شناسایی فرکانس رادیویی (RFID) پدید آمده است که توانمندی‌هایی را برای حس، به‌کارگیری و برقراری ارتباط در اینترنت فراهم کرده است [۱,۲].

معماری سنتی که غالباً در اینترنت استفاده می‌شود ممکن است نتواند نیازهای اینترنت اشیاء را برآورده نماید. امروزه معماری سرویس گرا و یا انواع معماری‌های لایه‌ای و انعطاف‌پذیر به‌عنوان راهکار ارائه‌شده است و همان‌طور که در جدول ۱ می‌بینیم، از آن به‌عنوان معماری ۳ لایه نیز یاد می‌شود [۳].

جدول ۱: مدل معماری ۳ لایه اینترنت اشیا

لایه	نام لایه	کاربرد
۱	Network of Things	شامل هوشمند سازها یا فعال‌کننده‌ها
۳	Application	شامل بسترهای نرم افزاری موردنیاز جهت به‌کارگیری اطلاعات
۲	Cloud Computing (service oriented)	پردازش‌های مبتنی بر سرویس جهت پوشش دهی کامل تجهیزات فعال‌کننده

لایه اول: این لایه شامل هوشمند سازها یا فعال‌کننده‌ها هست. در این لایه تجهیزاتی که امکان اتصال به کالاها را داشته درعین‌حال امکان برقراری ارتباط بی‌سیم با شبکه‌های موجود را نیز دارا می‌باشند قرار داده‌شده است. این تجهیزات دارای تنوع و گوناگونی فراوانی بوده که بنا به نیاز و نوع خدمات موردنظر و کارایی آن‌ها مورداستفاده قرار می‌گیرد مانند RFIDها، انواع حسگرها، میکروچیپ ها، تجهیزات پردازش تصویری و... گاهی جهت پوشش دهی کامل اشیاء نیاز به استفاده از ترکیبی از این تجهیزات است که مستلزم شناخت نوع خدمت و کالا، فرایندی که باید طی شود و کاربرد نهایی هست [۴].

لایه دوم: در این لایه ترکیبی از انواع شبکه‌های مختلف راداریم که جهت پوشش دهی کامل تجهیزات فعال‌کننده قابل‌استفاده می‌باشند تا تمامی اشیاء امکان اتصال به اینترنت را داشته و اطلاعات جمع‌آوری‌شده توسط آن‌ها به‌صورت یکپارچه به سیستم مرکزی ارسال گردد. با به‌کارگیری این شبکه‌ها، اطلاعات جمع-آوری شده کاملاً به‌روز، دقیق و قابل‌اطمینان بوده و نیز سرعت دریافت، تجزیه‌وتحلیل این اطلاعات بسیار چشم‌گیر است.

لایه سوم: در این لایه بسترهای نرم‌افزاری موردنیاز جهت به‌کارگیری اطلاعات جمع‌آوری‌شده شرح داده می‌شود. این بسترها که به‌نوعی به‌عنوان یک رابط کاربردی عمل می‌نمایند امکان مدیریت کامل اشیاء را از طریق درگاه اینترنت فراهم می‌آورند. این نرم‌افزارها می‌باید انعطاف‌پذیر بوده و سرویس‌های موردنظر کاربر را متناسب با نوع خدمت برایش فراهم نمایند. همچنین با پیاده‌سازی این نرم‌افزارها می‌باید امکان هماهنگی بین فرایندها فراهم شود [۴].

با توجه به اینکه بسترهای اینترنت اشیا مانند Cloud (منبع گرا) و Grid (برنامه گرا)، به‌صورت

غیرمتمرکز می‌باشند، یک روش امنیتی مبتنی بر خرد جمعی می‌تواند در افزایش امنیت اینترنت اشیا بسیار مؤثر باشد. با توجه به ظهور و توسعه بلاک چین چنین مدلی قابل‌دسترسی هست.

مسئله اعتماد به دستگاه‌های اطلاعاتی درجایی که تائید یا مکانیسم‌های ارزیابی وجود ندارد، به‌ویژه هنگامی‌که این دستگاه‌ها اطلاعات حساسی نظیر معاملات اقتصادی با ارز مجازی را دربرمی‌گیرند، بسیار پیچیده است. بر این اساس در سال ۲۰۰۸ ساتوشی ناکاموتو مفهوم بنیادی بیت کوین را ارائه کرد که بازتاب بسیار زیادی داشته است. بیت کوین، ارز رمزنگاری‌شده مجازی است که بدون پشتیبانی هیچ‌گونه سازمان یا نهاد مالی متمرکزی ارزش خود را حفظ می‌کند [۵].

در حقیقت بیت کوین اولین سازمان خودگردان غیرمتمرکز کاربردی DAO بود که با مجموعه‌ای از قوانین و توابع خودمختار کد نویسی شده با پروتکل اجماع توزیع‌شده کار می‌کرد.

از سوی دیگر مفهومی که محبوبیت آن فراتر از خود ارز رمزنگاری‌شده است، بلاک چین است که پس از بیت کوین، قراردادهای هوشمند بر روی بلاک چین اتریم به وجود آمدند. بعد از قراردادهای هوشمند، DAO به‌صورت عمومی و به شکل امروزی آن مطرح شد [۶].

در ادامه این مقاله پس از بررسی اقدامات انجام‌شده درزمینه‌ی امنیت اینترنت اشیا، به تحلیل بلاک چین پرداخته و سپس یک روش امنیتی مبتنی بر خرد جمعی و بلاک چین برای امنیت IOT پیشنهاد می‌گردد.

۲- ادبیات تحقیق

جهت به دست آوردن بینشی عمیق نسبت به جنبه‌های مختلف اینترنت اشیا و بلاک چین، منابعی که به‌طور مستقیم و یا غیرمستقیم به موضوع این تحقیق ارتباط دارند را موردمطالعه قرار داده و در ادامه به شرح آنچه در راستای رسیدن به نتیجه مطلوب کمک کرده‌اند پرداخته می شود.

۱-۲- امنیت در اینترنت اشیا

امنیت در اینترنت اشیاء یکی از مهم‌ترین دغدغه‌های کاربران و تولیدکنندگان نرم‌افزار و سخت‌افزار وسایل موردنیاز هست بطوریکه می‌توان گفت اصلی‌ترین چالش پیش روی اینترنت اشیاء برای گسترش در بین جوامع محسوب می‌گردد.

ترس از حملات احتمالی از طریق اینترنت، سرقت اطلاعات و از بین رفتن حریم خصوصی توسط هرگونه شخص و یا سازمانی می‌تولند ضربات جبران‌ناپذیری را برای مصرف‌کنندگان و کاربران ایجاد نماید، گسترش دامنه کاربرد و هوشمند سازی شهرها، کارخانه‌ها و خانه‌های مسکونی می‌تواند اطلاعات بسیار ارزشمندی را ایجاد نماید، گسترش شبکه‌های بی‌سیم و افزایش پهنای باند مورداستفاده، تنوع وسایل ساخته‌شده جهت هوشمند سازی و همچنین تنوع در پروتکل‌های ارتباطی این‌گونه وسایل و از طرفی محدودیت‌های فیزیکی برای حس‌گرها و دروازه‌ها همانند حافظه و سیستم پردازش اطلاعات و عدم توانایی نصب دیواره‌های دفاعی راه را برای هکرها و سارقان اطلاعات بازنموده که لازم است تا با تدابیر متفاوت و شناسایی حملات احتمالی و ضعف‌های موجود از طریق به‌کارگیری مؤثرترین روش‌ها راه را برای نفوذ این‌گونه سوءاستفاده‌ها مسدود کرد [۷].

در حال حاضر مخاطرات بسیاری در خصوص اینترنت اشیا وجود دارد و به همین دلیل نمی‌توان امنیت آن را صد در صد دانست. در اینترنت اشیا، دستگاه‌ها اطلاعاتی را فرستاده و دستوراتی را دریافت می‌کنند، ازاین‌رو نفوذ هکر و سوءاستفاده

آن چندان هم دور از انتظار نیست [۵].

۲-۲- چشم‌اندازی به فناوری بلاک چین

فناوری بلاک چین در اصل تلفیق سه فناوری قدیمی امضای دیجیتال، ارتباط نظیر به نظیر و فرایند اجماع بر اساس خرد جمعی است که به روشی جدید ارائه‌شده است. ازینرو این فناوری از طریق ایجاد امکان توزیع اطلاعات دیجیتال بدون کپی کردن آن، ستون فقرات نوع جدیدی از اینترنت را ایجاد کرد. این فرایند در ابتدا برای پول دیجیتال بیت کوین طراحی شد، اما در حال حاضر جامعه فناوری در حال پیدا کردن دیگر کاربردهای بالقوه برای این فناوری است.

شیوه کار پروتکل بلاک چین به‌طور خلاصه بدین شرح هست:

۱- هر تراکنشی که انجام می‌گیرد توسط کلید خصوصی کاربران امضا می‌شود.

۲- سپس توسط شبکه نظیر به نظیر به اطلاع تمامی اعضای شبکه می‌رسد.

۳- عده‌ای هستند که صحت‌وسقم این تراکنش را بررسی می‌کنند و آن را در یک بلوک ذخیره می‌کنند و سعی می‌کنند از بلوک را بچسبانند به زنجیره بلوک‌های قبل.

۴- و درنهایت آن‌ها در اختیار همه اعضای شبکه قرار دهند [۹].

بلاک چین مکانیسمی است که امکان تائید معاملات را توسط گروهی از عوامل نامطمئن فراهم می‌کند. بلاک چین دفتر کل پراکنده غیرقابل تغییر، شفاف، امن و قابل حسابرسی را فراهم می‌کند. بلاک چین را می‌توان به‌صورت آزاد و کامل برای دسترسی به همه معاملاتی که از زمان اولین معامله در سیستم صورت گرفته است، بکار برد و در هرزمانی توسط هر نهادی قابل بازبینی و تطبیق است. پروتکل بلاک چین اطلاعات را در زنجیره‌ای از بلاک‌ها قرار می‌دهد که هر بلاک مجموعه‌ای از معاملاتی را که در زمان معین با بیت کوین صورت گرفته است، ذخیره می‌کند. بلاک‌ها با ارجاع به بلاک قبلی به هم متصل شده و زنجیره‌ای را تشکیل می‌دهند [۶].

۲-۳- ادغام فناوری بلاک چین و اینترنت اشیا

اینترنت اشیا فرآیندها را بهینه می‌سازد تا بخشی از عصر دیجیتال باشند و همین امر باعث می گردد تا حجم زیادی داده به دست آید که سطح بی‌سابقه‌ای از دانش و آگاهی را فراهم سازد. این دانش توسعه کاربردهای هوشمند نظیر بهبود مدیریت و کیفیت زندگی شهروندان را از طریق دیجیتالی کردن خدمات در شهرها تسهیل می‌کند. در طی چند سال گذشته فناوری‌های رایانش ابری در فراهم کردن کارکرد لازم برای اینترنت اشیا به‌منظور تحلیل و پردازش اطلاعات و تبدیل آن‌ها به کارها و دانش ریل تایم کمک کرده‌اند. این رشد بی‌سابقه در اینترنت اشیا فرصت‌های جدیدی را به وجود آورده است مانند مکانیسم‌هایی برای دسترسی و اشتراک اطلاعات. پارادایم داده‌های باز بارزترین مورد از این کار است. بااین‌حال، به‌طوری‌که در بسیاری از سناریوها روی‌داده است، یکی از مهم‌ترین آسیب‌پذیری‌ها در این کارها عدم وجود اطمینان است. ساختارهای متمرکز نظیر ساختاری که در رایانش ابری بکار رفته است کمک زیادی به توسعه اینترنت اشیا کرده‌اند؛ اما ازنظر شفافیت داده‌ها به‌عنوان جعبه سیاه عمل می‌کنند و شرکت‌کنندگان شبکه به‌روشنی نمی‌دانند که اطلاعاتی که ارائه می‌دهند چگونه و کجا بکار می‌رود [۱۰].

فرایند ارتباطات در اینترنت اشیا پیش از سال

۲۰۰۵ به‌صورت Centralized یا متمرکز انجام می‌گشت و امروزه با توجه به روی کار آمدن Cloud شکل دسترسی به داده‌ها به‌صورت Decentralized یا غیر متمرکز تغییر یافت و چنانچه پیش‌بینی می‌شود در آینده دسترسی به داده‌ها به‌صورت بلاک چین، نظیر به نظیر خواهد شد و بدین ترتیب از محیط متمرکز به Distributed یا توزیع شده پیشرفت خواهد داشت.

ادغام فناوری‌های نویدبخشی نظیر اینترنت اشیا، بلاک چین، هوش مصنوعی و داده‌کاوی که از آن‌ها به‌عنوان Four Big یاد می‌شود، و این کار باارزشی محسوب می‌شود [۱۱]. بلاک چین می‌تولند با فراهم کردن سرویس مطمئن اشتراک اطلاعات به‌صورت قابل‌ردیابی، اینترنت اشیا را غنی سازد. منابع داده را می‌توان در هرزمانی شناسایی کرد و در طول زمان داده‌ها بدون تغییر می‌ملند، درنتیجه امنیت افزایش می‌یابد. در مواردی که اطلاعات اینترنت اشیا باید به‌صورت امن بین شرکت‌کنندگان زیادی به اشتراک گذاشته شود، این ادغام تحولی کلیدی خواهد بود. برای مثال، برای رای گیری الکترونیک، یا به‌روز سازی Franeware های دستگاه‌های متصل در IOT، همچنین بهبود اقتصاد مشارکتی در حوزه‌هایی نظیر شهرهای هوشمند و خودروهای هوشمند.

اشتراک داده‌های مطمئن می تواند برای عضو کردن شرکت‌کنندگان جدید در اکوسیستم‌ها مطلوب باشد و به بهبود خدمات و سازگاری آن‌ها کمک کند؛ بنابراین استفاده از بلاک چین می‌تواند اینترنت اشیا را با اطلاعات مطمئن و امن کامل سازد و به‌عنوان کلیدی برای حل مسائل مقیاس‌پذیری، محرمانگی و قابلیت اطمینان در رابطه با اینترنت اشیا شناخته شود.

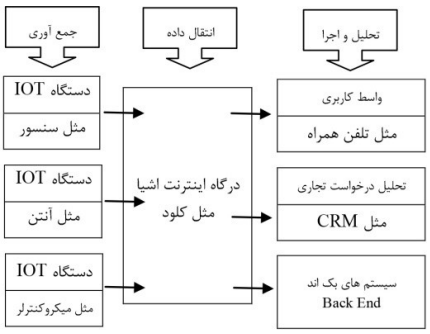
کارکردی که بلاک چین برای اینترنت اشیا فراهم می‌کند، بسیار مفید و به توسعه فناوری‌های اینترنت اشیا در آینده کمک خواهد کرد. باید توجه داشت که هنوز چالش‌های تحقیقاتی و مسائل حل‌نشده زیادی باقی است که باید برای استفاده بی‌نقص از این دو فناوری به‌صورت باهم موردمطالعه قرار گیرند.

ازجمله پروژه‌هایی که درزمینه‌ی اینترنت اشیا و بلاک چین انجام‌شده است می‌توان به پروژه Slock که پلی به‌سوی بلاک چین و محیط فیزیکی باز کرد و در آن افراد می‌تولنند اموال شخصی خود را به اجاره دیگران قرار دهند [۱۲].

همچنین پروژه Enigma که روی بیت کوین کار می‌کند و در آن روشی برای حل مشکل حریم خصوصی ارائه داد و همچنین درصدد کاهش پردازش بیش‌ازاندازه گام نهاد؛ و یا پروژه ADEPT که توسط سامسونگ و IBM از سال ۲۰۱۵ روی اتریم انجام شد و در آن پروسه ماینینگ را نسبت به قدرت و ظرفیت هر ماینر متعادل می‌سازد [۱۲].

۲-۴- روش سنتی اینترنت اشیا

اینترنت اشیا این امکان را برای پلتفرم‌ها فراهم می کند تا دستگاه ها بتوانند اطلاعاتشان را ذخیره کنند. همچنین یک‌زبان مشترک نیز ارائه می‌کند تا دستگاه‌ها با یکدیگر ارتباط برقرار کنند و مردم بتوانند از آن‌ها بهره ببرند.



شکل ۱: نمونه سیستم اینترنت اشیا

دستگاه‌های ارتباطی (سانسورها) در وسایل کاربردی روزمره ما از قبیل تلفن همراه، تلویزیون، سیستم کنترل دمای داخلی، لوازم برقی، ماشین‌ها، چراغ‌های راهنمایی و تجهیزات صنعتی قرارگرفته‌اند. این سانسورها اطلاعات مربوط به موقعیت دستگاه‌های متصل را به‌طور مداوم بیرون می‌دهند و امکان تبادل اطلاعات از طریق اینترنت را برای دستگاه‌ها فراهم می‌کنند.

پس‌ازآن پلتفرم‌های IOT داده‌ها را به‌منظور استخراج اطلاعات مهم آنالیز کرده و برای شروع یک دستور یا عمل جدید، آن‌ها را با دستگاه‌های دیگر به اشتراک می‌گذارد [۱۳].

دستگاه‌های IOT سنتی وابسته به یک مهندسی متمرکز هستند. به این صورت که اطلاعات از دستگاه به محل ذخیره‌ی ابری فرستاده می‌شوند، یعنی جایی که اطلاعات از طریق تجزیه تحلیل پردازش‌شده و سپس دوباره به دستگاه متصل به IOT بازمی‌گردند. مقیاس‌پذیری این سیستم متمرکز بااتصال میلیاردها دستگاه به شبکه IOT در سال‌های آتی، بسیار محدود خواهد بود و امنیت شبکه به خاطر داشتن میلیاردها نقطه‌ضعف به خطر می‌افتد. همچنین اگر قرار باشد در آینده اشخاص ثالث به‌طور مداوم هر تراکنش کوچک بین دستگاه‌ها را تائید و بررسی کنند، این سیستم به یک سیستم کند و بسیار پرهزینه تبدیل خواهد شد [۱۴].

در شبکه‌های IOT دستگاه‌ها مدام در حال تبادل اطلاعات بسیار مهم از طریق اینترنت‌اند. این موضوع باعث می‌شود که آن‌ها به هدف اصلی هکرها تبدیل بشوند. ازاین‌رو حریم خصوصی و امنیت دو دغدغه اصلی IOT خواهند بود [۱۴].

یکی از معروف‌ترین حملات دستبرد به اطلاعات، حمله DDOS و میرای بات نت بود که باعث ایجاد اختلال در خدمات اینترنتی دوربین‌های مداربسته و DVR های تقریباً تمام بخش‌های سواحل شرقی آمریکا ازجمله شبکه‌های توییتر، نتفلیکس و ردیت شد [۱۵].

یکی دیگر از این خطرها متوجه ۵۰ هزار دستگاه تنظیم ضربان قلب سازمان FDA (سازمان غذا و دارو آمریکا) در سال ۲۰۱۷ بود. هکرها می‌توانستند به دلیل وجود شکاف‌های امنیتی، در عملکرد دستگاه ضربان‌ساز در بدن بیمار اختلال ایجاد کنند.

ازآنجاکه هسته بلاک چین یک دفتر کل توزیع‌شده، رمزنگاری‌شده و ایمن است که امکان مبادله امن اطلاعات را فراهم می‌کند و هدف از این تحقیق رسیدن به مکانیسمی است که محرمانگی، یکپارچگی و قابلیت دسترسی به داده‌های منتقل‌شده و دریافتی توسط گره‌ها در شبکه اینترنت اشیا را با استفاده از فناوری بلاک چین فراهم کند [۹].

چالش‌های پیش رو برای ادغام بلاک چین و IoT بسیار زیاد است ازجمله گمنامی گره‌ها، مقیاس‌پذیری و احراز هویت که در اینجا راه‌حلی جهت بهبود مسئله احراز هویت ارائه خواهد شد.

۵-۲- قراردادهای هوشمند بلاک چین

قراردادهای هوشمند[۱] در شبکه‌های بلاک چینی، یک توافق برای دستگاه‌ها ایجاد می‌کنند که در صورت تکمیل شرایط خاص اجراشده و باعث می‌شوند که آن‌ها به‌صورت امن و مستقل کار کنند. ازاین‌رو تبادل اطلاعات کم‌هزینه‌تر، مقیاس‌پذیرتر و مستقل‌تر خواهد بود (نیاز نیست هیچ شخص ثالثی

[۱] Smart Contract

بر مبادلات نظارت داشته باشد). این قرارداد هوشمند می‌تواند از نیت افرادی که می‌خواهند از این اطلاعات به نفع خودشان استفاده کنند نیز جلوگیری کند. در چنین سیستمی اطلاعات در سرتاسر یک شبکه امنیتی رمزنگاری‌شده غیرمتمرکز منتشر می‌شوند. بدین ترتیب دست بردن در امنیت شبکه کار بسیار دشواری خواهد بود.

درنهایت در یک شبکه متمرکز، احتمال ازکارافتادن فقط با یک اشتباه کوچک بسیار زیاد است. در یک شبکه غیرمتمرکز بلاک چینی این ریسک از طریق میلیون‌ها گره که اطلاعات را بر اساس یک سیستم نظیر به نظیر جابجا می‌کنند، کاهش می‌یابد و مابقی شبکه IoT بدون مشکل کار کند.

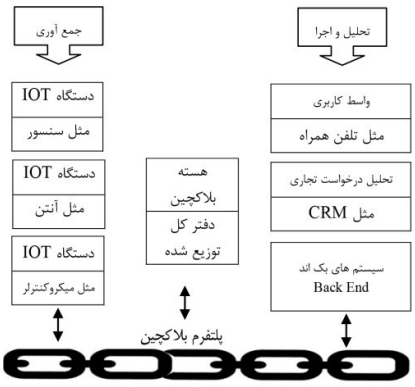
یکی از مهم‌ترین ویژگی‌های بلاک چین، تغییرناپذیری آن است، بلاک چین بر اساس یک مدل خرد جمعی کار می‌کند؛ یعنی بایستی ۵۱ درصد از کاربران داخل یک بلاک چین برای انجام یک تراکنش و یا ورود به سیستم به همان بلاک چین، تأییدیه بدهند تا آن ورود و یا تراکنش انجام پذیرد. به همین دلیل تقریباً تغییرهای غیرمعمول و مشکوک عملاً غیرممکن هستند. همچنین برای برهم زدن صحت یک بلاک چین، هکرها می‌بایست تعداد زیادی از موجودیت‌های مستقل در بلاک چین را تغییر دهند پس شفافیت کامل بلاک چین به شرکت‌ها کمک می‌کند تا در صورت رخ دادن نقص امنیتی، بتوانند با واکنشی سریع‌تر به حالت اولیه برگردند.

۳- مدل پیشنهادی (مدل پنج لایه بر اساس قراردادهای هوشمند بلاک چین)

در این تحقیق با تغییر بر روی معماری سه لایه اینترنت اشیا یک مدل جدید مبتنی بر بلاک چین ارائه می گردد و با استفاده از دفتر کل پراکنده (Ledger) مبتنی بر بلاک چین، جهت بالا بردن امنیت اینترنت اشیا اقدام گردد. نکته قابل توجه این است که در این سیستم بر خلاف بیت کوین نشانه‌ها به‌جای اینکه ارزش پولی داشته باشند، در مورد توزیع اختیار رأی دادن بین گره‌ها و تبادلات معین تصمیم می‌گیرند تا از حملات رد سرویس (DoS) در انتقال اطلاعات جلوگیری شود. همچنین منظور از تراکنش هر نوع تراکنش مالی و یا هر ارتباطی که بین دستگاه‌ها ایجاد شود، می باشد.

۱-۳- فاز اول : ایجاد ارتباط نظیر به نظیر

با حذف درگاه اینترنت اشیا به‌صورت متمرکز عملاً یک اتصال P۲P میان دستگاه‌ها ایجاد می‌کنیم. (شکل ۲)



شکل ۲: نمونه تغییریافته شده با بلاک چین

۲-۳- فاز دوم : تنظیم قرارداد های هوشمد به صورت غیر متمرکز

با ارائه دفتر کل پراکنده (Ledger)، جهت تنظیم قراردادهای هوشمند به‌صورت غیرمتمرکز، عملاً یک ساختار غیرقابل تغییر برای ثبت اطلاعات فراهم می‌کنیم و لایه‌های پروتکل بلاک چین و کاربری بلاک چین را به مدل ۳ لایه اینترنت اشیا اضافه می‌کنیم. (جدول ۲)

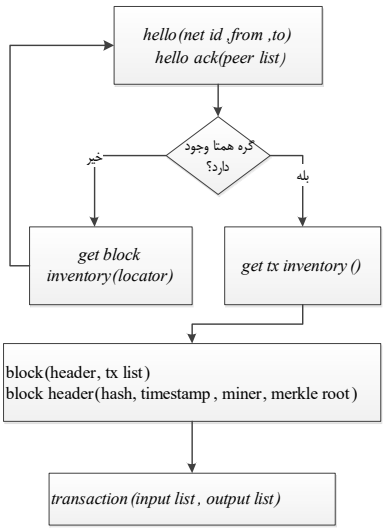
جدول ۲: مدل معماری ارائه‌شده با بلاک چین

لایه	نام لایه	کاربرد
۱	Network of Things	شامل هوشمند سازها یا فعال‌کننده‌ها
۲	Cloud Computing (service oriented)	پردازش‌های مبتنی بر سرویس جهت پوشش دهی کامل تجهیزات فعال‌کننده
۳	لایه هوشمند پروتکل بلاک چین	توافق نظر و تصمیم‌گیری با استفاده از خرد جمعی و ماینینگ
۴	لایه هوشمند کاربرد بلاک چین	ساختارهای امنیتی اینترنت اشیا با استفاده از بلاک چین
۵	Application	شامل بسترهای نرم‌افزاری موردنیاز جهت به‌کارگیری اطلاعات

۳-۳- فاز سوم : افزودن لایه هوشمند پروتکل بلاک چین به معماری سه لایه اینترنت اشیا

در لایه پروتکل بلاک چین الگوریتم اتفاق‌نظر برای راه‌اندازی انتقال دیتا، میان گره‌های موجود در شبکه را مطرح می‌سازیم. یعنی تصمیم‌گیری برای استفاده از پلت فرم بلاک چین.

لایه پروتکل بلاک چین الگوریتم اتفاق‌نظر برای قبول یا رد تراکنش، میان گره‌های موجود در شبکه را در برمی‌گیرد. ما مجموعه‌ای از پیام‌ها را در این لایه تعریف می‌کنیم تا دررسیدن به نظری مشترک درباره بلاک چین در میان همه گره‌های شرکت‌کننده کمک کند.



شکل ۳ فلوچارت لایه هوشمند پروتکل بلاک چین

برای تضمین اینکه همه گره‌های اینترنت اشیا نظر یکسانی نسبت به بلاک چین داشته باشند، قواعدی را برای لایه پروتکل بلاک چین تعریف می‌کنیم تا اتفاق‌نظر حاصل شود. خلاصه‌ای از این قواعد عبارت‌اند از:

- هر گره با دریافت هر تراکنش آن را در استخر حافظه[۱] خود ذخیره می‌کند و دوباره پخش می‌کند.
- با هر تیک ساعت، گره سعی می‌کند بلوک جدیدی را استخراج کند
- با ایجاد بلوک جدید، گره نظر خود را درباره بلاک چین بروز می‌کند و بلوک را به همتاهایش پخش می‌کند.
- میزان دشواری برای بلوک بعدی طوری بروز می‌شود که میانگین زمان پیش‌بینی‌شده برای یافتن بلوک بعدی (بر اساس عددی

[۱] Memory Pool (mempool)

معین از بلوک‌های آخر گرفته می‌شود) برابر با مقداری معین باشد.

- با دریافت بلوک جدید، گره تائید می‌کند که بلوک با همه قواعد پروتکل مطابقت دارد و همه تبادلات در بلوک طبق قواعد پروتکل و کاربری است.
- بعد از تائید بلوک دریافتی، گره نظر خود را درباره بلاک چین بروز می‌کند، تبادلات شامل شده را از استخر حافظه پاک می‌کند و بلوک را پخش می‌کند.
- درنهایت، همه گره‌ها نظر یکسان درباره بلاک چین دارند [۱۶].

بدین ترتیب میان گره‌ها امنیت بر اساس خرد جمعی جهت برقراری بلاک چین برقرار می‌شود حال پس از راه‌اندازی بلاک چین نیازمند به احراز هویت بین گره‌ها هستیم لذا در ادامه به اقدامات انجام‌شده در لایه کاربردی می‌پردازیم.

۳-۴- فاز چهارم : افزودن لایه هوشـــمند کاربردی بلاک چین به معماری سه لایه اینترنت اشیا

در لایه کاربری بلاک چین تبادلات خاص امنیتی در اینترنت اشیا را برقرار ساخته و چگونگی تراکنش آن‌ها را برای لایه‌های بالاتر را تعریف می‌سازیم.

در بحث فناوری بلاک چین، کلید خصوصی رمزنگاری‌شده یک ابزار مالکیت قدرتمند را فراهم می‌کند که نیازهای احراز هویت را برآورده می‌کند. داشتن یک کلید خصوصی به معنای مالکیت است.

اما تائید اعتبار کافی نیست، داشتن مجوز، دارا بودن اعتبار کافی برای انجام تراکنش و ... نیاز به اعتمادسازی دارند و برای این کار نیاز به یک شبکه توزیع‌شده نظیر به نظیر است. یک شبکه توزیع‌شده از فساد یا شکست مجموعه جلوگیری می‌کند.

امنیت این شبکه توزیع‌شده باید تضمین‌شده باشد. تائید تراکنش‌ها نتیجه اجرای قوانین پروتکل توسط تمام شبکه است.

لایه کاربری بلاک چین تبادلات خاص امنیتی در اینترنت اشیا را برقرار ساخته و چگونگی تراکنش آن‌ها را برای لایه‌های بالاتر تعریف می‌کند. کارکرد اصلی که به‌وسیله مدل کاربری پیشنهادی ما فراهم می‌شود احراز هویت و صلاحیت برای دستگاه‌ها در شبکه‌های اینترنت اشیا است.

در این روش برای هر گره یک مجموعه با ۴ پشته تعریف می‌کنیم و در پشته‌ها به ترتیب مقادیر ۱-id ۲-K_{pu} کلید عمومی ۳- K_{pr} کلید خصوصی و ۴-KDS تولیدکننده کلید عمومی برای جلوگیری از حمله قرار می‌دهیم.

این روش از ترکیب رمزنگاری و احراز هویت به‌منظور تائید هویت دو طرف استفاده می‌کند، در اینجا نیز کلیدهای عمومی باید از KDS استعلام شود. در سمت فرستنده عبارت فاش نوشته با استفاده از کلید خصوصی رمز شده و با کلید عمومی گیرنده رمزگشایی شود و توسط شبکه ارسال می‌گردد. در سمت گیرنده این پیام ابتدا با کلید خصوصی گیرنده سپس با کلید عمومی فرستنده از حالت رمز خارج می‌شود. این کار برای فراهم کردن احرازهویت پویا و اجتناب از حملات نمایش مجدد (ری پلی) در شبکه است.

۴- مطالعات میدانی (Case Study)

ازآنجاکه جهت راســـت آزمایی و نتیجه‌گیری از تحقیق به‌دســت‌آمده نیازمند به جمع‌آوری داده‌های کمی و کیفی هســـتیم، لذا از روش مطالعات میدانی بهره برده و در ادامه به شرح آن می‌پردازیم.

۱-۴- ناحیه بندی شهر هوشمند

برای این منظور فرض می‌کنیم شهر مدنظر را ناحیه

بندی کردیم و در هر ناحیه یک گره گیرنده بی‌سیم قرار دارد. از طرف دیگر در تمامی ماشـــین‌های این شـهر هوشـمند حسـگرهایی تعبیه گشـته اسـت که وظیفه آن اعلام وجود در ناحیه به نودهای گیرنده موجود در همان ناحیه هسـت به این صـورت که در صـــورت ورود یک ماشـــین از ناحیه قبلی به ناحیه جدید باید تعداد ماشـین‌های موجود در ناحیه قبلی یک عدد کم شـود و تعداد ماشـین‌های موجود در ناحیه جدید یک عدد اضـافه شـود. پس می‌توان با ارتباط میان نودها با یکدیگر این مشکل را رفع کرد بدین‌صورت که در صورت اعلام تراکنش یک ماشین با یک نود سایر نودها بررسی کنند که اگر ماشین در ناحیه خود موجود اســت، آن‌ها از ناحیه خارج سازند. پس اولین قانون در شبکه این خواهد بود که هر ماشـــین تنها در یک ناحیه موجود هســـت. به‌عبارت‌دیگر شـناسـه ماشـین‌های موجود در کل شـــبکه باید به‌صـــورت یونیک، تنها در یک ناحیه ثبت‌شده باشد.

۲-۴- اطلاع‌رسانی از سطح ترافیک

پس از ثبت ماشـــین‌ها در نواحی نیازمند به اطلاع‌رســـانی از ســـطح ترافیک موجود در مســـیر انتخابی هستیم. لذا ماشین‌هایی که قصد سفر به مســـیری جدید را دارند پیش از حرکت باید به گیرنده‌های موجود در مسیرهای انتخابی درخواست بفرستند و گیرنده‌ها در پاسخ بر اساس فرمول‌های خاص ترافیک سنجی به ماشینی که قصد سفر به مســـیر ناحیه را دارد مجوز ورود را صـــادر یا لغو می‌کنند.

حال اگر پهنای بلند ناحیه را p در نظر گرفته و تعداد ماشـــین‌های موجود را q در نظر بگیریم و ترافیک ناحیه را T در نظر بگیریم می‌توان از فرمول $T=\frac{q}{p}$ میزان ترافیک ناحیه را به دســـت آورد و برحسب مسافت هر مسیری که مقدار T آن کمتر بود، می‌توان مسیر انتخابی برای سفر در نظر گرفت.

حال با توجه به مطالعات میدانی عنوان‌شده قصد داریم تا جهت ثبت ارتباط میان ماشـین و گره‌های ناحیه (قسمت اول) از بلاک چین استفاده کنیم.

۳-۴- نحوه عملکرد

جهت صـــحت گذاری بر مقادیر ماشـــین‌های موجود در ناحیه‌ها و تراکنش انتقال یک ماشـین از یک ناحیه به ناحیه دیگر مدل بلاک چین (بیت کوین) استفاده می‌کنیم. بدین‌صورت که تراکنش‌ها به‌صـــورت پشـــت ســـر هم در بلاک‌هایی ذخیره می‌گردند و تمامی نودها دسترسی مشاهده و تائید ایجاد بلاک‌ها رادارند و در صـــورت عدم تائید نباید بلاک تراکنش ایجاد گردد حال با توجه به شـکل ۴ فرض می‌کنیم:

۱-ماشین A از ناحیه ۱ به ناحیه ۲ منتقل شد.

۲-داده اعلام وجود از سمت ماشین به گره ناحیه ۲ ارسال می‌گردد

۳-گره ناحیه ۲ ورود ماشین را ثبت می‌کند.

۴-گره ناحیه ۲، ID ماشـــین را به گره ناحیه قبل (ناحیه ۱) اطلاع‌رسانی می‌کند

۵-گره ناحیه ۱، ماشـــین را از جدول ماشـــین‌های فعلی حذف کرده یا فلک خروج را فعال می‌کند.

مجوز ورود به ناحیه با استفاده از بلاک چین:

پهنای باند ناحیه ۲، $N_2p=150$ هســـت و تعداد ماشـین ناحیه ۲، در حال حاضـر $N_2q=41$ عدد هست.

۲ آیتم بالا تائید شده و بلاک اول را می‌سازد

ماشـــین a از ناحیه ۱ به ناحیه ۲ وارد می‌شـــود پس تعداد ماشـین ناحیه ۲ از ۴۱ به ۴۲ تغییر پیدا می‌کند. اگر $p-q>0$ باشد (تائید می‌شود و به‌عنوان

دومین بلاک ذخیره می‌گردد)

تعداد ماشین ناحیه ۱ به میزان یک واحد کم می‌شود (تائید می‌شود و به‌عنوان سومین بلاک ذخیره می‌گردد)

در ادامه به همین ترتیب بلاک‌ها ساخته شده و درصورتی‌که مقدار p-q<۰ شود بلاک جدید تائید نمی‌شود و در اصل تراکنش صورت نمی‌پذیرد و ماشین باید پشت گیت صف انتظار (پشت چراغ‌قرمز) بماند تا زمانی که p-q ناحیه جدید عددی بزرگ‌تر از ۰ شود.

با توجه به مثال گفته‌شده و شرح آن‌که در شکل ۴ قابل‌مشاهده هست به بررسی چگونگی کار در لایه پروتکل بلاک چین خواهیم پرداخت.

شکل ۴: پیاده‌سازی تصویری کیس استادی

۴-۴- طراحی بلاک چین Case Study

همان‌طور که گفته شد به‌طورکلی بلاک چین یک نوع سیستم ثبت اطلاعات و گزارش است. تفاوت آن با دستگاه‌های دیگر این است که اطلاعات ذخیره‌شده روی این نوع سیستم، میان همه اعضای شبکه به اشتراک گذاشته می‌شوند و با استفاده از رمزنگاری امکان حذف و دست‌کاری اطلاعات ثبت‌شده تقریباً غیرممکن است.

بیت کوین اولین کاربرد از این فناوری بود و از بلاک چین برای ذخیره اطلاعات دارایی کاربران بهره برد. اگر بلاک چین یک سیستم‌عامل باشد، بیت کوین نرم‌افزاری روی این سیستم‌عامل است.

هدف ما از ارائه این طرح ساخت یک سیستم بلاک چین جهت ثبت اطلاعات ترافیکی نواحی شهر هوشمند هست و نام آن را TrafficPoint می‌گزاریم.

در هر بلاک هر اطلاعاتی می‌تواند ثبت شود؛ که ما در اینجا اطلاعات مربوط به تعداد ماشین‌های موجود در هر ناحیه را قرار خواهیم داد. در بلاک چین، اطلاعات در بلاک‌ها قرار می‌گیرند و باهم به‌صورت زنجیره‌ای مرتبط می‌شوند.

برای مثال بلاک چین (شکل ۵) را در نظر بگیرید، هر بلاک یک ناحیه ترافیکی را نشان می‌دهد که ID ماشین‌های موجود در آن ناحیه در آن ثبت‌شده هستند.

شکل ۵: بلاک چین کیس استادی

با مشاهده شکل ۵ برای بلاک ناحیه ۱ (Block۱) که حاوی اطلاعات ورود ماشین‌های A,B,C,D,E,F است، هش بلاک «132fds32fswrf4s» است. در بلاک چین، هش بلاک‌های بعدی حاوی هش بلاک قبلی هم هستند. هش در هر بلاک چین با یک تابع ریاضی خاص به دست می‌آید که توسعه‌دهندگان آن را مشخص می‌کنند. کوچک‌ترین تغییر در اطلاعات یک بلاک، هش آن را به‌طورکلی تغییر می‌دهد. و درنتیجه بلاک‌های بعدی هم غیر معتبر خواهند شد به همین دلیل این فناوری بلاک چین یا زنجیره

بلاک‌ها نام دارد.

اگر کسی محتوای یک بلاک را تغییر دهد و هش بلاک‌های بعدی را به‌روزرسانی کند، چه می‌شود؟ این امکان وجود دارد اما شما توزیع را در نظر نگرفته‌اید. داده‌های بلاک چین در یک کامپیوتر یا سرور خاص ذخیره نمی‌شوند. هر کامپیوتر یا سیستمی که به شبکه وصل شود یک نسخه از بلاک چین را دریافت می‌کند.

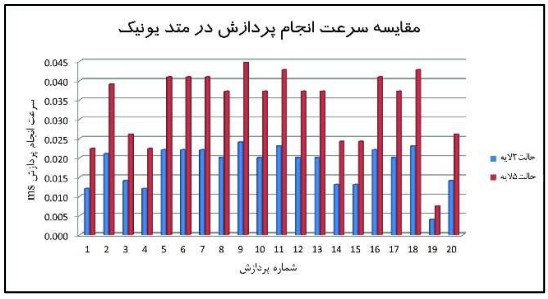
۵- اثر بلاک چین بر سرعت و پایداری IOT

در ادامه به بحث و مشاهده در رابطه با نتایج به‌دست‌آمده از مطالعات میدانی می‌پردازیم و با آزمایش بر روی ۲۰ پردازش اول پشت سر هم در حالات قیدشده به تجمیع مشاهدات می‌پردازیم و درنهایت به نتیجه‌گیری نهایی در رابطه با تحقیق می‌رسیم.

۵-۱- بحث

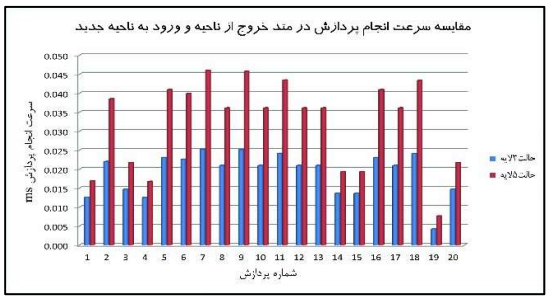
برای به دست آوردن یک تحلیل قابل‌استفاده از سرعت عملکرد سامانه می‌بایست در دو متد در رابطه با آن بحث کرد:

متداول (یونیک): هنگامی‌که فقط ماشین جدید در ناحیه جدید معرفی می‌گردد حالت اول با در نظر گرفتن قراردادهای هوشمند و حالت دوم بدون در نظر گرفتن قراردادهای هوشمند.



شکل ۶: نمودار مقایسه سرعت حالت یونیک با و بدون قرارداد هوشمند

متد دوم: هنگامی‌که فقط ماشین از ناحیه پیشین خروج و به ناحیه جدید وارد می‌شود حالت اول با در نظر گرفتن قراردادهای هوشمند و حالت دوم بدون در نظر گرفتن قراردادهای هوشمند.



شکل ۷: نمودار مقایسه سرعت حالت خروج از ناحیه قبلی و ورود به ناحیه جدید با و بدون قرارداد هوشمند

همچنین می‌توان تفاوت امنیت میان استفاده از بستر قراردادهای هوشمند و حالت عادی را در جدول شماره ۳ به بحث کشید.

جدول (۳): مقایسه امنیت میان حالت بلاک چین (۵لایه) و حالت عادی(۳لایه)

اتک	بدون در نظر گرفتن بلاک چین	با در نظر گرفتن بلاک چین
Sql Injection	به دلیل وجود تنها یک دیتا بیس مرکزی احتمال دارد	به دلیل وجود دفتر کل پراکنده امکان ندارد
DDOS	به دلیل وجود یک هسته مرکزی امکان‌پذیر است	فنّاوری blockchain می‌تواند ایجاد شبکه‌های IoT را امکان‌پذیر سازد که (P۲P)هستند.
Man in the Middle	به دلیل یک مرحله احراز هویت ممکن است	به دلیل وجود چندین مرحله احراز هویت در هش بین بلاک‌ها غیرممکن

۵-۲- مشاهدات

بر اساس مقایساتی که در شکل ۶ و همچنین شکل ۷ مشاهده می‌کنیم در حالات اول پایداری گره‌ها

دارای تعدادی پراکندگی بوده ولی در حالتی که از قراردادهای هوشمند استفاده کردیم پایداری گره‌ها با افزایش تعداد گره‌ها رو به افزایش هست.

مشاهده می‌کنیم سرعت عملکرد در حالتی که از قراردادهای هوشمند استفاده نکرده‌ایم بدون در نظر گرفتن ناپایداری‌ها تقریباً در یک اندازه و در حدود ۰.۰۲ میلی‌ثانیه هست اما با اعمال قراردادهای هوشمند سرعت انجام پردازش با بیشتر شدن تعداد گره‌ها افزایش پیدا می‌کند.

همچنین بر اساس جدول شماره ۳ مشاهده می‌کنیم در حالت استفاده از قراردادهای هوشمند امنیت بسیار بالاتر از حالت عادی خواهد شد.

۶- نتیجه‌گیری

این تحقیق روش جدیدی را جهت بهبود مسئله امنیت IoT به‌وسیله بلاک چین ارائه داده است. در این مقاله نشان داده شده که بلاک چین راه‌حلی عملی برای مسئله امنیت IoT است. روش Disturbuted Peer to Peer یک مدل Scale Out است و این بدان معنی است که هر چه میزان نودهای شبکه بالاتر برود پایداری شبکه بیشتر می‌گردد و این امر در امنیت نتیجه چشم‌گیری است همچنین ویژگی‌های مقاومت در برابر مداخله و اعتماد غیرمتمرکز امکان ساخت سرویس امن احراز هویت و صلاحیت را فراهم می سازد. باید توجه داشت که تحقیق حاضر عمدتاً سعی دارد چالش‌های پیاده‌سازی بلاک چین را در شبکه IoT بشناسد. در حال حاضر، نتایج کامل و دقیقی درباره مقیاس‌پذیری یا عملکرد بلاک چین در شبکه IoT در دست نیست همچنین یکی از مسائل مهم در رابطه با پیچیدگی زمان هست که در آینده امید است موردتحقیق قرار گیرد.

۷- پیشنهاد برای تحقیقات آتی

اگرچه این تحقیق در حوزه امنیت IoT در بستر بلاک چین توانست در بهبود سطح پایداری شبکه نتیجه مطلوبی را حاصل سازد اما هنوز شبکه‌های IoT سطوح حملات و آسیب‌پذیری‌های وسیعی دارند. تحقیق حاضر را می‌توان به‌گونه‌ای بسط داد که سطوح حملات بیشتری را پوشش دهند و کاربردهای خاص IoT را در برگیرد و همچنین جهت حل مشکلات منوط به پیچیدگی زمانی اقدام نمود و برای برآوردن الزامات عملکردی سیستم بلادرنگ بهینه‌سازی شود.

راهکارهای رفع این مشکلات را برای تحقیقات آتی قراردادیم و امیدواریم در این راستا بتوانیم به نتایج چشمگیری دست پیدا کنیم.

۸- مراجع

[۱] *Gokhale, Pradyumna, Omkar Bhat, and Sagar Bhat. "Introduction to IOT." International Advanced Research Journal in Science, Engineering and Technology ۵٫۱ (۲۰۱۸): ۴۱ - 44.*

[۲] Balasubramaniam, Yamunaa, and P. S. V. Sathyanarayanan. (Enhancing Connected Vehicle Security with Block chain) (۲۰۱۸).

[۳] Gupta, Yash. "The applicability of blockchain in the Internet of Things." ۲۰۱۸ ۱۰th International Conference on Communication Systems & Networks (COMSNETS). IEEE, ۲۰۱۸.

[۴] Gia, Tuan Nguyen. "Fault tolerant and scalable IoT-based architecture for health monitoring." ۲۰۱۵ IEEE Sensors Applications Symposium (SAS). IEEE, ۲۰۱۵.

[۵] Androulaki, Elli. "Hyperledger fabric: a distributed operating system for permissioned blockchains." Proceedings of the Thirteenth EuroSys Conference. ACM, 2018.

[۶] Balasubramaniam, Yamunaa, and P. S.

V. Sathyanarayanan. "Enhancing Connected Vehicle Security with Block chain. « (۲۰۱۸).

[۷] Dorri, Ali. "Blockchain for IoT security and privacy: The case study of a smart home." ۲۰۱۷ IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, 2017.

[۸] Abera, Tigist. "Things, trouble, trust: on building trust in IoT systems." Proceedings of the ۵۳rd Annual Design Automation Conference. ACM, ۲۰۱۶.

[۹] Mattila, Juri. The blockchain phenomenon–the disruptive potential of distributed consensus architectures. No. ۳۸. ETLA working papers, ۲۰۱۶.

[۱۰] Díaz, Manuel, Cristian Martín, and Bartolomé Rubio. "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing." Journal of Network and Computer applications ۶۷ (۲۰۱۶): ۹۹- 117.

[۱۱] Yazdinejad, Abbas. "Blockchain-enabled Authentication Handover with Efficient Privacy Protection in SDN-based ۵G Networks." arXiv preprint arXiv: ۱۹۰۵٫۰۳۱۹۳ (۲۰۱۹).

[۱۲] Vahid Rad - Great Blessing of Blockcain Technology – ۲۰۱۸

[۱۳] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." ۲۰۱۵ IEEE World Congress on Services. IEEE, 2015.

[۱۴] Rivera, J., and R. van der Meulen. "Forecast alert: internet of things—endpoints and associated services, worldwide, ۲۰۱۶." Gartner (۲۰۱۶).

[۱۵] Hallman, Roger. "IoDDoS-The Internet of Distributed Denial of Sevice Attacks-A Case Study of the Mirai Malware and IoT-Based Botnets." IoTBDS. ۲۰۱۷.

[۱۶] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system. (۲۰۰۸).

محمد سعید صفایی صادق مدرک کارشناسی خود را در رشته مهندسی نرم‌افزار کامپیوتر در سال ۱۳۸۸ از دانشگاه آزاد اسلامی واحد آشتیان و مدرک کارشناسی ارشد خود را در سال ۱۳۹۸ در رشته مهندسی فناوری اطلاعات گرایش شبکه‌های کامپیوتری از دانشگاه آزاد اسلامی واحد آشتیان اخذ کرده است.

زمینه‌های پژوهشی موردعلاقه ایشان عبارت‌اند از: بلاک چین، محاسبات توزیع‌شده.

شمس اله قنبری مدرک کارشناسی خود را در رشته ریاضی و علوم کامپیوتر در سال ۱۳۷۶ از دانشگاه صنعتی امیرکبیر، مدرک کارشناسی ارشد خود را در سال ۱۳۸۰ از دانشگاه مازندران، و مدرک دکترا در سال ۱۳۹۴ از دانشگاه UPM مالزی در رشته High Performance Computing اخذ کرده است.

ایشان در حال حاضر به‌عنوان هیات علمی دانشگاه آزاد مشغول به کار هست. زمینه‌های پژوهشی موردعلاقه ایشان عبارت‌اند از: محاسبات توزیع‌شده، محاسبات ابری، الگوریتم‌های زمانبندی، محاسبات نرم، محاسبات فراگیر و مجازی سازی

نشانی رایانامه ایشان عبارت است از:

myrshg@Gmail.com