



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^۱ و^۲

چکیده

اینترنت اشیا^۱ برای اولین بار در سال ۱۹۹۹ توسط کوین اشتون^۲ مورد استفاده قرار گرفت و بر اساس آمار منتشر شده از موسسه تحقیقاتی و پژوهشی IDC به عنوان 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 از 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: saeidsafaei@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 Improving Authentication on the Internet of Things

Mohammad Saeid Safaei Sadegh^{*1} and Shamsollah Ghanbari²

^{1,2} Islamic Azad University Branch of Ashtian

Abstract

The internet has been developed for the first time in 1999 by Kevin Ashton, based on statistics published by research and research institute IDC as one of the highest - earning projects since 2006. 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. صفایی صادق، ش. قنبری، ارائه یک مدل امنیتی مبتنی بر قراردادهای هوشمند بلاک چین جهت بهبود احراز هویت در اینترنت اشیا، دوفصلنامه محاسبات و سامانه های توزیع شده، سال دوم، شماره اول، شماره پیاپی ۲، سال ۱۳۹۷، ص ۱-۱۵



۱- مقدمه

اینترنت اشیا مفهومی است که در آن اشیای فیزیکی به اینترنت وصل می شوند و با اشیای دیگر در ارتباط قرار می گیرند و بدین ترتیب از دستگاه های ساده به دستگاه های هوشمند تبدیل می گردند.

رشد فعلی جوامع و تحول سریع در فناوری ارتباطات، موجب افزایش تعداد دستگاه های الکترونیکی مناسب در بسیاری از حوزه ها گشته است. اینترنت اشیا، به صورت مجموعه ای از فناوری ها از جمله شبکه های حسگر بی سیم (WSN) و شناسایی فرکانس رادیویی (RFID) پدید آمده است که توانمندی هایی را برای حس، به کارگیری و برقراری ارتباط در اینترنت فراهم کرده است [۱،۲].

معماری سنتی که غالباً در اینترنت استفاده می شود ممکن است نتواند نیازهای اینترنت اشیا را برآورده نماید. امروزه معماری سرویس گرا و یا انواع معماری های لایه ای و انعطاف پذیر به عنوان راهکار ارائه شده است و همان طور که در جدول ۱ می بینیم، از آن به عنوان معماری ۳ لایه نیز یاد می شود [۳].

جدول ۱: مدل معماری ۳ لایه اینترنت اشیا

لایه	نام لایه	کاربرد
۱	Network of Things	شامل هوشمند سازها یا فعال کننده ها
۳	Application	شامل بسترهای نرم افزاری موردنیاز جهت به کارگیری اطلاعات
۲	Cloud Computing (service oriented)	پردازش های مبتنی بر سرویس جهت پوشش دهی کامل تجهیزات فعال کننده

لایه اول: این لایه شامل هوشمند سازها یا فعال کننده ها هست. در این لایه تجهیزاتی که

امکان اتصال به کالاها را داشته درعین حال امکان برقراری ارتباط بی سیم با شبکه های موجود را نیز دارا می باشند قرار داده شده است. این تجهیزات دارای تنوع و گوناگونی فراوانی بوده که بنا به نیاز و نوع خدمات موردنظر و کارایی آن ها مورداستفاده قرار می گیرد مانند RFID ها، 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 شبکه های مختلف را داریم که جهت پوشش دهی کامل تجهیزات فعال کننده قابل استفاده می باشند تا تمامی اشیاء امکان اتصال به اینترنت را داشته و اطلاعات جمع آوری شده توسط آن ها به صورت یکپارچه به سیستم مرکزی ارسال گردد. با به کارگیری این شبکه ها، اطلاعات جمع آوری شده کاملاً به روز، دقیق و قابل اطمینان بوده و نیز سرعت دریافت، تجزیه و تحلیل این اطلاعات بسیار چشم گیر است.

لایه سوم: در این لایه بسترهای نرم افزاری موردنیاز جهت به کارگیری اطلاعات جمع آوری شده شرح داده می شود. این بسترها که به نوعی به عنوان یک رابط کاربردی عمل می نمایند امکان مدیریت کامل اشیاء را از طریق درگاه اینترنت فراهم می آورند. این نرم افزارها می باید انعطاف پذیر بوده و سرویس های موردنظر کاربر را متناسب با نوع خدمت برایش فراهم نمایند. همچنین با پیاده سازی این نرم افزارها می باید امکان هماهنگی بین فرایندها فراهم شود [۴].

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



موضوع این تحقیق ارتباط دارند را مورد مطالعه قرار داده شده است و در ادامه به شرح آنچه در راستای رسیدن به نتیجه مطلوب کمک کرده‌اند پرداخته می‌شود.

۲-۱- امنیت در اینترنت اشیا

امنیت در اینترنت اشیا یکی از مهم‌ترین دغدغه‌های کاربران و تولیدکنندگان نرم‌افزاری و سخت‌افزاری وسایل مورد نیاز هست بطوریکه می‌توان گفت اصلی‌ترین چالش پیش روی اینترنت اشیا 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 می‌تواند 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 مورد استفاده، 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 باز نموده 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،

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 قابل دسترسی هست.

مسئله اعتماد به دستگاه‌های اطلاعاتی درجایی که تائید یا مکانیسم‌های ارزیابی وجود ندارد، به‌ویژه هنگامی که این دستگاه‌ها اطلاعات حساسی نظیر معاملات اقتصادی با ارزش 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، ارزش رمزنگاری شده 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 توزیع شده کار می‌کرد.

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

در ادامه این مقاله پس از بررسی اقدامات انجام‌شده در زمینه‌ی 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



برای دسترسی به همه معاملاتی که از زمان اولین معامله در سیستم صورت گرفته است، بکار برد و در هر زمانی 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 می‌گردد 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 به منظور 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. باین حال، به طوری که در بسیاری از سناریوها روی داده 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 از نظر شفافیت داده‌ها به عنوان جعبه سیاه عمل می‌کنند و شرکت‌کنندگان شبکه به روشنی نمی‌دانند که اطلاعاتی که ارائه می‌دهند چگونه و کجا بکار می

دستگاه‌ها اطلاعاتی را فرستاده و دستوراتی را دریافت می‌کنند، از این رو 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 ارائه شده 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 به طور 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 صحت و وسقم 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 در نهایت آن‌ها در اختیار همه اعضای شبکه قرار دهند [۹].

بلاک چین مکانیسمی است که امکان تأیید معاملات را توسط گروهی از عوامل نامطمئن فراهم می‌کند. بلاک چین دفتر کل پراکنده غیر قابل تغییر، شفاف، امن و قابل حسابرسی را فراهم می‌کند. بلاک چین را می‌توان به صورت آزاد و کامل



رود [۱۰].

سازد و به عنوان کلیدی برای حل مسائل مقیاس پذیری، محرمانگی و قابلیت اطمینان در رابطه با اینترنت اشیا شناخته شود.

کارکردی که بلاک چین برای اینترنت اشیا فراهم می کند، بسیار مفید و به توسعه فناوری های اینترنت اشیا در آینده کمک خواهد کرد. باید توجه داشت که هنوز چالش های تحقیقاتی و مسائل حل نشده زیادی باقی است که باید برای استفاده بی نقص از این دو فناوری به صورت باهم مورد مطالعه قرار گیرند.

از جمله پروژه هایی که در زمینه ی اینترنت اشیا و بلاک چین انجام شده است می توان به پروژه Slock که پلی به سوی بلاک چین و محیط فیزیکی باز کرد و در آن افراد می توانند اموال شخصی خود را به اجاره دیگران قرار دهند [۱۲].

همچنین پروژه Enigma که روی بیت کوین کار می کند و در آن روشی برای حل مشکل حریم خصوصی ارائه داد و همچنین درصد کاهش پردازش بیش از اندازه گام نهاد؛ و یا پروژه ADEPT که توسط سامسونگ و IBM از سال ۲۰۱۵ روی اتریم انجام شد و در آن پرو سه ماینینگ را نسبت به قدرت و ظرفیت هر ماینر متعادل می سازد [۱۲].

۲-۴- روش سنتی اینترنت اشیا

اینترنت اشیا این امکان را برای پلتفرم ها فراهم می کند تا دستگاه ها بتوانند اطلاعاتشان را ذخیره کنند. همچنین یک زبان مشترک نیز ارائه می کند تا دستگاه ها با یکدیگر ارتباط برقرار کنند و مردم بتوانند از آن ها بهره ببرند.

فرایند ارتباطات در اینترنت اشیا پیش از سال ۲۰۰۵ به صورت Centralized یا متمرکز انجام می گشت و امروزه با توجه به روی کار آمدن Cloud شکل دسترسی به داده ها به صورت Decentralized یا غیر متمرکز تغییر یافت و چنانچه پیش بینی می شود در آینده دسترسی به داده ها به صورت بلاک چین، نظیر به نظیر خواهد شد و بدین ترتیب از محیط متمرکز به Distributed یا توزیع شده پیشرفت خواهد داشت.

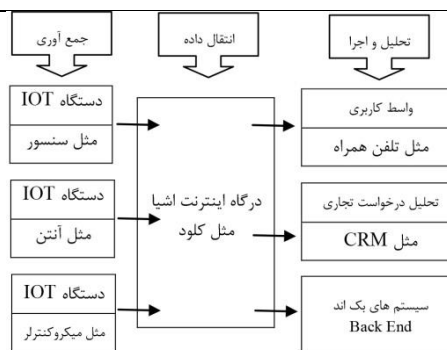
ادغام فناوری های نویدبخشی نظیر اینترنت اشیا، بلاک چین، هوش مصنوعی و داده کاوی که از آن ها به عنوان Four Big یاد می شود، و این کار بازرشی محسوب می شود [۱۱]. بلاک چین می تواند با فراهم کردن سرویس مطمئن اشتراک اطلاعات به صورت قابل ردیابی، اینترنت اشیا را غنی سازد. منابع داده را می توان در هر زمانی شناسایی کرد و در طول زمان داده ها بدون تغییر می ماند، در نتیجه امنیت افزایش می یابد. در مواردی که اطلاعات اینترنت اشیا باید به صورت امن بین شرکت کنندگان زیادی به اشتراک گذاشته شود، این ادغام تحولی کلیدی خواهد بود. برای مثال، برای رای گیری الکترونیک، یا به روز سازی Firmware های دستگاه های متصل در IOT، همچنین بهبود اقتصاد مشارکتی در حوزه هایی نظیر شهرهای هوشمند و خودروهای هوشمند.

اشتراک داده های مطمئن می تواند برای عضو کردن شرکت کنندگان جدید در اکوسیستم ها مطلوب باشد و به بهبود خدمات و سازگاری آن ها کمک کند؛ بنابراین استفاده از بلاک چین می تواند اینترنت اشیا را با اطلاعات مطمئن و امن کامل



[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. از این رو حریم خصوصی و امنیت دو دغدغه اصلی IOT خواهند بود [۱۴].



شکل ۱: نمونه سیستم اینترنت اشیا

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 از جمله 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.

از آنجا که 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 پیش‌رو برای ادغام بلاک چین و IoT بسیار زیاد است از جمله گمنامی گره‌ها، مقیاس‌پذیری و احراز هویت که در اینجا راه‌حلی جهت بهبود مسئله احراز هویت ارائه خواهد شد.

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 قرار گرفته‌اند. 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.

پس از آن پلتفرم‌های IOT داده‌ها را به منظور 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 با اتصال میلیاردها دستگاه به شبکه IOT در سال‌های آتی، بسیار محدود خواهد بود و امنیت شبکه به خاطر داشتن میلیاردها نقطه ضعف به خطر می‌افتد. همچنین اگر قرار باشد در آینده اشخاص ثالث به‌طور مداوم هر تراکنش کوچک بین دستگاه‌ها را تأیید و بررسی کنند، این سیستم به یک سیستم کند و بسیار پرهزینه تبدیل خواهد شد



۲-۵- قراردادهای هوشمند بلاک چین

قراردادهای هوشمند^۱ در شبکه های بلاک چینی، یک توافق برای دستگاه ها ایجاد می کنند که در صورت تکمیل شرایط خاص اجرا شده و باعث می شوند که آن ها به صورت امن و مستقل کار کنند. از این رو تبادل اطلاعات کم هزینه تر، مقیاس پذیرتر و مستقل تر خواهد بود (نیاز نیست هیچ شخص ثالثی بر مبادلات نظارت داشته باشد). این قرارداد هوشمند می تواند از نیت افرادی که می خواهند از این اطلاعات به نفع خودشان استفاده کنند نیز جلوگیری کند. در چنین سیستمی اطلاعات در سرتاسر یک شبکه امنیتی رمزنگاری شده غیرمتمرکز منتشر می شوند. بدین ترتیب دست بردن در امنیت شبکه کار بسیار دشواری خواهد بود.

در نهایت در یک شبکه متمرکز، احتمال از کار افتادن فقط با یک اشتباه کوچک بسیار زیاد است. در یک شبکه غیرمتمرکز بلاک چینی این ریسک از طریق میلیون ها گره که اطلاعات را بر اساس یک سیستم نظیر به نظیر جابجا می کنند، کاهش می یابد و مابقی شبکه IoT بدون مشکل کار کند.

یکی از مهم ترین ویژگی های بلاک چین، تغییرناپذیری آن است، بلاک چین بر اساس یک مدل خرد جمعی کار می کند؛ 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 می بایست تعداد زیادی از موجودیت های مستقل در بلاک چین را تغییر دهند پس شفافیت کامل بلاک چین به

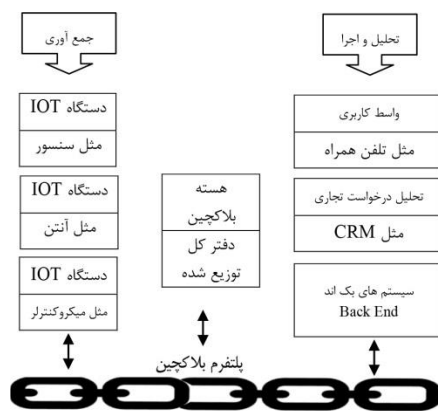
شرکت ها کمک می کند تا در صورت رخ دادن نقص امنیتی، بتوانند با واکنشی سریع تر به حالت اولیه برگردند.

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 نشانه ها به جای اینکه ارزش پولی داشته باشند، در مورد توزیع اختیار رأی دادن بین گره ها و تبادلات معین تصمیم می گیرند 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 دستگاه ها ایجاد شود می باشد.

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

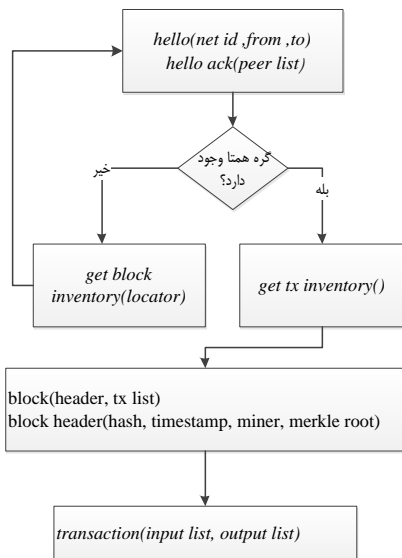
با حذف درگاه اینترنت اشیا به صورت متمرکز عملاً یک اتصال P2P میان دستگاه ها ایجاد می کنیم. (شکل ۲)



^۱ Smart Contract



قبول یا رد تراکنش، میان گره‌های موجود در شبکه را در برمی‌گیرد. ما مجموعه‌ای از پیام‌ها را در این لایه تعریف می‌کنیم تا در رسیدن 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 اتفاق نظر 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 به روز می‌شود که میانگین زمان

شکل ۲: نمونه تغییر یافته شده با بلاک چین

۲-۳- فاز دوم : تنظیم قرارداد های هوشمند به

صورت غیر متمرکز

با ارائه دفتر کل پراکنده (Ledger)، جهت تنظیم قراردادهای هوشمند به صورت 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 ارائه شده با بلاک چین

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

۳-۳- فاز سوم : افزودن لایه هوشمند

پروتکل بلاک چین به معماری سه لایه

اینترنت اشیا

در لایه پروتکل بلاک چین الگوریتم اتفاق نظر 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 اتفاق نظر برای

^۱ Memory Pool (mempool)



از فساد یا شکست مجموعه جلوگیری می کند.

امنیت این شبکه توزیع شده باید تضمین شده باشد. تأیید تراکنش ها نتیجه اجرای قوانین پروتکل توسط تمام شبکه است.

لایه کاربری بلاک چین تبادلات خاص امنیتی در اینترنت اشیا را برقرار ساخته و چگونگی تراکنش آن ها را برای لایه های بالاتر تعریف می کند. کارکرد اصلی که به وسیله مدل کاربری پیشنهادی ما فراهم می شود احراز هویت و صلاحیت برای دستگاه ها در شبکه های اینترنت اشیا است.

در این روش برای هر گره یک مجموعه با ۴ پشته تعریف می کنیم و در پشته ها به ترتیب مقادیر $id-1$ ، $K_{pu}-2$ کلید عمومی، $K_{pr}-3$ کلید خصوصی و $4-KDS$ تولیدکننده کلید عمومی برای جلوگیری از حمله قرار می دهیم.

این روش از ترکیب رمزنگاری و احراز هویت به منظور تأیید هویت دو طرف استفاده می کند، 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 می گردد. در سمت گیرنده این پیام ابتدا با کلید خصوصی گیرنده سپس با کلید عمومی فرستنده از حالت رمز خارج می شود.

این کار برای فراهم کردن احراز هویت پویا و اجتناب از حملات نمایش مجدد (Replay Attack) در شبکه است.

۴- مطالعات میدانی (Case Study)

از آنجاکه جهت راست آزمایی و نتیجه گیری از تحقیق به دست آمده نیازمند به جمع آوری داده های کمی و کیفی هستیم، لذا از روش مطالعات میدانی

پیش بینی شده برای یافتن بلوک بعدی (بر اساس عددی معین از بلوک های آخر گرفته می شود) برابر با مقداری معین باشد.

- با دریافت بلوک جدید، گره تأیید می کند که بلوک با همه قواعد پروتکل مطابقت دارد و همه تبادلات در بلوک طبق قواعد پروتکل و کاربری است.

- بعد از تأیید بلوک دریافتی، گره نظر خود را درباره بلاک چین بروز می کند، تبادلات شامل شده را از استخر حافظه پاک می کند و بلوک را پخش می کند.

- در نهایت، همه گره ها نظر یکسان درباره بلاک چین دارند [۱۶].

بدین ترتیب میان گره ها امنیت بر اساس خرد جمعی جهت برقراری بلاک چین برقرار می شود حال پس از راه اندازی بلاک چین نیازمند به احراز هویت بین گره ها هستیم لذا در ادامه به اقدامات انجام شده در لایه کاربردی می پردازیم.

۳-۴- فاز چهارم : افزودن لایه هوشمند

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 آن ها را برای لایه های بالاتر را تعریف می سازیم.

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

اما تأیید 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 توزیع شده نظیر به نظیر است. یک شبکه توزیع شده



بهره برده و در ادامه به شرح آن می پردازیم.

۴-۱- ناحیه بندی شهر هوشمند

برای این منظور فرض می کنیم شهر مدنظر را ناحیه بندی کردیم و در هر ناحیه یک گره گیرنده بی سیم قرار دارد. از طرف دیگر در تمامی ماشین های این شهر هوشمند حسگرهایی تعبیه گشته است که وظیفه آن اعلام وجود در ناحیه به نودهای گیرنده موجود در همان ناحیه هست به این صورت که در صورت ورود یک ماشین از ناحیه قبلی به ناحیه جدید باید تعداد ماشین های موجود در ناحیه قبلی یک عدد کم شود و تعداد ماشین های موجود در ناحیه جدید یک عدد اضافه شود. پس می توان با ارتباط میان نودها با یکدیگر این مشکل را رفع کرد بدین صورت که در صورت اعلام تراکنش یک ماشین با یک نود سایر نودها بررسی کنند که اگر ماشین در ناحیه خود موجود است، آن ها از ناحیه خارج سازند. پس اولین قانون در شبکه این خواهد بود که هر ماشین تنها در یک ناحیه موجود هست. به عبارت دیگر شناسه ماشین های موجود در کل شبکه باید به صورت یونیک، تنها در یک ناحیه ثبت شده باشد.

۴-۲- اطلاع رسانی از سطح ترافیک

پس از ثبت ماشین ها در نواحی نیازمند به اطلاع رسانی از سطح ترافیک موجود در مسیر انتخابی هستیم. لذا ماشین هایی که قصد سفر به مسیری جدید را دارند پیش از حرکت باید به گیرنده های موجود در مسیرهای انتخابی درخواست بفرستند و گیرنده ها در پاسخ بر اساس فرمول های خاص ترافیک سنجی به ماشین هایی که قصد سفر به مسیر ناحیه را دارد مجوز ورود را صادر یا لغو می کنند.

برای مثال اگر پهنای باند ناحیه را p در نظر

گرفته و تعداد ماشین های موجود را q در نظر بگیریم و ترافیک ناحیه را T در نظر بگیریم می توان از رابطه $T = \frac{q}{p}$ میزان ترافیک ناحیه را به دست آورد و برحسب مسافت هر مسیری که مقدار T آن کمتر بود، می توان مسیر انتخابی برای سفر در نظر گرفته شود.

حال با توجه به مطالعات میدانی عنوان شده قصد داریم تا جهت ثبت ارتباط میان ماشین و گره های ناحیه (قسمت اول) از بلاک چین استفاده کنیم.

۴-۳- نحوه عملکرد

جهت صحت گذاری بر مقادیر ماشین های موجود در ناحیه ها و تراکنش انتقال یک ماشین از یک ناحیه به ناحیه دیگر مدل بلاک چین (بیت کوین) استفاده می کنیم. بدین صورت که تراکنش ها به صورت پشت سر هم در بلاک هایی ذخیره می گردند و تمامی نودها دسترسی مشاهده و تأیید ایجاد بلاک ها را دارند و در صورت عدم تأیید نباید بلاک تراکنش ایجاد گردد حال با توجه به شکل ۴ فرض می کنیم:

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

۲- داده اعلام وجود از سمت ماشین به گره ناحیه ۲ ارسال می گردد.

۳- گره ناحیه ۲ ورود ماشین را ثبت می کند.

۴- گره ناحیه ۲، ID ماشین را به گره ناحیه قبل (ناحیه ۱) اطلاع رسانی می کند.

۵- گره ناحیه ۱، ماشین را از جدول ماشین های فعلی حذف کرده یا فلک خروج را فعال می کند.

مجوز ورود به ناحیه با استفاده از بلاک چین:

پهنای باند ناحیه ۲، $N2p=150$ هست و

تعداد ماشین ناحیه ۲، در حال حاضر $N2q=41$ عدد هست.



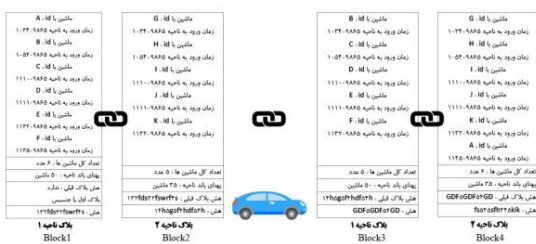
شبکه به اشتراک گذاشته می شوند و با استفاده از رمزنگاری امکان حذف و دست کاری اطلاعات ثبت شده تقریباً غیرممکن است.

بیت کوین اولین کاربرد از این فناوری بود و از بلاک چین برای ذخیره اطلاعات دارایی کاربران بهره برد. اگر بلاک چین یک سیستم عامل باشد، بیت کوین نرم افزاری روی این سیستم عامل 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 می گزاریم.

در هر بلاک هر اطلاعاتی می تواند ثبت شود؛ که ما در اینجا اطلاعات مربوط به تعداد ماشین های موجود در هر ناحیه را قرار خواهیم داد. در بلاک چین، اطلاعات در بلاک ها قرار می گیرند و باهم به صورت زنجیره ای مرتبط می شوند.

برای مثال بلاک چین (شکل ۵) را در نظر بگیرید، هر بلاک یک ناحیه ترافیکی را نشان می دهد که ID ماشین های موجود در آن ناحیه در آن ثبت شده هستند.



شکل ۵: بلاک چین کیس استادی

با مشاهده شکل ۵ برای بلاک ناحیه ۱ (Block1) که حاوی اطلاعات ورود ماشین های A,B,C,D,E,F است، هش بلاک «132fds32fswrf4s» است. در بلاک چین، هش بلاک های بعدی حاوی هش بلاک قبلی هم هستند. هش در هر بلاک چین با یک تابع ریاضی

۲ آیتم بالا تائید شده و بلاک اول را می سازد

ماشین a از ناحیه ۱ به ناحیه ۲ وارد می شود پس تعداد ماشین ناحیه ۲ از ۴۱ به ۴۲ تغییر پیدا می کند. اگر $p-q > 0$ باشد (تائید می شود و به عنوان دومین بلاک ذخیره می گردد).

تعداد ماشین ناحیه ۱ به میزان یک واحد کم می شود (تائید می شود و به عنوان سومین بلاک ذخیره می گردد).

در ادامه به همین ترتیب سایر بلاک ها ساخته می شود.

در صورتی که مقدار $p-q < 0$ شود بلاک جدید تائید نمی شود و در اصل تراکنش صورت نمی پذیرد و ماشین باید پشت گیت صف انتظار (پشت چراغ قرمز) بماند تا زمانی که $p-q$ ناحیه جدید عددی بزرگ تر از ۰ شود.

با توجه به مثال گفته شده و شرح آن که در شکل ۴ قابل مشاهده هست به بررسی چگونگی کار در لایه پروتکل بلاک چین خواهیم پرداخت.



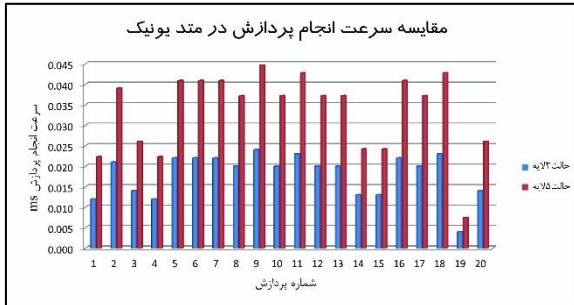
شکل ۴: پیاده سازی تصویری کیس استادی

۴-۴- طراحی بلاک چین Case Study

همان طور که گفته شد به طور کلی بلاک چین یک نوع سیستم ثبت اطلاعات و گزارش است. تفاوت آن با دستگاه های دیگر این است که اطلاعات ذخیره شده روی این نوع سیستم، میان همه اعضای

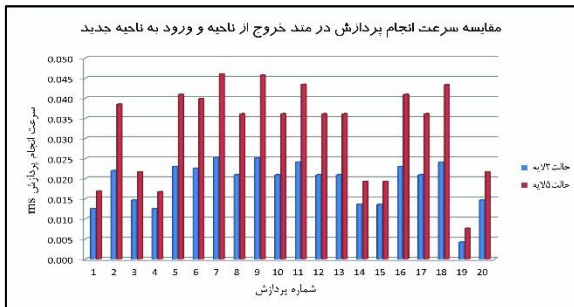


متداول (یونیک): هنگامی که فقط ماشین جدید در ناحیه جدید معرفی می گردد حالت اول با در نظر گرفتن قراردادهای هوشمند و حالت دوم بدون در نظر گرفتن قراردادهای هوشمند.



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

متد دوم: هنگامی که فقط ماشین از ناحیه پیشین خروج و به ناحیه جدید وارد می شود 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 می توان تفاوت امنیت میان استفاده از بستر قراردادهای هوشمند و حالت عادی را در جدول شماره ۳ به بحث کشید.

خاص به دست می آید که توسعه دهندگان آن را مشخص می کنند. کوچک ترین تغییر در اطلاعات یک بلاک، هش آن را به طور کلی تغییر می دهد.

مثلاً اگر یک کاراکتر به اطلاعات ماشین های ناحیه ۱ اضافه شود، هش بلاک تغییر می کند و در نتیجه بلاک های بعدی هم غیر معتبر خواهند شد به همین دلیل این فناوری بلاک چین یا زنجیره بلاک ها نام دارد.

اگر کسی محتوای یک بلاک را تغییر دهد و هش بلاک های بعدی را به روزرسانی کند، چه می شود؟ این امکان وجود دارد اما شما توزیع را در نظر نگرفته اید. داده های بلاک چین در یک کامپیوتر یا سرور خاص ذخیره نمی شوند. هر کامپیوتر یا سیستمی که به شبکه وصل شود یک نسخه از بلاک چین را دریافت می کند.

حال مثلاً با ورود ماشین A از ناحیه ۱ به ناحیه ۲ باید در قالب یک بلاک جدید اطلاعات ناحیه ۱ تغییر کند و ماشین A از آن حذف گردد (Block3) و به همین ترتیب در بلاک بعدی اطلاعات ناحیه ۲ تغییر کرده و ماشین A به آن اضافه می گردد (Block4).

۵- اثر بلاک چین بر سرعت و پایداری IOT

در ادامه به بحث و مشاهده در رابطه با نتایج به دست آمده از مطالعات میدانی می پردازیم و با آزمایش بر روی ۲۰ پردازش اول پشت سر هم در حالات قید شده به جمع مشاهدات می پردازیم و در نهایت به نتیجه گیری نهایی در رابطه با تحقیق می رسیم.

۵-۱- بحث

برای به دست آوردن یک تحلیل قابل استفاده از سرعت عملکرد سامانه می بایست در دو متد در رابطه با آن بحث کرد:



Scale Disturbuted Peer to Peer یک مدل

Out است و این بدان معنی است که هر چه میزان نودهای شبکه بالاتر برود پایداری شبکه بیشتر می گردد و این امر در امنیت نتیجه چشم گیری است همچنین ویژگی های 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 چالش های پیاده سازی بلاک چین را در شبکه IoT بشناسد. در حال حاضر، نتایج کامل و دقیقی درباره مقیاس پذیری 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 مورد تحقیق 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 شبکه های IoT سطوح حملات و آسیب پذیری های وسیعی دارند. تحقیق حاضر را می توان به گونه ای بسط داد که سطوح حملات بیشتری را پوشش دهند و کاربرد های خاص IoT را در برگیرد و همچنین جهت حل مشکلات منوط به پیچیدگی زمانی اقدام نمود و برای برآوردن الزامات عملکردی سیستم بلادرنگ بهینه سازی شود.

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

۸- مراجع

[1] Gokhale, Pradyumna, Omkar Bhat, and Sagar Bhat. "Introduction to IOT." *International Advanced Research Journal in Science, Engineering and Technology* 5.1 (2018): 41 - 44.

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

حالت عادی (۳ لایه)

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 امکان پذیر است	فناوری blockchain می تواند ایجاد شبکه های IoT را امکان پذیر سازد که (P2P) هستند.
Man in the Middle	به دلیل یک مرحله احراز هویت ممکن است	به دلیل وجود چندین مرحله احراز هویت در هش بین بلاک ها غیرممکن

۵-۲- مشاهدات

بر اساس مقایساتی که در شکل ۶ و همچنین شکل ۷ مشاهده می کنیم در حالات اول پایداری گره ها دارای تعدادی پراکندگی بوده ولی در حالتی که از قراردادهای هوشمند استفاده کردیم پایداری گره ها با افزایش تعداد گره ها رو به افزایش هست.

مشاهده می کنیم سرعت عملکرد در حالتی که از قراردادهای هوشمند استفاده نکرده ایم بدون در نظر گرفتن ناپایداری ها تقریباً در یک اندازه و در حدود ۰,۰۲ میلی ثانیه هست اما با اعمال قراردادهای هوشمند سرعت انجام پردازش با بیشتر شدن تعداد گره ها افزایش پیدا می کند.

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

۶- نتیجه گیری

این تحقیق روش جدیدی را جهت بهبود مسئله امنیت IoT به وسیله بلاک چین ارائه داده است. در این مقاله نشان داده شده که بلاک چین راه حلی عملی برای مسئله امنیت IoT است. روش



"Forecast alert: internet of things—endpoints and associated services, worldwide, 2016." Gartner (2016).

[15] Hallman, Roger. "IoDDoS-The Internet of Distributed Denial of Service Attacks-A Case Study of the Mirai Malware and IoT-Based Botnets." *IoTBDS*. 2017.

[16] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system. (2008).



محمد سعید صفایی صادق

مدرک کارشناسی خود را در رشته مهندسی نرم افزار 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 شبکه های کامپیوتری از دانشگاه آزاد اسلامی واحد آشتیان اخذ کرده است. زمینه های پژوهشی موردعلاقه ایشان عبارتند از: بلاک چین، محاسبات توزیع شده



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 به عنوان هیات علمی دانشگاه آزاد مشغول به کار هست. زمینه های پژوهشی موردعلاقه ایشان عبارتند از: محاسبات توزیع شده، محاسبات ابری، الگوریتم های زمانبندی، محاسبات نرم، محاسبات فراگیر و مجازی سازی

نشانی رایانامه ایشان عبارت است از: myrshg@gmail.com

[2] Balasubramaniam, Yamunaa, and P. S. V. Sathyanarayanan. (Enhancing Connected Vehicle Security with Block chain) (2018).

[3] Gupta, Yash. "The applicability of blockchain in the Internet of Things." 2018 10th International Conference on Communication Systems & Networks (COMSNETS). IEEE, 2018.

[4] Gia, Tuan Nguyen. "Fault tolerant and scalable IoT-based architecture for health monitoring." 2015 IEEE Sensors Applications Symposium (SAS). IEEE, 2015.

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

[6] Balasubramaniam, Yamunaa, and P. S. V. Sathyanarayanan. "Enhancing Connected Vehicle Security with Block chain. « (2018).

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

[8] Abera, Tigist. "Things, trouble, trust: on building trust in IoT systems." *Proceedings of the 53rd Annual Design Automation Conference*. ACM, 2016.

[9] Mattila, Juri. *The blockchain phenomenon—the disruptive potential of distributed consensus architectures*. No. 38. ETLA working papers, 2016.

[10] 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* 67 (2016): 99 - 117.

[11] Yazdinejad, Abbas. "Blockchain-enabled Authentication Handover with Efficient Privacy Protection in SDN-based 5G Networks." *arXiv preprint arXiv:1905.03193* (2019).

[12] Vahid Rad - *Great Blessing of Blockchain Technology – 2018*

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

[14] Rivera, J., and R. van der Meulen.