دوفصلنامه محاسبات و سامانه‌های توزیع شده
سال هفتم، شماره ۱، شماره پیاپی ۱۳، صفحه ۱۰۶ تا ۱۲۳، سال ۱۴۰۳

مرور و مقایسه بر تکنیک‌های افزایش امنیت سیستم‌های اینترنت اشیاء مبتنی بر بلاک‌چین

مائده رحمانی[۱]، فرشید وظیفه دوست[۲]، سمیه کدخدا ده‌خانی[۲]، حمید زنگی آبادی زاده[۳] و مهدی قاسمی[۳]
[۱] دانشکده مهندسی کامپیوتر گرایش نرم افزار ،دانشگاه پیام نور مرکز بین الملل کیش
[۲] دانشکده مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز از دانشگاه پیام نور مرکز بین الملل قشم
[۳] دانشکده مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز ،دانشگاه پیام نور مرکز بین الملل کیش

چکیده

دستگاه‌های اینترنت اشیاء که به سرعت در حال رشد هستند، به دلیل ماهیت غیرمتمرکز، قدرت محاسباتی محدود و اتکا به مدل‌های امنیتی متمرکز، چالش‌های امنیتی قابل توجهی ایجاد می‌کنند. فناوری بلاک‌چین به دلیل ماهیت غیرمتمرکز، تغییرناپذیر و شفاف آن به عنوان یک راه حل بالقوه ظاهر شده است و امنیت پیشرفته‌ای را برای محیط‌های اینترنت اشیاء فراهم می‌کند. این مطالعه یک استراتژی امنیتی مبتنی بر بلاک‌چین را با هدف کاهش خطرات امنیتی در شبکه‌های اینترنت اشیاء پیشنهاد می‌کند. این مطالعه نشان می‌دهد که فناوری بلاک‌چین می‌تواند با پرداختن به محدودیت‌های مدل‌های امنیتی سنتی و متمرکز، امنیت شبکه اینترنت اشیاء را به طور قابل‌توجهی بهبود بخشد. می‌توان دستگاه‌های بلاک‌چین و اینترنت اشیاء را ترکیب کرد و با استفاده از احراز هویت دستگاه قراردادهای هوشمند، تأیید یکپارچگی داده‌ها، و دسترسی به نتایج، سرعت احراز هویت، کارایی انرژی، تأخیر کلیدی مناسب‌تر را بهبود بخشید. محیط های اینترنت اشیاء این سیستم با استفاده از مکانیسم‌های اجماع سبک وزن، می‌تواند مصرف انرژی پایین را حفظ کند و در عین حال، تراکنش‌های با حجم بالا را در زمان واقعی پردازش کند.

کلمات کلیدی: افزایش امنیت ، شبکه های اینترنت اشیاء و بلاک‌چین

تاریخچه‌ی مقاله:
تاریخ ارسال: ۱۴۰۲/۱۱/۲۷
تاریخ اصلاحات: ۱۴۰۳/۰۵/۰۳
تاریخ پذیرش: ۱۴۰۳/۰۶/۰۱
تاریخ انتشار: ۱۴۰۳/۰۶/۳۰
ایمیل نویسنده مسئول:Maede9708@gmail.com

۱ – مقدمه

اینترنت اشیاء که به سرعت در حال گسترش است، صنعت را متحول کرده است و اشیاء روزمره را به دستگاه‌های به هم پیوسته‌ای تبدیل کرده است که از لوازم خانگی هوشمند ذخیره، به اشتراک گذاشته و پردازش می‌کنند و امکان کنترل فن‌آوری‌ها تا سنسورهای صنعتی و سیستم‌های نظارت سلامت تا دستگاه‌های انعطاف‌پذیر اینترنت اشیاء، اتوماسیون و برنامه‌های کاربردی را به طور تصاعدی افزایش داده است، اما استفاده گسترده از دستگاه‌های اینترنت اشیاء چالش‌های امنیتی قابل توجهی را نیز ارائه می‌کند. این دستگاه‌ها اغلب از نظر قدرت محاسباتی، حافظه و قدرت کمبود دارند و آنها را به ویژه در برابر طیف وسیعی از حملات سایبری مانند حملات انکار سرویس توزیع شده، دسترسی غیرمجاز، نقض داده‌ها و تغییرات آسیب‌پذیر می‌سازد. مدل‌های امنیتی متمرکز بر طبیعت سنتی در رسیدگی به نیازهای امنیتی منحصر به فرد شبکه‌های اینترنت اشیاء ناکافی هستند. سیستم‌های متمرکز معمولاً برای احراز هویت دستگاه‌ها، نظارت بر جریان داده‌ها و انجام ارتباطات ایمن به یک نقطه کنترل تکیه می‌کنند. با این حال، این رویکرد با آسیب‌پذیری‌های قابل‌توجهی همراه است، مانند نقاط شکست، حداقل تخریب ناپذیری، سطوح بالای حملاتی که مقامات متمرکز را هدف قرار می‌دهند و راه‌حل‌های امنیتی متمرکز اینترنت اشیاء نیز با افزایش چشمگیر تعداد دستگاه‌ها، افزایش بیشتر خطر آسیب را دشوارتر می‌کند. فناوری بلاک‌چین با ساختار غیرمتمرکز، شفاف و تغییرناپذیر خود، راه حلی امیدوارکننده برای افزایش امنیت شبکه‌های اینترنت اشیاء ارائه می‌دهد. بلاک‌چین که در ابتدا برای تراکنش‌های مالی ایمن در ارزهای رمزنگاری شده توسعه یافته بود، تبدیل به یک فناوری همه کاره شده است که در زمینه-های مختلفی از جمله زنجیره تامین، مراقبت‌های بهداشتی مورد استفاده قرار می‌گیرد و اکنون بلاک‌چین با اهرم امنیت

سایبری، شبکه‌های اینترنت اشیاء را قادر می‌سازد از مدل‌های امنیتی متمرکز به غیرمتمرکز تبدیل شوند و قابلیت اتصال فعال می‌شود[۱].

رشد انفجاری در استقرار اینترنت اشیاء به دلیل اتکا به ذخیره‌سازی متمرکز داده که در برابر نقض داده ها آسیب-پذیر است، چالش‌های امنیتی و حریم خصوصی قابل توجهی را به همراه داشته است. ویژگی‌های غیرمتمرکز و مقاوم در برابر دستکاری بلاک‌چین‌ها راه حلی بالقوه برای این چالش‌ها ارائه می‌دهد و چارچوبی امن برای مدیریت داده ها در اینترنت اشیاء ارائه می دهد. این مطالعه با هدف ارائه یک بررسی جامع از یکپارچگی اینترنت اشیاء و بلاک‌چین و تجزیه و تحلیل نیازمندی‌ها، چالش‌ها و راه‌حل‌های منحصربه‌فردی است که هنگام تلاقی این دو فناوری به وجود می‌آیند. در این مقاله در بخش اول به مفاهیم عمومی بلاک‌چین و اینترنت اشیاء پرداخته می‌شود و سپس در بخش اصلی به بلاک‌چین برای اینترنت اشیاء، کاربرد بلاک‌چین در اینترنت اشیاء ، بلاک‌چین برای اینترنت اشیاء و مقایسه مطالعات مرتبط ادغام اینترنت اشیاء و بلاک چین جهت افزایش امنیت بررسی خواهد شد.

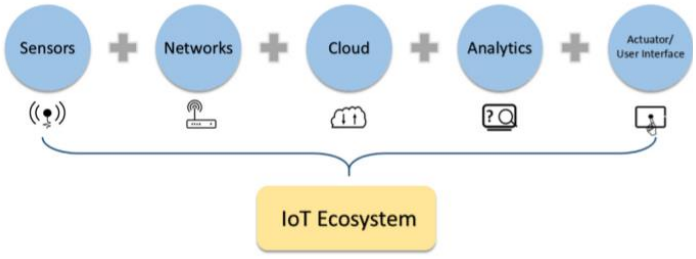
۲ – اینترنت اشیاء

امروزه اینترنت به مسئله‌ای فراگیر تبدیل شده و تقریبا هر گوشه از کره جهان را تحت پوشش قرار داده‌است و به شیوه‌های غیر قابل تصور بر زندگی انسان تاثیر می‌گذارد و به هر حال، این روند هنوز ادامه دارد. حال جهان وارد عصر اتصال جامع شده که در آن انواع گسترده وسایل به وب وصل می‌شوند. در واقع جهان وارد عصر "اینترنت اشیاء" شده‌است که مولفین در این زمینه به شیوه‌های مختلف به تعریف این مسئله پرداختند. در زیر به معرفی دو تعریف پرداخته شده-است[۲]:

- ورمیزن با همکاران اینترنت اشیاء را صرفا تعادل بین جهان فیزیکی و دیجیتال تعریف می‌کنند. جهان دیجیتال از طریق حس گره‌ها و محرک‌های بی-شماری با جهان فیزیک تعادل برقرار می‌کند.

پنالوپز با همکاران اینترنت اشیاء را به عنوان الگویی تعریف می‌کنند که در آن محاسبه و شبکه‌بندی قابلیت‌ها در هر نوع شی امکان‌پذیر نهفته شده‌است. از این توانمندی‌ها برای جستجوی وضعیت شی و تغییر وضعیت آن در صورت ممکن استفاده می‌شود. به بیان ساده‌تر، اینترنت اشیاء اشاره به نوع تازه‌ای از جهان دارد که در آن تقریبا تمامی ابزارها و وسایل که استفاده می‌شود به شبکه‌ای متصل‌اند. می‌توان از آنها به طور مشترک استفاده کرد تا فعالیت‌های پیچیده‌ای را انجام داد که نیاز به درجه هوش بالایی دارد.

از دید کاربران، یک سیستم اینترنت اشیاء معمولی با توجه به سهم و عملکرد اجزای موجود در سیستم اینترنت اشیاء شامل پنج مولفه اصلی: دستگاه ها یا سنسورها (ترمینال)، شبکه ها (زیرساخت ارتباطی)، ابر (مخزن داده و زیرساخت پردازش داده)، تجزیه و تحلیل (الگوریتم محاسباتی و داده کاوی) و محرک ها یا رابط های کاربر (خدمات) است که نمایی از این مولفه ها در شکل ۱ نمایش داده شده است[۳].



شکل ۱: اجزای یک سیستم اینترنت اشیاء[۳].

در واقع اصطلاح اینترنت اشیاء با توجه به چارچوب مفهومی سال ۲۰۲۰ از طریق فرمولی ساده به صورت زیر است[۴]:

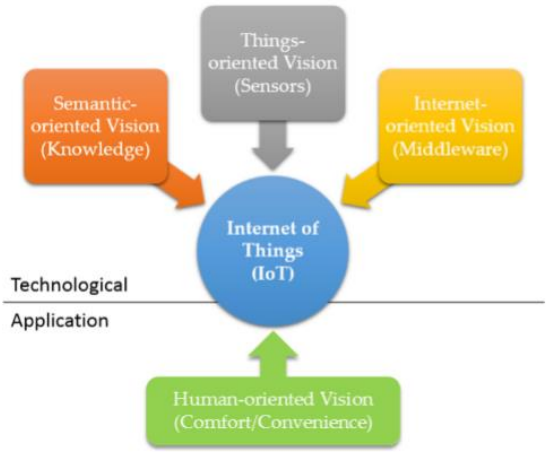
IoT= Services+ Data+ Networks + Sensors

اینترنت اشیاء یک نوع پلت فرم منبع بازاست که برنده اولین جایزه بوده، کشف و ادغام دستگاه‌های مبتنی بر اینترنت اشیاء را فراهم می‌کند. اینترنت اشیاء تلفیقی از شبکه‌های ناهمگن از جمله فناوری تراشه است و به دلیل رشد سریع برنامه‌های اینترنتی مانند تدارکات، کشاورزی، جامعه هوشمند، انتقال هوشمند، سیستم‌های کنترل و ردیابی به تدریج بیشتر و بیشتر گسترش می‌یابند. طبق تجزیه و تحلیل محققین در سال ۲۰۲۰ اشیاء، اینترنت اشیاء نیمه هوشمند و بخشی مهم از زندگی اجتماعی انسان خواهند بود[۴].

۳- چهار الگوی اصلی تعریف اینترنت اشیاء

به طور گسترده‌ای استفاده از فن‌آوری‌های جدید یک پیش نیاز اساسی برای دستیابی به تحقق ساختمان‌های هوشمند شناخته می‌شود که شامل: استقرار سنسور، مهندسی داده‌های بزرگ و تجزیه و تحلیل، ابر و مه است اما به آنها محدود نمی‌شود[۵, ۶].

در میان این فن‌آوری‌های پشتیبانی، یکی از زمینه-های پرطرفدار توسعه اینترنت اشیاء است که به عنوان یکی از چالش‌های ساختمان‌های هوشمند برای مقابله با یک شبکه پیچیده از موجودیت‌های عملکردی به هم پیوسته در جنبه-های مختلف ساختمان است. با استفاده از اینترنت اشیاء، یک پتانسیل عظیم برای پیشرفت قابل توجه در جهت اهداف پیش‌بینی شده وجود دارد. از نظر فناوری، اینترنت اشیاء ممکن است به عنوان همگرایی سه الگوی اصلی: چشم انداز چیزگرا، چشم‌انداز اینترنت محور و چشم انداز معناگرا شناخته شود. بر این اساس، نویسندگان یک چشم‌انداز انسان محور که به عنوان الگوی چهارم در سمت برنامه ادغام شود، پیشنهاد می‌کنند که نمایی از آن در شکل ۲ نمایش داده شده‌است[۷].



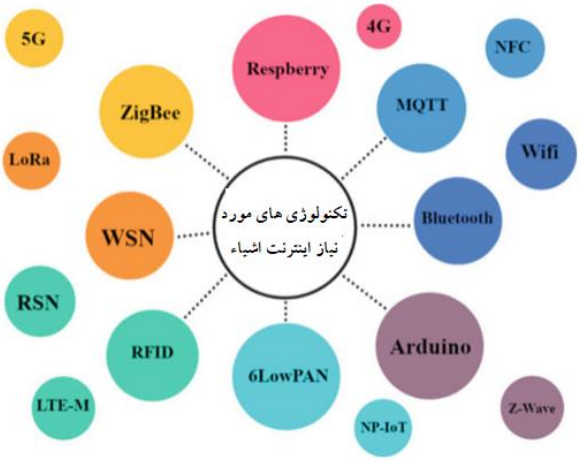
شکل۲: چهار الگوی اصلی تعریف اینترنت اشیاء[۷].

معماری اینترنت اشیاء ساخته شده تا تمام اشیاء را به قابلیت شناسایی، سنجش، شبکه و پردازش مجهز کند، بنابراین این اشیاء می‌توانند اطلاعات را با یکدیگر تبادل و به اشتراک بگذارند و خدمات پیشرفته را از طریق اینترنت توسعه دهند. بنابراین، اتصال بیشتر بینش عمیق سیستم‌های پیچیده را تسهیل کرده و قابلیت‌های تصمیم‌گیری آگاه از زمینه پویا و خودمختاری هوشمند را فراهم می‌کند. این قابلیت‌ها راه را برای دستیابی به اهداف در ساختمان‌های هوشمند که دارای هوش محیطی یکپارچه‌اند، با ایجاد یک شبکه جهانی با پشتیبانی از رایانش فراگیر و بافت آگاه[1] میان دستگاه‌ها، محیط فراهم می‌کند[۸].

۴- تکنولوژی های مورد نیاز اینترنت اشیاء

اینترنت اشیاء یکی از نوآوری‌های در حال توسعه قرن حاضر است. جنبه‌های مختلف آن مانند زیرساخت، معماری و امنیت، نقش مهمی در شکل‌گیری دنیای دیجیتالی بلندمدت ایفا می‌کند. دستگاه‌های متصل که عموماً به عنوان اینترنت اشیاء شناخته می‌شوند، به سرعت در حال گسترش هستند. چارچوب شبکه باید با ارائه یک شبکه خوب و ارائه خدمات مبتنی بر برنامه، برای همه این دستگاه‌ها مناسب باشد. با توجه به اینکه اینترنت اشیاء به عنوان مرحله متعاقب پیشرفت وب به آهستگی افزایش می‌یابد، شناخت حوزه های بالقوه مختلف برای کاربرد اینترنت اشیاء و پرس و جو در مورد چالش‌های مربوط به این برنامه ها بسیار مهم است.

در حال حاضر، فقط دو نوع ارتباط وجود دارد: انسان با انسان و انسان با دستگاه. با این حال، اینترنت اشیاء آینده‌ای خارق‌العاده را برای وب تضمین می‌کند که در آن اتصال ماشین به ماشین حالت اولیه ارتباط است. اینترنت اشیاء به دلیل خلاقیت و عامل سرگرم کننده‌اش بسیار جذاب است و پیش‌بینی می‌شود که اینترنت اشیاء در آینده بسیار پیشرفته‌تر شود[۹].



شکل۳: نمایی از تکنولوژی های مورد نیاز اینترنت اشیاء[۱۰].

اینترنت اشیاء را می‌توان در دنیای واقعی با ادغام چندین فن‌آوری و پروتکل همانطور که در شکل ۳ نشان داده شده است تحقق بخشید. در این بخش، برخی از فناوری‌های فعال کننده مرتبط ارائه شده است[۱۰]:

شناسایی فرکانس رادیویی[2]: یک فناوری مبتنی بر تبادل اطلاعات با استفاده از سیگنال‌های الکترومغناطیسی

[1] context-awareness

[2] Radiofrequency identification (RFID)

است. این یک فناوری ارتباطی غیر تماسی است که عموماً برای دنبال کردن و شناسایی دستگاه‌های اینترنت اشیاء بدون هیچ گونه تماسی استفاده می‌شود. از تبادل اطلاعات در فاصله کوتاه از طریق سیگنال های رادیویی پشتیبانی می کند. از محدوده فرکانس ۱۲۵ کیلوهرتز برای فرکانس پایین، ۱۳.۵۶ مگاهرتز برای فرکانس بالا ، [۸۶-۹۶۰، ۴۳۳] مگاهرتز برای فرکانس فوق‌العاده و [۲.۴۵، ۵.۸] گیگاهرتز برای مایکروویو استفاده می‌کند.

این سیستم از یک برچسب شناسایی فرکانس رادیویی، یک خواننده شناسایی فرکانس رادیویی و یک آنتن تشکیل شده است. تگ شناسایی فرکانس رادیویی یک تراشه کوچک است که دارای یک شماره شناسایی منحصر به فرد است و به آنتن متصل است. هر تگ شناسایی فرکانس رادیویی به یک دستگاه اینترنت اشیاء متصل است. خواننده شناسایی فرکانس رادیویی دستگاه را شناسایی می کند و با جستجوی برچسب شناسایی فرکانس رادیویی از طریق سیگنال های مناسب، اطلاعات را دریافت می کند. آنتن شناسایی فرکانس رادیویی به گونه ای تنظیم شده است که فقط محدوده کوچکی از فرکانس های حامل را در مرکز سیستم شناسایی فرکانس رادیویی پوشش دهد.

شبکه حسگر بی‌سیم[3]: زیرساختی متشکل از محاسبات، حسگر و دستگاه‌های ارتباطی است که به مدیر اجازه می دهد تا ابزار، مشاهده و به رویدادها و پدیده ها در محیط های مشخص واکنش نشان دهد. شبکه حسگر بی سیم می‌تواند نقش مهمی در اینترنت اشیاء ایفا کند زیرا می‌تواند تعداد قابل توجهی از گره های حسگر را پشتیبانی کند و در عین حال عمر باتری کافی را حفظ کند. شناسایی فرکانس رادیویی و شبکه حسگر بی سیم را می‌توان برای اکتساب داده در اینترنت اشیاء استفاده کرد، اما عمدتاً شناسایی فرکانس رادیویی برای شناسایی دستگاه استفاده می‌شود. در مقابل، شبکه حسگر بی سیم برای درک پارامتر از محیط اطراف آنها استفاده می‌شود.

شبکه حسگر شناسایی فرکانس رادیویی[4]: شبکه حسگر شناسایی فرکانس رادیویی یک شبکه حسگر بی-سیم و یکپارچه‌سازی سیستم شناسایی فرکانس رادیویی است.

ادغام این دو فناوری می‌تواند حوزه برنامه‌ها را گسترش دهد و همچنین ارزش افزوده‌ای را به برنامه‌های موجود ارائه می‌دهد. پیاده سازی‌های مختلف شبکه حسگر شناسایی فرکانس رادیویی با موفقیت به دست آمد. به عنوان مثال، ادغام شناسایی فرکانس رادیویی و شبکه حسگر بی‌سیم نظارت مستمر داده‌ها را در سراسر زنجیره تامین مواد غذایی فراهم می‌کند و اطمینان حاصل می‌کند که خرده فروشان الزامات را در طول تحویل و ذخیره سازی محصول مانند حفظ دما و رطوبت مورد نیاز برآورده می‌کنند.

ارتباطات میدان نزدیکی: ارتباطات میدان نزدیک مبتنی بر فناوری مورد استفاده برای شناسایی فرکانس رادیویی است. با استفاده از باند شناسایی فرکانس رادیویی فرکانس بالای ۱۳.۵۶ مگاهرتز، ارتباط کوتاه برد بین دستگاه ها را فراهم می‌کند. ارتباطات میدان نزدیکی امکان ارتباط بین دو دستگاه را بدون تماس در حداکثر فاصله تقریباً ۲۰ سانتی-متری یا کمتر می‌دهد. فناوری ارتباطات میدان نزدیکی تعامل دو طرفه ساده و ایمن بین دستگاه های الکترونیکی را امکان-پذیر می‌کند. الحاق ارتباطات میدان نزدیکی به محصولات الکترونیکی مصرفی، چشم‌اندازهایی را برای برنامه‌های اینترنت اشیاء مانند تبادل تماس، بلیط الکترونیکی، پرداخت الکترونیکی و غیره ایجاد کرده است.

آردوینو: محیط توسعه یکپارچه آردوینو مجموعه-ای از نرم‌افزارهای منبع باز و بردهای توسعه است. بردهای توسعه آردوینو ممکن است با دریافت ورودی و تغییر خروجی دستگاه‌های الکتریکی مختلف به عنوان یک مینی کامپیوتر عمل کنند. همچنین، می‌توان آن را به راحتی با استفاده از زبان C برنامه ریزی کرد، پاک کرد و در هر زمان در محیط توسعه یکپارچه آردوینو دوباره برنامه‌ریزی کرد.

رزبری: برای سیستم عامل لینوکس طراحی شده است، اما در حال حاضر، نسخه‌های بهینه شده لینوکس را دارد که محبوب ترین آنها رزبین است. برد رزبری پای دارای رم، پردازنده، تراشه گرافیکی، رابط‌ها و کانکتورهای مختلف برای دستگاه‌های خارجی و همچنین پشتیبانی از تجهیزات جانبی ورودی و خروجی متعدد است.

زیگ‌بی: یک فناوری شبکه بی‌سیم است که برای ارتباط از راه دور با مصرف انرژی کم در نظر گرفته شده است. این یک پروتکل سطح بالا برای ارتباط وسایل شخصی یا

[3] wireless sensor network
[4] Radiofrequency identification Sensor Network

خانگی است. این بر اساس استاندارد شبکه بی‌سیم شخصی IEEE 802.15.4 (WPAN) است و از سیگنال‌های رادیویی دیجیتال کم مصرف استفاده می‌کند. فاصله انتقال زیگ‌بی بین ۱۰ تا ۱۰۰ متر است. از مزایای آن می‌توان به بهره وری انرژی، پیچیدگی کم، هزینه کم، نرخ داده پایین و امنیت اشاره کرد. این می‌تواند از رمزگذاری استاندارد رمزگذاری پیشرفته هنگام صحبت با همتایان خود استفاده کند.

پروتکل فشرده‌سازی سرآیندهای پروتکل اینترنت نسخه ۶[5]: پروتکل اینترنت نسخه ۶ روی سیستم شبکه شخصی بی سیم کم مصرف، یک شبکه مش بی سیم با مصرف انرژی کم است که هر گره دارای آدرس پروتکل اینترنت نسخه ۶ خاص خود است که به آن اجازه می دهد مستقیماً به اینترنت متصل شود. بر اساس پروتکل مسیریابی نسخه ۶ پروتکل اینترنت برای شبکه‌های کم مصرف و با تلفات، هر گره والد خود را انتخاب می‌کند. سه نوع گره: یک گره سینک، یک گره میانی و یک گره برگ وجود دارد.

۵- امنیت اینترنت اشیاء

مسائل مربوط به امنیت و حریم خصوصی اینترنت اشیاء ممکن است توسط افراد به نفع خود مدیریت شود. اینترنت اشیاء دنیایی را پیش‌بینی می‌کند که در آن اشیاء مشترک می‌توانند با یکدیگر ارتباط برقرار کرده و به اینترنت متصل شوند تا سیستم‌های هوشمند و خود پیکربندی شوند. علیرغم مزایای توسعه اینترنت اشیاء، امنیت و حفظ حریم خصوصی همچنان به عنوان موانع مهمی برای طراحی، انطباق و پیشرفت اینترنت اشیاء دیده می شود. نگرانی در مورد امنیت و حفظ حریم خصوصی مسائل اصلی است که باید در هر اینترنت اشیاء مورد توجه قرار گیرد. برای مسائل مربوط به امنیت، تعدادی از تحقیقات راه حل‌هایی ارائه کرده اند. به منظور حفاظت از اینترنت اشیاء، نگرانی‌های امنیتی در لایه مربوط به اینترنت اشیاء باید برطرف شود.

نگرانی‌های امنیت و حفظ حریم خصوصی اینترنت اشیاء اخیراً توجه و تلاش زیادی را به خود جلب کرده است. واژه نامه امنیت اینترنت (۲۰۲۳) حریم خصوصی در اینترنت اشیاء را اینگونه توصیف می کند: «حق یک نهاد (اغلب یک شخص)، که از طرف خودش عمل می کند، تصمیم بگیرد که تا چه حد با محیط اطراف خود درگیر شود، مانند اینکه چقدر تمایل دارد اطلاعات مربوط به خود را به دیگران فاش کند. در اینترنت اشیاء، شبکه‌ای از داده‌ها از یک سرور به همراه یک منطقه به دنبال جمع آوری اطلاعات است. برنامه‌ها باید در تمام مراحل کنترل شوند، از جمله در دستگاه، ذخیره‌سازی، ارتباطات و پردازش یکی از نگرانی‌های مهمی که باید در اینترنت اشیاء حل شود، حفظ حریم خصوصی و حفاظت از داده‌های حساس است[۱۱].

گره‌های حسگر شبکه اینترنت اشیاء که دارای محدودیت انرژی، نیرو کم و خود سازمان‌یافته مسیرهای مشترک و داده‌های عظیمی هستند، ذخیره‌سازی و پردازش را در طی ارتباط از راه دور در کانال‌های ضعیف و غیر قابل اطمینان انجام می‌دهند. این مسئله برای تهیه پروتکل‌های مسیریابی ایمن، مقیاس‌پذیر و دارای انرژی کارآمد برای چنین تکنولوژی بی‌سیم بسیار مهم است. در بخش زیر مشخصاتی برای ایمن‌سازی معرفی و ارائه شده‌است[۱۲]:

شناسایی و اصالت: شناسایی فرآیندی است که در آن اشیاء یا گره باید هویت خود را در شبکه ثابت کنند. این مورد لازم است تا گره‌های غیر مجاز نتوانند به شبکه اینترنت اشیاء متصل شوند. همچنین برای معتبر بودن داده‌ها، اصالت لازم است. احراز هویت گره‌ها از شبکه اینترنت اشیاء در برابر جلوگیری از دسترسی غیرقانونی گره محافظت می‌کند.

محرمانه بودن: در واقع محرمانه بودن در دسترس بودن داده‌ها فقط برای کاربران مجاز است و به گره‌های مخرب اجازه دسترسی داده نمی‌شود که به این مسئله "محرمانه بودن" گفته می‌شود. در اینترنت اشیاء، می‌توان با مکانیزم‌های مدیریت کلیدی ایمن، محرمانه بودن زیادی به دست‌آورد، باید اقدامات ایمنی رمزگذاری داده‌ها طراحی، توسعه و اعمال شود.

دسترس‌پذیری: برترین و اصلی‌ترین اولویت در امنیت، دسترس‌بودن است. در دسترس بودن یعنی سرویس-های داده و شبکه در صورت درخواست کاربران مجاز در شبکه اینترنت اشیاء در همه لایه‌ها حتی در صورت حملات مخرب در دسترس هستند. بیشترین حمله روی دسترس‌پذیری انکار سرویس است. پروتکل‌های مسیریابی ایمن و مبتنی بر اعتماد باید برای دستیابی به دسترس‌پذیری طراحی و استفاده شوند.

تمامیت(یکپارچگی): اطمینان از داده‌های دریافت شده توسط گیرنده یعنی چیزی که مقصد دریافت کرده همان چیزی باشد که فرستنده ارسال کرده‌است. در واقع یکپارچگی

[5] 6LowPAN

یعنی گره‌های دریافتی داده‌هایی که در ابتدا ارسال شده دریافت کنند. به دلیل انتشار موج رادیویی، بسته‌های داده ممکن است در اینترنت اشیاء دستکاری شده و در هنگام ارتباط با یکدیگر برخورد کنند. از همه مهم‌تر در شبکه اینترنت اشیاء، بسته‌های داده بر اساس استانداردهای پروتکل، جمع‌آوری، ذخیره، تحویل و دریافت می‌شوند، به همین دلیل باید یکپارچگی داده‌ها در طراحی شبکه‌های اینترنت اشیاء تعبیه شود.

اعتماد: اعتماد یعنی اطمینان، توانایی، قدرت یا حقیقت کسی یا چیزی است. اعتماد همچنین می‌تواند به صورت موقتی، قابل تغییر، ذهنی و نامتقارن تعریف شود. در اهداف اولیه امنیت و حریم خصوصی در هنگام تعاملات بین اشیاء مختلف، لایه‌های مختلف اینترنت اشیاء و برنامه‌های مختلف با اعتماد تضمین می‌شود. با اعتماد، امنیت و حریم خصوصی قابل اجرا است.

۶- خطرات امنیتی دستگاه اینترنت اشیاء

گسترش سریع دستگاه‌های اینترنت اشیاء عصری از اتصال و راحتی بی‌سابقه را آغاز کرده است. دستگاه‌های اینترنت اشیاء به جنبه‌های مختلف زندگی مدرن، از وسایل خانه هوشمند و حسگرهای صنعتی گرفته تا مانیتورهای مراقبت‌های بهداشتی و وسایل نقلیه خودران تبدیل شده‌اند. با این حال، این چشم‌انداز به هم پیوسته از چالش‌های امنیتی مصون نیست، و شبکه پیچیده‌ای از خطرات را ارائه می‌کند که باید به دقت مورد بررسی قرار گیرند. در این بخش، خطرات امنیتی بی‌شمار مرتبط با دستگاه‌های اینترنت اشیاء بررسی شده و آسیب‌پذیری‌هایی را که یکپارچگی داده‌ها، محرمانه بودن و قابلیت اطمینان کلی سیستم را به خطر می‌اندازند، روشن شده است[۱۳].

دسترسی غیرمجاز و نقض داده‌ها: یکی از مهم‌ترین خطرات امنیتی که دستگاه‌های اینترنت اشیاء را تهدید می‌کند، شبح دسترسی غیرمجاز و نقض داده‌ها است. ماهیت به هم پیوسته شبکه‌های اینترنت اشیاء، که اغلب دستگاه‌ها و پلتفرم‌های متنوعی را در بر می‌گیرد، زمینه مناسبی را برای عوامل مخربی که به دنبال ورود غیرمجاز هستند، فراهم می‌کند. مکانیسم‌های احراز هویت ناکافی، موضوعی تکرار شونده در ادبیات، این خطر را تقویت می‌کند و به دشمنان اجازه می‌دهد از حفاظت‌های رمز عبور ضعیف یا ناموجود سوء استفاده کنند و کنترل غیرمجاز بر دستگاه‌ها به دست آورند. پیامدهای دسترسی غیرمجاز فراتر از عملکرد دستگاه به خطر افتاده است. در سناریوهایی که دستگاه‌های اینترنت اشیاء داده‌های شخصی یا صنعتی حساس را جمع‌آوری می‌کنند، دسترسی غیرمجاز می‌تواند منجر به نقض شدید حریم خصوصی و نقض داده‌ها شود. جایی که دستگاه‌های اینترنت اشیاء به خطر افتاده برای راه‌اندازی حملات انکار سرویس در مقیاس بزرگ مورد استفاده قرار گرفتند. این حادثه بر تأثیرات آبشاری بالقوه اقدامات امنیتی ناکافی در اکوسیستم اینترنت اشیاء تأکید کرد. کاهش دسترسی غیرمجاز نیازمند پروتکل‌های احراز هویت قوی، از جمله احراز هویت چند عاملی و فرآیندهای نصب امن دستگاه است. ایجاد کانال‌های امن برای ارتباط دستگاه و ترکیب سخت‌افزار مقاوم در برابر دستکاری می‌تواند دستگاه‌ها را در برابر تلاش‌های دسترسی غیرمجاز تقویت کند.

عدم وجود رمزگذاری: فقدان یا اجرای ناکافی مکانیسم‌های رمزگذاری یک خطر امنیتی اساسی در دستگاه-های اینترنت اشیاء است. بسیاری از دستگاه‌های اینترنت اشیاء داده‌های حساس را از طریق شبکه‌ها منتقل می‌کنند و در صورت عدم وجود اقدامات رمزگذاری مناسب، آنها را در معرض رهگیری و دستکاری قرار می‌دهند. این آسیب‌پذیری به‌ویژه در برنامه‌هایی که حفظ حریم خصوصی و یکپارچگی داده‌ها مهم است، مانند مراقبت‌های بهداشتی، مالی و سیستم‌های کنترل صنعتی نگران‌کننده است. در دنیایی متصل که داده‌ها ارزشمند هستند، به خطر انداختن اطلاعات در حین انتقال پیامدهای شدیدی را به همراه دارد. دشمنان می‌توانند از کانال‌های رمزگذاری نشده برای استراق سمع ارتباطات، دستکاری داده‌ها یا انجام حملات انسان در میان استفاده کنند. نیاز به رمزگذاری انتها به انتها را نمی‌توان اغراق کرد، به خصوص در سناریوهایی که شامل داده های حساس یا حیاتی است. کاهش کمبود رمزگذاری شامل اتخاذ الگوریتم-های رمزگذاری قوی برای داده‌های در حال انتقال و داده‌ها در حالت استراحت است. اجرای شیوه‌های مدیریت کلید ایمن تضمین می‌کند که کلیدهای رمزگذاری به اندازه کافی محافظت می شوند و از رمزگشایی داده های رمزگذاری شده توسط اشخاص غیرمجاز جلوگیری می‌شود.

مکانیسم های احراز هویت ناکافی: احراز هویت، یک ستون اساسی امنیت سایبری، اهمیت بیشتری را در زمینه دستگاه‌های اینترنت اشیاء می‌گیرد. مکانیسم‌های احراز هویت ضعیف یا ناکافی دستگاه‌ها را در معرض خطرات امنیتی مختلفی از جمله دسترسی غیرمجاز، دستکاری داده‌ها و جعل هویت دستگاه قرار می‌دهد. با مطالعاتی که به آسیب‌پذیری دستگاه‌های مختلف اینترنت اشیاء در برابر مکانیسم‌های احراز هویت ساده و به راحتی قابل بهره‌برداری اشاره می‌کند، ادبیات بر شیوع این خطر تأکید می‌کند. سازندگان دستگاه اغلب راحتی کاربر را بر احراز هویت قوی اولویت می‌دهند، که منجر به رمزهای عبور پیش‌فرض، اعتبارنامه‌های به راحتی قابل حدس زدن یا حتی عدم وجود احراز هویت می‌شود. پرداختن به احراز هویت ناکافی شامل پیاده‌سازی اعتبارنامه‌های منحصر به فرد برای هر دستگاه و تشویق کاربران به سفارشی‌سازی رمزهای عبور در حین راه اندازی است. احراز هویت چندعاملی لایه‌ای از امنیت را اضافه می‌کند و کاربران را ملزم می‌کند تا قبل از دسترسی به دستگاه یا شبکه، چندین اشکال شناسایی را ارائه کنند.

آسیب‌پذیری‌های امنیتی فیزیکی: در حالی که بسیاری از گفتمان‌ها در مورد امنیت اینترنت اشیاء حول تهدیدات سایبری می‌چرخد، امنیت فیزیکی دستگاه‌ها را نمی‌توان نادیده گرفت. در تنظیمات صنعتی اینترنت اشیاء، جایی که دستگاه‌ها اغلب در محیط‌های چالش برانگیز کار می‌کنند، خطر دستکاری فیزیکی به یک نگرانی قابل توجه تبدیل می‌شود. دسترسی یا دستکاری غیرمجاز به حسگرها، محرک‌ها یا سایر اجزای فیزیکی می‌تواند عواقب گسترده‌ای داشته باشد، به طور بالقوه ایمنی را به خطر بیندازد، فرآیندهای حیاتی را مختل کند یا باعث خرابی تجهیزات شود. ایمن‌سازی دستگاه‌های اینترنت اشیاء در برابر تهدیدات فیزیکی نیازمند اقدامات سخت‌افزاری و نرم‌افزاری است. مقاومت فیزیکی در برابر دستکاری، محفظه‌های ایمن و کنترل‌های دسترسی قوی می‌توانند دسترسی فیزیکی غیرمجاز را خنثی کنند. علاوه بر این، ادغام حسگرهایی که دستکاری یا شرایط فیزیکی غیرعادی را تشخیص می‌دهند، یک لایه حفاظتی اضافی اضافه می‌کند.

آسیب‌پذیری در پروتکل‌های ارتباطی: آرایه متنوع پروتکل‌های ارتباطی دستگاه‌های اینترنت اشیاء، چشم‌انداز پیچیده‌ای از آسیب‌پذیری‌های بالقوه را معرفی می‌کند. بسیاری از پروتکل‌ها بدون ملاحظات امنیتی قوی طراحی شده‌اند و آنها را مستعد بهره‌برداری می‌کند. مطالعات عمیق آسیب‌پذیری‌هایی را در پروتکل‌های پرمصرف مانند MQTT و CoAP شناسایی کرده‌اند که نیاز به رویکرد امنیتی اول در طراحی و اجرای استانداردهای ارتباطی را برجسته می‌کند. بهره برداری از آسیب پذیری‌ها در پروتکل‌های ارتباطی می‌تواند مهاجمان را قادر به رهگیری، دستکاری یا مختل کردن جریان داده بین دستگاه‌های اینترنت اشیاء کند. حملات مرد میانی حملات بازپخش و تزریق بسته، تهدیدات بالقوه‌ای از طرف پروتکل‌های ارتباطی ناامن هستند. ماهیت پویا و در حال تکامل این پروتکل‌ها امنیت ارتباطات اینترنت اشیاء را پیچیده‌تر می‌کند. کاهش آسیب‌پذیری‌ها در پروتکل‌های ارتباطی نیازمند یک رویکرد فعالانه است، از جمله ممیزی‌های امنیتی منظم، به‌روزرسانی‌ها، و اتخاذ پروتکل‌های ایمن و مدرن. پیاده‌سازی مکانیسم‌های رمزگذاری و احراز هویت در سطح پروتکل، یک دفاع اضافی در برابر سوء استفاده‌های بالقوه می‌افزاید.

خطرات امنیتی زنجیره تامین: امنیت دستگاه‌های اینترنت اشیاء صرفاً به محیط عملیاتی آنها بستگی ندارد. کل چرخه عمر یک دستگاه، از ساخت تا دفع پایان عمر، یک ملاحظات مهم است. اگرچه خطرات امنیتی زنجیره تامین در بسیاری از بحث‌های پیرامون امنیت اینترنت اشیاء مورد بررسی قرار نگرفته است. سازش در هر مرحله از زنجیره تامین، خواه عمدی یا سهوی، می‌تواند آسیب‌پذیری‌هایی را ایجاد کند که ممکن است تا زمانی که مورد سوء استفاده قرار نگیرند، شناسایی نشوند. فرآیندهای تولید مستعد دستکاری، اجزای آسیب‌دیده یا به‌روزرسانی‌های سیستم‌افزار ناامن، بردارهای بالقوه حملات زنجیره تامین هستند. دشمنان ممکن است از آسیب‌پذیری‌های معرفی‌شده در طول تولید، توزیع، یا به‌روزرسانی‌های نرم‌افزار پس از خرید برای به دست آوردن دسترسی یا کنترل غیرمجاز بر دستگاه‌های اینترنت اشیاء سوء استفاده کنند. فراگیر شدن زنجیره‌های تامین جهانی، تلاش‌ها برای تضمین یکپارچگی و امنیت هر جزء را پیچیده‌تر می‌کند. کاهش خطرات امنیتی زنجیره تامین مستلزم ایجاد شیوه‌های شفاف و ایمن زنجیره تامین است. این شامل تأیید یکپارچگی اجزا، اطمینان از فرآیندهای تولید ایمن و پیاده‌سازی مکانیسم‌هایی برای شناسایی و رفع آسیب‌پذیری‌ها در طول

چرخه عمر دستگاه است. همکاری بین تولیدکنندگان دستگاه، تامین کنندگان و نهادهای نظارتی در تقویت امنیت کل زنجیره تامین بسیار مهم است.

نگرانی‌های حفظ حریم خصوصی: نگرانی‌های مربوط به حفظ حریم خصوصی در عصر اینترنت اشیاء، جایی که دستگاه‌ها به طور مداوم حجم زیادی از داده‌ها را جمع‌آوری و انتقال می‌دهند، بزرگ است. جمع‌آوری بی‌رویه داده‌ها، اغلب بدون رضایت صریح کاربر، سؤالات اخلاقی و پیامدهای حفظ حریم خصوصی را ایجاد می‌کند. برای مثال، در بخش مراقبت‌های بهداشتی، دستگاه‌های اینترنت اشیاء ممکن است داده‌های حساس بیمار را جمع‌آوری کنند، در حالی که دستگاه‌های خانه هوشمند به طور مداوم فعالیت‌ها و ترجیحات کاربران را زیر نظر دارند. ماهیت فراگیر اینترنت اشیاء ، همراه با حفاظت از حریم خصوصی ناکافی، می‌تواند منجر به نظارت غیرمجاز، نمایه‌سازی، یا قرار گرفتن در معرض ناخواسته اطلاعات شخصی شود. ایجاد تعادل بین بهره‌گیری از مزایای بینش مبتنی بر داده و محافظت از حریم خصوصی فردی یک چالش پیچیده است که مستلزم بررسی دقیق و رعایت اصول حریم خصوصی از طریق طراحی است. کاهش نگرانی‌های مربوط به حریم خصوصی شامل پیاده‌سازی مکانیسم‌های حفظ حریم خصوصی در هر دو سطح سخت‌افزاری و نرم‌افزاری است. سازندگان دستگاه باید اصول حفظ حریم خصوصی را بر اساس طراحی اتخاذ کنند و اطمینان حاصل کنند که جمع‌آوری داده‌ها به حداقل می‌رسد، ناشناس است و با رضایت صریح کاربر انجام می‌شود. علاوه بر این، رمزگذاری قوی و کنترل‌های دسترسی به محافظت از داده های حساس از دسترسی غیرمجاز کمک می‌کند[۱۳].

۷- بلاک‌چین

بلاک‌چین مجموعه‌ای دیجیتالی از تراکنش‌ها است که در یک دفتر کل توزیع شده در یک شبکه غیرمتمرکز نظارت و ثبت می‌شود، به این معنی که شبکه هیچ مرجع کنترل مرکزی ندارد. بلاک‌چین از بلوک‌های داده گسسته‌ای تشکیل شده است که هر کدام حاوی رکوردی از اطلاعات هستند و به صورت زمانی به یکدیگر متصل هستند. این واقعیت که این پیوندها قابل تغییر نیستند به ایجاد اعتماد در شبکه کمک می‌کند. با محافظت از تبادل اطلاعات در حین وقوع، این سیستم پیشگامانه آنها را مدیریت می‌کند.

تمرکززدایی از جمع‌آوری، ذخیره و پردازش داده‌ها با حصول اطمینان از یکپارچگی و تغییرناپذیری داده‌ها، اهداف فناوری بلاک‌چین هستند. بلاک‌چین یک دفتر کل دیجیتال است که اطلاعات را در ساختار داده‌ای به نام بلوک ذخیره می‌کند و آن را به یک پایگاه داده تبدیل می‌کند. پایگاه‌های داده نیز اطلاعات را در جداول ذخیره می‌کنند، اما نمی‌توان گفت که پایگاه داده یک بلاک‌چین است، با وجود اینکه بلاک‌چین یک پایگاه داده است. به دلیل تنوع در معماری، طراحی، رفتار و امنیت، نمی‌توان آنها را به جای یکدیگر مورد استفاده قرار داد. فناوری همتا به همتا یا بلاک‌چین به این معنی است که هیچ نهاد واحدی داده‌ها را کنترل نمی‌کند. توانایی‌ها در یک موجودیت متمرکز نیستند زیرا به‌روزرسانی اطلاعات از طریق مکانیزم اجماع انجام می‌شود. بنابراین، قدرت‌ها در یک نهاد متمرکز نیستند و به همین دلیل است که از دموکراسی در کار حمایت می‌کند. ورودی‌های غیرقابل تغییر داده نیز یکی از ویژگی‌های فناوری بلاک‌چین است. هر ورودی در یک بلاک-چین دارای خاصیت یک رکورد غیرقابل تغییر است زیرا با یک هش رمزنگاری محافظت می‌شود. در حالی که در پایگاه داده معماری یک مدل کلاینت-سرور است و مدیر می‌تواند تمام رکوردها را تغییر دهد، یا حتی حذف کند. شباهت‌های کمی بین هر دو وجود دارد، اما بسیاری از محققان استدلال می-کنند که وقتی برنامه‌ها غیرقابل اعتماد هستند، بلاک‌چین‌ها مناسب هستند، در حالی که پایگاه‌های داده زمانی مناسب هستند که عملکرد مهم‌تر از امنیت باشد[۱۴].

۸- ویژگی‌های بلاک‌چین

بلاک‌چین یک فناوری دفتر کل توزیع شده جدید، یکپارچه‌سازی ذخیره‌سازی توزیع شده، الگوریتم رمزگذاری، انتقال همتا به همتا، مکانیسم اجماع، قرارداد هوشمند و سایر فناوری‌ها است که می‌تواند به اشتراک‌گذاری اطلاعات و چشم انداز فوق‌العاده بین چندین طرف را تحقق بخشد، کارایی پردازش کسب و کار را بهبوددداده و باعث کاهش هزینه‌ها شود. در حال حاضر، با توسعه سریع جامعه، فناوری بلاک‌چین پتانسیل قوی در بسیاری از زمینه ها، مانند کاربرد در زنجیره تامین، پزشکی، امور مالی، حفاظت از حریم خصوصی، یادگیری فدرال و سایر زمینه‌های صنعتی نشان داده است. با این حال، در سناریوهای کاربردی مختلف، الزامات مختلفی برای کنترل دسترسی بلاک‌چین، توان عملیاتی، اندازه شبکه و

غیره وجود دارد. نحوه تعامل با داده‌ها و انتقال ارزش بین سیستم‌های مختلف بلاک‌چین به کانون تحقیقات در دانشگاه و صنعت تبدیل شده است. پس از راه اندازی بلاک‌چین در سال ۲۰۰۸، به عنوان یک نوآوری مخرب که ممکن است نحوه تعامل افراد، ایجاد هزینه‌های خودکار، پیگیری و نظارت بر تراکنش‌ها را تغییر دهد، به تکامل خود ادامه داد. الزام مقامات مرکزی برای نظارت و کنترل تراکنش‌ها و تعاملات بین اعضای مختلف ممکن است با استفاده از زنجیره بلوکی حذف شود که می‌تواند مقرون به صرفه باشد.

در یک محیط غیرقابل اعتماد، بلاک‌چین ویژگی‌های مطلوبی از جمله عدم تمرکز، استقلال، یکپارچگی، تغییرناپذیری، تأیید، تحمل خطا، ناشناس بودن، قابلیت حسابرسی و شفافیت را در اختیار کاربران قرار می‌دهد که با این ویژگی‌های پیشرفته، فناوری بلاک‌چین در چند سال اخیر توجه دانشگاهی و صنعتی زیادی را به خود جلب کرده است. برای اینکه به کسی کمک کند تا فناوری بلاک‌چین و مسائل امنیتی بلاک‌چین را درک کند، به ویژه برای کاربرانی که از بلاک‌چین برای انجام تراکنش‌ها استفاده می‌کنند و برای محققانی که فناوری بلاک‌چین را توسعه می‌دهند و مسائل امنیتی بلاک‌چین را بررسی می‌کنند، تلاش و زمان بسیاری از محققان صرف انجام این کار شد[۱۴].

بلاک‌چین، یک سیستم دفتر کل توزیع شده، تراکنش‌های ایمن، باز و غیرقابل تغییر را امکان‌پذیر می‌کند. این شبکه‌ای از پایگاه داده مشترک رایانه‌ها است که به روز نگه داشته می‌شود. هر بلوک در زنجیره بلوکی شامل مجموعه ای از تراکنش‌ها است و هر بلوک به بلوک قبلی در زنجیره مرتبط است. در نتیجه، تغییر داده‌های موجود در بلاک‌چین مستلزم تغییر هر بلوک در زنجیره است که انجام آن را بسیار دشوار می‌کند. ویژگی‌های اصلی بلاک‌چین در زیر ذکر شده است[۱۴]:

تغییرناپذیری: تغییرناپذیری بلاک‌چین به این معنی است که وقتی داده‌ها به بلاک‌چین اضافه می‌شوند، نمی‌توان آن‌ها را به راحتی تغییر داد یا حذف کرد. این باعث می‌شود بلاک‌چین برای برنامه‌هایی که به درجه بالایی از امنیت و شفافیت نیاز دارند، مانند تراکنش‌های مالی و مدیریت زنجیره تامین، ایده‌آل باشد.

شفافیت: به دلیل شفافیت بلاک‌چین، تمام گره‌های شبکه به تراکنش‌های یکسان و یک کپی از بلاک‌چین دسترسی دارند. این امر باعث می‌شود که کلاهبرداری یا فساد به شدت چالش برانگیز باشد.

امنیت: امنیت بلاک‌چین از طریق استفاده از انواع تکنیک‌های رمزنگاری مانند توابع هش، امضای دیجیتال و رمزگذاری به دست می‌آید. این به این دلیل است که بلاک چین مبتنی بر رمزنگاری است که یک فناوری بسیار امن است. رمزنگاری استفاده شده در بلاک‌چین دسترسی کاربران غیرمجاز به داده‌های موجود در بلاک‌چین را بسیار دشوار می‌کند.

تمرکززدایی: تمرکززدایی از بلاک‌چین از طریق استفاده از شبکه همتا به همتا حاصل می‌شود. این بدان معناست که هیچ مرجع مرکزی وجود ندارد که بلاک‌چین را کنترل کند. در عوض، بلاک‌چین توسط گره‌های موجود در شبکه کنترل می‌شود. این امر سانسور یا دستکاری زنجیره بلوکی را برای هر نهادی بسیار دشوار می‌کند. این امر آن را در برابر سانسور و دستکاری بسیار مقاوم می‌کند.

پایداری: تراکنش‌ها را می‌توان به سرعت تأیید کرد و تراکنش‌های نامعتبر توسط ماینرهای صادق پذیرفته نمی‌شوند. تقریباً غیرممکن است که تراکنش‌ها را پس از گنجاندن در بلاک چین حذف یا بازگردانید. بلوک‌های حاوی تراکنش‌های نامعتبر را می‌توان فوراً کشف کرد.

ناشناس بودن: هر کاربر می‌تواند با یک آدرس تولید شده با بلاک‌چین تعامل داشته باشد که هویت واقعی کاربر را آشکار نمی‌کند. توجه داشته باشید که بلاک‌چین به دلیل ضمانت حفظ حریم خصوصی به دلیل محدودیت ذاتی، نمی‌تواند حفظ کامل حریم خصوصی را تضمین کند.

قابلیت حسابرسی: بلاک‌چین بیت کوین داده‌های موجودی کاربر را بر اساس مدل خروجی تراکنش خرج نشده ذخیره می‌کند. هر تراکنش باید به برخی از تراکنش‌های خرج نشده قبلی اشاره کند. هنگامی که تراکنش جاری در بلاک چین ثبت می‌شود، وضعیت تراکنش‌های خرج نشده ارجاعی از مصرف نشده به مصرف شده تغییر می‌کند. بنابراین تراکنش‌ها را می‌توان به راحتی تأیید و ردیابی کرد.

۹- بلاک‌چین برای اینترنت اشیاء

هم بلاک‌چین و هم اینترنت اشیاء فناوری‌های نوظهوری هستند که پتانسیل بالایی دارند، اما هنوز به دلیل نگرانی‌های فنی و امنیتی، پذیرش گسترده‌ای ندارند. اینترنت اشیاء و بلاک‌چین برای حل چندین مشکل دست به دست هم می‌دهند. مدل متمرکز فعلی استقرار اینترنت اشیاء دارای چالش‌های امنیتی بسیاری است. یکی از راه‌های حل این مشکل، غیرمتمرکز کردن شبکه اینترنت اشیاء با ایجاد یک دفتر کل مبتنی بر مجوز است. فناوری بلاک‌چین یک تغییر دهنده بازی در حوزه امنیت داده‌ها است و این پتانسیل را دارد که شیوه تعامل کاربر با دستگاه‌های متصل خود را متحول کند. این می‌تواند حفظ حریم خصوصی و امنیت داده-ها را برای دستگاه های اینترنت اشیاء فراهم کند. اینترنت اشیاء به دستگاه‌های متصل در سراسر اینترنت امکان می‌دهد داده‌ها را به شبکه‌های بلاک‌چین منتقل کنند و سوابق مقاوم در برابر دستکاری تراکنش‌ها را در این فرآیند ایجاد کنند. اینترنت اشیاء امنیت و شفافیت را در اکوسیستم‌های اینترنت اشیاء افزایش می‌دهد. با ادغام اینترنت اشیاء با فناوری بلاک-چین، داده‌های اینترنت اشیاء را می‌توان ایمن، احراز هویت و غیرمتمرکز کرد، که باعث بهبود اعتماد، شفافیت، قابلیت ردیابی و قابلیت اطمینان در فرآیندها و اتوماسیون مبتنی بر اینترنت اشیاء می‌شود. ترکیب اینترنت اشیاء و بلاک‌چین به دستگاه هوشمند اجازه می‌دهد تا به طور مستقل عمل کند. می‌تواند از سازمان‌ها و افراد در برابر اشکال مختلف آسیب محافظت کند. می‌تواند قابلیت اطمینان و ردیابی شبکه را بهبود بخشد[۱۵].

بلاک‌چین (خصوصی) را می‌توان با استفاده از بلاک چین IBM به اینترنت اشیاء شناختی گسترش داد. این مجموعه‌ای از اینترنت اشیاء، هوش مصنوعی و بلاک‌چین است که منجر به برنامه‌های کاربردی اینترنت اشیاء جالب می‌شود. بسیاری از پلتفرم‌های بلاک‌چین بر روی اینترنت اشیاء در صنایع متمرکز هستند. آیوتا یکی از پلتفرم های بلاک چین با اینترنت اشیاء است. یک لایه برای انتقال داده وجود دارد. با بزرگتر شدن صنعت، چندین پلتفرم بلاک‌چین با تمرکز بر اینترنت اشیاء در حال ظهور هستند. یکی از اولین پلتفرم‌های اینترنت اشیاء بلاک‌چین آیوتا است که برای اینترنت اشیاء ایجاد شد و منجر به یک لایه انتقال داده و تراکنش تسویه شده برای دستگاه های متصل شد. هنگامی که از اینترنت اشیاء برای اتصال دستگاه‌ها به یکدیگر استفاده می‌شود، تعداد هکرهایی که بر امنیت تأثیر می‌گذارند نیز افزایش می‌یابد. بنابراین، یک اقدام امنیتی بسیار ضروری است.

در بلاک‌چین، بلوک‌ها با استفاده از تکنیک‌های رمزنگاری برای تشکیل یک بلاک‌چین ایمن می‌شوند. هنگامی که فناوری بلاک‌چین با اینترنت اشیاء استفاده می‌شود، یک برنامه اینترنت اشیاء ایمن بهتر ایجاد می‌شود که کمتر مستعد هکرها است. ماهیت غیرمتمرکز هکرها به ترکیب بهتر آن با دستگاه‌های اینترنت اشیاء کمک می‌کند. زیرا در مورد کاربردهای حیاتی اینترنت اشیاء مانند نظارت بر سلامت و نظارت بر ایمنی، هکرها می‌توانند با هک کردن تراکنش‌ها و ارتباطات، تهدیدات جدی ایجاد کنند. فناوری بلاک‌چین به از بین بردن این تهدیدات کمک می‌کند و همچنین هزینه ارتباطات را کاهش می‌دهد. بلاک‌چین امنیت را بدون دخالت مقامات تضمین می‌کند. برخی دیگر از محدودیت‌های اینترنت اشیاء توسط کلان داده و محاسبات ابری برطرف شده است[۱۶].

۱۰- کاربرد بلاک‌چین در اینترنت اشیاء

فناوری بلاک‌چین می‌تواند برای ایمن‌سازی سیستم‌های اینترنت اشیاء به طرق مختلف مورد استفاده قرار گیرد. چندین صنعت شروع به کشف کاربردهای بالقوه اینترنت اشیاء و بلاکچین برای بهبود کارایی و ایجاد اتوماسیون کرده اند. چند نمونه به شرح زیر ارائه شده است[۱۵]:

بانکداری: چندین بانک در حال معرفی فناوری بلاک‌چین برای ایجاد یک محیط مقیاس‌پذیر و غیرمتمرکز برای دستگاه‌ها و برنامه‌های کاربردی اینترنت اشیاء هستند. بانک‌ها با استفاده از پروتکل‌های جدید بلاک‌چین خدمات خود را بهبود می‌بخشند. امروزه بانک‌ها می‌توانند با هزینه‌های کم تسویه با یکدیگر معاملات مستقیم داشته باشند.

زنجیره تامین: توانایی ردیابی اجزای مورد استفاده در هواپیما، خودرو و سایر محصولات برای فعال کردن انطباق با مقررات و ایمنی ضروری است. بسیاری از شرکت‌ها در تلاش هستند تا دستگاه‌های اینترنت اشیاء را قادر سازند تا فرآیند حمل و نقل را ردیابی کنند. با ادغام دستگاه‌های اینترنت اشیاء مانند حسگرها و برچسب‌های RFID با یک شبکه بلاک‌چین، شرکت‌ها می‌توانند یک سیستم غیرمتمرکز و امن برای ردیابی محصولات در حین حرکت در زنجیره

تامین ایجاد کنند. به دلیل عدم شفافیت، ترکیب هر دو فناوری اینترنت اشیاء و بلاک‌چین قابلیت اطمینان و ردیابی شبکه را بهبود می‌بخشد.

شهرهای هوشمند: این شهرها همچنین از قدرت سیستم‌های اینترنت اشیاء با بلاک‌چین استفاده می‌کنند. همانطور که شهرهای بیشتری شروع به پیاده‌سازی استراتژی اینترنت اشیاء در زیرساخت‌های خود می‌کنند، بلاک‌چین این پتانسیل را دارد که موارد استفاده را افزایش دهد. در آینده، اینترنت اشیاء به طور بالقوه می‌تواند زیرساخت شهرهای هوشمند را تحت پوشش قرار دهد تا ارتباطات را بسیار ساده‌تر و کارآمدتر از امروز کند. اتحاد اینترنت اشیاء و فناوری بلاک-چین مدیریت از راه دور سیستم امنیتی کاربر، حذف زیرساخت‌های متمرکز را ممکن می‌سازد.

خانه‌های هوشمند: دستگاه‌های هوشمند مجهز به اینترنت اشیاء نقش مهمی در زندگی روزمره افراد دارند. بلاک‌چین و اینترنت اشیاء آینده فناوری خانه هوشمند هستند. در یک خانه هوشمند، دستگاه‌ها متصل هستند و می-توان از طریق نقطه مرکزی مانند کنسول بازی، تلفن هوشمند، تبلت یا لپ‌تاپ به آنها دسترسی داشت. برای فعال کردن این خانه‌های هوشمند، نقش اینترنت اشیاء بسیار مهم است. ادغام فناوری اینترنت اشیاء و بلاک چین، مدیریت از راه دور سیستم امنیتی کاربران را ممکن می‌سازد. به عنوان مثال، تلسترا[6]، یک شرکت مخابراتی و رسانه‌ای استرالیایی، راه حل‌های خانه هوشمند را ارائه می‌دهد. این شرکت برای اطمینان از اینکه هیچ کس نمی‌تواند داده‌های گرفته شده از دستگاه‌های هوشمند را دستکاری کند، بلاک‌چین را پیاده‌سازی کرده است.

صنعت خودرو: این صنعت در حال سرمایه‌گذاری در توسعه وسایل نقلیه خودکار است که توسط حسگرهای اینترنت اشیاء فعال می‌شوند و امکان تبادل اطلاعات مهم را به راحتی و به سرعت فراهم می‌کنند. این شرکت از حسگرهای فعال اینترنت اشیاء برای توسعه وسایل نقلیه کاملاً خودکار استفاده می‌کند. در ترکیب با بلاک‌چین، خودروهای خودمختار، پارکینگ هوشمند یا کنترل خودکار ترافیک می‌توان به دست آورد.

صنعت داروسازی: مشکل محصولات تقلبی در صنعت داروسازی هر روز در حال افزایش است. شفافیت و قابلیت ردیابی فناوری بلاک‌چین می‌تواند به کنترل حمل و نقل داروها از مبدا تا مقصد کمک کند.

کشاورزی: فناوری بلاک‌چین پتانسیل تغییر شکل کشاورزی را از تولید تا فروشگاه مواد غذایی دارد. حسگرهای اینترنت اشیاء را می‌توان در مزارع نصب کرد و داده‌های خود را مستقیماً به شبکه بلاک‌چین ارسال کرد تا زنجیره تامین بهبود یابد. بلاک‌چین برای مدیریت زنجیره تامین، صنعت کشاورزی را با بهبود ایمنی و کیفیت مواد غذایی و همچنین قابلیت ردیابی کل زنجیره تامین کشاورزی متحول می‌کند.

حمل و نقل کالا: حمل و نقل یک فرآیند پیچیده است که طرف‌های مختلف با اولویت‌های متفاوت را درگیر می‌کند. انتقال بار از یک مکان به مکان دیگر پیچیده است. با کمک یک بلاک‌چین فعال اینترنت اشیاء، امکان ذخیره دما، زمان رسیدن و وضعیت کانتینرهای حمل و نقل در حال حمل و نقل وجود دارد. تراکنش‌های غیرقابل تغییر بلاک‌چین به اطمینان حاصل می‌شود که همه افراد درگیر در این فرآیند می‌توانند به داده‌ها اعتماد کنند و برای انتقال سریع و کارآمد محصولات اقدام کنند.

امنیت سایبری: امنیت یکی از مهمترین مسائل اینترنت اشیاء است و یک مشکل دائمی است. همچنان که مقررات مربوط به توسعه و استفاده از آنها مطابقت دارد، به تکامل خود ادامه خواهد داد. با این حال، امکان سیستم امنیتی اینترنت اشیاء بلاک‌چین چیزی است که ممکن است پتانسیل بالایی داشته باشد. امنیت یکی از ویژگی‌های ذاتی بلاک‌چین است و این فناوری می‌تواند داده‌ها را مشروعیت بخشد و مطمئن شود که از یک منبع قابل اعتماد می‌آیند. از بلاک‌چین می‌توان برای محافظت از دستگاه های اینترنت اشیاء در برابر حملات سایبری با ارائه اقدامات امنیتی مختلف استفاده کرد.

حفظ حریم خصوصی: در اینترنت اشیاء، امنیت و حریم خصوصی به دلیل مقیاس گسترده و ماهیت توزیع شده شبکه‌های اینترنت اشیاء، یک چالش بزرگ باقی می‌ماند. دستگاه های اینترنت اشیاء ادغام شده با بلاک‌چین می‌توانند حریم خصوصی را بهبود بخشند.

[6] Telstra

تراکنش‌های خودکار: دستگاه‌های اینترنت اشیاء را می‌توان به گونه‌ای برنامه‌ریزی کرد که به‌طور خودکار تراکنش‌ها را روی بلاک‌چین راه‌اندازی کند و منجر به فرآیندهای کارآمدتر و ساده‌تر شود. اینها تنها چند نمونه هستند، اما پتانسیل ترکیب اینترنت اشیاء و بلاک‌چین بسیار فراتر از این برنامه‌ها است.

۱۱- مقایسه کارهای مرتبط ادغام اینترنت اشیاء و بلاک چین جهت افزایش امنیت

امروزه، اینترنت اشیاء به عنوان یک تکنیک در حال تکامل در نظر گرفته می‌شود که در هنگام به کارگیری مهندسی، با دامنه‌ای متولد شد، بنابراین بدون دخالت نیروی انسانی، مشکلات را حل می‌کند. نیروی کار هوشمند را قادر می‌سازد، یعنی تعاملی بین انسان و ماشین و همچنین بین ماشین ها ایجاد می‌کند.

اگرچه اینترنت اشیاء تحقق فرآیندها را تسهیل می‌کند، اما امنیت اطلاعات ذخیره شده در دستگاه ها ۱۰۰٪ قابل اعتماد نیست، زیرا داده‌ها را می‌توان در مسیر رسیدن به پایگاه داده یا زمانی که در آن ذخیره می‌شود تغییر داد، رهگیری یا فیلتر کرد. این تبدیل به یکی از بزرگترین چالش‌هایی است که فناوری اینترنت اشیاء دارد و هنوز نتوانسته است راه‌حلی قطعی ارائه دهد. حریم خصوصی و امنیت اطلاعات اهمیت خود را از زمان شروع اینترنت همانطور که نشان داده شد، از زمانی که داده‌ها در این رسانه مجازی شروع به گردش کردند و در این سناریو افراد غیرمجاز می‌توانند بدون نیاز به اجازه کسی آن اطلاعات را رهگیری کنند. اگرچه پروتکل های امنیتی برای جلوگیری از آن وجود دارد، سرورهایی که اطلاعات روی آن ها میزبانی می‌شود آسیب‌پذیر هستند، زیرا تحت یک معماری متمرکز کار می‌کنند. همیشه شرکت ارائه‌دهنده خدمات اینترنت اشیاء در کنترل است و می‌تواند قربانی یک حمله مخرب باشد یا اطلاعات مشتریان خود را به‌طور نادرست دستکاری کند. بنابراین، شرکت‌هایی که امنیت را تامین نمی‌کنند، جایی که می‌توانند اطلاعات ارائه‌شده را بر اساس منافع خود تغییر دهند، بنابراین ۱۰۰٪ قابل اعتماد نیستند، که نیاز به داده‌های تایید شده را نشان می‌دهد و بررسی می‌کنند که آیا اصلاح نشده‌اند، این امر با فناوری موجود عملا غیرممکن است. به طور خلاصه، هنگامی که اطلاعات به شبکه ارسال می شود، کاربر به طور خودکار کنترل خود را از دست می دهد و همچنین می تواند با توجه به اینکه اینترنت چقدر بزرگ و گسترده است، به محدودیت های غیرقابل تصوری گسترش یابد.

مناسب ترین راه برای مدیریت و حل مشکل استفاده از فناوری بلاک‌چین است، که در آن پتانسیل افزایش حکمرانی خوب و همچنین شفافیت و حریم خصوصی را دارد، این امر امنیت و حریم خصوصی مورد نیاز را فراهم می‌کند، علاوه بر این، به صورت غیرمتمرکز کار می‌کند. بلاک‌چین توزیعی از اطلاعات است که با گره‌های شبکه به اشتراک گذاشته می شود. به طور مشابه، رمزنگاری مورد استفاده در بلاک‌چین یک ویژگی کلیدی است، زیرا احراز هویت را در تمام تعاملات فراهم می‌کند. برای تحقیقات خود در مورد ادغام بلاک‌چین با اینترنت اشیاء، در سال ۲۰۱۸ گفته می‌شود: "چندین فناوری امنیتی و عملکردهای رمزنگاری مورد سوء استفاده قرار گرفته اند، یکی از آن هایی است که بلاک‌چین، در حال بهره برداری از سناریوهای مختلف است، با توجه به اینکه فناوری است که هر روز تکامل می‌یابد". در پاراگراف قبلی، نویسنده پتانسیل‌هایی را که بلاک چین در رابطه با امنیت و حریم خصوصی در ارائه خدماتی که این فناوری را برای مدیریت ارسال و دریافت اطلاعات یکپارچه می‌کنند، نشان می‌دهد[۱۷].

برای دریافت ایده روشنی از میزان استفاده از فناوری بلاک‌چین در دستگاه‌های اینترنت اشیاء، اینکه آیا استفاده از آن فوایدی ایجاد می‌کند یا خیر، یا اینکه چه مکانیسم‌ها و روش‌هایی برای دستیابی به اثر مثبت مناسب‌تر هستند، لازم است شواهد موجود در تحقیقات موجود در مورد فناوری بلاک چین و اینترنت اشیاء مرور شود[۱۷]. جدول ۱و۲ مطالعاتی را نشان می‌دهد که معلوم شد مقدار قابل توجهی از اطلاعات مرتبط را در مورد اینترنت اشیاء را مبتنی بر فناوری بلاک‌چین ارائه می دهند.

جدول ۱: بررسی کارهای مرتبط ادغام اینترنت اشیاء و بلاک چین جهت افزایش امنیت

توضیحات	مرجع مقاله	سال انتشار
این کار نشان می‌دهد که چگونه معماری بلاک‌چین به احراز هویت، کنترل دسترسی و یکپارچگی ذخیره‌سازی امنیت اینترنت اشیاء دست می‌یابد، که از تکنیک اجماع POW و PBFT استفاده می‌کند، با فناوری بلاک‌چین که از امنیت بهبودیافته بهره	[۱۸]	۲۰۱۸

می‌برد، به این نتیجه می‌رسد که بلاک چین با حداقل ترافیک اینترنت اشیاء در هر صحنه، دسترسی را کنترل کرده و الگوهای امن را شناسایی می‌کند.		
این مقاله سعی می‌کند چالش‌های بکارگیری فناوری بلاک‌چین و چگونگی بهبود بالقوه اینترنت اشیاء در شرکت‌ها را بررسی کند، همچنین مزایایی در بهبود امنیت دارد، با این نتیجه که هنگام اتخاذ تدابیر، گنجاندن اینترنت اشیاء و بلاک چین در معماری‌های دولتی مهم است، که نشان دهنده تعامل سریع بین ساکنان و همچنین برای رویه‌های استخراج است.	[۱۹]	۲۰۱۸
در این مقاله مفاهیم اصلی مورد تجزیه و تحلیل قرار گرفت و یک زنجیره بلوکی به عنوان شواهد دیجیتالی برای به کارگیری فناوری فین‌تک طراحی شد و به عنوان یک مزیت، بهبود امنیت را به دست آورد، با این نتیجه که بلاک چین سودمند است، زیرا با استفاده از یک روش تصادفی، تعمیم معماری‌ها را در زمان کمتری از مهر و موم شدن ایمن تطبیق می‌دهد.	[۲۰]	۲۰۱۹
این مقاله تعیین کرد که چگونه فناوری بلاک‌چین برای کاربرد در هوش مصنوعی و چالش‌های آن که به حریم خصوصی، مقیاس‌پذیری و تکنیک‌های اجماع می‌پردازد، مانند POS وPOA ، که مزایایی با بهبود امنیت قراردادهای هوشمند دارد، سازگار است، که نتیجه‌گیری می‌کند که اگرچه پذیرش فناوری هنوز بهترین نیست، اما ذخیره داده‌ها به روش غیرمتمرکز، بهبود مشکلات هوش مصنوعی برابر و سودمند است.	[۲۱]	۲۰۱۹
در این مقابله معماری بلاک‌چین مورد مطالعه و آزمایش قرار گرفت و می‌تواند امنیت مورد نیاز اینترنت اشیاء را از طریق کلیدهای خصوصی تامین کند. علاوه بر این، با کلیدهای عمومی مربوط به هر دستگاه اینترنت اشیاء، از طریق زنجیره‌ای از بلوک‌ها ذخیره می‌شود، همچنین دستکاری آن دشوار نیست و راحتی را فراهم می‌کند، به عنوان یک مزیت که ایمنی را بهبود می‌بخشد، به این نتیجه می‌رسد که فناوری مورد مطالعه یک عنصر اساسی در بخش عمومی است زیرا دستکاری آن آسان نیست، امنیت و راحتی را برای کاربران در دستگاه های خود فراهم می‌کند.	[۲۲]	۲۰۲۰
این مقاله یک کنترل دسترسی به نام اثبات احراز هویت را برای دستگاه‌های اینترنت اشیاء مبتنی بر بلاک‌چین پیشنهاد می‌کند تا بتواند با منابع محدود در سیستم توزیع‌شده خود به درستی کار کند، نتایج نشان می‌دهد که علاوه بر مقاومت در برابر حملات، کارآمد و مقیاس‌پذیر است که برای انطباق با سطح بالایی از همزمانی راحت است و به عنوان مزایایی باعث کاهش هزینه‌ها و بهبود زمان پاسخگویی می‌شود.	[۲۳]	۲۰۲۰
در این پروژه، فناوری‌های اینترنت اشیاء و بلاک‌چین با هم در داخل خانه پیاده‌سازی شدند تا تأثیر بلاک‌چین بر دستگاه‌های اینترنت اشیاء در یک خانه هوشمند را نشان دهند. با استفاده از کتابخانه Web3.py و همچنین زبان وایپر، از تکنیک اجماع اثبات اعتبار استفاده شد که به عنوان یک مزیت بهره‌وری در مصرف منابع را به همراه داشت و به این نتیجه رسید که فناوری پیاده سازی شده ایمن‌تر است، در برابر حملات داس و مرد میانی انعطاف ناپذیر است، بنابراین دسترسی به اطلاعات را کنترل می‌کند.	[۲۴]	۲۰۲۱
نمونه اولیه‌ای را برای مدیریت شناسه‌های اینترنت اشیاء مبتنی بر فناوری بلاک‌چین، همراه با قراردادهای هوشمند که امنیت، حریم خصوصی و اعتماد به اطلاعات مورد نیاز را ارائه می‌دهد، به عنوان یک مزیت بهبود امنیت را به دست می‌آورد، به این نتیجه رسید که بلاک‌چین یک سیستم قابل دوام و عملی است، قابل انطباق و گسترده در رویه های تجاری بزرگ است.	[۲۵]	۲۰۲۲
سیستمی مبتنی بر بلاک‌چین ساخت‌یافته برای شناسایی از طریق دستگاه‌های اینترنت اشیاء، با استفاده از تکنیک اجماع الگوریتم تحمل خطای بیزانس ، پیشنهاد کرد که نتیجه‌گیری می‌کند که فناوری پیشنهادی در دستگاه‌هایی با منابع محدود مانند اینترنت اشیاء، نیازمند است.	[۲۶]	۲۰۲۲

همچنین این بخش به بررسی مطالعات ادغام اینترنت اشیاء و بلاک‌چین کلیدی برای درک پیشرفت‌ها و چالش‌های فعلی در این زمینه می‌پردازد. این آثار منتخب زمینه و بینش‌های مرتبط با تحقیقات را ارائه می‌دهند و پیچیدگی‌ها و راه‌حل‌های بالقوه در افزایش امنیت اینترنت اشیاء از طریق فناوری بلاک‌چین را برجسته می‌کنند. جداول ۱-۲ و ۲-۲ مقایسه مختصری از مطالعات اینترنت اشیاء و بلاک‌چین را ارائه می‌دهد[۲۷].

در [۲۸]، کریستیدیس و همکاران در مورد پتانسیل آن برای متحول کردن دامنه از طریق تعاملات غیرمتمرکز، غیرقابل اعتماد و فرآیندهای خودکار از طریق قراردادهای هوشمند استدلال می‌کنند. علیرغم این وعده، آنها چالش‌های مهمی مانند مقیاس‌پذیری، حریم خصوصی و قابلیت اجرایی قانونی را تصدیق می‌کنند که باید به آنها رسیدگی شود. آنها راه‌حل‌های نوآورانه‌ای مانند «ادغام دوگانه» را برای استحکام قانونی پیشنهاد می‌کنند و تکنیک‌های حفظ حریم خصوصی را پیشنهاد می‌کنند، اگرچه اینها با مبادله در عملکرد و پیچیدگی همراه هستند. این مطالعه نشان می‌دهد که در حالی که بلاک‌چین می‌تواند مدل‌های کسب‌وکار جدید و کارآمدی در اینترنت اشیاء را فعال کند، استقرار چنین فناوری

مستلزم بررسی دقیق محدودیت‌های آن و تحقیقات مداوم برای کاهش معایب آن است.

علی الصداوی و همکاران [۲۹] تجزیه و تحلیل ظریفی از همگرایی اینترنت اشیاء و بلاک‌چین ارائه کرده‌اند و یک معماری سه لایه جدید را پیشنهاد کرده‌اند که محاسبات شبنم و محاسبات ابری را برای غلبه بر چالش های موجود در مقیاس‌پذیری، کارایی و تأخیر ادغام می‌کند. این معماری از تحمل خطای بیزانسی برای اجماع استفاده می‌کند و عملکرد سیستم و یکپارچگی داده‌ها را افزایش می‌دهد. علیرغم نقاط قوت سیستم پیشنهادی آنها، نویسندگان اذعان دارند که حساسیت تحمل خطای بیزانسی به حملات سیبیل[7] همچنان یک نگرانی است، با تقسیم به عنوان یک اقدام متقابل بالقوه اما پیچیده ارائه شده است. پذیرش این چالش‌ها توسط نویسندگان، بر ضرورت کاوش مداوم در تقویت چارچوب امنیتی یکپارچه‌سازی اینترنت اشیاء و بلاک چین تأکید می‌کند.

اوادده و همکاران [۳۰] یک چارچوب کنترل دسترسی نوآورانه برای اینترنت اشیاء ارائه می‌کند و از فناوری بلاک‌چین برای رفع نیاز روزافزون به امنیت قوی در چشم‌انداز در حال گسترش اینترنت اشیاء استفاده می‌کند. چارچوب آنها، دسترسی منصفانه، از طریق یک سیستم دوربین امنیتی هوشمند نمونه‌ای است که کاربرد عملی سیاست‌های کنترل دسترسی مبتنی بر هویت و مجاز را نشان می‌دهد. علیرغم مواجهه با چالش‌هایی مانند پردازش بلادرنگ و مقیاس‌پذیری بلاک‌چین، نویسندگان راه‌حل‌هایی مانند توسعه بلاک چین سفارشی و برنامه‌های افزودنی آتی از جمله یک لایه ذخیره‌سازی امن و یک مدل صورت‌حساب برای تشویق به اشتراک‌گذاری داده‌ها پیشنهاد می‌کنند. این کار نه تنها اثبات مفهومی برای کاربرد بلاک چین در امنیت اینترنت اشیاء ارائه می‌کند، بلکه راه‌هایی را برای پیشرفت‌های بیشتر در مکانیسم‌های کنترل دسترسی باز می‌کند.

وانگ و همکاران [۳۱] با معرفی یک طرح RDIC مبتنی بر بلاک چین به افزایش امنیت اینترنت اشیاء در شبکه‌های G۵ کمک کرده‌اند. تحقیقات آنها شواهد دقیقی از صحت و جعل ناپذیری این طرح ارائه می‌دهد که رویکرد ایمن و کارآمد را برای یکپارچگی داده ها تضمین می‌کند. استفاده از طرح RDIC آنها در اینترنت وسایل نقلیه از اهمیت ویژه ای برخوردار است و نیاز حیاتی به داده های قابل اعتماد در سیستم‌های خودروی خودران را برطرف می‌کند. کار وانگ و همکاران، درک مکانیسم‌های RDIC را بهبود می‌بخشد و زمینه‌ای را برای تحقیقات آینده در چارچوب‌های RDIC حفظ حریم خصوصی و چند مالکی ایجاد می‌کند، که تقاطع مهمی از فناوری بلاک چین و امنیت اینترنت اشیاء را نشان می‌دهد.

رانه و همکاران [۳۲] کاستی‌های ابزارهای سنتی مدیریت منابع پروژه را در صنعت مهندسی، تدارکات و ساخت و ساز ارزیابی می‌کند، که با سرعت سریع صنعت ۴.۰ تشدید می‌شود. آنها یک معماری یکپارچه بلاک چین و اینترنت اشیا را برای کاهش ناکارآمدی‌هایی مانند ورود دستی داده‌ها و به‌روزرسانی‌های تأخیری پیشنهاد می‌کنند و مزایای داده‌های بلادرنگ و هماهنگی منابع مستقل را برای بهبود تصمیم‌گیری و چابکی در عملیات برجسته می‌کنند. علیرغم وعده این یکپارچگی در افزایش تخصیص و استفاده از منابع، این نویسندگان همچنین چالش‌های پیاده‌سازی، از جمله نیاز به به‌روزرسانی‌های زیرساختی قابل‌توجه و سازگاری صنعت با شیوه‌های جدید را تشخیص می‌دهد، که رویکردی محتاطانه و در عین حال خوش‌بینانه را برای پذیرش این فناوری‌ها در PRM نشان می‌دهد.

ما و همکاران [۳۳] با برجسته کردن نقش‌های اساسی شدت کربن ، بهینه‌سازی کلی کربن به پیشرفت حسابداری کربن و پایش انرژی در زمان واقعی و بهینه‌سازی کربن حاشیه‌ای در ارزیابی مصرف انرژی و تأثیر زیست محیطی آن کمک کرده‌اند. ادغام آنها از حسگرهای اینترنت اشیا با فناوری بلاک‌چین، کسب و مدیریت داده‌ها را متحول کرده است و شفافیت و مقیاس‌پذیری سیستم‌های نظارت بر انرژی را بهبود بخشیده است. علیرغم مواجهه با چالش‌هایی مانند تأخیر داده‌ها و نوسانات در عوامل انتشار، این تحقیقات چارچوب امیدوارکننده‌ای برای ارتقای رفتارهای انرژی پایدار و بهبود استراتژی‌های پاسخ به تقاضا ارائه می‌دهد.

[7] sybil

جدول ۲: مقایسه کارهای مرتبط ادغام اینترنت اشیاء و بلاک چین جهت افزایش امنیت

دامنه برنامه : راه حل های پیشنهادی	چالش های شناسایی شده	مشارکت های اصلی	عنوان	مرجع
اینترنت اشیاء: راه حل هایی مانند ادغام دوگانه برای استحکام قانونی و تکنیک های حفظ حریم خصوصی را پیشنهاد می‌کند.	مقیاس‌پذیری، حریم خصوصی و قابلیت اجرایی قانونی.	در مورد پتانسیل بلاک چین و قراردادهای هوشمند در ایجاد تحول در اینترنت اشیاء از طریق تعاملات غیرمتمرکز و فرآیندهای خودکار بحث می‌کند.	بلاک چین و قراردادهای هوشمند برای اینترنت اشیاء	[۲۸]
ادغام اینترنت اشیاء و بلاک چین: از تحمل خطای بیزانسی برای اجماع، بهبود عملکرد سیستم و یکپارچگی داده‌ها استفاده می کند. حساسیت تحمل خطای بیزانسی به حملات سایبل را تشخیص می‌دهد و به عنوان یک اقدام متقابل، به اشتراک گذاری را پیشنهاد می‌کند.	به چالش‌های مقیاس‌پذیری، کارایی و تأخیر در سیستم‌های اینترنت اشیاء و بلاک چین می‌پردازد.	تجزیه و تحلیل دقیقی از همگرایی اینترنت اشیاء و بلاک‌چین ارائه می‌دهد و یک معماری سه لایه جدید را ارائه می‌دهد که محاسبات شبنم و محاسبات ابری را ادغام می‌کند.	نظرسنجی در مورد ادغام بلاک چین با اینترنت اشیاء برای افزایش عملکرد و حذف چالش‌ها	[۲۹]
امنیت اینترنت اشیاء: توسعه بلاک چین سفارشی و الحاقات آتی از جمله لایه ذخیره-سازی امن و مدل صورتحساب را برای ایجاد انگیزه به اشتراک گذاری داده‌ها پیشنهاد می-کند.	چالش‌ها در پردازش بلادرنگ و مقیاس‌پذیری بلاک چین در اینترنت اشیاء.	دسترسی منصفانه را ارائه می‌کند، یک چارچوب کنترل دسترسی مبتنی بر بلاک-چین برای اینترنت اشیاء، که از طریق یک سیستم دوربین امنیتی هوشمند نشان داده شده است.	دسترسی منصفانه: یک چارچوب جدید کنترل دسترسی مبتنی بر بلاک چین برای اینترنت اشیاء	[۳۰]
امنیت اینترنت اشیاء در شبکه های G5: استفاده از طرح RDIC در اینترنت وسایل نقلیه، به نیاز حیاتی به داده های قابل اعتماد در سیستم‌های خودروی خودمختار رسیدگی می کند.	نیاز به داده‌های قابل اعتماد و یکپارچگی داده‌های ایمن در سیستم‌های خودروی خودمختار و اینترنت اشیاء در شبکه های G.۵	یک طرح RDIC مبتنی بر بلاک‌چین را برای افزایش امنیت اینترنت اشیاء در شبکه های G۵، با مدارک دقیق صحت و جعل ناپذیری معرفی می‌کند.	یک طرح بررسی یکپارچگی داده از راه دور مبتنی بر بلاک‌چین برای اینترنت اشیاء در شبکه‌های	[۳۱]
مدیریت منابع پروژه در صنعت ۴.۰: ادغام بلاک چین و اینترنت اشیاء را برای داده‌های بلادرنگ و هماهنگی منابع مستقل با هدف بهبود تصمیم گیری و چابکی در عملیات پیشنهاد می‌کند.	چالش‌های وارد کردن دستی داده‌ها و به‌روزرسانی‌های تاخیری در ابزارهای سنتی PRMدر صنعتEPC	کاستی‌های ابزارهای سنتی مدیریت منابع پروژه (PRM) را در صنعت EPC ارزیابی می‌کند و یک معماری یکپارچه بلاک چین و اینترنت اشیاء را برای تصمیم‌گیری و چابکی عملیاتی افزایش می‌دهد.	تصمیم‌گیری مبتنی بر داده با معماری یکپارچه بلاک چین و اینترنت اشیاء: چشم انداز چابکی مدیریت منابع پروژه در صنعت ۴.۰	[۳۲]
مدیریت انرژی پایدار: الگوریتم های مدل سازی پیش بینی و یادگیری ماشین را برای بهینه‌سازی الگوهای مصرف انرژی، ترویج رفتارهای انرژی پایدار اعمال می کند.	چالش هایی مانند تاخیر داده ها و نوسانات در عوامل انتشار.	پیش بردن حسابداری کربن و پایش انرژی در زمان واقعی را، ادغام حسگرهای اینترنت اشیا با بلاک چین برای بهبود کسب اطلاعات و مدیریت در ارزیابی مصرف انرژی.	شبکه حسگر بلاک‌چین و اینترنت اشیا برای اندازه‌گیری، ارزیابی و تشویق حسابداری محیطی شخصی و استفاده کارآمد از انرژی در فضاهای داخلی.	[۳۳]

9- نتیجه‌گیری و کارهای آتی

افزایش سریع استفاده از اینترنت اشیاء منجر به معرفی چندین آسیب‌پذیری امنیتی شده است که شامل حملات عبوری هم به داده‌ها و هم به دستگاه‌ها می‌شود .دستگاه‌های اینترنت اشیاء کنونی از عدم رعایت احتیاط‌های ایمنی رنج می‌برند و عمدتاً به دلیل منابع کمیاب، استانداردهای نابالغ، سازگاری ضعیف، عدم حفاظت در طراحی نرم‌افزار و سخت‌افزار و مشکلات در استقرار و توسعه، نمی‌توانند به درستی از خود محافظت کنند. جامعه علمی علاقه قابل توجهی به این موضوع نشان داده است که منجر به تلاش‌های متعددی برای ایجاد یک پایه جهانی قوی برای سیستم‌های اینترنت اشیاء شده است .در این اکوسیستم، استفاده از یک فناوری متمرکز و توزیع‌شده به نام «بلاک‌چین» ممکن است راه‌حل‌هایی برای مسائل امنیتی، حریم خصوصی، قابلیت ردیابی، قابلیت اطمینان و سازگاری ارائه دهد .ماهیت اساسی فناوری بلاک چین یکپارچگی، اصالت و عدم انکار را تضمین می کند .علاوه بر این، فرآیند خودکارسازی و اعتبارسنجی

تراکنش‌ها را با استفاده از قراردادهای هوشمند تسهیل می‌کند. با توجه به تحقیقات ارائه شده در مقاله‌های مربوط به استفاده از فناوری بلاک چین، می‌توان گفت که اینترنت اشیاء از آنجایی که امکان حل و حتی غلبه بر چالش‌های امروزی را فراهم می‌کند، علاوه بر ارائه مزایای بسیاری در هنگام به‌کارگیری آن، اما موثر و کارآمد، با شروع از رویکرد ایمن‌تر، حائز اهمیت است. چندین پیاده‌سازی و استفاده از آزمایش‌ها پیدا شد که در آن فناوری بلاک‌چین با اینترنت اشیاء ادغام شده است، بنابراین نشان می‌دهد که این دو فناوری با هم کار می‌کنند و نه تنها راه بهتری برای ذخیره داده‌ها و حفظ ارتباط بین دستگاه‌ها و مشتریان ارائه می‌دهند، بلکه امنیت را تا سطحی که عملاً نفوذ آن غیرممکن است افزایش می‌دهد. می‌توان نتیجه گرفت که این فناوری کمک مثبتی در حوزه امنیت می‌کند، بنابراین در بهبود مقیاس‌پذیری شبکه مشهود است و امکان اجرای یک شبکه اینترنت اشیاء بزرگ‌تر را با استفاده از قدرت محاسباتی تمام گره‌هایی که به شبکه تعلق دارند برای بهینه‌سازی عملکرد با اجازه دادن به همه دستگاه‌های متصل برای از دست دادن خدمات، امکان‌پذیر می‌کند.

۱۰- منابع

1. Al Barazanchi, I.I. and W. Hashim, Enhancing IoT Device Security through Blockchain Technology: A Decentralized Approach. SHIFRA, 2023. 2023: p. 10-16.

2. Daissaoui, A., et al., IoT and big data analytics for smart buildings: A survey. Procedia computer science, 2020. 170: p. 161-168.

3. Sethi, P. and S.R. Sarangi, Internet of things: architectures, protocols, and applications. Journal of electrical and computer engineering, 2017. 2017(1): p. 9324035.

4. Bilal, M., A review of internet of things architecture, technologies and analysis smartphone-based attacks against 3D printers. arXiv preprint arXiv:1708.04560, 2017.

5. Hui, T.K., R.S. Sherratt, and D.D. Sánchez, Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. Future Generation Computer Systems, 2017. 76: p. 358-369.

6. Stojkoska, B.L.R. and K.V. Trivodaliev, A review of Internet of Things for smart home: Challenges and solutions. Journal of cleaner production, 2017. 140: p. 1454-1464.

7. Jia, M., et al., Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications. Automation in construction, 2019. 101: p. 111-126.

8. Whitmore, A., A. Agarwal, and L. Da Xu, The Internet of Things—A survey of topics and trends. Information systems frontiers, 2015. 17: p. 261-274.

9. Rahaman, M.M., A Review on Internet of Things-IoT-Architecture, Technologies, Future Applications & Challenges. International Journal of Science and Business, 2022. 14(1): p. 80-92.

10. Ahmid, M., O. Kazar, and E. Barka, Internet of Things Overview: Architecture, Technologies, Application, and Challenges, in Decision Making and Security Risk Management for IoT Environments. 2024, Springer. p. 1-19.

11.Mosud, Y., E. Ajulo, and A. Yinusa, Internet of Things (IoT) Security and Private Concerns: An Overview. 2023.

12.Sharma, S., A.V. Singh, and V. Dattana. A survey of IoT routing protocols based on security and trust management. in 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). 2020. IEEE.

13.Iwuanyanwu, U., et al., IoT Device Security Risks: A Comprehensive Overview and Mitigation Strategies. Journal of Things and Internet (JOTIN), 2023. 3(1): p. 38-43.

14.Kadkhoda dehkhani, S., et al., Blockchain Technology: A Review of Concepts, Blockchain Challenges in Public Services, and Blockchain Token Classification. Computing and distributed systems, 2023. 6(1): p. 118-136.

15.Matthew N. O. Sadiku, U.C.C.a.J.O.S., Blockchain in Iot: A Brief Review. Web of Scholars: Multidimensional Research Journal (MRJ) Volume: 02 Issue: 08 | 2023 ISSN: (2751-7543) http://innosci.org, 2023.

16.Alphonse, A.S. and M. Starvin, Blockchain and internet of things: An overview. Handbook of Research on Blockchain Technology, 2020: p. 295-322.

17.Vergaray, A.D., H.J.F. Rosales, and R.L. Cordova, Blockchain Technology Aimed at Solving Internet of Things Challenges: A Systematic Literature Review. TEM Journal, 2023. 12(2): p. 757.

18.Bao, Z., et al., IoTChain: A three-tier blockchain-based IoT security architecture. arXiv preprint arXiv:1806.02008, 2018.

19.Reyna, A., et al., On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems, 2018. 88: p. 173-190.
20.Matsuura, K., Token model and interpretation function for blockchain-based Fintech applications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2019. 102(1): p. 3-10.
21.Salah, K., et al., Blockchain for AI: Review and open research challenges. IEEE access, 2019. 7: p. 10127-10149.
22.Liang, N. Security transmission and storage of Internet of Things information based on blockchain. in IOP Conference Series: Materials Science and Engineering. 2020. IOP Publishing.
23.Zhang, Y., et al., An attribute-based collaborative access control scheme using blockchain for IoT devices. Electronics, 2020. 9(2): p. 285.
24.Acurio Conteron, O.D., Sistema de Smart Home Aplicando IoT y Blockchain. 2021.
25.Venkatraman, S. and S. Parvin, Developing an IoT identity management system using blockchain. Systems, 2022. 10(2): p. 39.
26.Al Ahmed, M.T., et al., Hierarchical blockchain structure for node authentication in IoT networks. Egyptian Informatics Journal, 2022. 23(2): p. 345-361.
27.Bobde, Y., et al., Enhancing Industrial IoT Network Security through Blockchain Integration. Electronics, 2024. 13(4): p. 687.
28.Christidis, K. and M. Devetsikiotis, Blockchains and smart contracts for the internet of things. IEEE access, 2016. 4: p. 2292-2303.
29. Al Sadawi, A., M.S. Hassan, and M. Ndiaye, A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. IEEE Access, 2021. 9: p. 54478-54497.
30.Ouaddah, A., A. Abou Elkalam, and A. Ait Ouahman, FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and communication networks, 2016. 9(18): p. 5943-5964.
31.Wang, H., et al., RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks. Journal of Parallel and Distributed Computing, 2021. 152: p. 1-10.
32.Rane, S.B. and Y.A.M. Narvel, Data-driven decision making with Blockchain-IoT integrated architecture: a project resource management agility perspective of industry 4.0. International Journal of System Assurance Engineering and Management, 2022. 13(2): p. 1005-1023.

مائده رحمانی، دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار ، دانشگاه پیام نور مرکز بین الملل کیش می باشد و نشانه رایانامه ایشان عبارتند از :
Maede9708@gmail.com

فرشید وظیفه دوست، فارغ التحصیل در مقطع کارشناسی ارشد رشته مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز از دانشگاه پیام نور مرکز بین الملل قشم می باشد و نشانه رایانامه ایشان عبارتند از :
Vazifehdoostfarshid@gmail.com

سمیه کدخدا ده خانی، فارغ التحصیل مقطع کارشناسی ارشد رشته مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز دانشگاه پیام‌نور قشم می باشد، او به عنوان کارشناس فناوری در دانشگاه پیام‌نور استان کرمان مشغول به کار می باشد و نشانه رایانامه ایشان عبارتند از :
Emailsk65@gmail.com

حمید زنگی آبادی زاده، دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز، دانشگاه پیام نور مرکز بین الملل کیش می باشد و نشانه رایانامه ایشان عبارتند از:
Hamid.zangiabadi@gmail.com

مهدی قاسمی، دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز ، دانشگاه پیام نور مرکز بین الملل کیش می باشد و نشانه رایانامه ایشان عبارتند از :
Mahdikmg1@gmail.com

efficiency, and more suitable key latency. IoT environments. Using lightweight consensus mechanisms, this system can maintain low energy consumption while processing high-volume transactions in real time.

روش ارجاع: م. رحمانی ، ف. وظیفه دوست ، س. کدخدا ده خانی، ح. زنگی آبادی زاده و م. قاسمی. مرور و مقایسه بر تکنیک‌های افزایش امنیت سیستم‌های اینترنت اشیاء مبتنی بر بلاکچین. دوفصلنامه محاسبات و سامانه‌های توزیع شده، سال هفتم، شماره۱، شماره پیاپی۱۳، صفحه ۱۰۶ تا ۱۲۳، سال ۱۴۰۳.

How to cite: M.Rahmani، F.Vazifehdoost، S.kadkhodadehkhani، H.Zangiabadi Zadeh، M.Ghasemi، Review and comparison of techniques for increasing the security of blockchain-based IoT systems. Journal of Distributed Computing and Systems (JDCS), Vol 7, Issue 1, Pages 106-123, 2024.

Review and comparison of techniques for increasing the security of blockchain-based IoT systems

M.Rahmani[1] ، F.Vazifehdoost[2]، S.kadkhodadehkhani[3] ،
H.Zangiabadi Zadeh[4] ،M.Ghasemi[5]

[1] Payame Noor University, Kish.
[2,3] Payame Noor University, Qeshm International Center.
[4,5]Payame Noor University, Kish International Center.

Abstract

The rapidly growing IoT devices pose significant security challenges due to their decentralized nature, limited computing power, and reliance on centralized security models. Blockchain technology has emerged as a potential solution due to its decentralized, immutable, and transparent nature, providing advanced security for IoT environments. This study proposes a blockchain-based security strategy aimed at mitigating security risks in IoT networks. This study demonstrates that blockchain technology can significantly improve the security of IoT networks by addressing the limitations of traditional and centralized security models. Blockchain and IoT devices can be combined and improved by using smart contract device authentication, data integrity verification, and results availability, authentication speed, energy