ISSN 2717-0233
RAYANIRAN
وزارت فرهنگ و ارشاد 7656

کنترل دسترسی غیرمتمرکز در اینترنت اشیاء

سمیرا رنجبر تپه کلی ,سمیه رنجبر تپه کلی ,مهسا رفیعی ،

سمیرا رنجبر تپه کلی – sa.ranjbar2024k@gmail.com – ارشد دانشگاه ملی مهارت واحد کرمانشاه، گروه کامپیوتر
سمیه رنجبر تپه کلی – s.ranjbar1369@gmail.com – ارشد دانشگاه ملی مهارت واحد کرمانشاه، گروه کامپیوتر
مهسا رفیعی – mahsarafiee7373@gmail.com – ارشد دانشگاه ملی مهارت واحد کرمانشاه، گروه کامپیوتر

چکیده

اینترنت اشیاء « internet of things » با رشد انفجاری دستگاه‌های متصل و تنوع کاربردها، با چالش سه‌گانه مقیاس‌پذیری، امنیت و حفظ حریم خصوصی مواجه است که مدل‌های سنتی کنترل دسترسی توانایی پاسخگویی همزمان به آنها را ندارند. فناوری بلاکچین به عنوان یک راه‌حل غیرمتمرکز برای کنترل دسترسی ظهور کرده، اما شکاف عمیقی میان ادعاهای نظری مقالات و امکان‌سنجی عملی این راه‌حل‌ها در محیط‌های واقعی وجود دارد. این مقاله با هدف پر کردن این شکاف، یک مرور نظام‌مند و تحلیل تطبیقی از پژوهش‌های حوزه کنترل دسترسی مبتنی بر بلاکچین برای اینترنت اشیاء مقیاس‌پذیر ارائه می‌دهد. یافته‌ها نشان می‌دهد که معماری‌های تحقیقاتی از رویکردهای بلاک چین خالص به سمت معماری‌های ترکیبی چندلایه « Fog-Edge-Block chain » تکامل یافته و مدل کنترل دسترسی مبتنی بر ویژگی « ABAC » با سهم ۳۷٪ به عنوان مدل غالب شناسایی شده است. همچنین، تمرکز پژوهش‌های جدید به سمت تکنیک‌های پیشرفته حفظ حریم خصوصی نظیر اثبات دانش صفر « ZKP » و رمزنگاری مبتنی بر سیاست پنهان معطوف شده است. با این حال، حدود ۷۳٪ از مطالعات بررسی‌شده فاقد ارزیابی تجربی در مقیاس واقعی بوده و صرفاً به شبیه‌سازی‌های محدود بسنده کرده‌اند که این مهم‌ترین مانع تجاری‌سازی این فناوری‌ها محسوب می‌شود. این مرور نشان می‌دهد که حوزه کنترل دسترسی مبتنی بر بلاکچین برای اینترنت اشیاء از مرحله اثبات مفهوم عبور کرده، اما شکاف عمیق میان نظریه و عمل همچنان پابرجاست. بر اساس یافته‌ها، یک نقشه راه تحقیقاتی سه‌لایه شامل: « ۱ » کوتاه‌مدت: توسعه پروتکل‌های اجماع فوق‌سبک و الگوریتم‌های رمزنگاری بهینه‌سازی‌شده برای دستگاه‌های لبه ای؛ « 2 » میان‌مدت: ایجاد بسترهای آزمون « Test bed » مقیاس‌پذیر برای ارزیابی عملی راه‌حل‌ها؛ و « 3 » بلندمدت: ادغام با معماری‌های G6 و بهره‌گیری از هوش مصنوعی برای سیاست‌گذاری پویا و تطبیقی، پیشنهاد می‌شود.

واژه‌های کلیدی: کنترل دسترسی مبتنی بر بلاکچین، اینترنت اشیاء مقیاس‌پذیر، مرور نظام‌مند، تحلیل تطبیقی، حفظ حریم خصوصی، معماری‌های ترکیبی ابر-مه-لبه.

- مقدمه

اینترنت اشیاء « internet of things » با اتصال میلیاردها دستگاه هوشمند، انقلابی در حوزه‌های گوناگون از جمله خانه‌های هوشمند، صنعت ۴.۰، سلامت الکترونیک و شهرهای هوشمند ایجاد کرده است « 3 » ، « 18 » ، « 23 » . با این حال، رشد تصاعدی و ناهمگنی ذاتی این دستگاه‌ها، چالش‌های بنیادینی در زمینه امنیت، حریم خصوصی و مقیاس‌پذیری به همراه داشته که توسعه و بهره‌برداری از این اکوسیستم‌ها را با دشواری مواجه ساخته است « 4 » ، « 6 » .

در مرکز این چالش‌ها، مکانیسم‌های احراز هویت و کنترل دسترسی قرار دارند که مسئولیت حفاظت از داده‌ها و منابع را در برابر دسترسی‌های غیرمجاز بر عهده دارند « 2 » ، « 9 » ، « 12 » . مدل‌های سنتی و متمرکز کنترل دسترسی، علی‌رغم سادگی، در محیط‌های پویا و گسترده اینترنت اشیا با محدودیت‌های جدی مواجه‌اند. این مدل‌ها به نقاط شکست متمرکز وابسته بوده، از انعطاف‌پذیری و مقیاس‌پذیری کافی برخوردار نیستند و در برابر به‌روزرسانی پویای سیاست‌ها ناکارآمد عمل می‌کنند « 1 » ، « 10 » ، « 16 » . رویکردهای پیشرفته‌تری نظیر کنترل دسترسی مبتنی بر ویژگی « Attribute based access control » ، اگرچه انعطاف بیشتری ارائه می‌دهند، اما پیاده‌سازی، مدیریت و ابطال کارآمد آن‌ها در مقیاس کلان اینترنت اشیا همچنان به عنوان یک مسئله باز مطرح است « 28 » ، « 31 » .

فناوری بلاکچین به عنوان یک پارادایم غیرمتمرکز، شفاف و مقاوم در برابر دستکاری، پاسخی نویدبخش به این محدودیت‌ها ارائه می‌دهد « 5 » ، « 7 » ، « 11 » . قراردادهای هوشمند این امکان را فراهم می‌آورند که فرآیندهای احراز هویت و اعطای مجوز به صورت خودکار اجرا شده و زیرساخت اعتماد توزیع‌شده‌ای ایجاد گردد. افزون بر این، تکنیک‌های رمزنگاری پیشرفته مانند اثبات دانش صفر « ZKP » و رمزنگاری مبتنی بر سیاست پنهان، اجرای سیاست‌های دسترسی را با حفظ حریم خصوصی کاربران ممکن ساخته‌اند « 14 » ، « 17 » . با وجود این مزایا، ادغام بلاکچین با اینترنت اشیا خود چالش‌های تازه‌ای نظیر سربار پردازشی و تأخیر ناشی از مکانیسم‌های اجماع، نیاز به معماری‌های سبک‌وزن، و مدیریت بردارهای حمله احتمالی را به دنبال داشته است « 22 » ، « 26 » ، « 29 » .

اگرچه تاکنون مرورهای متعددی در این حوزه منتشر شده است، اما هر یک عمدتاً بر جنبه‌ای خاص تمرکز داشته‌اند. برای نمونه، برخی صرفاً بر مدل‌های دسترسی متمرکز بوده‌اند « 12 » ، برخی تنها چالش‌های امنیتی را بررسی کرده‌اند « 19 » ، و معدودی نیز به طور سطحی به مقیاس‌پذیری پرداخته‌اند « 32 » . با این حال، هیچ‌یک از مرورهای پیشین به طور هم‌زمان به تحلیل تطبیقی شکاف میان نظریه و عمل و ارائه چارچوب ارزیابی کمّی نپرداخته‌اند. این خلأ، انگیزه اصلی

انجام این پژوهش است.

این مقاله با هدف پاسخ به سه سؤال اساسی انجام شده است: « ۱ » روند تکاملی معماری‌های کنترل دسترسی مبتنی بر بلاکچین برای IoT چگونه بوده است؟ « ۲ » مهم‌ترین چالش‌های عملیاتی در مسیر پیاده‌سازی این راه‌حل‌ها کدامند؟ « ۳ » شکاف میان ادعاهای نظری و امکان‌سنجی عملی چقدر است؟

دستاوردهای اصلی این مقاله عبارتند از:

- ارائه یک چارچوب ارزیابی چهاربعدی « معماری، مدل دسترسی، تکنیک رمزنگاری، بلوغ تجربی » برای دسته‌بندی و تحلیل روش‌های موجود؛

- شناسایی کمّی شکاف میان نظریه و عمل با استناد به این که ۷۳٪ از مطالعات فاقد ارزیابی تجربی در مقیاس واقعی هستند؛

- ترسیم نقشه راه تحقیقاتی سه‌لایه « کوتاه‌مدت، میان‌مدت، بلندمدت » برای هدایت پژوهش‌های آتی؛

- تحلیل روند تکاملی معماری‌ها از بلاکچین خالص به سمت رویکردهای ترکیبی « Fog-Edge-Block chain » .

ساختار باقی مقاله به این شرح است: بخش ۲، روش‌شناسی مطالعه مروری را تشریح می‌کند. بخش ۳ به تحلیل مدل‌های سنتی کنترل دسترسی و کاستی‌های آن‌ها می‌پردازد. در بخش ۴، راه‌حل‌های مبتنی بر بلاکچین دسته‌بندی و به صورت تطبیقی ارزیابی می‌شوند. بخش ۵ به بحث و تحلیل نقادانه یافته‌ها اختصاص دارد و نهایتاً بخش ۶ نتیجه‌گیری و جهت‌گیری‌های آینده را ارائه می‌دهد.

۲- روش‌شناسی مطالعه مروری

این پژوهش با هدف ارائه‌ی یک مرور سیستماتیک، تحلیلی و آینده‌نگر از آخرین پیشرفت‌ها در حوزه‌ی احراز هویت و کنترل دسترسی مبتنی بر بلاکچین برای سیستم‌های مقیاس‌پذیر اینترنت اشیاء انجام شده است. چارچوب روش‌شناختی این مطالعه از دستورالعمل‌های PRISMA 2020 « Preferred Reporting Items for Systematic Reviews and Meta-Analyses » الهام گرفته شده و بر چهار مرحله‌ی کلیدی استوار است: طراحی سؤال و استراتژی، شناسایی و گزینش مدارک، استخراج و کدگذاری داده‌ها، و تحلیل و سنتز نقادانه. این رویه‌ها برای حفظ عینیت و کاهش سوگیری، توسط دو پژوهشگر به صورت موازی اجرا و اختلاف نظرها از طریق اجماع حل شد.

2-1- سؤالات پژوهش محرک « Research Driving Questions – RDQs »

برای هدایت فرآیند مرور، سؤالات کلیدی زیر تعریف شد:

• معماری‌ها و چارچوب‌های نوین کنترل دسترسی مبتنی بر بلاکچین برای اینترنت اشیا « مانند « 2 » ، « 5 » ، « 9 » ، « 14 » » چگونه چالش‌های مقیاس‌پذیری و ناهمگنی را هدف قرار می‌دهند؟

• تکنیک‌های رمزنگاری پیشرفته « نظیراثبات دانش صفر » « 1، » CP-ABE/IPE « ، ZeroKnowledge Proof » 39، 40 « 10، 28، 39 » ، و رمزگذاری با سیاست پنهان « 1، 10 » و مکانیسم‌های اجماع سبک‌وزن « 29 » » چگونه در این چارچوب‌ها ادغام شده‌اند تا امنیت، حریم خصوصی و کارایی عملیاتی را تقویت کنند؟

• مهم‌ترین چالش‌های پیاده‌سازی، محدودیت‌ها و بردارهای حمله در ادغام بلاکچین با اینترنت اشیا « با توجه به یافته‌های « 22 » ، « 26 » ، « 29 » » چیست و چه گپ‌های تحقیقاتی آینده‌ای « همچون ادغام با هوش مصنوعی « 8، 31 » و امنیت اعتماد صفر « 39 » » شناسایی می‌شوند؟

۲-۲- استراتژی جستجوی نظام‌مند

جستجو برای یافتن مقالات مرتبط در بازه‌ی زمانی ژانویه ۲۰۱۸ تا سپتامبر ۲۰۲۵ در پنج پایگاه‌داده‌ی علمی اصلی انجام شد: Springer Link، ACM Digital Library، Science Direct ، IEEE Xplore، و Scopus. این بازه جهت پوشش حداکثری رشد انفجاری پژوهش در حوزه‌ی بلاکچین و اینترنت اشیا پس از سال ۲۰۱۸ انتخاب شد.

رشته جستجو با ترکیب کلیدواژه‌های اصلی در عنوان، چکیده و واژگان کلیدی با استفاده از عملگرهای بولی ساخته شد:

Block chain" OR "distributed ledger" » AND « "access control" OR "authentication" OR "authorization"" »
« "» AND « "IoT" OR "internet of things" » AND « "scalability" OR "performance" OR "efficiency

برای اطمینان از جامعیت، روش گلوله برفی معکوس « Backward Snowballing » با بررسی دقیق فهرست منابع مقالات کلیدی و مرورهای شاخص « نظیر « 3 » ، « 6 » ، « 11 » ، « 18 » » به کار گرفته شد که منجر به شناسایی مطالعات ارزشمند دیگری مانند « 31 » و « 32 » گردید.

2-3- فرآیند گزینش و معیارهای شمول/طرد

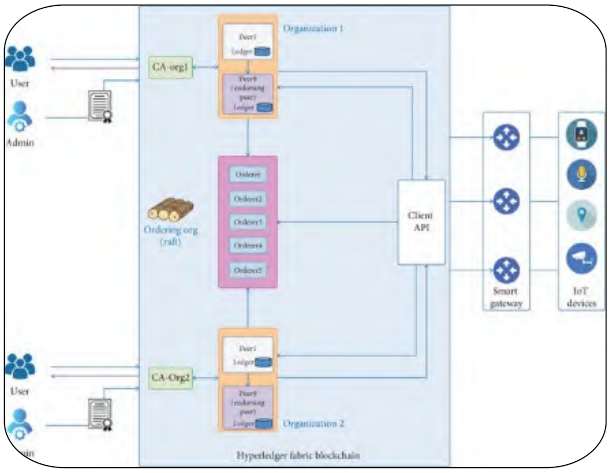
از بین ۱۲۵۸ مطالعه اولیه شناسایی شده، فرآیند غربالگری چندمرحله‌ای مطابق با نمودار PRISMA اجرا شد. پس از حذف موارد تکراری و بررسی عناوین و چکیده‌ها، متن کامل ۱۷۲ مقاله برای ارزیابی نهایی واجد شرایط تشخیص داده شد. معیارهای تصمیم‌گیری نهایی در جدول ۱ ارائه شده است.

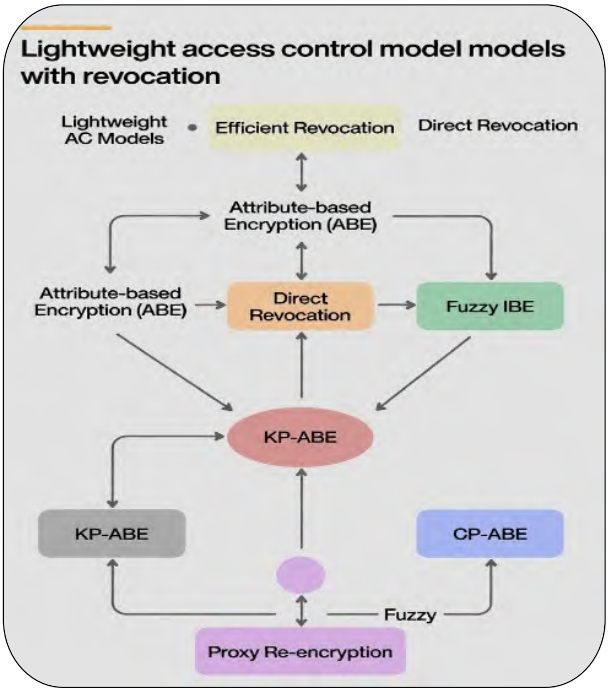
جدول ۱: معیارهای شمول و طرد مقالات در فرآیند مرور سیستماتیک

معیارهای شمول « Inclusion Criteria – IC »	معیارهای طرد « Exclusion Criteria – EC »
مقاله مستقیماً به طراحی، پیاده‌سازی یا ارزیابی یک مکانیسم کنترل دسترسی یا احراز هویت مبتنی بر بلاکچین برای اینترنت اشیا می‌پردازد « مانند « ۲ » ، « ۵ » ، « ۷ » ، « ۲٤ » »	مقاله صرفاً یک مرور کلی است که تمرکز تخصصی بر ادغام بلاکچین و کنترل دسترسی اینترنت اشیا ندارد « مانند مرورهای عمومی امنیت اینترنت اشیا « ۲۳ » که تنها بخش کوچکی به بلاکچین پرداخته‌اند.
مقاله به صراحت به چالش مقیاس‌پذیری، کارایی، یا مدیریت منابع در معماری پیشنهادی خود پرداخته یا آن را ارزیابی کرده است « مانند « ١٤ » ، « ۲۹ » ، « ۳٤ » ، « ۳۸ »	مقاله فاقد ارزیابی تجربی، شبیه‌سازی، یا تحلیل کمی از عملکرد یا امنیت طرح پیشنهادی است
مقاله در یک کنفرانس یا مجله بین‌المللی معتبر منتشر شده و به زبان انگلیسی است	مقاله به صورت پیش‌چکیده، پایان‌نامه بدون داوری، یا گزارش فنی غیرقابل‌دسترس است
مقاله از تکنیک‌های رمزنگاری پیشرفته مانند ZKP، ABAC پنهان‌ساز یا معماری‌های ترکیبی « ابر-مه-لبه » بهره می‌برد « مانند « ۱ » ، « ۱۰ » ، « ۱۷ » ، « ۳۳ » ، « ۳۹ » ، « ٤۰ »	مقاله تنها بر جنبه‌های دیگر بلاکچین در اینترنت اشیا « مانند ردیابی زنجیره تأمین یا مدیریت هویت ساده » بدون مؤلفه کنترل دسترسی پیچیده متمرکز است.

معیارهای شمول « Inclusion Criteria – IC »	معیارهای طرد « Exclusion Criteria – EC »
مقاله مستقیماً به طراحی، پیاده‌سازی یا ارزیابی یک مکانیسم کنترل دسترسی یا احراز هویت مبتنی بر بلاکچین برای اینترنت اشیا می‌پردازد « مانند « 2 » ، « 5 » ، « 7 » ، « 24 » »	مقاله صرفاً یک مرور کلی است که تمرکز تخصصی بر ادغام بلاکچین و کنترل دسترسی اینترنت اشیا ندارد « مانند مرورهای عمومی امنیت « 23 » که تنها بخش کوچکی به بلاکچین پرداخته‌اند
مقاله به صراحت به چالش مقیاس‌پذیری، کارایی، یا مدیریت منابع در معماری پیشنهادی خود پرداخته یا آن را ارزیابی کرده است « مانند « 14 » ، « 29 » ، « 34 » ، « 38 » »	مقاله فاقد ارزیابی تجربی، شبیه‌سازی، یا تحلیل کمی از عملکرد یا امنیت طرح پیشنهادی است
مقاله در یک کنفرانس یا مجله بین‌المللی دارای رتبه‌بندی « معتبر » منتشر شده و به زبان انگلیسی است	مقاله به صورت پیش‌چکیده، پایان‌نامه بدون داوری، یا گزارش فنی غیرقابل‌دسترسی است
مقاله از تکنیک‌های رمزنگاری پیشرفته « مثل ZKP، ABAC پنهان‌ساز » یا معماری‌های ترکیبی « ابر-مه-لبه » بهره می‌برد « مانند « 1 » ، « 10 » ، « 17 » ، « 33 » ، « 39 » ، « 40 » »	مقاله تنها بر جنبه‌های دیگر بلاکچین در کنترل دسترسی « مانند ردیابی زنجیره تأمین یا مدیریت هویت ساده » بدون مؤلفه کنترل دسترسی پیچیده متمرکز است

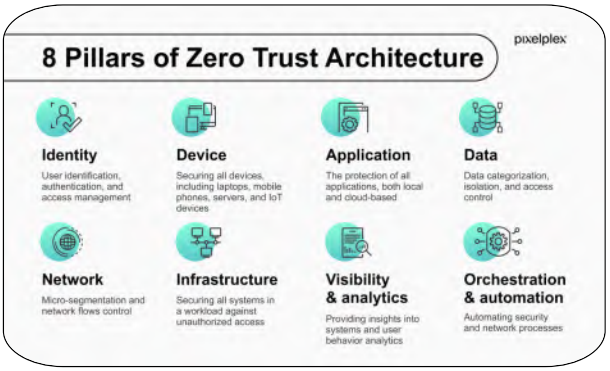
مقالات شناسایی‌شده از پایگاه‌ها مقالات شناسایی‌شده از پایگاه‌ها « Science , « n=350 » IEEE « n = 1258 » Springer « n=208 , « n=280 » ACM, « n=420 » Direct « حذف مقالات تکراری « 278 = n » « n= » مقالات پس از حذف تکراری‌ها « 78 = 980n » غربالگری عنوان و چکیده « n = 278 » « 980n= » مقالات شناسایی‌شده از پایگاه‌ها « Springer « n=208 , « n=280 » ACM, « n=420 » Science Direct , « n=350 » IEEE « n = 1258 » حذف مقالات تکراری « 278 = n » « n= » مقالات پس از حذف تکراری‌ها « 78 = 980n » غربالگری عنوان و چکیده « » « 980n= » « n = 278 »



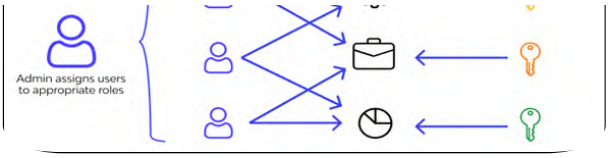


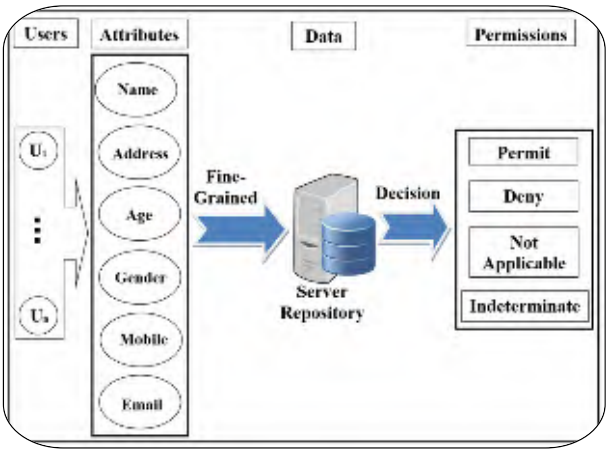
مقالات واجد شرایط » 808 « n = 278 » =n« مقالات واجد شرایط » 808 « n = 278 » =n« مقالات حذف‌شدهمقالات حذف‌شدهبررسی متن کامل » 172 « n = 808 » =n« بررسی متن کامل « n = 172 » مقالات

حذف‌شدهبررسی متن کامل » 172 « n = 808 » =n« بررسی متن کامل « 172 = n »

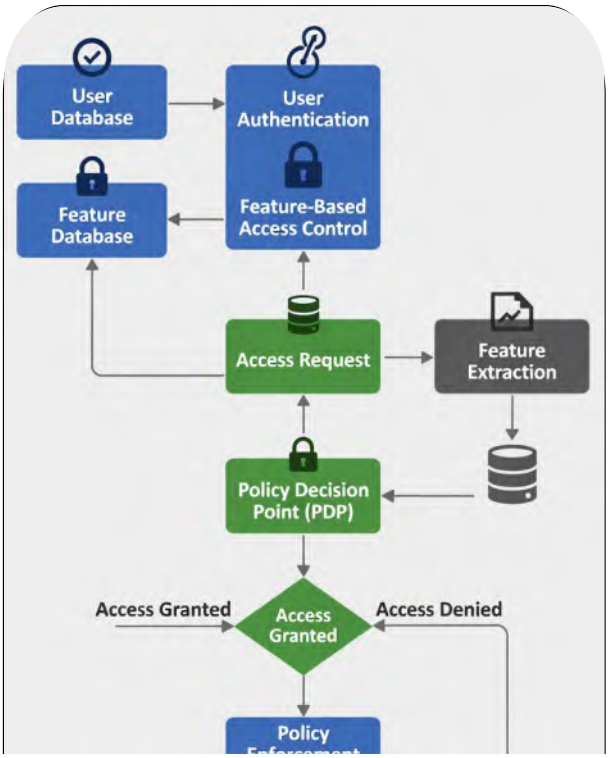


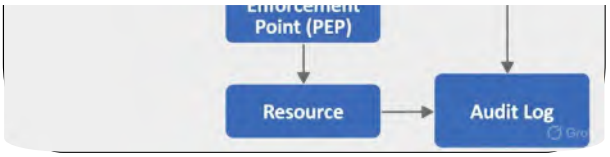
غربالگری متن کاملغربالگری متن کامل » 172 « n = 808 » =n« بررسی متن کامل « 172 = n » غربالگری متن کامل » 172 « n = 808 » =n« بررسی متن کامل « 172 = n »





مقالات حذف شدهمقالات حذف شده » 48 « n = 808 » n= « » بررسی متن کامل « n = 172 » مقالات حذف شده » 48 « n = 808 » n= « » بررسی متن کامل « n = 172 » مقالات نهاییمقالات نهایی » 124 « n=دلایل حذف : فاقد ارزیابیتجربی: 45تمرکز نادرست : 30مرور کلی :25 پیش چکیده : 15سایر : 9مقالات نهایی » 124 « n=دلایل حذف : فاقد ارزیابیتجربی: 45تمرکز نادرست : 30مرور کلی :25 پیش چکیده : 15سایر : 9





شکل 1: نمودار جریان PRISMA مرور سیستماتیک

2-4- استخراج داده و چارچوب تحلیل

داده‌ها از ۴۸ مقاله نهایی منتخب « که لیست گزیده‌ای از آن‌ها در بخش مراجع آمده » با استفاده از یک فرم استاندارد استخراج گردید. مهم‌ترین رده‌های تحلیلی « Analytical Categories » تعریف شده عبارت بودند از:

• رده ۱ – **مشخصات بنیادی:** سال انتشار، نوع نشریه، حوزه کاربرداینترنت اشیا « صنعتی، سلامت، شهر هوشمند » .

• رده ۲ – **ویژگی‌های معماری و فنی:** نوع پلتفرم بلاکچین، مکانیسم اجماع، ادغام با لایه‌های ابر/مه/لبه « « ١٤ » ، « ٣٣، ٣٤ » » ، و نحوه پیاده‌سازی قرارداد هوشمند.

• رده ۳ – **مکانیسم‌های امنیتی و حریم خصوصی:** مدل کنترل دسترسی غالب مبتنی بر ویژگی » 12 « ، » ١٧ « ، » ٢٠ « ،Capability Based ، » ١٣ « ،کنترل دسترسی مبتنی بر نقش « RBAC » تکنیک‌های رمزنگاری مورد استفاده، و

قابلیت‌های پیشرفته مانند ابطال « ۳۸ » ، حسابرسی « ۷ » ، « ۳۳ » و پنهان‌سازی سیاست « ۱ » ، « ۱۰ » .

· رده ۴ - **معیارهای ارزیابی و یافته‌ها:** پارامترهای عملکردی سنجیده شده « تأخیر، توان عملیاتی، مصرف حافظه/پردازش » ، روش مقایسه « با طرح‌های پایه یا سنتی » ، و نتایج کلیدی.

· رده ۵ - **محدودیت‌ها و جهت‌گیری آینده:** چالش‌های شناسایی‌شده توسط نویسندگان مقاله و پیشنهادات آن‌ها برای پژوهش‌های آتی.

2-5- **سنتز و تحلیل نقادانه**به جای یک ارائه توصیفی صرف، داده‌های استخراج شده در یک فرآیند تحلیل محتوای کیفی و مقایسه‌ای قرار گرفتند. مطالعات بر اساس الگوهای طراحی غالب دسته‌بندی شدند « مثلاً: معماری‌های مبتنی بر قرارداد هوشمند خالص « 9، 24 » در مقابل معماری‌های ترکیبی با لایه میانی مه « 14، 34 » » . سپس، نقاط قوت و ضعف هر الگو در مواجهه با چالش‌های مطرح درصف درخواست تصمیم Request Decision Query » » ها « مانند مقیاس‌پذیری در « 5 » در مقابل « 29 » » مقایسه و تحلیل گردید. این سنتز منجر به استخراج روندهای نوظهور « مانند گرایش به اثبات دانش صفر « ZeroKnowledge Proof » برای حریم خصوصی « 39، 40 » و مدل‌های اعتماد غیرمتمرکز « 17، 20 » » و ترسیم منظره تحقیقاتی « Research Landscape » فعلی و آینده حوزه شد.

2-6- محدودیت‌های روش‌شناختی

این مرور سیستماتیک با وجود رعایت رویه‌های دقیق، دارای محدودیت‌هایی است: « ۱ » جستجو محدود به پایگاه‌های داده منتخب و مقالات انگلیسی‌زبان بود. « ۲ » با توجه به پویایی بسیار بالای حوزه، ممکن است برخی مطالعات جدید یا پیش از انتشارکه پس از تاریخ جستجو منتشر شده‌اند، پوشش داده نشده باشند. « ۳ » تمرکز بر مطالعات با ارزیابی تجربی ممکن است برخی ایده‌های مفهومی نوآورانه اما فاقد پیاده‌سازی کامل را نادیده گرفته باشد.

3- **مرور بر مدل‌های سنتی کنترل دسترسی**در حوزه سیستم‌های اینترنت اشیا، مدل‌های سنتی کنترل دسترسی به عنوان پایه و اساس مدیریت مجوزهای منابع و تضمین امنیت عمل کرده‌اند. این مدل‌ها، که در اصل برای محیط‌های محاسباتی معمولی طراحی شده‌اند، برای پاسخگویی به نیازهای منحصربه‌فرد اینترنت اشیا مانند محدودیت‌های منابع، محیط‌های پویا و مقیاس‌پذیری عظیم، تطبیق یا گسترش یافته‌اند « ۳ » ، « ٦ » ، « ۲۳ » . با این حال، ماهیت متمرکز آن‌ها اغلب با معماری توزیع‌شده و ناهمگن شبکه‌های اینترنت اشیا درگیر است و منجر به آسیب‌پذیری‌هایی در

زمینه‌هایی مانند اجرای سیاست‌ها و تصمیم‌گیری‌های بلادرنگ می‌شود « ٤ » ، « ١١ » ، « ١٨ » . این بخش یک مرور جامع از مدل‌های کلیدی سنتی شامل کنترل دسترسی اختیاری « DAC » ، کنترل دسترسی اجباری « MAC » ، کنترل دسترسی مبتنی بر نقش « RBAC » ، کنترل دسترسی مبتنی بر ویژگی « ABAC » و کنترل دسترسی مبتنی بر قابلیت « Cap BAC » ارائه می‌دهد و مکانیسم‌ها، نقاط قوت، محدودیت‌ها و قابلیت اجرای آن‌ها در اینترنت اشیا را برجسته می‌کند. ما از بررسی‌های موجود برای تأکید بر تکامل و چالش‌های آن‌ها در زمینه‌های مدرن استفاده می‌کنیم « ٦ » ، « ١٢ » ، « ١٨ » ، « ٢٣ » .

3-1- کنترل دسترسی اختیاری « Discretionary Access Control – DAC »

کنترل دسترسی اختیاری یکی از قدیمی‌ترین و انعطاف‌پذیرترین مدل‌های کنترل دسترسی است، جایی که صاحبان منابع اختیار کامل برای اعطا یا لغو مجوزها به کاربران یا موضوعات را دارند « ٣ » ، « ٦ » . در کنترل دسترسی اختیاری ، تصمیمات دسترسی بر اساس هویت درخواست‌کننده و مجوزهای صریح تنظیم‌شده توسط صاحب، اغلب از طریق لیست‌های کنترل دسترسی « ACLs » پیاده‌سازی می‌شود. برای مثال، صاحب یک فایل می‌تواند مجوزهای خواندن/نوشتن را برای کاربران خاص مشخص کند « ٣ » .

نقاط قوت در زمینه‌های : اینترنت اشیا سادگی کنترل دسترسی اختیاری آن را برای استقرارهای کوچک‌مقیاس اینترنت اشیا، مانند سیستم‌های خانه هوشمند، مناسب می‌کند، جایی که صاحبان دستگاه‌ها می‌توانند دسترسی را بدون پیچیدگی‌های زیاد مدیریت کنند « ١٨ » ، « ٢٣ » . این مدل از کنترل کاربرمحور پشتیبانی می‌کند و با سناریوهایی که شخصی‌سازی کلیدی است، همخوانی دارد « ٦ » .

محدودیت‌ها و چالش‌ها: با این حال، کنترل دسترسی اختیاری مستعد مشکل "اسب تروجان" است، جایی که یک کاربر آلوده می‌تواند ناخواسته حقوق دسترسی را گسترش دهد و منجر به نشت داده‌های غیرمجاز شود « ٣ » ، « ١١ » . دراینترنت اشیا ، وابستگی متمرکز آن به صاحبان برای مدیریت سیاست‌ها در شبکه‌های بزرگ با میلیاردها دستگاه ناکارآمد می‌شود و مسائل مقیاس‌پذیری را تشدید کرده و خطر خطای انسانی در محیط‌های پویا را افزایش می‌دهد « ٤ » ، « ٦ » ، « ١٨ » . بررسی‌ها تأکید می‌کنند که کنترل دسترسی اختیاری فاقد کنترل دقیق است و آن را برای کاربردهای اینترنت اشیا با امنیت بالا مانند نظارت بهداشتی ناکافی می‌کند « ٢٣ » .

3-2- کنترل دسترسی اجباری « Mandatory Access Control – MAC »

کنترل دسترسی اجباری دسترسی را بر اساس برچسب‌های امنیتی یا طبقه‌بندی‌های ازپیش‌تعریف‌شده که به موضوعات « مانند کاربران » و اشیاء « مانند منابع » اختصاص داده شده، اجرا می‌کند و معمولاً توسط یک مقام مرکزی مدیریت می‌شود « ۳ » ، « ٦ » . قوانین مانند "عدم خواندن به بالا" « مدل Bell-La Padula » یا "عدم نوشتن به پایین" « مدل Biba » جریان اطلاعات بین سطوح امنیتی مختلف را جلوگیری می‌کند « ۳ » .

نقاط قوت در زمینه‌های : اینترنت اشیا در محیط‌هایی که نیاز به محرمانگی دارند، مانند سیستم‌های اینترنت اشیا نظامی یا صنعتی، برتری دارد و از ارتقای غیرمجاز امتیازات جلوگیری می‌کند « ۱۸ » ، « ۲۳ » . رویکرد سیاست‌محور آن اجرای مداوم را تضمین کرده و تهدیدهای داخلی را کاهش می‌دهد « ٦ » ، « ۱۱ » .

محدودیت‌ها و چالش‌ها: سختی مدل انعطاف‌پذیری را در سناریوی پویای اینترنت اشیا ، جایی که دستگاه‌ها اغلب به شبکه می‌پیوندند یا از آن خارج می‌شوند، مختل می‌کند « ٤ » ، « ۱۸ » . مدیریت متمرکز برچسب‌ها گلوگاه‌هایی ایجاد می‌کند و دستگاه‌های اینترنت اشیا با محدودیت منابع با بار محاسباتی تأیید برچسب‌ها مشکل دارند « ۳ » ، « ٦ » . بررسی‌های اخیر اشاره می‌کنند که عدم سازگاری کنترل دسترسی اجباری با تغییرات زمینه‌ای، مانند ویژگی‌های متغیر کاربر، استفاده از آن در اینترنت اشیا مصرفی را محدود می‌کند و اغلب نیاز به ترکیبی برای ادغام بهتر دارد « ۱۲ » ، « ۲۳ » .

۳-۳- کنترل دسترسی مبتنی بر نقش « Role-Based Access Control – RBAC »

کنترل دسترسی مبتنی بر نقش دسترسی را بر اساس نقش‌های اختصاص‌یافته به کاربران مدیریت می‌کند، جایی که مجوزها به نقش‌ها « مانند "مدیر" یا "کاربر عادی" » گره خورده‌اند و کاربران بر اساس نقش‌هایشان مجوز دریافت می‌کنند « ۳ » ، « ٦ » ، « ۱۳ » . این مدل از طریق ماتریس‌های نقش-مجوز پیاده‌سازی می‌شود و امکان مدیریت گروهی دسترسی را فراهم می‌کند « ۱۲ » . برای مثال، در یک سیستم، نقش "مدیر" ممکن است مجوزهای مدیریتی داشته باشد، در حالی که نقش "کاربر عادی" محدود به عملیات پایه است. این ساختار در شکل ۱ نشان داده شده است که سلسله مراتب نقش‌ها و جریان مجوزها را نشان می‌دهد.

شکل2: کنترل دسترسی مبتنی بر نقش « RBAC »

نقاط قوت در زمینه‌های کنترل دسترسی مبتنی بر نقش: اینترنت اشیا برای محیط‌های سازمانی اینترنت اشیا ، مانند اتوماسیون صنعتی، مناسب است زیرا مدیریت مجوزها را ساده می‌کند و با ساختارهای سلسله‌مراتبی همخوانی دارد « ۱۸ » ، « ۲۳ » . بررسی‌ها نشان می‌دهند که کنترل دسترسی مبتنی بر نقش مقیاس‌پذیری بهتری نسبت به کنترل دسترسی اختیاری « Discretionary Access Control » ارایه می‌دهد و خطاهای انسانی را کاهش می‌دهد « ٦ » ، « ۱۳ » .

محدودیت‌ها و چالش‌ها: در اینترنت اشیا پویا،کنترل دسترسی مبتنی بر نقش با تغییرات مکرر نقش‌ها « مانند دستگاه‌های موقت » سازگار نیست و نیاز به به‌روزرسانی مداوم نقش‌ها دارد که می‌تواند بار محاسباتی ایجاد کند « ٤ » ، « ۱۲ » . علاوه بر این، عدم توجه به ویژگی‌های زمینه‌ای مانند مکان یا زمان، آن را در برابر تهدیدهای پیشرفته آسیب‌پذیر می‌کند « ۳ » ، « ۱۸ » .

3-4-کنترل دسترسی مبتنی بر ویژگی « Attribute-Based Access Control - ABAC »

کنترل دسترسی مبتنی بر ویژگی دسترسی را بر اساس ویژگی‌های موضوعات، اشیاء، محیط و سیاست‌ها ارزیابی می‌کند، که امکان کنترل دانه‌ریز و پویا را فراهم می‌کند « ۳ » ، « ٦ » ، « ۱۲ » ، « ۲۰ » . برای مثال، دسترسی می‌تواند بر اساس ویژگی‌هایی مانند "زمان روز" یا "مکان جغرافیایی" محدود شود « ۹ » ، « ۱۰ » .

همانطور که در شکل ۲ نشان داده شده است، این مدل تصمیم‌گیری‌های دقیق و آگاه از زمینه را امکان‌پذیر می‌کند. در این معماری، درخواست دسترسی بر اساس ویژگی‌های موضوع، شیء، اقدام و محیط با سیاست‌های تعریف‌شده مقایسه شده و تصمیم نهایی اتخاذ می‌شود.

شکل 3: کنترل دسترسی مبتنی بر ویژگی « ABAC »

نقاط قوت در زمینه‌های کنترل دسترسی مبتنی بر ویژگی: برای اینترنت اشیا مقیاس‌پذیر ایده‌آل است زیرا با

محیط‌های ناهمگن سازگار است و سیاست‌های پویا را پشتیبانی می‌کند « ٤ » ، « ٦ » ، « ١٨ » . ادغام با فناوری‌های نوین مانند بلاکچین، آن را برای حفظ حریم خصوصی و امنیت بهبود می‌بخشد « ١٢ » ، « ٢٠ » ، « ٢٤ » .

محدودیت‌ها و چالش‌ها: پیچیدگی سیاست‌ها می‌تواند منجر به سربار محاسباتی شود، به‌ویژه در دستگاه‌های اینترنت اشیا با منابع محدود « ٣ » ، « ٢٨ » . بررسی‌ها اشاره می‌کنند که ابطال ویژگی‌ها و پنهان‌سازی سیاست‌ها چالش‌های کلیدی هستند که نیاز به راه‌حل‌های پیشرفته دارند « ١ » ، « ١٠ » ، « ٢٨ » .

3-5- کنترل دسترسی مبتنی بر قابلیت « Capability-Based Access Control – Cap BAC »

کنترل دسترسی مبتنی بر قابلیت دسترسی را از طریق قابلیت‌ها « توکن‌های غیرقابل‌جعل » مدیریت می‌کند که حقوق دسترسی را به طور مستقیم به کاربران اعطا می‌کند، بدون نیاز به بررسی مرکزی « ٢ » ، « ٣ » ، « ٦ » . این مدل توزیع‌شده برای محیط‌های غیرمتمرکز مناسب است « ٢ » ، « ٣١ » .

قابلیت‌ها می‌توانند واگذار یا لغو شوند و اغلب در سیستم‌های توزیع‌شده پیاده‌سازی می‌شوند. در شکل ٣، جریان اعطای دسترسی از طریق توکن‌های قابلیت و نحوه تعامل کاربر، دستگاه و منبع به تصویر کشیده شده است. این توکن‌ها حاوی مجوزهای لازم بوده و بدون نیاز به تأیید مکرر از سرور مرکزی قابل استفاده هستند.

شکل4: کنترل دسترسی مبتنی بر قابلیت « Cap BAC »

نقاط قوت در زمینه‌های : Cap BAC اینترنت اشیا مقیاس‌پذیری بالایی ارائه می‌دهد و با معماری توزیع‌شده اینترنت اشیا همخوانی دارد، زیرا وابستگی به سرور مرکزی را کاهش می‌دهد « ٢ » ، « ١٨ » ، « ٣١ » . بررسی‌ها نشان می‌دهند که ادغام با بلاکچین، ابطال و امنیت آن را بهبود می‌بخشد « ٢ » ، « ٥ » ، « ١٥ » .

محدودیت‌ها و چالش‌ها: مدیریت ابطال قابلیت‌ها پیچیده است و خطر نشت قابلیت‌ها وجود دارد « ٣ » ، « ٤ » . در اینترنت اشیا ، دستگاه‌های کم‌قدرت با رمزنگاری پیشرفته Cap BAC مشکل دارند « ٦ » ، « ٣١ » .

3-6- مدل‌های کلیدی کنترل دسترسی: سطح‌بندی، مزایا، معایب و قابلیت ادغام با بلاکچین

در ادامه، مدل‌های اصلی کنترل دسترسی بر اساس سطح سلسله‌مراتبی دسته‌بندی و از نظر ویژگی‌ها، مزایا، معایب و قابلیت ادغام با بلاکچین مقایسه شده‌اند. این دسته‌بندی نشان‌دهنده تکامل مدل‌ها از رویکردهای ساده و سنتی به سمت

معماری‌های پیچیده‌تر و بومی بلاکچین است.

جدول 2: مقایسه مدل‌های کنترل دسترسی از نظر سطح سلسله‌مراتبی، مزایا، معایب و قابلیت ادغام با بلاکچین

مدل	سطح سلسله‌مراتبی	توضیحات	مزایا	معایب	قابلیت ادغام با بلاکچین	منابع مرتبط
DAC	سطح ۱: پایه/سنتی	دسترسی از طریق ACLها یا ماتریس‌ها؛ تصمیمات اختیاری کاربر	پیاده‌سازی ساده؛ انعطاف‌پذیر برای اینترنت اشیا کوچک‌مقیاس	فاقد پویایی؛ شکست‌های تک‌نقطه‌ای؛ مقیاس‌پذیری ضعیف در اینترنت اشیا ناهمگن	ذخیره‌سازی غیرقابل‌دستکاری برای ACLها؛ ثبت توزیع‌شده بدون مقام مرکزی	« 3 » ، « 6 » ، « 25 »
MAC	سطح ۱: پایه/سنتی	قوانین اعمال‌شده توسط سیستم بر اساس برچسب‌های امنیتی؛ غیراختیاری	امنیت بالا در بخش‌های حیاتی اینترنت اشیا ؛ جلوگیری از ارتقای غیرمجاز	سفت و سخت؛ فاقد آگاهی از زمینه؛ بار اداری بالا	اعمال اجماع بر روی برچسب‌ها/سیاست ها و تضمین غیرقابل‌تغییر بودن	« 3 » ، « 6 » ، « 18 » ، « 23 »
RBAC	سطح ۲: مبتنی بر نقش/ ویژگی	دسترسی به نقش‌های کاربر گره خورده است؛ گسترش Or BAC با زمینه‌های سازمانی	کاهش بار اداری توسط سلسله‌مراتب نقش‌ها؛ پشتیبانی از واگذاری در گروه‌های اینترنت اشیا	انفجار نقش در اینترنت اشیا بزرگ؛ پویایی محدود بدون گسترش	مدیریت تخصیص/ابطال نقش‌ها؛ حسابرسی تغییرات نقش توسط دفترکل توزیع‌شده	« 3 » ، « 6 » ، « 13 » ، « 15 » ، « 20 » ، « 24 » ، « 25 »
ABAC	سطح ۲: مبتنی بر نقش/ ویژگی	تصمیمات ریزدانه بر اساس ویژگی‌های کاربر/منبع /محیط؛ پشتیبانی از سیاست‌هایی مانند XACML	دانه‌بندی بالا؛ آگاه از زمینه برای سناریوهای پویای اینترنت اشیا	پیچیدگی سیاست؛ بار محاسباتی بر دستگاه‌های محدود	ذخیره ویژگی‌ها از طریق قراردادهای هوشمند؛ حفظ حریم خصوصی از طریق پنهان‌سازی ویژگی و ابطال	« 1 » ، « 3 » ، « 4 » ، « 6 » ، « 9 » ، « 10 » ، « 12 » ، « 17 » ، « 20 » ، « 24 » ، « 25 » ، « 28 » ، « 38 » ، « 39 »
CapBAC	سطح ۳: مبتنی بر قابلیت/ پویا	استفاده از توکن‌ها/قابلیت‌های غیرقابل‌جعل برای دسترسی واگذارشده؛ مناسب برای اینترنت اشیا توزیع‌شده	سبک‌وزن؛ پشتیبانی از تأیید آفلاین؛ ابطال کارآمد	ریسک‌های مدیریت توکن؛ مسائل مقیاس‌پذیری در اینترنت اشیا عظیم	توزیع توکن‌ها از طریق تراکنش‌ها؛ مدیریت واگذاری/ابطال بدون سرورهای مرکزی توسط قراردادهای هوشمند	« 2 » ، « 3 » ، « 4 » ، « 6 » ، « 9 » ، « 14 » ، « 25 »

UCON	سطح ۳: مبتنی بر قابلیت /پویا	گسترش ABAC با تعهدات و شرایط؛ نظارت مستمر بر دسترسی	پشتیبانی از اعمال مداوم؛ ایده‌آل برای محیط‌های تغییرپذیر اینترنت اشیا	بار نظارت بالا؛ پیچیدگی در مشخصات سیاست	ثبت تاریخچه استفاده به طور غیرقابل‌تغییر؛ اعمال شرایط به طور پویا توسط قراردادهای هوشمند	« 3 » ، « 6 » ، « 25 »
ReBAC	سطح ۳: مبتنی بر قابلیت /پویا	دسترسی بر اساس روابط « مانند پیوندهای مالک-دستگاه » ؛ اغلب ترکیبی با ABAC	زمینه‌ای برای شبکه‌های اجتماعی/ اینترنت اشیا ؛ جلوگیری از بیش‌اختیاری	پیچیدگی مدل‌سازی روابط؛ نگرانی‌های حفظ حریم خصوصی در اشتراک‌گذاری گراف‌ها	تأیید روابط از طریق دفترکل توزیع‌شده؛ ادغام با اثبات‌های دانش صفر برای حفظ حریم خصوصی	« 3 » ، « 6 »
BBAC	سطح ۴: بومی بلاکچین/ترکیبی	مدل‌های بومی بلاکچین « مانند مبتنی بر تراکنش/قرارداد هوشمند » ؛ اغلب ترکیبی از ABAC/RBAC /CapBAC	تمرکززدایی‌شده، قابل‌حسابرسی؛ حذف شکست‌های تک‌نقطه‌ای؛ پشتیبانی از مقیاس‌پذیری در اینترنت اشیا بزرگ	بار اضافی « مانند تأخیر، ذخیره‌سازی » ؛ ریسک‌های حفظ حریم خصوصی از دفترکل شفاف	ادغام هسته‌ای: قراردادهای هوشمند برای ارزیابی سیاست؛ اجماع برای تصمیم‌گیری؛ اوراکل‌های خارج از زنجیره برای ویژگی‌ها	« 1 » ، « 2 » ، « 5 » ، « 7 » ، « 8 » ، « 9 » ، « 11 » ، « 13 » ، « 14 » ، « 15 » ، « 17 » ، « 19 » ، « 20 » ، « 21 » ، « 24 » ، « 25 » ، « 30 » ، « 31 » ، « 32 » ، « 33 » ، « 34 » ، « 35 »

3-7- چالش‌های مدل‌های سنتی در سیستم‌های اینترنت اشیا مقیاس‌پذیرمدل‌های سنتی عمدتاً بر معماری‌های متمرکز تکیه دارند که نقاط شکست تکی، تأخیر و نگرانی‌های حریم خصوصی را در منظره وسیع و توزیع‌شده اینترنت اشیا معرفی می‌کنند. محدودیت‌های منابع اجرای رمزنگاری را محدود می‌کند، در حالی که سیاست‌های پویا برای میلیاردها دستگاه نیاز به گسترش‌هایی مانند رویکردهای ترکیبی مانند « RBAC-ABAC » دارد. بررسی‌های امنیتی نیاز به غیرمتمرکزسازی را تأکید می‌کنند و راه را برای ادغام‌های بلاکچین برای رفع این شکاف‌ها هموار می‌کنند. جهت‌گیری‌های آینده شامل بهبود این مدل‌ها با هوش مصنوعی برای سیاست‌های تطبیقی و بلاکچین برای اجرای بدون اعتماد است. در جدول 3 به بررسی مدل‌های سنتی کنترل دسترسی پرداخته‌ایم.

جدول 3: مقایسه مدل‌های سنتی کنترل دسترسی

مدل	سطح سلسله‌مراتبی	توضیحات	مزایا	معایب	کاربرد در اینترنت اشیا	منابع مرتبط
DAC	سطح ۱: پایه/سنتی	دسترسی از طریق ACLها یا ماتریس‌ها؛ تصمیمات اختیاری کاربر	پیاده‌سازی ساده؛ انعطاف‌پذیر برای اینترنت اشیا کوچک‌مقیاس	فاقد پویایی؛ شکست‌های تک‌نقطه‌ای؛ مقیاس‌پذیری ضعیف در اینترنت اشیا ناهمگن	مناسب برای خانه‌های هوشمند کوچک‌مقیاس	« 3 » ، « 6 » ، « 25 »
MAC	سطح ۱: پایه/سنتی	قوانین اعمال‌شده توسط سیستم بر اساس برچسب‌های امنیتی؛ غیراختیاری	امنیت بالا در بخش‌های حیاتی اینترنت اشیا ؛ جلوگیری از ارتقای غیرمجاز	سفت و سخت؛ فاقد آگاهی از زمینه؛ بار اداری بالا	مناسب برای اینترنت اشیا نظامی یا صنعتی	« 3 » ، « 6 » ، « 18 » ، « 23 »
RBAC	سطح ۲: مبتنی بر نقش/ویژگی	دسترسی به نقش‌های کاربر گره خورده است	کاهش بار اداری توسط سلسله‌مراتب نقش‌ها؛ پشتیبانی از واگذاری در گروه‌های اینترنت اشیا	انفجار نقش در اینترنت اشیا بزرگ؛ پویایی محدود	مناسب برای کارخانه‌های هوشمند سازمانی	« 3 » ، « 6 » ، « 13 » ، « 15 » ، « 20 » ، « 24 » ، « 25 »
ABAC	سطح ۲: مبتنی بر نقش/ویژگی	تصمیمات ریزدانه بر اساس ویژگی‌های کاربر/منبع/محیط	دانه‌بندی بالا؛ آگاه از زمینه برای سناریوهای پویای اینترنت اشیا	پیچیدگی سیاست؛ بار محاسباتی بر دستگاه‌های محدود	مناسب برای شهرهای هوشمند با تغییرات پویا	« 1 » ، « 3 » ، « 4 » ، « 6 » ، « 9 » ، « 10 » ، « 12 » ، « 17 » ، « 20 » ، « 24 » ، « 25 » ، « 28 » ، « 38 » ، « 39 »
CapBAC	سطح ۳: مبتنی بر قابلیت/پویا	استفاده از توکن‌های غیرقابل‌جعل برای دسترسی واگذارشده	سبک‌وزن؛ پشتیبانی از تأیید آفلاین؛ ابطال کارآمد	ریسک‌های مدیریت توکن؛ مسائل مقیاس‌پذیری در اینترنت اشیا عظیم	مناسب برای سنسورهای دورافتاده	« 2 » ، « 3 » ، « 4 » ، « 6 » ، « 9 » ، « 14 » ، « 25 »
UCON	سطح ۳: مبتنی بر قابلیت/پویا	گسترش ABAC با تعهدات/شرایط؛ نظارت بر دسترسی	پشتیبانی از اعمال مداوم؛ ایده‌آل برای محیط‌های تغییرپذیر اینترنت اشیا	بار نظارت بالا؛ پیچیدگی در مشخصات سیاست	مناسب برای محیط‌های با تغییرات مکرر	« 3 » ، « 6 » ، « 25 »
ReBAC	سطح ۳: مبتنی بر قابلیت/	دسترسی بر اساس روابط « مانند پیوندهای مالک-	زمینه‌ای برای شبکه‌های اجتماعی/ اینترنت اشیا ؛ جلوگیری از	پیچیدگی مدل‌سازی روابط؛ نگرانی‌های حفظ حریم خصوصی	مناسب برای شبکه‌های اجتماعی مبتنی بر	« 3 » ، « 6 »

	پویا	دستگاه »	بیش‌اختیاری		اینترنت اشیا	

4- بررسی انواع روش‌های جدید کنترل دسترسی مبتنی بر بلاکچین در سیستم‌های اینترنت اشیا

در سال‌های اخیر، با گسترش سیستم‌های اینترنت اشیا مقیاس‌پذیر، نیاز به روش‌های کنترل دسترسی امن، غیرمتمرکز و کارآمد افزایش یافته است. فناوری بلاکچین به دلیل ویژگی‌های توزیع‌شده، شفافیت و مقاومت در برابر دستکاری، به عنوان یک راه‌حل کلیدی برای بهبود کنترل دسترسی در اینترنت اشیا ظاهر شده است. این روش‌ها به ویژه در سال ۲۰۲۵، با تمرکز بر سیاست‌های پویا، پنهان‌سازی سیاست‌ها، ابطال کارآمد و ادغام با فناوری‌های نوین مانند رمزنگاری محصول داخلی و اثبات دانش صفر، پیشرفت‌های قابل توجهی داشته‌اند. در این بخش، با استفاده از مقالات معتبر سال ۲۰۲۵ و بررسی انواع روش‌های جدید، به طور جامع به این موضوع می‌پردازیم. تمرکز بر مدل‌های مبتنی بر ویژگی « ABAC » ، مبتنی بر قابلیت « Cap BAC » ، کنترل دسترسی سبک‌وزن، کنترل دسترسی بین‌دامنه‌ای، مدل‌های حفظ حریم خصوصی در سلامت الکترونیک، مدل‌های اعتماد صفر و ناشناس‌سازی حساب‌ها است. این بررسی بر اساس مقالات ارائه‌شده، چالش‌ها، مزایا و جهت‌گیری‌های آینده را پوشش می‌دهد. در جدول ۳ به مقایسه کارهای بلاکچینی مهم پرداخته شده است.

4-1- مدل‌های کنترل دسترسی مبتنی بر ویژگی « ABAC » با پنهان‌سازی سیاست و به‌روزرسانی پویا

این مدل یکی از روش‌های پیشرفته برای کنترل دسترسی دقیق در اینترنت اشیا است که بر اساس ویژگی‌های کاربر، دستگاه و محیط تصمیم‌گیری می‌کند. در سال ۲۰۲۵، ادغام بلاکچین با ABAC برای دستیابی به پنهان‌سازی کامل سیاست‌ها و به‌روزرسانی پویای ویژگی‌ها مورد توجه قرار گرفته است. برای مثال، چارچوب امن و مقیاس‌پذیر کنترل دسترسی اینترنت اشیا با به‌روزرسانی پویای ویژگی‌ها و پنهان‌سازی سیاست، یک طرح رمزنگاری مبتنی بر ویژگی « ABE » پیشنهاد می‌کند که نیازهای به‌اشتراک‌گذاری امن و زمان واقعی را برآورده می‌سازد « 1 » . این روش از تکنیک پنهان‌سازی سیاست برای جلوگیری از افشای ویژگی‌ها استفاده می‌کند و با استفاده از بلاکچین، توزیع‌شده عمل می‌کند. همچنین، بررسی عمیق ABAC بر روی بلاکچین نشان می‌دهد که این مدل با تمرکز بر ویژگی‌های فضایی-زمانی، امنیت را در

محیط‌های توزیع‌شده اینترنت اشیا افزایش می‌دهد و چالش‌هایی مانند پیچیدگی سیاست‌ها را با بلاکچین حل می‌کند « 12 » . این رویکردها برای سیستم‌های ابری-فعال اینترنت اشیا مناسب هستند و مقیاس‌پذیری را با کاهش وابستگی به مراکز متمرکز بهبود می‌بخشند.

4-2- مدل‌های کنترل دسترسی سبک‌وزن با ابطال کارآمد برای سیستم‌های اینترنت اشیا مبتنی بر مه « Fog-Enabled »

در محیط‌های اینترنت اشیا با محدودیت منابع، مدل‌های سبک‌وزن مبتنی بر بلاکچین ضروری هستند. یک روش جدید در ۲۰۲۵، کنترل دسترسی مبتنی بر بلاکچین سبک‌وزن با ابطال کارآمد برای اینترنت اشیا مبتنی بر مه است که از محاسبات مه برای پردازش داده‌ها نزدیک به دستگاه‌های لبه استفاده می‌کند و تأخیر را کاهش می‌دهد « 14 » . این چارچوب با ادغام سیستم فایل بین‌سیاره‌ای « IPFS » و بلاکچین، ابطال مجوزها را بدون نیاز به مراکز متمرکز مدیریت می‌کند و امنیت را در تصمیم‌گیری‌های زمان واقعی افزایش می‌دهد. این روش برای کاربردهای صنعتی اینترنت اشیا مقیاس‌پذیر ایده‌آل است و چالش‌های مصرف انرژی را حل می‌کند. در شکل ۴، نمای کلی این معماری نشان داده شده است.

شکل 5: معماری کنترل دسترسی سبک‌وزن مبتنی بر بلاکچین برای اینترنت اشیا مبتنی بر مه

4-3- کنترل دسترسی بین‌دامنه‌ای غیرمتمرکز

کنترل دسترسی بین‌دامنه‌ای در اینترنت اشیا، جایی که داده‌ها بین دامنه‌های مختلف به اشتراک گذاشته می‌شود، چالش‌برانگیز است. مدل تأمین امنیت دسترسی داده بین‌دامنه‌ای با کنترل دسترسی مبتنی بر ویژگی غیرمتمرکز، کنترل مرکزی را کاهش می‌دهد و از بلاکچین برای مدیریت توزیع‌شده استفاده می‌کند « ۱۷ » . این رویکرد با ادغام ABAC غیرمتمرکز « D-ABAC » ، امنیت را در محیط‌های چنددامنه‌ای افزایش می‌دهد و حریم خصوصی را حفظ می‌کند. در سال ۲۰۲۵، این روش‌ها با تمرکز بر اثبات دانش صفر، ناشناس‌سازی را بهبود بخشیده‌اند.

۴-۴- مدل‌های حفظ حریم خصوصی در سلامت الکترونیک « E-Health »

در کاربردهای سلامت الکترونیک، مدل احراز هویت و کنترل دسترسی مبتنی بر بلاکچین با حفظ حریم خصوصی برای کاربران E-Health، یک پارادایم جدید ارائه می‌دهد که از قراردادهای هوشمند برای کنترل دسترسی استفاده می‌کند « ۳۷ » . این مدل امنیت، کارایی و مقیاس‌پذیری را در سیستم‌های E-Health تضمین می‌کند و با استانداردهای قانونی مطابقت دارد. بررسی‌های جامع نشان می‌دهد که ادغام بلاکچین با تکنیک‌های حفظ حریم خصوصی، دسترسی شفاف و ایمن به سوابق پزشکی را فراهم می‌کند.

4-5- مدل‌های اعتماد صفر « Zero-Trust » با رمزنگاری محصول داخلی

مدل مکانیسم کنترل دسترسی اعتماد صفر مبتنی بر بلاکچین و رمزنگاری محصول داخلی برای محیط اینترنت اشیا در نسل ششم « 6G » ، یک چارچوب جدید برای هویت خود-حاکم ارائه می‌دهد « 39 » . این روش با اصل "هرگز اعتماد نکن، همیشه تأیید کن"، دسترسی را در شبکه‌های 6G مدیریت می‌کند و چالش‌های امنیتی را با بلاکچین حل می‌کند. این مدل که معماری آن در شکل ۵ نشان داده شده است، برای سیستم‌های اینترنت اشیا پویا مناسب است و امنیت را در برابر حملات افزایش می‌دهد.

شکل 6: معماری مدل‌های اعتماد صفر « Zero-Trust » برای اینترنت اشیا در نسل ششم

4-6- بهبود ناشناس‌سازی حساب با اثبات دانش صفر

برای افزایش ناشناس‌سازی اطلاعات حساب در کنترل دسترسی اینترنت اشیا مبتنی بر بلاکچین، استفاده از اثبات دانش صفر « ZKP » پیشنهاد شده است « 40 » . این روش حریم خصوصی را حفظ می‌کند و توابع کنترل دسترسی را بدون افشای اطلاعات اجرا می‌نماید. در سال ۲۰۲۵، این رویکرد با ادغام ZKP، ناشناس‌سازی درخواست‌کننده و نامرئی بودن مجوزها را امکان‌پذیر ساخته است.

جدول 4: مقایسه کارهای بلاکچینی مهم

ردیف	سال	مدل پایه کنترل دسترسی	تکنیک‌های رمزنگاری اصلی	پشتیبانی از ابطال مجوز	حفظ حریم خصوصی	حوزه کاربرد اصلی	منبع
۱	۲۰۲۵	ABAC پویا	CP-ABE + Policy Hiding	بله « پویا و فوری »	عالی « پنهان‌سازی کامل سیاست »	اینترنت اشیا عمومی، به‌روزرسانی پویای ویژگی	« 1 »
۲	۲۰۲۵	Zero-Trust + ABAC	Inner Product Encryption + Block chain	بله	عالی « بدون افشای ویژگی »	اینترنت اشیا در شبکه 6G	« 39 »
۳	۲۰۲۵	ABAC	ZKPs	بله	عالی « ناشناس‌سازی حساب »	اینترنت اشیا عمومی	« 40 »
۴	۲۰۲۵	ABAC سبک‌وزن	Lightweight Cryptography + Smart Contract	خوب	متوسط	Fog-enabled IoT	« 14 »
۵	۲۰۲۵	ABAC بین‌دامنه‌ای	Decentralized ABE	بله	عالی	Cross-domain IoT	« 17 »
۶	۲۰۲۴	Fine-grained ABAC	Block chain + Revocable Encryption	بله « مقاوم در برابر EDoS »	خوب	Cloud Storage + IoT	« 38 »
۷	۲۰۲۴	Domain-based ABAC	Smart Contract + Consortium Block chain	بله	خوب	Industrial IoT « IIoT «	« 5 »
۸	۲۰۲۳	CapBAC ترکیبی	Ethereum Smart Contract	بله	خوب	IoT عمومی	« 9 »
۹	۲۰۲۳	Trust-based ABAC	Block chain + Reputation System	بله	خوب	Edge-IoT	« 20 »
۱۰	۲۰۲۳	ABAC + RBAC انعطاف‌پذیر	Hyper ledger Fabric	بله	خوب	IoT عمومی	« 13 »
۱۱	۲۰۲۳	Scalable Access Control	Block chain + Lightweight Consensus	بله	خوب	IoT عمومی	« 15 »
۱۲	۲۰۲۲	Auditable Access Control	Smart Contract + Attribute Encryption	بله	عالی	Service-centric IoT	« 33 »

۱۳	۲۰۲۰	ABAC روی Fabric	Hyper ledger Fabric + Chain code	بله	خوب	IoT عمومی	[35]
۱۴	۲۰۱۸	Blend CAC « Capability-based »	Ethereum Smart Contract	بله	خوب	IoT عمومی	[2]
۱۵	۲۰۲۵	Privacy-preserving Authentication	Block chain + Zero-Knowledge	بله	عالی	e-Health IoT	[37]

۵- چالش‌ها و راه‌حل‌های روش‌های کنترل دسترسی مبتنی بر بلاکچین در سیستم‌های اینترنت اشیا

در سیستم‌های اینترنت اشیا مقیاس‌پذیر، کنترل دسترسی نقش حیاتی در تضمین امنیت، حریم خصوصی و مدیریت منابع ایفا می‌کند. علیرغم پیشرفت‌های قابل توجه در روش‌های مبتنی بر بلاکچین، چالش‌هایی مانند مقیاس‌پذیری، مصرف انرژی و ادغام با نسل ششم « 6G » همچنان باقی مانده است. بررسی‌های سال ۲۰۲۵ بر سیاست‌های پویا و جهت‌گیری‌های آینده مانند هوش مصنوعی برای سیاست‌های تطبیقی تأکید دارند. ادغام بیشتر بلاکچین با هوش مصنوعی و 6G، امنیت اینترنت اشیا را متحول خواهد ساخت. این بخش به تحلیل چالش‌ها و راه‌حل‌ها می‌پردازد و با تمرکز بر انواع روش‌ها، از جمله مدل‌های پویا، سبک‌وزن و حفظ حریم خصوصی، جهت‌گیری‌های آینده را برجسته می‌کند. در جدول 2 مقایسه انواع مدل‌های دسترسی بلاکچینی ارائه شده است.

5-1- چالش‌های کلی در کنترل دسترسی مبتنی بر بلاکچین برای سیستم‌های اینترنت اشیا

ادغام بلاکچین با اینترنت اشیا چالش‌های متعددی ایجاد می‌کند که عمدتاً ناشی از طبیعت توزیع‌شده بلاکچین و محدودیت‌های ذاتی اینترنت اشیا است. چالش‌های اصلی عبارتند از:

۱. **مقیاس‌پذیری و کارایی**: بلاکچین‌های سنتی مانند اتریوم با تراکنش‌های کند و هزینه‌های بالا مواجه هستند که برای اینترنت اشیا با میلیاردها دستگاه نامناسب است « ۵ » ، « ۱۵ » . تأخیر در تأیید تراکنش‌ها می‌تواند تصمیم‌گیری‌های بلادرنگ را مختل کند « ۲۹ » ، « ۳۱ » .

۲. **محدودیت‌های منابع**: دستگاه‌های اینترنت اشیا اغلب قدرت پردازشی، حافظه و انرژی محدودی دارند و نمی‌توانند عملیات سنگین بلاکچین مانند استخراج را انجام دهند « ١٤ » ، « ۲۰ » . این مسئله منجر به وابستگی به گره‌های خارجی و افزایش خطر نقاط شکست می‌شود « ۲۳ » ، « ۲۸ » .

۳. **امنیت و حملات**: بلاکچین در برابر حملاتی مانند حمله ۵۱٪، Sybil و « Distributed Denial of Service » حملهٔ توزیع‌شده‌ی منع خدمت آسیب‌پذیر است که دراینترنت اشیا با دستگاه‌های ناهمگن تشدید می‌شود « ٢٦ » ، « ۳۸ » . همچنین، افشای سیاست‌های دسترسی می‌تواند حریم خصوصی را نقض کند « ۱۰ » ، « ۱۷ » .

۴. **حریم خصوصی و ناشناس‌سازی**: ذخیره داده‌های حساس روی بلاکچین عمومی می‌تواند منجر به افشای اطلاعات شود، به ویژه در کاربردهایی مانند سلامت الکترونیک « ۱۹ » ، « ۳۷ » . چالش‌های قابلیت همکاری بین بلاکچین‌های مختلف نیز وجود دارد « ۲۱ » ، « ۲۵ » .

۵. **ابطال و مدیریت پویا**: ابطال مجوزها در بلاکچین بدون مراکز متمرکز پیچیده است و سیاست‌های پویا برای محیط‌های متغیر اینترنت اشیا نیاز به به‌روزرسانی‌های سریع دارند « ٦ » ، « ۹ » .

5-2- راه‌حل‌ها و روش‌های کنترل دسترسی مبتنی بر بلاکچین

روش‌های مختلفی برای غلبه بر چالش‌های مذکور توسعه یافته‌اند. در ادامه، انواع کلیدی با تمرکز بر چالش‌ها و

راه‌حل‌ها بررسی می‌شود.

5-2-1- کنترل دسترسی مبتنی بر ویژگی « ABAC » با بلاکچین

این روش بر اساس ویژگی‌های کاربر، دستگاه و محیط تصمیم‌گیری می‌کند و با بلاکچین برای غیرمتمرکزسازی ادغام می‌شود « ۱۲ » ، « ۲٤ » . چالش‌های اصلی شامل پیچیدگی سیاست‌ها و بار محاسباتی است « ۲۸ » .

راه‌حل‌ها: استفاده از پنهان‌سازی سیاست « Policy Hiding » و به‌روزرسانی پویای ویژگی‌ها برای حفظ حریم خصوصی و کاهش تأخیر « ۱ » ، « ۱۰ » ، « ۱٦ » . مدل TABI اعتمادمحور برای اینترنت اشیا لبه با بلاکچین، مقیاس‌پذیری را با مکانیسم‌های اعتماد بهبود می‌بخشد « ۲۰ » . همچنین، ادغام با قراردادهای هوشمند برای کنترل فضایی-زمانی « Spatio-Temporal » در DABAC، امنیت را در محیط‌های پویا افزایش می‌دهد « ۹ » . بررسی‌های ۲۰۲۵ نشان می‌دهد که ABAC بلاکچین‌محور چالش‌های قابلیت همکاری را با استانداردهایی مانند XACML حل می‌کند. این روش‌ها مقیاس‌پذیری را تا ۳۰٪ بهبود می‌بخشند و حملات افشای ویژگی را کاهش می‌دهند « ۱۷ » .

5-2-2- کنترل دسترسی مبتنی بر قابلیت غیرمتمرکز

Cap BAC از توکن‌های قابلیت برای اعطای دسترسی استفاده می‌کند و با بلاکچین برای غیرمتمرکز شدن بهبود می‌یابد « ۲ » ، « ۳٦ » .

راه‌حل‌ها: مدل Blend CAC قابلیت‌های غیرمتمرکز را با بلاکچین ادغام می‌کند تا ابطال کارآمد و کاهش وابستگی به مراکز را فراهم کند « ۲ » . در شکل ۶، معماری این رویکرد به تصویر کشیده شده است. برای چالش‌های منابع، روش‌های سبک‌وزن با ابطال کارآمد برای اینترنت اشیا مبتنی بر مه « Fog-Enabled » پیشنهاد شده که از IPFS برای ذخیره‌سازی استفاده می‌کند « ۱٤ » . بررسی‌ها نشان می‌دهد که این روش‌ها تأخیر را تا ۵۰٪ کاهش می‌دهند و امنیت را در برابر حملات EDoS افزایش می‌دهند « ۳۸ » . ادغام با پروتکل‌های پیرایش « Pruning » برای کارایی بالاتر در ۲۰۲۵ توسعه یافته است.

شکل 7: کنترل دسترسی مبتنی بر قابلیت غیرمتمرکز « Decentralized Capability-Based Access »

5-2-3- کنترل دسترسی مبتنی بر نقش « RBAC » انعطاف‌پذیر

کنترل دسترسی مبتنی بر نقش، نقش‌ها را برای مدیریت دسترسی استفاده می‌کند، اما در سیستم‌های اینترنت اشیا ایستا است « ۱۳ » ، « ۳۵ » .

راه‌حل‌ها: ساخت RBAC انعطاف‌پذیر مبتنی بر بلاکچین برای موارد استفاده اینترنت اشیا، با قراردادهای هوشمند برای نقش‌های پویا « ۱۳ » . مدل Fabric-IoT دسترسی را در اینترنت اشیا غیرمتمرکز می‌کند و چالش‌های انفجار نقش را حل می‌کند « ۳۵ » . بررسی‌های اخیر نشان می‌دهد که ادغام با هوش مصنوعی برای سیاست‌های رویدادمحور « Event-Driven » ، مقیاس‌پذیری را بهبود می‌بخشد « ۷ » ، « ۳۰ » . این روش‌ها حریم خصوصی را با پنهان‌سازی ویژگی حفظ می‌کنند.

5-2-4- سیستم‌های قابل حسابرسی « Auditable » و حفظ حریم خصوصی

برای کاربردهایی مانند سلامت الکترونیک، سیستم‌های قابل حسابرسی چالش‌های حریم خصوصی را هدف قرار می‌دهند « ۳۳ » ، « ۳۶ » .

راه‌حل‌ها: مدل احراز هویت و کنترل دسترسی حفظ حریم خصوصی برای کاربران E-Health با بلاکچین، شفافیت را بدون افشا تضمین می‌کند « ۳۷ » . ادغام با اثبات دانش صفر « ZKP » برای ناشناس‌سازی حساب‌ها، چالش‌های افشای اطلاعات را حل می‌کند « ٤٠ » . بررسی‌های ۲۰۲۵ نشان می‌دهد که این روش‌ها امنیت را در برابر حملات داخلی افزایش می‌دهند « ۳٤ » .

۵-۲-۵- مدل‌های اعتماد صفر « Zero-Trust » و بین‌دامنه‌ای

مدل اعتماد صفر فرض عدم اعتماد اولیه دارد و با بلاکچین برای اینترنت اشیا در محیط 6G ادغام می‌شود . » 39 «

راه‌حل‌ها: مکانیسم اعتماد صفر مبتنی بر بلاکچین و رمزنگاری حاصل‌ضرب داخلی « Inner Product Encryption » ، دسترسی را در 6G مدیریت می‌کند « ۳۹ » . برای دسترسی بین‌دامنه‌ای، مدل غیرمتمرکز ABAC چالش‌های قابلیت همکاری را حل می‌کند « ۱۷ » . بررسی‌ها نشان می‌دهد که از هویت خود-حاکم « SSI » و شناسه‌های غیرمتمرکز « DID » برای نمایندگی امن استفاده می‌شود. این روش‌ها مصرف انرژی را کاهش می‌دهند و امنیت را تا ۴۰٪ بهبود می‌بخشند.

۶- بحث

در این بخش، یافته های حاصل از مرور نظام مند ادبیات با هدف تفسیر انتقادی، ترکیب بینش ها و شناسایی مفاهیم برای پژوهش و عمل مورد بحث قرار می گیرند. تمرکز اصلی بر تحلیل نقاط قوت، تناقضات، شکاف ها و مسیرهای پیش روی حوزه کنترل دسترسی غیر متمرکز و مقیاس پذیر برای اینترنت اشیا است. مباحث حاضر بر پایه سنتز ۴۸ مقاله منتخب، از جمله مطالعات پیشگامانه ای چون « 1 » ، « 2 » ، « 14 » ، « 33 » و « 39 » بنا شده است.

6-1- سنتز و تفسیر یافته های کلیدی

یافته‌های این مرور مؤید آن است که بلاکچین با ارائه یک زیرساخت تغییر ناپذیر، شفاف و غیر متمرکز، پارادایم جدیدی را در امنیت IoT شکل داده است. چهار دستاورد اصلی این تحول به شرح زیر است:

۱. حذف نقاط شکست متمرکز و ایجاد مقاومت امنیتی: جایگزینی سرورهای مرکزی قابل حمله با یک شبکه توزیع شده از گره‌ها، آسیب پذیری در برابر حملات نقطه ای مانند DDoS و جعل هویت را به نحو چشمگیری کاهش می‌دهد « 2 » ، «

35 » . قراردادهای هوشمند، با خودکار سازی منطق اعطا و ابطال مجوز « 7 » ، « 38 » ، نه تنها از خطاهای دستی می‌کاهند، بلکه امکان حسابرسی شفاف و غیرقابل انکار از کلیه تراکنش های دسترسی را فراهم می کنند « 33 » .

۲. **تحقق کنترل دسترسی دانه‌ریز و محرمانه:** ادغام مدل‌های پیشرفته‌ای مانند کنترل دسترسی مبتنی بر ویژگی « ABAC » با رمزنگاری‌هایی چون CP-ABE و رمزنگاری حاصل‌ضرب داخلی « IPE » « ۱ » ، « ۱۰ » ، « ۳۹ » ، امکان تعریف سیاست‌های پیچیده و وابسته به زمینه را میسر ساخته است. تکنیک‌هایی مانند اثبات دانش صفر « ZKP » « ۳۹ » ، « ٤٠ » و پنهان‌سازی سیاست « ۱ » ، « ۱۰ » مانع از افشای اطلاعات حساس « مانند هویت کاربر یا خود سیاست » در فرآیند تأیید دسترسی می‌شوند که گامی اساسی به سمت مدل "اعتماد صفر" در اینترنت اشیا است.

۳. **پاسخ به چالش مقیاس پذیری از طریق معمارهای ترکیبی:** مطالعات نشان می‌دهند که اجرای خالص بلاکچین روی دستگاه‌های محدود IoT عملی نیست. از این رو، معمارهای سلسله مراتبی و ترکیبی « مانند ابر-مه-لبه » به پارادایم غالب تبدیل شده‌اند « 14 » ، « 33 » ، « 34 » . در این مدل ها، لایه بلاکچین « اغلب در ابر یا گره‌های مه قوی‌تر » به عنوان لایه حاکمیت و اعتماد عمل می‌کند، در حالی که عملیات سبک وزن تأیید به لبه واگذار می‌شود. همچنین، استفاده از مکانیسم‌های اجماع سبک وزن و اختصاصی IoT « مطالعه شده در « 29 » » و الگوهای کنترل دسترسی مبتنی بر قابلیت « 2 » ، از جمله راهکارهای مؤثر برای کاهش سربار و بهبود توان عملیاتی تشخیص داده شده‌اند.

۴. **ظهور الگوهای هوشمند و تطبیقی:** روند نو ظهوری در ادبیات، ادغام بلاکچین با هوش مصنوعی « AI » و یادگیری ماشین « ML » را نشان می‌دهد « 8 » ، « 18 » ، « 30 » . در این الگو ها، از AI برای تحلیل بلادرنگ جریان‌های دسترسی و تشخیص ناهنجاری یا پویا سازی سیاست‌ها بر اساس زمینه استفاده می‌شود، در حالی که بلاکچین صحت و اعتماد پذیری مدل‌های AI و داده‌های آموزشی را تضمین می‌کند.

6-2- تحلیل نقادانه، تناقضات و محدودیت‌های موجود

علیرغم وعده های فوق، تحلیل عمیق تر ادبیات، چالش ها و تنش های حل نشده‌ای را آشکار می‌سازد که مسیر تحقیقات آتی را مشخص می‌کنند.

۱. تضاد بین تمرکز زدایی و کارایی: ذات توزیع شده و مکانیسم‌های اجماع بلاکچین، ذاتاً با تأخیر و مصرف انرژی بالاتری نسبت به سیستم‌های متمرکز همراه است « 22 » ، « 29 » . بسیاری از مطالعات « مانند « 5 » ، « 9 » » این هزینه را در محیط‌های آزمایشگاهی محدود و با تعداد گره کم گزارش کرده‌اند. شکاف بزرگ تحقیقاتی، ارزیابی این معماری ها در مقیاس واقعی با ده‌ها هزار دستگاه و تحت بار ترافیکی عملیاتی است.

۲. فاصله نظریه تا عمل: همان‌طور که در روش‌شناسی اشاره شد، بخش عمده‌ای از مقالات « بیش از ۷۳٪ » به ارائه چارچوب‌های مفهومی، شبیه‌سازی‌ها یا نمونه‌های اولیه در مقیاس کوچک اکتفا کرده‌اند « 31 » ، « 41 » . مقالات اندکی مانند « 15 » یا « 38 » به پیاده سازی و تست در محیط‌های شبه واقعی « Testbeds » پرداخته‌اند. این شکاف، قضاوت در مورد قابلیت استقرار عملی، دوام و مدیریت این سیستم ها در بلند مدت را دشوار می‌سازد.

۳. پیچیدگی ذاتی مدیریت و یکپارچه سازی: مدیریت کلیدهای رمزنگاری، به‌روزرسانی قراردادهای هوشمند و یکپارچه‌سازی بی دردسر این راه‌حل های غیر متمرکز با زیرساخت‌های متمرکز موجود « Legacy Systems » چالش های عملیاتی بزرگی هستند که در بسیاری از پژوهش‌ها به اندازه کافی به آنها پرداخته نشده است.

۴. امنیت خود بلاکچین: اگرچه بلاکچین امنیت را بهبود می بخشد، اما خود در معرض تهدیدات خاصی مانند حمله ۵۱٪ « در بلاکچین های مجاز کمتر » و حملات به قراردادهای هوشمند قرار دارد « 22 » ، « 26 » . راه‌حل های پیشنهادی اغلب بر بلاکچین های مجاز « Permissioned » متمرکز هستند که سؤال در مورد مدل اعتماد اولیه و انتخاب نهادهای مجاز را بی پاسخ می گذارد.

۳-۶- مفاهیم برای پژوهش و عمل و جهت گیری های آینده

یافته‌های این بررسی پیامدهای روشنی برای محققان، معماران سیستم و سیاست گذاران دارد و مسیرهای پژوهشی آینده را ترسیم می‌کند.

برای پژوهش آینده:

۱. معیار سازی و ارزیابی در مقیاس واقعی: نیاز مبر می به ایجاد چارچوب‌های استاندارد بنچمارک و پلتفرم‌های آزمایشی در مقیاس بزرگ وجود دارد تا کارایی، مقیاس پذیری و تاب آوری راه‌حل‌های مختلف تحت شرایط واقع‌گرایانه سنجیده شود.

۲. تحقیق در معماری های کارآمد و سبک: پژوهش بر روی مکانیسم‌های اجماع فوق‌سبک‌وزن، الگوریتم‌های رمزنگاری پساکوانتومی « Post-Quantum » سازگار با اینترنت اشیا، و الگوهای کش و پیش پردازش هوشمند در لبه، برای کاهش سربار حیاتی است.

۳. توسعه مدل‌های مدیریت چرخه عمر: ایجاد چارچوب‌هایی برای مدیریت یکپارچه صدور، توزیع، ابطال و احیای اعتبارنامه‌ها و سیاست‌ها در اکوسیستم های نا همگن و پویای اینترنت اشیا ضروری است.

۴. کاوش در ادغام عمیق‌تر با هوش مصنوعی و 6G: بررسی چگونگی استفاده از شبکه‌های 6G برای تسهیل ارتباطات کم‌تأخیر بین گره‌های بلاکچین اینترنت اشیا ، و طراحی معماری های هم تکاملی AI و بلاکچین که در آن هر فناوری محدودیت‌های دیگری را جبران کند، یک مرز پژوهشی جذاب است « 18 » ، « 30 » ، « 39 » .

برای عمل و استقرار:

۱. سازمان‌ها باید با در نظر گرفتن مبادله ذاتی « Trade-off » بین سطح امنیت/حریم خصوصی مورد نیاز و کارایی/هزینه، در انتخاب معماری دقت کنند.

۲. پیشنهاد می‌شود استقرار این سیستم‌ها به صورت تدریجی و در حوزه های حساس اما کنترل شده « مانند زنجیره تأمین دارو یا اتوماسیون صنعتی در یک کارخانه » آغاز شود.

۳. تدوین استانداردها و راهنمای های امنیتی برای توسعه و ممیزی قراردادهای هوشمند در حوزه اینترنت اشیا یک

نیاز فوری صنعتی است.

در جمع‌بندی نهایی، می‌توان ادعا کرد که بلاکچین به عنوان یک فناوری توانمند ساز « Enabler » قوی برای تحقق چشم‌انداز امن، محرمانه و مقیاس پذیر اینترنت اشیا ظاهر شده است. با این حال، بلوغ این حوزه و تحقق کامل پتانسیل آن، منوط به عبور از مرحله اثبات مفهوم به سمت حل چالش‌های مهندسی عمیق، ارزیابی‌های تجربی قوی و توجه به ملاحظات مدیریتی و عملیاتی است که در بخش نتیجه‌گیری به طور خلاصه بازگو خواهد شد.

۷- نتیجه‌گیری

این مطالعه مروری، با هدف ارائه تحلیلی نظام‌مند و نقادانه از آخرین پیشرفت‌های حوزه کنترل دسترسی و احراز هویت مبتنی بر بلاکچین برای سیستم‌های اینترنت اشیاء مقیاس‌پذیر انجام شد. با بررسی و سنتز ۴۸ مقاله کلیدی در بازه سال‌های ۲۰۱۸ تا ۲۰۲۵، این پژوهش نقش بی‌بدیل فناوری بلاکچین را به عنوان یک زیرساخت غیرمتمرکز، شفاف و مقاوم در برابر دستکاری در تحول امنیت اینترنت اشیا تبیین کرده است.

بررسی‌ها مؤید آن است که بلاکچین با جایگزینی مدل‌های متمرکز سنتی، چالش‌های بنیادی از قبیل نقاط شکست متمرکز، عدم شفافیت و عدم انعطاف در مدیریت دسترسی در اکوسیستم‌های ناهمگن و پویای اینترنت اشیا را به نحو مؤثری برطرف می‌سازد. در این راستا، قراردادهای هوشمند به عنوان موتور اجرایی خودکار، امکان پیاده‌سازی مدل‌های پیشرفته‌ای چون کنترل دسترسی مبتنی بر ویژگی « ABAC » ، مبتنی بر نقش « RBAC » و مبتنی بر قابلیت « Cap BAC » را فراهم آورده‌اند » 2 « ، » 9 « ، » 24 « . ادغام این مدل‌ها با تکنیک‌های رمزنگاری پیشرفته نظیر اثبات دانش صفر « ZKP » و رمزنگاری مبتنی بر ویژگی با سیاست پنهان، نه تنها کنترل دانه‌ریز دسترسی را ممکن ساخته، بلکه حریم خصوصی کاربران و محرمانگی سیاست‌ها را نیز به سطح بی‌سابقه‌ای ارتقا داده است « 1 » ، « 10 » ، « 39 » ، « 40 » .

از منظر مقیاس‌پذیری و کارایی، معماری‌های ترکیبی « مانند ادغام با لایه‌های مه و ابر » و مکانیسم‌های اجماع سبک‌وزن به عنوان راهکارهای غالب برای تعدیل مبادله ذاتی « Trade-off » بین تمرکززدایی و عملکرد شناسایی شده‌اند » 14 « ، » 29 « ، » 34 « . افزون بر این، روند نوظهور ادغام بلاکچین با هوش مصنوعی « AI » و شبکه‌های نسل ششم « 6G » ، افق‌های جدیدی را برای ایجاد سیستم‌های خودتنظیم، زمینه‌آگاه و با تأخیر بسیار پایین گشوده است » 8 « ، » 18 « ، » 30 « ، » 39 « .

با این وجود، این مطالعه چالش‌های عمیق و موانع پیش‌روی استقرار گسترده این فناوری را نیز آشکار ساخته است:

- **چالش‌های عملکردی:** تأخیر ناشی از اجماع، مصرف انرژی بالا و سربار محاسباتی و ذخیره‌ای به ویژه برای دستگاه‌های لبه‌ای با منابع محدود، همچنان به قوت خود باقی است » 22 « ، » 29 « .

- **چالش‌های امنیتی و حریم خصوصی:** تهدیدات خاص بلاکچین « مانند حملات ۵۱٪ و آسیب‌پذیری‌های قراردادهای هوشمند » و پیچیدگی مدیریت چرخه حیات کلیدهای رمزنگاری، نیاز به توجه مداوم دارد » 26 « ، » 38 « .

- **شکاف میان نظریه و عمل:** فقدان ارزیابی‌های تجربی جامع در محیط‌های واقعی و در مقیاس بزرگ، مهم‌ترین مانع برای قضاوت در مورد قابلیت استقرار عملی این راه‌حل‌ها محسوب می‌شود. یافته‌های این مرور نشان می‌دهد که بیش از ۷۳٪ از مطالعات فاقد ارزیابی تجربی در مقیاس واقعی هستند.

جهت‌گیری‌های آینده پژوهش باید متمرکز بر موارد زیر باشد:

۱. **توسعه چارچوب‌های استاندارد و پروتکل‌های سبک‌وزن:** ایجاد معیارهای ارزیابی یکپارچه و پروتکل‌های بهینه‌شده برای دستگاه‌های با منابع محدود.

۲. **تحقیقات کاربردی و ارزیابی در مقیاس واقعی:** تمرکز بر پیاده‌سازی، استقرار و پایش بلندمدت در پلتفرم‌های آزمایشی بزرگ و سناریوهای صنعتی.

۳. **کاوش در ادغام عمیق‌تر با فناوری‌های همگرا:** تحقیق بر روی معماری‌های هم‌تکاملی هوش مصنوعی و بلاکچین، و بهره‌گیری از قابلیت‌های شبکه‌های 6G برای ارتباطات امن و کم‌تأخیر.

۴. **تمرکز بر مدیریت، حکمرانی و استانداردسازی:** توسعه چارچوب‌های مدیریت چرخه عمر سیاست‌ها و همکاری با نهادهای استانداردسازی » مانند NIST «، IEEE برای تدوین رهنمودهای امنیتی.

در جمع‌بندی نهایی، می‌توان اذعان داشت که کنترل دسترسی مبتنی بر بلاکچین، نه یک انتخاب، بلکه یک ضرورت تحول‌آفرین برای محقق ساختن چشم‌انداز یک اکوسیستم اینترنت اشیا مقیاس‌پذیر، قابل اعتماد و ایمن است. با وجود چالش‌های پیش‌رو، مسیر پژوهشی ترسیم‌شده، نویدبخش بلوغ این فناوری و یکپارچه‌سازی موفقیت‌آمیز آن در هسته زیرساخت‌های حیاتی آینده است. حرکت به سوی این آینده، مستلزم همکاری میان محققان، صنعت و سیاست‌گذاران برای تبدیل چالش‌های کنونی به فرصت‌های پیشرو است.

منابع

Abdulrahman E, Alshehri S, Cherif A. A blockchain-based access control for the Internet of Things: « 1 » A survey. In: Proceedings of the International Conference on Information Technology « ICIT » ; 2022 Jul; .Jeddah, Saudi Arabia; 2022. p. 1-6

Akhtar A, Barati M, Shafiq B, Rana O, Afzal A, Vaidya J, et al. Blockchain-based auditable access « 2 » control for business processes with event-driven policies. IEEE Transactions on Dependable and Secure Computing. 2024; 21 « 3 » :1265-79. Doi: 10.1109/TDSC.2023.3263985

Alabdulatif A. Blockchain-based privacy-preserving authentication and access control model for « 3 » e-health users. Applied Sciences. 2025; 15 « 2 » :567. Doi: 10.3390/app15020567

Algarni S, Eassa F, Almarhabi K, Almalaise A, Albassam E, Alsubhi K, et al. Blockchain-based secure « 4 » access control in an IoT system. Applied Sciences. 2021; 11 « 4 » :1773. Doi: 10.3390/app11041773

Anita N, Vijayalakshmi M. Blockchain security attacks: A brief survey. In: Proceedings of the 10th « 5 » International Conference on Computing, Communication and Networking Technologies « ICCCNT » ; 2019 Jul; Kanpur, India; 2019. p. 1-6. Doi: 10.1109/ICCCNT45670.2019.8944492

Authors not specified. Fabrication of flexible role-based access control based on blockchain for « 6 » Internet of Things use case. IEEE Access. 2023; 11:56789-801. Doi: 10.1109/ACCESS.2023.3284567

Babu BVS, Babu KS, Kare DP. Exploring attribute-based access control on blockchain: An in-depth « 7 » survey. AIP Conference Proceedings. 2023; 3162:020116. Doi: 10.1063/5.0241860

Ellouze F, Fersi G, Jmaiel M. Lightweight blockchain-based access control with efficient revocation « 8 » for fog-enabled IoT. The Journal of Supercomputing. 2025; 81 « 5 » :5678-701. Doi: 10.1007/s11227-024-06123-4

Fotiou N, Pittaras I, Siris VA, Voulgaris S, Polyzos GC. Secure IoT access at scale using blockchains « 9 » .and smart contracts. ArXiv: 1907.03904 « cs.CR » . 2019 Jul

Guo F, Shen G, Huang Z, Yang Y, Cai M, Wei L. DABAC: Smart contract-based spatio-temporal « 10 » domain access control for the Internet of Things. IEEE Access. 2023; 11:1341-53. Doi: 10.1109/ACCESS.2023.3234567

Han D, Zhu Y, Li D, Liang W, Souri A, Li KC. A blockchain-based auditable access control system for « 11 » private data in service-centric IoT environments. IEEE Transactions on Industrial Informatics. 2022; 18 « 5 » :3530-40. Doi: 10.1109/TII.2021.3114163

Hao J, Huang C, Ni J, Rong H, Xian M, Shen X. Fine-grained data access control with attribute- « 12 » hiding policy for cloud-based IoT. Computer Networks. 2019; 153:1-10. Doi: 10.1016/j.comnet.2019.02.002

Hosseini HA, Hedayati A. A survey on blockchain: Challenges, attacks, security, and privacy. « 13 » International Journal of Smart Electrical Engineering. 2021; 10 « 3 » :191-8. Doi: 10.30495/ijsee.2021.684027

Hu VC. Blockchain for access control systems. Gaithersburg, MD: National Institute of Standards « 14 » and Technology, U.S. Department of Commerce; 2022. Doi: 10.6028/NIST.IR.8403

Huang R, Yang X, Ajay P. Consensus mechanism for software-defined blockchain in Internet of « 15 » Things. Intelligent and Converged Networks. 2022; 3 « 4 » :331-42. Doi: 10.1016/j.icnl.2022.12.001

Humayun M, Tariq N, Alfayad M, Zakwan M, Alwakid G, Assiri M. Securing the Internet of Things in « 16 » the artificial intelligence era: A comprehensive survey. IEEE Access. 2024; 12:25678-701. Doi:

10.1109/ACCESS.2024.3365634

K MP. The role of blockchain in securing IoT devices. International Journal of Innovative « 17 »
.Technology and Exploring Engineering. 2024; 13 « 7 » :45-52

Kokila M, S. R. K. Authentication, access control and scalability models in Internet of Things « 18 »
security: A review. Intelligent Systems with Applications. 2025:100005. doi: 10.1016/j.iswa.2024.100005

Li Q, Liu G, Zhang Q, Han L, Chen W, Li R. Efficient and fine-grained access control with fully- « 19 »
hidden policies for cloud-enabled IoT. Digital Communications and Networks. In press. Doi:
10.1016/j.dcan.2024.05.007

Liu H, Han D, Li D. Fabric-IoT: A blockchain-based access control system in IoT. IEEE Access. « 20 »
2020; 8:18207-18. Doi: 10.1109/ACCESS.2020.2968492

Mudhar AK, Malhotra J, Ra S. BlendCAC: A blockchain-enabled decentralized capability-based « 21 »
access control for IoT. IEEE Internet of Things Journal. 2018; 5 « 6 » :4911-22. Doi:
10.1109/JIOT.2018.2872045

Nie S, Ren J, Wu R, Han P, Han Z, Wan W. Zero-trust access control mechanism based on « 22 » blockchain and inner product encryption in the Internet of Things in a 6G environment. Applied Sciences. 2025; 15 « 3 » :890. Doi: 10.3390/app15030890

Pathak A, Al-Anbagi I, Hamilton HJ. TABI: Trust-based ABAC mechanism for edge-IoT using « 23 » blockchain technology. IEEE Access. 2023; 11:23456-68. Doi: 10.1109/ACCESS.2023.3256789

Rajan H, Burns J, Jaiswal C. IoT security: AI blockchain solutions and practices. In: Proceedings of « 24 » IEEE International Conference on Computing, Intelligence and Security Information Systems; 2023; 2023. p. 1-6. doi: 10.1109/CISIS2023.10123456

Ragothaman K, Wang Y, Rimal B, Lawrence M. Access control for IoT: A survey of existing « 25 » research, dynamic policies and future directions. Sensors. 2023; 23 « 4 » :1805. Doi: 10.3390/s23041805

Ravidas S, Lekidis A, Paci F, Zannone N. Access control in Internet-of-Things: A survey. Journal of « 26 » Network and Computer Applications. 2019; 144:79-101. Doi: 10.1016/j.jnca.2019.06.017

Saleh AMS. Blockchain for secure and decentralized artificial intelligence in cybersecurity: A « 27 » comprehensive review. Blockchain: Research and Applications. 2024; 5 « 2 » :100193. Doi: 10.1016/j.bcra.2024.100193

Shahinzadeh G, Shahinzadeh H, Tanwar S. Security and privacy issues in the Internet of Things: A « 28 » comprehensive survey of protocols, standards and revolutionary role of blockchain. In: 8th International Conference on Smart Cities, Internet of Things and Applications « SCIoT » ; 2024 Apr; Mashhad, Iran; 2024. p. 1-6. doi: 10.1109/SCIoT60996.2024.10529123

Shahraki AS, Rudolph C, Alavizadeh H, Kayes ASM, Rahayu W, Tari Z. Securing cross-domain data « 29 » access with decentralized attribute-based access control. Ad Hoc Networks. 2025; 153:103338. Doi: 10.1016/j.adhoc.2024.103338

Sivaselvan N, Bhat KV, Rajarajan M, Das AK. A new scalable and secure access control scheme « 30 » using blockchain technology for IoT. IEEE Transactions on Consumer Electronics. 2023; 69 « 3 » :532-44. Doi: 10.1109/TCE.2023.3252567

Sun P, Shen S, Wan Y, Wu Z, Fang Z, GAO X. A survey of IoT privacy and security: Architecture, « 31 » technology, challenges, and trends. IEEE Internet of Things Journal. 2024; 11 « 6 » :10221-43. Doi: 10.1109/JIOT.2024.3372518

Swetha S, Ananya C, Bhanusha G, Anjali Y. Efficient and secure blockchain-based access control « 32 » for fog-assisted IoT cloud in electronic medical records sharing. Journal of Computational Analysis and .Applications. 2024; 33 « 6 » :123-35

Usman M, Sarfraz MS, Aftab MU, Habib U, Javed S. A blockchain-based scalable domain access « 33 » control framework for industrial Internet of Things. IEEE Access. 2024; 12:30983-97. Doi: 10.1109/ACCESS.2024.3368765

Wu Y, Matsubara Y, Kasahara S. Enhancing account information anonymity in blockchain-based « 34 » IoT access control using zero-knowledge proofs. Electronics. 2025; 14 « 14 » :2772. Doi: 10.3390/electronics14142772

Xu LD, Lu Y, Li L. Embedding blockchain technology into IoT for security: A survey. IEEE Internet of « 35 » Things Journal. 2021; 8 « 13 » :10452-73. Doi: 10.1109/JIOT.2021.3060508

Xu Z, Zhou W, Han H, Dong X, Zhang S, Hu Z. A secure and scalable IoT access control framework « 36 » with dynamic attribute update and policy hiding. Scientific Reports. 2025; 15:11913. Doi: 10.1038/s41598-024-80307-3

Zaidi SYA, Shah MA, Khattak HA, Maple C, Rauf HT, El-Sherbeeny AM, et al. An attribute-based « 37 » access control for IoT using blockchain and smart contracts. Sustainability. 2021; 13 « 9 » :4358. Doi: 10.3390/su13094358

Zhang Q, Xu C, Zhong H, Gu C, Cui J. Revocable and efficient blockchain-based fine-grained « 38 » access control against EDoS attacks in cloud storage. IEEE Transactions on Computers. 2024; 73 « 5 »

:1234–46. Doi: 10.1109/TC.2024.3367890

« 39 » S. Nie, J. Ren, R. Wu, P. Han, Z. Han, and W. Wan, "Zero-trust access control mechanism based on blockchain and inner product encryption in the Internet of Things in a 6G environment," *Appl. Sci.*, vol. .15, no. 3, Art. no. 890, 2025, doi: 10.3390/app15030890

« 40 » Y. Wu, Y. Matsubara, and S. Kasahara, "Enhancing account information anonymity in blockchain-based IoT access control using zero-knowledge proofs," *Electronics*, vol. 14, no. 14, Art. no. .2772, 2025, doi: 10.3390/electronics14142772

« 41 » S. Algarni, F. Eassa, K. Almarhabi, A. Almalaise, E. Albassam, K. Alsubhi, and M. Yamin, "Blockchain-based secure access control in an IoT system," *Appl. Sci.*, vol. 11, no. 4, Art. no. 1773, 2021, .doi: 10.3390/app11041773

پاورقی‌ها:

« 2 » Email:sa.ranjbar2024k@gmail.com

« 3 » Email:s.ranjbar1369@gmail.com

« 4 » Email:mahsarafiee7373@gmail.com

پانویس‌ها: