بسم الله الرحمن الرحيم

**بسمه تعالی**

**دانشکده مهندسی برق-کامپیوتر**

پایان نامه دوره کارشناسی ارشدرشته مهندسی برق_ گرایش پدافند غیرعامل(افا)

عنوان:

# مدلسازی وتحلیل مخاطرات امنیتی NB-IOT وراهکارهای مقابله در شبکه LPWAN

توسط:

**محمد احمدی**

استاد راهنما:

**دکتر رضا خالقی**

استاد مشاور:

**دکتر سجاد پورسجادی**

**۳۰مهر۱۴۰۰**

**بسمه تعالی**

**دانشکده مهندسی برق-کامپیوتر**

پایان نامه دوره کارشناسی ارشد رشته مهندسی برق_ گرایش پدافند غیرعامل(افا)

مربوط به محمد احمدی

با عنوان:

**مدلسازی وتحلیل مخاطرات امنیتی NB-IOT وراهکارهای مقابله در شبکه LPWAN**

در تاریخ ۹۹/۷/۳۰توسط کمیته تخصص زیر مورد برسی قرار گرفت

وبا نمره.....ودرجه.....به تصویب رسید.

| ردیف | مسئولیت | عنوان | امضاء |
|---|---|---|---|
| ۱ | استاد راهنما اول | **دکتررضا خالقی** | |
| ۲ | استاد راهنما دوم | -------- | |
| ۳ | استاد مشاور | **دکتر سجاد پورسجادی** | |
| ۴ | استادداوربیرونی | | |
| ۵ | استادداورو داخلی | | |
| ۶ | مدیر تحصیلات تکمیلی دانشکده/مجتمع | | |

## ((من لم یشکر المخلوق لم یشکر الخالق))

خداوند متعال را شکر می گویم که توفیق تهیه ، تدوین و ویرایش مجدد این شیوه نامه را نصیب اینجانب نمود . در راستای انجام این اثر ، افرادی به طور مستقیم و یا غیر مستقیم نقش داشته اند که نام بردن از همه آنها در این جا میسر نیست . بنابراین ، از همه کسانی که در این راستا به نحوی همکاری داشته اند تشکر و قدردانی می نمایم . گرچه این شیوه نامه بر اساس مطالعات منابع علمی ، شیوه نامه های موجود در برخی از دانشگاههای کشور و تجربیات نویسنده تدوین شده ، ولی نقش اساتید گرامی به ویژه اساتید راهنما ، مشاور و داور در دوره های کارشناسی ارشد و دکترا در جهت دهی این مطالعات و تجربیات بسیار مؤثر بوده است . علاوه بر این ، دانشجویان مقاطع مختلف به ویژه دانشجویان کارشناسی ارشد و دکترا و همچنین نویسندگان محترمی که نقاط قوت و ضعف پایان نامه ها ، مقالات ، کتاب ها و سایر آثار علمی آنها مورد مطالعه ، راهنمایی و یا داوری این حقیر قرار گرفته ، به طور غیرمستقیم بر افزایش کیفیت این شیوه نامه به خصوص ویرایش سوم ) اثرگذار بوده اند . از همکاران گرامی که ضمن مرور ویرایش دوم شیوه نامه و ارایه برخی نقطه نظرات ، زمینه بازنگری ، تدوین و اجرایی شدن ویرایش سوم را با عنوان « شیوه نامه تدوین پایان نامه ها و رساله های دانشجویی شامل کارشناسی ، کارشناسی ارشد و رساله های دکترای تخصصی » در سطح دانشگاه فراهم نمودند سپاسگزاری می نمایم .

۳۰مهر۱۴۰۰_محمد احمدی

تمامی حقوق مادی و معنوی مترتب بر نتایج مطالعات،
ابتکارات و نواوری های حاصل از این تحقیق متعلق به
دانشگاه صنعتی مالک اشتر است.

## تائید صحت ، اصالت و رعایت امانت در پایان نامه / رساله

اینجانب محسن احمدی دانشجوی رشته برق_پدافند غیرعامل گرایش افا مقطع تحصیلی کارشناسی ارشد به شماره دانشجویی۹۸۱۴۲۱۰۲۵ صحت ، اصالت و رعایت امانت در پایان نامه ارساله را تائید و اعلام می نمایم کلیه نتایج این پایان نامه ارساله و نشریات مرتبط با آن ( از قبیل مقالات استخراج شده حاصل کار اینجانب و بدون هرگونه دخل و تصرف است و موارد نسخه برداری شده از آثار دیگران را با درج کامل مشخصات منبع ذکر کرده ام . علاوه براین ، هر گونه آثار مرتبط با این پایان نامه ارساله را با رعایت امانت منتشر نموده و یا خواهم نمود . بنابراین ، در تمامی آثار مرتبط ( نظیر مقاله ، ثبت اختراع ، شرکت در جشنواره ها و مواردی از قبیل ) حقوق مالکیت دانشگاه صنعتی مالک اشتر ( از جمله حقوق اساتید محترم راهنما و مشاور ) را رعایت می نمایم و هرگونه اثری را با هماهنگی و درج نام مبادی ذیصلاح دانشگاه ( از جمله اساتید محترم راهنما ) منتشر خواهم نمود . در صورت اثبات خلاف مندرجات فوق ویا هرگونه تخلفی که صحت ، اصالت و رعایت امانت در پایان نامه ارساله را مخدوش نماید ، دانشگاه می تواند مطابق با ضوابط و مقررات حاکم ( قانون حمایت از حقوق مؤلفان و مصنفان و قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی ، ضوابط و مقررات آموزشی ، پژوهشی و انضباطی با اینجانب رفتار نماید . بنابراین ، حق هرگونه اعتراض در خصوص احقاق حقوق مکتسب و تشخیص و تعیین تخلف و مجازات را از خویش سلب می نمایم . همچنین ، مسئولیت هرگونه پاسخگویی به اشخاص اعم از حقیقی و حقوقی و مراجع ذی صلاح ( اعم از اداری و قضایی ) به عهده اینجانب خواهد بود و دانشگاه هیچ گونه مسئولیتی در این خصوص نخواهد داشت . ۱۵ اردیبهشت ۱۳۹۳ نام و نام خانوادگی دانشجو اثر انگشت و امضاء

۳۰مهر ۱۴۰۰

محمد احمدی

فهرست مطالب

عنوان صفحه

**فصل سوم: الگوریتم پیشنهادی**

## فهرست جدول ها

فهرست شکل ها

| شماره شکل | عنوان شکل | صفحه |
|---|---|---|

نمادها(علایم اختصاری)

| نماد | عنوان | توضیح |
| --- | --- | --- |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# فصل اول: کلیات تحقیق

### ۱-۱. مقدمه

در فصل اول ابتدا بیان مسئله ارائه می‌گردد. سپس فرضیه ها، اهداف تحقیق بررسی می‌گردد. در ادامه ضرورت انجام تحقیق، روش تحقیق، جنبه نوآوری و قلمرو تحقیق مطرح و در نهایت ساختار پایان نامه ارائه می‌گردد.

### ۱-۲. بیان مسئله

اینترنت اشیاء یک معماری نوظهور اطلاعاتی است که زیرساخت شبکه ای را متصل می کند و انواع مختلف دستگاه ها را به یکدیگر متصل می کند. اینترنت اشیاء تعامل بین اشیا و خدمات را در محیطی امن و قابل‌اطمینان به هدف کاهش فاصله بین اشیای دنیای فیزیکی و سیستم‌های اطلاعاتی برقرار می نماید. اینترنت اشیاء خدمات و برنامه ها را در حوزه های مختلف کاربردی مانند نظارت بر سلامت، نظارت بر ورزش، نظارت بر حیوانات و خانه های هوشمند ارائه می کند. اشیاء در جهت بدست آوردن وضعیت هوشمند برای ایجاد و فراهم نمودن تصمیمات مربوطه هستند. همچنین می توانند با یکدیگرارتباط برقرار نمایند،همچنین به اطلاعاتی که توسط اشیاء دیگرجمع آوری گردیده است، دسترسی داشته باشند[۱-۳].

سه فاز اصلی را برای به ثمر رسیدن مرحله نخست اینترنت اشیاء در نظر گرفت. در فاز نخست هر شیء اطلاعات خاصی را در خود نگه می‌دارد، اما این افراد هستند که باید با استفاده از ابزارهایی مثلاً تلفن‌های هوشمند خود، این اطلاعات را استخراج نمایند. در فاز دوم، هر وسیله می‌تواند اطلاعات را در موعد تعیین شده برای کاربر ارسال کند. پس از تکمیل ارتباط میان اشیاء و انسان، نوبت ارتباط اشیاء با یکدیگر است. که در فاز سوم اشیاء بدون دخالت انسان با یکدیگر ارتباط برقرار می نمایند. با تکمیل این سه فاز مرحله نخست تکامل اینترنت اشیاء به اتمام می‌رسد. در نهایت دنیایی از ایده‌ها در مقابل توسعه‌دهندگان قرار می‌گیرد. هر وسیله اطلاعاتی را دارد که درون یک شبکه، در دسترس وسایل دیگر و مالک وسیله قرار می گیردو این توسعه‌دهندگان هستند که با خلاقیت خود از این اطلاعات استفاده بهینه می‌نمایند[۴].

دستگاه های متصل به اینترنت اشیا به جزئی از زندگی روزمره تبدیل شده اند. تعداد این دستگاه های متصل به شبکه اینترنت اشیا بیش از ۲۶,۶۶ میلیارد تا پایان سال ۲۰۱۹ عبور کرده است و همچنان در حال افزایش است زیرا در هر ثانیه ۱۲۷ دستگاه جدید در سراسر جهان به اینترنت متصل هستند. هرچه تعداد دستگاه های متصل به شبکه اینترنت اشیا بیشتر باشد، در برابر تهدیدات و خطرات امنیتی بیشتر آسیب پذیر می شود. بسیاری از دستگاه های اینترنت اشیا به اطلاعاتی با ماهیت بسیار حساس متصل هستند که فقط توسط افراد مجاز قابل دسترسی هستند. یکی از دلایل این آسیب پذیری در برابر خطرات امنیتی این است که تولیدکنندگان دستگاه هایی که به شبکه های اینترنت اشیا متصل می شوند ، حریم خصوصی یا امنیت دستگاه و داده ها را در

اولویت قرار نمی دهند. از این رو بسیاری از کاربران که از این موضوع بی اطلاع هستند هنوز این دستگاه ها را خریداری می کنند و آنها را به شبکه اینترنت اشیا متصل می کنند و خطر نقض امنیت و غیره را افزایش می دهند[۵, ۶].

اینترنت اشیاء باریک۱ که توسط پروژه مشارکت نسل سوم (GPP۳) در نسخه ۱۳ (Rel-13) استاندارد شده است ، یک راه حل پیشرو در زمینه شبکه های کم مصرف۲ است[۷].

این برنامه با بهره گیری از زیرساخت های سلولی[۸]، با تمرکز بر خدمات عظیم ماشین ارتباطی (mMTC)، مانند شهرهای هوشمند، نظارت بر محیط زیست و اتوماسیون صنعتی، از جمله دیگر برنامه های کاربردی اینترنت اشیاء ارزان قیمت و مقرون به صرفه است[۹, ۱۰].

فقدان اندازه گیری های مقیاس وسیع در دسترس، مانع از مدل های از دست دادن مسیر تجربی۳ (PL) برای NB-IoT شده است[۱۱].

بنابراین، تحقیقات مبتنی بر شبیه سازی در حال حاضر بر مدل هایی است که برای سایر فناوری های سلولی طراحی شده اند، تکیه می کنند، که البته با پهنای باند متفاوت، فرکانس حامل و استقرار زیرساخت ها، در میان موارد دیگر مشخص می شوند[۱۱].

با بررسی و تجزیه و تحلیل اینترنت اشیاء، می توان برخی از ویژگیهای دستگاههای اینترنت اشیا را دلیل آسیب پذیری امنیتی دانست[۱۲]. از جمله ویژگی های دستگاه های اینترنت اشیاء می توان به موارد زیر اشاره نمود:

جمع آوری داده های زمان واقعی برای انجام وظایف

آنها دائماً از LPWAN سلولی استفاده می کنند که Narrowband IoT و LTE-M نیز نامیده می شود.

این دستگاه ها پارامترهای فیزیکی را اندازه گیری می کنند و قادر به انجام اقدامات فیزیکی هستند.

همیشه به ابر متصل هستند.

این دستگاه ها توانایی تصمیم گیری را به تنهایی براساس داده های موجود دارند[۱۳].

فقط با ایمن سازی دستگاه های اینترنت اشیاء نمی توان امنیت را برقرار نمود[۱۴]. بلکه اینترنت اشیا به معنای یک سیستم کامل است و نه فقط دستگاههای روزمره و متداول، این سیستم علاوه بر تجهیزات اینترنت اشیاء شامل محاسبات ابری، رابط شبکه جهت اتصال و نرم افزار قابل نصب بر روی موبایلی که جهت کنترل دستگاه استفاده می شود[۱۵].

بنابراین در کنار دستگاه اینترنت اشیا، تمام این اجزای سیستم به یک اندازه در معرض تهدیدات امنیتی و چالش هایی هستند. در بخش پیشینه تحقیق و پژوهش این چالش ها بررسی می گردد.

1 Narrowband Internet of Things(NB-IoT)

2 Low Power Wide Area Networks (LPWANs)

3 path loss(PL)

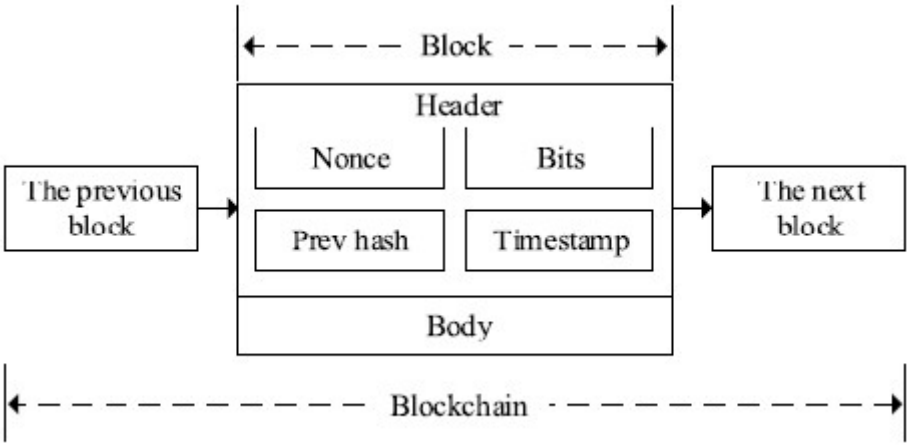
در این پایان نامه ضمن بهره گیری از بلاک چین به عنوان یک تکنولوژی نوظهور یک راهکار مقابله با مخاطرات امنیتی NB-IOT در شبکه LPWAN ارائه می گردد.

بلاک چین یک پلت فرم ذخیره سازی توزیع شده است که امنیت لازم، تغییرناپذیری داده های مهم، قابلیت ردیابی، شفافیت، استحکام را در کنار هم فراهم می کند[۱۶, ۱۷].

بلاک چین اطلاعات را به صورت بلوکی ذخیره می کند که به هم متصل شده اند و به روزرسانی یا حذف اطلاعات از بلوک ها امکان پذیر نیست. علاوه بر این، بلوک های جدید فقط می توانند در انتهای زنجیره اضافه شوند، که باعث می شود زنجیره بلوک تغییر ناپذیر و مقاوم باشد. با این حال، مهمترین ویژگی بلاکچین این است که برای تأیید تبادل اطلاعات به هیچگونه مشارکت شخص ثالث نیاز ندارد، زیرا همه اعضا یک نسخه از کل بلاکچین را ذخیره می کنند و پس از اضافه شدن بلوک جدید، هر عضو پایگاه داده خود را به روز می کند.

معمولا سیستم های احراز هویت دارای امنیت بالا از زیر ساخت کلید عمومی۴ بهره می گیرد. یک وسیله نقلیه جهت تبادل اطلاعات باید هویت محلی۵ اش در سامانه به عنوان گره مجاز ثبت شده باشد. لذا با ارسال یک شناسه رمزگذاری شده می تواند این هویت را اثبات نماید[۱۸].

بر اساس شکل ۱-۱ که ساختار بلاک چین را نمایش می دهد، بلاک چین یک پایگاه داده توزیع که از یک لیست در حال رشد از بلوک های زنجیر شده تشکیل شده است. بلاک چین یک دفترچه اصلی را بدون یک پایگاه داده متمرکز مبتنی بر گره های توزیع شده حفظ می کند. ساختار بلاک چین از یک شبکه توزیع شده نظیر به نظیر تشکیل شده است. هر گره با استفاده از یک کلید عمومی مدیریت می گردد. فرآیند تبادل اطلاعات و ارتباطات بین گره ها توسط کلید عمومی رمز گذاری می شود. هر گره می تواند یک اعتبار را با اعتبار امضای تولیدکننده فرآیند در برابر کلید عمومی خود تأیید کند. در ساختار بلاک چین همانگونه که در شکل ۱-۱ مشخص است هر بلاک از بلاک قبلی و بعدی خود مطلع است.




شکل ۱-۱. ساختار بلاک چین [۱۹]

4 Public Key Infrastructure (PKI)

5 Local Authentication Center (LAC)

### ۱-۳. اهمیت و ضرورت انجام تحقیق

امنیت یکی از پارامترهای مهم در اینترنت اشیاء می باشد. لذا ارائه یک راهکار امنیتی در جهت جلوگیری از حملات امری ضروری و مهم است. بلاک چین می تواند امنیت NB-IoT را بهبود ببخشد. امروزه هکرها و حمله کنندگان به سیستم های اطلاعاتی از جمله اینترنت اشیاء ضمن شناخت کامل شبکه به دنبال نقاط ضعف و حفره های امنیتی سیستم موجود هستند. لذا با علم بر این که سیستم های توزیع شده مدیریت تبادل اطلاعات آسیب پذیری در برابر خطرات دارند. لذا بهره گیری از بلاک چین می تواند تا حدودی امنیتی را افزایش دهد. لذا بهره گیری از بلاک چین جهت افزایش امنیت NB-IoT ضروری می باشد.

### ۱-۴. اهداف تحقیق

### ۱-۵. سوالات تحقیق

بهره گیری از ساختار بلاک چین امنیت NB-IoT را تا چه میزان بهبود می بخشد؟

بهره گیری از ساختار بلاک چین مخاطرات NB-IoT را  تا چه میزان کاهش می دهد؟

### ۱-۶. فرضیه تحقیق

بهره گیری از ساختار بلاک چین امنیت NB-IoT را بهبود می بخشد.

بهره گیری از ساختار بلاک چین مخاطرات NB-IoT را کاهش می دهد.

### ۱-۷. روش تحقیق

روش گردآوری اطلاعات به صورت کتابخانه‌ای می‌باشد. اینترنت، کتب مربوطه، مقالات و بهره گیری از مراجع معتبر دنیا مانند الزویز، اسپرینگر و IEEE در جهت بهبود وضعیت پژوهش کمک شایانی می کند.

مطالعه و بررسی کتب و مقالات، بررسی ساختار اینترنت اشیاء و NB-IoT، بررسی ساختار بلاک چین و ارائه راهکار بهینه روش پیشنهادی بر اساس مراحل زیر:

مطالعات اولیه در مورد سیستم های NB-IOT

بررسی روش های مدل سازی و تحلیل مخاطرات امنیتی

انتخاب روش (های) مناسب تامین امنیت و شبیه سازی آن

ارایه راهکاری برای افزایش امنیت

شبیه سازی راهکار پیشنهادی

نوشتن پایان نامه و مقاله بر اساس روش پیشنهادی

قلمر تحقیق افزایش امنیت در NB-IoT به کمک ساختار بلاک چین می باشد.

روش تحقیق در این پژوهش از نوع توصیفی تحلیلی و به‌صورت شبیه‌سازی می‌باشد. برای این منظور، بهبود مدل با استفاده از نرم افزار ارائه شده است. شبیه‌سازی واجرای آن با کمک گرفتن از نرم افزار انجام می‌گیرد و نتایج کسب شده جهت تأیید نتایج تئوری مورد بحث و بررسی قرار خواهند گرفت. فرآیند شبیه سازی در محیط OMNET++ ارائه می گردد.

### ۱-۸. جنبه نوآوری تحقیق

مدلسازی و تحلیل مخاطرات امنیتی NB-IOT و راهکار های مقابله در شبکه های LPWAN با بهره گیری از ساختار بلاک چین جنبه نوآوری این پژوهش محسوب می گردد.

### ۱-۹. ساختار پایان‌نامه

سازمان‌دهی این تحقیق به این شکل می‌باشد که این پایان‌نامه در ۵ فصل به شرح زیر طراحی‌شده است، در این فصل به کلیات تحقیق پرداخته شد که شامل بیان مسئله تحقیق، ضرورت انجام تحقیق، اهداف تحقیق، سؤال تحقیق، روش‌شناسی انجام تحقیق بوده و هرکدام به‌تفصیل بررسی شدند تا یک تصویر کلی از تحقیق صورت گرفته، ارائه شود.

فصل اول: کلیات تحقیق

فصل دوم: مبانی نظری و پیشینه تحقیق

فصل سوم: روش‌شناسی تحقیق

فصل چهارم: تجزیه‌وتحلیل داده‌ها

فصل پنجم: نتیجه‌گیری و ارائه‌ی پیشنهادهای آینده

# فصل دوم: مبانی نظری و پیشینه‌ی تحقیق

### ۲-۱. مقدمه

در فصل دوم مبانی نظری پژوهش به همراه پیشینه تحقیق بررسی می گردد. در بخش مبانی نظری پژوهش مفاهیم نظری پژوهش مطرح و این مفاهیم بسط داده می شود. همچنین در بخش پیشینه پژوهش، بررسی جامع بر روی کارهای گذشته در زمینه موضوع تحقیق مطرح و مزایا و معایب روشها بررسی می گردد.

### ۲-۲. مبانی نظری پژوهش

در بخش مبانی نظری پژوهش مفاهیمی مانند اینترنت اشیاء، مدل ها و معماری های به کاربرده شده در اینترنت اشیاء، معماری مرجع اینترنت اشیاء به همراه اینترنت اشیاء باریک مورد بررسی قرار خواهد گرفت.

#### ۲-۲-۱. اینترنت اشیاء

اینترنت اشیاء فناوری پیشرفته‌ای است که در آن برای هر شیء، قابلیت ارسال داده از طریق شبکه‌های ارتباطی اعم از اینترنت یا اینترانت فراهم می شود. مهمترین دلیل فراگیر شدن اینترنت اشیاء، قابلیت اتصال انواع اشیاء و وسایل به دنیای مجازی است. اینترنت اشیاء شبکه ای بی سیم بین اشیاء می‌باشد که دراین شبکه دستگاه‌ها (اشیاء) بدون دخالت انسان با یکدیگر ارتباط دارند، همچنین تکمیل کننده‌ای برای خانه‌ها، موبایل‌ها ودستگاه های مختلف می باشد که با یکدیگر به اینترنت متصل می شوند و قابلیت پردازش همزمان بااستفاده از آنالیز داده‌ها را دارند. این تکنولوژی انقلاب جدیدی در اینترنت است. اشیاء، خود را قابل تشخیص و شناسایی می سازند. همچنین آنها در حال بدست آوردن هوشمندی با ایجاد و فراهم سازی تصمیمات مربوطه هستند. آنها می توانند با یکدیگرارتباط برقرار کنند،همچنین به اطلاعاتی که توسط اشیاء دیگرجمع آوری شده، دسترسی داشته باشند[۳].

#### ۲-۲-۲. مدل ها / معماری های به کاربرده شده دراینترنت اشیاء

هدف نهایی تکنولوژی اینترنت اشیا ارتباط خودکار سیستم های مختلف می باشد تا خدمات جدیدی را برای کاربران فراهم کنند. بنابراین استانداردسازی برای اطمینان از برقراری ارتباط سیستم‌های متمایز ضروری می‌باشد. درحالی که انتظار می‌رود اینترنت اشیاء قسمت‌های مختلف اقتصاد در جامعه را تغییر دهد، باعث ایجاد اطلاعات(داده های) فراوانی خواهد شد. این موضوع، امکان ایجاد چالش های امنیتی را به وجود می آورد. بنابراین برای قابل استفاده کردن اینترنت اشیاء استاندارد های امنیتی برای حفاظت از افراد، تجارت‌ها و دولت‌هایی که ازاینترنت اشیاء استفاده می کنند، مورد نیاز است. دراین بخش به مرور برخی ازمعماری های پیشنهادی دراینترنت اشیاء می‌پردازیم. مدل های مرجع برای استانداردسازی دراینترنت اشیاء ضرروی می باشند زیرا می‌توانند دستورالعمل‌هایی که برای برنامه‌ریزی سیستم های اینترنت اشیاء ضروری می باشد مشخص کنند[۳].

در ادامه تعدادی از مدل ها و معماری ها اینترنت اشیاء اشاره می شود:

مدل اینترنت اشیاء A :مدل مرجع معماری (ARM به منظور ایجادقابلیت همکاری بین سیستم های مختلف اینترنت اشیا به کار رفته است. این معماری برای ایجاد معماری های مدل مرجع (RM) و معماری مرجع (RA)به کارمی رود. مدل مرجع پیشنهادی توسط اینترنت اشیا A-در برگیرنده موضوعاتی می باشد که در به‌طور مختصر تشریح می‌گردد [۲۰].

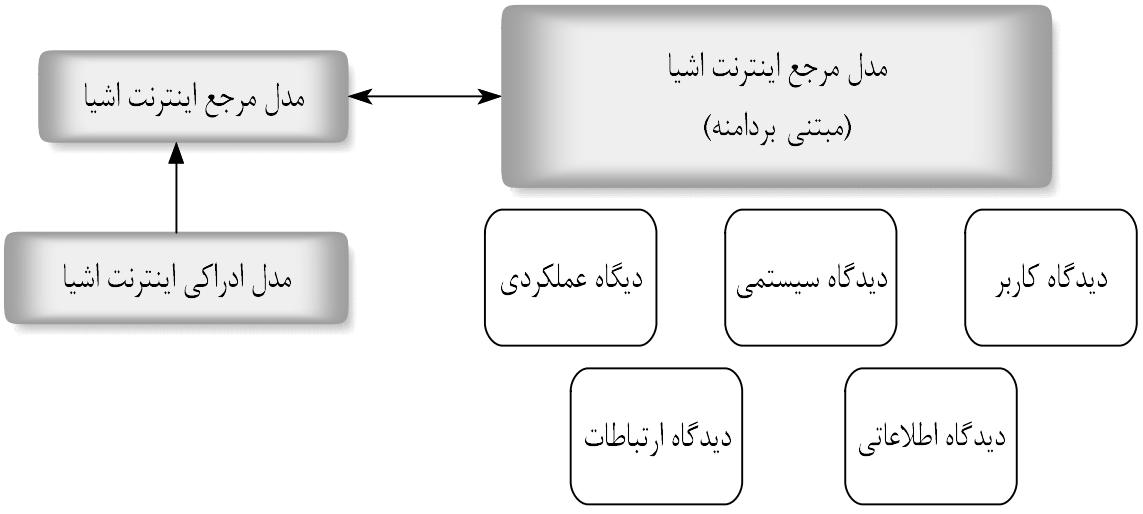
مدل ارتباطی اینترنت اشیاء: این مدل به بیان نمونه های ارتباطی اصلی برای ارتباطات سازمانی، اطمینان از قابلیت همکاری بین شبکه های ناهمگن می‌پردازد.( برای فهمیدن ویژگی‌هایی درباره ارتباطاتی که بین دستگاه‌های ناهمگن اینترنت اشیا و کل اینترنت وجود دارد)

مدل دامنه اینترنت اشیاء : یک مدل سطح بالا از مفاهیم (دستگاه‌ها، منابع و خدمات) است که جنبه‌های خاصی از دامنه اینترنت اشیا و روابط آن ها را نشان می‌دهد.( این مدل به شرح روابط بین آن ها که نشان دهنده جنبه هایی از دامنه اینترنت اشیا می باشد می پردازد)

مدل اطلاعاتی اینترنت اشیاء : این مدل ویژگی های داده های مدل دامنه اینترنت اشیا را مشخص می‌کند (این مدل به تشریح ویژگی های اطلاعاتی مدل دامنه اینترنت اشیا می پردازد). همچنین به تشریح مدل سازی دانش اینترنت اشیاء می پردازد.
(همچنین به شرح چگونگی مدلسازی دانش اینترنت اشیاء می‌پردازد.)

**۲-۲-۳. معماری مرجع اینترنت اشیاء**

این معماری ساخت سیستم اینترنت اشیاء را براساس یک مدل ادراکی/ مفهومی (CM) که شامل مهم‌ترین ویژگی‌ها در حوزه های مرتبط با آن می‌باشد ایجاد می‌کند، سپس، آن را از CM به عنوان مبنایی برای ایجاد یک سطح بالا مبتنی بر سیستم RM به کار می گیرد. این معماری از ۵ دیدگاه عملکردی سیستم، کاربر، اطلاعاتی و ارتباطی تشکیل یافته است. شکل ۲-۱ ارتباط بین این سه اجزا (RM,RA,CM) رانشان می دهد[۲۰].




شکل ۲-۱ ارتباط ادراکی(مفهومی) ، معماری مرجع ، مدل مرجع

## IEEE P2413 .۳-۲

استاندارد IEEE P2413 شرح معماری سیستم ومهندسی نرم افزار می باشد. هدف این استاندارد تمرکز بر دستیابی به قابلیت همکاری، همراه با سایر مشخصه‌های کیفیت مانند حفاظت، حفظ حریم شخصی و امنیت است.

### ۲-۳-۱. معماری مرجع صنعتی

این معماری یک استاندارد مبتنی بر معماری باز برای سیستم های اینترنت صنعتی است که عملیات صنعتی هوشمند را انجام می دهد و بر ویژگی‌های اساسی این نوع سیستم‌ها از قبیل امنیت، اطمینان و انعطاف پذیری تمرکز می‌کند.

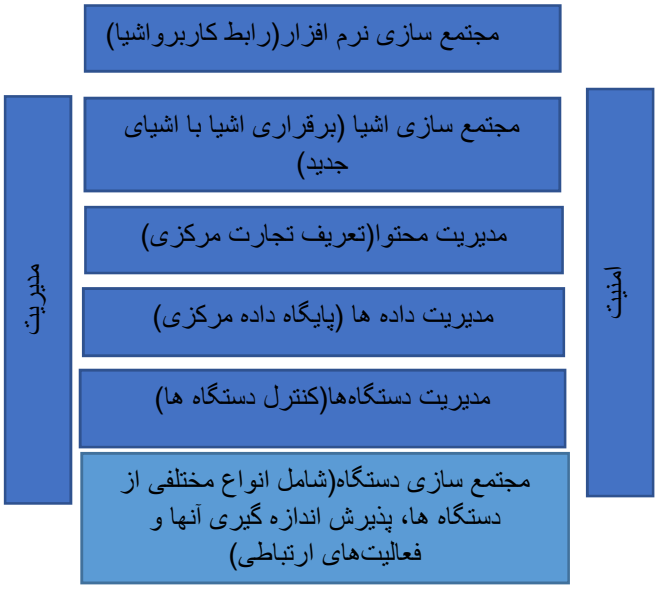
### ۲-۳-۲. مدل مرجع سیسکو

یک مدل مرجع توسط سیسکو بصورت هفت لایه (RM) مطابق شکل ۲-۲ ارائه شده است. پایین‌ترین سطح شامل دستگاه‌ها وکنترل کننده‌های فیزیکی (اشیاء) می‌باشد که به عنوان فناوری عملیاتی در نظرگرفته می‌شود و بالاترین سطح مربوط به آی تی می‌باشد. سه سطح پایین‌تر فناوری عملیاتی (OT) در نظر گرفته می شود .چهار سطح برتر مربوط به آی تی است. پایین ترین سطح آی تی در قسمت پشته ذخیره سازی است و به دنبال آن است که با انتزاع داده ها، برنامه ها، و همکاری و (فرآیندهای کسب و کار به انتها برسد [21].


شکل ۲-۲ معماری لایه ای مرجع اینترنت اشیاء

### ۲-۳-۳. معماری لایه ای مرجع اینترنت اشیاء

معماری RILAیک معماری یکپارچه می باشد که برای مشتریان وصنعت بهتر از اینرنت اشیاء Aعمل می‌کند. این معماری که بین اشیاء، دستگاه ها و کاربر عمل می کند شامل شش لایه مطابق شکل ۲-۳ می باشد. علاوه بر این لایه ها، دو لایه بخش، "امنیت" و "مدیریت" وجود دارد که بر تمام لایه های دیگر تأثیر می‌گذارد.




شکل ۲-۳ معماری لایه ای مرجع اینترنت اشیاء

این لایه ها به صورت مختصر در زیر شرح داده شده اند.

لایه یکپارچه سازی دستگاه : این لایه شامل انواع مختلفی از دستگاه ها، مقیاس ها و فعالیت‌های ارتباطی آن ها است .

لایه مدیریت دستگاه: این لایه ثبت نام دستگاه و اندازه گیری سنسور از لایه یکپارچه سازی و کنترل دستگاه های متصل به سیستم را به عهده دارد. هر تغییری در ثبت نام دستگاه و همچنین داده های اندازه گیری جدید باید از لایه یکپارچه سازی به لایه مدیریت وسیله انتقال داده شود، بنابراین اطلاعات می توانند به روز رسانی و ذخیره شوند.

لایه مدیریت داده ها: این لایه تمام اطلاعات اشیا را ذخیره می کند. اجرای لایه مدیریت داده بستگی به حالت های استفاده شده دارد.

لایه مدیریت محتوا: این لایه مسئول اموری همچون تعریف تولید و مصرف شرایط محیطی اشیاء، ارزیابی موقعیت محتوا نسبت به اهداف، فعالیت‌های مربوط به راه‌اندازی و منطبق کردن اهداف با قواعد ارزیابی شده می باشد و درنهایت موقعیت محتوا را برای سایر اشیاء منتشر می‌سازد. (هدف تجارت مرکزی را تعریف کرده و مسئول اموری همچون تعریف اهداف اشیاء، تولید و مصرف شرایط محیطی اشیاء، ارزیابی موقعیت محتوا نسبت به اهداف، فعالیت‌های مربوط به راه‌اندازی و منطبق کردن اهداف با قواعد ارزیابی شده می باشد و درنهایت موقعیت محتوا را برای سایر اشیاء منتشر می‌سازد.) لایه یکپارچه سازی اشیاء: مسئول یافتن اشیایی است که امکان برقراری ارتباط با اشیای جدید را می‌دهد و مسئول عوامل ثبت و برسی می‌باشد.

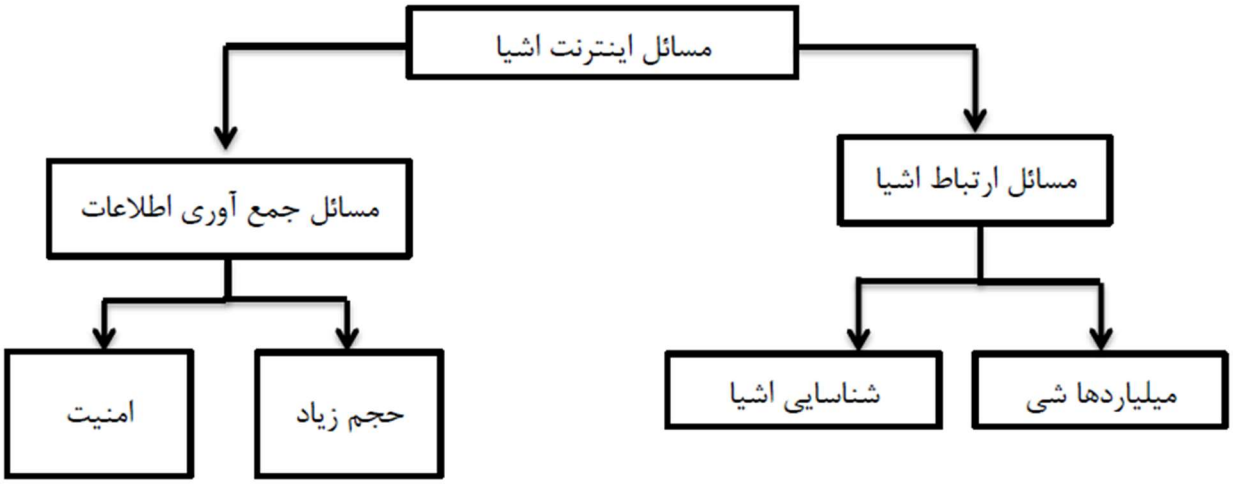
لایه یکپارچه سازی نرم افزار: این لایه  کاربر را به اشیاء متصل می‌کند و همچنین لایه سرویس و یا یک سطح مشترک لایه ساده را نیز مدنظر قرار می‌دهد[۲۲].

### ۲-۴. چالش‌های اینترنت اشیاء

چالش‌های متعددی برای اینترنت اشیاء وجود دارد که هنوز در مراحل تحقیقاتی قرار دارند .این چالش ها،مسائل بازی هستند که به دو دلیل اصلی زیر ایجاد شده اند [۲۳]:

حجم انبوه اطلاعات جمع آوری شده برای هر شیء

ارتباط میان سخت افزار سیستم ها. شکل ۲-۴ دسته بندی مشخص تری را از این موارد نشان می دهد.




شکل ۲-۴ دسته بندی چالش‌های اینترنت اشیاء

### ۲-۵.جمع آوری اطلاعات

مسائل این بخش می توانند به دو دسته اصلی تقسیم بندی شوند .اول به حجم زیاد اطلاعات جمع آوری شده که از تعداد بسیار زیاد اشیاء متصل شده به سیستم اینترنت اشیاء استخراج می شود .دوم بحث امنیت و حریم خصوصی اطلاعات است که به دلیل ارسال بیسیم اطلاعات باید مورد توجه قرار بگیرد.

### ۲-۵-۱. حجم زیاد اطلاعات جمع آوری شده

سیستمهای اینترنت اشیاء باید میلیاردها شیء را به یکدیگر متصل کنند و هر شیء باید اطلاعاتی را از خود منتشر کند .این اطلاعات باید در نقاطی جمع آوری شوند تا مورد بهره برداری قرار گیرند .به دلیل تعداد بسیار زیاد اشیاء IoT ، مقدار اطلاعات جمع آوری شده بسیار زیاد است .بنابراین، با مشکلات مختلف و زیادی درجمع آوری این اطلاعات مواجه خواهیم بود. ازجمله این مشکلات شامل:

۱-انتقال اطلاعات :حجم بسیار اطلاعات باید به صورت آنی منتقل شوند که لزوماً تضمین شده نیست .مهمترین دلیل این امر نیز مربوط به محدودیت های پهنای باند است.

۲-ذخیره: این مسأله به دلیل حجم بالای اطلاعاتی که باید ذخیره شوند و گرفتن نسخه پشتیبان از آنها مهم می شود.

۳-پردازش: اطلاعات جمع آوری شده اشیاء باید توسط کاربردهای وب پردازش و کنترل شوند تا فعالیت های کنترلی برای اشیاء مشخص شود .فرایند کنترل باید به صورت آنی انجام شود ونیازمند قدرت محاسباتی است.

### ۲-۶. امنیت و حریم خصوصی

مشخص است که دادهها بین اشیاء IoT به صورت بی سیم منتقل می شود . بنابراین امنیت و حریم خصوصی بسیار مهم می شود که باید به دقت بررسی شوند . در مورد امنیت، دلایل متعددی برای به خطرافتادن اطلاعات موجود در IoT وجود دارد . این دلایل شامل موارد زیر است:

حملات لایه فیزیکی : یک هکر میتواند اطلاعات درون دستگاه های IoT را استخراج یا حذف کند و یا تغییر دهد، چرا که این دستگاه ها در اکثر اوقات در محیط رها می شوند.

حمله به اطلاعات بیسیم : مهاجم ممکن است بتواند قبل از رسیدن اطلاعات به گیرنده، آن را بدست آورد . در این زمینه موضوعات مطالعاتی مختلف و متعددی از نظر امنیتی وجود دارد و یک چالش بزرگ محسوب می شود.

توان دفاعی پایین : بیشتر دستگاههای IoT امکان پذیرش بسته های امنیتی را به دلایلی مثل توان مصرفی، قدرت پردازشی، هزینه و صرفه جویی های دیگر، ندارند[24].

حریم خصوصی یک مقوله مهم در کشورهای متمدن است . حریم خصوصی یعنی فراهم آورنده اطلاعات یا یک کاربر تنها توسط مشاهده استفاده از سیستم وی قابل تشخیص باشد و حداقل ، تشخیص او باید بسیارسخت باشد . ( جمع آوری، هدایت و Miningاطلاعات در سیستمهای IoT به گونه دیگری صورت میگیرد و دلیل این امر، وجود راه حل های مختلف در سیستمهای IoTاست ( مثل سیستم کنترل منابع خانه .) بنابراین برای تضمین حریم خصوصی اطلاعات شخصی، باید از سه موضوع اصلی زیر اطمینان حاصل کنیم.

چه کسی اطلاعات شخصی را جمع آوری می کند.

این اطلاعات چگونه جمع آوری می شوند.

زمان فرایند جمع آوری چه قدر است.

ضمن اینکه باید تضمین شود که اطلاعات شخصی جمع آوری شده توسط افراد مجاز استفاده و در سرورهای مجاز ذخیره می شود .همچنین هر فرد باید بداند که چه اطلاعاتی از حریم خصوصی او در اختیار افراد مجاز قرار می گیرد و تمام این فرایند با آگاهی، اجازه و رضایت وی انجام شود.

**۲-۶ . ارتباطات اشیاء**

مسائل مربوط به ارتباط بین اشیاء در IoT به دو دسته تقسیم می شود .دسته اول، پاسخ به مسائل اشیاء، و دسته دوم مسائل RFIDدر زمینه خواندن، نوشتن، و انتقال اطلاعات اشیاء است .در ادامه به بررسی مسائل ارتباطی اشیاء می پردازیم. میلیاردها شیء درIoT وقتی ارتباط بین تعداد زیادی از اشیاء مطرح می شود، مسائل بسیاری نمایان می شود .از جمله این مسائل شامل موارد زیر است:

سخت افزار چه باشد؟

کدام سخت افزار برای ارتباط این حجم انبوه اشیاء مورد نیاز است؟

روش آدرس دهی ایده آل( پروتکل) برای هر شیء در سیستم چیست؟

آیا سازگاری بین تعداد زیادی از سخت افزارها به عنوان یک فاکتور ارتباطی می تواند باشد یا خیر؟

با تمرکز روی سیستم IoT ، دو مسأله مبهم مشخص می شود:

چگونه هر شیء تعریف شود.

نوع اطلاعات هر شیء بدست آید.

این مسائل با فناوری RFID قابل پاسخگویی است . اما این فناوری مشکلات متعددی مثل حریم خصوصی، تخطی و ناسازگاری در به روز رسانی اطلاعات دارد . علاوه بر این، تعریف این فناوری برای تمام اشیاء جهان ساده نخواهد بود . مهمترین چالش این راه حل ، کنترل آنی است . کنترل آنی یعنی ارتباط بین اشیاء سیستم (IoT مشاهده، تحلیل ، و استخراج اطلاعات ) باید به صورت آنی انجام پذیرد [۲۵].

**۲-۷. اینترنت اشیاء باریک**

NB-IoT به تازگی به انجمن LPWAN پیوسته است[۲۶]. NB-IoT یک رابط رادیویی LPWAN است که از طیف و معماری مجاز سلولی استفاده می کند[۸-۱۰].

این سیستم از طریق یک کانال جهانی ۲۰۰ کیلوهرتز برای ارتباطات موبایلی (GSM) یا یک بلوک منابع فیزیکی LTE (PRB) 180 کیلوهرتز کار می کند[۱۱].

باید یکی از این سه حالت رخ دهد:

به تنهایی ، بیش از یک کانال ۲۰۰ کیلوهرتز در طیف GSM ،

درون باند ، بیش از یک PRB واحد در مجموعه PRB های LTE ،

بند محافظ ، در داخل یک بند محافظ در بین مجموعه های مختلف PRB های LTE.

امروزه ، بسیاری از اپراتورهای تلفن همراه شبکه های NB-IoT را در سراسر جهان راه اندازی می کنند[۲۷]، در حالی که جامعه پژوهشی به چندین جنبه نظری با هدف دستیابی به راه حل هایی برای بهینه سازی سیستم می پردازد[۱۱].

در مورد همه فن آوری های بی سیم، اعتبار چنین راه حل هایی اغلب از طریق شبیه سازی انجام می شود ، بنابراین به مفروضات مدل سازی واقعی نیاز دارد[۱۱].

با توجه به اکو سیستم متنوع اینترنت اشیاء در آن چندین فناوری بی سیم توسعه داده شده است. برخی از این فناوری ها استاندار(به عنوان مثال بلوتوث و LoRaWAN) هستند و مدام در حال ارائه می باشند[۲۶].

اکوسیستم بسیار متنوع اینترنت اشیا در نتیجه تبلیغات اینترنت اشیا و افزایش سرمایه متقابل متقابل به شرکت ها و شرکت های نوپا ایجاد شده است. همه آنها الزامات را برآورده می کنند - یا حداقل سعی می کنند توسط مجموعه ای از برنامه های کاربردی که مرزهای آنها توسط محدودیت های تکنولوژیکی شکل می گیرد، ایجاد شوند[۲۶].

تطبیق برنامه های در حال ظهور با فناوری های موجود به یکی از چالش های اصلی ابتکارات اینترنت اشیا تبدیل شده است، به ویژه هنگامی که فناوری جدیدی در چشم انداز ظاهر می شود و نقشه باید دوباره ترسیم شود[۲۶].

یکی از اولین برنامه های اینترنت اشیا که ارزش پیشنهادی واضحی از خود نشان داد، اندازه گیری هوشمند بود[۲۶].

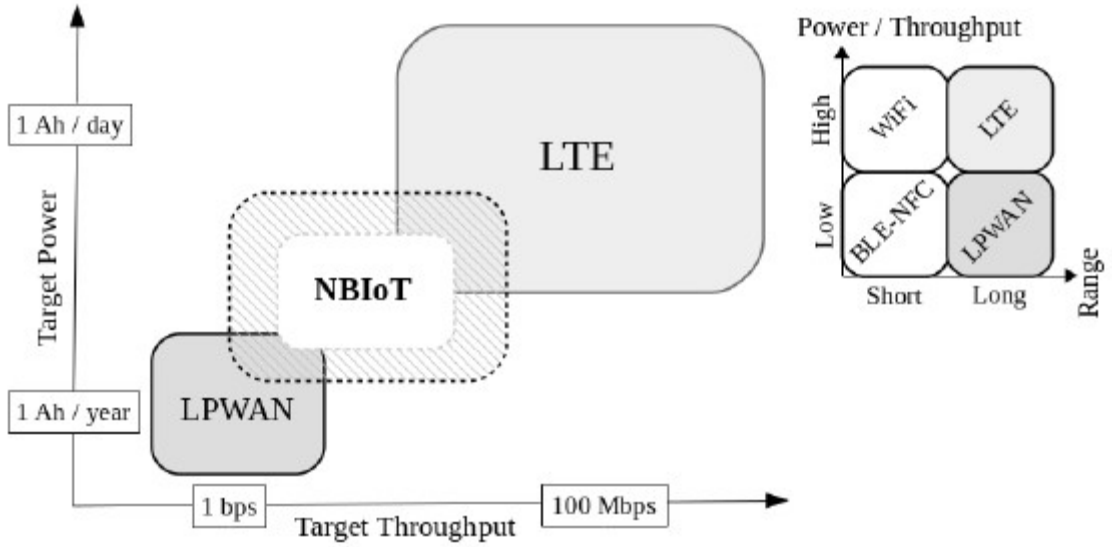
دسترسی از راه دور بدون دخالت به دستگاه های کنترلی امکان کاهش فاصله بین قرائت ها را فراهم می آورد، بنابراین خدمات جدیدی را برای کاربران (مانند قیمت گذاری پویا و تجزیه و تحلیل الگوهای استفاده) و اپراتورها (مانند تعادل بار بین چندین کاربر) ایجاد می کند[۲۶].

NB-IoT به عنوان افزونه LTE، در آن چارچوب تصور شد و مجموعه ای از مشخصات را نشان می دهد که به ویژه برای اندازه گیری هوشمند مناسب می باشد[۲۶].

به عنوان مثال، در مقایسه با LTE ، برخی از محدودیت ها برطرف شده است. دستگاه های NB-IoT به صورت ثابت دیده می شوند، فقط تکه های کوچکی از داده ها به صورت متناوب منتقل می شوند و برنامه ها به عنوان مقاوم در برابر تاخیر پیش بینی می شوند[۲۶].

در حالی که سایر ویژگی ها در NB-IOT نسبت به LTE تقویت شدند. تعداد زیادی دستگاه برای قرار دادن (چندین مرتبه بزرگتر از دستگاه های LTE)، اغلب در مکانهایی با پوشش ضعیف (به عنوان مثال، زیرزمین ساختمانها) و یا بدون منبع تغذیه با طول عمر معقول خدمات ارائه می دهند[۲۶].

در شکل ۲-۵ مدل NB-IoT را نمایش می دهد.




شکل ۲-۵ مدل NB-IoT

**۲-۸ . پیشینه پژوهش**

قبل از اشتراک داده ها، تأیید حقانیت هویت وسیله نقلیه ضروری تلقی می شود. در سال ۲۰۲۱ نویسندگان مرجع [۱۸] استفاده از یک سیستم مبتنی بر خوشه و عاری از هزینه های اضافی زیربنایی، یک پروتکل احراز هویت سبک و سریعتر پیشنهاد داده اند. علاوه بر این، در هنگام تأیید اعتبار و اختصاص اولویت عبور در روش پیشنهادی ، خدمات ویژه ای به وسایل نقلیه اضطراری ارائه می شود. تمام ارتباطات بلاکچین با استفاده از اینترنت پرسرعت 5G انجام می شود در حالی که اطلاعات رمزگذاری شده هنگام استفاده از الگوریتم امضای دیجیتال1024 -RSA برای بهبود امنیت، یکپارچگی و رازداری منتقل می شود. علاوه بر این، تجزیه و تحلیل عددی نشان می دهد که پروتکل های انتقال یافته پیشنهادی از نظر MAC و روش های معیار سنتی از نظر توان عملیاتی، تاخیر و میزان افت بسته عملکرد بهتری دارند.

در سال ۲۰۲۰ و در مرجع [۲۸] ترکیبی از رمزنگاری مبتنی بر هویت و مکانیسم امضای استفاده ارائه شده است. در زمان شبیه سازی حریم خصوصی بدون قید و شرط تحت حمله کامل قرار گرفته است. در این پژوهش همانند طرح های احراز هویت معمولاً هزینه محاسباتی بالایی دارد.

در سال ۲۰۲۰ در مرجع [۲۹] مکانیزم ارتباطی ایمن مبتنی بر  سرویس محاسبات ابری طراحی می گردد. در مدل پیشنهادی بلاکچین برای ذخیره سوابق پاداش و مجازات در مورد به اشتراک گذاری داده ها استفاده می شود. علاوه بر این، به منظور

محافظت از امنیت ارتباطات وسایل نقلیه در برابر وسایل نقلیه مخرب ، استراتژی ردیابی مربوطه نیز پیشنهاد می شود. با این حال، در طرح پیشنهادی اشاره ای به سیاست دسترسی نشده است ، کنترل دسترسی داده های بارگذاری شده بدون توجه به خواسته های صاحب داده ، به CSP بستگی دارد.

در سال ۲۰۲۰ نویسندگان مرجع [۳۰] یک طرح قابل تأیید برای دستیابی به اشتراک داده ها پیشنهاد می کند. استراتژی پنهان سازی سیاست برای پنهان کردن حریم خصوصی شخص صاحب داده طراحی می نماید. با توجه به ظرفیت ذخیره سازی کم و قدرت محاسباتی وسایل نقلیه ، عملی بودن تقسیم داده ها یا نگهداری از طریق مکانیسم سازگاری برای وسایل نقلیه عملی نیست.

در مرجع [۳۱]، سیستمی مبتنی بر فناوری Blockchain پیشنهاد شده است تا مشکل ارزیابی قابلیت اطمینان شرایط ترافیکی که توسط وسایل نقلیه پخش می شود را حل کند. در این سیستم ، اطلاعات جاده ای که از طریق وسایل نقلیه پخش می شوند می توانند توسط وسایل نقلیه مجاور به دست بیایند تا امتیاز اعتماد را بدست آورند. تجهیزات کنار جاده ای۶ داده ها را جمع آوری می کند و هرکدام اطلاعات را در یک بلوک بسته بندی می کنند و سعی می کنند آن را به Blockchain اضافه کنند. این سیستم تعامل بین وسایل نقلیه را تقویت کرده و از تأیید هویت متقابل بین وسایل نقلیه برای مطابقت با اطلاعات پخش شده از شرایط ترافیکی استفاده می کند. اما در این سیستم ، آیا هویت وسیله نقلیه صحیح است یا خیر، نمی توان تضمین کرد. علاوه بر این ، از نظر گزارش جاده اگر یک RSU منفرد و به تنهایی مورد حمله قرار بگیرد، مهاجم محتوای جمع آوری شده خود را تغییر دهد، ممکن است باعث پنهان شدن یا دستکاری در مورد اطلاعات جاده شود و در نتیجه باعث نادرست شدن جاده شود.

در مرجع [۳۲]، سیستم جمع آوری و تجزیه و تحلیل ویدیو مبتنی بر ابر به نام Kestrel طراحی شده است ، که از ویژگی های بصری ارزان برای استخراج صفات استفاده می کند. این مشکل ابهام مسیر را با همراهی با توصیف کننده های بصری وسیله نقلیه حل می کند و در عین حال مانیتورینگ مداوم را در یک شبکه دوربین ناهمگن متشکل از سیستم دوربین ثابت و دوربین در دستگاه های تلفن همراه انجام می دهد. اگر یک سیستم جستجو بر اساس هویت کاربر ایجاد شود، مدیریت اطلاعات در مورد جاده می تواند سودمند باشد اما در عین حال این مدیریت احتمال دارد حریم خصوصی ارائه دهندگان فیلم ها و تصاویر جاده ها را تهدید کند. اما اگر یک سیستم مدیریتی منظم و جامع وجود نداشته باشد، ممکن است پیدا کردن افراد دشوار است. البته کاربران وسیله نقلیه به عنوان شاهد نمی دانند که می توان از فیلم های آنها به عنوان مدرک استفاده کرد. بنابراین، لازم است که یک سیستم جمع آوری اطلاعات ترافیکی با حفظ حریم خصوصی ایجاد شود ، که وسیله نقلیه را قادر می سازد هنگام رانندگی ، فیلم ها و اطلاعات جاده ای را به صورت ناشناس بارگذاری کند[۳۳].

در مرجع [۳۳] یک سیستم خدمات عمومی خودکار، Viewmap را پیشنهاد کرد که می تواند فیلم های DashCam را به صورت ناشناس به اشتراک بگذارد. DashCam یک دوربین مجهز به وسیله نقلیه است که می تواند صحنه های اطراف وسیله نقلیه را ضبط کند. به منظور محافظت از حریم شخصی کاربران ، هر فیلم به عنوان نمای نمایش (VP) نمایش داده می شود.Anonymous VP جای صاحب خود را برای شرکت در بازیابی، اعتبار سنجی و پاداش سیستم می گیرد. به اعضای معتبر سیستم نمرات اعتماد داده می شوند. روش مدیریت اعتماد توزیع شده به کاربران امکان می دهد در حالی که در منبع قابل ردیابی نیستند ، پول نقد مجازی دریافت کنند و ناشناس بودن مسیر وسایل نقلیه ویدیویی را حفظ کنند. سیستم مدیریت اعتماد نه تنها

6 Road Side Unit (RSU)

می تواند فیلمهایی را برای کسب مدارک در زمینه تصادفات رانندگی جمع آوری کند ، بلکه از آن برای تحلیل شرایط زمان واقعی جاده نیز استفاده می شود.

در مرجع [۳۴] روشی خاص برای تسهیل ضبط و اشتراک گذاری فیلم برای وسایل نقلیه در حال حرکت را بر اساس G-VANET۵ ارائه می گردد. این برنامه به خودروها اجازه می دهد فیلم های جاده ای را از طریق برنامه های تأیید اعتبار خودرو و رمزگذاری ویدیو بارگذاری و بارگذاری کنند. این محافظت از هویت وسیله نقلیه شرکت کننده و حفظ حریم خصوصی محتوای ویدیو به شکل همزمان است.

در یک روش همجوشی۷ داده ها به نام تست نسبت وزنی متوالی (WSRT۸) برای مقابله با حملات Byzantine پیشنهاد شد. در معماری ad hoc هر گره ارزیابی طیف فرکانسی دارد و برای اینکار اقدام به جمع آوری داده‌ها و تهیه گزارش از ارزیابی گره های همسایه می‌کند. روش WSRT از دو مرحله اصلی تشکیل شده است:

اولین مرحله نگهداری اعتبار که در آن هر گره در ابتدا دارای ارزش اعتباری صفر است، پس از هر گزارش طیف محلی درست، ارزش اعتبار ۱ واحد افزایش خواهد یافت. مرحله دوم آزمون فرضیه گام های واقعی از WSPRT است که بر اساس آزمون نسبت احتمال متوالی محاسبه می‌شود۹[۳۵].

مؤلفان در مرجع [۳۶] در جهت تغییر به سمت معماری غیر متمرکز برای دوام پذیر کردن اکوسیستم وسیله IoT در حال گسترش عمل کرده اند. هزینه نگهداری مدل متمرکز کنونی از طرف تولید کننده بسیار بالا است، توزیع بروزرسانی های نرم افزاری برای میلیون ها وسیله را سال ها بعد از عدم ادامه تولید آنها در نظر بگیرید. در سمت سرویس گیرنده، به وسایلی که در پس زمینه «با منزل تماس می گیرند» کمبود اعتماد تعدیل یافته ای وجود دارد و یک رویکرد «امنیت از طریق شفافیت» نیاز است. این مسائل با یک مدل نظیر به نظیر بدون اعتماد مقیاس پذیر که می تواند به صورت شفاف عمل کند و داده ها را ایمن توزیع کند قابل حل هستند. مؤلفان به درستی اشاره می کنند که یک بلاک چین راه حل زیبایی را برای این مسئله ارائه می کند.

7 Fusion

8 Weighted Sequential Ratio Test

9 Sequential Probability Ratio Test

جدول ۲-۱ مقایسه پیشینه تحقیق

| مرجع | سبک مدیریت | روش | مزایا | معایب |
|---|---|---|---|---|
| [۱۸] | سیستم مدیریت اعتماد توزیع شده | یک سیستم مبتنی بر خوشه و عاری از هزینه های اضافی زیربنایی، یک پروتکل احراز هویت سبک و سریعتر پیشنهاد شده است. | از نظر توان عملیاتی، تاخیر و میزان افت بسته عملکرد بهتری دارند. | رمزگذاری / رمزگشایی مکرر باعث افزایش ترافیک می شود. |
| [۲۸] | سیستم مدیریت اعتماد توزیع شده | در مرجع ترکیبی از رمزنگاری مبتنی بر هویت و مکانیسم امضای استفاده شده است. | در زمان شبیه سازی حریم خصوصی بدون قید و شرط تحت حمله کامل قرار گرفته است. | در این پژوهش همانند طرح های احراز هویت معمولاً هزینه محاسباتی بالایی دارد. |
| [۲۹] | سیستم مدیریت اعتماد توزیع شده | مکانیزم ارتباطی ایمن مبتنی بر سرویس محاسبات ابری طراحی می گردد. | از بلاکچین برای ذخیره سوابق پاداش و مجازات در مورد به اشتراک گذاری داده ها استفاده می گردد. به منظور محافظت از امنیت تبادل اطلاعات و ارتباطات وسایل نقلیه در برابر وسایل نقلیه مخرب، استراتژی ردیابی پیشنهاد می شود. | با این حال، در طرح پیشنهادی اشاره ای به سیاست دسترسی نشده است ، کنترل دسترسی داده های بارگذاری شده بدون توجه به خواسته های صاحب داده ، به CSP بستگی دارد. |
| [۳۰] | سیستم مدیریت اعتماد توزیع شده | طرح قابل تأیید برای دستیابی به اشتراک داده ها پیشنهاد می کند. | استراتژی پنهان سازی سیاست برای پنهان کردن حریم خصوصی شخص صاحب داده طراحی می نماید. | با توجه به ظرفیت ذخیره سازی کم و قدرت محاسباتی وسایل نقلیه ، عملی بودن تقسیم داده ها یا نگهداری از طریق |

| | | | | |
|---|---|---|---|---|
| | | | | مکانیسم سازگاری برای وسایل نقلیه عملی نیست. |
| [۳۱] | سیستم مدیریت اعتماد توزیع شده | مشکل ارزیابی قابلیت اطمینان شرایط ترافیکی که توسط وسایل نقلیه پخش می شود | تعامل بین وسایل نقلیه را تقویت کرده و از تأیید هویت متقابل بین وسایل نقلیه برای مطابقت با اطلاعات پخش شده از شرایط ترافیکی استفاده می کند | آیا هویت وسیله نقلیه صحیح است یا خیر، نمی توان تضمین کرد. |
| [۳۲] | سیستم مدیریت اعتماد متمرکز | سیستم جمع آوری و تجزیه و تحلیل ویدیو مبتنی بر ابر به نام Kestrel | ویژگی های بصری ارزان جهت استخراج صفات | پردازش سنگین به علت مانیتورینگ مداوم شبکه |
| [۳۳] | سیستم مدیریت اعتماد متمرکز | سیستم جمع آوری اطلاعات توسط رانندگان خودروها | حفظ حریم خصوصی و ناشناس ماندن شخص ارسال کننده | به علت ناشناس ماندن ممکن است اطلاعات جعلی ارسال گردد. |
| [۳۴] | سیستم مدیریت اعتماد متمرکز | تأیید اعتبار خودرو و رمزگذاری ویدیو | محافظت از هویت وسیله نقلیه شرکت کننده و حفظ حریم خصوصی محتوای ویدیو به شکل همزمان | پر هزینه بودن فرآیند |
| [۳۵] | سیستم مدیریت توزیع شده | مقابله با حملات Byzantine در معماری ad hoc | جمع آوری داده‌ها و تهیه گزارش از ارزیابی گره های همسایه | مبتنی بر احتمال می باشد و دقت کافی را ندارد. |
| [۳۶] | سیستم مدیریت توزیع شده | خدمات پس از فروش بروز رسانی نرم افزارهای محصولات مبتنی بر اینترنت اشیاء | استفاده از بلاک چین جهت افزایش امنیت | هزینه نگهداری مدل متمرکز کنونی از طرف تولید کننده بسیار بالا |

# فصل سوم: الگوریتم پیشنهادی

### ۳-۱. مقدمه

تکنولوژی زنجیره بلوک[10] تکنولوژی دفتر کل توزیع شده که به طور مداوم بروز گردیده و هرگونه معامله در یک شبکه نظیر به نظیر را بدون تغییر و دستکاری ثبت می نماید. این تکنولوژی شفاف است و می تواند معاملات را بدون تمرکز پردازش نماید.

بلاک چین یک دفتر کل امن، پراکنده، شفاف، غیرقابل تغییر و قابل حسابرسی را مهیا می‌کند. بلاک چین را می‌توان به دو صورت آزاد و کامل جهت دسترسی به همه معاملاتی که از زمان اولین معامله در سیستم صورت گرفته است، استفاده نمود و در هر زمانی توسط هر نهادی قابل بازبینی و تطبیق می باشد. پروتکل بلاک چین اطلاعات را در زنجیره‌ای از بلاک‌ها ذخیره و نگهداری می کند که هر بلاک نیز مجموعه‌ای از معاملاتی است که در زمان مشخص و معین رخ داده است. بلاک‌ها با ارجاع به بلاک قبلی به هم متصل شده و زنجیره‌ای را تشکیل می‌دهند[۱].

در دهه نود میلادی الگوریتمی به نام کلونی مورچگان توسط Dorigo و همکارانش به عنوان یک رویکرد جدید متاهوریستی الهام گرفته از طبیعت برای حل مسائل بهینه سازی همبستگی ارائه شد.

ابتدا الگوریتم برای مسئله فروشنده در سفر استفاده شد. اخیراً ، برای بهبود عملکرد و همچنین استفاده از آن در سایر مشکلات بهینه سازی ، تمدید و یا اصلاح شده است.

الگوریتم بهینه سازی کلنی مورچه ها اساساً سیستمی مبتنی بر افراد است که رفتار طبیعی مورچه ها را شبیه سازی می کند ، از جمله مکانیزم های همکاری و سازگاری، منبع الهام بخش ACO رفتار جستجوی مورچه های واقعی است. در این پایان ضمن ترکیب الگوریتم کلونی مورچگان با ساختار بلاک چین رهیافت پیشنهادی امنیت NB-IoT را بهبود می بخشد.

### ۳-۲. روش پیشنهادی

با توجه به اینکه در این پایان از ترکیب الگوریتم کلونی مورچگان با ساختار بلاک چین در جهت تشخیص نفوذ در رایانش ابری ارائه می شود. لذا ابتدا معماری و ساختار الگوریتم کلونی مورچگان پیشنهادی مطرح و در ادامه ساختار بلاک چین بررسی می گردد. سپس مسئله فرمول بندی می گردد و روش پیشنهادی ارائه می گردد.

الگوریتم ACO بر اساس یک الگوی محاسباتی الهام گرفته از کلنی های مورچه واقعی و نحوه عملکرد آنها ساخته شده است. ایده استفاده از چندین مورچه محاسباتی سازنده است. بر اساس نتایج آزمایشات قبلی ذخیره شده در ساختار حافظه دینامیکی مورچه ، هر مورچه به محلول ساخته شده هدایت می شود. این الگو براساس مشاهده ای است که توسط متخصصان علوم اخلاقی در مورد محیط مورد استفاده مورچه ها برای انتقال اطلاعات در مورد کوتاه ترین مسیرهای رسیدن به غذا با استفاده از مسیرهای فرمونی انجام شده است. در حالی که یک مورچه جدا شده عملاً به طور تصادفی حرکت می کند ، اکتشاف ، مورچه ای که با یک ردیابی که قبلاً گذاشته شده بود می تواند آن را تشخیص دهد و با احتمال زیاد تصمیم به دنبال آن بگیرد ، بهره برداری کند و در نتیجه مسیر را با فرمون خاص خود تقویت کند. آنچه پدیدار می شود یک فرم است، فرآیند اتوکاتالیستی که از طریق آن هرچه مورچه ها بیشتر

10 Blockchain Technology

دنباله ای بروند ، دنباله رو جذابتر می شود. بنابراین این فرآیند با یک حلقه بازخورد مثبت مشخص می شود ، در طی آن احتمال انتخاب مسیر با تعداد مورچه هایی که قبلاً همان مسیر را انتخاب کرده اند افزایش می یابد. مکانیسم بالا الهام بخش الگوریتم های خانواده ACO است.

اطلاعات ابتکاری سطح فرومون پیمایش و گره با هم ترکیب می شوند و به اصطلاح قانون گذار احتمالی را تشکیل می دهند، نشانگر این احتمال است که مورچه k در مرحله زمانی t ویژگی i را در زیر مجموعه خود دارد:

رابطه (۳-۱)

$$P_i^k(t) = \begin{cases} \frac{[\tau_i(t)]^\alpha . [\eta_i]^\beta}{\sum_{u \in J^k} [\tau_u(t)]^\alpha . [\eta_u]^\beta} & if i \in J^k \\ 0 & otherwise \end{cases}$$

جایی که $J^k$ مجموعه ای از ویژگی های عملی است که مورچه k را می توان به زیر مجموعه آن اضافه کرد. همچنین $\tau_i$ مقدار فرمون و $\eta_i$ مقدار اطلاعات ابتکاری مرتبط با i می باشد. $\alpha$ نیز وزن نسبی فرمون و $\beta$ اطلاعات اکتشافی می باشد. که $\tau_i$ احتمال انتقال مورد استفاده توسط ACO تعادل بین شدت فرمون است (به عنوان مثال تاریخچه حرکتهای موفقیت آمیز قبلی) و $\eta_i$ اطلاعات ابتکاری (بیان کننده مطلوبیت حرکت) است. بهترین تعادل از طریق انتخاب مناسب پارامترهای α و β حاصل می شود. اگر α = 0 از اطلاعات فرمون استفاده نشود، به عنوان مثال تجربه جستجوی قبلی نادیده گرفته می شود. سپس جستجو به یک جستجو حریصانه تصادفی تنزل می یابد. به روزرسانی فرمون بخش مهمی برای کار مناسب الگوریتم ACO است. بعد از اینکه همه مورچه ها راه حل های خود را به پایان رساندند ، تبخیر فرمون در همه گره ها با استفاده از معادله (۳-۲) آغاز می شود و سپس طبق معادله (۳-۳) همه مورچه ها مقداری فرمون، i (t) را روی هر گره ای که استفاده کرده اند رسوب می دهند.

رابطه (۳-۲)

$$\tau_i(t) = (1-\rho)\tau_i(t)$$

رابطه (۳-۳)

$$\tau_i(t+1) = \tau_i(t) + \Delta\tau_i(t)$$

رابطه (۳-۴)

$$\Delta\tau_i(t) = \sum_{k=1}^{m} \Delta\tau_i^k(t)$$

که در آن m تعداد مورچه ها در هر تکرار است و $\rho \epsilon (0,1)$ضریب فروپاشی دنباله فرمون است. نقش اصلی تبخیر فرمون جلوگیری از رکود، یعنی وضعیتی است که در آن همه مورچه ها محلول یکسانی را می سازند. همه مورچه ها می توانند فرمون را طبق روابط (۳-۳) و (۳-۴) به روز کنند.

جایی که $\Delta\tau_i^k(t)$مقدار فرمونی است که توسط مورچه k در گره i در مرحله زمان t رسوب می کند، این مقدار بر طبق رابطه (۳-۵) محاسبه می گردد:

رابطه (۳-۵)

$$\Delta\tau_i^k(t) = \begin{cases} \varpi.\gamma\left(S^k(t)\right) + \phi.\left(\frac{n}{|S^k(t)|}\right) & if\ i\ \epsilon S^k(t) \\ 0 & Otherwise \end{cases}$$

جایی که $S^k(t)$ زیرمجموعه ویژگی است که توسط مورچه k در تکرار t پیدا می شود و $|S^k(t)|$طول آن است. فرمون با توجه به اندازه گیری عملکرد طبقه بندی شده، $\gamma\left(S^k(t)\right)$ و طول زیر مجموعه ویژگی به روز می شود. $\varpi$ و $\phi$ هم دو پارامتر عملکرد طبقه بندی شده و طول زیر مجموعه ویژگی ها می باشد. که$\varpi\epsilon[0,1]$ و همچنین $\phi = 1 - \varpi$ می باشد.

در ادامه ساختار بلاک چین طراحی می شود. در نهایت پس از اعمال ساختار بلاک چین و الگوریتم رمزنگاری مورد نظر به الگوریتم کلونی مورچگان اضافه می شود.

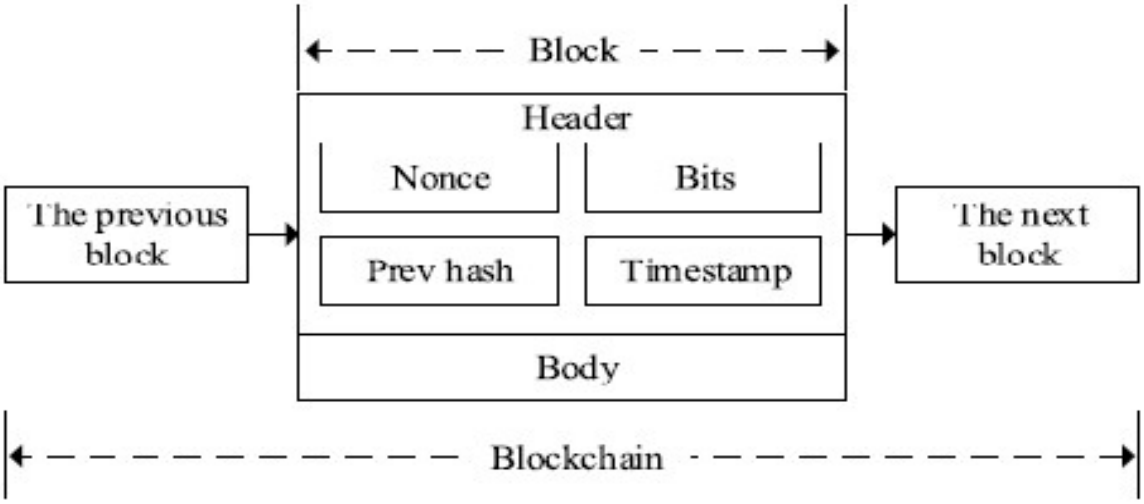
پیشرفت های اخیر در فناوری های بلاک چین فرصت هایی را برای غلبه بر محدودیت های تبادل اطلاعات مبتنی بر محاسبات ابری ایجاد می نماید. با این حال، ادغام بلاک چین با تبادل اطلاعات مبتنی بر محاسبات ابر هنوز هم در مراحل ابتدایی می باشد و تلاش های گسترده پژوهشی و تحقیقاتی جهت مقابله با تعداد بسیار از چالش های تحقیقاتی مورد نیاز است[۲].

مسائل امنیتی مانع اصلی برای بسیاری از کاربران است که هیچ نوع فعالیتی انجام نمی‌دهند. امنیت و حفظ حریم خصوصی در این دستگاه‌ها امری ممکن است که باید با دقت کافی، توجه به جزییات، انتخاب و استفاده از ابزارهای مناسب برای داده‌های کاربران و سایر داده‌ها انجام گیرد[۳].

یکی از مسائل مهم در صنعت اینترنت اشیا حفظ امنیت و حریم خصوصی است که بلاک‌چین توانسته در بهبود حریم خصوصی در برنامه‌های اینترنت اشیا کمک به حفظ حریم شخصی کند. در یک سیستم ابری می‌توان پیشنهاد داد که یک معماری خاصی طراحی شود تا افراد با استفاده از بلاک‌چین بتوانند به صورت غیرمتمرکز به ایجاد یک شبکه توزیع دستگاه پرداخته و در این روش از هیچ شخص ثالثی استفاده نشود.با گسترش تلفن همراه و خدمات مربوط به آن‌ها آسیب پذیری تعدادی از فیلترهای ضد تروجان برای شناسایی فایل‌های مشکوک از طریق الگوهای تطبیق پیشنهاد می‌شود که یک سرور مرکزی برای ذخیره و بروزرسانی الگوهای ویروس می‌باشد. این اقدامات برای ورود مهاجمان آسیب‌پذیر می‌باشد. بلاک‌چین می‌تواند به بهبود امنیت شبکه‌های توزیع کمک کند و در جهت برقراری زیرساخت‌های امنیتی بسیار مورد استفاده قرار گیرند[۴].

ابتدا ساختار بلاک چین دو بعدی مورد استفاده در این پژوهش مطرح می شود. یک Blockchain (همانگونه که در شکل ۳-۱ نشان داده شده است) یک پایگاه داده توزیع شده می باشد. در هر Blockchain یک لیست در حال رشد از بلوک های زنجیر شده به یکدیگر قرار دارند که یک دفترچه اصلی را بدون یک پایگاه داده متمرکز مبتنی بر گره های توزیع شده حفظ می کند.

ساختار Blockchain ، مبتنی بر یک شبکه توزیع شده نظیر به نظیر است که در آن هر گره با استفاده از یک کلید عمومی (PK) مشخص و مدیریت می شود. ارتباطات بین گره ها، توسط PK ها رمزگذاری می شوند و به کل شبکه پخش می شوند. هر گره می تواند یک اعتبار را با اعتبار امضای تولیدکننده فرآیند در برابر PK خود تأیید کند. در ساختار Blockchain هر بلاک از بلاک قبلی و بعدی خود مطلع است. در روش پیشنهادی از بلاک ها در جهت افزایش امنیت شبکه مبتنی بر محاسبات ابری استفاده می شود.



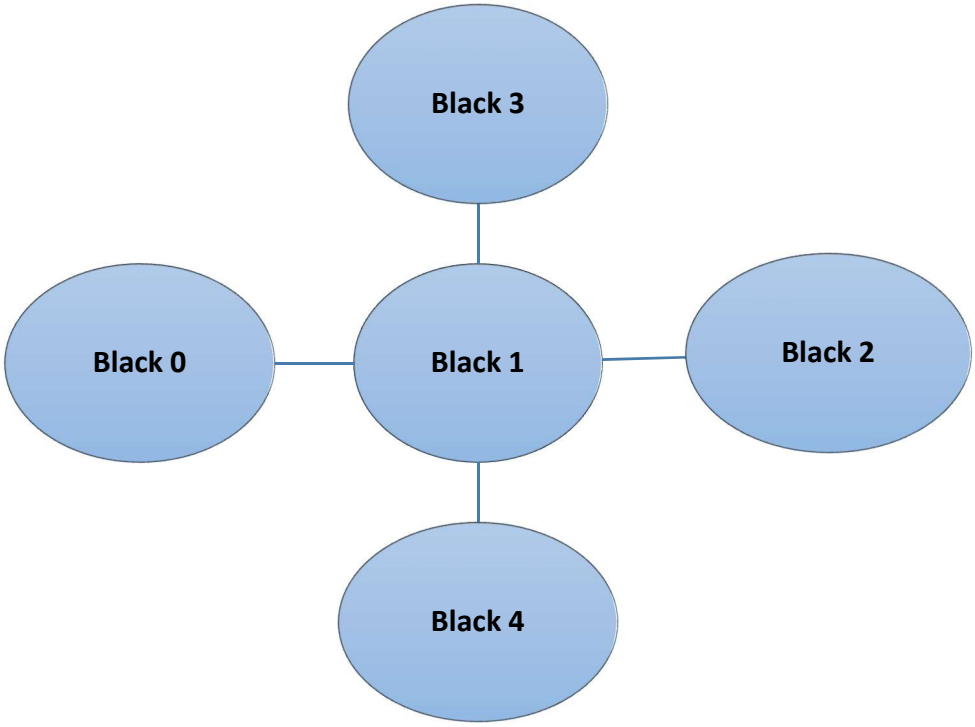

شکل ۳-۱. ساختار یک Blockchain [۵]

با توجه به ویژگی های غیر متمرکز و تغییر ناپذیر Blockchain، یک چارچوب امنیتی مبتنی بر Blockchain جهت پشتیبانی از خدمات محاسبات ابری، جهت افزایش امنیت می تواند چالش مطرح شده را تا حدی حل نماید.

بر اساس توضیحات داده شده در زمینه بلاک چین و ویژگی های آن باید در ساختار بلاک چین از یک روش بهینه رمزنگاری نامتقارن مناسب با شرایط شبکه بهره گرفت. در واقع بر اساس شکل ۳-۱ قسمت اصلی بدنه بلاک چین بخش رمزنگاری می باشد.

ترکیب الگوریتم رمز نگاری چند هدفه مبتنی بر Blockchain در افزایش امنیت محاسبات ابری تواند موثر واقع گردد.

ساختار بلاک چین پینشهادی دو بعدی است و هر بلاک دارای بلاک بالایی، بلاک پایینی، بلاک سمت چپ و بلاک سمت راست در صورت وجود مطابق شکل ۳-۲ می باشد.




شکل ۳-۲: ساختار همسایه ها هر بلاک

همانگونه که در شکل ۳-۲ مشخص است هر بلاک چین می تواند در چهار سمت بالا، پایین، چپ و راست خود بلاک های همسایه ای که هر کدام از آنها یک نیز یک بلاک  هستند داشته باشد. هر بلاک در این ساختار از شکل ۳-۱ به عنوان معماری اش تبعیت می نماید.

رمزنگاری سبک وزن به دلیل فراگیر بودن سامانه‌ها، حریم خصوصی کاربران در معرض تهدید است و محدودیت‌های شدیدی در منابع محاسباتی، تغذیه، حافظه، توان مصرفی و هزینه نیز حاکم می‌باشد. با توجه به گسترش محاسبات ابری، حفظ امنیت آن بیش از پیش احساس می‌شود. موضوع حفظ حریم خصوصی و امنیت همیشه یک مسئله مهم در این زمینه به حساب می‌آید. همچنین فناوری بلاک چین از طریق ایجاد امکان توزیع اطلاعات دیجیتال بدون کپی کردن، ستون فقرات نوع جدیدی از خدمات ارائه شده در اینترنت می‌باشد.

یکی از سیستم هایی که در سالهای اخیر، برای انجام عملیات رمزنگاری مورد استفاده قرار می گیرد، سیستم رمزنگاری مبتنی بر منحنی بیضوی است .این سیستم رمزنگاری برای نخستین بار در اواخر دهه 80 توسط کوبلیتز ارائه شد. به دلیل کوتاه بودن طول کلید و سطح بالای امنیتی آن، یکی از بهترین سیستم های رمزنگاری می باشد .از مزایای این سیستم نسبت به دیگر سیستمهای رمزنگاری، می توان به مواردی چون دارا بودن بالاترین درجه محرمانگی به ازای هر بیت، نیاز به حافظه کمتر، توان مصرفی کمتر و کاهش پهنای باند مورد نیاز سیستم اشاره کرد.

از مهمترین و بارز ترین ویژگی این الگوریتم انجام عملیات روی میدان های متناهی ایست.

در نهایت در روش پیشنهادی ساختار بلاک چین با الگوریتم کلونی مورچگان ترکیب و در نهایت ساختار و الگوریتم پیشنهادی در شکل ۳-۱ و همچنین شکل ۳-۲ ارائه می شود. در شکل ۳-۱ ساختار بلاک چین تعریف و الگوریتم کلونی مورچگان بر روی آن اعمال و در نهایت الگوریتم رمزنگاری ECC فراخوانی می گردد. سپس در شکل ۳-۴ روش رمزنگاری ECC فراخوانی و اجرا می شود.

**الگوریتم ۳-۱ ترکیب روشهای کلونی مورچگان و بلاک چین**

Begin

Start Initialize all parameters $\alpha, \beta, \rho, \mathrm{m}, \tau_0, \phi, \varpi, T$

Start Initialize BlackChain in pic 3-2.

t = 1.

for Each node i do

$\tau_i(t) = \tau_0$

end for

Place m ants, k = 1 to m. // Initialize a population of ants with random positions

while t <=T do

for Each ant k = 1 to m do

$S^k(t) = \{\ \}$

while Ant is able to increase the detection rate do

From current node, select next node i using Equation (3-1).

Add node i to subset $S^k(t)$.

end while

Calculate the subset length $|S^k(t)|$.

Calculate the $\gamma\left(S^k(t)\right)$:

end for

for Each node i do

Apply pheromone evaporation using Equation (3-2).

Calculate $\Delta\tau_i(t)$ using Equations (3-4,3-5).

Update pheromone using Equation (3-3).

end for

t = t + 1

end while

Return the subset $S^k(t)$ with highest $\gamma\left(S^k(t)\right)$ as the solution.

Call ECC( );

End

همچنین در شکل ۳-۲ ساختار رمزنگاری پیشنهادیECC مطرح می شود.

**الگوریتم ۳-۲ ساختار رمزنگاری پیشنهادی [۶]**

Begin

Generete Public_Key,Pricate_Key,Secret_Key

For each Data to

$$C(t)_1 = \left((K \coloneqq 1,2,3,\dots,n-1) * p_c\right) + \gamma_K$$

$$C(t)_2 = O_d + \left((K \coloneqq 1,2,3,\dots,n-1) * \alpha_K\right) + \gamma_K$$

$$O_d = \left((C(t)_2 - \beta_K) * C(t)_1\right) - \gamma_K$$

End For

End

در اینجا، $C(t)_1$ و $C(t)_2$دو متن رمزنگاری شده، K-تعداد تصادفی بین ۱ تا n-1 و داده های اصلی $O_d$ ایجاد می شود.

که $\alpha_K$ کلید عمومی، $\beta_K$ کلید خصوصی و $\gamma_K$ هم کلید مخفی می باشد. $p_c$نقطه روی منحنی می باشد.

**۳-۳. نتیجه گیری**

در روش پیشنهادی از ترکیب الگوریتم کلونی مورچگان و ساختار بلاک چین استفاده شده است. ابتدا الگوریتم کلونی مورچگان ارائه و پس از آن الگوریتم رمزنگاری ECC بر روی ساختار بلاک چین دوبعدی اعمال گردیده است. در ادامه و در فصل چهارم روش پیشنهادی در نرم افزار OMNET++ پیاده سازی و نتایج شبیه سازی مطرح می شود.

## منابع:


[١] S. Mukherjee and G. Biswas, "Networking for IoT and applications using existing communication technology," Egyptian Informatics Journal, vol. 19, no. 2, pp. 107-127, 2018.

[٢] A. Felfernig et al., "An overview of recommender systems in the internet of things," Journal of Intelligent Information Systems, vol. 52, no. 2, pp. 285-309, 2019.

[٣] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures ",IEEE Access, vol. 7, pp. 82721-82743, 2019.

[٤] B. Afzal, M. Umair, G. A. Shah, and E. Ahmed, "Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges," Future Generation Computer Systems, vol. 92, pp. 718-731, 2019.

[٥] H. Malik et al., "Radio resource management in NB-IoT systems: Empowered by interference prediction and flexible duplexing," IEEE Network, vol. 34, no. 1, pp. 144-151, 2019.

[٦] L. Cavo, S. Fuhrmann, and L. Liu, "Design of an area efficient crypto processor for 3GPP-LTE NB-IoT devices," Microprocessors and Microsystems, vol. 72, p. 102899, 2020.

[٧] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," ieee communications surveys & tutorials, vol. 19, no. 2, pp. 855-8.٢٠١٧ ,٧٣

[٨] O. Liberg, M. Sundberg, E. Wang, J. Bergman, J. Sachs, and G. Wikström, Cellular Internet of Things: From Massive Deployments to Critical 5G Applications. Academic Press, 2019.

[٩] Y.-P. E. Wang et al., "A primer on 3GPP narrowband Internet of Things," IEEE communications magazine, vol. 55, no. 3, pp. 117-123, 2017.

[١٠] J. Xu, J. Yao, L. Wang, Z. Ming, K. Wu, and L. Chen, "Narrowband internet of things: Evolutions, technologies, and open issues," IEEE Internet of Things Journal, vol. 5, no ,٣ .pp. 1449-1462, 2017.

[١١] G. Caso, Ö. Alay, L. De Nardis, A. Brunstrom, M. Neri, and M.-G. Di Benedetto, "Empirical Models for NB-IoT Path Loss in an Urban Scenario," IEEE Internet of Things Journal, 2021.

[١٢] J. Cao, P. Yu, X. Xiang, M. Ma, and H. Li, "Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9794-9805, 2019.

[١٣] H. Huang and L. Zhang, "Reliable and secure constellation shifting aided differential radio frequency watermark design for NB-IoT systems," IEEE Communications Letters, vol. 23, no. 12, pp. 2262-2265, 2019.

[١٤] W. S. Jeon, S. B. Seo, and D. G. Jeong, "Effective frequency hopping pattern for ToA estimation in NB-IoT random access," IEEE Transactions on Vehicular Technology, vol. 67, no. 10, pp. 10150-10154, 2018.

[١٥] A. Karaagac, E. Dalipi, P. Crombez, E. De Poorter, and J. Hoebeke, "Light-weight streaming protocol for the Internet of Multimedia Things: Voice streaming over NB-IoT," Pervasive and Mobile Computing, vol. 59, p. 101044, 2019.

[١٦] A. Rahman et al., "Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium," IEEE Access, vol. 8, pp. 209594-209609, 2020.

[١٧] M. Ahmed, "False image injection prevention using iChain," Applied Sciences, vol. 9, no. 20, p. 4328, 2019.

[١٨] A. Akhter, M. Ahmed, A. Shah, A. Anwar, and A. Zengin, "A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET," Sustainability, vol. 13, no. 1 ,p. 400, 2021.

[١٩] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," IEEE Access, vol. 7, pp. 56656-56666, 2019.

[٢٠] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," Internet of Things, vol. 10, p. 100081, 2020.

[٢١] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, 2019.

[٢٢] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for iot security," Digital Communications and Networks, vol. 6, no. 2, pp. 195-202, 2020.

[٢٣] C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare," in 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2012, pp. 922-926: IEEE.

[٢٤] M. Kavitha and P. V. Krishna, "IoT-Cloud-Based Health Care System Framework to Detect Breast Abnormality," in Emerging Research in Data Engineering Systems and Computer Communications: Springer, 2020, pp. 615-625.

[٢٥] L. M. Dang, M. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," Electronics, vol. 8, no. 7, p. 768, 2019.

[٢٦] B. Martinez, F. Adelantado, A. Bartoli, and X. Vilajosana, "Exploring the performance boundaries of NB-IoT," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5702-5712, 2019.

[٢٧] G. Association, "NB-IoT Deployment Guide to Basic Feature set Requirements," En ligne]. Disponible sur: https://www. gsma. com/iot/wp-content/uploads/2018/04/NB-IoT_Deployment_Guide_v2_5Apr2018. pdf.[Consulté le: 10-mai-201.٢٠١٩ ,[٩]

[٢٨] J. Li, Z. Zhang, L. Hui, and Z. Zhou, "A Novel Message Authentication Scheme With Absolute Privacy for the Internet of Things Networks," IEEE Access, vol. 8, pp. 39689-39699, 2020.

[٢٩] Y. Pu, T. Xiang, C. Hu, A. Alrawais, and H. Yan, "An efficient blockchain-based privacy preserving scheme for vehicular social networks," Information Sciences, vol. 540, pp. 308-324, 2020.

[٣٠] K. Fan et al., "A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks," IEEE Transactions on Vehicular Technology, 2020.

[٣١] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1495-1505, 2018.

[٣٢] T. Qiu, X. Wang, C. Chen, M. Atiquzzaman, and L. Liu, "TMED: A spider-Web-like transmission mechanism for emergency data in vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 67, no. 9, pp. 8682-8694, 2018.

[٣٣] M. Kim, J. Lim, H. Yu ,K. Kim, Y. Kim, and S.-B. Lee, "ViewMap: Sharing private in-vehicle dashcam videos," in 14th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 17), 2017, pp. 163-176.

[٣٤] T. Zhang, A. Chowdhery, P. Bahl, K. Jamieson, and S. Banerjee, "The design and implementation of a wireless video surveillance system," in Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, 2015, pp. 426-438.

[٣٥] T. Kieu-Xuan and I. Koo, "A Sequential Test Based Cooperative Spectrum Sensing Scheme Using Fuzzy Logic for Cognitive Radio Networks," in International Conference on Intelligent Computing, 2010, pp. 326-333: Springer.

[٣٦] P. Brody and V. Pureswaran, "Device democracy: Saving the future of the internet of things ", IBM, September, 2014.

[٣٧] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Future generation computer systems, vol. 88, pp. 173-190, 2018.

[٣٨] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, "Blockchain for cloud exchange: A survey," Computers & Electrical Engineering, vol. 81, p. 106526, 2020.

[٣٩] M. Movahednasab, B. Makki, N. Omidvar, M. R. Pakravan, T. Svensson, and M. Zorzi, "An energy-efficient controller for wirelessly-powered communication networks," IEEE Transactions on Communications, vol. 68, no. 8, pp. 4986-5002, 2020.

[٤٠] S. Zehir and M. Zehir, "Internet of things in blockchain ecosystem from organizational and business management perspectives," in Digital Business Strategies in Blockchain Ecosystems: Springer, 2020, pp. 47-62.

[٤١] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," IEEE Access, vol. 7, pp. 56656-56666, 2019.

[٤٢] D. V. K. Vengala, D. Kavitha, and A. S. Kumar, "Three factor authentication system with modified ECC based secured data transfer: untrusted cloud environment," Complex & Intelligent Systems, pp. 1-14, 2021.

Lib No.:MUT981421025

Degree: master of electrical engineering(M.Sc.)

Title: **Modeling and analysis of NB-IOT security risks and countermeasures in LPWAN networks**

Author: Mohsen.ahmadi

Supervisor: Dr.hosein.khaloeghi

Department: electrical engineering

Deta:

## Abstract:

In the name of God

Department of electrical engineering

**Modeling and analysis of NB-IOT security risks and countermeasures in LPWAN networks**

A Thesis

submitted in partial fulfillment of the requirements

for the degree of Master of Science (M.Sc.) in electrical engineering

By

**Mohamad.ahmadi**

Evaluated and approved by the Thesis Committee, on october. 21, 2021.

| NO. | Title | Responsibility | Signature |
|---|---|---|---|
| 1 | DR.r.khaloeghi | Supervisor(1) | |
| 2 | | Supervisor(2) | |
| 3 | | Advisor | |
| 4 | | Examiner(External) | |
| 5 | | Examiner (Internal) | |
| 6 | | DepartmentGraduate Coordinator | |

In the name of God

Department of electrical engineering

M.Sc.

Title

**Modeling and analysis of NB-IOT security risks and countermeasures in LPWAN networks**

By

**Mohsen.ahmadi**

Supervised by

**DR.r.khaloeghi**

**DR.S.PORSAJADI**

**october. 21, 2021**