کنترل دسترسی مبتنی بر اعتماد در اینترنت اشیاء صنعتی با به‌کارگیری زنجیره بلوکی

شیوا کریمیان[1]، سید غلامحسن طباطبایی[2]، رحیم اصغری[3]و*[1]

۱- کارشناسی ارشد مهندسی کامپیوتر گرایش رایانش امن، دانشگاه صنعتی مالک اشتر، تهران، ایران.

۲،۳- استادیار مجتمع دانشگاهی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر، تهران، ایران.

چکیده

با توجه به گسترش و پیشرفت روزافزون سامانه‌های هوشمند و نیاز به مدیریت یکپارچه و هماهنگی همه سامانه‌ها و دستگاه‌ها، نیاز هرچه بیشتر به گسترش و نوآوری در سامانه‌های اینترنت اشیاء احساس می‌شود. سامانه‌های مبتنی بر اینترنت اشیاء با توجه به افزایش بهره‌وری و کاهش نیاز به نظارت و عملگرهای نیروی انسانی، باعث کاهش سربارهای مالی و تجهیزات فنی سامانه‌ها می‌گردد و ازاین‌جهت در حوزه‌های صنعتی شاهد گسترش روزافزون این سامانه‌ها هستیم.

از اصلی‌ترین ملزومات گسترش بهره‌وری در حوزه‌های نرم‌افزاری و سخت‌افزاری سامانه‌ها برای کاربران، پایداری و صحت عملکرد سامانه‌ها و مهم‌تر از آن‌ها امنیت سامانه‌ها و اطلاعات در حال تبادل می‌باشد. چراکه در صورت وارد شدن آسیب به امنیت در سامانه اینترنت اشیا به دلیل اتصال حسگرهای مختلف با پروتکل‌های ارتباطی گوناگون و قابلیت اعمال تغییرات بر روی سامانه‌ها و دستگاه‌ها با استفاده از زیرساخت‌های اینترنت اشیا امکان از بین رفتن بانک‌های اطلاعاتی سامانه‌ها و اعمال تغییرات بر سامانه‌ها با قصد خرابکاری و آسیب رساندن تجهیزات و تحمیل هزینه‌های سنگین مادی و غیرمادی وجود دارد. در این پژوهش تلاش شده با بررسی اجزاء مختلف اینترنت اشیاء صنعتی و بررسی مسیرهای انتقال داده و پروتکل‌های آن‌ها نسبت به بررسی وضعیت امنیت آن‌ها و راهکارهای ارتقاء و بهبود امنیت مبتنی بر اعتماد گام‌های مؤثری برداشته شود.

کلمات کلیدی: اینترنت اشیاء، صنعتی، زنجیره بلوکی، کنترل دسترسی، امنیت سایبری، اعتماد.

۱. مقدمه

با توجه به نیاز استفاده از تجهیزات به‌روز و پیشرفته در صنعت به‌منظور افزایش بهره‌وری و افزایش سهم تجهیزات خودکارسازی در کنترل‌کننده‌های صنعت با چالش‌های گوناگونی ازجمله هزینه‌های اولیه بالا، پشتیبانی محدود، خدمات فنی ضعیف، عدم اعتماد به پایداری و صحت عملکرد در محیط‌های صنعتی و از همه مهم‌تر نگرانی از جهت میزان امنیت در این‌گونه تجهیزات و فناوری‌های نوین بوده که این موضوعات باعث کندتر شدن روند به‌روز شدن تجهیزات خودکارسازی و یکپارچه ساز می‌گردد. اینترنت و پروتکل‌های شناخته‌شده‌اش مدت‌هاست که در حال استفاده‌اند و به حالت پایدار رسیده‌اند. در مقابل اینترنت اشیا عمر چندانی ندارد و علاوه بر پروتکل‌های اینترنت، پروتکل‌ها و شیوه‌های ارتباطی گوناگون بی‌سیم و باسیم در یک شبکه وجود دارد که باعث پیچیده‌تر شدن شبکه ارتباطی و افزایش حوزه‌های امنیت می‌گردد. تفاوت مهم دیگر در این است که سخت‌افزارهای رایج در اینترنت با سخت‌افزارهای اینترنت اشیا تفاوت دارد. در سامانه‌های اینترنت اشیاء شاهد تجهیزات ارتباطی و مخابراتی با تنوع بسیار زیادی هستیم که در باندهای مختلف فرکانسی ارتباط برقرار می‌کنند. همچنین اولویت‌ها نیز در اینترنت اشیا

[1] **Corresponding author: Rahim asghari**
Email: meisam.mathhome@gmail.com

متفاوت است[۱,۲]. اینترنت اشیاء صنعتی یکی از راهکارهای پیشنهادی برای پیاده‌سازی کنترلر های یکپارچه باقابلیت کنترل و هدایت سامانه‌ها به‌صورت ریموت بوده که امروزه به جهت پشتیبانی بالا و انعطاف‌پذیری آن‌ها در نصب و بهره‌برداری در تجهیزات مختلف صنعتی از محبوبیت بالایی برخوردار می‌باشد. این تجهیزات بسته به کاربرد و نیازهای سامانه‌ها در انواع مختلفی در تنوع نرخ داده میزان مقاومت در برابر محیط‌های پر نویز صنعتی، شیوه‌های مختلف ارتباطی (باسیم و بی‌سیم) و پروتکل‌های مختلف ارتباطی می‌باشد. بسیاری از صنعت گران و تولیدکنندگان نسبت به سامانه‌های با فناوری‌های نوین به‌ویژه سامانه‌های اینترنت اشیاء را به دلیل اتصال تجهیزات درون شبکه‌های ارتباطی سلولی و یا ابری بسیار ناامن و غیرقابل‌اعتماد می‌دانند. درصورتی‌که وجود این تجهیزات در این مشاغل باعث نکات مثبت بسیار زیادی در حوزه بهره‌وری و افزایش راندمان مشاغل و قابلیت کنترل و مانیتورینگ می‌گردد و اعمال تغییرات را تحت شبکه ارتباطی میسر می‌سازد. با استفاده از راهکارهای امنیت دیجیتال و ارائه مستندات و نتایج آزمایش‌های عملیاتی این‌گونه تجهیزات امکان به دست آوردن اعتماد و نظر صاحبان مشاغل بسیار بیشتر می‌شود.

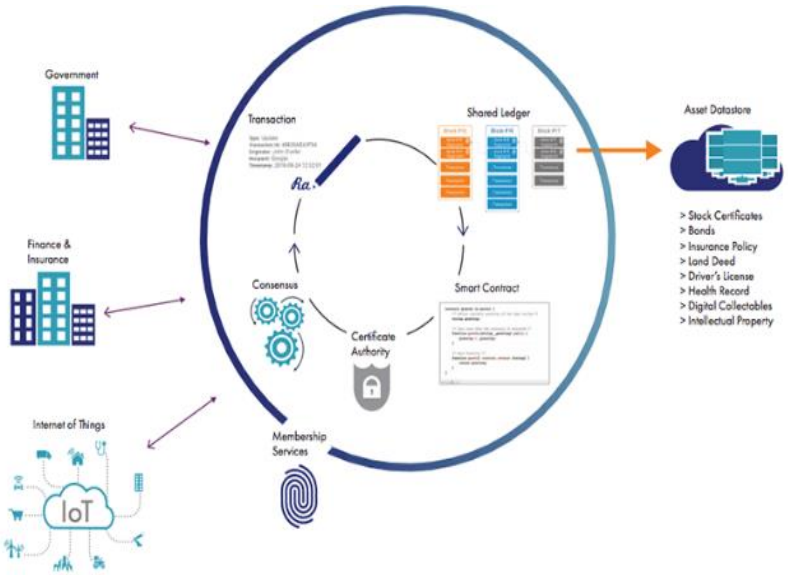
۲. فناوری زنجیره بلوکی و اینترنت اشیاء صنعتی

زنجیره بلوکی یک دفتر کل معاملات توزیع‌شده است که برای نگهداری سوابق تراکنش‌ها و عملیات استفاده می‌شود. این‌یک زنجیره به‌هم‌پیوسته از بلوک است که حاوی جزئیات مربوط به معاملات است. هنگامی‌که یک تراکنش جدید انجام می‌شود، یک بلوک با تمام جزئیات تراکنش مربوطه ایجاد می‌شود و سپس به بلوک‌های دیگر متصل می‌شود. اساساً یک سیستم توزیع‌شده را تشکیل می‌دهد که برخلاف بلوک‌های معمولی که دارای طراحی هاب مرکزی هستند، سطح بالایی از اتصال بین بلوک‌های تراکنش را دارد. ازآنجایی‌که زنجیره بلوکی‌ها توزیع و غیرمتمرکز هستند، مبادلات و تراکنش‌ها در سامانه‌های زنجیره بلوکی می‌توانند بدون تأیید سرور مرکزی انجام شوند؛ بنابراین، زنجیره بلوکی می‌تواند به‌طورکلی هزینه‌های سرور را کاهش دهد (با احتساب هزینه بهینه‌سازی و بهره‌برداری) و گلوگاه‌های اجرایی در سرور کانونی را کاهش دهد[۳, ۱۰].

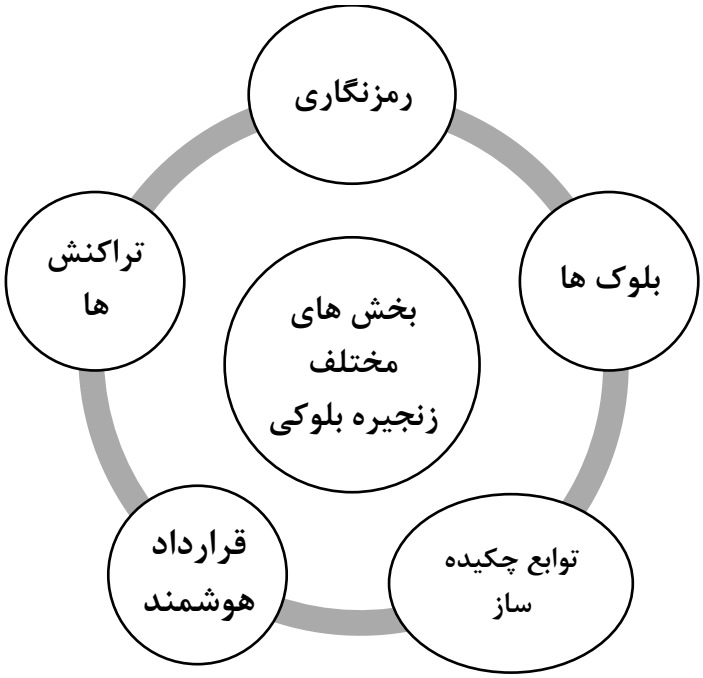
دست‌کاری داده‌ها در یک شبکه زنجیره بلوکی بسیار دشوار است زیرا بلوک‌ها به یکدیگر متصل هستند و کل مجموعه بلوک‌ها باید تغییر داده شود تا داده‌ها در هر بلوک تغییر کنند. علاوه بر این، هر بلوک ارتباطی توسط هاب های مختلف تأیید می‌شوند. به‌این‌ترتیب، هرگونه اعوجاج در شبکه را می‌توان به‌طور مؤثر شناسایی کرد[۴, ۱۱].

زنجیره بلوکی به کاربران اجازه می‌دهد تا سطح قابل‌توجهی از ناشناس بودن را در نظر بگیرند. تراکنش‌ها ثبت و رصد می‌شوند و محل آن‌ها ثبت می‌شود اما هویت فرد محفوظ است. علاوه بر این، کاربر می‌تواند چندین هویت ایجاد کند تا از شناسایی نیز فرار کند. چنین سطحی از ناشناس بودن به دلیل ماهیت توزیع‌شده شبکه‌های زنجیره بلوکی امکان‌پذیر است، هرچند می‌توان هویت کاربر را با مشاهده ترافیک شبکه و سیستم زنجیره بلوکی عمومی تعیین کرد [۵, ۱۲]. ازآنجایی‌که تمام مبادلات انجام‌شده در شبکه‌های زنجیره بلوکی با مهر زمانی تائید و ثبت می‌شوند، مشتریان می‌توانند به‌راحتی با مراجعه به هر هاب در سیستم مربوطه، صحت سوابق گذشته را بررسی و تائید کنند. در زنجیره بلوکی بیت کوین[1]، هر صرافی را می‌توان به‌صورت مکرر به صرافی‌های گذشته دنبال کرد. شفافیت اطلاعات ذخیره‌شده در زنجیره بلوکی را افزایش می‌دهد و آن را به‌راحتی قابل‌تأیید می‌کند [۶, ۱۰].

[1]. Bitcoin



شکل ۱. فناوری زنجیره بلوکی به‌عنوان یک زیرساخت[۱۰]



شکل ۲. کاربردهای زنجیره بلوکی برای کاربردهای صنعتی اینترنت اشیاء

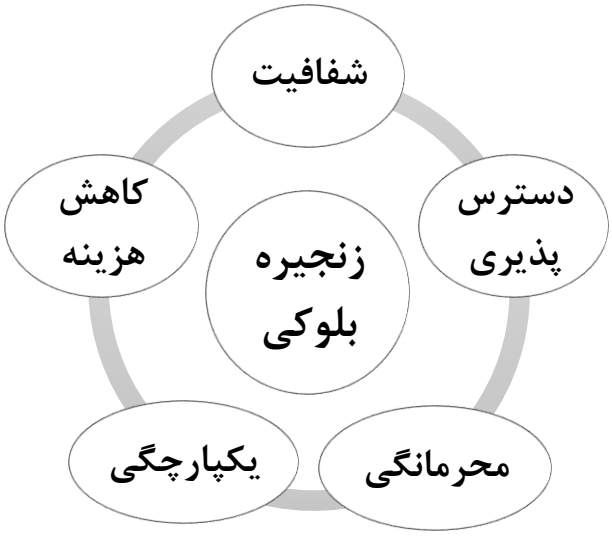
۲.۱ ویژگی‌های برجسته زنجیره بلوکی

زنجیره بلوکی‌ها اساساً با شبکه‌های تراکنش معمولی متفاوت هستند و دارای ویژگی‌های ویژه متنوعی هستند. عملکردهای کلیدی آن‌ها شامل رمزگذاری رمزنگاری (رمزنگاری نامتقارن)، هش کردن، بلوک‌های مرتبط و قراردادهای هوشمند است. گره‌ها به دلیل ماهیت توزیع‌شده خود می‌توانند مستقیماً بدون پردازش از طریق سرور مرکزی با یکدیگر ارتباط برقرار کنند. این به‌طور قابل‌توجهی زمان صرف شده برای پردازش تراکنش‌ها را کاهش می‌دهد و همچنین قابلیت اطمینان پلت فرم را بهبود می‌بخشد. حتی اگرچند گره از کار بیفتند، سیستم می‌تواند به کار خود ادامه دهد. این مورد در

سامانه‌های معمولی که خرابی هاب مرکزی می‌تواند کل شبکه را مختل کند، صادق نیست. تراکنش‌های رمزگذاری شده مستقیم حریم خصوصی را اعمال می‌کنند و جنبه‌های امنیتی سیستم را به میزان قابل‌توجهی افزایش می‌دهند. علاوه بر این، زنجیره بلوکی دارای مزیتی هستند که به‌راحتی قابل حسابرسی هستند و ازاین‌رو می‌توان تمام تراکنش‌های تاریخی را بررسی و تأیید کرد[۶].

۲.۲ مزایای به‌کارگیری فناوری زنجیره بلوکی در حوزه امنیت اینترنت اشیاء صنعتی

اینترنت اشیاء فناوری مربوط به آینده است. این فناوری در مورد برقراری ارتباط میان ابزارهای نسل بعد است تا شبکه ارتباطی به وجود بیاید. ابزارها و دستگاه‌ها در حال حاضر هم به هم متصل می‌شوند. ولی این فناوری نوعی نوآوری در حوزه برقراری ارتباط است. این فناوری دارای کارایی است و بسیاری از مسائل را بر طبق شرایط از پیش تعیین‌شده به‌صورت خودکار انجام می‌دهد [۲۰]. بااین‌حال نسل فعلی اینترنت اشیاء وابسته به رویکردی متمرکز است و موانع خاص خودش را دارد. این فناوری می‌تواند موردحمله از جانب افراد خرابکار قرار گیرد. حملات انکار سرویس توزیع‌شده هم به خاطر متمرکز بودن آن وجود دارد. این رویکرد متمرکز در بلندمدت اجرایی نیست و هزینه‌های نگهداری و زیرساختی تا حد زیادی افزایش خواهد یافت. زنجیره بلوکی می‌تواند با رویکردی نامتمرکز مشکلات اینترنت اشیاء را حل‌وفصل کند. به‌کارگیری فناوری دفتر کل توزیع‌شده، قادر به حل مشکلات امنیتی مرتبط با فرایند متمرکز است. بعلاوه قراردادهای هوشمند نقش مهمی در خودکار نمودن بسیاری از تعاملات اینترنت اشیاء دارند. از طرف دیگر، کاربر نهایی هم از وجود زنجیره بلوکی سود می‌برد، چون داده‌های آن‌ها روی شبکه از امنیت کافی برخوردار می‌شود. آن‌ها حتی می‌توانند در مورد تبادل داده‌ها با شروط خودشان تصمیم‌گیری کنند و از آن کسب درآمد نمایند. همچنین زنجیره بلوکی در مورد توکنیزه کردن اینترنت اشیاء هم مطرح است. توکنیزه کردن به خدمات اجاره‌ای شبکه‌ای هم کمک می‌کند[۱۴].



شکل ۳. مزایای زنجیره بلوکی برای استفاده در اینترنت اشیاء صنعتی

۲.۳ فناوری زنجیره بلوکی برای بهبود امنیت اینترنت اشیاء صنعتی

وقتی زنجیره بلوکی با اینترنت اشیاء صنعتی یکپارچه شود، چشم‌انداز امنیتی کل سیستم را افزایش می‌دهد. زنجیره بلوکی دارای خصوصیات عالی حریم خصوصی و امنیتی است که در سامانه‌های اینترنت اشیاء صنعتی ضروری است؛ بنابراین به سامانه‌های اینترنت اشیاء صنعتی کمک می‌کند تا بر اشکالات مهم خود غلبه کنند. ازآنجایی‌که زنجیره بلوکی شامل

بلوک‌هایی از داده‌ها هستند که به هم متصل و توزیع‌شده‌اند، در برابر حملات سریع‌تر و انعطاف‌پذیرتر هستند زیرا داده‌ها در هاب مرکزی ذخیره نمی‌شوند بلکه در سراسر شبکه پخش می‌شود. علاوه بر این، زنجیره بلوکی همچنین از الگوریتم‌های رمزگذاری قوی و تکنیک‌های هش استفاده می‌کنند و ازاین‌رو بسیار امن هستند. تراکنش‌های زنجیره بلوکی نیز شفاف هستند و هویت کاربران به‌راحتی قابل تائید است. این امر از نفوذ و آلودگی کاربران و دستگاه‌های مخرب به شبکه زنجیره بلوکی جلوگیری می‌کند. در محیط‌های اینترنت اشیاء صنعتی، بخش بزرگی از مکاتبات، همکاری ماشین به ماشین بدون هیچ واسطه انسانی است. در چنین شرایطی، ایجاد اعتماد در میان ماشین‌های مشارکت‌کننده آزمون بزرگی است که اینترنت اشیاء صنعتی هنوز به‌طور گسترده با آن مواجه نشده است. زنجیره بلوکی با اطمینان از اصالت دستگاه‌ها و ارائه حفاظت سایبری گسترده، اعتماد بین دستگاه‌ها را بهبود می‌بخشد. چنین شبکه‌هایی همچنین می‌توانند به‌طور فعال شناسایی کنند [۱۴].

شبکه‌های زنجیره بلوکی ضد دست‌کاری هستند و تغییر آن بسیار دشوار است. این در مورد دستگاه‌های اینترنت اشیاء صنعتی ضروری است زیرا هر تلاشی برای دست‌کاری یا تغییر حسگر یا ابزار می‌تواند بلافاصله شناسایی شود و اقدامات پیشگیرانه لازم انجام شود.

اگر یکپارچگی هر دستگاهی به خطر بیفتد، می‌توان آن را با خیال راحت و سریع از شبکه جدا کرد زیرا دستگاه‌های زنجیره بلوکی دارای طراحی توزیع‌شده هستند. آن‌ها به هیچ گره خاصی در شبکه وابستگی ندارند. ترتیب گردشی از رکورد برای به اشتراک‌گذاری اطلاعات بر روی یک سیستم توزیع‌شده، تراکنش‌های سریع را امکان‌پذیر می‌کند و بنابراین تقریباً خاموش شدن شبکه را غیرممکن می‌کند زیرا شکست هر یک از گره‌ها حداقل تأثیر را بر سیستم کلی خواهد داشت. امنیت مبتنی بر هش، بررسی شخصیت و تأیید منشأ در شناسایی دستگاه‌های متقلب و کاهش خطرات ضروری است. با اعتبارسنجی دستگاه‌ها برای ثبت‌نام در سیستم، ترتیبات اینترنت اشیاء صنعتی هماهنگ با زنجیره بلوکی می‌تواند امنیت را افزایش دهد [۱۵]. برای جمع‌بندی پیشینه پژوهش، خلاصه نتایج پژوهش‌های انجام‌شده صورت گرفته و در جدول ۱ مقایسه و دسته‌بندی‌شده است.

جدول ۱. پژوهش‌های انجام‌شده در حوزه کاربرد زنجیره بلوکی در امنیت اینترنت اشیاء

نویسنده	سال	زمینه	روش امن سازی و متد
Tuli et al [15]	۲۰۱۹	یکپارچه‌سازی سراسر اینترنت اشیاء، ماهواره و ابر	تکنیک‌های زنجیرهٔ بلوکی، احراز هویت و رمزنگاری
Jayasinghe[16]	۲۰۱۹	محافظت از حریم خصوصی	ترکیب توان زنجیره بلوکی با مفاهیم اعتماد و خلق زنجیرهٔ اعتماد
Bhattacharya et al [14]	۲۰۱۹	کاوش در حکم خدمت	ترکیب رایانش مرزی سیار و زنجیرهٔ بلوکی با مفاهیم مدیریت اعتماد
Fu et al[33]	۲۰۱۹	ردیابی مسیرهای توسعه دانش دامنه اینترنت اشیا: تحلیل مسیر اصلی	استفاده از روش تحلیل مسیر اصلی، بررسی مسیر توسعه دامنه برای ایجاد امنیت اینترنت اشیا
Jaskani et al[35]	۲۰۱۹	تحقیق در مورد چندین سیستم‌عامل برای اینترنت اشیا	استفاده از مدل برنامه‌نویسی درزمینهٔ توسعه و امنیت اینترنت اشیا

ur Rehman et al [32]	۲۰۱۹	نقش تجزیه‌وتحلیل داده‌های بزرگ در اینترنت اشیاء صنعتی	استفاده از فناوری‌ها، الگوریتم‌ها و تکنیک‌های اخیر BDA جهت توسعه دستگاه‌های هوشمند اینترنت اشیاء صنعتی
Banerjee et al [17]	۲۰۲۰	یک پردازشگر رمزنگاری قابل تنظیم برای اینترنت اشیا با امنیت	استفاده از روش رمزنگاری لایه‌ای برای ایجاد امنیت اینترنت اشیا
Blythe et al[40]	۲۰۲۰	بررسی تمایل به پرداخت برای دستگاه‌های ایمن اینترنت اشیا	استفاده از یک طراحی آزمایشی و یک روش ارزش‌گذاری مشروط، برای بهبود امنیت و آگاهی از اینترنت اشیا
Miskiewicz[31]	۲۰۲۰	اینترنت اشیا در بازاریابی: تجزیه‌وتحلیل کتاب‌سنجی	استفاده از ابزارهای نرم‌افزار VOSviewer و Scopus به‌عنوان یک استراتژی تحقیقاتی برای بررسی ساختار و پویایی انتشارات علمی به موضوعات توسعه اینترنت اشیا ازنقطه‌نظر بازاریابی
Peltonen et al [30]	۲۰۲۰	امنیت سازمانی برای اینترنت اشیا (IoT): راه‌اندازی سبک‌وزن با EAP-NOOB	استفاده از چارچوب استاندارد پروتکل تأیید اعتبار توسعه‌پذیر (EAP) برای راه‌اندازی امن دستگاه‌های محدود به منابع و امنیت اینترنت اشیا
Siegfried et al[29]	۲۰۲۰	زنجیره بلوکی و اینترنت صنعتی اشیا: طبقه‌بندی الزامات و تجزیه‌وتحلیل تناسب سیستماتیک	بررسی ادبیات توصیفی در مورد الزامات سیستم امنیت اینترنت اشیا
Khan et al [41]	۲۰۲۰	اینترنت صنعتی اشیا: پیشرفت‌های اخیر، توانمندسازی فن‌آوری‌ها و چالش‌های باز	بررسی ادبیات توصیفی در مورد امنیت و آگاهی از اینترنت اشیا
El-Masri & Hussain [33]	۲۰۲۱	زنجیره بلوکی به‌عنوان وسیله‌ای برای ایمن‌سازی اکوسیستم‌های اینترنت اشیا	استفاده از یک رویکرد یکپارچه‌سازی پردازش زبان طبیعی رایانه‌ای (NLP) با روش‌شناسی مرور ادبیات سیستماتیک در مورد امنیت اینترنت اشیا
Bi et al[36]	۲۰۲۱	اینترنت اشیا (IoT) و تحلیل کلان داده برای تولید دیجیتال (BDA) (DM)	استفاده از آنتروپی شانون برای اندازه‌گیری پیچیدگی سامانه‌ها و نشان دادن نقش EA در مدیریت پیچیدگی سیستم و دستیابی به ثبات سیستم در بلندمدت
Tsang et al[43]	۲۰۲۱	کاوش در هسته‌های فکری زنجیره بلوکی -اینترنت اشیا (BIoT)	استفاده از تحلیل عاملی اکتشافی (EFA)، تحلیل خوشه‌ای سلسله مراتبی (HCA)، خوشه‌بندی k-means (KMC) و مقیاس بندی چندبعدی (MDS) جهت بررسی سیستماتیک مبتنی بر تحلیل مجاورت استنادی (CPASR) هسته فکری BIoT.
Hansen & Bøgh [39]	۲۰۲۱	هوش مصنوعی و اینترنت اشیا در شرکت‌های کوچک و متوسط	بررسی راه‌حل‌های امنیتی اینترنت اشیا بسته به رویکرد پارادایم یادگیری ماشین موردنیاز

Latif et al[34]	۲۰۲۱	فناوری زنجیره بلوکی برای اینترنت اشیاء صنعتی: نظرسنجی جامع در مورد چالش‌های امنیتی، معماری‌ها، برنامه‌ها و جهت‌گیری‌های تحقیقاتی آینده	ارائه یک معماری مرجع چهار لایه اینترنت اشیاء صنعتی همراه با عملکردها و مسائل امنیتی هر لایه جهت بررسی فناوری زنجیره بلوکی برای اینترنت اشیاء صنعتی
Karthikeyan et al [41]	۲۰۲۱	افزایش امنیت در اینترنت اشیا	عملکرد امنیت شبکه نسبت به شکسته شدن کلید افزایش داده‌شده است. یک الگوریتم تلفیقی متشکل از الگوریتم‌هایRSA وECC استفاده شد
K.Priyadharshini & Aroul Canessane [46]	۲۰۲۱	الگوریتم امنیتی مبتنی بر زنجیره بلوکی در اینترنت اشیا چارچوبی برای ارتباطات محافظت‌شده در شهرهای هوشمند	ادغام سیستم پیشنهادی زنجیره بلوکی را با اینترنت اشیا و ایجاد یک پلت فرم ارتباطی محافظت‌شده را در شهر هوشمند
Kanwalinderjit Gagneja & Riley Kiefer[28]	۲۰۲۱	پروتکل امنیتی برای اینترنت اشیا: پیاده‌سازی و تجزیه‌وتحلیل مبتنی بر زنجیره بلوکی	ترکیبی از فناوری‌های زنجیره بلوکی و دستگاه‌های اینترنت اشیا در یک شبکه
Li[27]	۲۰۲۱	بهینه‌سازی سیستم اطلاعات مدیریت منابع انسانی سازمانی مبتنی بر اینترنت اشیا	انتخاب پیوند مبتنی بر نوع کسب‌وکار الگوریتم و الگوریتم سوئیچینگ چند پیوندی شمال جهت بهینه‌سازی سیستم اطلاعات منابع انسانی سازمانی بر اساس فناوری اولیه اینترنت اشیا
Wang et al [37]	۲۰۲۲	مکانیسم ذخیره‌سازی امنیت داده‌ها بر اساس اینترنت صنعتی زنجیره بلوکی	استفاده از فناوری زنجیره بلوکی می‌توان برای اطمینان از امنیت داده‌های اینترنت اشیا
Rondon et al[38]	۲۰۲۲	بررسی دستگاه‌های اینترنت اشیاء سازمانی (E-IoT): دیدگاه امنیتی	استفاده از دستگاه‌های اینترنت اشیاء سازمانی (E-IoT) به‌عنوان راه‌حل هوشمند برای برنامه‌های پیچیده‌تر (به‌عنوان‌مثال، روشنایی کامل).
Corallo et al[26]	۲۰۲۲	آگاهی از امنیت سایبری درزمینهٔ اینترنت صنعتی اشیا: مروری بر ادبیات سیستماتیک	تکنیک‌های اتخاذشده برای افزایش آگاهی شرکت در مورد امنیت سایبری درزمینهٔ اینترنت صنعتی اشیا (مانند بازی‌های جدی، پرسشنامه‌های آنلاین)
Kumar et al[42]	۲۰۲۲	نظرسنجی در مورد زنجیره بلوکی برای اینترنت اشیا صنعتی	بررسی اینترنت اشیا به‌عنوان یک مفهوم و تهدیدات مربوط به اینترنت اشیا و همچنین بررسی ارتباط از اینترنت اشیا صنعتی و زنجیره بلوکی
Huo et al[21]	۲۰۲۲	بررسی جامع زنجیره بلوکی در اینترنت اشیا صنعتی: انگیزه‌ها، پیشرفت‌های تحقیقاتی و چالش‌های آینده	بررسی الزامات فنی پلتفرم‌های زنجیره بلوکی را در برنامه‌های اینترنت اشیاء صنعتی

Luis Puche Rondon et al[19]	۲۰۲۲	بررسی دستگاه‌های اینترنت اشیاء سازمانی برای امنیت	آگاهی از اینترنت اشیا، راه‌حل برای ارتقا و چالش‌ها
Liu et al[15]	۲۰۲۲	بهبود مدیریت دانش سازمانی با اینترنت اشیا: مطالعه موردی از صنعت بیمه خودرو	با استفاده از مدل اجتماعی سازی-برونی سازی-ترکیب - داخلی سازی (SECI) فناوری‌های مبتنی بر اینترنت اشیا و تأثیرات آن بر فرآیند تصمیم‌گیری بیمه‌گر - ارزیابی ریسک و قیمت‌گذاری، عملکرد فرآیند کسب‌وکار- دقت و کارایی ادعا و نقش یک عملکردهای سیستم اینترنت اشیا موردبررسی قرار می‌گیرد

۳. راهکار پیشنهادی

اینترنت اشیا درعین‌حال که می‌تواند داده‌هایی جدید و اطلاعاتی مفید را در اختیار قرار دهد، آسیب‌پذیری‌های جدیدی را نیز برای سازمان به وجود می‌آورد؛ بنابراین، بسیار ضرورت دارد که نهادهای تجاری پیش از انجام هرگونه اقدامی، به مسائل امنیتی مربوط به کاربرد اینترنت اشیا در سازمان خود توجه کنند. باوجوداین حقیقت که چندین استاندارد مختلف برای محیط‌های توزیع‌شده وجود دارد، رمزنگاری و کنترل دسترسی نقش بسیار مهمی را در این قسمت ایفا می‌کنند. رمزنگاری روند انتقال داده‌های مبتنی به پیام‌های رمزنگاری‌شده هست که به نظر به‌صورت تصادفی و بدون معنی می‌باشد. روند رمزگشایی، این پیام‌های رمزنگاری‌شده را دوباره به پیام‌های متنی تبدیل می‌کند. روندهای رمزنگاری و رمزگشایی موجب شکل‌گیری روش‌های استفاده از داده‌های رمزی می‌شود. ایده‌ی کنترل دسترسی محدودیت‌های دسترسی خاصی را بر اساس سیاست‌های دسترسی بر روی کاربران سیستم قرار می‌دهد. به دلیل این‌که سرورهای ابری نه‌تنها شامل اطلاعات محرمانه‌ی افراد است، بلکه روندهای رمزنگاری و کنترل دسترسی مورداستفاده برای محافظت از داده‌ها نیز باید خودشان مورد محافظت قرار گیرند[۱۹].

راهکار پیشنهادی به‌صورت زیر بیان می‌گردد:

- برای کنترل دسترسی نوشتن از سیاست‌های نوشتن[1] بهره گرفته خواهد شد، چراکه روش‌های سنتی کنترل دسترسی مانند احراز هویت توسط نام کاربری و پسورد، نیاز دارد که سمت سرور تا حد ممکن قابل‌اعتماد باشد، اما در سیستم پیشنهادی ما ابر سروری ست که امنیت کمی دارد و نباید نام کاربری و پسوردها را برای احراز هویت در اختیار داشته باشد. بدین منظور از امضا مبتنی بر خصیصه استفاده خواهد شد. در این روش به همراه متن جدید رمزنگاری‌شده که قرار است برای کاربر فرستاده شود امضا کاربر مجاز به نوشتن نیز ارسال می‌شود. امضای کاربر در کنار داده‌ها به سمت کاربر درخواست‌کننده داده‌ها ارسال می‌شود تا کاربر به‌وسیله‌ی این امضا بتواند صحت اطلاعات دریافتی از ابر را احراز نماید. این امضا مبتنی بر خصیصه‌هایی است که کاربر در اختیار دارد و بر اساس سیاست نوشتن ایجاد می‌شود.
- ایجاد تغییرات بر روی الگوریتم رمز موجود برای رسیدن به اهداف تعیین‌شده از قبیل تلاش برای کاهش زمان رمزگذاری و زمان رمزگشایی. برای این منظور می‌توان از قابلیت برون‌سپاری[2] استفاده کرد تا با برون‌سپاری قسمتی از فرایند رمزنگاری و رمزگشایی به یک سرور مه[3] که تا حدی قابل‌اعتمادند انتقال داده می‌شود، علاوه بر اینکه بار

[1] Write policy
[2] O utsourcing capability
[3] Fog

محاسباتی را از دوش کاربران برمی‌داریم، از برخی حملات که به‌قصد سرقت اطلاعات انجام می‌شود و همچنین از امکان حملات تبانی[1] نیز جلوگیری کنیم.

- یکی از مهم‌ترین مواردی که در طراحی روش پیش نهادی باید در نظر گرفته شود توجه به امکان منقضی کردن دسترسی افراد پس از مدت‌زمان مشخص می‌باشد. چراکه ممکن است میزان دسترسی کاربران به داده‌ها تغییر کند و دیگر نباید اجازه دسترسی به آن اطلاعات را داشته باشد. برای این منظور از روش‌های ابطال دوقسمتی استفاده خواهد شد بدین ترتیب که قسمتی از کلید در ابر و قسمتی در دسترس کاربر خواهد بود و همچنین فهرستی از کاربران مجاز در ابر موجود خواهد بود. چنانچه کاربر درخواست دسترسی به داده‌ای در ابر را داشته باشد ابتدا ابر در لیست کاربران مجاز نام او را جستجو می‌کند و در صورت مجاز بودن کاربر، قسمتی از کلید که در اختیارش است را در اختیار کاربر قرار می‌دهد تا رمزگشایی را انجام دهد. نکته‌ی این روش در اینجاست که هیچ‌کدام از دو طرف (کاربر و ابر) نمی‌توانند بدون در اختیار داشتن قسمت دیگر کلید، اقدام به رمزگشایی کنند [۱۹].

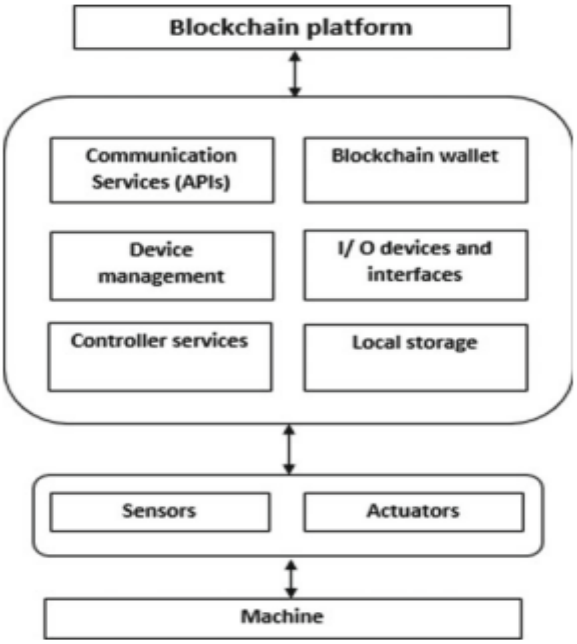
۴. راهکار استفاده از اینترنت صنعتی اشیاء و فناوری زنجیره بلوکی[2] در صنعت خودروسازی

BPIIOT از معماری توزیع‌شده، شبکه همتا به همتا و اتصال ایمن برای استفاده در بخش صنعتی استفاده می‌کند. این شبکه مبتنی بر قراردادهای هوشمند است که به‌عنوان توافق بین مشتریان و تولیدکنندگان عمل می‌کند. این قراردادهای هوشمند از طریق سیستم زنجیره بلوکی منتقل می‌شوند و در ایجاد اعتماد در بین ذینفعان ضروری هستند. پلتفرم زنجیره بلوکی، طبقه فروشگاه را با سرویس‌های ابری و داده ادغام می‌کند، درنتیجه سیستم توزیع‌شده‌ای را تضمین می‌کند که در آن داده‌ها بین گره‌ها به اشتراک گذاشته می‌شود. این دیجیتال‌سازی طبقه فروشگاه از طریق استفاده از پلتفرم‌های یکپارچه به دست می‌آید که راه‌حل‌های مدرن را سریع‌تر، ایمن‌تر، شفاف‌تر و کارآمدتر در مقایسه با نمونه‌های معمولی خود می‌سازد. دستگاه-های اینترنت اشیا صنعتی متصل به ماشین‌ها، آن‌ها را قادر می‌سازد تا اطلاعات مربوط به وظایف خود را مبادله کنند و از طریق سیستم زنجیره بلوکی به سمت ابر پیشرفت کنند. این ابزارها همچنین ارتباط ماشین به ماشین را در شبکه اینترنت اشیا صنعتی فعال می‌کنند و ازاین‌رو ماشین‌ها می‌توانند زمان اجرا و وظایف خود را بر این اساس بهینه کنند. دستگاه‌های اینترنت اشیا صنعتی مورداستفاده در شبکه عمدتاً از دو بخش تشکیل‌شده‌اند: برد رابط و یک کامپیوتر تک بردی[3]، برد رابط دارای عملکردهای ورودی/خروجی دیجیتال و آنالوگ است که حسگرها و محرک‌ها با آن تعامل دارند. برد رابط و کامپیوتر تک بردی توسط پورت‌های سریال و یک سری حسگر به هم متصل می‌شوند. حسگرها و درایورهای برنامه در کامپیوتر تک بردی نصب می‌شوند و متعاقباً استفاده از حسگرها و محرک‌ها را به حداکثر پتانسیل خود ممکن می‌سازند، زیرا درایورها به‌طور مکرر مطابق با الزامات فعلی به‌روزرسانی و سفارشی‌سازی می‌شوند. کامپیوتر تک بردی را می‌توان بر اساس نیازهای کاربر با استفاده از ناظر ابزار موجود در کامپیوتر تک بردی ویرایش و طراحی کرد. این کار با استفاده از یک رابط وب امکان‌پذیر است که می‌تواند برای نظارت بر وضعیت دستگاه‌ها نیز استفاده شود. علاوه بر این، واحد O/I موجود در کامپیوتر تک بردی می‌تواند به‌عنوان یک رابط برای اتصال پلتفرم Blockchain-IIOT به شبکه‌های خارجی عمل کند [۲۴].

شکل ۴، معماری سیستم Blockchain-IIoT پیشنهادی را نشان می‌دهد [۲۵]؛ که یک برد رابط و یک کامپیوتر تک بردی را در خود جای‌داده است. حسگرها و محرک‌ها با برد رابط که یک رابط متوالی با کامپیوتر تک بردی و با دستگاه دارد تعامل دارند. حسگرها به برقراری ارتباط بین برد رابط و کامپیوتر تک بردی کمک می‌کنند و کامپیوتر تک بردی را قادر می‌سازند تا اطلاعات حسگر را از برد رابط دریافت کند و علائم کنترلی را به محرک‌ها ارسال کند. مدیریت زنجیره بلوکی در کامپیوتر تک بردی با صدور و دریافت مبادلات از سیستم با شبکه زنجیره بلوکی ارتباط برقرار می‌کند. هر گجت اینترنت

[1] Collusion
[2] Blockchain-IIOT
[3] SBC

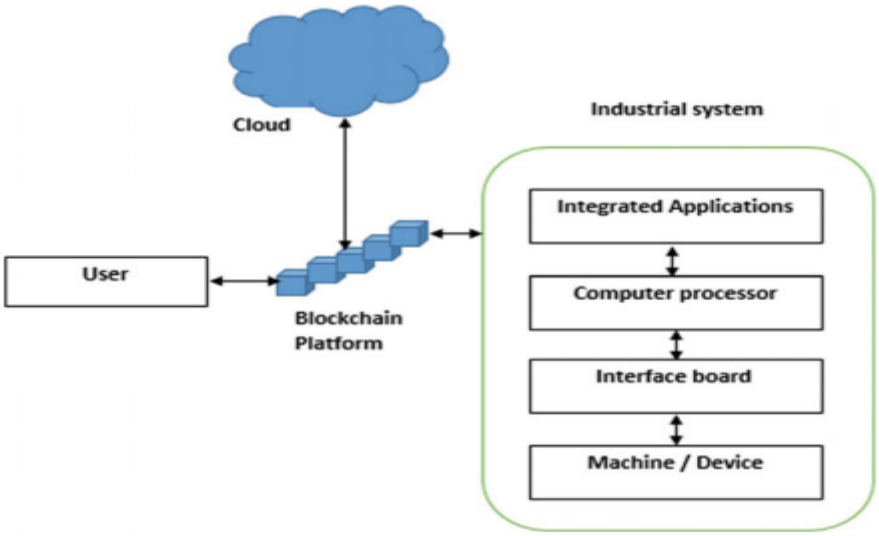
اشیا صنعتی رکورد خاص خود را در شبکه زنجیره بلوکی دارد و یک کیف پول زنجیره بلوکی را در کامپیوتر تک بردی نگهداری می‌کند. مدیریت کنترلر برای نظارت بر وضعیت ماشین، وضعیت کار و انتقال مبادلات به قراردادهای هوشمند در زنجیره بلوکی استفاده می‌شود [۲۶].



[۲۵]

شکل ۴. پلتفرم پیشنهادی Blockchain-IIoT.

شکل ۵، نحوه تعامل کاربران با سامانه‌های صنعتی مدرن را با استفاده از رابط Blockchain-IIoT نشان می‌دهد[۲۲]. سامانه‌های صنعتی از ماشین‌ها و دستگاه‌هایی تشکیل‌شده‌اند که به هم متصل و گروه‌بندی می‌شوند تا برنامه‌های کاربردی مجموعه‌ای را تشکیل دهند. پلت فرم پیشنهادی برای ذخیره داده‌ها و انجام تجزیه‌وتحلیل به ابر متصل است. بااین‌حال، تراکنش‌های بین کاربر، ابر و سیستم از طریق شبکه زنجیره بلوکی توزیع‌شده پردازش می‌شوند که اساساً به‌عنوان یک موجودیت متصل عمل می‌کند. این زنجیره بلوکی مقیاس‌پذیری بسیار خوبی را ارائه می‌دهد زیرا با افزایش اندازه شبکه و تعداد تراکنش‌ها، می‌توان بلوک‌های بیشتری را اضافه کرد. علاوه بر این، ازآنجایی‌که زنجیره بلوکی‌ها اساساً شبکه‌های همتا به همتا هستند، زنجیره با افزایش تعداد کاربران مقیاس می‌شود [۱۶].



شکل ۵. تعامل کاربر با پلتفرم زنجیره بلوکی [۲۲].

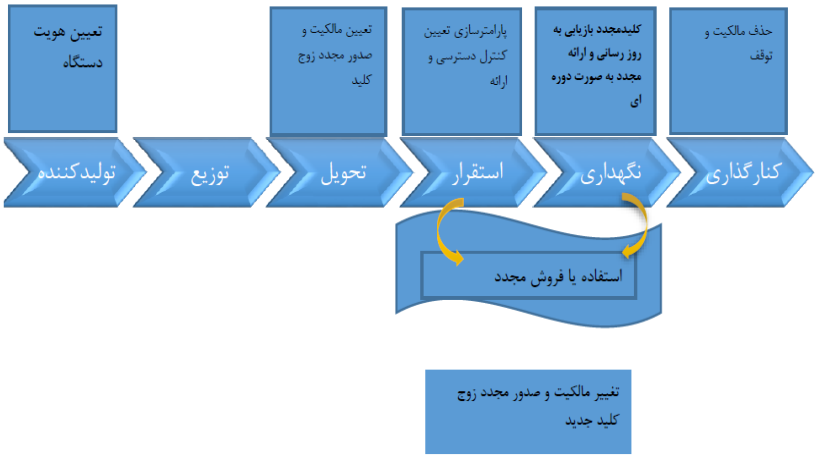
پروتکل‌های ارتباطی برنامه‌های کاربردی اینترنت اشیا صنعتی مشابه با پروتکل‌هایHTTP، MQTT ، CoAP یا XMPP یا حتی پروتکل‌های مربوط به مسیریابی مانند RPLو 6LoWPAN مطابق طراحی امن نیستند. این پروتکل‌ها باید در پروتکل‌های امنیتی دیگر مانند DTLS یا TLS برای پروتکل‌های پیام‌رسانی و برنامه‌های کاربردی پوشش داده شوند تا ارتباط امن ایجاد گردد. به‌طور مشابه برای مسیریابی، IPSec عموماً برای ایجاد امنیت در پروتکل‌های RPL و 6LoWPAN استفاده می‌شود. پروتکل‌های TLS،DTLS، IPSec یا حتی پروتکل TinyTLS سبک‌وزن ازنظر نیازهای محاسباتی و حافظه سنگین و پیچیده هستند و با مدیریت و حکمرانی متمرکز مدیریت کلید و توزیع با استفاده از پروتکل محبوب PKI پیچیده می‌شود. مدیریت کلید و توزیع با زنجیره بلوکی کاملاً حذف می‌شود زیرا هر دستگاه اینترنت اشیا صنعتی دارای GUID مخصوص به خود و زوج کلید نامتقارن قبلاً نصب‌شده و متصل به شبکه زنجیره بلوکی خواهد بود. این امر منجر به ساده‌سازی قابل‌توجه سایر پروتکل‌های امنیتی مانند DTLS بدون نیاز به دست‌کاری و تبادل گواهی PKI در مرحله دست دادن در مورد DTLS یا TLS یا IKE در مورد) IPSec می‌شود تا پارامترهای مجموعه رمز برای رمزنگاری و درهم سازی مبادله شده و کلیدهای اصلی و جلسات ایجاد گردد. بنابراین، پروتکل‌های امنیتی سبک‌وزن که با الزامات منابع محاسباتی و حافظه دستگاه‌های اینترنت اشیا صنعتی تناسب داشته و آن‌ها را دسته‌بندی می‌کنند، امکان‌پذیرتر می‌گردند [۱۷].

۴/۱ راهکارهای بالقوه زنجیره بلوکی

اینترنت درزمینهٔ اینترنت اشیا - زنجیره بلوکی مبتنی بر قرارداد هوشمند انتظار می‌رود که نقش مهمی در مدیریت، کنترل و مهم‌تر از همه حفظ امنیت دستگاه‌های اینترنت اشیا داشته باشد. در این بخش در مورد برخی ویژگی‌های ذاتی زنجیره بلوکی که برای اینترنت اشیا به‌طورکلی و برای امنیت اینترنت اشیا به‌طور خاص بین‌هایت سودمند می‌باشند، بحث می‌کنیم. فناوری اینترنت اشیا افراد، مکان‌ها و محصولات را به یکدیگر متصل می‌کند و موقعیت‌هایی برای فراهم آوردن ارزش ایجاد می‌کند؛ تراشه‌ها و حسگرها که داخل محصولات گذاشته می‌شوند، داده‌ها را به شبکه اینترنت اشیا منتقل می‌کنند. البته هنوز نگرانی‌های فنی و امنیتی زیادی در رابطه با این فناوری مطرح است؛ فناوری زنجیره بلوکی در این راستا می‌تواند به اینترنت اشیا کمک کرده و در حل بسیاری از مشکلات آن مفید واقع شود[۱۸].

فضای آدرس زنجیره بلوکی دارای فضای آدرس ۱۶۰ بیت برخلاف فضای آدرس IPv6 است که فضای آدرس ۱۲۸بیت دارد. آدرس زنجیره بلوکی درهم سازی ۲۰ بایت یا ۱۶۰ بیت کلید عمومی تولیدشده با ECDSA[1] (الگوریتم امضای دیجیتال منحنی بیضوی) می‌باشد. زنجیره بلوکی با داشتن آدرس ۱۶۰ بیت می‌تواند آدرس‌ها را به‌صورت آفلاین برای حدود 1.46×10^{48}دستگاه اینترنت اشیا تولید کرده و تخصیص دهد. احتمال تلاقی آدرس تقریباً 10^{48} است که برای ارائه GUID[2] (شناسه منحصربه‌فرد جهانی) به‌اندازه کافی امن محسوب می‌شود و نیازی به ثبت یا بررسی منحصربه‌فرد بودن در زمان تخصیص آدرس به دستگاه اینترنت اشیا وجود ندارد. در زنجیره بلوکی اختیار و حکمرانی متمرکز مشابه اختیار اعداد تخصیص‌یافته با اینترنت IANA[3] حذف می‌شود. در حال حاضر، IANA بر تخصیص آدرس‌های جهانی 4IP و IPv6 نظارت می‌کند. همچنین زنجیره بلوکی ۴.۳ میلیارد آدرس بیش از IPv6 ارائه می‌کند و بنابراین، یک راهکار مقیاس‌پذیرتر برای اینترنت اشیا نسبت به IPv6 ارائه می‌کند. درنهایت ذکر این نکته ارزشمند می‌باشد که بسیاری از دستگاه‌های اینترنت اشیا حافظه و ظرفیت محاسبه محدودیت دارند و ازاین‌رو برای اجرای یک پشته IPv6 مناسب نمی‌باشند[۱۹].

زنجیره بلوکی توان حل این چالش‌ها به شیوهای آسان، امن و کارآمد را دارا است. زنجیره بلوکی به‌طور گسترده برای ارائه قابل‌اعتماد و مجاز ثبت هویت، ردیابی مالکیت و نظارت بر محصول، کالا و دارایی استفاده‌شده است. روش‌هایی مانندTrus Chain، برای امکان‌پذیر ساختن تراکنش‌های قابل‌اعتماد با استفاده از زنجیره بلوکی در ضمن حفظ یکپارچگی تراکنش‌ها در یک محیط توزیع یافته پیشنهادشده است. دستگاه‌های اینترنت اشیا از این مورد مستثنی نیستند. زنجیره بلوکی برای ثبت و هویت بخشی به دستگاه‌های اینترنت اشیا متصل قابل‌استفاده می‌باشند و مجموعه‌ای از خصوصیات و روابط پیچیده را دارا هستند که در دفتر کل توزیع یافته زنجیره بلوکی قابل بارگذاری و ذخیره‌سازی می‌باشند [۲۰].



شکل ۶. مدیریت امنیت چرخه حیات دستگاه LOT[۲۰]

۴/۲ اجرای روش پیشنهادی بر روی شبکه خودروهای خودران

در زیست‌بوم اینترنت اشیاء صنعتی، شبکه مبتنی بر اینترنت اشیاء خودروهای خودران در نظر گرفته‌شده است. شبکه خودروهای خودران نیز مشابه شبکه اقتضایی در نظر گرفته‌شده است. زمانی که خودروها در یک ناحیه حضور دارند اطلاعات آن‌ها تا یک شعاع محدود برای خودروهای دیگر ارزشمند است. به علت قابلیت حرکت خودروها یا به تعبیر دقیق‌تر (نودهایی شبکه) این شبکه از اشیاء حالت پویایی و دینامیکی بالای دارد. اگر از دید یک نود (خودرو) به شبکه نگاه شود به‌طور مداوم

[1]. Elliptic Curve Digital Signature Algorithm
[2]. Global Unique Identifier
[3]. Internet Assigned Numbers Authority

نودهای جدید در شبکه احتمال اضافه شدن و یا خارج شدن دارند .نیاز به امنیت در جریان اطلاعات بین نودهای این شبکه کاملاً ملموس است زیرا هرگونه اطلاعات اشتباه می‌تواند به بروز خسارت‌های مالی و جانی منجر شود، برای تأمین امنیت جریان اطلاعات از دیدگاه راهکارهای مبتنی بر اعتماد راهکار مبتنی بر PKI[1] و نیز زنجیره بلوکی موردتوجه بیشتری قرارگرفته است. راهکار مبتنی بر PKI به‌رغم امنیت و کارایی بالا، با توجه به دینامیک بالای توپولوژی شبکه‌های خودروهای خودران و امکان قطع ارتباط مراکز زیرساخت[2] نمی‌تواند به تنهای مبنای اعتماد نودها قرار گیرد. راهکار مبتنی بر زنجیره بلوکی به علت ظرفیت امنیتی بالای زنجیره بلوکی حتی توسط شبکه خودروهای خودران تسلا مورداستفاده قرارگرفته است. راهکار پیشنهادی تحقیق حاضر استفاده هم‌زمان از راهکار PKI و راهکار زنجیره بلوکی با تغییر شیوه اعتماد مبنی بر رأی‌گیری زنجیره بلوکی می‌باشد. راهکار PKI به‌صورت Redundant در نظر گرفته‌شده و به افزایش توانایی زنجیره بلوکی در احصای میزان اعتماد در نودها پرداخته است. در تحقیق حاضر پیشنهادشده که اولاً تمام نودها مبنای اعتماد صفر[3] دارند همچنین اعتماد هر نود به سایر نودها به‌جای حالت باینری به‌صورت فازی (عدد بین ۰ تا ۱ کمتری تا بیشترین اعتماد) در نظر گرفته می‌شود. درنهایت هر نود اطلاعات دریافتی از نودهای دیگری را بر مبنای عدد اعتماد فازی آن‌ها مورداستفاده قرار می‌دهد، درواقع می‌توان گفت خودرو همواره احتمال خطا و اخلال را برای تمام نودها در نظر می‌گیرد و از اعتماد کامل خودداری می‌کند. در شبکه محلی ایجادشده از خودروهای خودران، هر نود یک بردار اعتماد به نودهای دیگر تشکیل می‌دهد. در ابتدا با توجه به اصل اعتماد صفر تمامی درایه‌های این بردار اعتماد، صفر هستند سپس از دو مکانیسم برای ارزیابی اعتماد استفاده می‌گردد. مکانیسم اول اعتبار سنجی داده‌های ارسالی نودهای دیگر است، یعنی هر نود بر اساس اعتبار سنجی که از داده نودهای دیگر دریافت می‌کند یک اعتماد بین ۰ و ۱ به آن‌ها می‌دهد شاید الگوریتم اعتبار سنجی جای بحث زیادی دارد اما باوجود روش‌های هوش مصنوعی یادگیری ماشین مبنی بر شبکه‌های عصبی عمیق است ارائه این الگوریتم امکان‌پذیر است اما موضوع بحث تحقیق حاضر نیست. از طرفی این اعتبار سنجی به تنهای تأثیرگذار نیست و در ادامه مورد تصحیح قرار خواهد گرفت. لذا در این شبکه به‌تمامی نودها ابتدابه‌ساکن در حال ارزیابی نودهای کناری صرفاً بر اساس اطلاعات و داده‌های ارسالی آن‌ها هستند و درایه‌های اعتماد در این مرحله با این مکانیسم مقداردهی اولیه می‌گردند در مرحله بعد مشابه رأی‌گیری در زنجیره بلوکی نودهای بردار اعتماد به‌دست‌آمده را در اختیار همدیگر قرار می‌دهند سپس هر نود از بردارهای اعتماد به‌دست‌آمده یک ماتریس اعتماد تشکیل داده و از روی این ماتریس بردار اعتماد جدید را محاسبه می‌کند محاسبه بردار اعتماد می‌تواند با یک متوسط گیری ساده و یا متوسط گیری وزن‌دار صورت بگیرد .با فرض متوسط گیری از هر ستون ماتریس اعتماد و تشکیل بردار اعتماد جدید واضح است که اولاً ارزیابی کلی نودها به‌صورت مشارکتی در میزان اعتماد تأثیرگذار است و هم مسئله رأی‌گیری و اجماع در آن لحاظ شده و هم اینکه به‌جای حالت باینری یک قابلیت منعطف و قوی‌تر به‌صورت فازی به آن اضافه‌شده است در این شبکه در صورت عدم وجود نودهای متخاصم پس از چند مرحله سطح اعتماد افزایش می‌یابد؛ اما وجود نودهای متخاصم ماتریس‌ها و بردارهای اعتماد تحت تأثیر قرار داده و انتظار می‌رود که روش پیشنهادی بیش از حالت رأی‌گیری در زنجیره بلوکی نسبت به این نودها مقاوم باشد.

۴٫۳ پیاده‌سازی و ارزیابی روش پیشنهادی

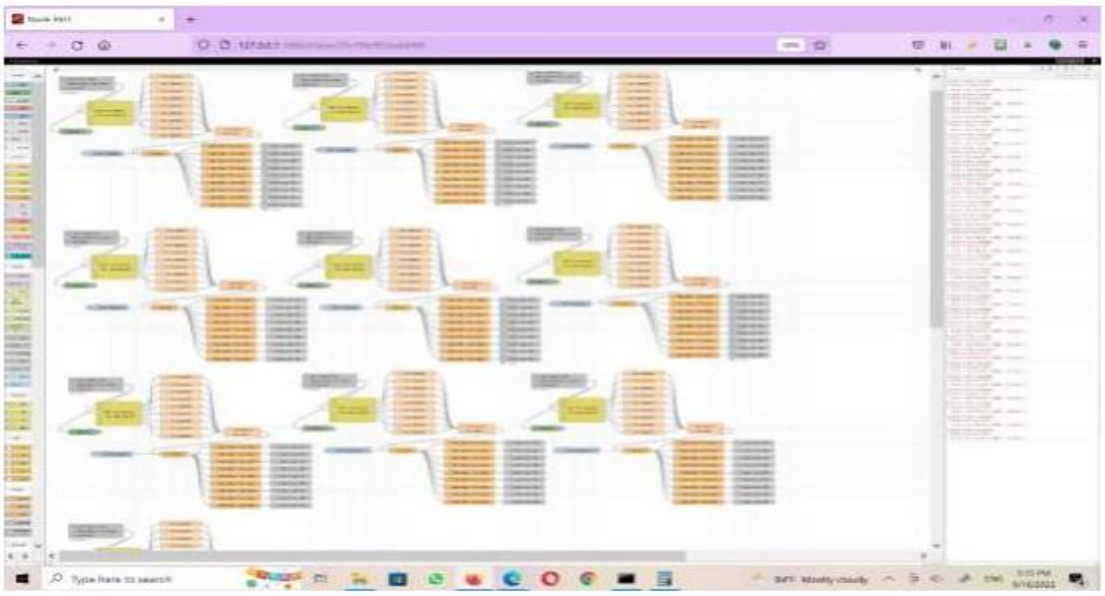
برای اثبات کارایی روش پیشنهادی یک حالت ساده‌سازی شده از یک شبکه محلی خودران متشکل از ۱۰ خودرو در پلتفرم NODE- RED پیاده‌سازی شده و در چند حالت بدون نودهای متخاصم و افزایش نودهای متخاصم از یک تا نصف نودها بررسی گردید. دو استراتژی برای نودهای متخاصم متصور می‌باشد. استراتژی اول ارائه داده‌های حرکتی صحیح و یا غلط به‌صورت تصادفی است. به این معنی که گاهی نود متخاصم داده‌های حرکتی صحیح ارائه می‌دهد و گاهی داده‌های

[1]. Public Key Infrastructure
[2]. Infrastructure
[3]. Zero Trust

حرکتی غلط ارائه می‌دهد. درواقع عدد اعتبار سنجی از داده‌های حرکتی این نودها از دید نودهای دیگر مدام در حال تغییر است چراکه هر زمان داده‌های حرکتی ارائه‌شده به‌صورت عمدی و اشتباه تغییر کند، عدد اعتبار سنجی کاهش می‌یابد. استراتژی دوم نودهای متخاصم ارائه بردار اعتماد غلط به سایر نودها می‌باشد این بردار اعتماد غلط در بدترین حالت شامل کمترین عدد اعتقاد برای نودهای سالم و بیشترین عدد برای نودهای متخاصم دیگر است. البته امکان بروز بدترین حالت تنها زمانی است که نودهای متخاصم از وجود همدیگر آگاه بوده و همکاری فعالی داشته باشند که این حالت به علت پیچیدگی‌های خاص خود در پیاده‌سازی در نظر گرفته نشده است. لذا با تغییر در تعداد نودهای متخاصم چند بار شبیه‌سازی انجام‌شده در Node-Redاجرا و نتایج بردار اعتماد بررسی گردید.

۴٫۴ پیاده‌سازی الگوریتم پیشنهادی

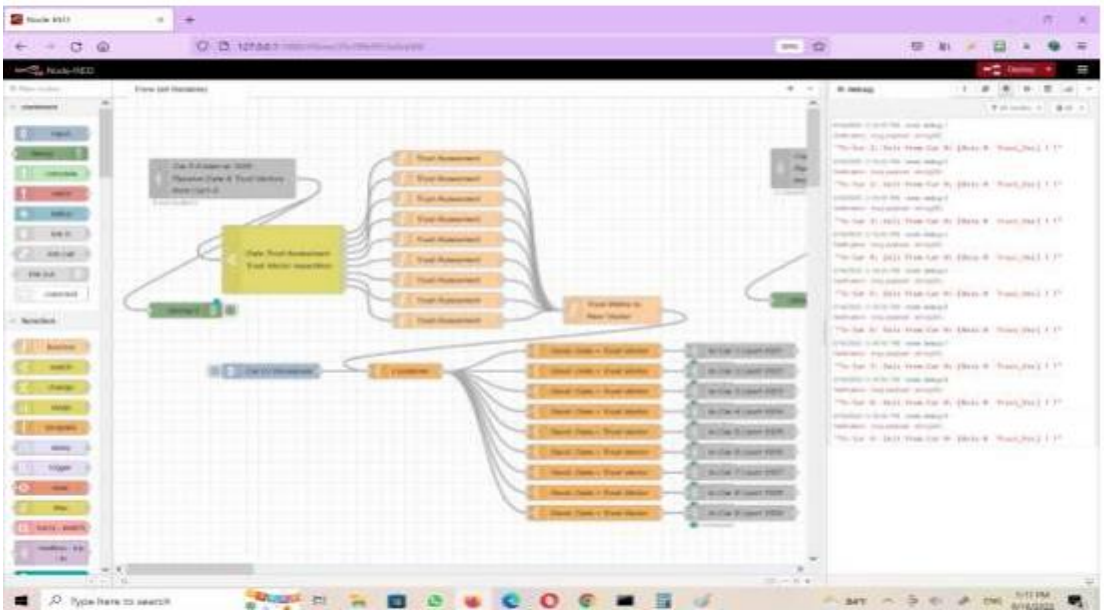
به‌منظور بررسی عملکرد الگوریتم پیشنهادی پلتفرم Node-Red در نظر گرفته‌شده است در این پلتفرم طبق شکل ۷، تعداد ۱۰ نود خودرو تعریف‌شده است.



شکل ۷. پیاده‌سازی شبکه متشکل از ۱۰ خودرو

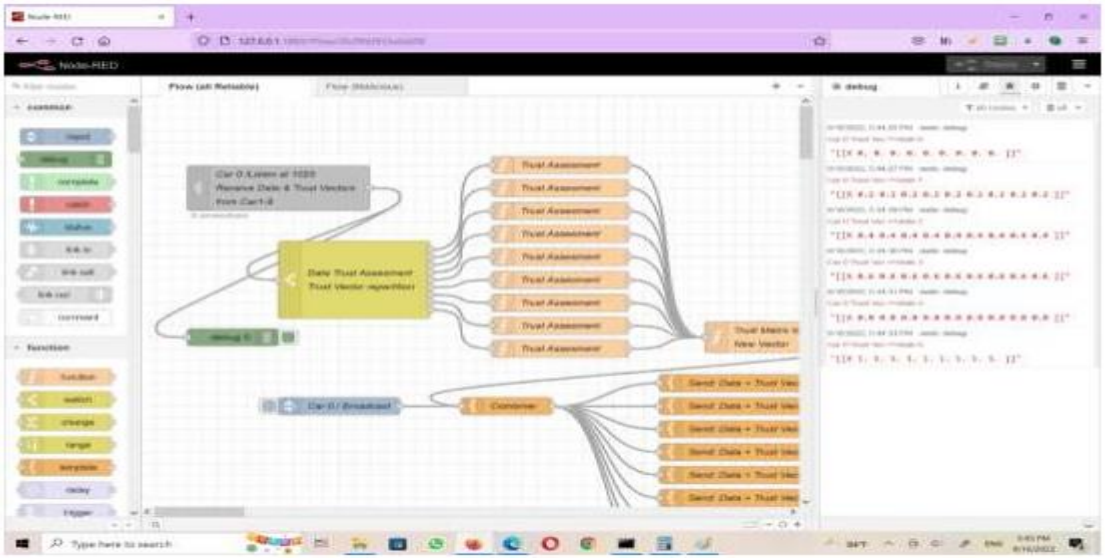
همچنین در شکل ۸، ساختار هر نود نشان داده‌شده است. این ساختار شامل دو بخش اصلی گیرنده[1] و فرستنده[2] هست. در بخش گیرنده اطلاعات طبق پروتکل TCP دریافت شده و سپس به تفکیک پورت به خودرو متناظر می‌گردد. هر خودرو داده‌های حرکتی و بردار اعتمادش را می‌فرستد. بردارهای اعتماد یک ماتریس مربعی اعتماد تشکیل می‌دهند که عناصر قطر اصلی را گیرنده از روی اعتبار سنجی داده‌های حرکتی قرار می‌دهد. درنهایت هر ستون ماتریس متوسط گیری شده و بردار اعتماد نهایی محاسبه می‌شود. بخش فرستنده هر خودرو داده نیز داده‌های حرکتی خودرو به همراه بردار اعتماد به‌روزرسانی شده را برای کلیه نودهای دیگر شبکه (خودروهای دیگر) می‌فرستد.

[1]. Listener
[2]. Broadcaster



شکل ۸. شماتیک یک نود در شبکه خودروها خودران موردبررسی

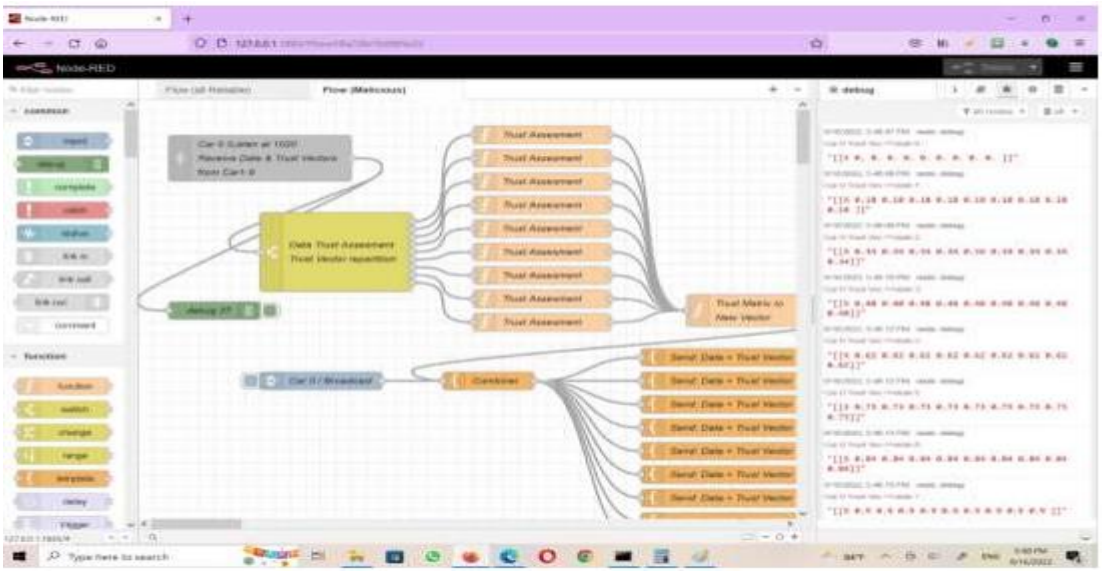
لازم به ذکر است که هر بار پس از اعتبار سنجی داده‌های حرکتی (مثال سرعت منطقی موقعیت منطقی و... که توسط یک برنامه هوش مصنوعی ارزیابی می‌گردد) مقدار ۰/۲ به عدد اعتماد هر نود اضافه می‌گردد همچنین همه نودها یک ساختار یکسان دارند. اگر همه نودها سالم باشند در هر مرحله عدد اعتماد به‌اندازه ۰/۲ افزایش‌یافته و عدد اعتماد متوسط گیری شده نیز به خاطر شرایط مشابه همه نودها $\frac{0.2+0.2+0.2+0.2+0.2+0.2+0.2+0.2+0.2+0.2}{10}$ همان ۰/۲ خواهد شد. پس از چند مرحله عدد اعتماد هر نود در برابر اعتماد به یک همگرا خواهد شد در شکل ۹، این فرآیند نشان داده‌شده است.



شکل ۹. فرآیند محاسبه و به‌روزرسانی بردار اعتماد هر نود در حالت بدون نود متخاصم

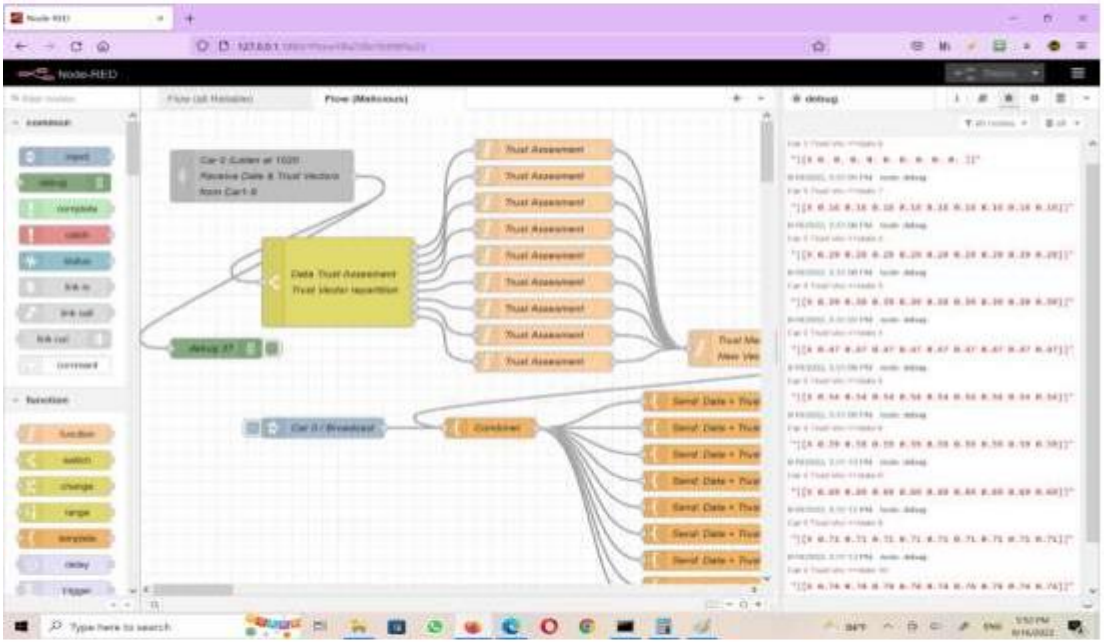
اگر یکی از نودها از این ۱۰ نود (درواقع معادل ۱۰ درصد کل نودهای شبکه) متخاصم باشد و این‌گونه عمل نماید که با ارسال اطلاعات حرکتی منطقی خود را به‌عنوان نود سالم نشان داده ولی در بردار اعتماد ارسالی، به همه همسایگان عدد صفر را اختصاص می‌دهد. آنگاه این عدد صفر باعث کاهش متوسط اعتماد محاسبه‌شده، در هر مرحله تکرار، می‌گردد. فرآیند

تغییرات بردار اعتماد باوجود یک نود متخاصم در شکل ۱۰ نشان داده‌شده است در این حالت میزان اعتماد به ۰/۹ همگرا می‌شود.



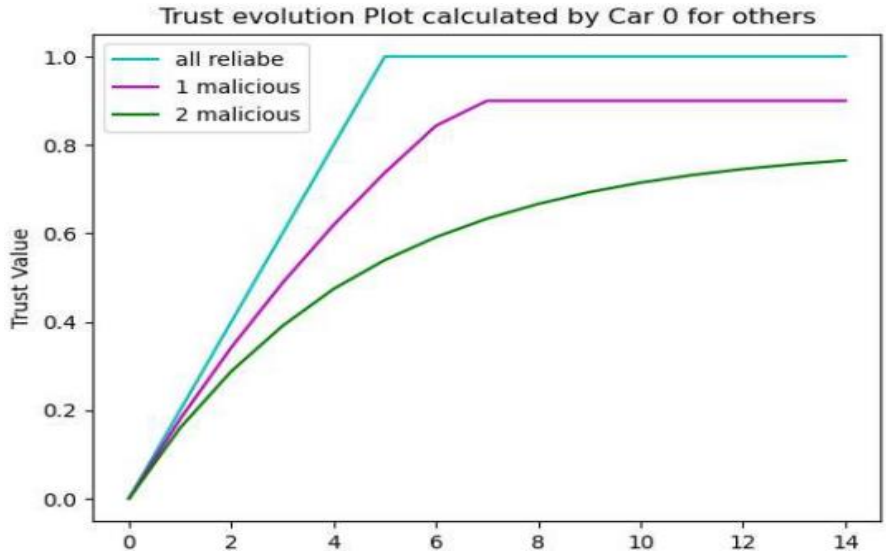
شکل ۱۰. فرآیند محاسبه و به‌روزرسانی بردار اعتماد هر نود در حالت وجود یک نود متخاصم

همچنین اگر ۲ نود شبکه (معادل ۲۰ درصد نودهای شبکه) متخاصم باشند و با اتخاذ استراتژی اعلام اعتماد صفر در تمام مراحل برای همسایگان عمل کنند آنگاه سطح متوسط اعتماد در هر مرحله تکرار، بیشتر کاهش می‌یابد. در شکل ۱۱، این فرآیند تغییرات بردار اعتماد نشان داده‌شده است. در این حالت میزان اعتماد به ۰/۸ همگرا می‌گردد.



شکل ۱۱. فرآیند محاسبه و به‌روزرسانی بردار اعتماد هر نود در حالت وجود ۲ نود متخاصم

درنهایت منحنی بردار اعتماد در سه حالت بیان‌شده که در شکل ۱۲ نشان داده‌شده است.



شکل ۱۲. منحنی تغییرات میزان اعتماد هر نود در سه حالت بررسی‌شده (بدون نود متخاصم - با یک نود متخاصم - با دو نود متخاصم)

۵. نتیجه‌گیری

از حفظ حریم خصوصی یک مسئله حیاتی برای امنیت اطلاعات است. روش‌های تأیید اعتبار و مکانیسم‌های رمزنگاری برای محافظت از حریم خصوصی کاربر استفاده می‌شود. از سوی دیگر، سازوکارهای رمزنگاری اطمینان می‌دهند که اطلاعات حساس و خصوصی در انتقال، ذخیره و پردازش محافظت می‌شود. حال برای برقراری امنیت در اینترنت اشیا با توجه به ساختار پیچیده‌ی آن ما معماری امنیتی که توسط سئو و همکارانش ارائه‌شده بود را در نظر گرفتیم و بررسی بخش‌های مختلف این ساختار به این نتیجه می‌رسیم که تنها یک سازوکار امنیتی نمی‌تواند برای مقابله با این تهدیدات کارساز باشد بلکه برای هر بخش با توجه به کاربرد و کارایی آن باید راهکار امنیتی مربوطه را در نظر گرفت.

اینترنت اشیا صنعتی تبادل خودکار داده‌ها را تسهیل می‌کند و این داده‌ها اغلب دارای اطلاعات حساس و اختصاصی هستند. دستگاه‌های اینترنت اشیا همچنین دارای قدرت پردازش ضعیف، معماری بسیار ساده و حداقل ظرفیت ذخیره‌سازی هستند. این باعث می‌شود که منابع موجود بر روی عملکردهای اصلی متمرکز شوند و درنتیجه آسیب‌پذیری‌های امنیتی و حریم خصوصی را نادیده بگیرند. مهاجمان تمایل دارند از این آسیب‌پذیری‌ها برای به خطر انداختن امنیت سیستم و دسترسی به داده‌های محرمانه استفاده کنند. سامانه‌های دفاع امنیتی متعارف معمولاً معماری‌های امنیتی متمرکزی دارند که ازنظر محاسباتی گران، حسابرسی دشوار و آسیب‌پذیر هستند، به‌ویژه با افزایش تعداد دستگاه‌های متصل این مسائل را می‌توان توسط زنجیره بلوکی با رویکرد ایمن، توزیع‌شده و غیرمتمرکز آن برطرف کرد. زنجیره بلوکی با سیستم توزیع‌شده خود تضمین می‌کند که تراکنش‌ها سریع، امن و خصوصی هستند. این انعطاف‌پذیری عالی را برای مهاجمان فراهم می‌کند زیرا زنجیره بلوکی را نمی‌توان دست‌کاری یا ویرایش کرد. ادغام مداوم آن با معماری اینترنت اشیا صنعتی در حال حاضر منجر به دگرگونی‌های قابل‌توجهی در صنایع مختلف شده است، مدل‌های کسب‌وکار جدید را به ارمغان می‌آورد و بازنگری در نحوه پیاده‌سازی سامانه‌ها و فرآیندهای موجود را تسهیل می‌کند. سیستم پیشنهادی حجم وسیعی از داده‌ها را برای محصولات و کاربران در صنعت تولید جمع‌آوری می‌کند که می‌تواند برای طیف وسیعی از افراد و سازمان‌ها مفید باشد. برای مثال، این سیستم به مصرف‌کنندگان اجازه می‌دهد که به‌آسانی به داده‌های دقیق مربوط به هر محصولی که از طریق زنجیره تأمین فعال ساخته‌شده است، دسترسی داشته باشند و درنتیجه به آن‌ها اجازه تصمیم‌گیری بهتر را می‌دهد. سازمان‌های درگیر در طراحی، ساخت و تولید می‌توانند درک بهتری از چگونگی استفاده از محصولات خود در زنجیره تأمین تحت پوشش زنجیره

بلوکی به دست آورند. این سطح بازخورد می‌تواند برای بهبود فن‌آوری و بازاریابی آن‌ها و همچنین برنامه‌ریزی تولید و برنامه فروش آن‌ها مورداستفاده قرار گیرد. علاوه بر این، زنجیره بلوکی همچنین می‌تواند برای انتقال اطلاعات و تخصیص منابع بین دستگاه‌ها برای کنترل و مدیریت کارآمد آن‌ها استفاده شود. اگرچه چالش‌هایی در معرفی زنجیره بلوکی به صنایع اصلی عمدتاً به دلیل هزینه‌های محاسباتی، تأیید تراکنش و مسائل یکپارچه‌سازی وجود دارد، آینده آن در چشم‌انداز اینترنت اشیا صنعتی بسیار امیدوارکننده به نظر می‌رسد.

۶. مراجع

[1] Djedjig, N., Tandjaoui, D., Medjek, F., & Romdhani, I. (2020). Trust-aware and cooperative routing protocol for IoT security. *Journal of Information Security and Applications*, *52*, 102467.

[2] Niraja, K. S., & Rao, S. S. (2021). A hybrid algorithm design for near real time detection cyber attacks from compromised devices to enhance IoT security. *Materials Today: Proceedings*.

[3] Mahbub, M. (2020). Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *Journal of Network and Computer Applications*, *168*, 102761.

[4] Huang, S. Lin, C. Zhou, K. Yao, Y. Lu, H. & Zhu, F. (2020). Identifying physical-layer attacks for IoT security: An automatic modulation classification approach using multi-module fusion neural network. *Physical Communication*, *43*, 101180.

[5] Alzahrani, B. & Fotiou, N. (2020). Enhancing internet of things security using software-defined networking. *Journal of Systems Architecture*, *110*, 101779.

[6] Hajiheidari, S. Wakil, K. Badri, M. & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. *Computer Networks*, *160*, 165-191.

[7] Yan, H. Chen, Z. & Jia, C. (2019). SSIR: Secure similarity image retrieval in IoT. *Information Sciences*, *479*, 153-163.

[8] Roldán, J. Boubeta-Puig, J. Martínez, J. L. & Ortiz, G. (2020). Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks. *Expert Systems with Applications*, *149*, 113251.

[9] Velmurugan, P., Sridhar, S. S., & Gotham, E. (2021). An advanced and effective encryption methodology used for modern IoT security. *Materials Today: Proceedings*.

[10] Miraz, M. H., & Ali, M. (2018). Applications of blockchain technology beyond cryptocurrency. *arXiv preprint arXiv:1801.03528*.

[11] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

[12] Conoscenti, M., Vetro, A., & De Martin, J. C. (2016, November). Blockchain for the Internet of Things: A systematic literature review. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)* (pp. 1-6). IEEE.

[13] Gross, H., Hölbl, M., Slamanig, D., & Spreitzer, R. (2015, December). Privacy-aware authentication in the internet of things. In *International Conference on Cryptology and Network Security* (pp. 32-39). Springer, Cham.

[14] Sharma, T. K. (2018). How does blockchain use public key cryptography. *Preuzeto*, *24*, 2020.

[15] Huh, S., Cho, S., & Kim, S. (2017, February). Managing IoT devices using blockchain platform. In *2017 19th international conference on advanced communication technology (ICACT)* (pp. 464-467). IEEE.

[16] Colombo, A. W., Bangemann, T., Karnouskos, S., Delsing, J., Stluka, P., Harrison, R., ... & Lastra, J. L. (2014). Industrial cloud-based cyber-physical systems. *The Imc-aesop Approach*, *22*, 4-5.
[17] Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. *Digital Communications and Networks*, *4*(3), 149-160.
[18] Wu, D., Thames, J. L., Rosen, D. W., & Schaefer, D. (2013). Enhancing the product realization process with cloud-based design and manufacturing systems. *Journal of Computing and Information Science in Engineering*, *13*(4).
[19] Teslya, N., & Ryabchikov, I. (2018, May). Blockchain platforms overview for industrial IoT purposes. In *2018 22nd Conference of Open Innovations Association (FRUCT)* (pp. 250-256). IEEE.
[20] Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, 254–269.. ACM.
[21] Brody, P., & Pureswaran, V. (2014). Device democracy: Saving the future of the internet of things. *IBM, September*, *1*(1), 15.
[22] Jesus, E. F., Chicarino, V. R., De Albuquerque, C. V., & Rocha, A. A. D. A. (2018). A survey of how to use blockchain to secure internet of things and the stalker attack. *Security and Communication Networks*, *2018*.
[23] Buck J (2017) Bringing blockchain to IoT. https://cointelegraph.com/news/bringingblockchain-to-iot. Accessed Jan2019.
[24] Chrisjan P (2018) How significant is blockchain in Internet of Things? https://cointelegraph. com/news/how-significant-is-blockchain-in-internetof-things/. Accessed Feb 2019.
[25] Dickson, B. (2016). Blockchain has the potential to revolutionize the supply chain. Tech Crunch, 25.
[26] Rooyen JV (2017) Blockchains for supply chain—part 1. https://resolvesp.com/blockchainssupply-chains/. Accessed Jan 2019.
[27] Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of information management*, *39*, 80-89.
[28] Miller, D. (2018). Blockchain and the internet of things in the industrial sector. *IT professional*, *20*(3), 15-18.
[29] Siegfried, N., Rosenthal, T., & Benlian, A. (2020). Blockchain and the Industrial Internet of Things: A requirement taxonomy and systematic fit analysis. *Journal of Enterprise Information Management*.
[30] Peltonen, A., Inglés, E., Latvala, S., Garcia-Carrillo, D., Sethi, M., & Aura, T. (2020). Enterprise security for the internet of things (IoT): lightweight bootstrapping with EAP-NOOB. *Sensors*, *20*(21), 6101.
[31] Miskiewicz, R. (2020). Internet of things in marketing: Bibliometric analysis.
[32] ur Rehman, M. H., Yaqoob, I., Salah, K., Imran, M., Jayaraman, P. P., & Perera, C. (2019). The role of big data analytics in industrial Internet of Things. *Future Generation Computer Systems*, *99*, 247-259.
[33] Fu, H., Wang, M., Li, P., Jiang, S., Hu, W., Guo, X., & Cao, M. (2019). Tracing knowledge development trajectories of the internet of things domain: A main path analysis. *IEEE Transactions on Industrial Informatics*, *15*(12), 6531-6540.
[34] Latif, S., Idrees, Z., e Huma, Z., & Ahmad, J. (2021). Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges,

architectures, applications, and future research directions. *Transactions on Emerging Telecommunications Technologies*, *32*(11), e4337.

[35] Jaskani, F., Manzoor, S., Amin, M., Asif, M., & Irfan, M. (2019). An investigation on several operating systems for internet of things. *EAI Endorsed Transactions on Creative Technologies*, *6*(18).

[36] Bi, Z., Jin, Y., Maropoulos, P., Zhang, W. J., & Wang, L. (2021). Internet of things (IoT) and big data analytics (BDA) for digital manufacturing (DM). *International Journal of Production Research*, 1-18.

[37] Wang, J., Chen, J., Ren, Y., Sharma, P. K., Alfarraj, O., & Tolba, A. (2022). Data security storage mechanism based on blockchain industrial Internet of Things. *Computers & Industrial Engineering*, *164*, 107903.

[38] Rondon, L. P., Babun, L., Aris, A., Akkaya, K., & Uluagac, A. S. (2022). Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective. *Ad Hoc Networks*, *125*, 102728.

[39] Hansen, E. B., & Bøgh, S. (2021). Artificial intelligence and internet of things in small and medium-sized enterprises: A survey. *Journal of Manufacturing Systems*, *58*, 362-372.

[40] Blythe, J. M., Johnson, S. D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science*, *9*(1), 1-9.

[41] Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies and open challenges. *Computers & Electrical Engineering*, *81*, 106522.

[42] Kumar, R. L., Khan, F., Kadry, S., & Rho, S. (2022). A survey on blockchain for industrial internet of things. *Alexandria Engineering Journal*, *61*(8), 6001-6022.