**امنیت اینترنت اشیاء (IoT): بررسی، راه‌حل‌های بلاک‌چین، و چالش‌های باز**

**چکیده**

با ظهور خانه‌های هوشمند، شهرهای هوشمند، و اشیاء هوشمند، مفهوم اینترنت اشیاء (IoT) ظهور کرده است، به عنوان حوزه‌ای که تاثیر، پتانسیل، و رشد غیرقابل باوری داشته و با پیش‌بینی شرکت سیسکو تا سال 2020 نزدیک به 50 میلیارد دستگاه به هم متصل خواهند بود. با این حال، هک کردن اکثر این دستگاه‌های اینترنت اشیاء ساده است و این دستگاه‌ها در معرض خطر هستند. به طور معمول، این دستگاه‌های اینترنت اشیاء توانایی‌های محاسباتی، ذخیره‌سازی، و ظرفیت شبکه‌ای محدودی دارند و بنابراین آنها نسبت به دیگر دستگاه‌های انتهایی از قبیل گوشی‌های هوشمند، تب‌لت‌ها، یا کامپیوترها بیشتر در برابر حمله‌ها آسیب‌پذیرتر هستند.

ما در این مقاله به بررسی و مرور مسائل عمده‌ی امنیتی در اینترنت اشیاء می‌پردازیم. ما مسائل امنیتی مشهور را با توجه به معماری لایه‌ای اینترنت اشیاء مرور و دسته‌بندی می‌کنیم، علاوه بر این پروتکل‌های استفاده شده برای شبکه‌بندی، ارتباطات، و مدیریت را نیز بررسی و مرور می‌کنیم. ما نیازهای امنیتی برای اینترنت اشیاء را به همراه حمله‌ها، تهدیدات، و راه‌حل‌های نوآورانه مطرح می‌کنیم. علاوه بر این، مسائل امنیتی اینترنت اشیاء را با راه‌حل‌های موجود در مقالات مرتبط دیگر جدول‌بندی و ترسیم می‌کنیم. از همه مهمتر اینکه ما در مورد چگونگی بلاک‌چین بحث می‌کنیم، بلاک‌چین که یک فناوری زیرساخت برای بیت‌کوین است و می‌تواند یک عامل کلیدی برای حل مسائل امنیتی زیادی در اینترنت اشیاء باشد. این مقاله همچنین مسائل باز تحقیقاتی و چالش‌های موجود در امنیت اینترنت اشیاء را شناسایی می‌کند.

**کلمات کلیدی:** امنیت IoT؛ بلاک‌چین؛ پروتکل‌های IoT؛ امنیت شبکه؛ امنیت داده‌ها.

**1. مقدمه**

با رشد سریع دستگاه‌های هوشمند و شبکه‌های پر سرعت، اینترنت اشیاء (IoT) به پذیرش عمومی و محبوبیت گسترده‌ای به عنوان استاندارد اصلی برای شبکه‌های کم توان و پر اتلاف (LLNs) دست یافته است، شبکه‌های LLN که منابع محدودی دارند. اینترنت اشیاء شبکه‌ای را ارائه می‌دهد که در آن "اشیاء" یا دستگاه‌های تعبیه شده دارای حسگرهایی هستند که از طریق یک شبکه‌ی خصوصی یا عمومی به هم متصل شده‌اند [2 و 1]. دستگاه‌ها در اینترنت اشیاء می‌توانند از راه دور کنترل شوند تا عملکرد موردنظر را انجام دهند. اشتراک‌گذاری اطلاعات میان دستگاه‌ها سپس از طریق شبکه‌ای انجام می‌شود که از پروتکل‌های استاندارد ارتباطی استفاده می‌کند. محدوده‌ی دستگاه‌های هوشمند به هم متصل یا "اشیاء" از لوازم زینتی ساده‌ی قابل پوشیدن گرفته تا ماشین‌های بزرگ را شامل می‌شود که هر یک دارای تراشه‌های حسگر هستند. به عنوان مثال، کفش‌های هوشمند Lenovo شامل تراشه‌هایی است که پشتیبانی از ردیابی و تحلیل داده‌های تناسب اندام را فراهم می‌کنند [3]. به طور مشابه، لوازم خانگی الکتریکی شامل ماشین‌های لباسشویی، و یخچال‌ها می‌توانند به صورت از راه دور از طریق اینترنت اشیاء کنترل شوند. دوربین‌های امنیتی نصب شده برای نظارت بر یک مکان نیز می‌توانند در هر نقطه از جهان به صورت از راه دور کنترل و نظارت شوند.

به غیر از استفاده‌ی شخصی، اینترنت اشیاء به نیازهای جامعه نیز به خوبی پاسخ می‌دهد. دستگاه‌های هوشمند متعددی که در حال حاضر با عملکردهای متنوعی از قبیل نظارت بر جراحی در بیمارستان‌ها، تشخیص شرایط آب و هوایی، فراهم نمودن ردیابی و اتصال در اتومبیل‌ها، و شناسایی حیوانات با استفاده از تراشه‌های زیستی[[1]](#footnote-1) به نیازهای خاص جامعه پاسخ می‌دهند [4]. داده‌هایی که از طریق این دستگاه‌ها جمع‌آوری شده‌اند، ممکن است به صورت بی‌درنگ پردازش شوند تا کارایی کل سیستم بهبود یابد.

اهمیت آینده‌ی اینترنت اشیاء به دلیل کاربرد آن در زندگی روزمره‌ی کاربران کاملا مشهود است. به علت تکامل روش‌های سخت‌افزاری از قبیل بهبود پهنای‌باند با استفاده از شبکه‌های رادیو شناختی جهت رسیدگی به طیف‌های فرکانسی کمتر مصرف شده، اینترنت اشیاء به سرعت در حال رشد است [6 و 5]. در ادبیات این حوزه، شبکه‌های حسگر بی‌سیم[[2]](#footnote-2) (WSN) سیستم‌های ماشین-به-ماشین[[3]](#footnote-3) (M2M) یا سیستم‌های سایبری-فیزیکی[[4]](#footnote-4) (CPS) به عنوان اجزای تکمیلی برای مفهوم گسترده‌تر اینترنت اشیاء تکامل یافته‌اند. در نتیجه، مسائل امنیتی مربوط به WSN، M2M، یا CPS نیز در زمینه‌ی اینترنت اشیاء با پروتکل IP به عنوان استاندارد اصلی برای اتصال به وجود می‌آید. بنابراین معماری استقرار کلی باید از حمله‌ها در امان باشد، زیرا ممکن است سرویس‌های ارائه شده توسط اینترنت اشیاء با مشکل مواجه شوند و همچنین حریم خصوصی، یکپارچگی یا محرمانگی داده‌ها نیز در معرض خطر قرار بگیرند. از آنجایی که الگوی اینترنت اشیاء در واقع مجموعه‌ای از شبکه‌ها، و دستگاه‌های ناهمگن به هم متصل است، به همین دلیل این الگو مسائل امنیتی رایج در شبکه‌های کامپیوتری را نیز به ارث می‌برد. منابع محدود نیز چالش‌های بیشتری را برای امنیت اینترنت اشیاء ایجاد می‌کند، زیرا دستگاه‌های کوچک یا اشیاء حاوی حسگر، حافظه و توان محدودی دارند. در نتیجه، راه‌حل‌های امنیتی باید با معماری‌های طراحی شده برای منابع محدود سازگار شوند.

در سال‌های اخیر تلاش زیادی برای مقابله با مسائل امنیتی در الگوی اینترنت اشیاء صورت گرفته است. برخی از این رویکردها تنها به مسائل امنیتی در یک لایه‌ی خاص توجه می‌کنند، در حالی که رویکردهای دیگر سعی دارند امنیت انتها-به-انتها[[5]](#footnote-5) را برای اینترنت اشیاء فراهم کنند. در بررسی جدیدی که توسط Alaba و همکارانش [7] صورت گرفته است، مسائل امنیتی از لحاظ کاربرد، معماری، ارتباطات، و داده‌ها دسته‌بندی شده‌اند. این دسته‌بندی پیشنهادی برای امنیت اینترنت اشیاء با معماری لایه‌ای رایج تفاوت دارد. سپس تهدیدات موجود برای اینترنت اشیاء در زمینه‌ی اجزای سخت‌افزاری، شبکه و برنامه‌های کاربردی مورد بحث قرار گرفته است. به طور مشابه، بررسی دیگری که توسط Granjal و همکارانش [8] صورت گرفته است، مسائل امنیتی موجود در پروتکل‌های تعریف شده برای اینترنت اشیاء را مورد بررسی و تحلیل قرار داده است. تحلیل‌های امنیتی ارائه شده در مراجع [11-9] به بحث و مقایسه‌ی سیستم‌های متفاوت مدیریت کلید و الگوریتم‌های رمزنگاری پرداخته‌اند. به طور مشابه، نویسندگان مراجع [14-12] به ارائه‌ی یک ارزیابی مقایسه‌ای از سیستم‌های تشخیص نفوذ پرداخته‌اند. تحلیلی از مسائل امنیتی محاسبات مه در مراجع [16 و 15] ارائه شده است. یک بررسی صورت گرفته توسط Sicari و همکارانش [17] در مورد روش‌های پیشنهاد شده برای فراهم نمودن محرمانگی، امنیت، کنترل دسترسی و حریم خصوصی در اینترنت اشیاء به همراه امنیت میان‌افزار بحث می‌کند. نویسندگان در مورد مدیریت اعتماد، احراز هویت، مسائل حریم خصوصی، امنیت داده‌ها، امنیت شبکه، و سیستم‌های تشخیص نفوذ بحث می‌کنند. الگوهای مبتنی بر محاسبه لبه‌ای مه از جمله محاسبات ابری متحرک[[6]](#footnote-6)، محاسبات لبه‌ای متحرک و محاسبات مه، هویت و احراز هویت، سیستم‌های کنترل دسترسی، امنیت شبکه، مدیریت اعتماد، تحمل‌پذیری خطا و پیاده‌سازی قانونی در مرجع [18] مورد بحث قرار گرفته‌اند.

مروری بر روش‌های حفاظت از حریم خصوصی در اینترنت اشیاء در مرجع [19] ارائه شده است. نویسنده‌ی این مرجع به شرح محاسبات چند-طرفی[[7]](#footnote-7) پرداخته است که برای حفاظت از حریم خصوصی کاربران اینترنت اشیاء مورد استفاده قرار می‌گیرند. روش‌های بررسی اعتبار و کنترل دسترسی مبتنی بر ویژگی به عنوان راه‌حل‌های کارآمدی برای حفاظت از حریم خصوصی در اینترنت اشیاء شرح داده شده‌اند. Zhou و همکارانش [20] به بحث در مورد تهدیدات مختلف امنیتی و اقدامات احتمالی مقابله‌ای برای اینترنت اشیاء مبتنی بر ابر پرداخته‌اند. نویسندگان این مرجع، تهدیدات حریم خصوصی هویت و مکان، به خطر افتادن گره، اضافه یا حذف لایه، و مدیریت کلید برای اینترنت اشیاء را با استفاده از ابرها شرح داده‌اند. بررسی دیگری توسط Zhang و همکارانش [21] در مورد مسائل مهم امنیتی در اینترنت اشیاء از لحاظ شناسایی منحصربه‌فرد اشیاء، احراز هویت و مجوز دسترسی، حریم خصوصی، نیاز به روش‌های رمزنگاری سبک، بدافزار، و آسیب‌پذیری‌های نرم‌افزاری بحث می‌کند. اینترنت اشیاء-یک پروژه در مرجع [21] در واقع یک معماری مرجع برای اینترنت اشیاء را شرح می‌دهد که با نیازهای پیاده‌سازی اعتماد، حریم خصوصی، و امنیت منطبق است. مدل اعتماد انتظار دارد که یکپارچگی (صحت) داده‌ها و محرمانگی فراهم شود، در حالی که ارتباطات انتها-به-انتها را از طریق یک روش احراز هویت ممکن می‌سازد. علاوه بر این، برای پیشگیری از استفاده‌ی نابه‌جا (غیرمجاز) از داده‌ها، مدل حریم خصوصی نیاز دارد که سیاست‌ها و روش‌های دسترسی برای رمزنگاری و رمزگشایی تعریف شوند. جنبه‌ی امنیتی از ترکیب سه لایه برای سرویس‌ها، ارتباطات، و برنامه‌های کاربردی تشکیل شده است. به طور مشابه، پروژه‌ی امنیتی متن‌باز برنامه‌ی کاربردی وب[[8]](#footnote-8) (OWASP) [23] به شرح ده عدد آسیب‌پذیری رایج برای معماری اینترنت اشیاء می‌پردازد. این آسیب‌پذیری‌ها عبارتند از واسط‌های ناامن موجودیت‌های معماری اینترنت اشیاء، پیکربندی نامناسب امنیتی، امنیت فیزیکی و نرم‌افزار/firmware ناامن.

در مقایسه با مقالات مروری دیگر، نوآوری‌های ما در این مقاله را می‌توان به صورت زیر خلاصه کرد:

* تحلیل پارامتری تهدیدات امنیتی و نگاشت آنها به راه‌حل‌های ممکن برای اینترنت اشیاء.
* دسته‌بندی مسائل امنیتی اینترنت اشیاء با توجه به لایه‌های آن، و اقدامات مقابله‌ای استفاده شده برای رسیدگی به این مسائل.
* بحث در مورد مشخصات اصلی راه‌حل‌های امنیتی مبتنی بر بلاک‌چین و تحلیل کارایی آنها برای امن نمودن اینترنت اشیاء.
* مطرح نمودن مسیرهای تحقیقاتی آینده برای راه‌حل‌های ممکن جهت مسائل باز امنیت اینترنت اشیاء.

مقاله در ادامه به صورت زیر سازماندهی شده است. بخش 2 به معرفی معماری اینترنت اشیاء و چالش‌های امنیتی می‌پردازد، چالش‌هایی که هر لایه از پشته‌ی پروتکلی مستقر در اینترنت اشیاء با آنها روبرو است. بخش 3 مسائل مهم امنیتی را دسته‌بندی می‌کند، در حالی که بخش 4 نگاشتی از راه‌حل‌های پیشنهادی را تحلیل کرده و شرح می‌دهد. راه‌حل‌های متعددی مربوط به امنیت بلاک‌چین در بخش 5 مورد بحث و تحلیل قرار گرفته است. ما در بخش 6، در مورد موانع موجود برای امنیت اینترنت اشیاء و راه‌حل‌های ممکن برای آنها بحث کرده و سپس در بخش 7 از مقاله نتیجه‌گیری می‌کنیم.

**2. معماری اینترنت اشیاء و چالش‌های امنیتی**

همانطور که در شکل 1 نشان داده شده است، یک استقرار معمولی اینترنت اشیاء شامل دستگاه‌های ناهمگن با حسگرهای نهفته‌ای است که از طریق یک شبکه متصل شده‌اند. دستگاه‌ها در اینترنت اشیاء به صورت منحصربه‌فردی قابل شناسایی هستند و اغلب با مشخصاتی از قبیل توان کم، حافظه‌ی کوچک و قابلیت پردازشی محدود مشخص می‌شوند. دروازه‌ها برای اتصال دستگاه‌های اینترنت اشیاء با دنیای بیرون مستقر می‌شوند تا داده‌ها و سرویس‌ها را به صورت از راه دور برای کاربران اینترنت اشیاء فراهم نمایند.



شکل 1. مرور کلی بر عناصر اینترنت اشیاء.

*2-1. پروتکل‌ها و استانداردهای اینترنت اشیاء*

شکل 2 یک معماری لایه‌ای با پروتکل‌های رایج اینترنت اشیاء را نشان می‌دهد که برای برنامه‌های کاربردی و پیام‌رسانی، مسیریابی/هدایت، دستگاه‌های فیزیکی مورد استفاده قرار می‌گیرند و همچنین موارد کلیدی برای مدیریت و احراز هویت را نشان می‌دهد. این معماری شامل استانداردها و پروتکل‌هایی است که معمولا برای شبکه‌های بی‌سیم شخصی با نرخ پایین[[9]](#footnote-9) (LR-WPANs) [24] مورد استفاده قرار می‌گیرند، و همچنین شامل پروتکل‌هایی است که به تازگی برای شبکه گسترده‌ی کم توان[[10]](#footnote-10) (LPWAN) تکامل یافته‌اند.



شکل 2. پروتکل‌ها و استانداردهای رایج اینترنت اشیاء.

برای LR-WPANها، 802.15.4 استاندارد IEEE دو لایه‌ی سطح پایین را توصیف می‌کند: لایه‌ی فیزیکی و لایه‌ی کنترل دسترسی به رسانه[[11]](#footnote-11) (MAC). مشخصات لایه‌ی فیزیکی مربوط به ارتباطات از طریق کانال‌های بی‌سیمی است که باندهای فرکانسی مختلف و نرخ‌های داده‌ی متفاوتی دارند. مشخصات لایه‌ی MAC مربوط به روش‌هایی برای دسترسی به کانال و همچنین هماهنگ‌سازی است. با توجه به کوچک بودن حداکثر واحد انتقال[[12]](#footnote-12) (MTU) استفاده شده توسط استاندارد IEEE 802.15.4، یک لایه‌ی تطبیق IPv6 بر روی شبکه شخصی بی‌سیم کم-توان (6LoWPAN) بر روی لایه‌ی پیوند قرار گرفته است تا توانایی‌های ارتباطی مبتنی بر IP گره‌ی حسگر را افزایش دهد. هر دستگاه در اینترنت اشیاء به صورت منحصربه‌فرد با یک آدرس شبکه‌ی IPv6 شناسایی می‌شود. پروتکل مسیریابی برای شبکه‌های کم-توان و با اتلاف[[13]](#footnote-13) (RPL) [25] برای پشتیبانی از محیط‌های 6LoWPAN مورد استفاده قرار می‌گیرد. استاندارد RPL از ترافیک نقطه-به-نقطه و همچنین ارتباطات بین چندین نقطه و یک نقطه پشتیبانی می‌کند.

به علت محدود بودن محموله‌ی بار بسته[[14]](#footnote-14)، طراحی برنامه‌ی کاربردی در اینترنت اشیاء از پروتکل دیتاگرام کاربر[[15]](#footnote-15) (UDP) [26] برای ارتباطات استفاده می‌کند، زیرا این پروتکل نسبت به TCP کارآمدتر بوده و پیچیدگی کمتری دارد. علاوه بر این، فشرده‌سازی سرآیند[[16]](#footnote-16) (هِدر) UDP ممکن است برای استفاده‌ی بهتر از فضای محدود محموله‌ی بار بسته انجام شود [27]. برای پیام‌های کنترلی، از قبیل مشخص نمودن مقصد غیرقابل‌دسترس، و کشف همسایه، پروتکل پیام کنترل اینترنت[[17]](#footnote-17) (ICMP) [28] توسط 6LoWPAN مورد استفاده قرار می‌گیرد. پروتکل برنامه کاربردی محدود (CoAP) [29] یک مدل مبتنی بر درخواست-پاسخ برای شبکه‌های کم-توان و با اتلاف زیاد در محیط‌های با منابع محدود ارائه می‌دهد. پروتکل CoAP از ارتباطات پیام به صورت ناهمگام پشتیبانی می‌کند و همچنین نگاشت HTTP را برای دسترسی به منابع اینترنت اشیاء از طریق HTTP ارائه می‌دهد.

LPWAN ارتباطات بلند بُرد را برای "اشیاء" در اینترنت اشیاء ممکن می‌سازد. در مقایسه با یک WAN بی‌سیم که نیاز به توان بیشتری برای کار با نرخ-بیت بالا دارد، LPWAN از ارتباطات کم-توان با نرخ-بیت پایین پشتیبانی می‌کند. LPWAN از پروتکل LoRaWAN برای ارتباطات بین دروازه‌ها و دستگاه‌های انتهایی استفاده می‌کند، در عین اینکه از نرخ‌های مختلف داده در یک شبکه با اشیائی پشتیبانی می‌کند که این اشیاء با باتری کار می‌کنند. به طور مشابه، باند-باریک اینترنت اشیاء[[18]](#footnote-18) (NB-IoT) در واقع یک پروتکل 3GPP برای ارتباطات در LPWAN است که پوشش داخل ساختمان را با استفاده از طیف LTE ارائه می‌دهد. پروتکل بی‌وزن[[19]](#footnote-19) از سه استاندارد مختلف برای ارتباطات در LPWAN استفاده می‌کند تا به ترتیب از حالت‌های یک-طرفه، دو طرفه و کم-توان پشتیبانی کند.

*2-2. نیازهای امنیتی برای اینترنت اشیاء*

برای یک استقرار امن اینترنت اشیاء، روش‌ها و پارامترهای متعددی مورد نیاز هستند که در ادامه شرح داده می‌شوند.

*2-2-1. حریم خصوصی، محرمانگی و یکپارچگی داده‌ها*

از آنجایی که داده‌های اینترنت اشیاء از طریق چندین گام در شبکه منتقل می‌شوند، یک روش رمزنگاری مناسب برای تضمین محرمانگی داده‌ها مورد نیاز است. با توجه به ادغام سرویس‌ها، دستگاه‌ها و شبکه‌های متنوع، داده‌های ذخیره شده بر روی یک دستگاه در برابر نقض حریم خصوصی آسیب‌پذیر هستند و این نقض ممکن است با در معرض خطر قرار گرفتن گره‌های موجود در یک شبکه‌ی اینترنت اشیاء رخ دهد. دستگاه‌های اینترنت اشیاء در برابر حمله‌هایی حساس هستند که ممکن است یک مهاجم قصد داشته باشد با دستکاری داده‌های ذخیره شده برای اهداف خرابکارانه، یکپارچگی و صحت داده‌ها را از بین ببرد.

*2-2-2. احراز هویت، صدور مجوز دسترسی و حسابرسی*

برای امن نمودن ارتباطات در اینترنت اشیاء، احراز هویت بین دو طرف ارتباط مورد نیاز است. برای دسترسی خاص و مجاز به سرویس‌ها، دستگاه‌ها باید احراز هویت شوند. تنوع روش‌های احراز هویت ارائه شده برای اینترنت اشیاء عمدتا به دلیل تنوع معماری‌ها و محیط‌های ناهمگن زیرساخت است که از دستگاه‌های اینترنت اشیاء پشتیبانی می‌کنند. این محیط‌ها با چالشی برای تعریف پروتکل کلی استاندارد برای احراز هویت در اینترنت اشیاء روبرو هستند. به طور مشابه، روش‌های صدور مجوز دسترسی تضمین می‌کنند که دسترسی به سیستم‌ها یا اطلاعات تنها با موارد مجاز و دارای مجوز دسترسی صورت می‌گیرد. یک پیاده‌سازی مناسب از روش‌های صدور مجوز دسترسی و احراز هویت می‌تواند باعث ایجاد یک محیط قابل اعتماد شود که محیط امنی را برای ارتباط تضمین می‌کند. علاوه بر این، حسابرسی به مصرف منابع به همراه بازرسی و گزارش‌دهی نیز یک روش قابل‌اطمینان برای مدیریت امن شبکه است.

*2-2-3. دسترس‌پذیری سرویس‌ها*

حمله‌هایی که بر روی دستگاه‌های اینترنت اشیاء صورت می‌گیرند، ممکن است از طریق حمله‌های رایج جلوگیری از سرویس[[20]](#footnote-20) (DoS) مانع از ارائه‌ی سرویس‌ها شوند. استراتژی‌های مختلفی از جمله حمله‌های sinkhole، مهاجمین تولیدکننده‌ی پارازیت[[21]](#footnote-21)، یا حمله‌های بازپخش[[22]](#footnote-22)، به سوءاستفاده از اجزای موجود در لایه‌های مختلف اینترنت اشیاء می‌پردازند تا کیفیت سرویس[[23]](#footnote-23) (QoS) ارائه شده به کاربران اینترنت اشیاء را تضعیف نمایند.

*2-2-4. بهره‌وری انرژی*

دستگاه‌های اینترنت اشیاء معمولا منابع محدودی دارند و با توان کم و ظرفیت ذخیره‌سازی کم مشخص می‌شوند. حمله‌های صورت گرفته بر روی معماری‌های اینترنت اشیاء ممکن است باعث افزایش مصرف انرژی شوند، این حمله‌ها با ارسال سیل‌آسای درخواست‌های جعلی یا تکراری برای سرویس‌ها موجب اتلاف منابع اینترنت اشیاء می‌شوند.

*2-3. نقاط انفرادی شکست*

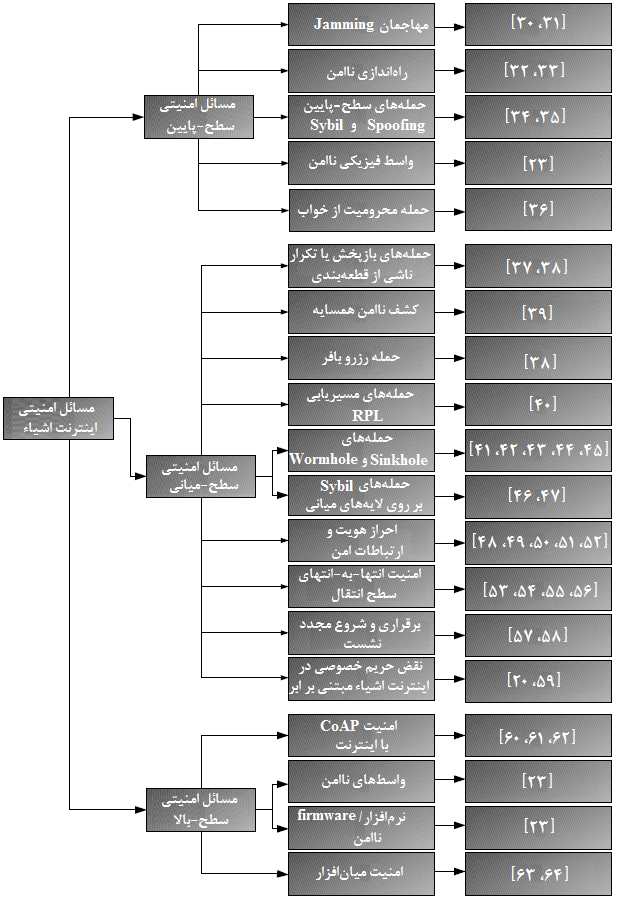
رشد مداوم شبکه‌های ناهمگن برای زیرساخت مبتنی بر اینترنت اشیاء ممکن است باعث ایجاد تعداد زیادی نقاط شکست انفرادی شود که این امر منجر به خرابی سرویس‌های پیش‌بینی شده از طریق اینترنت اشیاء می‌شود. این امر نیاز به توسعه‌ی یک محیط غیرقابل دستکاری برای تعداد زیادی از دستگاه‌های اینترنت اشیاء و همچنین ارائه‌ی روش‌های جایگزین برای پیاده‌سازی یک شبکه‌ی تحمل‌پذیر خطا دارد.

**3. دسته‌بندی مسائل امنیتی**

از آنجایی که الگوی اینترنت اشیاء طیف گسترده‌ای از وسایل و تجهیزات، از تراشه‌های پردازشی نهفته‌ی کوچک گرفته تا سرورهای بزرگ انتهایی را در بر می‌گیرد، نیاز دارد تا مسائل امنیتی در سطوح مختلفی رسیدگی شوند.

یک دسته‌بندی از مسائل امنیتی برای اینترنت اشیاء در شکل 3 به همراه مراجع مربوط به هر مسئله ارائه شده است. ما تهدیدات امنیتی را با توجه به معماری استقرار اینترنت اشیاء به شرح زیر دسته‌بندی می‌کنیم.

* مسائل امنیتی سطح پایین
* مسائل امنیتی سطح میانی
* مسائل امنیتی سطح بالا



شکل 3. دسته‌بندی مسائل امنیتی و مراجع مرتبط

*3-1. مسائل امنیتی سطح پایین*

سطح اول امنیت مربوط به مسائل امنیتی در لایه‌های فیزیکی و پیوند داده در ارتباطات و همچنین سطح سخت‌افزار است که در ادامه شرح داده شده‌اند.

**مهاجمان حمله‌ی jamming** (پارازیت). حمله‌های jamming بر روی دستگاه‌های بی‌سیم در اینترنت اشیاء سعی در از بین بردن شبکه‌ها دارند و این کار را با خراب کردن سیگنال‌های فرکانس رادیویی بدون دنبال کردن پروتکل خاصی انجام می‌دهند [30 و 31]. تداخل رادیویی به شدت بر عملیات شبکه تاثیر می‌گذارد و می‌تواند بر ارسال و دریافت داده‌ها توسط گره‌ها اثر بگذارد، در نتیجه به عملکرد بد یا رفتار غیرقابل پیش‌بینی سیستم منجر شود.

**راه‌اندازی اولیه‌ی ناامن**. یک روش امن برای راه‌اندازی و پیکربندی اینترنت اشیاء در لایه‌ی فیزیکی، عملکرد صحیح و مناسب کل سیستم را بدون نقض حریم خصوصی و اختلال سرویس‌های شبکه تضمین می‌کند [32 و 33]. ارتباطات لایه‌ی فیزیکی نیز باید امن شوند تا در دسترس گیرنده‌های غیرمجاز قرار نگیرند.

**حمله‌های سطح-پایین Sybil و Spoofing**. حمله‌های Sybil در یک شبکه‌ی بی‌سیم توسط گره‌های مخرب Sybil صورت می‌گیرند، گره‌هایی که از هویت‌های جعلی برای کاهش کاربردپذیری اینترنت اشیاء استفاده می‌کنند. در لایه‌ی فیزیکی، یک گره‌ی Sybil ممکن است از مقادیر تصادفی و جعل شده‌ی آدرس MAC برای جا زدن خود به عنوان یک دستگاه دیگر استفاده کند، در حالی که قصد تخریب و تخلیه‌ی منابع شبکه را دارد [35 و 34]. در نتیجه، گره‌های قانونی و مشروع در شبکه ممکن است نتوانند به منابع دسترسی داشته باشند.

**واسط فیزیکی ناامن**. عوامل فیزیکی مختلف، تهدیدات جدی را برای عملکرد مناسب دستگاه‌های اینترنت اشیاء به وجود می‌آورند. در یک امنیت ضعیف فیزیکی، نرم‌افزار می‌تواند از طریق واسط‌های فیزیکی مورد دسترسی قرار بگیرد، و ابزارهای آزمایش/دیباگ ممکن است برای به خطر انداختن گره‌های موجود در شبکه مورد سوءاستفاده قرار بگیرند [23].

**حمله‌ی محرومیت از خواب**. دستگاه‌هایی با انرژی محدود در اینترنت اشیاء در برابر حمله‌های "محرومیت از خواب" آسیب‌پذیر هستند، این حمله‌ها باعث می‌شوند که گره‌های حسگر همیشه بیدار باشند [36]. وقتی مقدار زیادی از وظایف در محیط 6LoWPAN برای اجرا تنظیم می‌شوند، حمله‌های محرومیت از خواب منجر تخلیه‌ی باتری می‌شوند.

*3-2. مسائل امنیتی سطح میانی*

مسائل امنیتی سطح میانی به طور عمده مربوط به ارتباطات، مسیریابی و مدیریت نشست است و همانطور که در ادامه شرح داده شده‌اند، در لایه‌های شبکه و انتقال اینترنت اشیاء رخ می‌دهند.

**حمله‌های بازپخش یا تکرار (تکثیر) به علت تکه تکه شدن**. تکه‌تکه شدن بسته‌های IPv6 در دستگاه‌های منطبق بر استاندارد IEEE 802.15.4 مورد نیاز است، زیرا این دستگاه‌ها با اندازه‌ی کوچک قاب کار می‌کنند. بازسازی قسمت‌های تکه‌ی بسته در لایه‌ی 6LoWPAN ممکن است منجر به تخلیه‌ی منابع، سرریزی بافر و راه‌اندازی مجدد دستگاه شود [37]. تکه‌های تکراری ارسال شده توسط گره‌های مخرب بر سرهم‌بندی مجدد بسته تاثیر می‌گذارد، بدین ترتیب مانع از پردازش دیگر بسته‌های قانونی و مجاز می‌شوند [38].

**کشف همسایه** **به صورت ناامن.** معماری استقرار اینترنت اشیاء نیاز دارد که هر دستگاه در شبکه به صورت منحصربه‌فردی شناسایی شود. ارتباطات پیامی برای شناسایی باید به صورت امنی صورت گیرد تا تضمین شود که داده‌های ارسال شده به یک دستگاه در ارتباطات انتها-به-انتها در نهایت به مقصد مشخص شده می‌رسد. مرحله‌ی کشف همسایه که پیش از مرحله‌ی انتقال داده‌ها انجام می‌شود، شامل گام‌های مختلفی از جمله کشف مسیریاب و ترجمه‌ی آدرس[[24]](#footnote-24) است [39]. استفاده از بسته‌های کشف همسایه بدون تایید و اعتبارسنجی مناسب ممکن است پیامدهای شدیدا سختی به همراه جلوگیری از سرویس (DoS) داشته باشد.

**حمله‌ی رزرو بافر**. از آنجایی که یک گره‌ی دریافت‌کننده باید فضای بافر را برای سرهم نمودن بسته‌های ورودی رزرو کند، از این رو یک مهاجم ممکن است از این مورد برای سرریزی فضای بافر با ارسال بسته‌های ناقص بهره ببرد [38]. این حمله منجر به جلوگیری از سرویس (DoS) می‌شود، زیرا با پُر شدن فضای بافر توسط بسته‌های ناقص ارسال شده توسط مهاجم، دیگر فضایی برای تکه‌های بسته‌های دیگر (بسته‌های کاربردهای قانونی) نمی‌ماند و آنها دور ریخته می‌شوند.

**حمله‌ی مسیریابی RPL**. پروتکل مسیریابی IPv6 برای شبکه‌های کم-توان و با اتلاف[[25]](#footnote-25) (RPL) در برابر حمله‌های مختلف آسیب‌پذیر است، حمله‌هایی که از طریق گره‌های به خطر افتاده‌ی موجود در شبکه رخ می‌دهند [40]. این حمله ممکن است منجر به تخلیه‌ی منابع و شنود شود.

**حمله‌های sinkhole و wormhole**. با حمله‌های sinkhole، گره‌ی مهاجم به درخواست‌های مسیریابی پاسخ می‌دهد، بنابراین باعث می‌شود تا مسیر بسته‌ها از گره‌ی مهاجم عبور کند و این امر می‌تواند بعدا برای اجرای فعالیت مخرب بر روی شبکه مورد استفاده قرار گیرد [42 و 41]. حمله‌ها بر روی شبکه ممکن است به علت تخریب عملیات 6LoWPAN توسط حمله‌های wormhole باشد، در حمله‌ی wormhole یک تونل بین دو گره ایجاد می‌شود، به گونه‌ای که بسته‌های رسیده به یک گره بلافاصله به گره‌ی دیگر می‌رسد [45-43]. این حمله‌ها پیامدهای شدیدی از جمله شنود، نقض حریم خصوصی و جلوگیری از سرویس (DoS) را در پی دارند.

**حمله‌های Sybil بر روی لایه‌های میانی**. همانند حمله‌های Sybil بر روی لایه‌های سطح پایین، گره‌های Sybil می‌توانند برای کاهش عملکرد شبکه و حتی نقض حریم خصوصی داده‌ها مورد استفاده قرار گیرند. ارتباطات انجام گرفته توسط گره‌های Sybil که از هویت‌های جعلی در یک شبکه استفاده می‌کنند، ممکن است منجر به هرزنگاری (spamming)، انتشار بدافزار یا راه‌اندازی حملات فیشینگ شود [47 و 46].

**احراز هویت و ارتباطات امن**. دستگاه‌ها و کاربران در اینترنت اشیاء باید از طریق سیستم‌های مدیریت کلید احراز هویت شوند. هر حفره‌ی حلقه‌ای (loophole) در امنیت لایه‌ی شبکه یا سربار زیاد ارتباطات امن ممکن است منجر به آسیب‌پذیری‌های زیادی در شبکه شود [50-48]. به عنوان مثال، با توجه به منابع محدود، سربار امنیت سطح انتقال دیتاگرام (DTLS) باید به حداقل برسد، و روش‌های رمزنگاری تضمین‌کننده‌ی ارتباطات امن داده‌ها باید با توجه به کارایی و کمبود دیگر منابع در نظر گرفته شوند [52 و 51].

**امنیت انتها-به-انتهای سطح انتقال**. امنیت انتها-به-انتهای سطح انتقال سعی دارد روش امنی را به گونه‌ای ارائه دهد که داده‌های ارسال شده توسط گره‌ی فرستنده، توسط گره‌ی مقصد مورد نظر به صورت قابل اعتمادی دریافت شود [54 و 53]. این امر به روش‌های احراز هویت جامعی نیاز دارد که ارتباط امن پیام را به صورت رمزنگاری شده و بدون نقض حریم خصوصی تضمین کند، و در عین حال با حداقل سربار کار کند [56 و 55].

**برقراری و شروع مجدد نشست**. ربودن نشست در لایه‌ی انتقال با پیام‌های جعلی می‌تواند منجر به جلوگیری از سرویس (DoS) شود [58 و 57]. یک گره‌ی مهاجم می‌تواند خود را به هویت گره‌ی قربانی در آورد تا به نشست بین دو گره ادامه دهد (یعنی گره‌ی مهاجم به جای گره‌‌ی قربانی، با جعل هویت وی، به ارتباط با طرف دیگر ارتباط ادامه دهد). گره‌های در حال ارتباط ممکن است با تغییر شماره ترتیب بسته‌ها، نیاز به ارسال مجدد پیام‌ها داشته باشند.

**نقض حریم خصوصی بر روی اینترنت اشیاء مبتنی ابر**. حمله‌های مختلفی که ممکن است محرمانگی هویت و مکان را نقض کنند، ممکن است بر روی ابر یا در اینترنت اشیاء مبتنی بر شبکه‌های تحمل‌پذیر تاخیر رخ دهند [59 و 20]. به طور مشابه، یک فراهم‌کننده‌ی مخرب سرویس ابر که استقرار اینترنت اشیاء مبتنی بر آن است، می‌تواند به اطلاعات محرمانه‌ای که به یک مقصد خاص ارسال می‌شوند، دسترسی داشته باشد.

*3-3. مسائل امنیتی سطح بالا*

همانطور که در ادامه شرح داده شده است، مسائل امنیتی سطح بالا به طور عمده مربوط به برنامه‌های کاربردی در حال اجرا بر روی اینترنت اشیاء است.

**امنیت CoAP با اینترنت**. لایه‌ی سطح بالا، که شامل لایه‌ی برنامه‌ی کاربردی است، نیز در برابر حملات آسیب‌پذیر می‌باشد [62-60]. پروتکل برنامه‌ی کاربردی محدود شده[[26]](#footnote-26) (CoAP) در واقع یک پروتکل انتقال وب برای دستگاهی با منابع محدود است که از ملحقات DTLS با حالت‌های مختلف امنیتی استفاده می‌کند تا امنیت انتها-به-انتها را تامین نماید. پیام‌های CoAP فرمت خاصی را دنبال می‌کنند که در گزارش RFC-7252 [29] تعریف شده است، که برای ارتباط باید رمزنگاری شود. به طور مشابه، چندپخشی[[27]](#footnote-27) پشتیبانی شده در CoAP نیاز به مدیریت مناسب کلید و روش‌های احراز هویت دارد.

**واسط‌های ناامن**. برای دسترسی به سرویس‌های اینترنت اشیاء، واسط‌هایی که از طریق وب، تلفن همراه، و ابر مورد استفاده قرار می‌گیرند، در برابر حمله‌های مختلف آسیب‌پذیر هستند که ممکن است به شدت بر حریم خصوصی داده‌ها تاثیر بگذارد [23].

**نرم‌افزار/firmware ناامن**. آسیب‌پذیری‌های متعددی در اینترنت اشیاء وجود دارند که از جمله‌ی آنها به مواردی اشاره نموده که توسط نرم‌فزار/firmware ایجاد می‌شوند [23]. کدی که با زبان‌های از قبیل JSON، XML، SQLi و XSS نوشته شده است، باید به دقت مورد آزمایش قرار گیرد. به طور مشابه، بروزرسانی‌های نرم‌افزار/firmware نیز باید به صورت امن و مطمئنی انجام شود.

**امنیت میان‌افزار**. میان‌افزار اینترنت اشیاء که برای برقراری ارتباط میان موجودیت‌های ناهمگن در الگوی اینترنت اشیاء طراحی شده است، باید برای ارائه‌ی سرویس‌ها به اندازه‌ی کافی امن باشد. واسط‌ها و محیط‌های مختلفی باید با استفاده از میان‌افزار ترکیب شوند تا ارتباطات امنی را ارائه دهند [64 و 63].

**4. راه‌حل‌های امنیتی برای اینترنت اشیاء**

تهدیدات امنیتی در اینترنت اشیاء از آسیب‌پذیری‌های موجود در اجزای مختلف از قبیل برنامه‌های کاربردی/واسط‌ها، اجزای شبکه، نرم‌افزار، firmware، و دستگاه‌های فیزیکی بهره می‌برند که این موارد در سطوح مختلفی موجود هستند. کاربران در یک الگوی اینترنت اشیاء از طریق پروتکل‌ها با این اجزاء تعامل دارند که ممکن است اقدامات امنیتی آنها در هم شکسته شود. اقدامات متقابل برای تهدیدات امنیتی به بررسی آسیب‌پذیری‌های موجود در این تعامل در لایه‌های مختلف می‌پردازند تا به سطح خاصی از امنیت دست یابند. پروتکل‌های متنوعی که از استقرار اجزاء پشتیبانی می‌کنند، به پیچیدگی این اقدامات متقابل می‌افزایند. بررسی کلی راه‌حل‌های اصلی امنیتی پیشنهاد شده در مقالات مرتبط در این بخش ارائه شده است. یک تحلیل مقایسه‌ای از تهدیدات امنیتی، و راه‌حل‌های ممکن برای آنها در سطح-پایین، سطح میانی زیر لایه انتقال، سطح-میانی شامل لایه انتقال، و سطح-بالایی به ترتیب در جدول‌های 1 تا 4 ارائه شده است. تحلیل مقایسه‌ای پارامترهای تهدیدها، پیامدهای آنها، لایه‌های متاثر (تحت تاثیر قرار گرفته)، سطوح مرتبط و راه‌حل‌های ممکن پیشنهاد شده در مقالات مرتبط را در نظر می‌گیرد.

جدول 1. طرحی از تهدیدات، پیامدها، و راه‌حل‌های امنیتی اینترنت اشیاء در سطح پایین.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| شماره ترتیب | مسئله‌ی امنیتی | پیامدها | لایه‌های متاثر | سطوح اینترنت اشیاء | راه‌حل‌های پیشنهادی | مراجع |
| 1 | مهاجمان Jamming | اختلال و جلوگیری از سرویس | لایه‌ی فیزیکی | سطح-پایین | اندازه‌گیری قدرت سیگنال، محاسبه‌ی نرخ تحویل بسته، کدگذاری بسته‌ها با کدهای اصلاح خطا، و تغییر فرکانس‌ها و مکان‌ها | [66، 31، 30] |
| 2 | حمله‌های Sybil و Spoofing | اختلال در شبکه، جلوگیری از سرویس | لایه‌ی فیزیکی | سطح-پایین | اندازه‌گیری قدرت سیگنال، و تخمین کانال | [70-68، 35، 34] |
| 3 | راه‌اندازی و پیکربندی ناامن | نقض حریم خصوصی و جلوگیری از سرویس | لایه‌ی فیزیکی | سطح-پایین | تنظیم نرخ انتقال داده‌ها بین گره‌ها، و معرفی نویز مصنوعی | [67، 33، 32] |
| 4 | واسط فیزیکی ناامن | نقض حریم خصوصی، جلوگیری از سرویس | سخت‌افزار | سطح-پایین | اجتناب از دسترسی نرم‌افزار/firmware به USB، ماژول‌های TPM مبتنی بر سخت‌افزار، و اجتناب از ابزارهای آزمایش کردن و دیباگ | [23] |
| 5 | حمله‌ی محرومیت از خواب | مصرف انرژی | لایه‌ی پیوند | سطح-پایین | سیستم تشخیص نفوذ مبتنی بر چند-لایه | [36] |

جدول 2. طرحی از تهدیدات، پیامدها، و راه‌حل‌های امنیتی اینترنت اشیاء سطح میانی زیر لایه انتقال.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| شماره ترتیب | مسئله‌ی امنیتی | پیامدها | لایه‌های متاثر | سطوح اینترنت اشیاء | راه‌حل‌های پیشنهادی | مراجع |
| 1 | حمله‌های بازپخش یا تکرار ناشی از قطعه‌بندی | اختلال و جلوگیری از سرویس | لایه‌ی تطبیقی 6LoWPAN، و لایه‌ی شبکه | سطح-میانی | معرفی برچسب زمانی و گزینه‌های nonce برای محافظت در برابر حمله‌های بازپخش، و ارزیابی قطعه از طریق زنجیره‌های هش | [38، 37] |
| 2 | کشف ناامن همسایه | IP Spoofing | لایه شبکه | سطح-میانی | احراز هویت با استفاده از رمزنگاری منحی بیضوی (ECC) مبتنی بر امضاها | [39] |
| 3 | حمله رزرو بافر | مسدود کردن بافر مجدد | لایه‌ی تطبیقی 6LoWPAN، و لایه شبکه | سطح-میانی | رویکرد شکستن بافر موردنیاز برای انتقال کامل قطعه‌ها | [38] |
| 4 | حمله مسیریابی RPL | شنود، حمله مرد میانی | لایه شبکه IPv6 | سطح-میانی | احراز هویت مبتنی بر امضا و هش کردن، و نظارت بر رفتار گره | [57، 40] |
| 5 | حمله‌های Sinkhole و Wormhole | جلوگیری از سرویس | لایه شبکه | سطح-میانی | ارزیابی رتبه از طریق تابع زنجیره هش، مدیریت سطح اعتماد، تحلیل رفتار و ارتباطات گره‌ها، تشخیص ناهنجاری از طریق IDS، مدیریت کلید رمزنگاری، پیمایش گراف، و اندازه‌گیری قدرت سیگنال | [84-76، 45-41] |
| 6 | حمله‌های Sybil | نقض حریم خصوصی، Spamming، خطای بیزانتین، همه‌پخشی غیرقابل اعتماد | لایه‌ی شبکه | سطح-میانی | راه رفتن تصادفی بر روی گراف‌های اجتماعی، تحلیل رفتار کاربر، و نگهداری از لیست‌های کاربران مورد اعتماد/غیر قابل اعتماد | [89-86، 47، 46] |
| 7 | احراز هویت و ارتباطات امن | نقض حریم خصوصی | لایه‌ی تطبیقی 6LoWPAN، لایه انتقال، لایه شبکه | سطح-میانی | AH و ESP فشرده، فشرده‌سازی هدر و AES مبتنی بر نرم‌افزار، TPM با استفاده از RSA، احراز هویت ترکیبی SHA1/AES، احراز هویت با استخراج‌کننده، رمزنگاری مقادیر نوع ارسال بار بسته با AH فشرده، IACAC با استفاده از رمزنگاری منحنی بیضوی، logهای توزیع شده، و نگاشت همریخت متقارن | [100، 20، 59، 101، 99، 96، 93، 92، 52-48] |

جدول 3. طرحی از تهدیدات، پیامدها، و راه‌حل‌های امنیتی اینترنت اشیاء در سطح-میانی شامل لایه انتقال.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| شماره ترتیب | مسئله‌ی امنیتی | پیامدها | لایه‌های متاثر | سطوح اینترنت اشیاء | راه‌حل‌های پیشنهادی | مراجع |
| 1 | امنیت انتها-به-انتهای سطح انتقال | نقض حریم خصوصی | لایه‌ی انتقال، و لایه شبکه | سطح-میانی | DTLS-PSK با nonceها، مسیریاب مرزی 6LoWPAN با ECC، الگوریتم‌های مبتنی بر رمز DTLS، IPSec فشرده، فشرده‌سازی هدر DTLS، IKEv2 با استفاده از UDP فشرده، و امنیت مبتنی بر AES/CCM با شناسایی و صدور مجوز دسترسی | [105-102، 93، 92، 56-53] |
| 2 | ایجاد و شروع مجدد نشست | جلوگیری از سرویس | لایه انتقال | سطح-میانی | احراز هویت با کلید مخفی طولانی مدت، و رمزنگاری مبتنی بر کلید متقارن | [106، 58، 57] |

جدول 4. طرحی از تهدیدات، پیامدها، و راه‌حل‌های امنیتی اینترنت اشیاء در سطح بالایی.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| شماره ترتیب | مسئله‌ی امنیتی | پیامدها | لایه‌های متاثر | سطوح اینترنت اشیاء | راه‌حل‌های پیشنهادی | مراجع |
| 1 | امنیت CoAP با اینترنت | تنگنا در شبکه، جلوگیری از سرویس | لایه‌ی برنامه‌ی کاربردی، و لایه‌ی شبکه | سطح-بالا و سطح-میانی | نگاشت TLS/DTLS و HTTP/CoAP، پروکسی آینه (MP) و کشف منابع، تونل TLS/DTLS و فیلتر کردن پیام با استفاده از 6LBR | [108، 62-60] |
| 2 | واسط‌های ناامن | نقض حریم خصوصی، جلوگیری از سرویس، اختلال در شبکه | لایه‌ی برنامه‌ی کاربردی | سطح-بالا | اجازه ندادن به کلمات عبور ضعیف، آزمایش کردن واسط در برابر آسیب‌پذیری‌های ابزارهای نرم‌افزاری (SQLi و XSS)، و استفاده از https به همراه دیواره‌ی آتش | [23] |
| 3 | نرم‌افزار/firmware ناامن | نقض حریم خصوصی، جلوگیری از سرویس، اختلال در شبکه | لایه‌ی برنامه‌ی کاربردی، لایه‌ی انتقال، لایه‌ی شبکه | سطح-بالا، سطح-میانی، و سطح-پایین | بروزرسانی‌های منظم و امن نرم‌افزار/firmware، استفاده از امضاهای فایل، و رمزنگاری با تایید | [23] |
| 4 | امنیت میان‌افزار | نقض حریم خصوصی، پیشگیری از سرویس، اختلال در شبکه | لایه‌ی برنامه‌ی کاربردی، لایه‌ی انتقال، لایه‌ی شبکه | سطح-بالا، سطح-میانی، و سطح-پایین | ارتباطات امن با استفاده از احراز هویت، سیاست‌های امنیت، مدیریت کلید میان دستگاه‌ها، دروازه‌ها و اجزای M2M، امنیت M2M لایه‌ی سرویس، میان‌افزار شفاف با استفاده از روش‌های احراز هویت/رمزنگاری | [111، 110، 64، 109، 63] |

*4-1. راه‌حل‌های امنیتی سطح پایین*

در شبکه‌های حسگر بی‌سیم، حمله‌های jamming مربوط به دخالت باعث تداخل و برخورد پیام‌ها یا سیل‌آسا شدن کانال‌ها می‌شود. رویکردی برای تشخیص حمله‌های jamming توسط Young و همکارانش [65] ارائه شده است. تشخیص این نوع حمله‌ها با اندازه‌گیری قدرت سیگنال امکانپذیر است که سپس برای استخراج سیگنال‌های نویز-مانند مورد استفاده قرار می‌گیرد. این مقادیر آماری سپس با مقادیر آستانه‌ی سفارشی شده برای تشخیص حمله مقایسه می‌شوند. Xu و همکارانش [30] رویکردی را برای تشخیص حمله‌های jamming از طریق محاسبه‌ی نرخ تحویل موفق بسته پیشنهاد داده‌اند. الگوریتم‌های پیشنهادی با بررسی ثبات قدرت سیگنال و مکان گره‌ها کار می‌کنند. روش ضد-jamming دیگری با استفاده از توابع رمزنگاری و کدهای اصلاح خطا توسط Noubir و همکارانش ارائه شده است [31]. این رویکرد با کدگذاری بسته‌ها از طریق تقسیم آن به بلوک‌ها و قرار دادن بیت‌های بسته‌ی کدگذاری شده در میان آنها عمل می‌کند. به طور مشابه، استراتژی‌های ترکیب گشت‌زنی کانالی[[28]](#footnote-28) و عقب‌نشینی‌های مکانی[[29]](#footnote-29) نیز برای مقابله با حمله‌های jamming پیشنهاد شده است [66]. گشت‌زنی کانالی در واقع دستگاه‌های ارتباطی قانونی را قادر می‌سازد تا فرکانس‌های کانال را تغییر دهند، در حالی که عقب‌نشینی‌های مکانی باعث می‌شوند که این دستگاه‌ها در حین حرکت به سمت یک مکان مورد نظر در یک فاصله‌ی خاص، مکان خود را تغییر دهند.

برای یک ارتباط امن لایه‌ی فیزیکی، چارچوبی با هدف راه‌اندازی امن اینترنت اشیاء توسط Pecorella و همکارانش ارائه شده است [67]. یک حداقل نرخ داده بین گره‌های فرستنده و دریافت‌کننده پیکربندی می‌شود تا از عدم وجود شنودکنندگان اطمینان حاصل شود. رویکردهای دیگری از معرفی نویز مصنوعی [33 و 32] در سیگنال‌ها برای امن نمودن ارتباطات مورد استفاده قرار گرفته است.

یک گره‌ی مخرب Sybil ممکن است از مقادیر جعلی آدرس MAC برای جلوه دادن خود به عنوان یک دستگاه دیگر استفاده کند. این امر می‌تواند منجر به اتلاف منابع و همچنین جلوگیری از دسترسی به دستگاه‌های قانونی و مجاز در شبکه شود. رویکردی با تشخیص حمله‌های Sybil با استفاده از اندازه‌گیری قدرت سیگنال توسط Demirbas و همکارانش ارائه شده است [68]. رویکرد آنها با توسعه‌ی گره‌های تشخیص‌دهنده‌ای عمل می‌کند که مکان فرستنده را در حین انتقال پیام محاسبه می‌کنند. ارتباطات پیامی دیگری با همان مکان فرستنده ولی با هویت فرستنده‌ی متفاوت، به عنوان یک حمله‌ی Sybil در نظر گرفته می‌شود. فرضیات در نظر گرفته شده در این رویکرد پیشنهادی، آن را برای شبکه‌های ایستا مناسب و قابل اجرا می‌سازد. رویکردهای دیگری توسط chen و همکارانش [35] و Li و همکارانش [69] ارائه شده‌اند که از اندازه‌گیری قدرت سیگنال برای آدرس‌های MAC برای تشخیص حمله‌ی spoofing استفاده می‌کنند. رویکرد دیگری توسط Xiao و همکارانش [34] ارائه شده است که از تخمین کانال نیز برای تشخیص حمله‌های Sybil استفاده می‌کند. رویکرد از تعداد هویت‌ها و دیگر پارامترهای مرتبط به تخمین کانال استفاده می‌کند تا گره‌های Sybil را تشخیص دهد. به طور مشابه، رویکرد مطرح شده در مرجع [70] نیز از پاسخ کانال برای تفاوت قائل شدن میان کاربران قانونی و مهاجمان استفاده می‌کند.

دستگاه‌هایی که امنیت فیزیکی نامناسبی دارند، با داشتن واسط‌های خارجی توصیف می‌شوند که دسترسی به firmware یا نرم‌افزار را فراهم می‌کنند، و ابزارهای آسیب‌پذیری را برای مواردی مانند آزمایش کردن و اشکال‌زدایی فراهم می‌کنند. پروژه‌ی امنیت باز برنامه‌ی کاربردی وب[[30]](#footnote-30) (OWASP) پیشنهاداتی را برای بهبود امنیت فیزیکی دستگاه‌ها در اینترنت اشیاء ارائه می‌دهد [23]. باید از واسط‌های غیرضروری سخت‌افزاری از قبیل USBها اجتناب شود، زیرا USBها دسترسی به firmware/نرم‌افزار دستگاه را فراهم می‌آورند. ابزارهای آزمایش و اشکال‌زدایی نیز باید غیرفعال شوند و روش‌های مبتنی بر سخت‌افزار از قبیل ماژول‌های بستر مورد اعتماد[[31]](#footnote-31) (TPMs) باید مورد استفاده قرار گیرند تا امنیت فیزیکی بهبود یابد.

چارچوبی برای کاهش حمله‌های محروم‌سازی از خواب در شبکه‌های حسگر بی‌سیم در مرجع [36] شرح داده شده است. چارچوب پیشنهادی از یک رویکرد مبتنی بر خوشه استفاده می‌کند که در آن هر خوشه به بخش‌های متعددی تقسیم می‌شود. مصرف انرژی با پیشگیری از ارتباطات راه دور کاهش می‌یابد. این چارچوب، عمل تشخیص نفوذ را با یک مدل پنج-لایه‌ای شبکه حسگر بی‌سیم انجام می‌دهد. هماهنگ‌کننده‌ی یک خوشه شامل یک سیستم تشخیص نفوذ گسترش یافته به همراه گره‌های رهبر و گره‌های چاهک در لایه‌های بالایی مدل WSN است. به طور مشابه، گره‌های دنبال‌کننده‌ی موجود در لایه‌های پایین‌تر مدل شبکه‌ی حسگر بی‌سیم به سیستم‌های تشخیص نفوذ ساده‌ای مجهز هستند.

*4-2. راه‌حل‌های امنیتی سطح میانی*

تهدیدات ناشی از حمله‌های بازپخش که با تکه تکه شدن بسته‌ها در 6LoWPAN به وجود می‌آید، با اضافه کردن قسمت برچسب زمانی و nonce به بسته‌های تکه تکه شده مورد رسیدگی قرار می‌گیرد [37]. این بسته‌ها به لایه‌ی انطباق 6LoWPAN متناظر با بسته‌های تکه تکه شده اضافه می‌شود. قسمت برچسب زمانی و nonce به ترتیب برای بسته‌های یک-طرفه و دو-طرفه کار می‌کنند. مقدار برچسب زمانی 64-بیتی در تکه‌ها تضمین می‌کند که اعلان‌های تکراری و اضافی در شبکه حذف شوند. قسمت nonce تضمین می‌کند که اعلان تنها در پاسخ به یک درخواست جدید ساخته شود. به طور مشابه، یک استراتژی زنجیره‌ی محتوا در مرجع [38] ارائه شده است که انتقال مرتب تکه‌های بسته‌های IPv6 را در 6LoWPAN تضمین می‌کند. محتویات تکه‌ها به تولید زنجیره‌ی هش اضافه می‌شوند تا قطعه‌ها اعتبارسنجی شوند.

یک چارچوب امنیتی با ماژول‌هایی برای کشف امن همسایه، احراز هویت، تولید کلید و رمزنگاری داده‌ها توسط Riaz و همکارانش [39] ارائه شده است. برای کشف امن همسایه، رمزنگاری منحنی بیضوی[[32]](#footnote-32) (ECC) [71] مورد استفاده قرار می‌گیرد. امضاهای کلید عمومی ECC برای شناسایی گره‌ها در مرحله‌ی کشف همسایه به کار گرفته می‌شوند. سیستم‌های مدیریت کلید متقارن و نامتقارن برای استقرار بسته به نیازهای برنامه‌ی کاربردی پیشنهاد می‌شوند. داده‌های رمز شده سپس رد و بدل می‌شود تا امنیت گره-به-گره تضمین شود.

از طریق یک حمله‌ی رزرو بافر، بافر مجدد در یک گره ممکن است مسدود شود. این حمله می‌تواند از طریق رویکرد تقسیم بافر کاهش یابد [38]، در این رویکرد هزینه‌ی راه‌اندازی حمله افزایش می‌یابد و این کار با نیاز به قطعه‌بندی کامل بسته‌هایی انجام می‌دهد که باید در بازه‌های زمانی کوتاه به صورت انفجاری ارسال شوند. هر گره نیاز دارد که درصد تکمیل یک بسته را محاسبه نموده و رفتار ارسال قطعه‌ها را ثبت کند. پس از وقوع بار بیش از حد (یعنی پُر شدن بافر)، گره می‌تواند بسته‌هایی را حذف کند که کمترین درصد را دارند یا تغییرات خیلی زیادی در الگوی ارسال قطعات آنها وجود دارد.

برای مقابله با حمله‌های مهاجم[[33]](#footnote-33) در حین مسیریابی از طریق پروتکل مسیریابی IPv6 برای شبکه‌های کم توان و با اتلاف زیاد (RPL)، یک سرویس امنیتی برای احراز هویت رتبه و شماره‌ی نسخه‌ها توسط Dvir و همکارانش ارائه شده است [40]. پروتکل RPL با ایجاد گراف بدون دور جهت‌دار[[34]](#footnote-34) (DAG) با ریشه در هر دروازه کار می‌کند. شماره‌ی نسخه وقتی بروزرسانی می‌شود که نسخه‌ی جدیدی از DAG مقصدگرا ساخته می‌شود. RPL از رتبه‌ها برای نمایش کیفیت مسیر به گره‌های چاهک نهایی استفاده می‌کند. مقدار رتبه‌ی یک گره ممکن است با اتصال به ریشه برای شنود (استراق سمع) کاهش یابد. روش امنیتی پیشنهادی با نام شماره‌ی نسخه و احراز هویت رتبه (VeRA) از تابع هش (SHA [72])، تابع MAC (HMAC [37] و امضای دیجیتال (RSA [74]) و غیره) برای احراز هویت شماره نسخه‌ها و رتبه‌ها استفاده می‌کند. به طور مشابه، با RPL، مقدار رتبه‌ی محاسبه شده بر اساس رتبه‌ی والد ترجیح داده شده[[35]](#footnote-35)، به دیگر گره‌ها همه‌پخشی می‌شود. استاندارد RPL نیاز دارد که گره‌ی والد رتبه‌ی کمتری از فرزند داشته باشد. یک حمله توسط Le و همکارانش [75] ارائه شده است که گره‌ی مخرب را به گونه‌ای تنظیم می‌کند که بدترین والد را به جای بهترین والد انتخاب کند. گره‌ی به خطر افتاده، پیام‌های DAO را هدایت نمی‌کند، در نتیجه از طریق گره‌های مخرب در حین انتقال پیام‌ها به تاخیر ترافیک افزوده می‌شود. این حمله بسته به بار موجود برای هدایت در آن منطقه‌ی شبکه شدت می‌یابد. برای مقابله با حمله، پیشنهاد شده است که رفتار گره برای پارامترهای مختلف از جمله پیام‌های تحویل داده شده و تاخیر انتها-به-انتها و غیره مورد نظارت قرار گیرد.

برای مقابله با حمله‌های sinkhole در شبکه‌های کم-توان و با اتلاف زیاد، روشی با ترکیب روش‌های غلبه-بر-شکست[[36]](#footnote-36) و احراز هویت توسط Weekly و همکارانش [41] ارائه شده است. برای اعتبارسنجی و تایید رتبه‌ی مربوط به یک پیام شئ اطلاعات مقصد[[37]](#footnote-37) (DIO)، یک تابع هش یک-طرفه به همراه یک تابع زنجیره‌ی هش مورد استفاده قرار می‌گیرد. یک مقدار هش تولید شده برای یک عدد تصادفی که توسط گره‌ی ریشه انتخاب شده است، از طریق پیام DIO همه‌پخشی می‌شود. گره‌های معتبر موجود در شبکه هش‌های بیشتری را پیش از هدایت پیام‌ها انجام می‌دهند، در حالی که گره‌های به خطر افتاده و آسیب دیده با مقادیر هش دریافت شده به برقراری ارتباط می‌پردازند. پس از همگرایی درخت مسیریابی، ریشه یک همه‌پخشی را با مقدار تصادفی که در ابتدا انتخاب شده است، انجام می‌دهد تا تک تک گره‌ها را اعتبارسنجی نماید. وجود یک عدم تطابق در یک گره به معنی یک مقدار رتبه‌ی نامعتبر والد است. به طور مشابه، روش غلبه-بر-شکست والد نیز پیام DIO را با یک قسمت خاص امضا شده توسط گره‌ی ریشه تقویت می‌کند. این قسمت خاص در واقع نشان‌دهنده‌ی گره‌های غیر-ریشه است که قادر نیستند 30% از داده‌های حسگر را در فواصل زمانی مشخصی انتقال دهند. بدین ترتیب والدهای چنین گره‌هایی برای ارتباطات بعدی در لیست سیاه قرار می‌گیرند. رویکرد دیگری توسط Firoz و همکارانش [42] به شناسایی گره‌های مشکوک می‌پردازد و این کار را با تحلیل رفتار گره‌های همسایه انجام می‌دهد. پس از آن نیاز است که گره‌های مشکوک به عنوان یک black hole (حفره‌ی سیاه) تایید شوند. استراتژی دیگری برای مقابله با حمله‌های sinkhole با استفاده از سطوح متفاوت اعتماد توسط Pirzada و همکارانش ارائه شده است [43]. رویکرد آنها از ویژگی‌های مختلف پروتکل مسیریابی مبدأ پویا[[38]](#footnote-38) (DSR) استفاده می‌کند تا حمله‌های sinkhole و wormhole را در شبکه‌های بی‌سیم تشخیص داده و از آنها پیشگیری کند. این رویکرد بر اساس سطوح دقت و صحت است که با اعتبارسنجی و تایید بسته‌های هدایت شده از طریق برخی بررسی‌های صحت و یکپارچگی محاسبه می‌شوند. به طور مشابه، یک پروتکل مسیریابی اد هاک [76] با ترکیب الگوریتم‌های مبتنی بر رمزنگاری متقارن برای امن نمودن گره‌ها در برابر گره‌های به خطر افتاده‌ی بی‌سیم در یک شبکه طراحی شده است. رویکرد دیگری از تشخیص حمله‌های wormhole در شبکه‌های حسگر بی‌سیم بدین صورت است که فاصله‌های تخمین زده شده میان همسایگان همه‌پخشی می‌شود [44]. سپس انحرافات شبکه برای تشخیص اتصالات همسایگان مشکوک و wormhole مورد بررسی قرار می‌گیرد. رویکرد دیگری توسط Wazid و همکارانش [4] پیشنهاد شده است که سعی دارد حمله‌های sinkhole یا wormhole را برای یک شبکه‌ی حسگر بی‌سیم سلسله‌مراتبی تشخیص دهد. کل شبکه به خوشه‌های متعددی تقسیم می‌شود که هر خوشه شامل یک گره‌ی حسگر با توان بالا است که برای تشخیص گره‌های sinkhole در خوشه‌ی خود کار می‌کند. رویکردهای متعددی با استفاده از یک روش تشخیص نفوذ برای تشخیص و پیشگیری از حمله‌های sinkhole ارائه شده است [77 و 78]. استراتژی‌های پیشنهادی در واقع تحلیل بسته‌های شبکه، و تشخیص ناهنجاری را با استفاده از قوانین از پیش تعریف شده ترکیب می‌کنند. رویکردهای دیگر تشخیص wormhole از گراف‌های شبکه [81-79]، تحلیل قدرت سیگنال پیام‌ها [82]، یا سیستم‌های مدیریت کلید [84 و 83] استفاده می‌کنند.

حمله‌های Sybil بر روی لایه‌ی شبکه از هویت‌های ساختگی برای ایجاد چندین هویت منحصربه‌فرد به نام گره‌های Sybil استفاده می‌کند [85]. این حمله‌ها یک تهدید جدی برای سیستم‌های توزیع شده و نظیر-به-نظیر[[39]](#footnote-39) (P2P) از جمله اینترنت اشیاء ایجاد می‌کنند. همچنین این حمله‌ها ممکن است بر دفاع در برابر خطاهای بیزانتین تاثیر بگذارد و به موجب آن مانع از همه‌پخشی قابل اعتماد در شبکه شود. در شبکه‌های اجتماعی، یک رابطه‌ی اعتماد برای محدود ساختن ایجاد هویت‌های Sybil در نظر گرفته شده است. اقدامات مقابله‌ای با استفاده از گره‌های اجتماعی، شناسایی گره‌های Sybil را برای گره‌های قانونی و مجاز ممکن می‌سازند و این کار را با پیمودن گراف از طریق پیاده‌روی تصادفی یا استفاده از الگوریتم‌های تشخیص جامعه انجام می‌دهند [88-86 و 46]. به طور مشابه، رفتار کاربران در مورد فعالیت‌های آنها در شبکه مورد بررسی قرار می‌گیرد، و متعاقبا، کاربرانی با یک الگوی ثابت در فعالیت‌های خود به عنوان کاربران Sybil در نظر گرفته می‌شوند [47 و 46]. برای شبکه‌های متحرک (موبایل)، ممکن است لیستی از کاربران مورد اعتماد و غیر قابل اعتماد برای تشخیص گره‌های Sybil نگهداری شود [89].

برای امن نمودن لایه‌ی شبکه در شبکه‌های مبتنی بر IPv6 که از لایه‌ی تطبیقی 6LoWPAN استفاده می‌کنند، فرمت‌های فشرده شده‌ای از سرآیند (هدر) احراز هویت[[40]](#footnote-40) (AH) [90] و کپسوله‌سازی محموله‌ی بار امنیتی[[41]](#footnote-41) (ESP) [91] در مرجع [50] پیشنهاد شده است. 8 بیت از هدر آدرس‌دهی IPv6 به عنوان مشخصات لایه‌ی تطبیقی 6LoWPAN برای تعریف انواع ارسال و آدرس‌دهی هدر مورد استفاده قرار می‌گیرند. هدرهای فشرده شده در ارتباطات در دو حالت مورد استفاده قرار می‌گیرند: حالت انتقال و حالت تونل، که به رمزنگاری محموله‌ی بار بستگی دارد. ارزیابی روش‌های مختلف رمزنگاری پیاده‌سازی شده برای فرمت امنیتی جدید پیشنهادی نشان می‌دهد که الگوریتم SHA1 [72] نیاز به زمان و انرژی کمتری دارد. به طور مشابه، یک فرمت فشرده شده‌ی IPsec نیز توسط Reza و همکارانش [93، 92 و 49] برای تامین امنیت انتها-به-انتها شرح داده شده است. نویسندگان از هدر احراز هویت (AH) و کپسوله‌سازی محموله‌ی بار امنیتی (ESP) برای تامین امنیت با استفاده از IPsec استفاده می‌کنند. کدگذاری هدرهای AH و ESP با استفاده از کدگذاری NHC انجام می‌شود که این کدگذاری در روش فشرده‌سازی HC!# تعریف شده است [94]. برای احراز هویت و رمزنگاری، انواع مختلفی از SHA1 و AES پیاده‌سازی شده‌اند. کدگذاری بیتی (bitwise) باعث کاهش اندازه‌ی بسته می‌شود، با این حال، رویکرد پیشنهادی از لحاظ مصرف انرژی و متوسط زمان پاسخ باعث ایجاد سربار می‌شود.

روش دیگری برای امن نمودن لایه‌ی شبکه‌ی 6LoWPAN با پشتیبانی از مقادیر جدید نوع ارسال توسط Granjal و همکارانش [48] پیشنهاد شده است. نویسندگان، استفاده از مقادیر رزرو شده را برای بایت محموله‌ی بار را پیشنهاد کرده‌اند، مطابق با آنچه در RFC 4944 [95] ارائه شده است. اولین 3 بیت از مقادیر نوع ارسال به شرح هدر امنیتی و حالت مصرف می‌پردازند، در حالی که 3 بیت باقیمانده به شرح انواع هدرهای آدرس‌دهی 6LoWPAN می‌پردازند. برای استخراج اطلاعات از یک بسته در رابطه با الگوریتم‌های رمزنگاری و کلیدهایی که برای پرازش بسته باید اعمال شوند، یک اندیس دو-بایتی پارامترهای امنیتی[[42]](#footnote-42) (SPI) مورد استفاده قرار گرفته است. در مقابل این رویکرد، Mahalle و همکارانش [51] پروتکلی را برای امن نمودن اینترنت اشیاء در برابر حمله‌های جلوگیری از سرویس (DoS)، مرد میانی، و بازپخش پیشنهاد کرده‌اند. حمله‌های DoS ممکن است وقتی بر روی دستگاه‌های با منابع محدود صورت گیرد که مهاجمان پیام‌هایی را برای مصرف منابع آنها ارسال کنند. به طور مشابه، کلیدهای مخفی که با شنود آشکار شده‌اند، ممکن است منجر به سرقت هویت و در نتیجه وقوع حمله‌های مرد میانی در یک محیط شبکه شود. علاوه بر این، اطلاعات هویت یا گواهینامه‌ها می‌توانند توسط مهاجمان برای تاثیر بر ترافیک شبکه بازپخش شوند. رویکرد پیشنهادی با نام احراز هویت و کنترل دسترسی بر اساس قابلیت (IACAC) به تولید کلیدهای مخفی با استفاده از الگوریتم دیفی هلمن مبتنی بر رمزنگاری منحنی بیضوی می‌پردازد. برای ارتباطات و دسترسی، دستگاه‌ها از طریق رمزنگاری با کلیدهای مخفی به صورت متقابل احراز هویت می‌شوند. یک کنترل دسترسی مبتنی بر قابلیت پیاده‌سازی شده است که در آن، قابلیت نشان‌دهنده‌ی یک ساختار شامل حقوق دسترسی و شناسه‌ی دستگاه است. با دسترسی مبتنی بر قابلیت، برقراری ارتباطات میان دو دستگاه در ابتدا مورد تایید قرار می‌گیرد. علاوه بر این، قابلیت دستگاه برای انجام عملکردهای موردنظر، پیش از اجرای عملیات واقعی مورد بررسی قرار می‌گیرد.

Kothmayr و همکارانش [97 و 96] رویکردی را برای امنیت انتها-به-انتها با استفاده از احراز هویت دو-طرفه از طریق رمزنگاری کلید عمومی شرح داده‌اند. یک سرور کنترل دسترسی مورد اعتماد برای ذخیره‌ی حقوق دسترسی ناشران در شبکه مستقر می‌شود. گواهینامه‌ی ناشر و متصدی گواهینامه[[43]](#footnote-43) (CA) باید بر روی سایت ناشر وجود داشته باشد. احراز هویت ممکن است از طریق تراشه‌های ماژول بستر مورد اعتماد (TPM) [98] با استفاده از RSA یا از طریق کلیدهای از پیش به اشتراک گذاشته شده‌ی DTLS انجام شود. با TPMها، گواهینامه‌های RSA در قالب X.509 منتقل می‌شوند. ارتباطات انتها-به-انتها تنها زمانی آغاز می‌شوند که احراز هویت مشترکین با سرور کنترل دسترسی صورت گرفته باشد. نشان داده شده است که رویکرد پیشنهادی با انرژی کم و فضای کمی از حافظه کار می‌کند. روش دیگری از احراز هویت و صدور مجوز دسترسی بر اساس چندین عامل توسط Huang و همکارانش [99] پیشنهاد شده است. روش پیشنهادی، احراز هویت با کلمه‌ی عبور و استفاده از کارت‌های هوشمند را ترکیب می‌کند. سپس یک استخراج‌کننده‌ی فازی برای استخراج رشته‌ی تصادفی از بیومتریک‌ها مورد استفاده قرار می‌گیرد. پروتکل احراز هویت از چهار عملیات مربوط به ایجاد پارامترهای امنیتی، ذخیره‌سازی اطلاعات ثبت‌نام در پایگاه‌داده، احراز هویت، و اصلاح گواهینامه‌های احراز هویت پشتیبانی می‌کند. نویسندگان همچنین یک روش مستقل احراز هویت را پیشنهاد داده‌اند که نیازی به اتصال به سرور احراز هویت ندارد.

یک چارچوب توزیع شده برای ارتباطات امن میان شبکه‌های اینترنت اشیاء توسط Henze و همکارانش ارائه شده است [59]. برای محافظت از یک شبکه‌ی اینترنت اشیاء از یک فراهم‌کننده‌ی مخرب سرویس ابری، چارچوب پیشنهادی اجازه‌ی پیکربندی شبکه را از یک مکان مرکزی می‌دهد. این چارچوب پیام‌های کنترلی در مکان‌های مختلف را ثبت می‌کند تا از طریق دروازه‌های مختلف تایید نماید. اندازه‌ی پیام‌های ثبت شده با حذف پیام‌های قدیمی به صورت مداوم کاهش می‌یابد. سپس تایید پیام‌های ثبت شده برای نشان دادن رفتار مخرب مورد استفاده قرار می‌گیرد که به نوبه‌ی خود از اینترنت اشیاء مبتنی بر ابر در برابر دستکاری، منع، افزودن، و دستکاری در ترتیب پیام‌ها محافظت می‌کند. با هدف حفاظت از حریم خصوصی از هویت و مکان در اینترنت اشیاء مبتنی بر ابر، یک روش احراز هویت با هدایت امن بسته توسط Zhou و همکارانش [20] ارائه شده است. الگوریتم پیشنهادی از نگاشت همریختی متقارن برای شبکه‌های تحمل‌پذیر تاخیری استفاده می‌کند که اتصال پایدار انتها-به-انتها ندارند و بدین ترتیب نیاز است تا گره‌های میانی در حین انتقال پیام‌ها همکاری داشته باشند. به طور مشابه، یک بستر برای امن نمودن داده‌های به اشتراک گذاشته شده در میان دستگاه‌های اینترنت اشیاء در پروژه‌ی SMARTIE ارائه شده است [100]. بستر داده‌ی ارائه شده توسط پروژه‌ی SMARTIE، یک روش احراز هویت برای دسترسی به سرویس به همراه کتابخانه‌های متفاوت برای مدیریت کلیدهای رمزنگاری را تعریف می‌کند. برای ارائه‌ی یک کانال امن برای ارتباطات میان دستگاه‌های اینترنت اشیاء و ابر، پروژه یک پروتکل امن و سبک وزن CoAP را با استفاده از رمزنگاری منحنی بیضوی تعریف می‌کند. به طور مشابه، برای حفاظت از حریم خصوصی در حین اشتراک‌گذاری داده‌ها و فراهم نمودن ردیابی امن اشیاء در اینترنت اشیاء، این پروژه شامل میان‌افزار و سرویس‌های مبتنی بر مکان می‌باشد.

برای تامین امنیت انتها-به-انتها، استفاده از TLS-PSK توسط Brachmann و همکارانش پیشنهاد شده است [53]، در عین اینکه ارتباط میان HTTP و CoAP را نیز ممکن سازد. این روش نیاز به ترجمه‌ی پیام از لایه‌ی DTLS و دیگر پروتکل‌های سطح-بالا دارد. به طور مشابه، برای امن نمودن چندپخشی[[44]](#footnote-44) پیام‌ها، بسطی از DTLS با ترکیب PSK و nonceها پیشنهاد شده است تا از کلیدهای نشست مذاکره پشتیبانی کنند. برای امنیت سطح انتقال، یک روش واگذاری احراز هویت نیز با استفاده از مسیریاب مرزی 6LoWPAN[[45]](#footnote-45) (6LBR) پیشنهاد شده است که بسته‌ها را متوقف می‌کند، محاسباتی را برای احراز هویت کلید عمومی انجام می‌دهد و بسته‌ها را هدایت می‌کند [54]. یک سرور کنترل دسترسی نیز برای پشتیبانی از احراز هویت میان 6LBR و دستگاه‌های حسی در نظر گرفته شده است. رمزنگاری منحنی بیضوی (ECC) برای پیاده‌سازی امنیت سطح انتقال به کار گرفته شده است. ارتباطات انتها-به-انتهای امن شده با 6LBR، در مورد کلیدها مذاکرده نموده و برای دیگر مراحل احراز هویت در میان هر دو انتها مبادله می‌شوند. محاسبات واگذار شده به 6LBR، با وجود محاسبات سنگین مورد نیاز برای ECC، باعث عملکرد بهتر برای ارتباطات امن می‌شوند. چارچوب دیگری به نام BlinkToSCoAP برای تامین امنیت انتها-به-انتها در اینترنت اشیاء در مرجع [55] پیشنهاد شده است. چارچوب پیشنهادی به ترکیب پیاده‌سازی‌های سبکی از CoAP، DTLS، و 6LoWPAN می‌پردازد تا اینترنت اشیاء را امن نماید. رمز DTLS مبتنی بر الگوریتم‌های 128-بیتی AES و 26-بیتی SHA است. نشان داده شده است که چارچوب پیشنهادی در دستگاه‌های با محدودیت منابع با حداقل نیازها از لحاظ اندازه‌ی حافظه‌ی RAM، اندازه‌ی حافظه‌ی فلش، و مصرف انرژی کار می‌کند. یک استراتژی شامل فشرده‌سازی هدر برای پروتکل 6LoWPAN برای کاهش سربار DTLS توسط Sinthan و همکارانش [52] ارائه شده است. استراتژی پیشنهادی، فشرده‌سازی هدر DTLS را انجام می‌دهد و از پیاده‌سازی AES مبتنی بر نرم‌افزار استفاده می‌کند. استراتژی فشرده‌سازی باعث بهبود مصرف انرژی و همچنین مدت زمان پاسخ شبکه می‌شود.

پروژه RERUM [104] چارچوبی را برای برنامه‌های کاربردی اینترنت اشیاء در شهر هوشمند ارائه می‌دهد تا حریم خصوصی و امنیت را تضمین نماید. برای توسعه‌ی برنامه‌های کاربردی قابل اعتماد، رویکردهای مبتنی بر یکپارچگی داده‌ها و احراز هویت مورد استفاده قرار گرفته‌اند. روش‌های کنترل دسترسی برای سیستم‌های قابل تعویض به صورت پویا، به همراه احراز هویت گام-به-گام و انتها-به-انتها برای ارتباطات امن به/از اشیاء در اینترنت اشیاء مورد استفاده قرار گرفته‌اند. همچنین این روش سعی دارد حریم خصوصی را از طریق روش‌های امضا و روش‌های حسی فشرده‌سازی تضمین می‌کند. چارچوب دیگر برای آزمایش با پروتکل‌های امنیتی در زیرساخت مبتنی بر اینترنت اشیاء در پروژه‌ی ARMOUR پیاده‌سازی شده است [107]. پروژه سعی دارد در سناریوهای مبتنی بر اینترنت اشیاء مانند شهر هوشمند و مراقبت از سلامتی به برقراری امنیت و ارزیابی اعتماد بپردازد. پیاده‌سازی ARMOUR به تعریف معماری امنیت، برقراری بسترهای آزمایشی، اجرای آزمایش‌ها، و تولید برچسب‌های گواهینامه می‌پردازد. آزمایش‌های می‌توانند برای تضمین اتصال قابل اعتماد انتها-به-انتها و همچنین نیازهای امنیتی مختص هر لایه مورد استفاده قرار گیرد. به طور مشابه، پروژه‌ی BUTLER [105] پشتیبانی از سیستم‌های اطلاعات آگاه به زمینه برای سیستم‌های اینترنت اشیاء از جمله خانه‌های هوشمند، خرید هوشمند، مراقبت از سلامتی هوشمند، و شهرهای هوشمند را فراهم می‌کند. سرویس‌های پیاده‌سازی شده در پروژه، برقراری ارتباطات قابل اعتماد را برای اشیاء موجود در اینترنت اشیاء با استفاده از اطلاعات زمینه ممکن می‌سازد. پروژه شامل پروتکل‌های سبک رمزنگاری با هدف بهبود محرمانگی و یکپارچگی داده‌ها است.

روش‌های مختلف فشرده‌سازی هدر برای تامین امنیت انتها-به-انتها پیشنهاد شده‌اند. Reza و همکارانش [103] رویکردی را برای فشرده‌سازی رکورد DTLS و سرآیندهای دست‌دهی به همراه پیام‌های مختلف دست‌دهی شرح می‌دهند تا در داخل یک MTU تنها از 6LoWPAN قرار گیرد. رویکرد پیشنهادی بیت‌های هدر را برای ترکیب کدگذاری رکورد و بایت دست‌دهی و همچنین کدگذاری هدر رکورد پس از تکمیل دست‌دهی کدگذاری می‌کند. به طور مشابه، یک نسخه‌ی ارتقاء یافته از DTLS شامل فشرده‌سازی هدر برای تضمین امنیت اینترنت اشیاء در مرجع [102] ارائه شده است. برای فشرده‌سازی هدر بعدی مبتنی بر UDP[[46]](#footnote-46) (NHC)، 05 بیت مخصوص در هدر DTLS برای شناسایی هدرهای فشرده شده مورد استفاده قرار می‌گیرد، در عین اینکه 03 بیت باقیمانده برای نمایش جمع مقابله‌ای[[47]](#footnote-47) و پورت‌ها مورد استفاده قرار می‌گیرد. به طور مشابه، برای رکورد و هدرهای دست‌دهی که اندازه‌ی 13 و 12 بایتی دارند، استراتژی پیشنهادی هدرها را به ترتیب به اندازه‌ی 05 بایت 03 بایت فشرده می‌سازد. برای CoAP، ارتقائی در DTLS با ترکیب فشرده‌سازی هدر، سربار DTLS را کاهش می‌دهد، در نتیجه مصرف انرژی و زمان پاسخ را بهبود می‌دهد. یک پیاده‌سازی از تبادل کلید اینترنت[[48]](#footnote-48) (IKE) که سعی دارد مدیریت کلید را برای 6LoWPAN بهبود دهد، توسط Shahid و همکارانش ارائه شده است [56]. پروتکل IKE توسط IPSec برای مدیریت کلیدها به کار گرفته می‌شود، ولی به نظر می‌رسد که برای دستگاه‌های با منابع محدود مناسب نیست. نویسندگان یک نسخه‌ی فشرده از IKEv2 را با استفاده از یک فرمت فشرده‌ی UDP پیشنهاد داده‌اند که ممکن است به عنوان هدر IKE تشخیص داده شود. فیلدهای مختلف هدر IKE در هنگام استفاده از روش کدگذاری NHC فشرده می‌شوند. این مرجع همچنین استفاده از فیلد شناسه‌ی پروتکل را در امنیت مربوط به محموله‌ی بار IKEv2 برای امنیت لایه‌ی پیوند IEEE 802.15.4 ارائه کرده‌اند.

یک روش احراز هویت متقابل برای مدیریت امن نشست با استفاده از روش‌های رمزنگاری مبتنی بر کلید توسط Park و همکارانش ارائه شده است [57]. روش پیشنهادی در ابتدا یک عدد تصادفی انتخاب می‌کند، و رمزنگاری را انجام می‌دهد، و یک کلید نشست تولید می‌کند که متعاقبا برای رمزنگاری عدد تصادفی دیگر مورد استفاده قرار می‌گیرد. مقدار رمز شده سپس برای احراز هویت به کار گرفته می‌شود. برای هر نشست، یک کلید نشست ممکن است بدون نیاز به تکرار پارامترها تولید شود. به طور مشابه، روش دیگری از رمزنگاری با استفاده از هش‌ها برای دستگاه‌های با منابع محدود با پشتیبانی توابع هش نیز ارائه شده است. این روش به علت سربار کم محاسباتی، کارآمد است. روش دیگری از احراز هویت متقابل برای محیط‌های مبتنی بر محاسبات مه که دستگاه‌های با منابع محدود دارند، در مرجع [58] پیشنهاد شده است. روش پیشنهادی که Octopus نام دارد، نیاز به یک کلید مخفی با طول عمر زیاد دارد که سپس برای احراز هویت با سرورهای مه مورد استفاده قرار می‌گیرد.

یک اقتباس از تبادل HIP Diet برای بهبود امنیت اینترنت اشیاء توسط Hummen و همکارانش مورد استفاده قرار گرفته است [106]. با ترکیب یک روش کارآمد برای شروع مجدد نشست، سربار عملیات مبتنی بر کلید عمومی کاهش یافته است. شروع مجدد نشست باعث می‌شود که همتایان عملیات سنگینی را در حین برقراری نشست انجام می‌دهند. سپس حالت نشست ذخیره می‌شود که متعاقبا شروع مجدد نشست را با احراز هویت مجدد بهبود می‌دهد. مذاکره‌ی مورد نیاز برای شروع مجدد نشست ممکن است با DTLS و IKEv2 تکمیل شود.

*4-3. راه‌حل‌های امنیتی سطح بالا*

برای امن نمودن شبکه‌های کم توان و با اتلاف[[49]](#footnote-49) (LLN) مبتنی بر CoAP متصل به اینترنت، رویکردی با ترکیب TLS و DTLS توسط Brachmann و همکارانش ارائه شده است [60]. رویکرد پیشنهادی برای سناریوهایی کار می‌کند که مسیریاب مرزی 6LoWPAN[[50]](#footnote-50) (6LBR) شبکه‌ی LLN را به منظور دسترسی از راه دور به دستگاه‌ها به اینترنت وصل می‌کند. گره‌های LLN برای ارائه‌ی سرویس‌ها به کلاینت‌های CoAP و HTTP مورد استفاده قرار می‌گیرند. نگاشتی از TLS و DTLS برای ارائه‌ی امنیت انتها-به-انتها ارائه شده است که از شبکه‌های LLN در برابر حمله‌های مبتنی بر اینترنت محافظت می‌کند. محاسبات نگاشتی وقتی به دستگاه‌های با منابع-محدود واگذار می‌شود، ممکن است سربار قابل توجهی را به آنها تحمیل کند. رویکرد دیگری از امن نمودن پیام‌ها برای کاربردهای ارتباطی از طریق اینترنت با استفاده از قسمت‌های امنیتی متعدد CoAP توسط Granjal و همکارانش [61] پیشنهاد شده است. گزینه‌های جدید امنیتی مربوط به CoAP عبارتند از: SecuirtyOn، SecurityToken و SecurityEncap. گزینه‌ی SecurityOn مربوط به حفاظت از پیام‌های CoAP در سطح برنامه‌ی کاربردی هستند. گزینه‌ی SecurityToken امکان شناسایی و احراز هویت را برای فراهم نمودن دسترسی به منابع CoAP در سطح برنامه‌ی کاربردی تسهیل می‌کند. گزینه‌ی SecurityEncap از پیکربندی گزینه‌ی SecurityOn استفاده می‌کند و عمدتا انتقال داده‌های مورد نیاز برای احراز هویت و حفاظت در برابر بازپخش داده‌ها را انجام می‌دهد. یک امنیت مبتنی بر AES/CCM برای حفاظت از پیام‌ها در آن قرار گرفته است. با استفاده از گزینه‌های بالا، رویکرد پیشنهادی نشان داده است که از لحاظ فضای محموله‌ی بسته، مصرف انرژی و میزان ارتباطات بهتر عمل می‌کند. به طور مشابه، برای اینترنت اشیاء مبتنی بر شبکه‌های IP، یک مدل امنیتی با 6LBR برای فیلتر کردن پیام به کار گرفته شده است تا امنیت انتها-به-انتهای پیشنهادی در مرجع [108] را فراهم کند. تونل TLS-DTLS می‌تواند ایجاد شود، در عین اینکه 6LBR برای نگاشت در طول عملیات دست‌دهی[[51]](#footnote-51) مورد استفاده قرار می‌گیرد. به طور مشابه، با دو میزبانی که یک کلید مشترک را به اشتراک می‌گذارند، پیشنهاد شده است تا اعتبارسنجی پیام یا تشخیص پیام‌های بازپخش در دستگاه CoAP انجام شوند. یک مدل امنیتی انرژی کارآمد با استفاده از رمزنگاری کلید عمومی برای اینترنت اشیاء مبتنی بر CoAP توسط Sethi و همکارانش ارائه شده است [62]. مدل امنیتی پیشنهادی در یک نمونه‌ی اولیه پیاده‌سازی شده است که به ترتیب از یک پروکسی آینه[[52]](#footnote-52) (MP) و دایرکتوری منبع برای نمایش سروری که به درخواست‌ها در حین حالت خواب رسیدگی می‌کند و لیستی از منابع موجود بر روی سرور (یا نقاط انتهایی) استفاده می‌کند. پروکسی آینه (MP) نقاط انتهایی را ثبت‌نام می‌کند، منابع را به یک درخت منابع اضافه می‌کند و همچنین کلیدهای عمومی نقاط انتهایی را ذخیره می‌کند. منابع از طریق شناسه‌های خود در دسترس کلاینت‌ها قرار می‌گیرند. کلیدهای عمومی به کلاینت ارسال می‌شوند که متعاقبا برای احراز هویت بروزرسانی‌های داده‌ها مورد استفاده قرار می‌گیرند. پیاده‌سازی نمونه‌ی اولیه نشان داده است که به مقدار کمی انرژی برای دستگاه‌های منابع-محدود نیاز دارد.

پروژه OWASP [23] پیشنهاد تمهیداتی برای امن نمودن اینترنت اشیاء را ارائه می‌دهد. برای مقابله با واسط‌های ناامن سطح-بالا، روش‌های امنیتی شامل پیکربندی‌هایی برای عدم اعتماد به کلمات عبور ضعیفريال آزمایش کردن واسط در برابر آسیب‌پذیری‌های شناخته شده‌ی ابزارهای نرم‌افزاری (SQLi و XSS)، استفاده از https به همراه دیواره‌ی آتش هستند. علاوه بر این، نرم‌افزار یا firmware نصب شده بر روی دستگاه باید به طور منظم از طریق یک روش انتقال رمزنگاری شده بروزرسانی شود. فایل‌های بروزرسانی باید از یک سرور امن دانلود شوند و این فایل‌ها باید پیش از نصب امضا شده و به درستی اعتبارسنجی شوند.

میان‌افزار VIRTUS [63] که توسط Conzon و همکارانش [63] ارائه شده است، یک روش احراز هویت و رمزنگاری را برای امن نمودن برنامه‌های کاربردی توزیع شده در حین اجرا در یک محیط اینترنت اشیاء پیاده‌سازی می‌کند. میان‌افزار از یک رویکرد ارتباطی رویداد-محور استفاده می‌کند، در عین اینکه از TSL و SASL نیز برای یکپارچگی داده‌ها، رمزنگاری و اعتبارسنجی جریان XML استفاده می‌کند. روش احراز هویت در واقع تبادل داده‌ها و دسترسی به منابع را تنها برای کاربران مجاز تضمین می‌کند. میان‌افزار VIRTUS که با سرویس‌های وب ادغام شده است، باعث پیاده‌سازی برنامه‌های کاربردی قابل اعتماد و مقایس‌پذیر برای اینترنت اشیاء می‌شود. یک چارچوب معنایی به نام Otsopack [109] به عنوان یک میان‌افزار عمل می‌کند تا باعث شود پیاده‌سازی‌های ناهمگن به صورت امنی با یکدیگر تعامل داشته باشند. برای قابلیت همکاری، این چارچوب از فرمت معنایی مبتنی بر محاسبات فضایی سه‌گانه[[53]](#footnote-53) (TSC) برای تعامل بین برنامه‌های کاربردی در حال اجرا در داخل یک فضای مجازی استفاده می‌کند. برای تبادل امن داده‌ها، یک راه‌حل امنیتی مبتنی بر Open-ID پیشنهاد شده است. یک فراهم‌کننده‌ی هویت برای اعطای مجوز دسترسی به داده‌های محدود برای کاربران مجاز مورد استفاده قرار گرفته است.

یک سرور میان‌افزار که از فیلتر کردن داده‌ها در حین ارتباط میان محیط‌های ناهمگن اینترنت اشیاء پشتیبانی می‌کند، توسط Liu و همکارانش ارائه شده است [64]. میان‌افزار پیشنهادی از روش کارآمدی برای نامگذاری، آدرس‌دهی، و نمایه‌گذاری در میان محیط‌های ناهمگن پشتیبانی می‌کند. ویژگی‌های استاندارد احراز هویت، مجوز دسترسی، و حسابرسی[[54]](#footnote-54) (AAA) از طریق یک سلسله‌مراتب کلید با کلیدهایی برای ریشه، برنامه‌های کاربردی، و سرویس‌ها پیاده‌سازی شده‌اند. برای ثبت سرویس، یک پورتال مبتنی بر وب پیاده‌سازی شده است تا دسترسی به سرویس‌ها را تنها برای کاربران مجاز فراهم کند. برای ارتباطات ماشین-به-ماشین (M2M) در محیط اینترنت اشیاء، یک معماری استاندارد با لایه‌های مختلف برای امنیت در مرجع [110] پیشنهاد شده است. معماری پیشنهادی شامل لایه‌هایی برای سرویس‌های امنیتی مربوط به قابلیت‌های امنیتی، محیط، و انتزاع است. برای امنیت لایه‌ی سرویس M2M، پیشنهاد شده است که محتویات منابع رمزنگاری شوند و تبادل امن پیام با استفاده از نشست‌های TLS یا DTLS صورت گیرد. معماری امنیتی دیگری برای میان‌افزار اینترنت اشیاء توسط Ferriera و همکارانش ارائه شده است [112]. این معماری امنیتی از روش‌های رمزنگاری استاندارد از قبیل AES برای فراهم نمودن حریم خصوصی داده‌ها استفاده می‌کند. به طور مشابه، امنیت انتها-به-انتها و روش‌های باز احراز هویت پیاده‌سازی شده‌اند. استقرارهای مبتنی بر معماری پیشنهادی قادر به امن نمودن ارتباطات برای موجودیت‌های اینترنت اشیاء از جمله کاربران، اشیاء، و سرویس‌های هستند.

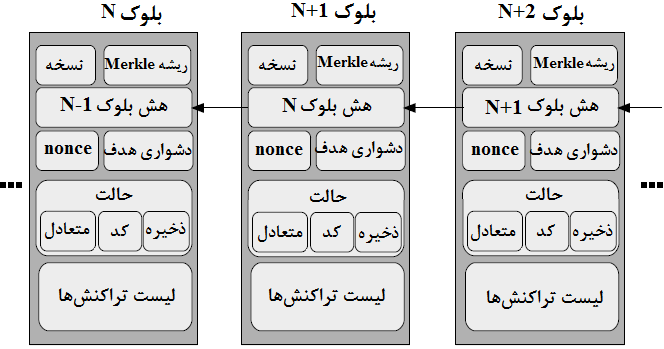
**5. راه‌حل‌های بلاک‌چین برای امنیت اینترنت اشیاء**

فناوری بلاک‌چین از سوی جامعه‌ی صنعتی و پژوهشی به عنوان یک فناوری طغیانگر پیش‌بینی شده است که نقش مهمی در مدیریت، کنترل کردن، و از همه مهمتر حفظ امنیت دستگاه‌های اینترنت اشیاء را دارد. این بخش به تشریح این مورد می‌پردازد که چگونه بلاک‌چین می‌تواند یک فناوری کلیدی برای ارائه‌ی راه‌حل‌های امنیتی مناسب برای مسائل چالش‌برانگیز امروزی در امنیت اینترنت اشیاء باشد. این بخش در ابتدا پس‌زمینه‌ی مختصری در مورد بلاک‌چین ارائه می‌دهد، و سپس به مطرح نمودن آن دسته از مسائل و چالش‌های باز امنیت اینترنت اشیاء می‌پردازد که بلاک‌چین ممکن است راه‌حلی برای آنها ارائه دهد. این بخش همچنین راه‌حل‌های مبتنی بر بلاک‌چین ارائه شده برای مسائل امنیتی اینترنت اشیاء را نیز بررسی می‌کند.

*5-1. پس‌زمینه*

یک بلاک‌چین اساسا یک پایگاه‌داده‌ی دفتر کل[[55]](#footnote-55) غیرمتمرکز، به اشتراک گذاشته شده، و تغییرناپذیر است که فهرست (رجیستری) دارایی‌ها و تراکنش‌ها را در سرتاسر یک شبکه‌ی نظیر-به-نظیر (P2P) ذخیره می‌کند. بلاک‌چین در واقع بلوک‌هایی از داده‌ها را به هم می‌پیوندد (زنجیر می‌کند) که توسط ماینرها برچسب زمانی زده شده و تایید شده‌اند. بلاک‌چین از رمزنگاری منحنی بیضوی[[56]](#footnote-56) (ECC) و هش کردن SHA-256 جهت ارائه‌ی اثبات رمزنگاری قوی برای احراز هویت و یکپارچگی داده‌ها استفاده می‌کند [112]. به طور اساسی، بلوک داده‌ها شامل لیستی از تمام تراکنش‌ها و یک هش به بلوک قبلی است. بلاک‌چین یک پیشینه‌ی کامل از تمام تراکنش‌ها دارد و یک اعتماد توزیع شده‌ی سراسری بین‌المللی را ارائه می‌دهد. شخص ثالث مورد اعتماد[[57]](#footnote-57) (TTP) یا مقامات مسئول و سرویس‌های متمرکز می‌توانند مختل شوند، یا در معرض خطر قرار گرفته یا هک شوند. این موارد هر چند که اکنون قابل اعتماد هستند، ولی می‌توانند در آینده مورد سوءاستفاده قرار گرفته و رفتاری بدی از خود نشان دهند. در بلاک‌چین، هر تراکنش در دفتر کل عمومی به اشتراک گذاشته شده توسط توافق اکثریت گره‌های ماینر مورد بررسی قرار می‌گیرد، گره‌های ماینری که به صورت فعال در بررسی و تایید تراکنش‌ها شرکت دارند. در یک شبکه‌ی بیت‌کوین [113]، ماینرها به بلاک با محاسبه‌ی یک هش با صفرهای عمده جهت ایجاد یک هدف دشوار اعتبار می‌دهند. به محض اینکه تراکنش‌ها با توافق اکثریت ماینرها مورد بررسی و تایید قرار می‌گیرد، بلوک داده‌ها دیگر غیرقابل تغییر هستند، یعنی داده‌ها نمی‌توانند هرگز حذف شده یا تغییر داده شوند. بلاک‌چین می‌تواند بدین صورت ساخته شود: (1) شبکه مجاز (یا خصوصی) که می‌تواند به گروه خاصی از شرکت‌کنندگان محدود شود، یا (2) شبکه‌ی کمتر-مجاز یا عمومی که برای پیوستن عموم آزاد است. بلاک‌چین‌های مجاز حریم خصوصی بیشتر و کنترل دسترسی بهتری را ارائه می‌دهند.

شکل 4 یک ساختار طراحی معمولی از یک بلاک‌چین را نشان می‌دهد. ساختار طراحی عمدتا از سرآیند (هِدر) بلوک و بدنه‌ی بلوک تشکیل شده است که شامل لیستی از تراکنش‌ها می‌باشد. سرآیند بلوک شامل قسمت‌های مختلفی است (فیلدهای مختلف)، یکی از آنها شماره‌ی نسخه برای پیگیری نرم‌افزاری ارتقاهای پروتکل است. همچنین، سرآیند شامل یک برچسب زمانی، اندازه‌ی بلوک، و تعداد تراکنش‌ها است. قسمت ریشه‌ی Merkle نشان‌دهنده‌ی مقدار هش بلوک فعلی است. هش کردن درخت Merkle معمولا در سیستم‌های توزیع شده و شبکه‌های P2P برای اعتبارسنجی کارآمد داده‌ها مورد استفاده قرار می‌گیرد. قسمت nonce برای الگوریتم اثبات-کار (proof-of-work) به کار گرفته می‌شود، و یک مقدار شمارنده‌ی آزمایشی است که هش را با صفرهای پیشرو[[58]](#footnote-58) تولید می‌کند. دشواری هدف در واقع تعداد صفرهای پیشرو را مشخص می‌کند، و برای حفظ زمان‌بلوکی تقریبا برابر با 10 دقیقه برای Bitcoin [114]، و 17.5 ثانیه برای Ethereum [115] مورد استفاده قرار می‌گیرد. دشواری هدف به صورت دوره‌ای قابل تنظیم است و در طول زمان با افزایش توان محاسباتی سخت‌افزار (با صفرهای پیشرو بیشتر) افزایش می‌یابد. زمان‌بلوکی با طراحی تنظیم می‌شود تا زمان انتشار بلوک‌ها را برای رسیدن به تمام ماینرها، و زمان رسیدن به یک توافق و اجماع را بین تمام ماینرها محاسبه کند.



شکل 4. ساختار طراحی بلاک‌چین که زنجیره‌ی بلوک‌ها را با سرآیند (هدر) و قسمت‌های بدنه نشان می‌دهد.

Bitcoin یکی از اولین و محبوب‌ترین برنامه‌های کاربردی است که بر بالای زیرساخت بلاک‌چین اجرا می‌شود. به طور کلی، بلاک‌چین bitcoin بستر و فناوری زیرساخت برای بسیاری از رمزهای دیجیتال[[59]](#footnote-59) مشهور (ارز رمز) شده است. با این حال، با پیشرفت بلاک‌چین Ethereum، که قراردادهای هوشمند را پیاده‌سازی می‌کند، فضای مصرف بالقوه از بلاک‌چین به صورت بی‌نهایت در آمده است. بلاک‌چین Ethereum در جولای سال 2015 راه‌اندازی شده و در دسترس عموم قرار گرفته است. پس از آن، بسترهای بلاک‌چین مشابهی با قراردادهای هوشمند اخیرا ظهور کرده‌اند. این بسترهای نوظهور شامل Hyperledger [116]، Eris [117]، Stellar [118]، Ripple [119]، و Tendermint [120] می‌باشند. برخلاف بلاک‌چین bitcoin که عمدتا برای تراکنش‌های ارز دیجیتال مورد استفاده قرار می‌گیرد، بلاک‌چین Ethereum قابلیت ذخیره‌ی رکوردها، و از همه مهمتر، اجرای قراردادهای هوشمند را دارد. اصطلاح قراردادهای هوشمند در ابتدا توسط Nick Szabo در سال 1994 ابداع شده است. یک قرارداد هوشمند به طور اساسی یک پروتکل معامله (تراکنش) کامپیوتری شده است که شرایط موجود در قرارداد را اجرا می‌کند. در تعریف ساده، قراردادهای هوشمند در واقع برنامه‌هایی هستند که توسط کاربران نوشته شده‌اند تا بر روی بلاک‌چین بارگذاری و اجرا شوند. زبان اسکریپت‌نویسی یا برنامه‌نویسی برای قراردادهای هوشمند Solidity نام دارد که یک زبان مشابه JavaScript است. بلاک‌چین Ethereum، EVM[[60]](#footnote-60) (ماشین‌های مجازی Ethereum) را فراهم می‌کند که به طور اساسی گره‌های استخراج‌کننده (ماینر) هستند. این گره‌ها قادر به اجرای این برنامه‌های یا قراردادها به صورت رمزنگاری شده و غیرقابل تحریف و قابل اعتماد هستند.

Ethereum از ارز دیجیتالی خود به نام Ether پشتیبانی می‌کند. همانند bitcoin، در Ethereum نیز کاربران می‌تواند سکه‌ها را با استفاده از تراکنش‌های عادی با یکدیگر مبادله کنند که در دفتر کل ثبت می‌شود، و برای چنین تراکنش‌هایی، نیازی به یک حالت بلاک‌چین در bitcoin نیست. با این حال، برای Ethereum برای پشتیبانی از اجرای قراردادهای هوشمند، یک حالت بلاک‌چین مورد استفاده قرار می‌گیرد که در شکل 4 نشان داده شده است. یک قرارداد هوشمند دارای حساب و آدرس خود است، و کد اجرایی خود و تعادل سکه‌های Ether را نیز به آن مرتبط می‌سازد. ذخیره‌سازی به صورت پایدار است و کد را نگه می‌دارد تا بر روی گره‌های EVM اجرا شود. ذخیره‌سازی EVM نسبتا گران است، برای ذخیره‌سازی‌های بزرگ باید به بلاک‌چین آپلود شود، و برای ذخیره‌سازی داده‌ها به صورت غیرمتمرکز و از راه دور مواردی مانند BitTorrent، IPFS، یا Swarm نیز می‌تواند مورد استفاده قرار گیرند. با این حال قراردادهای هوشمند می‌توانند یک هش اعتبارسنجی از چنین اطلاعات ذخیره شده‌ای راه دوری نگهداری کنند.

موارد استفاده و کاربردهای احتمالی قراردادهای هوشمند بلاک‌چین بسیار زیاد و بی‌پایان است، و از ارز دیجیتال و معاملات گرفته تا تراکنش‌های مستقل ماشین-با-ماشین، از زنجیره‌ تامین و ردیابی دارایی‌ها گرفته تا کنترل دسترسی و اشتراک‌گذاری به صورت خودکار، از هویت دیجیتال و رأی‌گیری برای صدور گواهینامه گرفته تا مدیریت، و مدیریت سوابق (رکوردها)، داده‌ها، یا آیتم‌ها می‌باشد [121]. استقرارهای تجاری مبتنی بر بلاک‌چین به سرعت در حال افزایش هستند. به عنوان مثال، SafeShare [122] راه‌حل بیمه را با استفاده از بلاک‌چین مبتنی بر bitcoin ارائه کرده است. به طور مشابه، IBM چارچوب بلاک‌چین خود را با استفاده از بستر Hyperledger Fabric راه‌اندازی نموده است [123]. این چارچوب از توسعه‌ی برنامه‌های کاربردی بلاک‌چین پشتیبانی می‌کند و برخلاف چارچوب‌های دیگر، نیازی به ارز دیجیتال ندارد. بلاک‌چین IBM به صورت تجاری در بانک‌ها، سیستم‌های زنجیره‌ی تامین، و شرکت‌های حمل و نقل کالا مورد استفاده قرار گرفته است.

*5-2. راه‌حل‌های بالقوه‌ی بلاک‌چین*

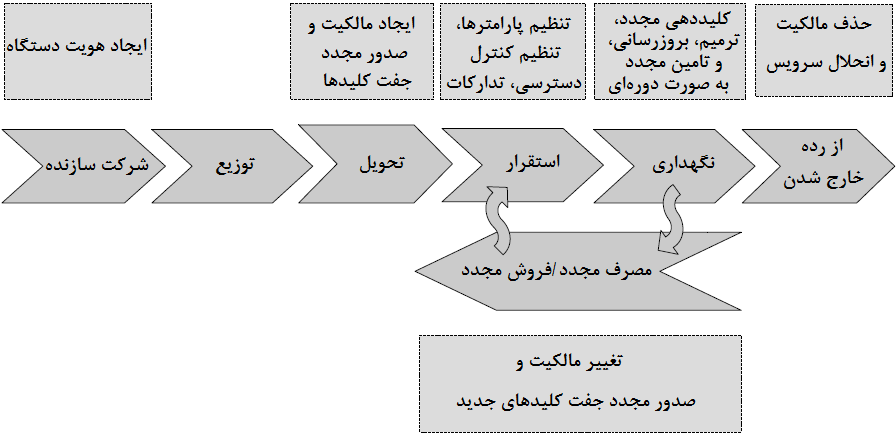
در زمینه‌ی اینترنت اشیاء، بلاک‌چین بر اساس قراردادهای هوشمندی است که انتظار می‌رود نقش مهمی در مدیریت، کنترل، و از همه مهمتر در امن‌سازی دستگاه‌های اینترنت اشیاء داشته باشد. ما در این بخش به بحث و خلاصه‌سازی برخی از ویژگی‌های ذاتی بلاک‌چین می‌پردازیم که می‌تواند به طور کلی برای اینترنت اشیاء، و به ویژه برای امنیت اینترنت اشیاء بسیار مفید باشد.

**فضای آدرس**. بلاک‌چین یک فضای آدرس 160-بیتی دارد، بر خلاف فضای آدرس IPv6 که فضای آدرس 128-بیتی دارد [112]. یک آدرس بلاک‌چین به صورت 20 بایت یا یک هش 160-بیتی از کلید عمومی تولید شده توسط ECDSA[[61]](#footnote-61) (الگوریتم امضای دیجیتال منحنی بیضوی) است. با آدرس 160-بیتی، بلا‌ک‌چین می‌تواند آدرس‌های آفلاین را برای حدود 1048 1.46 عدد دستگاه اینترنت اشیاء تولید کرده و به آنها اختصاص دهد. احتمال تداخل آدرس‌ها (یعنی تولید دو آدرس یکسان برای دو دستگاه متفاوت) تقریبا برابر با 1048 است، که برای ارائه‌ی یک GUID[[62]](#footnote-62) (شناسه‌ی منحصربه‌فرد سراسری) به اندازه‌ی کافی امن به نظر می‌رسد و در هنگام انتساب و تخصیص یک آدرس به یک دستگاه اینترنت اشیاء، نیاز به هیچ ثبت‌نام یا اعتبارسنجی یکتایی نیست. با بلاک‌چین، یک مقام مسئول و دولت متمرکز، همانطور که در مقام مسئول اعداد تخصیص داده شده در اینترنت[[63]](#footnote-63) (IANA) وجود دارد، حذف شده است. در حال حاضر، IANA بر تخصیص آدرس‌های کلی IPv4 و IPv6 نظارت می‌کند، علاوه بر این، بلاک‌چین تعداد 4.3 میلیارد آدرس بیشتر از IPv6 فراهم می‌کند، بنابراین، این دلایل بلاک‌چین را نسبت به IPv6 یک راه‌حل مقیاس‌پذیرتر برای اینترنت اشیاء می‌سازند. در نهایت، شایان ذکر است که اکثر دستگاه‌های اینترنت اشیاء ظرفیت محاسباتی و حافظه‌ی محدودی دارند، و از این رو برای اجرای یک پشته‌ی IPv6 مناسب نخواهند بود.

**هویت اشیاء[[64]](#footnote-64) (IDoT) و کنترل آنها**. مدیریت هویت و دسترسی[[65]](#footnote-65) (IAM) برای اینترنت اشیاء باید مسائل چالش‌برانگیز زیادی را به صورت کارآمد، امن، و قابل اعتماد مورد رسیدگی قرار دهد. یک چالش اصلی به روابط مالکیت و هویت دستگاه‌های اینترنت اشیاء رسیدگی می‌کند. مالکیت یک دستگاه در طول عمر دستگاه از کارخانه‌ی سازنده، عرضه‌کننده، خرده فروش، و مصرف‌کننده تغییر می‌کند [124 و 51]. اگر دستگاه دوباره به فروش برسد، از کار بیفتد، یا به خطر بیفتد (آلوده شود)، آنگاه مالکیت مصرف‌کننده‌ی یک دستگاه اینترنت اشیاء می‌تواند تغییر یابد یا لغو شود. مدیریت ویژگی‌ها و روابط یک دستگاه اینترنت اشیاء نیز چالش دیگری است. ویژگی‌های یک دستگاه می‌تواند شامل کارخانه‌ی سازنده، ساخت، نوع، شماره سریال، استقرار مختصات GPS، مکان، و غیره باشد. به غیر از ویژگی‌ها، توانایی‌ها، و ویژگی‌ها، دستگاه‌های اینترنت اشیاء روابط نیز دارند. روابط اینترنت اشیاء ممکن است شامل دستگاه-به-انسان، دستگاه-به-دستگاه، یا دستگاه-به-سرویس باشد. یک رابطه‌ی دستگاه اینترنت اشیاء می‌تواند توسط کسی مستقر شود، توسط کسی مورد استفاده قرار گیرد، توسط کسی حمل و نقل شود، توسط کسی فروخته شود، توسط کسی ارتقاء یابد، توسط کسی تعمیر شود، و غیره.

بلاک‌چین توانایی حل این چالش‌ها را به سادگی، به صورت امن و کارآمدی دارد. بلاک‌چین به طور گسترده‌ای برای فراهم نمودن قابل اعتماد و مجاز ثبت‌نام هویت، ردیابی مالکیت و نظارت بر محصولات، کالاها، و دارایی‌ها مورد استفاده قرار گرفته است. رویکردهایی مانند TrustChain [125] برای ممکن ساختن تراکنش‌های قابل اعتماد با استفاده از بلاک‌چین، در عین حفظ صحت و یکپارچگی تراکنش‌ها در یک محیط توزیع شده پیشنهاد شده‌اند. دستگاه‌های اینترنت اشیاء استثناء نیستند. بلاک‌چین می‌تواند برای ثبت‌نام و دادن هویت به دستگاه‌های متصل اینترنت اشیاء، دستگاه‌هایی با مجموعه‌ای از ویژگی‌ها و روابط پیچیده مورد استفاده قرار گیرد، این مجموعه ویژگی‌ها و روابط پیچیده می‌توانند بر روی دفتر کل توزیع شده‌ی بلاک‌چین آپلود و ذخیره شوند.

بلاک‌چین همچنین یک مدیریت غیرمتمرکز قابل اعتماد، اداره، و ردیابی در هر نقطه از زنجیره‌ی تامین و چرخه‌ی حیات یک دستگاه اینترنت اشیاء را فراهم می‌کند، همانطور که در شکل 5 نشان داده شده است. زنجیره تامین می‌تواند شامل چندین بازیگر مانند کارخانه، فروشنده، عرضه‌کننده، توزیع‌کننده، حمل‌کننده، نصب‌کننده، مالک، تعمیرکار، نصب مجدد کننده، و غیره باشد. همانطور که در شکل 5 نشان داده شده است، در طول چرخه‌ی حیات یک دستگاه اینترنت اشیاء، جفت‌کلیدها می‌توانند تغییر یافته و مجددا به چندین نقطه صادر شوند. صدور جفت‌کلیدها می‌تواند در ابتدا توسط کارخانه‌ی سازنده انجام شود، و سپس به صورت دوره‌ای پس از استقرار توسط مالک صورت گیرد.



شکل 5. مدیریت امنیتی چرخه حیات دستگاه اینترنت اشیاء.

**احراز هویت و یکپارچگی (صحت) داده‌ها**. با طراحی، داده‌های ارسال شده توسط دستگاه‌های اینترنت اشیاء متصل به شبکه‌ی بلاک‌چین همیشه به صورت رمزنگاری اثبات و امضا خواهند شد که توسط فرستنده‌ی واقعی ارسال شده‌اند، یعنی کسی که یک کلید عمومی منحصربه‌فرد و GUID دارد، و بدین ترتیب احراز هویت و صحت (یکپارچگی) داده‌های منتقل شده تضمین خواهد شد. علاوه بر این، تمام تراکنش‌های انجام شده با یا توسط یک دستگاه اینترنت اشیاء در دفتر کل توزیع شده‌ی بلاک‌چین ثبت شده و می‌توانند به صورت امنی ردیابی شوند.

**احراز هویت، مجوز دسترسی، و حریم خصوصی**. قراردادهای هوشمند بلاک‌چین توانایی ارائه‌ی قوانین و منطق غیر-متمرکز احراز هویت را دارند تا بدین وسیله قادر به فراهم نمودن احراز هویت تکی و یا چند طرفه‌ی یک دستگاه اینترنت اشیاء باشند. همچنین در مقایسه با پروتکل‌های معمولی صدور مجوز دسترسی مانند مدیریت دسترسی بر اساس نقش[[66]](#footnote-66) (RBAC)، OAuth 2.0، OpenID، OMA DM و LWM2M، قراردادهای هوشمند در بلاک‌چین می‌توانند قوانین مجوز دسترسی را به صورت کارآمدتر و با پیچیدگی کمتری برای دستگاه‌های متصل اینترنت فراهم آورند. این پروتکل‌ها امروزه به طور گسترده‌ای برای احراز هویت دستگاه‌های اینترنت اشیاء، صدور مجوز دسترسی، و مدیریت آنها مورد استفاده قرار می‌گیرند. علاوه بر این، همچنین با استفاده از قراردادهای هوشمند حریم خصوصی داده‌ها نیز می‌تواند تضمین شود، این قراردادها قوانین، شرایط، و زمان دسترسی را به کاربر خاصی یا گروه خاصی از کاربران یا ماشین‌ها می‌دهد تا اجازه‌ی دسترسی به داده‌های ذخیره شده یا در حال انتقال را داشته، صاحب آنها شده و آنها را کنترل نمایند. قراردادهای هوشمند می‌توانند این حقوق را تعریف کنند که چه کسی حق بروزرسانی، ارتقاء، تعمیر و اضافه کردن نرم‌افزار یا سخت‌افزار اینترنت اشیاء، ریست کردن دستگاه اینترنت اشیاء، ارائه جفت کلیدهای جدید، راه‌اندازی یک سرویس یا درخواست تعمیر، تغییر مالکیت، و تامین یا تامین مجدد دستگاه را دارد.

**ارتباطات امن**. پروتکل‌های ارتباطی برنامه‌ی کاربردی اینترنت اشیاء از جمله HTTP، MQTT، CoAP، یا XMPP، یا حتی پروتکل‌های مربوط به مسیریابی از جمله RPL و 6LoWPAN، با طراحی امن نیستند. چنین پروتکل‌هایی باید در داخل دیگر پروتکل‌های امنیتی از قبیل DTLS یا TLS برای پیام‌رسانی و پروتکل‌های کاربردی قرار بگیرند تا ارتباطات امنی را فراهم کنند. به طور مشابه، برای مسیریابی، IPSec معمولا برای تامین امنیت پروتکل‌های RPL و 6LoWPAN مورد استفاده قرار می‌گیرد. DTLS، TLS، IPSec، یا حتی پروتکل‌های سبک-وزن TinyTLS از لحاظ نیازهای ارتباطی و حافظه سنگین و پیچیده هستند، و با یک مدیریت متمرکز و مدیریت و توزیع کلید با استفاده از پروتکل مشهور PKI پیچیده‌تر می‌شوند. با بلاک‌چین، مدیریت و توزیع کلید کلا حذف می‌شود، زیرا هر دستگاه اینترنت اشیاء GUID منحصربه‌فرد خود را داشته و به محض نصب و اتصال به شبکه‌ی بلاک‌چین نیز یک جفت کلید نامتقارن خواهد داشت. این امر باعث ساده‌تر شدن دیگر پروتکل‌های امنیتی مانند DTLS خواهد شد، زیرا هیچ نیازی به رسیدگی و تبادل گواهینامه‌های PKI در مرحله‌ی دست‌دهی در مورد DTLS یا TLS (یا IKE در مورد IPSec) وجود ندارد تا در مورد پارامترهای مجموعه‌ی رمز برای رمزنگاری و هش کردن جهت ایجاد کلیدهای ارشد و نشست مذاکره صورت گیرد. بنابراین، پروتکل‌های سبک-وزن امنیتی متناسب با نیازهای منابع محاسباتی و حافظه در دستگاه‌های اینترنت اشیاء، بیشتر امکانپذیر شده‌اند.

*5-3. کارهای مرتبط در زمینه‌ی بلاک‌چین و اینترنت اشیاء*

در ادبیات کارهای مرتبط، تحقیقات بر روی امنیت اینترنت اشیاء و بلاک‌چین به گونه‌ای محدود شده است که اکثر این کارهای تحقیقاتی با تمرکز بر روی استفاده از فناوری بلاک‌چین به طور کلی برای بهره بردن از اینترنت اشیاء صورت گرفته است. نویسندگان در مرجع [126] به دسته‌بندی 18 عدد از موارد استفاده‌ی بلاک‌چین پرداخته‌اند، که چهار مورد از آنها برای اینترنت اشیاء است. چهار دسته از موارد استفاده برای اینترنت اشیاء عبارتند از: ثبت تغییرناپذیر رویدادها و مدیریت کنترل دسترسی به داده‌ها [127]، تبادل و معامله‌ی داده‌های جمع‌آوری شده‌ی اینترنت اشیاء [128 و 129]، و مدیریت کلید متقارن و نامتقارن برای دستگاه‌های اینترنت اشیاء [130 و 131]. نویسندگان در مرجع [124] چالش‌های موجود برای هویت را در اینترنت اشیاء مطرح کرده‌اند. این چالش‌ها در درجه‌ی اول شامل روابط مالکیت و هویت، احراز هویت و مجوز صدور دسترسی، مدیریت و حفظ داده‌ها و حریم خصوصی می‌باشند. ما در بخش 5-1، در این مورد بحث می‌کنیم که بلاک‌چین چگونه می‌تواند یک عامل کلیدی برای حل این چالش‌ها باشد.

نویسندگان در مرجع [132] یک چارچوب مبتنی بر بلاک‌چین را برای اینترنت اشیاء صنعتی[[67]](#footnote-67) (IIoT) ارائه می‌کنند. این چارچوب دستگاه‌های IIoT را قادر می‌سازد تا با ابر و همچنین شبکه بلاک‌چین ارتباط برقرار کنند. هر دستگاه IIoT به یک سیستم کامپیوتری تک-بورد[[68]](#footnote-68) (SBC) مجهز است که قابلیت‌های واسط کنترل و ارتباط را برای هر دو سمت ابری و Ethereum بلاک‌چین دارد. دستگاه‌های IIoT برای ارسال داده‌ها به ابر برای ذخیره‌سازی و تحلیل، و تراکنش‌های ارسال/دریافت به دیگر دستگاه‌های موجود در شبکه‌ی بلاک‌چین، و همچنین برای فعالسازی اجراها در قراردادهای هوشمند طراحی شده‌اند. به عنوان اثباتی برای مفهوم، نویسندگان یک بستر ساده را با استفاده از بورد Arduino Uno و قراردادهای هوشمند Ethereum پیاده‌سازی نموده‌اند و به طور خلاصه شرح داده‌اند که این بستر چگونه می‌تواند برای نگهداری از ماشین و تشخیص‌های هوشمند مورد استفاده قرار بگیرد.

برنامه‌های کاربردی قراردادهای هوشمند بلاک‌چین برای اینترنت اشیاء توسط Chritidis و همکارانش [133] بررسی شده است. نویسندگان در این مرجع شرح داده‌اند که چگونه قراردادهای هوشمند بلاک‌چین می‌توانند جریان کاری مستقل و اشتراک‌گذاری سرویس‌ها میان دستگاه‌های اینترنت اشیاء را تسهیل و پشتیبانی کنند، همانطور که در مرجع [134] ارائه شده است. علاوه بر این، نویسندگان در این مورد بحث می‌کنند که اینترنت اشیاء چگونه می‌تواند از شبکه‌های بلاک‌چین در جنبه‌های مرتبط با صدور صورتحساب، تجارت الکترونیک، حمل و نقل و مدیریت زنجیره‌ی تامین بهره ببرد. به علاوه، آنها سناریویی را شرح می‌دهند که بلاک‌چین می‌تواند خرید و فروش انرژی را به طور خودکار میان دستگاه‌های اینترنت اشیاء مانند کنتورهای هوشمند ممکن سازد. قراردادهای هوشمند می‌توانند برای تنظیم معیارهای تعریف شده توسط کاربر برای معامله‌ی انرژی مورد استفاده قرار گیرند. نویسندگان همچنین سناریوی دیگری را برای ردیابی اموال در طول حمل و نقل با کانیتنر با استفاده از قراردادهای هوشمند و اینترنت اشیاء شرح می‌دهند.

**6. چالش‌های باز و مسیرهای تحقیقاتی آینده**

این بخش در مورد چالش‌هایی بحث می‌کند که پیاده‌سازی موثر امنیت در دستگاه‌های اینترنت اشیاء با آنها روبرو است.

*6-1. محدودیت‌های منابع*

معماری منابع-محدود اینترنت اشیاء به مانع اصلی در تعریف یک مکانیزم قوی امنیتی تبدیل شده است. برخلاف الگوهای معمولی، الگوریتم‌های رمزنگاری باید برای کار در این محدودیت‌ها محدود شوند. با هر بار همه‌پخشی[[69]](#footnote-69)، یا چندپخشی[[70]](#footnote-70) اطلاعات موردنیاز برای تبادل کلیدها یا گواهینامه‌ها، منابع ذخیره‌سازی و انرژی باید از عهده‌ی این کار بر بیایند تا بتوانند پیاده‌سازی موفقی از پروتکل‌های امنیتی و ارتباطی را برای اینترنت اشیاء ارائه دهند. چنین امری مستلزم این است که این پروتکل‌ها دوباره طراحی شوند تا با وجود محاسبات پیچیده‌ی موردنیاز، سبک و کم حجم بوده و انرژی کارآمد باشند و با روش‌های مهار انرژی بهبود یابند [135].

*6-2. دستگاه‌های ناهمگن*

با وجود دستگاه‌های ناهمگن از وسایل کم توان مجهز به حسگر گرفته تا سرورهای سطح بالا، لازم است تا یک چارچوب امنیتی چند-لایه‌ای پیاده‌سازی شود. چارچوب باید در ابتدا خود را با منابع موجود سازگار کند، سپس در مورد انتخاب روش‌های امنیتی در لایه‌های اینترنت اشیاء پیش از ارائه‌ی هرگونه سرویسی به کاربران انتهایی تصمیم‌گیری می‌کند. چنین چارچوب امنیتی سازگار پویایی به هوشمندی نیاز دارد، که مستلزم استانداردسازی منابعی است که در معماری‌های اینترنت اشیاء مستقر می‌شوند.

*6-3. قابلیت همکاری میان پروتکل‌های امنیتی*

برای استانداردسازی یک روش کلی امنیتی برای اینترنت اشیاء، پروتکل‌های پیاده‌سازی شده در لایه‌های مختلف باید با ارائه‌ی روش‌های تبدیل، با یکدیگر همکاری کنند. سپس در داخل روش کلی، یک ترکیب موثر و کارآمدی از استانداردهای امنیتی در هر لایه می‌تواند از طریق در نظر گرفتن محدودیت‌های معماری تعریف شود.

*6-4. نقاط انفرادی شکست*

با شبکه‌ها، معماری‌ها، و پروتکل‌های ناهمگن موجود، الگوی اینترنت اشیاء بیشتر از هر الگوی دیگری نسبت به نقاط شکست آسیب‌پذیر شده است. کارهای تحقیقاتی زیادی برای تضمین دسترس‌پذیری مناسب عناصر اینترنت اشیاء، به ویژه برای برنامه‌های کاربردی حیاتی همچنان مورد نیاز است. این امر به روش‌ها و استانداردهایی نیاز دارد تا در کنار معرفی افزونگی (برای مقابله با نقاط شکست)، توازن میان هزینه و قابلیت‌اطمینان کل زیرساخت را نیز حفظ کند (یعنی برای مقابله با نقاط شکست، تعدادی عنصر اضافی و تکراری در نظر گرفته می‌شود تا در صورت خراب شدن یکی، دیگری به کار خود ادامه دهد و از ایجاد اخلال در شبکه جلوگیری کند، هر چند این کار باعث افزایش قابلیت‌اطمینان سیستم می‌شود ولی باعث افزایش هزینه نیز می‌گردد).

*6-5. آسیب‌پذیری‌های سخت‌افزار/firmware*

با وجود دستگاه‌های کم-هزینه و کم-توانی که در همه جا حاضر هستند، معماری اینترنت اشیاء ممکن است بیشتر در معرض آسیب‌پذیری‌های سخت‌افزاری قرار بگیرد. نه تنها عملکرد بد فیزیکی، بلکه پیاده‌سازی الگوریتم‌های امنیتی در سخت‌افزار، مسیریابی و روش‌های پردازش بسته‌های داده نیز باید پیش از استقرار در اینترنت اشیاء مورد ارزیابی قرار بگیرند. تشخیص و کاهش هر گونه آسیب‌پذیری کشف شده پس از استقرار بسیار دشوار است. بنابراین یک پروتکل استاندارد ارزیابی یک ضرورت لازم برای کنترل امنیت اینترنت اشیاء است.

*6-6. بروزرسانی‌ها و مدیریت مورد اعتماد*

یکی از مسائل باز کلیدی برای تحقیقات آینده، ارائه‌ی مدیریت و بروزرسانی‌های مقیاس‌پذیر و قابل اعتماد نرم‌افزار میلیون‌ها دستگاه اینترنت اشیاء است. علاوه بر این، مسائل مربوط به مدیریت امن و قابل اعتماد مالکیت دستگاه اینترنت اشیاء، زنجیره‌ی تامین، و حریم خصوصی داده‌ها نیز از مسائل باز تحقیقاتی هستند که نیاز به رسیدگی توسط جامعه‌ی تحقیقاتی دارند تا یک استقرار مقیاس‌پذیر گسترده و وسیعی از اینترنت اشیاء را تقویت نمایند. فناوری بلاک‌چین می‌تواند یک روش ممکن برای چنین راه‌حل‌های امنیتی اینترنت اشیاء باشد. با این حال، خود فناوری بلاک‌چین نیز به نوبه‌ی خود با چالش‌های تحقیقاتی در رابطه با مقیاس‌پذیری، کارایی، داوری/مقررات، و تداخل کلید روبرو است که باید مورد رسیدگی قرار گرفته و حل شوند.

*6-7. آسیب‌پذیری‌های بلاک‌چین*

با وجود ارائه‌ی رویکردهای قوی برای امن نمودن اینترنت اشیاء، سیستم‌های بلاک‌چین همچنان آسیب‌پذیر هستند [136]. روش توافق کلی که به قدرت هش کردن ماینر (miner) بستگی دارد، می‌تواند به خطر بیفتد، که این امر به مهاجم اجازه می‌دهد تا بلاک‌چین را میزبانی کند. به طور مشابه، کلیدهای خصوصی با تصادفی‌سازی محدود شده می‌توانند برای سوءاستفاده و به خطر انداختن حساب‌های بلاک‌چین مورد استفاده قرار گیرند. همچنان نیاز است که روش‌های موثری برای تضمین حریم خصوصی تراکنش‌ها و پیشگیری از حمله‌های مسابقه‌ای[[71]](#footnote-71) تعریف شوند که این حمله‌ها ممکن است به دو برابر شدن هزینه‌ی صرف شده در حین تراکنش منجر شوند.

**7. نتیجه‌گیری**

امروزه دستگاه‌های اینترنت اشیاء ناامن بوده و قادر به دفاع از خود نیستند. علت این امر عمدتا به دلیل وجود منابع محدود در دستگاه‌های اینترنت اشیاء، استاندادرهای نابالغ، و فقدان طراحی، توسعه، و پیاده‌سازی امن سخت‌افزاری و نرم‌افزاری است. همچنین تنوع منابع در اینترنت اشیاء مانع از تعریف یک روش کلی قوی برای امن نمودن لایه‌های اینترنت اشیاء شده است. ما در این مقاله به بررسی و مرور مسائل عمده‌ی امنیتی در اینترنت اشیاء پرداخته‌ایم. ما این مسائل را بسته به سطح بالا، سطح میانی، و سطح پایین لایه‌های اینترنت اشیاء دسته‌بندی نموده‌ایم. ما به طور خلاصه در مورد روش‌هایی بحث نموده‌ایم که در مقالات مختلف برای ارتقای امنیت اینترنت اشیاء در سطوح مختلف پیشنهاد شده‌اند. یک تحلیل پارامتری از حمله‌ها در اینترنت اشیاء و راه‌حل‌های احتمالی آنها نیز ارائه شده است. ما پیامدهای حمله‌ها را در نظر گرفته و آنها را به راه‌حل‌های ممکن ارائه شده در مقالات نگاشت نموده‌ایم. ما همچنین در این مورد بحث نموده‌ایم که بلاک‌چین چگونه می‌تواند به برخی از مهمترین مسائل امنیتی اینترنت اشیاء رسیدگی نموده و آنها را حل نماید. مقاله همچنین مسائل باز تحقیقاتی و چالش‌های آینده را مطرح و تعریف کرده است، مسائلی که نیاز به رسیدگی بیشتر توسط جوامع تحقیقاتی دارند تا راه‌حل‌های امنیتی قابل‌اطمینان، کارآمد، و مقیاس‌پذیر برای اینترنت اشیاء ارائه شود.

1. biochips [↑](#footnote-ref-1)
2. Wireless Sensor Networks (WSN) [↑](#footnote-ref-2)
3. Machine-to-Machine (M2M) [↑](#footnote-ref-3)
4. Cyber-Physical Systems (CPS) [↑](#footnote-ref-4)
5. end-to-end [↑](#footnote-ref-5)
6. Mobile Cloud Computing [↑](#footnote-ref-6)
7. multi-party [↑](#footnote-ref-7)
8. Open Web Application Security Project (OWASP) [↑](#footnote-ref-8)
9. Low Rate Wireless Personal Area Networks (LR-WPANs) [↑](#footnote-ref-9)
10. Low Power Wide Area Network (LPWAN) [↑](#footnote-ref-10)
11. Medium Access Control (MAC) [↑](#footnote-ref-11)
12. Maximum Transmission Unit (MTU) [↑](#footnote-ref-12)
13. Routing Protocol for Low-Power and Lossy Networks (RPL) [↑](#footnote-ref-13)
14. payload [↑](#footnote-ref-14)
15. User Datagram Protocol (UDP) [↑](#footnote-ref-15)
16. header [↑](#footnote-ref-16)
17. Internet Control Message Protocol (ICMP) [↑](#footnote-ref-17)
18. Narrow-Band Internet of Thins (NB-IoT) [↑](#footnote-ref-18)
19. Weightless protocol [↑](#footnote-ref-19)
20. Denial-of-Service (DoS) [↑](#footnote-ref-20)
21. jamming adversaries [↑](#footnote-ref-21)
22. replay attacks [↑](#footnote-ref-22)
23. Quality of Service (QoS) [↑](#footnote-ref-23)
24. address resolution [↑](#footnote-ref-24)
25. IPv6 Routing Protocol for Low-Power and Lossy Network (RPL) [↑](#footnote-ref-25)
26. Constrained Application Protocol (CoAP) [↑](#footnote-ref-26)
27. multicast [↑](#footnote-ref-27)
28. channel surfing [↑](#footnote-ref-28)
29. spatial retreats [↑](#footnote-ref-29)
30. Open Web Application Security Project (OWASP) [↑](#footnote-ref-30)
31. Trusted Platform Modules (TPMs) [↑](#footnote-ref-31)
32. Elliptic Curve Cryptography (ECC) [↑](#footnote-ref-32)
33. adversary attacks [↑](#footnote-ref-33)
34. Directed Acyclic Graph (DAG) [↑](#footnote-ref-34)
35. preferred parent [↑](#footnote-ref-35)
36. failover [↑](#footnote-ref-36)
37. Destination Information Object (DIO) [↑](#footnote-ref-37)
38. Dynamic Source Routing (DSR) [↑](#footnote-ref-38)
39. Peer-to-Peer (P2P) [↑](#footnote-ref-39)
40. Authentication Header (AH) [↑](#footnote-ref-40)
41. Encapsulating Security Payload (ESP) [↑](#footnote-ref-41)
42. Security Parameters Index (SPI) [↑](#footnote-ref-42)
43. Certificate Authority (CA) [↑](#footnote-ref-43)
44. multicast [↑](#footnote-ref-44)
45. 6LoWPAN Border Router (6LBR) [↑](#footnote-ref-45)
46. Next Header Compression (NHC) [↑](#footnote-ref-46)
47. checksum [↑](#footnote-ref-47)
48. Internet Key Exchange (IKE) [↑](#footnote-ref-48)
49. Low-power and Lossy Network (LLN) [↑](#footnote-ref-49)
50. 6LoWPAN Border Router (6LBR) [↑](#footnote-ref-50)
51. handeshake [↑](#footnote-ref-51)
52. Mirror Proxy (MP) [↑](#footnote-ref-52)
53. Triple Space Computing (TSC) [↑](#footnote-ref-53)
54. Authentication, Authorization, and Accounting (AAA) [↑](#footnote-ref-54)
55. ledger [↑](#footnote-ref-55)
56. Elliptic Curve Cryptography (ECC) [↑](#footnote-ref-56)
57. Trusted Third Parties (TTP) [↑](#footnote-ref-57)
58. leading zeros [↑](#footnote-ref-58)
59. cryptocurrencies [↑](#footnote-ref-59)
60. Ethereum Virtual Machines (EVM) [↑](#footnote-ref-60)
61. Elliptic Curve Digital Signature Algorithm (ECDSA) [↑](#footnote-ref-61)
62. Global Unique Identifier (GUID) [↑](#footnote-ref-62)
63. Internet Assigned Numbers Authority (IANA) [↑](#footnote-ref-63)
64. Identity of Things (IDoT) [↑](#footnote-ref-64)
65. Identity and Access Management (IAM) [↑](#footnote-ref-65)
66. Role Based Access Management (RBAC) [↑](#footnote-ref-66)
67. Industrial Internet of Things (IIoT) [↑](#footnote-ref-67)
68. Single-Board Computer (SBC) [↑](#footnote-ref-68)
69. broadcast [↑](#footnote-ref-69)
70. multicast [↑](#footnote-ref-70)
71. race attacks [↑](#footnote-ref-71)