تاریخ دریافت مقاله: ۹۶/۰۹/۲۳
تاریخ پذیرش مقاله: ۹۷/۰۲/۱۷

بررسی معماری امنیتی اینترنت اشیاء: چالش‌ها و راهکارها

بهاره پهلوان‌زاده*
استادیار گروه پژوهشی طراحی و عملیات سیستم‌ها، مرکز منطقه‌ای اطلاع‌رسانی علوم و فناوری، شیراز، ایران
پست الکترونیکی: pahlevanzadeh@ricest.ac.ir

سارا کلینی
کارشناس ارشد هوش ماشین و رباتیک، مرکز منطقه‌ای اطلاع‌رسانی علوم و فناوری، شیراز، ایران
پست الکترونیکی: koleini@ricest.ac.ir

چکیده

هدف از ایجاد و گسترش فناوری اینترنت اشیاء (IoT)، توانمندسازی اشـیاء برای اتصال به شیء دیگر بدون در نظر گرفتن زمان و مکان اسـت. برای پیاده‌سـازی چنین هدفی چالش‌های فراوان بسـیاری وجـود دارد که یکی از مهم‌ترین این چالش‌ها، چالش‌های امنیتی است. جهت اعمال سیاسـت‌های امنیتی ابتدا لازم اسـت که ساختار سیستم IoT به‌صورت دقیق شـناخته شود. در این مقاله، معماری اینترنت اشیاء با تکیه بر الزامات امنیتی بر اساس چارچوب چهار لایه‌ای پیشنهادی مبنی بر لایه ادراکی، لایه شبکه، لایه حمایتی و لایه برنامه کاربردی شرح داده می‌شود. در این بررسـی، تهدیدات و آسیب‌پذیری‌های متداول در معماری IoT مطابـق با معماری امن چهار لایه و در قالب چارچوب جامع پیشـنهادی مورد بحث قرار گرفته اسـت. همچنین مروری بر پروتکل‌های امنیتی مورد اسـتفاده در لایه‌های مختلف معماری امنیتی IoT انجام شـده و مقایسـه‌ای بر الگوریتم‌هـای رمزنگاری سـبک وزن نوینی که به منظور حفاظت اطلاعـات در تمام چهار لایه معمـاری IoT مورد استفاده قرار گرفته، ارائه شده است.

واژه‌هـای کلیدی: اینترنت اشیاء (IoT)، امنیت، معماری امـن اینترنـت اشـیاء، پروتکل‌هـای امنیتـی ارتباطاتی، الگوریتم‌های رمزنگاری سبک وزن

۱- مقدمه

در زمان ظهور هر فناوری، آنچه ابتدا مورد توجه قرار می‌گیرد تئوری اولیه و شـیوه کارکرد آن اسـت. پس از کاربردی شدن فناوری جدید، به تدریج معایب و نکات منفی آن نظیر مسائل امنیتی، مسائل اجتماعی و... مطرح می‌گردد. هم اینک با گسـترش اینترنت و تجهیزات هوشمند، چالش امنیتی اینترنت اشیاء (IoT) نیز مطرح می‌باشد. در سال‌های اخیر، تعداد دستگاه‌های (اشیاء) متصل به اینترنت بیش از تعداد افراد بوده و انتظار می‌رود که در سـال ۲۰۲۰ بیش از ۵۰ میلیارد شیء به اینترنت متصل گشته و تخمین زده می‌شود که به ازای هر نفر، هفت دستگاه متصل به اینترنت وجود خواهد داشت[۱]. یکی از موضوعات چالش برانگیز در چنین محیطی که محدودیتی در اتصال اشیاء به اینترنت وجود نـدارد، توجه به جنبه‌های امنیتی اسـت. تهدیدهای امنیتی شبکه با وسعت دسترسی اینترنت افزایش می‌یابد. از آنجا که هر شـیء یا دستگاه در IoT دارای قابلیت‌های

* نویسندهٔ مسئول

شبکه‌ای است (اتصال اشیاء به اینترنت و برقراری ارتباط با یکدیگر)، از این‌رو لازم است تا ملاحظات امنیتی ویژه‌ای برای اینترنت اشـیاء در نظر گرفت. گرچه سـازوکارهای سـنتی امنیتی نظیر بارو[1]، سیسـتم‌های تشخیص حملات و جلوگیـری از نفـوذ (IPS[2] و IDS[3]) در لبه اینترنت اعمال می‌شود و از این سـازوکارها به منظور حفاظت شبکه از حملات خارجی استفاده می‌گردد، اما این سازوکارها برای حفظ امنیت نسـل بعدی اینترنت کافی نمی‌باشد. معماری بدون مرز IoT، ملاحظات بیشـتری را در کنترل دسترسی به شـبکه، احراز هویت، محرمانگی و صحت نرم‌افزارهای کاربـردی طلب می‌نماید. جهت حصـول اطمینان از امنیت داده‌ها و خدمات ارائه شده در محیط IoT، خصوصیت‌هایی نظیر محرمانگی، صحت و جامعیت، احراز هویت، توجه به اختیارات قانونی، کنترل دسترسـی، در دسـترس بودن و حفظ حریم خصوصی، باید تضمین شـود[۲] . IoT دارای خصوصیـات و محدودیت‌های منحصر به فردی در زمان ساخت سازوکارهای دفاعی علیه تهدیدات امنیتی سایبری اسـت که می‌توان این چالش‌ها را به‌صورت زیر خلاصه کرد[۳]:

فناوری‌های چندگانه

IoT در برگیرنـده چنـد فناوری نظیر شناسـه امواج رادیویی RFID[4] و شبکه‌های حسگر بی‌سیم WSN[5]، محاسبات ابری و مجازی‌سازی اسـت که هرکدام آسیب‌پذیری‌های خاص خود را دارند و جهـت امنیت IoT باید تمام زنجیرهٔ این فناوری را امن نمود.

کاربردهای چندگانه

فناوری IoT کاربردهای متنوعی در حوزه‌های سلامت، صنعت، ساختمان‌های هوشمند و شهرهای هوشمند داشته و هر یک از ایـن کاربردها، نیازهای امنیتی خاص خود را دارند.

مقیاس‌پذیری

با اتصال میلیاردها شـیء به اینترنت، مقیاس‌پذیری از نکات بسیار مهم در زمان ایجاد سازوکارهای موثر دفاعی مطرح می‌شود.

داده‌های کلان

نه تنها تعداد اشیاء هوشمند زیاد است، بلکه داده‌هایی که به‌وسیله هر شیء نیز تولید می‌شود بسیار حجیم است. هر شـیء به‌وسیلهٔ تعداد زیادی حسگر حمایت شده و هر حسـگر تولید کننده داده‌های بسیار زیادی در طول زمان است. بنابراین لازم است تا سازوکار دفاعی موثری جهت امنیت داده‌های کلان پیاده‌سازی گردد.

دسترس‌پذیری[6]

دسـترس‌پذیری اشاره به پیوسـتگی عملیاتی سیستم در بـازه زمانـی طولانـی دارد. امنیت نقش عمـده‌ای در دسترس‌پذیری بالا را ایفا می‌نماید.

محدودیت منابع

اکثـر دسـتگاه‌های IoT دارای محدودیت منابع نظیر پردازنـده، حافظه و محدوده ارسـال داده‌ها هسـتند. این مسئله باعث راحتی حمله محروم‌سازی از سرویس(DoS[7]) بـا اسـتفاده از محدودیت‌های منابع می‌شـود. مهاجم به راحتی می‌تواند قابلیت‌های منابع محدود را دراختیار گرفته و از ایـن طریق باعث اختلال در ارائه خدمات گردد. علاوه بـر آن، این محدودیت‌هـا در زمان اجـرای الگوریتم‌های رمزنگاری باعث چالش جدیدی می‌شوند.

دسترسی از راه دور

معمولا بسـیاری از حسگرهای IoT در مکان‌های امن که دسترسی به آن‌ها چندان راحت نیست نصب می‌شوند. حمله‌کننـده می‌تواند به راحتی و بدون دیده شـدن به این تجهیزات نفوذ یابد. بنابراین سیستم‌های پایش امنیتی باید در محل‌های امن نصب شـده و در شـرایط بسیار سخت

1- Firewall
2- Intrusion Prevention Systems
3- Intrusion Detecttion Systems
4- Radio-frequency IDentification
5- Wireless sensor networks
6- Availability
7- Denial of Service

عمـــل نمایند. راه حل دیگر، جابجایـــی فیزیکی دوره‌ای این تجهیزات است.

پویایی

انتظار می‌رود اشـــیاء هوشـــمند در IoT مکان خود را به‌صورت پویا تغییر دهند. این امر مشکلات اضافی را در هنگام ایجاد سازوکارهای دفاعی کارآمد به‌وجود می‌آورد.

خدمات حساس به تأخیر

انتظار می‌رود که اکثر برنامه‌های کاربردی IoT حساس به تاخیر باشـــند و بنابراین بایـــد از اجزای مختلف IoT در مقابل حملاتی که ممکن است زمان سرویس آن‌ها را کاهش داده و یا باعث اختلال سرویس شود، محافظت نمود.

ادامه مقاله به شرح زیر سازماندهی و ارائه شده است: در بخش دوم مقایسه امنیت در شبکه‌های متداول بی‌سیم و IoT ارائه شده است. در بخش سوم ضمن بررسی معماری اینترنت اشـــیاء در قالب یک چارچوب چهـــار لایه‌ای (لایه ادراکی، لایه شـــبکه، لایه حمایتی و لایه برنامه کاربردی)، ســـایر حملات رایج و ملاحظات امنیتی در هر لایه شـــرح داده می‌شود. رایج‌ترین پروتکل‌های امنیتی مورد استفاده در فنـــاوری IoT در بخـــش چهارم بیان شـــده و در بخش پنجم ســـازوکارهای رمزگذاری موجود در IoT شرح داده شده است. در نهایت چشم‌اندازها، چالش‌ها و موضوعات تحقیقاتـــی آینده در حوزه امنیتی IoT مورد بررســـی قرار گرفته است.

۲- مقایسه امنیت در شبکه‌های متداول بی‌سیم و IoT

تفاوت‌های اساسی بین IoT و شبکه‌های بی‌سیم معمولی در رابطه با نحوه برخورد با مسئله امنیت و حریم خصوصی وجـــود دارد. برای مثال، اســـتقرار و نحـــوه کارکرد IoT در مقایسه با اینترنت معمولی بسیار متمایز است. شبکه‌های IoT بر بستر شبکه‌های کم قدرت و نقصان پذیر[8] مستقر می‌شوند. شبکه‌های LLN شـــبکه‌هایی هســـتند که دارای محدودیت منابعی همچون انرژی، حافظه و پردازش می‌باشند. در حالی که سایر شـــبکه‌ها دارای همبندی بسیار پویایی بوده که بر روی برنامه‌های کاربردی تکیه می‌کنند [٤]. در شبکه‌های LLN امکان از دســـت دادن داده‌ها بـــه علت جعل هویت گره وجود دارد. به‌عنوان مثال، در فرایند انتقال داده‌ها، اگر مهاجم بتواند با اســـتفاده از هر هویتی به شـــبکه متصل شود، در آن‌صورت فرض می‌شود که مهاجم می‌تواند یک گره معتبر در شبکه باشـــد. لذا از طریق برنامه‌های کاربردی هوشمند، خوانشگرها می‌توانند توســـط یک مهاجم دستکاری شده و پیام‌های کنترل نادرستی را ارسال نمایند [٤].

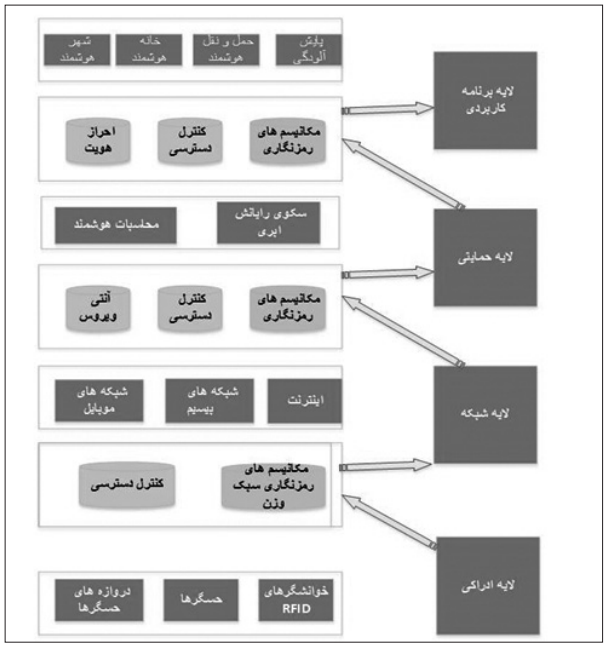
ویژگی‌های امنیتی و ملزومات آن در تجهیزات موجود در هر دو شبکه IoT و شبکه‌های متداول نیز متفاوت هستند .[٥] در لایـــه ادراکی IoT، گره‌های حســـگرها دارای قدرت محاســـباتی محدود و ظرفیت ذخیره‌سازی کمی هستند که این امر باعث می‌شـــود تا برنامه‌های ارتباطاتی با فرکانس بالا و رمزنگاری کلید عمومی برای ایمن‌ســـازی تجهیزات IoT غیرممکن باشد.

علاوه بـــر این، پروتکل‌های ارتباطی در هر دو شـــبکه متفاوت بوده و هر لایه دارای پروتکل ارتباطی خاص خود می‌باشد. به‌عنوان مثال، نسخه جدید پروتکل IP یعنی IPv6[9] در لایه ادراکی IoT از طریق شـــبکه‌های بی‌سیم شخصی اســـتفاده می‌شـــود، در حالی که وای‌فای[10] در لایه فیزیکی شـــبکه‌های متداول به‌کار برده می‌شود. در لایه شبکه ،IoT DTLS[11] به‌عنوان یک پروتکل ارتباطی مورد اســـتفاده قرار می‌گیـــرد، در حالی‌که در شـــبکه متـــداول از پروتکل TCP استفاده می‌شود.

در لایـــه کاربـــردی IoT از پروتـــکل CoAP[12] به‌عنوان جایگزیـــن پروتکل HTTP[13] موجود در شـــبکه‌های متداول اســـتفاده شده اســـت. [٦] به‌طور خلاصه می‌توان گفت که معماری امنیتی در شـــبکه‌های متداول بر اســـاس دیدگاه کاربران طراحی شـــده و قابلیت اجرا برای ایجاد ارتباطات

8- Low-power and Lossy Networks: LLN

9- Internet Protocol Version 6
10- Wifi
11- Datagram Transport Layer Security
12- Constrained Application Protocol
13- Hypertext Transport Protocol



شکل ۱: چارچوب ۴ لایه‌ای معماری IoT بر اساس ملاحظات امنیتی

میان ماشـــین‌ها را ندارد. مباحث امنیتی در هر دو شـــبکه ممکن اســـت مشابه باشـــند، اما از رهیافت‌ها و تکنیک‌های متفاوتی در رفع مشکلات امنیتی هر شبکه استفاده می‌شود [۷].

۳- معماری امنیتی IoT

در IoT، فناوری حسگرها، فناوری شبکه‌های کامپیوتری و فناوری کنترل هوشمند با یکدیگر ترکیب شده تا ارتباط میان اشـــیاء محقق گردد. در این مقالـــه جهت پرداختن به جزئیـــات امنیتی، معماری امن IoT را مطابق شـــکل (۱) به ٤ لایه اصلی یعنی لایه ادراکی، لایه شـــبکه، لایه حمایتی و لایه برنامه‌های کاربردی تفکیک می‌نماییم. در ادامه هر یک از لایه‌ها به همراه حملات رایج و ملاحظات امنیتی هر لایه شرح داده می‌شود:

۳-۱- لایه ادراکی[14]

این لایه به دو بخش تقسیم می‌شود: گره یا کانال‌های ادراکی (شامل حســـگرها، کنترل‌کننده‌ها و غیره) و شبکه ادراکی که به لایه شبکه متصل می‌شود[۸] . در لایه ادراکی انواع مختلفی از اطلاعات از طریق گره‌های ادراکی یا همان

14- Perception Layer

جدول ۱: مقایسه کانال های ادراکی IoT بر اساس امنیت[۹]

نوع امنیت	RFID	حسگرها	دروازه‌های حسگرها
رمزنگاری	ضعیف	متوسط	-
احراز هویت	متوسط	قوی	قوی
مجوز دسترسی	متوسط	قوی	قوی
حریم خصوصی	متوسط	متوسط	ضعیف

دســـتگاه‌های فیزیکی جمع‌آوری می‌شود. انواع مختلفی از گره‌های ادراکی یا حســـگرها از جمله خوانشگرهای RFID، GPS[15]ها، دســـتگاه‌های اندازه‌گیری هوشـــمند، و وســـایل الکترونیکی خانگی هوشـــمند به جمع‌آوری داده‌ها شـــامل خصوصیات اشـــیاء، داده‌های مربوط به شـــرایط محیطی و کنتـــرل آن‌ها در قالـــب داده‌های هوشـــمند جهت تبدیل به دســـتورالعمل‌هایی برای ارســـال به لایه شبکه ادراکی می‌پردازند.

به‌عبارت دیگر وظیفه اصلی این لایه جمع‌آوری داده‌ها و تبدیل داده‌های دنیای فیزیکی به‌صورت داده‌های دیجیتالی است. داده‌های جمع‌آوری شده معمولا از طریق شبکه‌های بی‌ســـیم به مراکز داده منتقل می‌شـــود. در صورتی که از معیارهای امنیتی موثری اســـتفاده نشـــود، این داده‌ها به راحتی پایش، کپی برداری و در نهایت مخدوش می‌گردند. بـــه دلیل ماهیت تجهیـــزات موجود در این لایـــه که دارای ظرفیت حافظه و توان الکتریکی کمی هســـتند بایســـتی از الگوریتم‌های رمزنگاری سبک در تجهیزات IoT (رجوع به بخش پنجم مقاله) استفاده نمود. همچنین باید به حملاتی که از خارج از شبکه صورت می‌پذیرد توجه کرده و داده‌های حسگرها را به منظور حفظ صحت و جامعیت، محرمانگی، احراز هویت و دسترس‌پذیری حفاظت نمود.

جدول (۱) کانال‌های ادراکی IoT را از دیدگاه امنیتی با تمرکز بر رایج‌ترین فناوری‌های استفاده شده در IoT مانند RFID، حسگرها و دروازه‌های حسگرها مقایسه می کند[۹].

۳-۱-۱ حملات رایج در لایه ادراکی

همان‌طور که در شـــکل (۱) نشان داده شده است، لایه ادراکی از خوانشـــگرهای RFID، حســـگرها و دروازه‌های

15- Global Positioning System

جدول ۲: برخی از حملات رایج در لایه ادراکی [۱۰-۱۵]

حملات رایج در لایه ادراکی		
Accessibility	Jamming	Secure localization
Collisions	Man in the Middle(MITM)	Selforganization
Counterfeiting	Misconfiguration	Signal Lost
Data Newness	Modification	Spoofing
Eavesdropping	Node Failure	Survivability
Exhaustion	Node Outage	Sybil
Fabrication	Node Subversion	Tampering
False Node Message Corruption	Passive Information Gathering	Timing management
Hacking	Protocol Tunneling	Tractability
Interruption	Repudiation	Unfairness
Interception	Robustnes	War Dialing

حسگرها تشکیل شده است که ممکن است تحت تاثیر حملات زیادی همچون موارد ذکر شده در زیر و نیز در جدول (۲) قرار گیرد: [۱۰-۱۵]

• محروم‌سازی از سرویس: حملات DOS از معمول‌ترین حملات در اینترنت بوده و باعث می‌گردد که منابع شبکه و سرویس‌های آن از طریق درخواست‌های مداوم مهاجمان غیرقابل دسترس باشند.

• حملات زمان بندی[16]: به وسیله تحلیل زمان مورد نیاز جهت اجرای الگوریتم رمزنگاری به منظور به‌دست آوردن اطلاعات کلیدی انجام می‌شود.

• تسخیر گره[17]: در این حملات گره‌های مهم و کلیدی نظیر دروازه‌ها توسط مهاجمان کنترل می‌شوند. پیامد آن افشاکردن تمام اطلاعات از جمله کلیدهای تطابق داده‌ها و کلیدهای ارتباطاتی گروه[18] بوده و متعاقب آن تهدید برای امنیت تمام شبکه وجود خواهد داشت.

• گره جعلی[19]: حمله‌کننده گره جعلی را درسیستم اضافه می‌کند و به ورود اطلاعات جعلی در شبکه پرداخته و از انتشار داده حقیقی جلوگیری می‌نماید.

• همانندسازی اشیاء[20]: در طول فرایند تولید یک شیء، یک سازنده نامناسب می‌تواند به راحتی ویژگی‌های فیزیکی، سیستم عامل/ نرم‌افزار یا پیکربندی امنیتی این محصول را به اشتراک بگذارد.

• جایگزینی مخرب اشیاء[21]: در هنگام نصب یک شیء، ممکن است یک شیء با نوع مشابه خود با کیفیت پایین‌تر که دارای مشکلات امنیتی است، بدون تشخیص جایگزین شود.

• استخراج پارامترهای امنیتی[22]: اشیایی که در محیط‌های خارج از سازمان (مانند حسگرها، محرک‌ها و غیره) مستقر شده‌اند معمولا از لحاظ فیزیکی به درستی محافظت نشده و به راحتی می‌توانند توسط مهاجم تسخیر شوند. ممکن است مهاجم از این اشیاء برای استخراج اطلاعات امنیتی آن مانند کلید (مثلا کلید دستگاه، کلید خصوصی، کلید گروه) استفاده کرده و یا مجددا آن را جهت رسیدن به اهدافش برنامه‌ریزی کند.

• تهدیدات حریم خصوصی[23]: تهدیدات امنیتی حریم خصوصی کاربران ممکن است شامل ردیابی مکانی اشیاء باشد. مهاجم می‌تواند اطلاعات را براساس داده‌های جمع‌آوری شده، استخراج کند و از این طریق الگوهای رفتاری کاربر مورد نظر را به‌دست آورد.

۳-۱-۲ راهکارها و ملاحظات امنیتی در لایه ادراکی

حفاظت از دستگاه‌های نقطه پایانی در لایه ادراکی از

16- Timing attack
17- Node capture
18- Group communication key
19- Fake node
20- Cloning of things
21- Malicious substitutions of things
22- Security parameters extraction
23- Privacy Threat

اهمیت زیادی برخوردار بوده و باید با اســتفاده از وسایل مختلف به ایمن‌سازی این تجهیزات مبادرت ورزید. بهترین شیوه این کار، انجام موارد زیر است:

• غیرفعال نمودن اتصال تجهیزات خارجی مانند گرداننده‌های USB[۲۴] و اجازه استفاده از آن‌ها پس از تایید فنی

• از کارانداختن دسترســی مستقیم دستگاه‌های با اهمیت ویژه به اینترنت

• حصول اطمینان از غیر فعال بودن ســرویس‌های بدون اســتفاده یا مســدود کردن آن‌ها نظیر درگاه‌هــای باز و پروتکل‌های غیر امن

• کنترل دسترسی و احراز هویت دستگاه در زمان اتصال

• روزآمد نمودن سیستم عامل تجهیزات

• جلوگیری از دسترسی گره‌های نامربوط

• حفاظت از محرمانگی انتقال اطلاعات میان گره‌ها

• تبادل کلید امنیتی

• رمزنگاری داده‌ها با استفاده از الگوریتم‌ها و پروتکل‌های رمزنگاری بســیار ســبک وزن (در قســمت۵ همین مقاله توضیح داده شده است.)

۳-۲- لایه شبکه

لایه شــبکه مســئولیت انتقال اطلاعات از لایه ادراکی، پــردازش اولیه اطلاعات و دســته‌بندی را بــه عهده دارد. این قسمت موجب تســهیل در اتصال و انتقال اطلاعات از دستگاه‌ها و دروازه‌ها می‌شود. انتقال اطلاعات در این لایه بر اساس چند شبکه اصلی یعنی اینترنت، شبکه‌های ارتباطی موبایل، شبکه‌های ماهواره‌ای، شبکه‌های حسگر بی‌سیم[۲۵]، شبکه‌های توری بی‌سیم[۲۶] و سیستم‌های سرپرستی اخذ و کنترل داده[۲۷] اســتوار است. باید به ویژگی‌های زیرساخت شــبکه و پروتکل‌های ارتباطی جهت تبــادل اطلاعات بین دســتگاه‌ها نیز توجه نمود. هم اینک امنیت طراحی شــده در معماری اینترنت بر اســاس رفتار افراد طراحی شده و نمی‌توان لزوما آن را به ســازوکار امنیتی بین ماشین‌های موجــود در IoT تعمیــم داد. ارتباط دســتگاه‌ها با یکدیگر می‌تواند از طریق شــبکه‌هایی که دارای زیرســاخت‌های متفاوتی هستند صورت پذیرد.

به دلیل وجود تعداد بسیار زیادی از دستگاه‌ها در IoT، چنانچه از روش‌های معمول احراز هویت جهت شناسایی این دســتگاه‌ها استفاده شــود، در عمل باعث وجود حجم زیادی از داده‌ها و ایجاد ترافیک ســنگین در شــبکه شده، بنابرایــن، جهت شناســایی تعداد بســیار زیــاد گره‌ها از فناوری IP موجود استفاده نمی‌گردد. با استفاده از فناوری بازیابی اطلاعات و مهندسی اجتماعی، نفوذگرها به سادگی قادر می‌باشند تا حجم زیادی از اطلاعات خصوصی افراد را جمع‌آوری نمایند. با ایجاد نسل بعدی شبکه‌ها[۲۸] استفاده از IPv6 در شبکه‌ها فراگیر می‌شود و سازوکارهای امنیتی شبکه بر اســاس IPv6 مد نظر قرار می‌گیرد[۱۶] که امنیت بیشتری نسبت به IPv4 را ارائه می‌دهند.

۳-۲-۱ انواع حملات موجود در لایه شبکه

گســتردگی IoT باعث می‌شود که به مسائل امنیتی در خصوص احراز هویت روبرو شــویم. در این لایه باید به محرمانگــی، صحــت و جامعیت داده‌ها نیــز توجه خاص شــود و علاوه بر آن حمــلات DDOS را باید مد نظر قرار داده و راه‌حل‌هــای امنیتی در خصــوص مواجهه با آن را پیاده‌سازی نمود.

گرچه هسته شبکه از قابلیت حفاظت ایمنی نسبی برخوردار اســت اما نباید دسترسی غیر معتبر به شبکه، استراق سمع اطلاعات، آسیب به صحت و جامعیت و محرمانگی، حملات مرد میانی[۲۹]، حملات جعلی، ســرقت اینترنتی، رخنه، سرقت هویت، هرزنامه‌ها و ویروس‌ها را نادیده گرفت[۱۷].

در شبکه‌های سیار حملاتی نظیر ردیابی، محروم‌سازی از سرویس، bluesnarfing, bluejacking, bluebugging , alteration, corruption, deletion [۱۸] وجود دارد.

در ادامه به شرح دو حمله اصلی مسیریابی[۳۰] و بازپخش[۳۱]

24- Universal Serial Bus
25- WSN: Wireless Sensor Network
26- Wireless Mesh Network: WMN
27- Supervisory Control and Data Acquisition: SCADA
28- Next Generation Network: NGN
29- Man in the Middle
30- Routing attack
31- Replay attack

در این لایه می پردازیم:

حمـــلات مســـیریابی: از طریق جعل یا ارســـال مجدد اطلاعات مســـیریابی، ممکن اســـت حمله‌کننـــده حلقه‌های مسیریابی را ایجاد نموده و باعث مقاومت در انتقال داده‌ها، افزایش یا کاهش طول مسیر، ایجاد پیام‌های خطا، افزایش تاخیر در شـــبکه، و جذب یا دفع ترافیک شبکه گردد. سایر حملات مربوط به مسیریابی عبارتند از[۱۰]:

• حمله ســـیاه چاله[۳۲]: در این حمله مهاجم اعلام می‌کند که دارای مســـیری با کیفیت بالا است، به این ترتیب او را قادر می‌سازد تا هر بسته‌ای را از مسیر جعلی عبور دهد.

• حمـــل و نقـــل انتخابـــی[۳۳]، جایی که مهاجم ممکن اســـت بســـته‌های ارســـالی را انتخاب کند یا به سادگی یک بسته را رها کند

• حمله کرم چاله[۳۴]، جایی که یک مهاجم ممکن است بسته‌ها را در یک مکان در شـــبکه ثبت کـــرده و آن‌ها را در مکان دیگری تونل کند و ســـپس آن‌ها را به شبکه انتقال دهد. در نتیجه بر رفتار شبکه و در حد زیادی بر عملکرد مسیریابی اثر می‌گذارد[۱۹].

• حمله سی‌بل[۳۵]، به این ترتیب مهاجم هویت چندگانه را به سایر اشیاء در شبکه ارائه می‌دهد.

• حملات بازپخش: حمله‌کننده مبادرت به ارســـال بسته‌ای که قبلا توســـط مقصد دریافت شـــده، می‌پردازد تا اعتماد سیســـتم را به‌دســـت آورد. این حمله در احـــراز هویت و تخریب صحت گواهینامه‌ها به‌کار برده می‌شود.

۳-۲-۲ راهکارها و ملاحظات امنیتی در لایه شبکه

نکات و راهکارهای امنیتی شـــاخص در لایه شبکه در سه دستهٔ شبکه‌های فیزیکی، اتصال از راه دور، شبکه‌های بی‌سیم قابل تمرکز و بحث می‌باشد که به اختصار در زیر به آن پرداخته شده است:

راهکارهای امنیتی شاخص در شبکه‌های فیزیکی

اعمال امنیت فیزیکی در شـــبکه، برای مثال استفاده از دوربین‌های مدار بسته، کارت‌های ورودی جهت ثبت ورود افراد، ایجاد مناطق امن جهت جلوگیری از دسترســـی‌های غیر معتبر

استفاده از سازوکارهای امنیتی نظیر بارو، IPS/IDS و فهرست کنترل دسترسی[۳۶] در شبکه

راهکارهای امنیتی شاخص در اتصال از راه دور و سیار

• اعمال ســـازوکارهای قوی (نظیر تأیید هویت چندگانه[۳۷]) جهت احراز هویت کاربران مجاز به منظور دسترســـی به شبکه از راه دور

• استفاده از کانال‌های ارتباطاتی امن

نظیر VPN-S2S[۳۸] جهت دسترســـی کارکنان به شـــبکه سازمان

راهکارهای امنیتی شاخص در شبکه‌های بی‌سیم

• اســـتفاده از تنظیمات مطمئن دســـتگاه‌ها و دروازه‌ها در زمان دسترسی از طریق بی‌سیم

• اســـتفاده از الگوریتم‌های رمزنگاری (رجوع به قسمت ۵ مقاله) و احراز هویت

۳-۳- لایه حمایتی

لایه حمایتی، ســـکوی حمایتی قابل اعتمـــادی را برای لایـــه برنامه کاربـــردی فراهم می‌ســـازد. در ایـــن لایه از طریق شـــبکه‌های توری[۳۹] و رایانش ابری انواع مختلفی از محاسبات هوشمند سازماندهی می‌شود. پردازش داده‌های حجیم و تصمیم‌گیری هوشـــمند در خصوص رفتار شبکه در این لایه صورت گرفته و چالش بهبود توانایی تشخیص اطلاعات مخرب از داده‌های سالم همواره وجود دارد. این لایه بـــه معماری امنیتی قوی و بهره‌گیری از الگوریتم‌ها و پروتکل‌های رمزنگاری قوی نیاز دارد.

۳-۳-۱ حملات رایج در لایه حمایتی

تهدیدات امنیتی و آســـیب‌پذیری‌های بســـیاری در این لایه وجود دارد، از جمله مدیریت هویت، تغییرات دینامیکی

32- blackhole یا Sinkhole
33- Selective transformation
34- Wormwhole
35- Sybil

36- ACL Access Control List:
37- Multi Factor Authentication: MFA
38- VPN Site to Site
39- Grid

در دســتگاه‌های IoT (ناهمگونی) که سبب عدم دسترسی داده‌های ارسال شــده به یک گره معتبر می‌شود. از دیگر تهدیــدات این لایه کنترل دسترســی بــه داده‌ها، پیچیدگی سیســتم، امنیت فیزیکی، رمزنگاری، امنیت زیرســاختی، هویت کاربر، رویکرد مدیریتی به امنیت و تنظیمات اشتباه نرم‌افزارهــا [۲۰] تهدیدات حریم خصوصی را می‌توان نام برد.

۳-۳-۲ راهکارها و ملاحظات امنیتی در لایه حمایتی

ملاحظــات و راهکارهای امنیتی مهمــی که در این لایه می‌توان به‌کار گرفت به شرح زیر می‌باشد:

• اعمــال راهکارهای ایمنی در ماشــین‌های مجازی نظیر روزآمدسازی سیستم عامل، نحوه دسترسی به ماشین‌های مجازی[۴۰] و به‌کارگیری از ســازوکارهای کنترلی قوی در برنامه‌های کاربردی

• ایمن‌سازی داده‌های موجود در ابر با استفاده از فناوری مناسب و الگوریتم‌های رمزنگاری تایید شده

• طراحــی راه‌حل‌هــای بازیابی در زمان بحــران و تداوم ســرویس‌دهی با تهیه تصویــر لحظه‌ای از ماشــین‌های مجازی، پشتیبان‌گیری و وجود ماشین‌های مجازی آماده به کار در وبگاه تامین کننده‌های ابری

• حفاظــت از وب از طریــق شناســایی و جلوگیــری از ترافیک‌هــای مخرب توســط باروها مبتنی بــر میزبان و استفاده از IPS/IDS

• پایــش ثبت وقایــع[۴۱] خصوصا برای کاربــران مجاز و مدیریــت مجتمع ثبت وقایــع از چند منبع بــا راه‌حل‌های SIEM[۴۲] به منظور تجزیه و تحلیل حوادث امنیتی

۳-٤- لایه برنامه کاربردی

لایه برنامه کاربردی، نهایی ترین لایه محسوب می‌شود و می‌تواند به روش‌های مختلف بر اساس خدماتی که ارائه می‌دهد، ساخته شود.

در این لایه کاربران نهایی اجازه اســتفاده از اطلاعات را از طریــق تجهیزات هوشــمند دارند. هــدف ایجاد IoT نیــز اســتفاده از برنامه‌های کاربردی در جهت هوشــمند شــدن ســبک زندگی و کاهش حجم کار است. در این لایه ســرویس‌های شخصی سازی شده متناسب با نیاز کاربر فراهم می‌شود. برنامه‌های کاربردی مانند شبکه هوشمند، شهر هوشمند، سیســتم مراقبت‌های بهداشتی هوشمند و پروتکل‌های حمل و نقل هوشمند، در این لایه وجود دارند. [۲۱] یک پروتکل لایه کاربردی بر روی چند سیستم نهایی توزیع شده اســت که در آن برنامه در یک سیستم پایانی از یــک پروتکل برای تبادل بســته‌های اطلاعاتی با برنامه موجود در سیستم دیگری استفاده می‌کند [۲۲,۲۳] . علاوه بــر پروتکل CoAP[۴۳] پروتکل‌هــای دیگری نیز در این لایه وجود دارد که در جدول (۳) به آن‌ها اشاره شده است[۲٤-۲٦].

جــدول (۳) نشــان می‌دهدکه پروتــکل CoAP بر روی UDP[٤٤] اجــرا می‌گردد و از ایــن رو، در زمره پروتکل‌های ســبک وزن قرار گرفته و برای برنامه‌های کاربردی که به پهنای باند پایین نیاز دارند، توصیه می‌شود. CoAP استفاده از پروتــکل DTLS را به‌عنوان پروتــکل ارتباطی امن مجاز می‌داند. [۲۵]. امنیت پروتکل‌هــای MQTT[٤٥] و AMQP[٤٦] با استفاده از پروتکل‌های TLS / SSL[٤٧] مدیریت می‌شود.[۲٦]

از طریق رابط[٤٨] این لایه، کاربر به IoT دسترسی دارد. راهکارهای امنیتی برای محیط‌هــای برنامه‌های کاربردی مختلف متفاوت اســت. در حال حاضر اســتاندارد جهانی جهت ساخت این لایه وجود ندارد.[۹] اما برخی از شرکت‌ها از راه حل‌هایی بر اســاس معماری 6LoWPAN[٤٩] استفاده می‌نمایند. به اشتراک‌گذاری داده‌ها یکی از ویژگی‌های این لایه اســت که مسائلی در خصوص حفظ حریم خصوصی داده‌ها، کنترل دسترســی و افشــای اطلاعات را به‌وجود می‌آورد[۲۷]. هر برنامه کاربردی، دارای کاربران بســیار

40- Virtual Machine: VM
41- Log Monitoring
42- Security Information and Event Management

43- COnstrained Application Protocol
44- User Datagram Protocol
45- Message Queue Telemetry Transport
46- Advanced Message Queuing Protocol
47- Transport Layer Security/Secure Sockets Layer
48- Interface
49- Low-power Wireless Personal Area Networks

جدول ۳: مقایسه پروتکل‌های رایج در لایه برنامه کاربردی

پروتکل‌های رایج لایه برنامه کاربردی در IoT	ویژگی‌های پروتکل			
	پروتکل انتقال	معماری	پروتکل امن استفاده شده	حمایت از QoS
MQTT (Message Queue Telemetry Transport)	TCP	Publish/Subscribe	TLS/SSL	بلی
AMQP (Advanced Message Queuing Protocol)	TCP	Publish/Subscribe	TLS/SSL	بلی
CoAP (constrained application protocol)	UDP	Request/Response	DTLS	بلی
XMPP (Extensible Messaging and Presence Protocol)	TCP	Publish/Subscribe Request/Response	TLS/SSL	خیر
DDS (Data Distribution Service)	/TCP UDP	Publish/Subscribe	TLS/SSL	بلی
RESTFUL (Representational State Transfer)	HTTP	Request/Response	HTTPS	خیر
Web socket	TCP	Publish/Subscribe Client/Server	TLS/SSL	خیر
SMQTT (Secure MQTT)	TCP	Publish/Subscribe	اختصاصی	بلی

زیادی است. بنابراین جهت جلوگیری از دسترسی کاربران غیر مجاز باید از سازوکارهای احراز هویت مختص هر برنامه استفاده کرد. همچنین باید توجه داشت که سازوکارهای حفاظت از داده‌ها و الگوریتم‌های پردازش داده‌ها بدون عیب و نقص نبوده و ممکن است باعث از دست دادن داده‌ها و حتی آسیب های فاجعه باری گردد.

جهت رفع مشکل امنیت در این لایه دو جنبه در نظر گرفته می‌شود: یکی شرایط احراز هویت و توافق کلیدی در سراسر شبکه ناهمگن ودیگری حفاظت از حریم خصوصی کاربران است. علاوه براین، آموزش و مدیریت امنیت اطلاعات به ویژه مدیریت رمز عبور بسیار مهم می‌باشد[۲۸].

۳-۴-۱ حملات رایج در لایه برنامه کاربردی

در این قسمت به ذکر چند حمله متداول در این لایه پرداخته می‌شود:

• حمله جایگزینی میان‌افزار[۵۰]: هنگامی که یک شیء در حال اجرا بوده و یا در مرحله تعمیر و نگهداری است، سیستم عامل، نرم‌افزار و میان‌افزار آن ممکن است جهت بهره‌برداری از قابلیت‌های جدید ارتقاء یابد. مهاجم ممکن است بتواند از طریق این ارتقاء با استفاده از جایگزینی اشیاء مخرب، باعث اختلال در رفتار عملیاتی شیء گردد.

• تزریق SQL[۵۱]

• حملات XSS[۵۲]

50- Firmware
51- SQL injection
52- Cross-site scripting

• حملات سرریز میانگیر [۵۳]
• OWASP[۵۴]
• (CWE/SANS[۵۵])
• (SAFECode[۵۶])
• حمله جعل[۵۷]
• حمله بویش[۵۸]

۳-۴-۲ راهکارها و ملاحظات امنیتی در لایه برنامه کاربردی

جهت ایمن‌سازی برنامه‌های کاربردی، لازم است تا موارد زیر در نظر گرفته شود:

• ایجاد برنامه‌های کاربردی (وب، برنامه‌های کاربردی موبایل، برنامه‌های ابری، ...) با کدهای استاندارد ایمن جهت به حداقل رساندن حملات
• بررسی صحت داده‌های ورودی
• آزمون برنامه‌های کاربردی (پویا، ایستا و دوگانه) جهت تشخیص آسیب‌پذیری آن‌ها و اعمال اقدام صحیح جهت رفع آسیب(ها) و جلوگیری از افشای اطلاعات
• به کارگیری از امضا کد شده[۵۹]: جهت اطمینان مشتریان از صحت نرم‌افزار
• پایش فایل‌های بسیارمهم به منظور جلوگیری از هرگونه تغییرات غیرمجاز
• تایید هویت کاربران
• توجه به امنیت ذخیره‌سازی و بازیابی داده‌ها در هر مرحله از انتقال داده‌ها[۲۴]
• دارا بودن امضای دیجیتالی، امضای گواهی‌نامه و زنجیره گواهی‌نامه یک بسته بروزرسانی نرم‌افزار [۲۶]
• رمزنگاری تصاویر نرم‌افزار در هنگام انتقال در صورت پشتیبانی دستگاه از ارتقاء نرم‌افزار از راه دور
• غیرفعال کردن درگاه‌های نرم‌افزار که برای عملیات عادی لازم نیست
• استفاده از کلید رمزنگاری یگانه (متفاوت از سایر کلیدهای نرم‌افزار) جهت تایید نرم‌افزار نهایی.
• جداسازی مولفه‌های حساس نرم‌افزار مانند فرایندهای رمزنگاری از سایر اجزای نرم‌افزاری و یا امتیازدهی بیشتری به آن‌ها

53- Buffer overflow
54- Open Web Application Security Project
55- Common Weakness Enumeration
56- Software Auusrance Forum for Excellence in Code
57- Phishing attack
58- Sniffing attack
59- Code Signing

۴- پروتکل‌های امنیتی در IoT

پس از شرح لایه‌های مختلف معماری امن IoT، ضروری است تا در این قسمت پروتکل‌های رایج در این حوزه معرفی شوند. از پروتکل‌های مختلفی جهت ارتباط و انتقال داده‌ها در لایه‌های مختلف معماری امنیتی IoT استفاده می‌شود که به همراه مشخصات و راهکارهای امنیتی برای هر کدام به‌طور خلاصه در جدول (٤) شرح داده شده است. از آنجا که تبادل کلیدهای همه منظوره از راه‌حل‌های امنیتی در دامنه اینترنت مطرح می‌باشد، پروتکل‌های امنیتی /TCP IP به‌عنوان یکی از قسمت‌های مهم در طراحی راه‌حل‌های امنیتی مبتنی بر IP در IoT محسوب می‌گردد. بسیاری از پروتکل‌ها نظیر,DTLS HIP[۶۱], TLS/SSL ,IKEv2/IPsec60 و EAP[۶۲] راه‌حل‌هایی هستند که در 6LoWPAN به‌کار گرفته شده تا انتقال داده‌های امن‌تری را در محیط IoT به‌وجود آورند. علاوه براین، با استفاده از پروتکل‌هایی مانند IPSec، در دسترس بودن و غیر جعلی بودن برای جریان داده‌ها ایجاد می‌شود[١٦]. به منظور اعمال این الگوریتم‌ها، باید از پردازشگرهای خاصی نظیر پردازنده‌های سیگنال دیجیتال[۶۳] جهت تامین نیازمندی‌های فرایند محاسبات کلان استفاده نمود. اغلب این پردازنده‌ها یک رده الگوریتم رمزنگاری را حمایت می‌کنند. شرح پروتکل‌های امنیتی IP در IoT در جدول (٥) و ارتباط میان آن‌ها در لایه‌های مختلف در شکل (٢) نشان داده شده است.

پروتکل‌های IKEv2/IPsec و HIP در لایه شبکه در نظر گرفته می‌شوند تا انتقال داده امن را فراهم سازند. هر دو از تبادل کلید جهت تصدیق صحت داده‌ها استفاده می‌کنند.

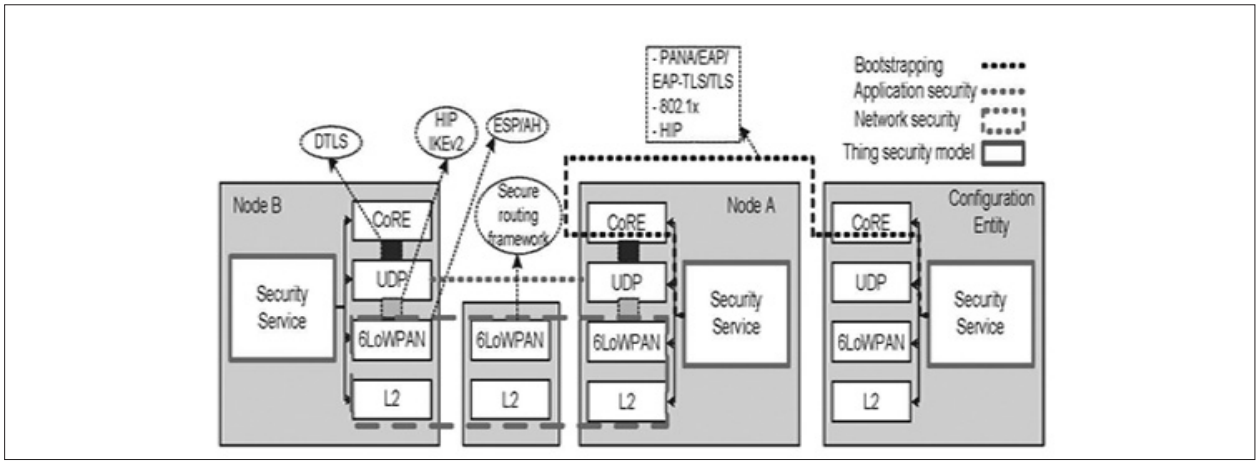
60- Internet Key Exchange / Internet Protocol Security
61- Host Identity Protocol
62- Extensible Authentication Protocol
63- Digital Signal Processing: DSP

جدول ۴: پروتکل‌های ارتباطاتی موجود در IoT [۱۶]

پروتکل‌های ارتباطاتی در IoT	مشخصات و راهکارهای امنیتی
Wi-Fi	اعمال الگوریتم‌های رمزنگاری Temporal Key Integrity Protocol (TKIP) Advanced Encryption Standard (AES) Wired Equivalent Privacy (WEP) استفاده از پروتکل‌های دسترسی حفاظت شده Wi-Fi Protected Access (WPA) Wi-Fi Protected Access II (WPA2) اعمال روش های Extensible Authentication Protocol EAP جهت احراز هویت در لایه دو شبکه
بلوتوث	اعمال امنیت به‌صورت جفتی در دستگاه‌ها غیرفعال نمودن بلوتوث در زمان عدم نیاز
Zigbee(802.15.4)	رمزنگاری لایه پیوند با ۱۲۸ بیت AES
6LoWPAN	ایجاد وضعیت امن با استفاده از رمزنگاری لایه پیوند ۸۰۲,۱۵,۴ دسترسی به لیست کنترل (Access Control List: ACL)
Weightless	ایجاد ارتباط رمزشده بین ایستگاه اصلی و دستگاه
GSM (Global System for Mobile Communications)	استفاده از الگوریتم احراز هویت (A3) جهت حفاظت از دسترسی های غیر مجاز استفاده از الگوریتم تولید کلید رمزدار (A8) که در SIM قرار گرفته است احراز هویت موقتی مشترک موبایل به منظور جلوگیری از نفوذ
3G	احراز هویت متقابل، تولید کلید یکپارچه و کلید رمزدار صحت و جامعیت داده‌ها احراز هویت کاربر

جدول ۵: پروتکل‌های امنیتی IP در IoT [۱۶,۲۹]

پروتکل‌های امنیتی IP در IoT	مشخصات و راهکارهای امنیتی
IKEv2/IPsec (Internet Key Exchange / Internet Protocol Security)	گواهینامه ۵۰۹.X جهت احراز هویت پروتکل تبادل کلید دیفی- هلمن جهت برقراری امنیت نشست‌ها تولید کلید رمزنگاری با استفاده از امنیت اشتراکی استقرار تونل امن
TLS/SSL (Transport Layer security / Secure Sockets Layer)	گواهینامه ۵۰۹.X جهت احراز هویت استفاده از کلیدهای غیر متقارن۵۰۹.X جهت تبادل کلیدهای متقارن استفاده از کلیدهای متقارن جهت رمزنگاری داده‌ها
DTLS (Datagram Transport Layer Security)	نمودار داده بر اساس TLS
HIP (Host Identified Protocol)	پروتکل شناسایی میزبان شناسایی میزبان بر اساس کلید عمومی به جای نشانی IP و DNS
EAP (Extensible Authentication Protocol)	پروتکل احراز هویت بسط پذیر حمایت یک چارچوب احراز هویت از چند شیوه احراز هویت کار در لایه پیوند استفاده از پروتکل‌های مختلف جهت انتقال پیام‌های EAP حمایت از سازوکارهای تحویل کلید
SSH (Secure Shell)	پروتکل رمزگذار شبکه استفاده از رمزنگاری کلید عمومی جهت احراز هویت متقابل ایجاد کانال امن جهت عبور داده‌ها



شکل ۲: ارتباط میان پروتکل‌های امنیتی IP در IoT [۲۹]

پروتکل TLS امنیت در TCP و نسخه مبتنی بر نمودار داده آن یعنی DTLS تامین کننده امنیت UDP جهت انتقال داده‌ها می‌باشد. کارکرد هر دو پروتکل به یکدیگر شباهت دارند. پروتکل EAP از چند روش جهت احراز هویت با شناسایی و انتقال مجدد داده‌ها استفاده می‌نماید اما در این روش قطعه کردن[۶۴] اندازه بسته‌ها مجاز نمی‌باشد. پروتکلی برای حمل احراز هویت برای دسترسی به شبکه[۶۵] (PANA) در لایه شبکه برای EAP نیز وجود دارد تا دسترسی به شبکه را برای کاربران آن ایجاد نماید. پروتکل PANA بر اساس UDP در بین EAPهای همگن و EAPهای تایید کننده اجرا می‌شود[۲۹].

۵- سازوکارهای رمزنگاری در IoT

به منظور حل مسئله حفاظت اطلاعات شخصی در IoT، به میان افزارهایی از قبیل سازوکارهای رمزنگاری و رمزگشایی جهت تثبیت مدل بهبود یافته IoT بر اساس زیرساخت اولیه آن نیاز می‌باشد. همان‌طور که در شکل (۱) نیز مشاهده می‌شود، سازوکارهای رمزنگاری در تمام چهار لایه معماری وجود دارد. سازوکار رمزنگاری در IoT به دلیل محدودیت‌های موجود در منابع تجهیزات از جمله انرژی و توان محاسباتی، فرایند ساده‌ای نمی‌باشد[۳]. الگوریتم‌های رایج جهت رمزنگاری نظیر MD5[۶۶], SHA[۶۷], AES[۶۸], RSA[۶۹] دارای محاسبات پیچیده و سنگین بوده، بنابراین نیاز به پیاده‌سازی راه‌حل‌های رمزنگاری سبک وزن جهت حفظ محاسبات، ارتباطات، ذخیره‌سازی و سرانجام مصرف بهینه انرژی می‌باشد. مسئله موجود آن است که رمزنگاری سبک بر اساس کلیدهای متقارن کار می‌کند که به معنای به اشتراک گذاشتن کلیدهای متقارن در دستگاه‌های مختلف IoT است و به این ترتیب خود می‌تواند به چالش امنیتی تبدیل شود. تعدادی از راهکارهای رمزنگاری رشته‌ای[۷۰]، قطعه‌ای[۷۱] و توابع درهمساز[۷۲] سبک شده با لحاظ نمودن محدودیت‌ها در پیاده‌سازی سخت‌افزاری و نرم‌افزاری پیشنهاد شده است[۳۰-۳۲].

۵-۱- الگوریتم‌های رمزنگاری سبک وزن رشته‌ای

در این روش، متن ساده به‌طور کامل با رشته کلیدی شبه تصادفی که دارای همان طول متن ساده است، رمزنگاری می‌شود. عملیات رمزنگاری متشکل از XORing متن ساده و رشته کلیدی است. اگر چه این دسته از الگوریتم‌های رمزنگاری جایگزینی برای رمزنگاری قطعه‌ای است، اما استفاده از آن هنوز هم به دلیل طولانی بودن فاز مقداردهی اولیه محدود است. عیب این روش، غیرقابل استفاده بودن بعضی از پروتکل‌های ارتباطی است. با این حال، مزیت اصلی آن‌ها سادگی اجرا در سخت‌افزار و سهولت استفاده

64- Fragmentation
65- Protocol for Carrying Authentication for Network Access:PANA
66- Message Digest algorithm 5
67- Secure Hash Algorithm
68- Advanced Encryption Standard
69- Rivest–Shamir–Adleman
70- Stream cipher
71- Block cipher
72- Hash function

جدول ۶: مقایسه الگوریتم‌های رمزنگاری سبک وزن رشته‌ای.[۳۳,۳۴]

Technology Value[µm]	Area (GE)	Key Size (bits)	Algorithm
0.13	284	56	A2U2
0.13	1294	80	Grain v1
0.13	2599	80	Trivium
0.13	3188	80	Mickey

در زمانی است که اندازه متن ساده ناشناخته است.

الگوریتم‌های GRAIN v1 (تجزیه و تحلیل گسترده، با انعطاف‌پذیری بیشتر در پیاده‌سازی، دارای نسخه‌ای با حمایت از احراز هویت)، Trivium(تجزیه و تحلیل گسترده در طراحی و پشتیبانی از کلیدهای ۸۰ بیتی)، Mickey v2 (انعطاف‌پذیری کمتر در پیاده‌سازی) از نمونه‌های پرکاربرد در IoT می‌باشند. مقایسه الگوریتم‌های رمزنگاری سبک وزن رشته‌ای در جدول (٦) نشان داده شده است [۳۳,۳٤]. در این جدول، GE یک واحد اندازه‌گیری است که برای مشخص کردن پیچیدگی مدارهای الکترونیکی دیجیتال به‌طور مستقل از تولید کننده و فناوری استفاده می‌شود و به یک منطقه سیلیکونی برای فناوری تولید اختصاصی مربوط می‌شود. Technology Value به سطح فناوری پردازش نیمه هادی اشاره دارد.

۵-۲- الگوریتم‌های رمزنگاری سبک وزن در حالت قطعه‌ای

در محیط‌های منابع محدود، ارتباط اشیاء هوشمند باید بر محدودیت‌های خاصی از انرژی، عملکرد و کارایی غلبه کند. در رمزنگاری قطعه‌ای گروه‌هایی با طول بیت ثابت به نام قطعه تولید و توسط یک کلید متقارن مشخص شده است. رمزنگاری بر اساس قطعه، به‌عنوان اجزای ابتدایی در طراحی بسیاری از پروتکل‌های رمزنگاری بوده وبه‌طور گسترده‌ای در پیاده‌سازی رمزنگاری داده‌ها استفاده می‌شوند.[۳۵] برای اطمینان از امنیت ارتباطات، کلیدهای قطعه سبک وزن تا پایان دهه ۱۹۹۰ معرفی شدند. الگوریتم‌های زیر از جمله الگوریتم‌های نوع قطعه‌ای می‌باشند [۳۰-۳۲]

جدول ۷: مقایسه الگوریتم‌های رمزنگاری سبک وزن در حالت قطعه‌ای [۳۶-۳۸].

Technology Value[µm]	Area (GE)	Block Size (bits)	Key Size (bits)	Algorithm
0.18	402	48	80	PRINTcipher
0.18	1570	64	128	PRESENT
0.18	2168	64	184	DESXL
0.25	3048	64	128	HIGHT
0.13	1054	64	80	KATAN
0.13	684	64	80	KTANTAN
0.18	1265	64	128	LED
0.18	1981	64	64	KLEIN
0.13	683	64	80	Piccolo
0.18	1320	64	80	LBlock

AES 128 تغییر یافته DESL ،(AES) سبک شده، (DES SIMON و SPECK) با هدف ساده‌سازی، انعطاف‌پذیری و کارایی بهتر با لحاظ نمودن محدودیت‌های سخت‌افزاری و نرم‌افزاری)، همچنین ISO/IEC 29192-2:2012 دو رمزنگاری قطعه‌ای به نام‌های CLEFIA (با اندازه قطعه ۱۲۸ بیتی و اندازه کلید ۱۲۸، ۱۹۲یا ۲٥٦ بیتی) و PRESENT (با تاکید بر مشکل محدودیت سخت‌افزاری، با اندازه قطعه ٦٤ بیتی و اندازه کلید ۸۰ یا ۱۲۸بیتی) را ارائه داده که جهت استفاده در تجهیزات IoT به‌کار گرفته می‌شوند.

از مزایای الگوریتم‌های رمزنگاری سبک وزن قطعه‌ای نسبت به الگوریتم‌های رمزنگاری قطعه‌ای مرسوم، می‌توان به کوچک‌تر شدن اندازه قطعه (با هدف صرفه جویی در حافظه)، کوچک‌تر شدن اندازه کلید (با هدف صرفه جویی در مصرف انرژی[٣٦])، سادگی دور با تکرار بیشتر (با هدف دسترسی به امنیت)، برنامه‌های زمان بندی کلیدی ساده‌تر(با تولید کلیدهای فرعی) اشاره کرد. مقایسه برخی دیگر از الگوریتم‌های رمزنگاری سبک وزن در حالت قطعه‌ای در جدول (۷) نشان داده شده است [۳٦-۳۸].

جدول ۸: مقایسه توابع درهمساز[۳۴]

Technology Value[µm]	Area (GE)	Output size (bits)	Algorithm
1600	0.18	64	DM-PRESENT-80
865	0.18	80	PHOTON-80/20/16
2330	0.18	128	H-PRESENT-128
1379	0.18	128	U-Quark
4353	0.18	128	Armadillo-2B
2296	0.18	224	S-Quark
1702	0.18	160	D-Quark
2520	0.13	64	[Keccak-f[200
1060	0.13	128	SPONGENT-128
1728	0.13	224	SPONGENT-224
5527	0.13	160	SHA-1
5988	0.13	512	Cube 32

۵-۳- الگوریتم‌های رمزنگاری سبک وزن با استفاده از توابع درهمساز

از توابع درهمساز برای تایید یکپارچگی پیام، امضای دیجیتال و اثر انگشت استفاده می‌شود. با توجه به محدودیت منابع، استفاده از توابع درهمساز رمزنگاری سبک وزن برای کاهش استفاده از سخت‌افزارها و مصرف انرژی لازم است.

از الگوریتم‌های رمزنگاری سبک وزن پیشنهادی با استفاده از توابع درهمساز می‌توان به موارد زیر اشاره کرد[۳۰-۳۲]:

PHOTON،Quark،SPONGENT،SPONGENT و Lesamnta-LW

که همگی دارای ساختار و توابع داخلی سبک وزن شده با مصرف انرژی کمتر می‌باشند. از طرفی با کوچک‌تر کردن اندازه پیام‌ها می‌توان حجم محاسباتی را با درنظر گرفتن کارایی الگوریتم حفظ نمود که این به نوبه خود مزیت دیگر الگوریتم‌های در همساز سبک وزن شده در حوزه IoT است.

با بررسی های انجام شده، مشخص گردید که استفاده از الگوریتم‌های رمزنگاری قطعه‌ای کارایی بهتری در IoT دارد[۱۶]. مقایسه توابع درهمساز متداول در جدول (۸) نشان داده شده است[۳۴].

۵-۴- الگوریتم‌های رمزنگاری سبک وزن متقارن و نا متقارن مورد استفاده در IoT

همان‌طور که بیان شد، الگوریتم‌های رمزنگاری متعارف

جدول ۹: چند الگوریتم رمزنگاری سبک وزن متقارن[۳۶]

الگوریتم متقارن	طول کد	اندازه کلید	جلوگیری از حملات احتمالی
AES	2606	128	MITM
HEIGHT	5672	128	Saturation Attack
TEA	1140	128	Related Key Attack
PRESENT	936	80	Differential Attack

در سناریوی IoT به دلیل محدودیت‌های منابع و شرایط موجود مانند مصرف انرژی، محدودیت استفاده از باتری، و زمان واقعی اجرا مناسب نبوده، بنابراین از رمزنگاری سبک وزن به علت سازگاری بیشتر در محیط IoT استفاده می‌گردد. تعدادی از الگوریتم‌های رمزنگاری سبک وزن وجود دارد که در حال حاضر در دسته‌های تحقیقاتی الگوریتم‌های متقارن و نامتقارن تقسیم‌بندی می‌شوند. اما این الگوریتم‌های سبک وزن هنوز تضمین امنیت در زمان واقعی، زمان اجرا، مصرف انرژی و نیاز به حافظه را نمی‌دهد. الگوریتم‌های متقارن فاقد احراز هویت بوده در حالی که الگوریتم‌های نامتقارن دارای مسئله اندازه کلید بزرگ‌تر و مصرف حافظه بیشتر می‌باشد. این امر بر روی جمع‌آوری و پردازش اطلاعات در زمان واقعی تاثیر گذاشته و باعث اتلاف منابع IoT می‌گردد. جدول (۹) چند الگوریتم رمزنگاری سبک وزن متقارن و جدول (۱۰) چند الگوریتم رمزنگاری سبک وزن نامتقارن در حوزه IoT به همراه حملات احتمالی که از آن جلوگیری می‌شود را نشان می‌دهد[۳۶].

الگوریتم AES دارای سه نسخه ۱۲۸، ۱۹۲ و ۲۵۶ بیتی است. این الگوریتم در لایه برنامه کاربردی IoT وتحت پروتکل CoAP اجرا می‌گردد. کلید الگوریتم HEIGHT در مرحله‌های رمزنگاری و رمزگشایی تولید می‌شود. لی و همکاران وی پیشنهاد یک اجرای موازی را که نیاز به انرژی کمتری دارد ارائه کردند.[۳۷]. از الگوریتم TEA[۷۳] برای محیط‌های محدود مانند شبکه حسگر یا اشیای هوشمند استفاده می‌شود. کد این الگوریتم در چند خط نوشته شده است. از یک برنامه پیچیده استفاده نمی‌کند بلکه از عملیات ساده XOR جهت اضافه کردن و تغییر دادن

73- *Tiny Encryption Algorithm*

جدول ۱۰: چند الگوریتم رمزنگاری سبک وزن نامتقارن[۳۶]

الگوریتم نامتقارن	طول کد	اندازه کلید	جلوگیری از حملات احتمالی
RSA	۹۰۰	۱۰۲۴	Modules Attack
ECC(Elliptic-curve cryptography)	۸۸۳۸	۱۶۰	Timing Attack

استفاده می‌نماید.

PRESENT به‌عنوان الگوریتم سبک وزن برای امنیت استفاده می‌شود.

الگوریتم RSA به دلیل اندازه کلیدی بزرگ آن متعلق به سیستم رمزنگاری سبک وزن نیست. اما به دلیل استفاده از دو عدد اول بزرگ و اجرای عملیات ماجولار، دارای امنیت بیشتر بوده و باعث افزایش حریم خصوصی کاربران می‌شود. الگوریتم ECC نیاز به اندازه کلید کوچک‌تر دارد. به این ترتیب، سرعت پردازش آن سریع‌تر بوده و نیاز به حافظه کمتری دارد و مناسب پیاده‌سازی در سخت‌افزارهای IoT است[۳۸] . در ادامه برخی از تحقیقات اخیر در مورد کاربرد رمزنگاری سبک در IoT در جدول (۱۱) نشان داده شده است.

۶- چشم‌اندازها، چالش‌ها و مسیرهای تحقیقاتی آینده

در این قسمت به چالش‌های موجود در راستای اجرای موثر امنیت در فناوری IoT و موضوعات پژوهشی قابل بررسی در آینده در حوزه امنیت IoT پرداخته می‌شود.

• محدودیت‌های منابع

منابع محدود موجود در معماری IoT، مانع اصلی تعریف یک سازوکار قوی امنیتی در این فناوری می‌گردد. لذا با توجه به این محدودیت‌ها، به منظور پیاده‌سازی موفق پروتکل‌های امنیتی و ارتباطی برای IoT بایستی دستگاه‌های ذخیره‌سازی و همچنین نیازهای انرژی نیز در نظر گرفته شود. این امر مستلزم طراحی مجدد این پروتکل‌ها با توجه به نیاز به سبک‌وزنی به همراه بهبود تکنیک‌های برداشت انرژی[۷۴] که نیاز به محاسبات پیچیده‌ای ندارند، می‌باشد [۴۶ , ۴۷].

جهت حفظ صحت و جامعیت داده‌های حجیم در حین تراکنش بین اشیاء در شبکه‌های هوشمند (با محدودیت‌هایی همچون توان محاسباتی و منابع انرژی) بهترین راهکار بهبود الگوریتم‌های رمزنگاری سبک وزن در تجهیزات IoT، جهت بهره وری بیشتر می‌باشد؛ که به‌عنوان یک موضوع داغ در حوزه امنیت IoT مطرح است.

• تجهیزات ناهمگن

با توجه به محدوده دستگاه‌های ناهمگن که از دستگاه‌های کوچک کم قدرت دارای حسگر آغاز و به کارسازهای نهایی ختم می‌شود، لازم است تا چارچوب امنیتی چند لایه‌ای پیاده‌سازی شود. ابتدا، باید این چارچوب خود را با منابع موجود سازگار نماید، سپس تصمیم‌گیری بر اساس انتخاب سازوکارهای امنیتی در لایه‌های IoT پیش از ارائه خدمات به کاربر نهایی، انجام پذیرد. پیاده‌سازی چنین چارچوب امنیتی سازگار و پویا و هوشمند مستلزم استانداردسازی منابعی است که در معماری IoT به‌کار برده می‌شوند [۴۷].

• قابلیت همکاری[۷۵] پروتکل‌های امنیتی

جهت استانداردسازی سازوکار امنیت جهانی به منظور استفاده در IoT، پروتکل‌هایی که در لایه‌های مختلف اجرا می‌شوند، باید سازوکارهای ساده با قابلیت تبدیل و همکاری با یکدیگر را ارائه نمایند. به همراه سازوکارهای جهانی، ترکیب موثری از استانداردهای امنیتی در هر لایه می‌تواند با توجه به محدودیت‌های معماری تعریف شود.

• نقاط شکست[۷۶]

با وجود شبکه‌ها، معماری‌ها و پروتکل‌های ناهمگن، معماری و الگوهای مطرح در حوزه IoT به نقاط تک نقطه‌ای آسیب‌پذیرتر از سایر الگوها تبدیل می‌شود[۴۷] . میزان قابل توجهی از کارهای تحقیقاتی لازم است تا جهت اطمینان از دسترسی مناسب به عناصر و تجهیزات زیرساختی

74- Energy harvesting technique
75- Interoperablity
76- Points of Failure

جدول۱۱: تحقیقات اخیر در مورد کاربرد رمزنگاری سبک در IoT[۳۹-۴۵]

مرجع	راهکار پیشنهادی	توصیف	سایر ویژگی‌ها
Bose et al. (2015)[39]	طرح سبک وزن برای ایجاد کانال امن	پیشنهاد E2E تطبیقی و بهبود امنیت با حداقل مصرف منابع	انرژی متر هوشمند
Sahraoui &Bilami(2015) [40]	امنیت end-to-end سبک وزن در IoT	مدل فشرده سازی و طرح توزیع برای مبادله 6 LoWPAN HIP	راندمان مطلوب کاهش مصرف انرژی محافظت در برابر حمله DoS
Yang et al. (2016)[41]	داده‌های امن سبک وزن IoT در حوزه سلامت	سیستم پیشنهادی کنترل دسترسی توزیع شده از اطلاعات سلامت در حوزه‌های مختلف پزشکی محافظت شده را ارائه می‌دهد	کاهش سرباری تحلیل امنیتی کاهش زمان محاسبه
Al Salami et al.(2016) [42]	رمز گذاری سبک وزن برای خانه های هوشمند	جهت استفاده در برنامه‌های کاربردی خانه های هوشمند با دو زیر الگوریتم و"KEYEncrypt" "DATAEncrypt"	مدیریت کلید عمومی انعطاف پذیر بهره وری کاهش هزینه
Baskar et al.(2016) [43]	رمزنگاری سبک وزن برای محیط‌هایی با منابع محدود	الگوریتم رمزنگاری سبک وزن با حداقل محاسبه با استفاده از کلید مبتنی بر نقشه Chaos پیشنهاد شده و در یک FPGA اجرا شده است	امنیت قوی افزایش کارآیی
ERNEST (2017) [44]	رمزنگاری سبک وزن برای (Internet of Everything:IoE)	فناوری جدید و سبک وزن اولیه برای نسل بعدی از رمزنگاری سبک وزن پیشنهاد شده است	بهبود ساختار گرداننده‌های IoE اندازه کد دودویی، معیارهای حافظه و زمان اجرا
Bui et al. (2017) [45]	بهینه سازی سخت‌افزاری AES برای برنامه‌های کاربردی IoT با سطوح مختلف امنیتی	ایجاد سطوح امنیتی مختلف را از طریق اندازه های مختلف کلید، بهینه سازی قدرت و انرژی برای هر دو DataPath و key expansion	کاهش مصرف انرژی افزایش توان عملیاتی . افزایش امنیت

IoT، مخصوصا برای برنامه‌هـــای کاربردی حیاتی انجام پذیرد. این امر به ســـازوکارها و استانداردهایی نیاز دارد تـــا افزونگی را با توجه به مبادلات موجود میان هزینه‌ها و قابلیت اطمینان کل زیرساخت در نظر بگیرد.

• آسیب‌پذیری‌های سخت‌افزاری و میان افزاری

با فراگیـــری اســـتفاده از دســـتگاه‌های کم‌هزینه و کم مصرف، معماری IoT بیشـــتر در معرض آسیب‌پذیری‌های ســـخت‌افزاری قرار می‌گیرد. این امر تنها به عملکرد فیزیکی تجهیزات محدود نشده و پیاده‌سازی الگوریتم‌های امنیتی در سخت‌افزارها، مسیریابی و سازوکارهای پردازش بسته را نیز شامل می‌شـــود؛ به‌صورتی که باید پیش از استقرار در IoT تأیید گردد. تشـــخیص و کاهش آسیب‌پذیری‌هایی که پس از استقرار تجهیزات مورد سوء استفاده قرار می‌گیرد، دشوار اســـت. بنابراین یک الزام ضروری آنست که از یک پروتکل اســـتاندارد، برای تایید امنیت تجهیزات IoT استفاده گردد.

• بروزرسانی و مدیریت معتبر

یکی از مسائل مهم باز برای تحقیقات آینده ارائه مدیریت و به روزرسانی نرم‌افزارهای مقیاس‌پذیر و قابل اعتماد به میلیون‌ها دستگاه IoT اســـت. علاوه برآن، مسائل مربوط به امنیـــت، مالکیت معتبر دســـتگاه IoT، حریم خصوصی داده‌ها را می‌توان به‌عنوان مســـائل مربوط به تحقیقات باز در این حوزه دانســـت که به منظور ترویج مقررات وسیع و گســـترده در IoT باید توســـط جامعـــه تحقیقاتی مورد توجه قرار گیرد. فناوری زنجیـــره بلوکی[۷۷] می‌تواند برای راه‌حل‌های امنیتی IoT مفید باشـــد. با ایـــن حال، فناوری

۷۷- Blockchain پایگاه داده توزیع شـــده و مبتنی بر اجماع است که به‌صورت مستمر فهرســـتی از رکوردها را کـــه هرکدام به گزینه‌های قبلی فهرســـت ارجاع می‌دهند را حفظ می‌کند و بدین وسیله در مقابله با تضعیف یا بازنگری غیرمجاز تقویت می‌شود.

زنجیـــره بلوکی به خودی خـــود چالش‌های تحقیقاتی را با توجه به مقیاس‌پذیـــری، کارایی و برخوردهای کلیدی باز می‌نماید که بایستی مورد توجه محققان قرار گیرد.

• آسیب‌پذیری‌های زنجیره بلوکی

با وجود ارائه رویکردهای قوی برای ایمن‌ســـازی IoT، فناوری زنجیره بلوکی نیز آســـیب‌پذیر هســـتند[۴۸]. این سازوکار بســـتگی به قدرت درهمســـازی داشته و امکان این‌که مهاجـــم میزبانی زنجیره بلوکی را در دســـت گیرد وجود دارد. به‌طور مشـــابه، کلید خصوصی با محدودیت تصادفی بودن می‌تواند برای سوء استفاده از حساب‌های زنجیره بلوکی مورد سوء استفاده قرار گیرد. لذا تحقیق در خصوص ارائه ســـازوکارهای موثر برای حصول اطمینان از حفظ حریم خصوصی، تراکنش‌ها و جلوگیری از حملات، بایستی مورد توجه محققان حوزه امنیت قرارگیرد.

۷- نتیجه گیری

ایجـــاد و توســـعه IoT با بســـیاری از مباحث امنیتی و چالش‌های زیربنایی مواجه است. از آنجا که در این فناوری ادغام حســـگرها و اشیاء مختلف بدون دخالت انسان جهت برقراری ارتباط فراهم می‌شـــود، از این رو در نظر گرفتن پروتکل‌ها و ســـازوکارهایی برای ایمن‌سازی فناوری‌های ارتباطـــی و برنامه‌هـــای کاربردی مورد اســـتفاده در IoT در لایـــه بندی‌های دقیق‌تر بدون اعمال ســـربار ضروری می‌باشد.

مشـــخصات امنیتـــی تجهیزات IoT همیشـــه بـــه دلیل تهدیدهـــای امنیتی جدید اعمال شـــده بر روی دســـتگاه‌ها تغییر می‌کند، از این رو امنیت IoT به موضوع مهم مدیریتی تبدیل شده اســـت. مدیریت موثر تهدیدات نیاز به ارزیابی صحیح و دقیق برای کاهش تهدیدهای شـــناخته شـــده در محیـــط IoT را دارد. طبقه‌بندی امنیـــت در IoT باید تجزیه و تحلیل جامعی از ســـازوکارهای امنیتـــی را ارائه دهد و این‌که چگونه می‌توان از اطلاعـــات تمام لایه‌ها برای ارائه دهندگان سیســـتم و تحلیلگران جهـــت طراحی و تجزیه و تحلیل سیســـتم‌های ایمن استفاده کرد. مشکلات امنیتی در IoT می‌تواننـــد در لایه‌های مختلـــف رخ دهند. ویژگی‌های امنیتی مختلف از قبیل محرمانه بـــودن، یکپارچگی، احراز هویت، مجوزدسترسی، در دســـترس بودن و حفظ حریم خصوصی، باید برای اطمینان از امنیت در کل سیستم IoT تضمین شود. این هدف با توجه به ویژگی‌های محیطی IoT به شدت چالش برانگیز است.

رویکردهای امنیتی IoT نشان‌دهنده نیاز به طراحی یک طبقه‌بندی امنیتی جدید است که به سادگی و با دقت بیشتر برای رده‌بندی تهدیدات و آسیب‌پذیری‌های امنیتی در IoT بـــه‌کار برده شـــود. در این مقاله، چارچوبـــی چهارلایه‌ای برای معماری امنیتی IoT پیشنهاد شد. همچنین، ویژگی‌ها و عملکرد هر لایه بر اســـاس تهدیدات و آسیب‌پذیری‌های مختلف مشخص گردید و راهکارها و ملاحظات امنیتی که امـــکان بهبود خدمات امنیتی را در هر لایه IoT ایجاد نماید، بیان گردید.

برخی از چالش‌های امنیتی مطرح در معماری چهار لایه ای امنیتی IoT تشـــریح شده در این مقاله، مختص یک لایه خاص نبوده و باید در تمام لایه‌ها آن چالش (مانند حفاظت از داده‌هـــا و توجه به خصوصی بـــودن آن‌ها) را در نظر گرفت.

علاوه بـــر معماری شـــرح داده شـــده، جهت حصول اطمینان از امن بودن سیســـتم IoT در پیاده‌سازی شبکه‌ها لازم است تا اصول اولیه امنیتی از جمله ایجاد محیط شبکه سالم و امن، ایجاد حفاظت درجه‌بندی شده، شبکه اطلاعاتی حفاظت از داده‌ها با برقراری امنیت سیستم‌های اطلاعاتی مهم، دفاع فعال و توانایی حفاظت از منابع، پیشگیری جامع و بهبـــود امنیت اطلاعات، تقویت مدیریت فناوری، پژوهش مســـتمر در زمینه فناوری و اطمینان از قابلیت کنترل IoT مدنظر قرار گیرد.

با توجه به این‌که معماری امنیتی اینترنت اشـــیاء هنوز در مرحلـــه اکتشـــافی خود اســـت، لذا ضروری اســـت تا پژوهشگران به امنیت IoT توجه ویژه نموده و راهکارهای

مناسبی جهت مقابله با تهدیدات موجود و جدید در این فناوری را ارائه دهند.

چشم‌اندازها، چالش‌ها و موضوعات تحقیقاتی داغ روز در حوزه امنیت IoT شامل آسیب‌پذیری‌های زنجیره بلوکی، بروزرسانی و مدیریت معتبر، آسیب‌پذیری‌های سخت‌افزاری و میان افزاری، محدودیت‌های منابع، تجهیزات ناهمگن، قابلیت همکاری پروتکل‌های امنیتی و نقاط شکست به تفصیل در قسمت ٦ مقاله بیان شد.

در نهایت با توجه به چشم‌اندازهای امنیتی آتی در حوزه IoT، استانداردسازی سازوکار امنیت جهانی و یافتن تکنیک‌های رمزنگاری موثر و کارآمد سبک وزن از جمله حوزه‌های مهم و قابل تحقیق مطرحی است که قابلیت جایگزینی با راهکارهای محاسباتی سنتی گران قیمت مشابه را داشته باشد.

مراجع

1. Zhou, H., The Internet of Things in the Cloud: A Middleware Perspective, CRC Press, Boca Raton, FL, 2012.

2. Rekleitis, E., RizomilIoTis, P. and S. Gritzalis," A Holistic Approach to RFID Security and Privacy", Proc. 1st Int 'l Workshop Security of the Internet of Things (SecIoT 10), Network Information and Computer Security Laboratory, 2010.

3. Raye, A and Salam, S., Internet of things: from hype to reality, Springer, 2017.

4. Lu, C., "Overview of Security and Privacy Issues in the Internet of Things", online. available: https://www.cse.wustl.edu/~jain/cse574-14/ftp/security/index.html, 2014.

5. Suo, H., Wan, J., Zou, C., Liu, J., "Security in the internet of things: A review". Proceedings −2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, 3, 648–651, 2015.

6. Milbourn, T., "IP versus CoAP for IoT Communications", July 15, 2016, online. available: https://www.u-blox.com/en/blog/ip-versus-coap-iot-communications.

7. Kai, P., "DEMO: An IDS framework for internet of things empowered by 6LoWPAN". Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS '13, October, 2016, 1337–1340, 2016.

8.Tsai, C.-W., Lai, C.-F. , Vasilakos, A.V. "Future internet of things: open issues and challenges" .Wirel. Netw., 20 (8) (2014), pp. 2201-2217

9. Fadele Ayotunde, A., Mazliza, O, Ibrahim Abaker Targio, H., et al. "Internet of Things security: A Survey",Journal Of Network And Computer Applications Vol. 88, 10-28 , 2017

10. Borgohain, T., Kumar, U., and Sanyal, S., "Survey of Security and Privacy Issues of Internet of Things," Jan. 2015.online.available:https://www.researchgate.net/publication/270763270

11.Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., and Qiu, D. "Security of the Internet of Things: perspectives and challenges". Wireless Networks, 20(8), 2481–2501, 2014.

12. Massis, B. "The Internet of Things and its impact on the library". New Library World, 117(3/4), 289–292, 2016.

13. Zhang, Y., Shen, Y., Wang, H., Yong, J., and Jiang, X. "On Secure Wireless Communications for IoT Under Eavesdropper Collusion". IEEE Transactions on Automation Science and Engineering, 13(3), 1281–1293, 2015.

14. Liu, Y., Cheng, C., Gu, T., Jiang, T., Member, S., and Li, X. "A Lightweight Authenticated Communication Scheme for Smart Grid", IEEE Sensors Journal, Vol. 16, Issue. 3, 836–842, 2016

15. Manjulata, A.K., "Survey on lightweight primitives and protocols for rfid in wireless sensor networks", International Journal of Communication Networks and Information Security (IJCNIS), vol.6 , No.1, 29–43, 2014

16. online. available: http://www.postscapes.com/internet-of-things-protocols

17.. Akhunzada, A., Gani, A., Anuar, N. B., Abdelaziz, A., Khan, M. K., Hayat, A., and Khan, S. U. "Secure and dependable software defined networks". Journal of Network and Computer Applications, Vol. 61, 199–221,2016

18. Bekara, C. "Security issues and challenges for the IoT-based smart grid". Procedia Computer Science, Vol. 34, 532–537,2014

19. Hu,Y, Perrig,A, Johnson, DB, "Wormhole attacks in wireless networks" , IEEE Journal on Selected Areas in Communications,vol. 24, issue. 2, 2016

20. Horrow, S., and Anjali, S. "Identity Management Framework for Cloud Based Internet of Things". SecurIT '12 Proceedings of the First International Conference on Security of Internet of Things, 200–203, 2012.

21.Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu," Security of the Internet of Things: perspectives and challenges"Wireless Network., vol. 20, No. 8, , 2481-2501, 2014

22.Oen, H. M., 2015. "Interoperability at the Application Layer in the Internet of Things" ,2015, available online: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2352735/13131_FULLTEXT.pdf?sequence=1

23. Nolin, J., Olson, N., "The Internet of Things and convenience.", Internet Res. Vol.26, No. 2, 360–376., 2016

24. Nolin, J., Olson, N., "Security threats in the application layer in IOT applications",
International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 477 – 480, 2017

25. Raza,Sh., Helgason, T., Papadimitratos, P. Voigt, T., "SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things", Future Generation Computer Systems, Vol. 77, 40-51, 2017

26. IoT Security Compliance Framework, IoT Security Foun-

41. Yang Y, Zheng X, Tang C. “Lightweight distributed secure data management system for health internet of things.”, Journal of Network and Computer Application, Vol.89, 2016.
42. Al Salami S, Baek J, Salah K, Damiani E “Lightweight encryption for smart home.”, Proceeding of 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, pp 382–388, 2016
43. Baskar C, Balasubramaniyan C, Manivannan D, “Establishment of light weight cryptography for resource constraint environment using FPGA.”, Proced Comput Sci 78: 165–171, 2016
44. Ernest W “Light primitives and new technologies are driving the next generation of lightweight cryptography”. Available Online http://semiengineering.com/lightweight-cryptography-for-the-ioe/, 2017
45. Bui, D., Puschini ,D., Bacles-Min ,S., “AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications” , IEEE Transactions on Very Large Scale Integration (VLSI) Systems,Vol. 25, Issue 12 • Dec. 2017
46. Kamalinejad, P., Mahapatra, C., Sheng, Z., Mirabbasi, S., Leung, V. C., & Guan, Y. L. Wireless energy harvesting for the Internet of Things. IEEE Communications Magazine, 53(6), 102-108.2015.
47. Ahmad Khan M., Salah, Kh., IoT security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems, Volume 82,2018,
48. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. A survey on the security of blockchain systems. Future Generation Computer Systems.2017.
dation, 2016, online. available: https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf
27. Yang, G., Xu, J, Chen, Qi, P, Z. H, and Wang, H. Y., “Security characteristic and technology in the internet of things,”. Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.
28. Ding, C., Yang, L. J. and Wu, M. “Security architecture and key technologies for IoT/CPS”, ZTE Technology Journal, vol. 17, no. 1, 2011.
29. IOT security: A survey, online. available: http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_sec/index.html
30. Mckay,K., Bassham, L.,”Report on Lightweight Cryptography”.NIST, https://doi.org/10.6028/NIST.IR.8114
31. Katagi, M and Moriai, S,” Lightweight cryptography for internet of things” sony corporation, pp 7-10, 2008
32.Usman, M, et al, “SIT: a lightweight encryption algorithm for secure internet of things”, international journal of advanced computer science and applications, vol 8, no 1, 2017
33. C. Manifavas, G. Hatzivasilis, K. Fysarakis, K. Rantos, “Lightweight cryptography for embedded systems – a comparative analysis”, Proceedings of the DPM/SETOP, 333–349, 2013.
34. Guo, X., Schaumont, P., “The technology dependence of lightweight hash implementation
Cost”, Proceedings of the ECRYPT Workshop on Lightweight Cryptography (LC2011), 2011.
35. “Block Cipher Modes”. NIST Computer Security Resource Center. online available: https://csrc.nist.gov/projects/block-cipher-techniques Retrieved by 20.4.2018
36. Singh, S., Kumar Sharma, P., · Moon, S.Y, Park, J.H, “Advanced lightweight encryption algorithms for IoT devices: survey, hallenges and solutions”, Journal of Ambient Intelligence and Humanized Computing,2017
37. Chai, Q., Gong, G,” A cryptanalysis of hummingbird-2: the differential sequence analysis”, IACR Cryptology ePrint Archive 2012, p. 233, 2012
38. D. Lee, D.-C. Kim, D. Kwon, H. Kim, “Efficient hardware implementation of the lightweight block encryption algorithm Lea”, Sensors, vol. 14, No.1, 975–994. 2014.
37. Lee, JH, Lim, DG “Parallel architecture for high-speed block cipher, HIGHT”. International Journal of Security Application, vol. 8, No.2 ,59–66, 2014.
38. Eisenbarth T, Kumar S.” A survey of lightweight-cryptography implementations”. IEEE Desi Test Comput. Vol. 24, No. 6,1–12, 2003
39. Bose, T., Bandyopadhyay, S., Ukil, A., Bhattacharyya, A., and Pal, A. “Why not keep your personal data secure yet private in IoT: Our lightweight approach.”, Proceedings of the 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 1–6, 2015
40. Sahraoui S, Bilami A “Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things” Computer Networks, Vol. 91,26–45, 2015.