

کلیات اینترنت اشیا

محمدیاسین داوده

۱۶ آبان ۱۳۹۹

۱ تعریف

اینترنت چیزها، اشیا یا همه چیز (IoT)^۱ شبکه‌ای از «اشیا» است که به نرم‌افزار، سنسور و دیگر فناوری‌های مرتبط جهت برقراری ارتباط و تبادل داده با دیگر دستگاه‌های روی شبکه‌ای جهانی (اینترنت) مجهز شده‌اند. غالباً اشیا دستگاه‌هایی مجهز به حسگرها، هویت یا داده هستند که به یک شبکه وصل شوند. این اشیا می‌توانند از وسایل خانگی، کشاورزی گرفته تا پوشاک را شامل باشند. از این فناوری در زمینه‌هایی مانند، خانه‌های هوشمند، اتوماسیون، یادگیری ماشین، جمع‌آوری داده و دیگر زمینه‌ها استفاده می‌شود.^[۱] به نحوی می‌توان گفت که IoT الگویی در به کارگیری فناوری‌های قدیمی به نحوی جدید است. ترکیب این اشیا با تکنولوژی ما را قادر ساخته تا تعامل راحت‌تر و کنترل بیشتری روی دنیای مجازی داشته باشیم.

۱.۱ مهمترین فناوری‌ها

به گفته Lee مهمترین فناوری‌ها و سرویس‌های پر استفاده کنونی برای پیاده‌سازی IoT به این شرح است:

- RFID^۲
- WSN^۳
- Middleware
- پردازش ابری
- نرم‌افزار IoT

۱.۱.۱ RFID

فناوری پر کاربرد RFID، امروزه در همه جای جهان برای شناسایی اشیای غیر کامپیوتری استفاده می‌شود. این فناوری را می‌توانید در بلیط‌ها، عوارضی‌ها و برجسب‌های خرید روی کالاها که به طور اتوماتیک خود را معرفی کرده یا داده‌ای را منتقل می‌کنند پیدا کنید.

Internet of things^۱
Radio Frequency Identification^۲
Wireless Sensor Networks^۳

WSN ۲.۱.۱

شبکه‌های سنسورهای بی‌سیم (WSN) شبکه‌ای متشکل از تعدادی دستگاه‌های مجهز به سنسورها یا سنسورها است که به هدف جمع‌آوری اطلاعات در فضایی کار گذاشته می‌شوند. از چنین شبکه‌هایی در جاهایی مانند مزارع توربین‌های بادی استفاده می‌شود.

۳.۱.۱ پردازش ابری و نرم‌افزار

اما IoT فقط نیازمند سخت‌افزار نیست. میانه‌افزارها و پروتکل‌های مختلفی برای ارتباط برقرار کردن بین چنین دستگاه‌هایی استفاده می‌شود. به علت نفوذ توزیع‌شده و گسسته IoT پردازش و ذخیره‌سازی اطلاعات در این زمینه چالش‌های خاص خود را دارد. راه حل مهمی که برای این مسئله و اتصال IoT مطرح می‌شود پردازش ابری است.

۲ معماری چهارلایه

معماری‌های متفاوتی برای اینترنت اشیا موجود است. از عام‌ترین آنها معماری چهارلایه است. لایه‌ها در این معماری از این قرار است [۳، ۴]:

۱. اشیا یا سنسورها و عملگرها (Actuator)

۲. گیتوی

۳. لبه IoT یا پردازش

۴. API^۴



شکل ۱: چهار لایه رایج IoT

^۴Application Programming Interface

۱.۲ اشیا

این لایه فیزیکی شامل سنسورها و عملگرها است که داده‌ها را جمع‌آوری یا عملی را به انجام می‌رسانند.

۲.۲ گیتوی

لایه گیتوی تا حد امکان به اشیا نزدیک است. در این لایه سیگنال‌های سنسورها جمع‌آوری شده و در صورت آنالوگ بودن تبدیل به دیجیتال می‌شوند. همچنین سیگنال‌های خروجی به عملگرها در صورت نیاز در این مکان به داده‌های آنالوگ تبدیل می‌شوند.

۳.۲ لبه

در لبه داده‌ها پردازش شده و با پردازش و تحلیل گلچین می‌شوند. داده‌های خام به اطلاعات تبدیل شده و پیش‌پردازش‌های لازم پیش از ارسال روی ابر را در دسترس قرار دادن روی آنها انجام می‌شود. علاوه بر آن تحلیل‌ها، بصری‌سازی و یادگیری ماشین در این مرحله انجام می‌شود. خروجی لبه آماده برای استفاده نهایی یا ذخیره‌سازی است و کاملاً پالایش شده است.

۴.۲ API

در این لایه اطلاعات ذخیره یا برای مصرف ارائه می‌شوند. این لایه معمولاً در ابر قرار دارد و به واسطه چنین فناوری‌هایی ارائه می‌شود.

۳ نقش الگوریتم‌های رمزنگاری در امنیت اینترنت اشیا

نگرانی‌هایی درباره این فناوری، به خصوص در حوزه‌های امنیت و حریم خصوصی وجود دارد. اهمیت این موضوع از این جهت است که این فناوری به طور مستقیم با کنترل اعضای حیاتی انسان‌ها و سیستم‌ها ارتباط دارد (اعضای مصنوعی افراد). علاوه بر کنترل، حجم کلانی از داده‌ها درباره جزئیات زندگی افراد و سیستم‌های مختلف توسط این اشیا جمع‌آوری می‌شود و نقص امنیتی در آنها می‌تواند به درز این اطلاعات منجر شود.

اصلی درباره امنیت این فناوری به گستردگی و طیف وسیع دستگاه‌ها و پروتکل‌ها و نقاط مشترک کم بین آنها است. علاوه بر آن، بیشتر دستگاه‌ها نظارت و کنترل نمی‌شوند. بر اساس گزارش اخیر Unit 42 «۵۷٪ دستگاه‌های IoT به حملات سطح متوسط یا بالا^۵ آسیب‌پذیری هستند» و «۹۸٪ تمام ترافیک دستگاه‌های IoT رمزنگاری نشده است». این گروه با بررسی ۲۰۱ میلیون دستگاه IoT در سطح آمریکا که از سرویس‌های آنها استفاده می‌کردند این گزارش را تهیه کرده‌اند[۵].

علاوه بر این بحث‌های قدیمی‌تری مانند بحث سؤال برانگیز امنیت نرم‌افزارها و سیستم‌عامل‌های متن بسته، امنیت اطلاعات ذخیره‌شده و قابل دسترسی از اینترنت مطرح است. الگوریتم‌های رمزنگاری امنیت نسبی را برای ارتباط اشیا با یکدیگر فراهم می‌کنند. اهمیت این الگوریتم‌ها به خصوص در شبکه‌های بسته نمود پیدا می‌کند.

^۵احتمالاً بر اساس Common Vulnerability Scoring System (جزئیات: <https://www.first.org/cvss/>) (specification-document)

مطابق گفته‌های Khan پروتکل‌های کاربردی ارتباط IoT مانند HTTP، MQTT، CoAP و XMPP و حتی پروتکل‌های مسیریابی مانند RPL و 6LoWPAN امن نیستند به همین دلیل رمزنگاری و استفاده از پروتکل‌های لایه بالاتری مانند TLS و DTLS لازم است. چالش انتخاب و پیاده‌سازی این الگوریتم‌ها به منابع بسیار محدود اشیا باز می‌گردد. الگوریتم‌های مرسوم رمزنگاری زیر کاربرد گسترده‌ای در حوزه IoT دارند:

- DES و Triple DES

- AES

- RSA

- Twofish

علاوه بر این، در سال‌های استفاده از بلاکچین در امنیت IoT مطرح شده است.

مراجع

- [1] Wikipedia. Internet of things. URL https://en.wikipedia.org/wiki/Internet_of_things&oldid=979730325.
- [2] Kyoochun Lee, In & Lee. The internet of things (iot): Applications, investments, and challenges for enterprises. *Business Horizons*, 58 (4):431–440, 2015. URL <https://fardapaper.ir/mohavaha/uploads/2018/03/Fardapaper-The-Internet-of-Things-IoT-Applications-investments-and-challenges-for-enterprises.pdf>.
- [3] Jyotsna Vadakkanmarveetil. 4 layers of the internet of things, 10 2018. URL <https://www.jigsawacademy.com/4-layers-of-the-internet-of-things/>.
- [4] Sarveshbhatt. Four layer and seven layer architecture in the internet of things, 6 2019. URL <https://techtalkwithbhatt.com/2019/06/02/four-layer-and-seven-layer-architecture-in-the-internet-of-things/>.
- [5] Unit 42. 2020 unit 42 iot threat report, 3 2020. URL <https://unit42.paloaltonetworks.com/iot-threat-report-2020/>.
- [6] Khaled Khan, Minhaj Ahmad & Salah. Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395–411, 2018.
- [7] Kenneth. The 4 stages of iot architecture (2020 ultimate guide), 12 2019. URL <https://robots.net/it/4-stages-of-iot-architecture/>.