Arman Process Journal 2(4): 1-5, Winter 2022

Arman Process Journal
(APJ)

Homepage: www.armanprocessjournal.ir

# IoT Security Challenges and Solutions

***S. Ganjkhanloo*[*,1], *Z. Bigdeli*[2]**

[1] *Department of Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran*
[2] *Department of Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran*

Received: 2 October 2021
Accepted: 26 December 2021

**KEYWORDS:**
Internet of Thing
Security Protocols
Privacy
Architecture

[1] Corresponding author
*ganjkhanloo.s@yahoo.com*

## ABSTRACT

The Internet of Things (IoT) is one of the fastest technologies to be used in a variety of applications in the last decade and is in fact a large distributed network in which billions of intelligent devices are connected. Smart devices connect wirelessly or wirelessly to communicate, process, compute and monitor various real-time scenarios. The Internet of Things promises a world in which intelligent communication from most devices is possible via the Internet anywhere, anytime with the least possible human assistance. However, security and privacy are the main concerns of the Internet of Things that can affect its sustainable development. Inadequate device updates, lack of efficient and robust security protocols, user ignorance, and active device monitoring are some of the major security challenges that the Internet of Things faces. In this article, we have dealt with the issue of IoT security from different dimensions and examined the related challenges and solutions.

| NUMBER OF REFERENCES | NUMBER OF FIGURES | NUMBER OF TABLES |
|---|---|---|
| 16 | 1 | 0 |

نشریه تخصصی آرمان پردازش، دوره ۲، شماره ۴، زمستان ۱۴۰۰

فصلنامه تخصصی آرمان پردازش

(APJ)

Homepage: www.armanprocessjournal.ir

# چالش های امنیتی اینترنت اشیاء و راهکارها

سمیه گنج خانلو*[۱] و زهرا بیگدلی[۲]

۱ دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد زنجان، زنجان، ایران

۲ دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد زنجان، زنجان، ایران

## چکیده

اینترنت اشیا از سریع‌ترین فناوری‌هایی است که در دهه اخیر در کاربردهای مختلف مورد استفاده قرار گرفته است و درواقع یک شبکه توزیع شده بزرگ است که در آن میلیاردها دستگاه به هم متصل هستند. ابزارهای هوشمند به صورت بی سیم یا سیمی برای ارتباط، پردازش، محاسبات و نظارت بر سناریوهای زمان واقعی مختلف متصل می شوند. اینترنت اشیا نوید جهانی را می دهد که در آن ارتباطات هوشمند از اکثر دستگاه ها از طریق اینترنت در هر مکان و در هر زمان با کمترین کمک ممکن انسانی امکان پذیر است. با این حال، امنیت و حریم خصوصی نگرانی های اصلی اینترنت اشیا هستند که می توانند بر توسعه پایدار آن تأثیر بگذارند. به روز رسانی نامناسب دستگاهها، عدم وجود پروتکل های امنیتی کارآمد و قوی، ناآگاهی کاربران و نظارت فعال دستگاه ها از جمله چالش های امنیتی مهمی است که اینترنت اشیا با آن مواجه است. در این مقاله از ابعاد مختلف به مساله امنیت در اینترنت اشیاء پرداخته و چالش ها و راهکارهای پیش رو را بررسی نموده ایم.

**واژگان کلیدی:**
اینترنت اشیا
پروتکل امنیتی
محرمانگی
معماری

[۱] نویسنده مسئول
ganjkhanloo.s@yahoo.com

| تعداد جداول | تعداد شکل ها | تعداد مراجع |
|---|---|---|
| ۰ | ۱ | ۱۶ |

## مقدمه

اینترنت اشیاء[1] یا به اختصار IoT به میلیاردها دستگاه فیزیکی در سراسر جهان گفته می‌شود که به اینترنت متصل هستند و اطلاعات را جمع‌آوری می‌کنند و با کاربر و سایر دستگاه‌های متصل به اشتراک می‌گذارند. تقریبا هر چیزی که بتواند به شبکه اینترنت متصل شود، بخشی از اینترنت اشیا است. دستگاه‌های متصل به اینترنت می‌توانند راهی برای پیش‌بینی در مورد همه چیز، از رفتار مصرف‌کننده گرفته تا وقایع آب‌وهوایی، باشند؛ اما این دستگاه‌ها در عین حال دسترسی هکرها به فضای خصوصی افراد برای سرقت و فاش کردن اطلاعات شخصی آن‌ها را آسان‌تر می‌کنند. بسته به اینکه از چه کسی بپرسید، اینترنت اشیا قرار است آینده تکنولوژی را دگرگون کند یا همچون ربات غول‌پیکر افسارگسیخته‌ای، پایان عصر تکنولوژی بشر را رقم بزند. برخی از مزایای اینترنت اشیا امکان دسترسی به اطلاعات از هر نقطه در هر زمان در هر دستگاه، بهبود ارتباط بین دستگاه‌های الکترونیکی متصل، انتقال بسته‌های داده از طریق شبکه متصل و صرفه جویی در وقت و هزینه و خودکارسازی وظایف به بهبود کیفیت خدمات یک شرکت و کاهش نیاز به مداخله انسانی، می باشد [۳-۱]. از معایب اینترنت اشیا نیز این است که با افزایش تعداد دستگاه‌های متصل و به اشتراک گذاری اطلاعات بیشتر بین دستگاه‌ها، احتمال سرقت اطلاعات محرمانه توسط هکر نیز افزایش می‌یابد. ممکن است شرکت‌ها در نهایت مجبور به مقابله با تعداد زیادی دستگاه IoT شوند و جمع آوری و مدیریت داده‌ها از همه این دستگاه‌ها چالش برانگیز خواهد بود. اگر اشکالی در سیستم وجود داشته باشد، احتمالاً هر دستگاه متصل خراب می‌شود. از آنجا که هیچ استاندارد بین المللی سازگاری برای اینترنت اشیا وجود ندارد، برقراری ارتباط بین دستگاه‌های سازندگان مختلف دشوار است [۴].

## چالش های امنیتی و حریم خصوصی اینترنت اشیا

امنیت اینترنت اشیا زیرمجموعه‌ای از امنیت سایبری است که بر حفاظت، نظارت و رفع تهدیدات مربوط به اینترنت اشیا یا شبکه دستگاه‌های متصل که داده‌ها را از طریق اینترنت جمع‌آوری، ذخیره و به اشتراک می‌گذارد، تمرکز می‌کند . چالش‌های اینترنت اشیا درزمینه امنیت می‌تواند بسیار بحث‌برانگیز باشد زیرا بسیاری از دستگاه‌های اینترنت اشیا با امنیت قوی ساخته نشده‌اند. اینترنت اشیا میلیاردها دستگاه را به اینترنت متصل می‌کند و شامل استفاده از میلیاردها نقطه داده است که همه آن‌ها باید ایمن شوند. به دلیل گسترش سطح حمله، امنیت اینترنت اشیا و حریم خصوصی اینترنت اشیا به عنوان نگرانی‌های اصلی ذکر شده است. از آنجا که دستگاه‌های اینترنت اشیا به هم متصل هستند، تنها کاری که یک هکر باید انجام دهد این است که از یک آسیب پذیری برای دستکاری همه داده‌ها سوء استفاده کرده و آن‌ها را غیر قابل استفاده کند. تولیدکنندگانی که دستگاه‌های خود را به طور مرتب یا اصلاً به روز نمی‌کنند، در برابر مجرمان سایبری آسیب پذیرتر هستند. علاوه بر این، دستگاه‌های متصل اغلب از کاربران می‌خواهند اطلاعات شخصی خود، از جمله نام، سن، آدرس، شماره تلفن و حتی حساب‌های رسانه‌های اجتماعی را وارد کنند. هکرها تنها تهدید اینترنت اشیا نیستند [۸-۵]. حفظ حریم خصوصی یکی دیگر از نگرانی‌های مهم کاربران اینترنت اشیا است. به عنوان مثال، شرکت‌هایی که دستگاه‌های IoTمصرف کننده را تولید و توزیع می‌کنند، می‌توانند از این دستگاه‌ها برای به دست آوردن و فروش اطلاعات شخصی کاربران استفاده کنند . اینترنت اشیا علاوه بر افشای اطلاعات شخصی، خطری برای زیرساخت‌های حیاتی، از جمله برق، حمل و نقل و خدمات مالی نیز ایجاد می‌کند. لذا، دستگاه‌های اینترنت اشیاء در معرض چالش‌ها و آسیب‌پذیری‌های امنیتی ذاتی هستند. در ادامه چند نمونه از چالش‌های اینترنت اشیا درزمینه امنیت بسط داده شده است [۱۱-۹].

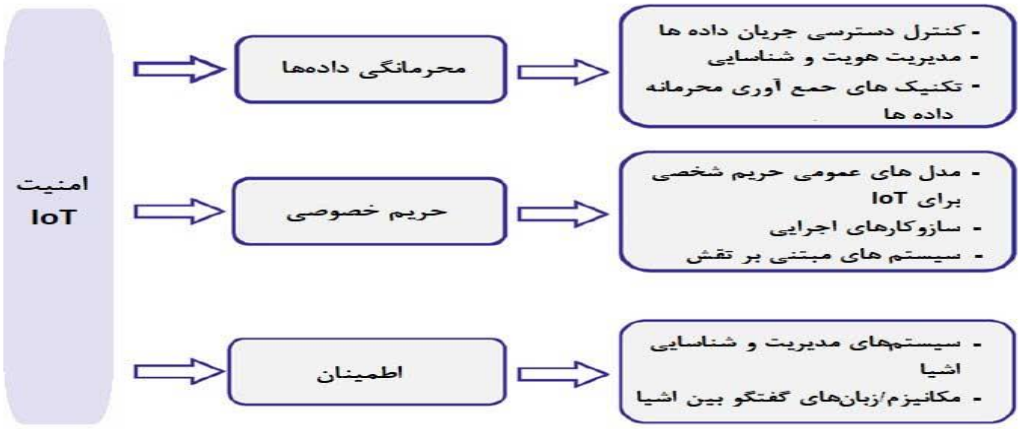
- دستگاههای سایه: یکی از مهم‌ترین چالش‌های درزمینه امنیت، خطر وجود دستگاه‌های سایه یا دستگاه‌هایی است که به شبکه اینترنت اشیا متصل هستند اما توسط صاحب شبکه مجاز یا شناخته‌شده نیستند.
- عدم به‌روزرسانی نرم‌افزارهای قابل‌اعتماد: سیستم‌های اینترنت اشیا اغلب به‌درستی جهت حفاظت از آسیب‌پذیری‌های امنیتی به‌روز نمی‌شوند. دستگاه‌های اینترنت اشیا معمولاً کوچک هستند و در مکان‌های دورافتاده مستقر می‌شوند. ممکن است یک سازمان هزاران دستگاه IoT برای مدیریت داشته باشد، بنابراین امکان فراموش کردن محل استقرار دستگاه‌های IoT برای سازمان‌ها وجود دارد. همچنین، بسیاری از دستگاه‌های اینترنت اشیا برای به‌روزرسانی نرم‌افزار به خود کاربران وابسته هستند اما بسیاری از کاربران از آن آگاهی ندارند [۱۲].
- آسیب‌پذیری واسط: مبادله داده‌ها از طریق شبکه توسط رابط برنامه‌نویسی برنامه،تنها بخش کوچکی از کار دستگاه‌های IoT است . آسیب‌پذیری‌های درون API ها یک خطر امنیتی مهم محسوب می‌شوند.
- رمزهای پیش‌فرض: اگر کاربران گذرواژه‌های پیش فرض اشیا را تغییر ندهند، مهاجمان با فهرست گذرواژه‌های پیش‌فرض IoT می‌توانند برای دسترسی غیرمجاز به یک دستگاه و شبکه آن استفاده کنند.
- استانداردها: ازآنجایی‌که هیچ‌گونه API اینترنت اشیاء واحدی وجود ندارد، استاندارد واحدی نیز برای کنترل طراحی انواع نرم‌افزارهایی که آن‌ها اجرا می‌کنند یا نحوه تبادل داده‌ها موجود نیست.
- وسعت تعداد سیستم‌های اینترنت اشیا در یک شبکه واحد: یکی از دلایل نگرانی امنیت اینترنت اشیا افزایش اتصال انواع دستگاه‌های اینترنت اشیا به شبکه است. در این شرایط، در صورت عدم ایمن‌سازی مناسب سطح وسیع‌تری از حمله صورت می‌گیرد.

## راهکارهای امنیتی در اینترنت اشیا:

در IoT حفاظت از داده‌های کاربران بسیار مهم است. بدین منظور سیستم‌های اینترنت اشیا باید از نظر امنیتی امکان تشخیص بدافزارها یا تهدیدها را داشته باشند و پروتکل‌های امنیتی استاندارد را رعایت

[1] Internet of Thing (IoT)

نمایند. در غیر این صورت کل یک سیستم می‌تواند توسط اتصال یک دستگاه غیرمجاز به خطر بیفتد. ریسک‌ها و خطرات ممکن شامل حفاظت از کلان داده‌های تولید شده و داده‌های ضروری که قدرت و فواید اینترنت اشیا را افزایش می‌دهند، می‌باشد که این ضرورت را ایجاد می‌کند در لایه طراحی سیستم‌های مختلف ، تمامی موارد امنیتی را لحاظ نمود. مهم ترین ابعاد در بکارگیری راهکارهای امنیتی در اینترنت اشیا در شکل زیر نمایش داده شده است [۱۵-۱۳]:




شکل۱. ابعاد راهکارهای امنیتی در اینترنت اشیا

باوجود تفاوت نقش هریک از صنایع در امنیت اینترنت اشیا، تمام آن‌ها می‌توانند از یک‌سری دستورالعمل‌های مشترک برای ارزیابی و رسیدگی به مسائل احتمالی چالش‌های اینترنت اشیا استفاده کنند. در ادامه به بررسی این مسئله پرداخته شده است [۱۴-۱۶]:

کشف و طبقه‌بندی مناسب دستگاه‌هایIoT : تمام ذی‌نفعان باید برای کشف دستگاه‌های غیرمجاز ظاهرشده در یک شبکه اینترنت اشیا بکوشند. داشتن اطلاعات دقیق برای درک و طبقه‌بندی این دستگاه‌ها بسیار حیاتی است.

پیگیری مداوم رفتار دستگاه: پس از کشف تمام سیستم‌های موجود در یک شبکه اینترنت اشیا توسط تیم امنیتی، می‌بایست نقش موردنظر هر دستگاه جهت پیش‌بینی الگوهای رفتاری دستگاه مشخص گردد.

ارزیابی ریسک: برای ارزیابی دقیق ریسک، ذی‌نفعان باید مشخصات میزان ریسک را برای هر دستگاه ارائه‌شده در شبکه‌های خود، معین کنند. سپس، حوادث امنیتی را به‌طور مناسب اولویت‌بندی کنند و در صورت وجود آسیب‌پذیری امنیتی برای دستگاهی که مدیریت می‌کنند، بدانند که ابتدا کدام دستگاه‌ها باید به‌روز شوند.

اعمال سیاست‌گذاری: مسئول امنیت باید برای محافظت‌از دستگاه‌های پرخطر، آسیب‌پذیر یا مهم ماموریت از سایر شبکه‌ها تعیین کنند و نحوه برقراری ارتباط هر دستگاه را کنترل کنند. دسترسی به سایر منابع شبکه را مدیریت کنند و از ارزیابی و ایمنی دستگاه‌های جدید در بی‌درنگ اطمینان حاصل کنند.

امنیتAPI : APIها ستون فقرات بیشتر وب‌سایت‌های پیچیده هستند و امنیت آنها باید بصورت مداوم ردیابی گردد.

کنترل دسترسی به شبکه: کنترل دسترسی به شبکه می‌تواند به شناسایی و موجودی دستگاه‌های IoT متصل به شبکه کمک کند. این‌یک خط پایه برای ردیابی و نظارت بر دستگاه‌ها فراهم می‌کند می‌تواند به امنیت اینترنت IOT بسیار کمک کند.

تقسیم‌بندی دستگاه‌ها: دستگاه‌های اینترنت اشیا که نیاز به اتصال مستقیم به اینترنت دارند باید به شبکه‌های خود تقسیم شوند و دسترسی محدود به شبکه سازمانی داشته باشند.

دروازه‌های امنیتی: دروازه‌های امنیتی که به‌عنوان واسطه بین دستگاه‌های اینترنت اشیا و شبکه عمل می‌کنند، نسبت به خود دستگاه‌های اینترنت اشیا، قدرت پردازش، حافظه و قابلیت‌های بیشتری دارند، که به آن‌ها امکان پیاده‌سازی ویژگی‌هایی مانند فایروال‌ها را می‌دهد تا اطمینان حاصل شود که هکرها نمی‌توانند به دستگاه‌های اینترنت اشیا که متصل می‌شوند دسترسی پیدا کنند.

مدیریت و به‌روزرسانی مداوم نرم‌افزار و ضدویروس ها: بسیار مهم است که ابزاری برای به‌روزرسانی نرم‌افزارها از طریق اتصالات شبکه یا از طریق اتوماسیون فراهم شود. افشای هماهنگ آسیب‌پذیری‌ها نیز برای به‌روزرسانی دستگاه‌ها در اسرع در امنیت اینترنت اشیا وقت مهم است.

## نتیجه گیری

اینترنت اشـــیا یکی از مباحث روز در عصـــر جدید فناوری اطلاعات و ارتباطات می باشد که با فراگیر شدن کاربرد آن در حوزه های کاربردی مختلف، م سئله امنیت و حریم خ صو صی آن توجه زیادی را به سمت خود جلب نموده ا ست و به مو ضوعی بحث برانگیز در این حوزه تبدیل شده ا ست. با توجه به اینکه در آینده نه‌چندان دور از اینترنت ا شیا، در برنامه‌های کاربردی مانند مراقبت پزشـــکی (نظارت بر بیمار از راه دور، نظارت بر ســـالمندان)، شـــبکه هوشـــمند، اتوماســـیون خانگی (امنیتی، گرمایشـــی، رعد و برق) و شـــهرهای هوشـــمند (پایش آلودگی، حوادث

غیرمترقبه) ا ستفاده خواهد شد، باید چهارچوب منا سب این سامانه‌ها طراحی شود. این قراردادها باید قابلیت اطمینان و امنیت بالایی دا شته با شند تا بتوانند در مقابل نفوذ و حملات به سیستم‌ها مقاومت نمایند. بنابراین، با توجه به اهمیت حوزه امنیت در اینترنت ا شیا، در این مقاله سعی شد چالش‌ها و مشکلات امنیتی این فنّاوری به دقت مورد بررسی قرار گیرد و راهکارهای بنیادین مطرح گردد.

## منابع


[1] Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, *10*(4), 2233-2243.

[2] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC)*, *80*, 1-50.

[3] Sahmim, S., & Gharsellaoui, H. (2017). Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review. *Procedia computer science*, *112*, 1516-1522.

[4] Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(05), 164.

[5] Jose, D. V., & Vijyalakshmi, A. (2018). An overview of security in Internet of Things. *Procedia computer science*, *143*, 744-748.

[6] Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: a survey. *Information systems frontiers*, *17*(2), 243-259.

[7] Wei, W., Yang, A. T., Shi, W., & Sha, K. (2016, October). Security in internet of things: Opportunities and challenges. In *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)* (pp. 512-518). IEEE.

[8] Sadique, K. M., Rahmani, R., & Johannesson, P. (2018). Towards security on internet of things: applications and challenges in technology. *Procedia Computer Science*, *141*, 199-206.

[9] Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*(3), 423-441.

[10] Kouzinopoulos, C. S., Spathoulas, G., Giannoutakis, K. M., Votis, K., Pandey, P., Tzovaras, D., & Nijdam, N. A. (2018, February). Using blockchains to strengthen the security of internet of things. In *International ISCIS Security Workshop* (pp. 90-100). Springer, Cham.

[11] Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on emerging topics in computing*, *5*(4), 586-602.

[12] Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772-5781). IEEE.

[13] Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review*, *38*, 100312.

[14] Ukil, A., Sen, J., & Koilakonda, S. (2011, March). Embedded security for Internet of Things. In *2011 2nd National Conference on Emerging Trends and Applications in Computer Science* (pp. 1-6). IEEE.

[15] Oracevic, A., Dilek, S., & Ozdemir, S. (2017, May). Security in internet of things: A survey. In *2017 international symposium on networks, computers and communications (ISNCC)* (pp. 1-6). IEEE.

[16] Tahsien, S. M., Karimipour, H., & Spachos, P. (2020). Machine learning based solutions for security of Internet of Things (IoT): A survey. *Journal of Network and Computer Applications*, *161*, 102630.

[17] Sain, M., Kang, Y. J., & Lee, H. J. (2017, February). Survey on security in Internet of Things: State of the art and challenges. In *2017 19th International conference on advanced communication technology (ICACT)* (pp. 699-704). IEEE.

[18] Aldowah, H., Ul Rehman, S., & Umar, I. (2018, June). Security in internet of things: issues, challenges and solutions. In *International conference of reliable information and communication technology* (pp. 396-405). Springer, Cham.

[19] Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of Things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5-484). IEEE.