Arman Process Journal
(APJ)
Homepage: www.armanprocessjournal.ir

Functions of the Security Dimensions in the Internet of Things

Gh. Vatanian*[*,1],

[1] *Computer Science Department, Islamic Azad University, Science and Resaerch Branch, Tehran, Iran*

Received: 15 June 2022
Accepted: 29 Septebber 2022

KEYWORDS:

Internet of Thing

Security

Information Technology

Protocol

ABSTRACT

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. Internet of Things security is a subset of cybersecurity that focuses on protecting, monitoring and remediating threats related to the Internet of Things, or the network of connected devices that collect, store, and share data over the Internet. IoT security challenges can be very controversial because many IoT devices are not built with strong security. Security risk in IoT is critical because the sensitivity of the data IoT devices collect and store, as well as the systems they manage, is much greater than traditional personal network security strategies. In this article, we discuss the functions of the security aspects of the Internet of Things.

[1] Corresponding author
ghvatanian@yahoo.com

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
14	0	0

نشریه تخصصی آرمان پردازش، دوره ۳، شماره ۲، تابستان ۱۴۰۱

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

کارکردهای ابعاد امنیتی اینترنت اشیاء

غلامرضا وطنیان[*،1]،

[1] گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران

چکیده

اینترنت اشیا سیستمی از دستگاه‌های محاسباتی مرتبط، ماشین‌های مکانیکی و دیجیتال، اشیاء یا افرادی است که با شناسه‌های منحصربه‌فرد و توانایی انتقال داده‌ها از طریق شبکه بدون نیاز به ارتباط انسان به انسان ارائه می‌شوند. امنیت اینترنت اشیا زیرمجموعه‌ای از حوزه 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. اساسا چالش‌های اینترنت اشیا درزمینه امنیت می‌تواند بسیار بحث‌برانگیز باشد زیرا بسیاری از دستگاه‌های اینترنت اشیا با امنیت قوی ساخته نشده‌اند. از این رو خطرات و تهدیدات امنیتی در اینترنت اشیا بسیار حیاتی می باشند، زیرا حساسیت داده‌هایی که دستگاه‌های اینترنت اشیاء جمع‌آوری و می‌کنند و همچنین سیستم‌هایی که آن‌ها مدیریت می‌کنند، به‌مراتب بیشتر از استراتژی‌های مرتبط با امنیت شبکه شخصی و سنتی است. در این مقاله به کارکردهای ابعاد امنیتی اینترنت اشیا می پردازیم.

واژگان کلیدی:

اینترنت اشیا

امنیت

فناوری اطلاعات

پروتکل

تعداد جداول	تعداد شکل ها	تعداد مراجع
۰	۰	۱۴

مقدمه

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 [۱] . خطر امنیت در اینترنت اشیا بیشتر است زیرا حساسیت داده‌هایی که دستگاه‌های اینترنت اشیاء جمع‌آوری و می‌کنند و همچنین سیستم‌هایی که آن‌ها مدیریت می‌کنند، به‌مراتب بیشتر از استراتژی‌های مرتبط با امنیت شبکه شخصی و سنتی است. امنیت در اینترنت اشیا به علت چندلایه بودن زیرساخت‌های آن، پیچیده بوده و از اهمیت ویژه‌ای برخوردار است [۳-۲]. گاها، به برخی از این فرایندهای امنیتی تمرکز بیشتری می‌شود. به‌عنوان‌مثال، مرکز عملیات امنیتی(SOC)، شناسایی و به‌روزرسانی نرم‌افزار دستگاه‌های IoT را مدیریت می‌کند. با این حال، سایر جنبه‌های امنیت در اینترنت اشیا، مانند آزمایش API ها برای آسیب‌پذیری و اطمینان از رمزگذاری داده‌ها، به ابزارهای اضافی نیاز دارند.

چالش‌های اینترنت اشیا

اینترنت اشیا یکی از نوین ترین سیستم های تکنولوژی بوده که از آن با تحت عنوان انقلاب چهارم صنعتی یاد می شود. در حوزه اینترنت اشیاء با جهانی روبرو هستیم که در آن سازندگان کالای خود را با استانداردهای خاص خود عرضه می کنند و مشخص نیست با تداوم این گوناگونی، میلیارد ها وسیله ای که پیکره اینترنت اشیاء را تشکیل می دهند آینده این شبکه را به کدام سمت هدایت خواهند کرد. لذا، دستگاه‌های اینترنت اشیاء همواره در معرض چالش‌ها و آسیب‌پذیری‌های امنیتی ذاتی هستند. در ادامه مهم ترین چالش‌های اینترنت اشیا درزمینه امنیت بصورت خلاصه توضیح داده شده است [۶-۴]:

- خطر وجود دستگاه‌های سایه یا دستگاه‌هایی است که به شبکه اینترنت اشیا متصل هستند اما توسط صاحب شبکه مجاز یا شناخته‌شده نیستند [۸-۷].
- عدم به‌روزرسانی نرم‌افزارهای قابل‌اعتماد
- آسیب‌پذیری واسط های اینترنت اشیاء
- رمزهای پیش‌فرض
- عدم وجود استاندارد واحد وسعت بی رویه تعداد سیستم‌های اینترنت اشیا در یک شبکه واحد
- عدم امنیت اعتبار ورودی پیش‌فرض
- به‌روز رسانی ضعیف نرم‌افزاری
- عدم رمزگذاری ارتباطات
- رابط کاربری ناامن
- حفاظت ضعیف از حریم خصوصی
- سوءاستفاده از آسیب‌پذیری‌ها
- سر ریز بافر
- تزریق کد
- تزریق اسکریپت از طریق وب‌سایت
- حمله از طریق بدافزار
- حملات رمزعبور
- اسنیفینگ یا حملات با واسطه انسان
- اسپوفینگ یا ظاهرسازی سایبری(Spoofing)
- کنترل بات‌نت
- دسترسی و کنترل از راه دور
- نشت اطلاعاتی
- عدم وجود راه‌حل برای فیلتر ترافیک با ایمنی پایین

برای رفع چالش های اینترنت اشیا روش ها و معیارهای مختلفی پیشنهاد شده است. در ادامه مقاله به برخی از مهم ترین این راهکارها درجهت بهبود امنیت در حوزه اینترنت اشیا می پردازیم.

بهبود امنیت در اینترنت اشیا

امنیت اینترنت اشیاء و حریم شخصی به طور گسترده ای از مسائل مهم در زمینه فناوری اینترنت اشیاء شناخته شده اند. از یک طرف، محرمانه بودن و یکپارچگی اطلاعات منتقل شده و ذخیره شده باید تضمین گردد، و احراز هویت و مکانیزم های صدور مجوز برای جلوگیری از دسترسی نادرست و ناشایست کاربران و یا دستگاه های غیر مجاز نادرست فراهم گردد. از سوی دیگر، حریم خصوصی کاربران، به عنوان توانایی پشتیبانی از حفاظت داده ها و گمنام ماندن کاربران باید به عنوان یک جنبه اساسی به ویژه در ارائه اطلاعات حساس و یا شخصی در نظر گرفته شود. در ادامه به مهم ترین راهکارها درجهت بهبود ابعاد امنیتی در حوزه اینترنت اشیا اشاره خواهیم داشت [۱۴-۹]:

- اطمینان از آسیب‌پذیری و صحت به‌روزرسانی نرم‌افزار اجراشده بر روی دستگاه‌های IoT
- محافظت از آسیب‌پذیری API های برقرارکننده ارتباط در دستگاه‌های اینترنت اشیا

- نظارت بر نفوذ شبکه‌های اینترنت
- ذخیره‌سازی ایمن داده‌های جمع‌آوری‌شده در دستگاه‌های IoT یا بارگیری شده در مرکز داده
- تغییر گذرواژه‌ها و نام‌های کاربری پیش‌فرض
- نصب آخرین به‌روزرسانی نرم‌افزاری روی تجهیزات IoT
- اعمال تنظیمات قفل ورود به سیستم
- احراز هویت دومرحله‌ای و رمزگذاری
- ایجاد یک شبکه ثانویه برای دستگاه‌های IoT
- ایمن‌سازی Wi-Fi خانگی
- عدم اتصال دائمی دستگاه به اینترنت
- کشف و طبقه‌بندی مناسب دستگاه‌های IoT
- پیگیری مداوم رفتار دستگاه
- نوع داده‌های تولیدشده
- زمان آنلاین و آفلاین شدن
- ارزیابی ریسک
- اعمال سیاست‌گذاری درخصوص استانداردسازی امنیت
- تریاژ و اولویت‌بندی هشدار و شکار تهدید مدیریت شده
- ادغام اطلاعات تهدید
- به‌روزرسانی نرم‌افزار و سیستم‌عامل
- تصویب اعتبارنامه
- احراز هویت دستگاه

در نهایت لازم به ذکر است، پیچیدگی ذاتی اینترنت اشیاء، که در آن نهادهای ناهمگن متعدد واقع در زمینه های مختلف می توانند اطلاعات را با یکدیگر مبادله کنند، پیچیدگی های بیشتر طراحی و بکارگیری مکانیزم های امنیتی کارآمد، سازگار و مقیاس پذیر را می طلبد. در اینترنت اشیاء، ابزار اصلی کانال ارتباطی، اینترنت است. بنابراین، برنامه های کاربردی اینترنت اشیاء باید از هر دو حمله کننده های فعال و غیر فعال حفاظت شوند. علاوه بر امنیت اینترنت، زیرساخت اینترنت اشیاء باید امنیت اینترانت، امنیت داده ها، امنیت نرم افزار، امنیت سخت افزار و امنیت فیزیکی ارائه کند. با داشتن اینترنت اشیاء می توان پیش بینی کرد که مجرمان سایبری در مرحله اول به نقاط به وجود آمدن و انتقال اطلاعات، مراکز ارسال دستورات، نقاط و مدخل های شبکه حمله خواهند نمود . پس محافظت را باید برای این نقاط فراهم نمود. با توجه به نفوذ فناوری اینترنت اشیاء در تمامی ابعاد زندگی و تهدید افراد توسط بدافزارها، استفاده از یک معماری امن برای مقابله با این تهدیدات مورد توجه قرار می گیرد. یکی از مکانیزم های ایجاد امنیت در اینترنت اشیاء بهره گیری از معماری مناسب می باشد.

نتیجه گیری

امروزه مسأله امنیت اینترنت اشیا نیز به یکی از بزرگ‌ترین دغدغه‌های تکنولوژی برای کارشناسان امنیتی تبدیل شده است. متأسفانه تکنولوژی‌های هوشمند مبتنی بر اینترنت اشیا در عین حال که جذاب هستند، فرصت‌هایی ارایه می‌دهند که مجرمان سایبری به راحتی قادر به هک وسایل و تجهیزات هوشمند خواهند بود. حریم خصوصی و امنیت از مهمترین چالشهای اینترنت اشیا (IoT)است. به روزرسانی های نادرست دستگاه ، کمبود پروتکل های امنیتی موثر و قوی ، عدم آگاهی کاربر و نظارت بر دستگاه فعال از جمله چالش هایی است که IoT با آن روبرو است. در این مقاله به طور مختصر به چالشهای اساسی امنیتی در اینترنت اشیا پرداخته و این موضوع را از جنبه های مختلف مورد بررسی قرا دادیم. در ادامه چندین مسئله امنیتی اینترنت اشیا، تهدیدات و مخاطرات موجود در حوزه امنیت و حریم خصوصی را تشریح نموده و راه حل هائی برای ارتقا امنیت در اینترنت اشیا را ارائه نمودیم.

منابع و مآخذ

[1] Zhang, C., & Green, R. (2015, April). Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. In

Proceedia Computer Science, *201*, 437-444.

[10] Dammak, M. (2021). *Authentication and authorization security solution for the internet of thing* (Doctoral dissertation, Université Bourgogne Franche-Comté; Université de la Manouba (Tunisie)).

[11] Viriyasitavat, W., Da Xu, L., Bi, Z., & Hoonsopon, D. (2021). User-Oriented Selections of Validators for Trust of Internet-of-Thing Services. *IEEE Transactions on Industrial Informatics*, *18*(7), 4859-4867.

[12] Zhang, G., & Xie, J. (2019, July). Blockchain-enabled security-aware applications in home internet of thing. In *2019 International Conference on Communications, Information System and Computer Engineering (CISCE)* (pp. 559-565). IEEE.

[13] Dagnaw, G. A., & Tsige, S. E. (2019). Impact of Internet of Thing in Developing Country: Systematic Review. *Internet Things Cloud Comput*, *7*(3), 65.

[14] Nizami, Y., & Garcia-Palacios, E. (2014). Internet of thing. A proposed secured network topology.

Proceedings of the 18th symposium on communications & networking (pp. 8-15).

[2] Ouaddah, A., Bouij-Pasquier, I., Abou Elkalam, A., & Ouahman, A. A. (2015, March). Security analysis and proposal of new access control model in the Internet of Thing. In *2015 international conference on electrical and information technologies (ICEIT)* (pp. 30-35). IEEE.

[3] Tanwar, S., Patel, P., Patel, K., Tyagi, S., Kumar, N., & Obaidat, M. S. (2017, July). An advanced internet of thing based security alert system for smart home. In *2017 international conference on computer, information and telecommunication systems (CITS)* (pp. 25-29). IEEE.

[4] Rueda-Rueda, J. S., & Portocarrero, J. M. (2021). Framework-based security measures for Internet of Thing: A literature review. *Open Computer Science*, *11*(1), 346-354.

[5] Alreshidi, A., & Ahmad, A. (2019). Architecting software for the internet of thing based systems. *Future Internet*, *11*(7), 153.

[6] Khalid, A. (2016). Internet of Thing architecture and research agenda. *International Journal of Computer Science and Mobile Computing*, *5*(3), 351-356.

[7] Shadeed, M., & Moreb, M. (2021, July). Lightweight Encryption for Multimedia in the Internet of thing (iot). In *2021 International Conference on Information Technology (ICIT)* (pp. 27-32). IEEE.

[8] Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *2012 international conference on computer science and electronics engineering* (Vol. 3, pp. 648-651). IEEE.

[9] Albany, M., Alsahafi, E., Alruwili, I., & Elkhediri, S. (2022). A review: Secure Internet of thing System for Smart Houses.