**به نام خدا**

**ابعاد امنیتی اینترنت اشیاء چه اهمیتی در عملکرد اشیاء هوشمند دارند؟**

اینترنت اشیاء (IoT) با ایجاد شبکه‌ای میان اشیاء، نحوه استفاده از آن‌ها را آسان‌تر و قابل کنترل‌تر می‌نماید. اینترنت اشیاء را می‌توان در تجهیزات خانگی، کارخانه‌ای و صنعتی، سازمان‌ها و ادارات و یا دستگاه‌های سطح شهر ایجاد نمود. توجه به ابعاد امنیتی اینترنت اشیاء، موضوعی بسیار مهم در این حوزه است.

# ****تهدیدات امنیتی IoT چیست؟****

توقع بر این است که تا سال ۲۰۲۵ بیشتر از پنجاه میلیارد از وسایل بشر به اینترنت متصل باشند. این پدیده در ظاهر موضوعی جذاب و حیرت‌آور است اما در کنار پیشرفت‌های علمی خیره کننده و محاسن بسیارش، امنیت IoT با تهدیدات و چالش‌های عدیده‌ای روبه‌رو است. به عنوان مثال می‌توان موارد ذیل را برشمرد:

1. عدم توافق بین‌المللی در اجرای استانداردها و اقدامات مربوط به امنیت اینترنت اشیاء.
2. جمع آوری اطلاعات شخصی کاربر بر روی حسگرها و ضعف در حفظ این اطلاعات.
3. عدم قابلیت وصله زدن (patch) در تعداد زیادی از دستگاه‌هایی که اینترنت اشیاء دارند، باعث می‌شود تا در معرض خطر همیشگی قرار گیرند. نبود امنیت موروثی باعث به خطر افتادن آن‌ها به صورت زنجیره‌وار می‌شود و مسیر دست‌یابی به اطلاعاتشان توسط بات نت‌های بزرگ را هموار می‌سازد.
4. وجود هزاران وبکم و ساعت هوشمند کودکان با درجه امنیت بسیار پایین به بسیاری از هکرها این امکان را داده است تا موقعیت کاربران را ردیابی نمایند، مکالمات آن‌ها را بشنوند و حتی با آن‌ها تماس برقرار نمایند. در واقع قیمت پایین اشیاء هوشمند کوچک، امنیت آن‌ها را تحت الشعاع قرار داده است.
5. متصل شدن ماشین‌های صنعتی به اینترنت، زمینه را برای حمله‌ی سایبری هکرها فراهم می‌سازد. به وجود آمدن نوع جدیدی از جاسوسی به نام جاسوسی صنعتی و حملات تخریب کننده به زیرساخت های اساسی، از خطرات احتمالی حضور اینترنت اشیاء در صنعت است.
6. وجود مسیرهای ناامنِ اینترنت اشیاء در سازمان‌ها، ادارات و اماکنی از این قبیل به نفوذگران این امکان را می‌دهد تا به راحتی به اطلاعات محرمانه آن‌ها در روندهای تجاری، مالکیت‌های معنوی و اطلاعات مشتریان دست یابند.

## **سه اصل مهم اینترنت اشیاء**

* **محرمانگی** **:**این اصل مانع از شنود می‌شود.
* **صحت:** ما را مطمئن می‌سازد که تبادل پیام‌ها میان دستگاه‌های IoT به وسیله هکرها دستکاری نشده است.
* **در دسترس بودن:** این اطمینان خاطر را به ما می‌دهد که تجهیزات IoT از دسترس خارج نشده‌اند و به درستی در حال انجام مأموریت خود هستند.

نکته شایان اهمیت این است که میزان برقراری امنیت در تمام اشیاء یکسان نمی‌باشد و بر اساس میزان کارکرد اشیاء متفاوت است.

## **روش‌های عملکرد بهتر در ابعاد امنیتی اینترنت اشیاء**

1. استفاده از شیوه‌های احراز هویت جدید با به‌کارگیری تجربه الگوریتم‌های رمزنگاری – اعتبار سنجی قوی.
2. استفاده از موقعیت جغرافیایی اشیاء.
3. به‌کارگیری شناسه‌های قدرتمند.
4. ارتقاء سیستم نام دامنه (DNS) با استفاده از DHCP و DNSSEC به منظور جلوگیری از حملات سایبری.
5. استفاده از تکنولوژی امنیت لایه‌ای.

صنعت جدید اینترنت اشیاء، مدام در حال تغییر و به‌روزرسانی است. نکته‌ای که معماران شبکه را با نگرانی و چالش روبه‌رو می‌سازد عدم رشد تکنولوژی امنیت اشیاء همزمان با سرعت ارتقاء این صنعت است. مدل‌های امنیتی طراحی شده با طراحی‌های جدید شبکه در IoT ،کارایی خود را از دست می‌دهند و زمینه هک شدن اطلاعات را فراهم می‌سازند.