مروری بر امنیت در اینترنت اشیاء

شکوفه خوش‌نظر[۱]

[۱] مربی، دانشگاه ولایت، ایرانشهر، Sh.khoshnazar@velayat.ac.ir

چکیده

هدف از ایجاد و گسترش فناوری اینترنت اشیاء، توانمندسازی اشیاء برای اتصال به شیء دیگر است. برای پیاده‌سازی چنین هدفی چالش-های بسیاری وجود دارد که یکی از مهمترین آنها چالش‌های امنیتی است. در اینترنت اشیاء، هر دستگاه متصل می‌تواند یک درگاه احتمالی به زیرساخت اینترنت اشیاء و یا داده‌های شخصی باشد. نگرانی‌های امنیت و حریم خصوصی داده بسیار مهم هستند، اما با ورود پیچیدگی، نقاط ضعف امنیتی و آسیب‌پذیری‌های احتمالی در مواردی مانند تصمیم‌گیری‌های خودگردان، خطرات احتمالی مربوط به اینترنت اشیاء سطح جدیدی به خود گرفته‌اند. در این مقاله، به بررسی اینترنت اشیا، مزایا و چالش‌های پیش‌روی آن و معرفی برخی راه‌ها برای این چالش امنیت پرداخته‌شده‌است.

واژه های کلیدی

اینترنت اشیا، امنیت، حریم خصوصی، بلاکچین.

مقدمه

در سال‌های اخیر در زمینه‌ی ارتباطات راه دور و بی‌سیم موضوع جدیدی به نام اینترنت اشیاء به وجود آمده که توسط اشتون در سال ۱۹۹۱ در یک سخنرانی معرفی شده‌است. او جهانی را توصیف کرد که در آن هر چیزی، ازجمله اشیاء بی‌جان برای خود هویت دیجیتال داشته‌باشند. اینترنت اشیاء سطح ارتباطات را کاملا بالا برده، زیرساخت‌های فیزیکی را با زیرساخت‌های فناوری اطلاعات اتصال می‌دهد. همچنین، اجازه می‌دهد تمامی اشیا به اینترنت وصل شده و به تبادل داده بپردازند. وقتی همه چیز به هم متصل شود، اشیاء بی‌جان هم صاحب ذهن می-شود و تجهیزات هم قابلیت تبادل داده و هوشمندی پیدا می‌کنند. این پدیده باعث می‌شود تا تفاوت بین انسان و ماشین محو شود. در واقع در مفهوم اینترنت اشیاء، بسیاری از اشیایی که در محیط ما قرار دارند در یک قالب مشخص به یک شبکه متصل می‌شوند. اینترنت اشیاء، شبکه-هایی از اشیاء فیزیکی و مجازی متصل به اینترنت است که امکان دستیابی به آن از طریق اینترنت فراهم می‌گردد. اشیاء متصل شده از فناوری‌های تعبیه شده درون خود نظیر حسگرها استفاده می‌نمایند تا بتوانند چیزی را حس کرده و آن را مبادله نمایند. این قابلیت، نظام تصمیم‌گیری را در حوزه‌های مختلفی تحت تأثیر خود قرار داده‌است. [۱]

با توجه به پیشرفت‌های اخیر شاهد ساخت تجهیزاتی هستیم که علاوه بر اینکه سیار هستند، پوشیدنی بوده و یا دستگاه‌های ادغام شده ای با حافظه و قدرت پردازشی بالا و مجهز به تکنولوژی‌های حسگر متنوع هستند. افزایش کارایی دستگاه‌های مرتبط با اینترنت اشیاء منجر به ارائه خدمات بیشتر و بهتر به کاربر نهایی خواهدشد. در حال حاضر فناوری اینترنت اشیاء کاربردهایی نظیر موارد زیر را هر چه بیشترگسترش می‌دهد:

- خانه های هوشمند (کنترل محیطی و لوازم هوشمند)
- شهر هوشمند (کنترل منابع مثلا روشنایی معابر، مدیریت زباله، مدیریت آب و انرژی، کنترل ترافیک و ...)
- صنعت (کنترل فرآیند)
- ساختمان‌سازی (مدیریت ساخت هوشمند)
- خدمات موقعیت، مدیریت و نظارت بر سلامت و ... [۲]

در اینترنت اشیا از دستگاه‌های مختلفی استفاده می‌شود که ممکن است با تکنولوژی‌های ارتباطی متفاوتی با یکدیگر در حال تعامل باشند. همین امر چالش‌های مختلفی را از نظر امنیتی به دنبال خواهد داشت. برخی از مهم‌ترین چالش‌ها عبارتند از:

- نیاز به ایمن‌سازی دستگاه‌های متفاوت به دلیل استفاده از فناوری-ها و دستگاه‌های متعدد که هر کدام آسیب‌پذیری‌های خاص خود را دارند.

- عدم امکان استفاده از مکانیزم‌های دفاعی متمرکز به دلیل قابلیت مقیاس‌پذیری و گسترده بودن دستگاه‌های اینترنت اشیا.

- متفاوت بودن نیازمندی‌های امنیتی دستگاه‌های مختلف به دلیل کاربرد متفاوت هرکدام در سطح کاربر، دولت و سازمان ها.

- افزایش میزان داده‌ها و اطلاعات و نیاز به مکانیزم امنیتی قوی برای جلوگیری از وقوع مشکل برای داده‌ها.

- نیاز به حفاظت در برابر حملاتی که سرویس‌دهی را دچار اختلال زمانی می‌کنند برای دستگاه‌هایی که به سرویس‌دهی با حداقل تاخیر نیاز دارند.

- پیش‌بینی حملات سایبری به منظور جلوگیری از انجام یا وقوع آنها روی دستگاه‌ها یا شبکه اینترنت اشیا.

به طورکلی هدف از انجام این پژوهش، تأکید بر اهمیت امنیت در عرصه اینترنت اشیا است که می‌بایست از ابتدای کار توجه ویژه‌ای به آن نمود، زیرا نیمی از وظیفه حفظ امنیت بر عهده زیرساخت‌های مناسب و مابقی بر عهده رابط کاربری است. به منظور دستیابی به امنیت موردنیاز لازم است به تمامی مواردی که موجب دستیابی به این امر می‌گردد به یک میزان توجه نمود. به عنوان مثال می‌توان گفت که نجات جان بشر از کاربردهای راه صحیح استفاده از علم است درحالی‌که ساخت بمب اتم عکس این موضوع است، حال اگر همین را به اینترنت اشیا بسط دهیم متوجه اهمیت حفظ و ارتقا امنیت در این فنّاوری خواهیم شد.

امنیت در اینترنت اشیاء

گرچه اینترنت اشیا، کیفیت زندگی مردم و روال کاری سازمان‌ها را بهبود می‌بخشد، اما بستری آسیب‌پذیر در برابر حمله احتمالی هکرهاست. مطالعات نشان می‌دهد که بیش از نیمی از دستگاه‌های اینترنت اشیاء موجود در دنیا در معرض آسیب‌های امنیتی هستند. برخی از دستگاه‌های اینترنت اشیا به علت عدم رمزگذاری انتقال، رابط وب ناامن و عدم حفاظت کافی از نرم‌افزار، آسیب‌پذیرند. برخی از برنامه‌های اینترنت اشیا از زیرساخت‌های حساس و خدمات استراتژیک مانند شبکه‌های هوشمند و حفاظت از تأسیسات پشتیبانی می‌کنند و تعدادی از اپلیکیشن‌های اینترنت اشیا مقدار زیادی از اطلاعات شخصی در مورد خانواده، سلامت و وضعیت مالی فرد را جمع‌آوری می‌کنند. رعایت نشدن نکات امنیتی و بی‌توجهی به حریم خصوصی سبب ایجاد مقاومت در پذیرش اینترنت اشیا توسط افراد و سازمان‌ها خواهد بود.

اینترنت اشیاء در برگیرنده چند فناوری نظیر شناسه امواج رادیویی (RFID) و شبکه‌های حسگر بیسیم، محاسبات ابری و مجازی‌سازی است که هرکدام آسیب‌پذیری‌های خاص خود را دارند و برای امنیت اینترنت اشیاء باید تمام زنجیره این فناوری را امن نمود. فناوری اینترنت اشیاء کاربردهای متنوعی در حوزه‌های سلامت، صنعت، ساختمان‌های هوشمند و شهرهای هوشمند داشته و هر یک از این کاربردها، نیازهای امنیتی خاص خود را دارند.

با بررسی مقالات و کتاب‌هایی که در حوزه امنیت اینترنت اشیاء ارائه شده‌اند، می‌توان دریافت که امنیت باید در تمام سطوح بسته‌ها و سرویس‌ها نیز در نظر گرفته شود. بنابراین در تمام مراحل توسعه سیستم، ویژگی‌های امنیتی وجود خواهند داشت.

به این نوع توسعه امنیت، رویکرد "دفاع در عمق" گفته می‌شود. این رویکرد، امنیت را در دل شبکه اینترنت اشیاء گنجانده و به سازمان‌ها و شرکتها اجازه می‌دهد تا با درگیر کردن مهاجمین به صورت لایه به لایه، زمان بیشتری برای دفاع از منابع خود داشته‌باشند[۳].

چشم اندازها و چالش‌های امنیت در اینترنت اشیاء

در این قسمت به چالش‌های موجود در راستای اجرای موثر امنیت در فناوری اینترنت اشیاء پرداخته می‌شود.

- **تجهیزات ناهمگن**

با توجه به محدوده دستگاه‌های ناهمگن که از دستگاه‌های کوچک و کم قدرت دارای حسگر آغاز و به سیستم‌ها و زیرساخت‌های 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 اینترنت اشیاء 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 اینترنت اشیاء به کار برده می‌شوند[۴].

- **قابلیت همکاری پروتکل‌های امنیتی**

جهت استانداردسازی امنیت جهانی به منظور استفاده در اینترنت اشیاء پروتکل‌هایی که در لایه‌های مختلف اجرا می‌شوند، باید فرآیندهایی 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 محدودیت های معماری تعریف شود.

- **نقاط شکست**

با وجود شبکه‌ها، معماری‌ها و پروتکل‌های ناهمگن، معماری و الگوهای مطرح در حوزه اینترنت اشیاء به نقاط تک نقطه‌ای

آسیب‌پذیرتر از سایر الگوها تبدیل می‌شود [۴]. میزان قابل توجهی از کارهای تحقیقاتی لازم است تا جهت اطمینان از دسترسی مناسب به عناصر و تجهیزات زیرساختی اینترنت اشیاء مخصوصا برای برنامه‌های کاربردی حیاتی انجام پذیرد. این امر به استانداردهایی نیاز دارد تا افزونگی را با توجه به مبادلات موجود میان هزینه‌ها و قابلیت اطمینان کل زیرساخت در نظر بگیرد.

- **آسیب‌پذیری‌های سخت‌افزاری و میان افزاری**

با فراگیری استفاده از دستگاه‌های کم‌هزینه، معماری اینترنت اشیاء بیشتر در معرض آسیب‌های سخت‌افزاری قرار می‌گیرد. این امر تنها به عملکرد فیزیکی تجهیزات محدود نشده و پیاده‌سازی الگوریتم‌های امنیتی در سخت‌افزارها، مسیریابی و فرآیندهای پردازش بسته را نیز شامل می‌شود. تشخیص و کاهش آسیب-پذیری‌هایی که پس از استقرار تجهیزات مورد سوء استفاده قرار می‌گیرد، دشوار است. بنابراین ضروری است که از یک پروتکل استاندارد، برای تایید امنیت تجهیزات اینترنت اشیاء استفاده گردد.

- **بروزرسانی و مدیریت معتبر**

یکی از مسائل مهم، به روزرسانی نرم‌افزارهای مقیاس‌پذیر و قابل اعتماد در بین میلیون‌ها دستگاه است. علاوه برآن، مسائل مربوط به امنیت، مالکیت معتبر دستگاه و حریم خصوصی داده‌ها را می‌توان به عنوان مسائل مربوط به تحقیقات در این حوزه دانست که به منظور ترویج مقررات گسترده در اینترنت اشیاء باید توسط جامعه تحقیقاتی مورد توجه قرار گیرد. فناوری بلاکچین می‌تواند برای راه‌حل‌های امنیتی اینترنت اشیاء مفید باشد. با این حال، فناوری بلاکچین به خودی خود چالش‌های تحقیقاتی را با توجه به مقیاس‌پذیری، کارایی و برخوردهای کلیدی باز می‌نماید که بایستی مورد توجه محققان قرار گیرد.

- **آسیب‌پذیری‌های بلاکچین**

با وجود ارائه رویکرد های قوی برای ایمن‌سازی، فناوری بلاکچین نیز آسیب‌پذیر است [۵]. این فرآیند بستگی به قدرت درهم‌سازی داشته و امکان اینکه مهاجم، میزبانی بلاکچین را در دست گیرد وجود دارد. به طور مشابه، کلید خصوصی با محدودیت تصادفی بودن می‌تواند برای سوء استفاده از حساب‌های بلاکچین مورد سوء استفاده قرار گیرد. لذا تحقیق در خصوص ارائه فرآیندهای موثر برای حصول اطمینان از حفظ حریم خصوصی، تراکنش‌ها و جلوگیری از حملات، بایستی مورد توجه محققان حوزه امنیت قرارگیرد.

نتیجه‌گیری

ایجاد و توسعه اینترنت اشیاء با بسیاری از مباحث امنیتی و چالش‌های زیربنایی مواجه است. از آنجا که در این فناوری ادغام حسگرها و اشیاء مختلف بدون دخالت انسان جهت برقراری ارتباط فراهم می‌شود، از این رو در نظر گرفتن پروتکل‌ها و فرآیندهایی برای ایمن‌سازی فناوری‌های ارتباطی و برنامه‌های کاربردی مورد استفاده در اینترنت اشیاء در لایه-بندی‌های دقیق‌تر بدون اعمال سربار ضروری می‌باشد. مشخصات امنیتی تجهیزات اینترنت اشیاء همیشه به دلیل تهدیدهای امنیتی جدید اعمال شده بر روی دستگاه‌ها تغییر می‌کند، از این رو امنیت اینترنت اشیاء به موضوع مهم مدیریتی تبدیل شده است. مدیریت موثر تهدیدات نیاز به ارزیابی صحیح و دقیق برای کاهش تهدیدهای شناخته شده در محیط اینترنت اشیاء دارد. طبقه‌بندی امنیت در اینترنت اشیاء باید تجزیه و تحلیل جامعی از سازوکارهای امنیتی را ارائه دهد و اینکه چگونه می‌توان از اطلاعات تمام لایه‌ها برای ارائه دهندگان سیستم و تحلیلگران جهت طراحی و تجزیه و تحلیل سیستم‌های ایمن استفاده کرد. مشکلات امنیتی در اینترنت اشیاء می‌توانند در لایه‌های مختلف رخ دهند. ویژگی‌های امنیتی مختلف از قبیل محرمانه بودن، یکپارچگی، احراز هویت، مجوزدسترسی، در دسترس بودن و حفظ حریم خصوصی، باید برای اطمینان از امنیت در کل سیستم اینترنت اشیاء تضمین شود. این هدف با توجه به ویژگی‌های محیطی اینترنت اشیاء به شدت چالش برانگیز است.

رویکردهای امنیتی اینترنت اشیاء نشان‌دهنده نیاز به طراحی یک طبقه‌بندی امنیتی جدید است که به سادگی و با دقت بیشتر برای رده-بندی تهدیدات و آسیب‌پذیریهای امنیتی در اینترنت اشیاء به کار برده شود. در این مقاله، برخی از چالش‌های امنیتی مطرح در اینترنت اشیاء تشریح شد.

چشم‌اندازها و چالش‌ها در حوزه امنیت اینترنت اشیا شامل بلاکچین، به روزرسانی و مدیریت معتبر، آسیب‌پذیری‌های سخت‌افزاری و میان‌افزاری، محدودیت‌های منابع، تجهیزات ناهمگن، قابلیت همکاری پروتکل‌های امنیتی و نقاط شکست بیان شد. در نهایت با توجه به چشم‌اندازهای امنیتی آتی در حوزه اینترنت اشیاء، استانداردسازی امنیت جهانی و یافتن تکنیک‌های رمزنگاری موثر از جمله حوزه‌های مهم و قابل تحقیق مطرحی است که قابلیت جایگزینی با راه‌کارهای محاسباتی سنتی گران قیمت مشابه را داشته باشد.

مراجع و منابع

[1] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

[۲] صانعی, ساره و دادخدازاده خبیصی, حدیثه,۱۳۹۹, " *ارائه پروتکل هایی در جهت افزایش امنیت مبتنی بر اینترنت اشیا* (IOT)", ششمین کنفرانس بین المللی راهکارهای نوین در مهندسی، علوم اطلاعات و فناوری در قرن پیش رو, تهران .

[۳] مهندس حمیدرضا ا ,مهندس عاطفه پ ,مهندس حمیدرضا خوش ا .امنیت و حریم خصوصی در اینترنت اشیاء .منادی امنیت فضای تولید و تبادل اطلاعات (افتا). ۱۳- سال ۱۳۹۴.

[4] Ahmad Khan M., Salah, Kh., IoT security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems, Volume 82, 2018.

[5] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. A survey on the security of blockchain systems. Future Generation Computer Systems. 2017.