# مروری بر روش‌های برقراری امنیت در اینترنت اشیاء

حسین محمدی[1*]، فرهاد رسولیار[2]

[1،2] پوهنځی کامپیوتر ساینس، پوهنتون غالب (هرات)

**ایمیل**: humohammadi5@gmail.com

## چکیده

اینترنت اشیاء (IoT-Internet of Things ) مفهومی نوین و فناوری پیشرفته در عرصه تکنالوژی معلوماتی و ارتباطات است که امکان تبادل داده میان اشیاء، انسان‌ها و حیوانات را از طریق شبکه‌های ارتباطی نظیر انترنت یا اینترانت فراهم می‌سازد. گسترش اینترنت اشیاء (IoT) ایجاد شبکه‌های پیچیده‌ای از دستگاه‌های متصل، مسائل امنیتی و حفظ حریم خصوصی را به چالش کشیده است. این مقاله به تحلیل آسیب‌پذیری‌های کلیدی در لایه‌های ارتباطی و تجهیزات فیزیکی IoT می‌پردازد و نقش مشکلات استانداردسازی، ضعف احراز هویت و محدودیت‌های رمزنگاری را بررسی می‌کند. همچنین اثربخشی راه‌حل‌هایی نظیر رمزنگاری سبک، احراز هویت چندلایه، شبکه‌های بلاک‌چین و الگوریتم‌های هوش مصنوعی برای تشخیص نفوذ و ارتقای امنیت سیستم‌ها تحلیل شده است. روش استفاده شده در این تحقیق توصیفی-تحلیلی به‌بررسی و تحلیل چالش‌ها و راه‌حل‌های امنیتی در اینترنت اشیاء (IoT) می‌پردازد .نتایج نشان می‌دهد که ترکیب این روش‌ها می‌تواند سطح امنیت IoT را به‌طور قابل توجهی افزایش دهد، اما نیازمند استندردهای یکپارچه و توسعه تحقیقات کاربردی در این حوزه است. بیشتر آسیب‌پذیری‌های امنیتی در لایه‌های ارتباطی و تجهیزات فیزیکی IoT مشاهده می‌شود. نبود استندردهای یکپارچه امنیتی، مشکل احراز هویت و ضعف در رمزنگاری از چالش‌های اصلی هستند. راه‌حل‌هایی نظیر استفاده از رمزنگاری سبک، احراز هویت چندلایه، شبکه‌های بلاک‌چین و به‌کارگیری الگوریتم‌های هوش مصنوعی برای تشخیص نفوذ، در بهبود امنیت مؤثر هستند.

**کلمات کلیدی:** اینترنت اشیاء، امنیت اطلاعات، حریم خصوصی، معماری IoT، تهدیدات سایبری

**مقدمه**

در چشم‌انداز دیجیتال فراگیر امروزی، اینترنت تأثیر عمیقی بر هستی جهانی گذاشته و سفری مداوم به سوی اتصال فراگیرتر را رقم زده است که آغازگر عصر اینترنت اشیا (IoT) است. اینترنت اشیا، اختراعی پیشگامانه در دهه‌های اخیر، تعامل بین قلمروهای فیزیکی و دیجیتال را متحول می‌کند، همانطور که توسط ورمسان و همکارانش تعریف شده است. در این چشم‌انداز به هم پیوسته، دنیای دیجیتال از طریق مجموعه‌ای از حسگرها و محرک‌ها با دنیای فزیکی درگیر می‌شود. پنا-لوپز و همکارانش تفسیر گسترده‌ای ارائه می‌دهند و اینترنت اشیا را به‌عنوان الگویی توصیف می‌کنند که در آن محاسبات و شبکه‌سازی به‌طور یکپارچه در تقریباً هر شیء ادغام می‌شوند و امکان پرس‌وجو و اصلاح از راه دور را فراهم می‌کنند. به طور کلی، اصطلاح "اینترنت اشیا" قلمروی متحول‌کننده‌ای را توصیف می‌کند که در آن تقریباً هر دستگاه روزانه به‌طور پیچیده‌ای به یک شبکه متصل است و امکان استفاده مشترک برای کارهای هوشمند و خودکار را فراهم می‌کند. مفهوم اینترنت اشیا اولین بار توسط پیتر تی. لوئیس در سال ۱۹۸۵ معرفی شد و آن را به‌عنوان ادغام افراد، روندها و تکنالوژی با دستگاه‌ها و حسگرهای به هم پیوسته تعریف کرد. این امر، نظارت از راه دور، ارزیابی وضعیت، دستکاری و تحلیل روند این دستگاه‌ها را تسهیل می‌کند. سفر اینترنت اشیا، به دور از پایان خود، نوید آینده‌ای را می‌دهد که در آن دستگاه‌های متنوع به‌طور یکپارچه به وب متصل می‌شوند و وجود انسان را به روش‌های بی‌سابقه‌ای تغییر می‌دهند (Vermesan, 2022).

اینترنت اشیا شبکه‌ای از دستگاه‌های به‌هم پیوسته با حسگرها، محرک‌ها، پردازنده‌ها و فناوری‌های ارتباطی مختلف است. حسگرها داده‌های بلادرنگ را از حالت‌های داخلی و محیط‌های خارجی، از تلفن‌های همراه گرفته تا اجاق‌های مایکروویو، جمع‌آوری می‌کنند. محرک‌ها نیز به نوبه خود به داده‌ها یا دستورات پاسخ می‌دهند و امکان اتومیشن و کنترول از راه دور دستگاه‌های فزیکی را فراهم

می‌کنند. داده‌های جمع آوری‌شده توسط حسگرها یا در لبه شبکه یا روی سرورهای مرکزی پردازش می‌شوند و برخی از پیش‌پردازش‌ها مستقیماً در حسگرها یا دستگاه‌های انتهایی اتفاق می‌افتد. داده‌های پردازش‌شده سپس برای تجزیه و تحلیل، ذخیره‌سازی و پردازش بیشتر به‌سرورهای راه دور منتقل می‌شوند. این داده‌ها اساس تجزیه و تحلیل، تصمیم‌گیری و اقدامات بعدی را تشکیل می‌دهند که می توانند فزیکی (مثلاً تنظیم ترموستات هوشمند) یا مجازی (مثلاً ارسال اعلان‌ها) باشند. کاربردهای اینترنت اشیا گسترده و متنوع هستند و جنبه‌های مختلف زندگی‌ما را تحت تأثیر قرار می‌دهند. از راحتی شخصی در خانه‌های هوشمند گرفته تا نوآوری‌های مراقبت‌های بهداشتی و تناسب اندام، اینترنت اشیا پتانسیل تأثیرگذاری بر جنبه‌های شخصی، مالی، فزیکی، آموزشی، حرفه‌ای و روانی افراد را دارد (Peña-López, 2005) . در خانه‌های هوشمند، اینترنت اشیا امکان کنترول از راه دور لوازم برقی، روشنایی، دم کردن قهوه، تنظیم ترموستات و حتی عملیات بدون دخالت دست را از طریق دستورات صوتی فراهم می‌کند. در مراقبت‌های بهداشتی، دستگاه‌های پوشیدنی اینترنت اشیا نظارت از راه دور را ارائه می‌دهند و به‌مراقبان و متخصصان مراقبت‌های بهداشتی اجازه می‌دهند در مواقع اضطراری کمک به‌موقع ارائه دهند. علاوه بر این، افراد می‌توانند از دستگاه‌های پوشیدنی برای ردیابی الگوهای خواب، فعالیت بدنی و تناسب اندام کلی استفاده کنند. این مثال‌ها تنها بخش کوچکی از چشم‌انداز وسیع کاربردهای اینترنت اشیا را نشان می‌دهند و نشان‌دهنده امکانات و چالش‌های هیجان‌انگیزی هستند که محققان برای آینده درحال بررسی آن‌ها هستند.

اینترنت اشیا پتانسیل تغییر نحوه تعامل افراد با فناوری را دارد و راحتی، کارایی و شخصی‌سازی بیشتری را در زندگی روزمره فراهم می‌کند. اینترنت اشیا با وجود تأثیر دگرگون‌کننده‌اش، با چالش‌هایی روبرو است. تعداد زیاد دستگاه‌ها و داده‌های قابل توجه تولید شده، چالش‌های قابل توجهی را ایجاد می‌کنند، به طوری که پیش‌بینی می‌شود ۴۱,۶ میلیارد دستگاه اینترنت اشیا تا سال ۲۰۲۵، ۷۹,۴ زتابایت داده تولید کنند. پرداختن به‌این موضوع نیازمند معماری‌های مقیاس‌پذیر و

قابلیت‌های پردازشی پیشرفته است. علاوه بر این، اینترنت اشیا به شدت به ارتباطات بی‌سیم متکی است که منجر به‌چالش‌هایی مانند اعوجاج و عدم اطمینان در مکان‌های پراکنده جغرافیایی می‌شود. تضمین انتقال داده‌های قابل اعتماد به‌یک چالش اساسی تبدیل می‌شود و بر نقش حیاتی فناوری‌های ارتباطی در چشم‌انداز اینترنت اشیا تأکید دارد. فراتر از موانع فنی، چالش‌های عمومی و خاص حوزه‌های مختلف برای موفقیت اینترنت اشیا بسیار مهم هستند. شناسایی و پرداختن به‌این چالش‌های چندوجهی به‌صورت جمعی برای آزادسازی پتانسیل کامل اینترنت اشیا و غلبه بر موانع برای پذیرش و ادغام گسترده‌تر در زندگی‌ما ضروری است (Gillis, 2021).

## روش تحقیق

این مقاله با استفاده از روش توصیفی-تحلیلی به‌بررسی و تحلیل چالش‌ها و راه‌حل‌های امنیتی در اینترنت اشیاء (IoT) می‌پردازد.

**روش توصیفی:** ابتدا وضعیت موجود IoT، ساختار شبکه‌ها، تجهیزات فزیکی و لایه‌های ارتباطی بررسی شده و آسیب‌پذیری‌های کلیدی شناسایی می‌شوند. این مرحله شامل مرور منابع علمی، گزارش‌ها، استندردهای امنیتی و مطالعات موردی می‌باشد.

**روش تحلیلی:** سپس با استفاده از تحلیل مقایسه‌ای و طبقه‌بندی، نقاط ضعف و چالش‌ها مورد بررسی قرار می‌گیرند و اثربخشی راه‌حل‌های امنیتی (رمزنگاری سبک، احراز هویت چندلایه، شبکه‌های بلاک‌چین[۳۵]، الگوریتم‌های هوش مصنوعی) تحلیل می‌شود. این تحلیل شامل مقایسه عملکرد روش‌های مختلف، بررسی محدودیت‌ها و استخراج نتیجه‌گیری‌های عملیاتی می‌باشد.

[۳۵] بلاک‌چین (Blockchain): بلاک‌چین یک دفترکل توزیع‌شده و غیرمتمرکز است که اطلاعات در آن در قالب «بلوک‌های» متوالی ذخیره می‌شوند. هر بلوک شامل مجموعه‌ای از تراکنش‌ها، برچسب زمانی (Timestamp)و هش رمزنگاری‌شده بلوک قبلی است که این زنجیره‌سازی، تغییرناپذیری و یکپارچگی داده‌ها را تضمین می‌کند.

**منابع مورد استفاده** :منابع مورد استفاده شامل مقالات علمی (ژورنال‌ها و کنفرانس‌ها)، استندردهای صنعتی، گزارش‌های امنیتی و مطالعات موردی هستند. تعداد منابع به‌دقت در بخش منابع ذکر می‌شود تا اعتبار و گستره تحلیل مشخص شود.

**معماری و ساختار اینترنت اشیاء**

بستر اینترنت اشیاء بر امواج رادیویی بی سیمی قرارداده شده که به‌دستگاه‌های مختلف این امکان را می‌دهند تا از طریق اینترنت با یکدیگر ارتباط برقرار کنند. این بستر شامل استندردهایی مانند وای فای، بلوتوث کم مصرف، NFC[۳۶] و RFID[۳۷] می‌باشد. دستگاه‌ها در اینترنت اشیاء اطلاعات خود را به‌دستگاه‌های پیشرفته انتقال می‌دهند که این دستگاه پیشرفته ممکن است گوشی هوشمند، واحد کنترول مانند ترموستات هوشمند یا دستگاه اختصاصی که حکم دروازه اینترنت را دارد، باشند. دستگاه‌های اختصاصی خیلی مهم هستند زیرا یک سنسور ممکن است دارای ارتباط مستقیم به‌اینترنت نباشد. از این رو، ارتباط دستگاه‌های اختصاصی از طریق ارتباطی با مصرف انرژی کم مانند بلوتوث و ZigBee[۳۸] صورت می‌پذیرد.

سیستم اینترنت اشیاء از سه بخش سرویس، شبکه و دستگاه تشکیل شده است. زمانیکه یک دستگاه اینترنت اشیاء اطلاعاتی را از سنسور دریافت می‌کند آن را به سرویس ابری خواهد فرستاد. حال شرایطی را در نظر بگیرید که می‌خواهید حرارت

---

[۳۶] NFC (Near Field Communication) یا ارتباط میدان نزدیک یک فناوری بی‌سیم کوتاه‌برد است که امکان تبادل داده بین دستگاه‌ها را در فاصله بسیار نزدیک (حدود ۴ تا ۱۰ سانتی‌متر) فراهم می‌کند.

[۳۷] RFID (Radio-Frequency Identification) یا شناسایی با امواج رادیویی یک فناوری بی‌سیم است که برای شناسایی و ردیابی اشیاء، حیوانات یا افراد با استفاده از برچسب‌ها (Tags) و خواننده‌ها (Readers) طراحی شده است.

[۳۸] ZigBee یک استاندارد ارتباطی بی‌سیم کم‌مصرف و کوتاه‌برد است که برای شبکه‌های حسگر و دستگاه‌های اینترنت اشیاء (IoT) طراحی شده است. این فناوری بر پایه پروتکل IEEE 802.15.4 عمل می‌کند و برای کنترول و مانیتورینگ دستگاه‌های کوچک و کم‌مصرف مناسب است.

خانه خود را اندازه گیری کنید. واحد تهویه مطبوع بر درجه نظارت دارد، ممکن است برنامه ریزی شده باشد که حرارت را تا درجه خاصی نگه دارد یا این‌که در ساعات مشخصی برای شروع کار روشن شود. تمامی این اطلاعات جمع آوری شده و به سرویس ابری فرستاده می‌شود تا از طریق گوشی هوشمند بتوانید حرارت و دیگر اطلاعات را چک کنید. اگر قصد دارید یکی از روزها زودتر به‌خانه برگردید می‌توانید از طریق سرویس ابری و اتصال اینترنت، واحد تهویه خانه را فعال کنید تا زمانی که به‌خانه می‌رسید حرارت و هوای منزل متعادل باشد. تمامی این دستورات را می‌توانید از طریق گوشی هوشمند به‌واحد تهویه بفرستیدو این مثالی از خانه هوشمند است، در شهر هوشمند هم در کنترول هوشمند ترافیک، کنترول هوشمند روشنایی سرک‌ها و غیره از اینترنت اشیاء استفاده می‌شود.

**کاربردهای اینترنت اشیاء**

اینترنت اشیاء می‌تواند در زمینه های مختلفی باعث بهبود کیفیت زندگی شود از جمله آن می‌توان به‌موارد ذیل اشاره کرد:

- در شهرها در پارکینگ هوشمند، سلامت ساختمانی، طراحی نقشه آلودگی صوتی شهرها، روشنایی هوشمند، مدیریت ضایعات و سیستم حمل و نقل هوشمند.
- در زمینه محیط زیست در تشخیص آتش سوزی جنگل‌ها، آلودگی هوا، پیشگیری لغزش‌های سطح زمین و برف کوچ و تشخیص زودرس زلزله.
- در سیستم آبرسانی و فاضلاب، در بررسی کیفیت آب، نشت آب، سیلاب رودخانه‌ها، شبکه هوشمند انرژی، سطح مخازن، جریان آب و برآورد موجودی انبارها.
- در زمینه تجهیزات امنیتی و اضطراری، در حفاظت پیرامونی، حضور مایع، مواد منفجره و گازهای خطرناک.

- در پرچون فروشی، در کنترول زنجیره تأمین پرداخت، نرم افزارهای خرید هوشمند، مدیریت محصولات هوشمند.
- در زمینه تدارکات می‌توان به‌کیفیت شرایط حمل و نقل، تشخیص عدم تطابق انبارداری و نهادهای پیگیری اشاره کرد.
- در کاربرد کنترول صنعتی می‌توان نرم افزار کیفیت هوای داخل ساختمان، مانیتورینگ حرارت، حضور لایه ازون، موقعیت داخل و وسیله‌های خود تشخیص را نام برد.
- از نمونه کاربرد آن در زراعت می‌توان خانه‌های سبز و گلخانه‌ها را نام‌برد.
- در پرورش حیوانات می‌توان بهداشت زاد و ولد، ردیابی حیوانات و میزان گازهای سمی را نام‌برد.
- در خانه‌های هوشمند در مصرف انرژی و آب، لوازم برقی کنترول از راه دور و سیستم‌های تشخیص نفوذ را نام‌برد.
- در زمینه سلامت الکترونیک می‌توان تشخیص سقوط طیاره‌ها، یخچال‌های پزشکی، مراقبت از ورزشکاران، مراقبت از بیماران و اشعه‌ماورای بنفش را نام برد.

**چالش‌های موجود در زمینه اینترنت اشیاء**

با وجود کاربردهای فراوان اینترنت اشیاء در زندگی روزمره و در جنبه‌های مختلف، چالش‌هایی در اینترنت اشیاء وجود دارند که باید در نظر گرفته شوند. از نظر مقیاس پذیری، برنامه‌های کاربردی اینترنت اشیاء که نیارز به‌تعداد زیادی وسایل دارند، اغلب پیاده سازی‌شان به‌علت محدودیت‌های زمانی، حافظه، پردازش و محدودیت‌های انرژی دشوار است (Gillis, 2021) . به‌عنوان مثال، محاسبه تغییرات حرارت در اطراف کشور نیاز به‌وسایل زیادی دارد و به‌مقدار غیر قابل مدیریت داده منجر می‌شود. و سخت افزار به‌کارگرفته شده در اینترنت اشیاء اغلب ویژگی‌های عملیاتی متفاوتی از قبیل نرخ نمونه برداری و توزیع

خطا دارند، در عین‌حال سنسورها و اجزای به‌کار اندازنده اینترنت اشیاء خیلی پیچیده هستند. همه این عوامل به‌شکل گیری شبکه ناهم‌گنی از اینترنت اشیاء که در آن داده‌های اینترنت اشیاء ناهم‌گن خواهند بود کمک خواهند کرد. علاوه‌براین، انتقال حجم زیادی داده در شبکه پیچیده و ناهم‌گن پر هزینه خواهد بود. بنابراین، اینترنت اشیاء نیاز به‌فشرده سازی داده و ترکیب داده به منظور کاهش حجم داده دارد. متعاقباً، استندردسازی آگاهی پردازش داده برای اینترنت اشیاء آینده خیلی مطلوب خواهد بود. علاوه‌براین، هکرها، نرم‌افزار مخرب و ویروس در روند ارتباط ممکن است داده و جامعیت اطلاعات را از بین ببرند. با توسعه تکنولوژی اینترنت اشیاء ، نا امنی اطلاعات به‌طور مستقیم کل سیستم اینترنت اشیاء را تهدید خواهد کرد. از آنجا که اینترنت اشیاء یک معماری تکنیکی مبتنی بر اینترنت سراسری با فراهم کردن امکان تبادل کالاها و سرویس‌ها در شبکه‌های زنجیره‌ای تقاضای سراسری است، تاثیری بر امنیت و حریم خصوصی سهام‌داران دارد. این سیستم‌ها باید با تأمین انعطاف پذیری در مورد حملات، اعتبارسنجی داده‌ها، کنترول دسترسی و حفظ حریم مشتری، نیازهای‌ما را رفع کنند. از این رو موضوع حفظ حریم خصوصی و امنیت از مسائل مهمی هستند که در طراحی سیستم‌های مبتنی بر اینترنت اشیاء در نظر گرفته شوند.

### ۱. حفظ حریم خصوصی

پتانسیل کامل اینترنت اشیاء بستگی به‌استراتیژی‌هایی دارد که مربوط به انتخابات حریم خصوصی در سراسر طیف گسترده‌ای از انتظارات است (Vermesan, 2022).جریان‌های داده و ویژگی کاربر فراهم شده توسط دستگاه های اینترنت اشیاء می‌تواند ارزش‌های باور نکردنی و منحصر به‌فرد برای کاربران اینترنت اشیاء را باز کند اما حقوق حریم خصوصی و توجه به‌انتظارات حریم

خصوصی کاربر برای تضمین اعتماد و اطمینان کاربرهای اینترنت، دستگاه‌های متصل شده و سرویس‌های مرتبط ضروری هستند.

### ۲. امنیت

با این که موضوع امنیت در زمینه تکنولوژی اطلاعات خیلی جدید نیست، ویژگی‌های بسیاری از پیاده سازی اینترنت اشیاء ارائه چالش‌های جدید و منحصر به فرد امنیتی است. در نظر گرفتن این چالش‌ها و تأمین امنیت محصولات اینترنت اشیاء و سرویس‌ها باید اولویت اصلی باشد. کاربرها باید اعتماد داشته باشند که وسایل اینترنت اشیاء و سرویس‌های داده مربوط از آسیب‌پذیری مصئون هستند، مخصوصاً زمان‌هایی که تکنولوژی در زندگی روزانه‌ما فراگیرتر و یکپارچه می‌شود. سرویس‌ها و دستگاه‌های اینترنت اشیاء با امنیت ضعیف می‌توانند به‌عنوان نقاط ورود بالقوه برای حمله سایبری محسوب شوند و اطلاعات کاربر را با ترک جریان داده‌ها به‌اندازه کافی محافظت شده در معرض سرقت قرار دهند.

طبیعت به‌هم پیوسته وسایل اینترنت اشیاء بدین معنی است که هر دستگاه با امنیت پایین که آنلاین متصل شده، به‌طور بالقوه بر امنیت و انعطاف پذیری اینترنت در سطح سراسری تأثیر می‌گذارد. این چالش توسط ملاحظات دیگر مانند استقرار در مقیاس انبوه دستگاه‌ها به‌دستگاه‌های دیگر و احتمال کار کردن با این دستگاه‌ها در محیط‌های نا امن تقویت می‌شود.

### ۳. نیازمندی‌های حفظ حریم خصوصی و امنیت

حریم خصوصی شامل مخفی سازی اطلاعات شخصی و همچنین توانایی کنترول مواردی است که برای این اطلاعات اتفاق افتاده است. حق حریم خصوصی می‌تواند به‌عنوان یک حق اساسی و غیر قابل انکار انسانی و یا به‌عنوان یک حق شخصی یا مالکیت در نظر گرفته شود (Gillis, 2021). انتساب برچسب‌ها به اشیاء ممکن است برای کاربران ناشناخته باشد و ممکن است هیچ سیگنال صوتی یا

تصویریی برای جلب توجه کاربران وجود نداشته باشد. در نتیجه، افراد می‌توانند بدون آن‌ها حتی با شناخت آن‌ها دنبال شوند و داده‌های خود را ترک کنند و یا حداقل آثار آن در فضای مجازی را دریابی کنند. علاوه بر تشدید مسئله، نه‌تنها دولت تمایل به‌جمع‌آوری داده‌های مرتبط دارد بلکه طرفداران خصوصی از قبیل شرکت‌های بازاریابی هم تمایل به‌جمع آوری داده دارند.

از آنجایی که روندهای تجاری درگیر هستند، درجه بالای قابلیت اطمینان مورد نیاز است. از این رو نیازمندی‌های حریم خصوصی و امنیت ذیل بیان شده اند:

۱. انعطاف پذیری به‌حملات: سیستم باید از نقاط تک شکست خودداری کند و خودش را با شکست‌های گروهی سازگار کند.
۲. کنترول دسترسی: تأمین کننده اطلاعات باید قادر به پیاده سازی کنترول دسترسی روی داده فراهم شد ه باشد.
۳. اعتبار سنجی داده: به‌عنوان یک هدف، آدرس برگشت داده شده و اطلاعات شیء باید اعتبار سنجی شود.
۴. حریم خصوصی مشتری: معیارهایی باید در نظر گرفته شوند که فقط تأمین کننده اطلاعات قادر به‌استنتاج از مشاهده استفاده از سیستم مراجعه مربوط به یک مشتری خاص می‌باشد و حداقل استنتاج باید خیلی به‌سختی انجام شود.

**امنیت در اینترنت اشیاء**

تضمین امنیت، قابلیت اطمینان، انعطاف پذیری، ثبات برنامه‌های کاربردی و خدمات اینترنت به‌منظور ترویج اعتماد و استفاده از اینترنت ضروری است. کاربرها باید اعتماد داشته باشند که وسایل اینترنت اشیاء و سرویس‌های داده مرتبط از آسیب پذیری مصئون هستند، مخصوصاً وقتی این تکنالوژی در زندگی روزانه‌ما فراگیر تر و یکپارچه میشود ولی اگر افراد باور نداشته باشند وسایل متصل شده آن‌ها و اطلاعات آن‌ها بطور قابل قبولی از سوء استفاده و آسیب مصئون هستند، این کاهش اعتماد باعث کاهش استفاده از اینترنت میشود و این خود عواقبی در تجارت

الکترونیک، نوآوری فنی و عملاً هر مورد دیگری از فعالیت های آنلاین دارد. از این رو، تضمین امنیت در محصولات اینترنت اشیاء به عنوان بالاترین اولیت در این بخش باید در نظر گرفته شود. بحث امنیت در اینترنت اشیاء میتوان در دو بخش امنیت دستگاه های اینترنت اشیاء امنیت خود سیستم اینترنت اشیاء مطرح شود.

**۱. چالش های امنیتی سیستم اینترنت اشیاء**

امنیت کلی و انعطاف پذیری اینترنت اشیاء تابعی است که چگونه خطرات امنیتی ارزیابی و اداره می شود. امنیت وسیله، شامل تابعی از ریسک که دستگاه با آن سازگار خواهد شد، خسارتی که چنین سازشی باعث خواهد شد و زمان و منابع مورد نیاز برای بدست آوردن سطح خاصی از حفاظت میباشد. اگر کاربری مانند اپراتوریک سیستم کنترول ترافیک یا شخصی با یک وسیله پزشکی فعال شده از طریق اینترنت، نتواند درجه بالاتری از خطر امنیتی را تحمل کند، وی باید مقادیر قابل توجهی منابع را برای محافظت از سیستم یا وسیله از حمه مصرف کند. از چالش های موجود در سیستم اینترنت اشیاء میتوان موارد زیر را بر شمرد:

- طراحی خوب
- هزینه در برابر تعادل امنیت
- استندردها و مقیاس های مورد استفاده
- محرمانه بودن اطلاعات، احراز هویت و کنترول دسترسی
- قابلیت بروزرسانی فیلد
- مسئولیت پذیری اشتراکی
- قراردادهای سخت افزاری و نرم افزاری
- از کارافتادگی دستگاه

**۲. چالش های امنیتی وسایل اینترنت اشیاء**

در زمینه امنیت داستگاه ها نیز با چالش هایی مواجه هستیم که میتوان به موارد زیر اشاره کرد:

- بعضی وسایل اینترنت اشیاء به احتمال زیاد در مکان هایی مستقر میشوند که در آن بدست آوردن امنیت فیزیکی دشوار یا غیر ممکن است. حمله کننده ها ممکن است دسترسی فیزیکی مستقیم به وسایل اینترنت اشیاء داشته باشند.
- تعداد زیادی وسایل اینترنت اشیاء بدون قابلیت بروز رسانی طراحی شده اند و یا روند بروز رسانی در آن‌ها غیر عملی است.
- توسعه های اینترنت اشیاء زیادی شامل مجموعه ای از دستگاه های یکسان است. این همگونی تأثیر بالقوه هر آسیب پذیری امنیتی بوسیله تعداد خالص از دستگاه هایی که همه دارای ویژگی های مشابه هستند را پر رنگ میکند.
- وسایل اینترنت اشیاء زیادی در حالتی عمل میکنند که کاربر دید کمی در مورد کار داخلی دستگاه یا چگونگی تولید جریان های داده در آن دارد یا اصلاً دید عمیقی ندارد.
- بسیاری از وسایل اینترنت اشیاء با یک سرویس پیش بینی شده زمان طولانی تری از آن‌هایی که با تجهیزات تکنولوژی بهتری ساخته شده اند عمر میکنند. از این رو، مکانیزم های امنیتی ای مورد نیاز است که برای همه طول عمر دستگاه ها مناسب باشند.
- بسیاری از وسایل اینترنت اشیاء از قبیل سنسورها و اقلام مصرفی، اینترنت طوری طراحی شده اند که در یک مقیاس بزرگ گسترش یابند.

**راه حل های برقراری امنیت در سیستم اینترنت اشیاء**

وسایل اینترنت اشیاء با امنیت ضعیف می توانند به عنوان نقاط بحرانی برای حمه سایبری با اجازه دادن به افراد مخرب که وسیله ای را دوباره برنامه نویسی کنند یا باعث سوء عملکرد آن شود. همراه با کمبود طراحی امنیتی بالقوه، افزایش تعداد و ماهیت دستگاه های اینترنت اشیاء فرصت های حمه را افزایش می دهد. بر این اساس، نیاز به برقراری امنیت برای توسعه راه حل های مؤثر و مربوط به چالش های

امنیتی اینترنت اشیاء مورد نیاز خواهد بود که به خوبی در مورد مقیاس و پیچیدگی مسائل مناسب باشند.

امنیت میتواند به طریق مختلفی و در سطوح مختلفی برای سیستم اینترنت اشیاء فراهم شود. به عنوان نمونه در روشی امنیت به صورت انتها به انتها برقرار میشود که در این روش امنیت در سطوح شبکه و دستگاه ها برای عمل کردن اینترنت اشیاء ضروری است. سیستم هوشمندی که دستگاه ها را قادر به انجام کارهایشان میکند باید به آن‌ها امکان تشخیص و خنثی سازی حملات را بدهد و یا در روشی امنیت بصورت پایین – بالا برای سیستم تعریف میشود که در آن امنیت باید در کل طول عمر سیستم از طراحی اولیه تا محیط عملیاتی که شامل حراحل راه اندازی زیر میباشد، تأمین شود:

۱. راه اندازی مطمئن
۲. کنترول دسترسی
۳. احراز هویت دستگاه
۴. دیواره های آتش
۵. بروزرسانی ها

و یا در بعضی موارد امنیت باید از سطح سیستم عامل شروع شود که در این روش، کنترول های امنیتی نرم افزاری باید در سطح سیستم عامل معرفی شوند، از مزایای قابلیت های امنیتی سخت افزاری که وارد بازار میشود بهرهببرند و تا دستگاه برای نگهداری پایگاه محاسبه مطمئن توسعه داده شود. پیاده سازی امنیت در سطح سیستم عامل به طراحان دستگاه‌ها و توسعه دهندگان قابلیت پیکربندی سیستم ها برای آشکارسازی حملات و تضمین امنیت سکوهای آن‌ها را میدهد. از روش های برقراری امنیت در سیستم های اینترنت اشیاء که در این مقاله بررسی شده اند را میتوان به موارد زیر اشاره کرد:

در روشی برسی شده در، مشهورترین طرح صنعتی مبتنی بر تکنولوژی اطلاعات جدید بر اساس کد تولید الکترونیکی معرفی شده بوسیله کد تولید الکترونیکی جهانی و GSI[۳۹] است. اشیاء، اشیای فیزیکی با حمل تگ های RFID با یک تک کد تولید الکترونیکی هستند. زیر ساخت سرویس های اطلاعاتی کد تولید الکترونیکی را هم بطور محلی و هم از راه دور به مشترکین پینهاد میکند. اطلاعات بطور کامل روی تگ RFID ذخیره نیم شوند اما تأمین اطلاعات بوسیله سرورهای توزیع شده روی اینترنت از طریق اتصال با کمک یک سرویس نامگذاری شیء انجام میشود.

سرویس نامگذاری شیء معتبر است (با اتصال متا داده و سرویس ها) به این معنا که موجودیت با داشتن کنترول تغییر متمرکز روی اطلاعات درباره کد تولید الکترونیکی مشابه موجودیت مشابهی است که کد تولید الکترونیکی را به مورد مربوط نسبت میدهد. بنابراین، همچنین معمار میتواند با قادر ساختن محیط های هوشمند به تشخیص و شناسایی اشیاء و دریافت اطلاعات از اینترنت به منظور تسهیل قابلیت تطبیقی آن‌ها، به عنوان ستون فقرات برای محاسبات فراگیر عمل کند. ریشه سرویس نامگذاری شیء مرکزی بوسیله شرکت خصوصی Verisign[٤٠]، فراهم کننده سرویس های زیرساختی اینترنت، اداره میشود.

سرویس نامگذاری شیء مبتنی بر سرویس نام دامنه شناخته شده ای است. بطور تکنیکی به منظور استفاده از سرویس نام دامنه برای پیدا کردن اطلاعات درباره آیت، گزینه کد تولید الکترونیکی باید به فرمتی که سرویس نام دامنه بتواند بفهمد

---

[۳۹] ( سیستم اطلاعات جغرافیایی / GSI (Geographic Information Sys**tem** یک فناوری برای جمع آوری، ذخیره‌سازی، تحلیل و نمایش داده‌های مکانی و جغرافیایی است. GSI به سازمان‌ها و کاربران این امکان را می‌دهد که اطلاعات مکانی را به صورت نقشه‌ای و تحلیلی مدیریت و مورد بررسی قرار دهند.

[٤٠] Verisignیک شرکت آمریکایی مشهور در حوزه فناوری اطلاعات و امنیت اینترنت است که بیشتر به دلیل مدیریت دامنه‌های سطح بالای اینترنت (TLD) و ارائه خدمات امنیت سایبری و DNS شناخته می‌شود.

تبدیل شود که عموماً به شکل محدود شده با dot[41]، شکل چپ به راست همه نام های دامنه تبدیل شود. از آنجایی که کد تولید الکترونیکی از لحاظ دستوری به نام دامنه درست کدگذاری شده و سپس در زیرساخت های سرویس نام دامنه در نظر گرفته میشود. به این دلیل، با این وجود، سرویس نامگذاری شیء همه نقاط ضعف سرویس نام دامنه از قبیل افزونگی محدود شده در پیاده سازی های خاص و ایجاد نقاط شکست تک را به ارث خواهد برد.

روش دیگری برای افزایش امنیت و حریم خصوصی سیستم های نظیر به نظیر هستند که مقیاس پذیری و عملکرد خوبی دارند. این سیستم ها میتوانند بر اساس جداول هَش توزیع شده باشند. کنترول دسترسی، باید در خود سرویس های اطلاعاتی کد تولید الکترونیکی واقعی پیاده سازی شود و نه در داده های ذخیره شده در DHT[42]. به طور خاص، احراز هویت مشتری میتواند با انتشار رازهای مشترک با استفاده از رمزنگاری کلید عمومی انجام شود.

در مقایسه با روش ارائه شده در، این مهم است که تک RFID که به یک شیء متصل شده میتواند در مقیاسی بزرگتر به منظور اجازه دادن به مشتری ها در تصمیم گیری بر مورد استفاده آن‌ها از تگ های غیر فعال شوند. غیر فعال سازی تگ های RFID همچنین میتوانند با قرار دادن آن‌ها در یک توپولوژی مِش حفاظت شده از فویل شناخته شده به عنوان قفس فارادی که بوسیله سیگنال های رادیویی با فرکانس های خاص یا بوسیله حذف یا از بین بردن آن ها انجام شود. با این وجود، هر دوی این ها معایب خاصی دارند.

وضوح برای اطلاعات قابل شناسایی غیر شخصی برگشت داده شده بوسیله RFID مورد نیاز می باشد. یک RFID فعال میتواند ردیابی جابجایی های رؤیت

---

[41] اصطلاح dot در حوزه اینترنت و دامنه‌ها معمولاً به نقطه موجود در نام دامنه‌ها اشاره دارد و نقش کلیدی در سیستم نام دامنه (DNS) دارد.

[42] DHT (Distributed Hash Table) یا جدول پراکنده "هش" یک ساختار داده و فناوری شبکه‌ای است که برای ذخیره و جستجوی داده‌ها به صورت توزیع‌شده در شبکه‌های همتا به همتا (Peer to Peer) استفاده می‌شود.

کنندگان یک رویداد را بدون شناسایی افراد بطوری که آن‌ها غیر قابل شناسایی بمانند را انجام دهد. با این حال، سوالی که باقی میماند این است که آیا چنین اطلاعاتی پوشش داده نشده توسط قوانید حریم خصوصی سنتی باید بدون هیچ محدودیتی گرد آوری شوند. در روش دیگری از برقراری امنیت اینترنت اشیاء بررسی شده در، اینترنت اشیاء به سه لایه تقسیم میشود، لایه دریافت، لایه انتقال و لایه کاربرد برای تحلیل جزئی مسائل امنیتی اینترنت اشیاء ، بر طبق انتقال داده در فاز اینترنت اشیاء ، لایه دریافت به گره های دریافت تقسیم شده و شبکه دریافت لایه انتقال به شبکه دسترسی، شبکه هسته و شبکه محلی تقسیم شده و لایه کاربرد به لایه پشتیبانی کاربرد و برنامه های کاربردی اینترنت اشیاء تقسیم میکنیم. هر لایه پشتیبانی تکنیکی دارد، این تکنولوژی ها در همه سطوح نقش غیر قابل تعویضی بازی میکنند. اما این تکنیک ها کم یا زیاد میتوانند مسائل نا امنی، حریم خصوصی و مسائل دیگر امنیتی داده را سبب شوند. در این روش، اینترنت اشیاء باید شامل امنیت همه لایه ها باشد. لایه دریافت شامل امنیت RFID، امنیت شبکه‌های حسگر بی‌سیم، امنیت RSN[۴۳] و سایر باشد.

**نتیجه‌گیری**

نتایج این تحقیق نشان می‌دهد که امنیت در اینترنت اشیاء همچنان یکی از موانع اصلی گسترش و پذیرش گسترده این فناوری است. بیشترین آسیب‌پذیری‌ها در لایه‌های ارتباطی و تجهیزات فیزیکی مشاهده می‌شود و نبود استندردهای جامع امنیتی، ضعف در مکانیزم‌های احراز هویت و محدودیت‌های پردازشی دستگاه‌ها، چالش‌های کلیدی به شمار می‌روند. بررسی راهکارها نشان داد که استفاده از رمزنگاری سبک، احراز هویت چندلایه، بلاک‌چین و الگوریتم‌های هوش

[۴۳] RSN (Robust Security Network)یک استاندارد امنیتی در شبکه های بی‌سیم است که به ویژه در شبکه های Wi-Fi برای تضمین امنیت ارتباطات طراحی شده است RSN .بخشی از IEEE 802.11i است و به‌عنوان جایگزین(WEP (Wired Equivalent Privacy و بهبود WPA (Wi-Fi Protected Access) عمل می‌کند.

مصنوعی می‌تواند کارایی و امنیت سیستم‌های IoT را به شکل قابل توجهی ارتقا دهد. با این حال، هیچ‌کدام از روش‌های موجود به تنهایی پاسخگوی تمامی نیازها نیستند و ترکیب رویکردهای چندگانه همراه با انکشاف استندردهای بین‌المللی، مسیر اصلی تحقیقات آینده محسوب می‌شود.

**کارهای آینده**

با توجه به گستردگی تهدیدات امنیتی در اینترنت اشیاء، تحقیقات آینده باید بر توسعه چارچوب‌های استندرد و یکپارچه امنیتی متمرکز شود. از سوی دیگر، طراحی الگوریتم‌های رمزنگاری سبک و مقاوم متناسب با محدودیت منابع دستگاه‌هایIoT ، ضرورت دارد. ترکیب هوش مصنوعی و یادگیری ماشین برای پیش‌بینی و تشخیص سریع حملات و همچنین بهره‌گیری از فناوری بلاک‌چین برای مدیریت غیرمتمرکز اعتماد، از مسیرهای نویدبخش تحقیقاتی محسوب می‌شود. علاوه بر این، پژوهش‌های آینده باید به مدل‌سازی ریسک، حفظ حریم خصوصی در مقیاس کلان و توسعه مکانیزم‌های خودترمیمی در شبکه‌های IoT بپردازند. همکاری‌های بین‌المللی در زمینه سیاست‌گذاری و استندردسازی نیز می‌تواند زمینه‌ساز ارتقای امنیت این فناوری در سطح جهانی باشد.

**References**


Vermesan, O. F. (2022). *Internet of things strategic research roadmap.* In *Internet of Things: Global technological and societal trends from smart environments and spaces to green ICT* (pp. 9–52). River Publishers.

Peña-López, I. (2005). *ITU Internet report 2005: The Internet of Things.* International Telecommunication Union (ITU).

Gillis, A. (2021, August 17). *What is internet of things (IoT)?* IOT Agenda. Retrieved from https://www.techtarget.com/iotagenda/

Sethi, P., & Sarangi, S. R. (2017). *Internet of Things: Architectures, protocols, and applications. Journal of Electrical and Computer Engineering*, Article ID 9324035. https://doi.org/10.1155/2017/9324035

Cook, D. J. (2017). *MavHome: An agent-based smart home.* In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications* (pp. 521–524). IEEE.

Dalal, P. A. (2020). *Internet of Things (IoT) in healthcare system: IA3 (Idea, Architecture, Advantages and Applications).* In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC).* Springer.

Dell Technologies. (2023). *Internet of Things and data placement.* Retrieved from https://www.delltechnologies.com

Rose, K., Eldridge, S., & Chapin, L. (2015). *The Internet of Things: An overview.* The Internet Society (ISOC).

Ashton, K. (2019). *Internet of Things. RFID Journal.* Retrieved from https://www.rfidjournal.com

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2021). *Security of the Internet of Things: Perspectives and challenges. Wireless Networks, 20*(8), 2481–2501. https://doi.org/10.1007/s11276-014-0731-0

Weber, R. H. (2020). *Security of the Internet of Things: New security and privacy challenges. Computer Law & Security Review, 26*(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

Tamboli, J. K., & Shaikh, M. A. (2021). *Security in the Internet of Things.* In *Communication, cloud and big data: Proceedings of CCB 2014* (pp. 122–128). Springer.

Fabian, B., & Günther, O. (2017). *Distributed ONS and its impact on privacy.* In *IEEE International Conference on Communications* (pp. 1223–1228). IEEE.

Liu, L., & An, D. (2016). *ALOHA-based anti-collision algorithms used in RFID system.* In *Proceedings of the IEEE International Conference on Networking and Mobile Computing* (pp. 1–4). IEEE.

# A Review of Security Methods in the Internet of Things (IoT)

Hussain Mohammadi[1*], Farhad Rasoolyar[2]

**Corresponding Author Email:** humohammadi5@gmail.com

The Internet of Things (IoT) is an innovative concept and an advanced technology in the field of information and communication technology, enabling data exchange among objects, humans, and animals through communication networks such as the Internet or intranet. The expansion of IoT and the creation of complex networks of connected devices have posed significant challenges to security and privacy.

This article analyzes key vulnerabilities in the communication layers and physical devices of IoT and examines the impact of issues such as lack of standardization, weak authentication, and encryption limitations. It also evaluates the effectiveness of solutions such as lightweight encryption, multi-layer authentication, block chain networks, and artificial intelligence algorithms for intrusion detection and enhancing system security. The results indicate that combining these approaches can significantly improve the security of IoT systems; however, the development of unified standards and applied research in this area is necessary. Most security vulnerabilities are observed in the communication layers and physical devices of IoT. The lack of unified security standards, weak authentication, and encryption limitations are the main challenges. Solutions such as lightweight encryption, multi-layer authentication, Blockchain networks, and AI-based intrusion detection are effective in improving security.

**Keywords:** Internet of Things (IoT), Information Security, Privacy, IoT Architecture, Cyber Threats