IJCITAI
International Journal of Computer, Information Technology and Artificial Intelligence (IJCITAI)

مجله بین‌المللی کامپیوتر، فناوری اطلاعات و هوش مصنوعی

https://ijcitai.ir

دوره ۱ – شماره ۱ (پاییز ۱۴۰۴) – صفحه ۳۹ تا ۴۸

تحول دیجیتال و چالش‌های امنیتی در عصر اینترنت اشیاء (IoT): تحلیل ریسک‌ها و راهکارهای نوین در شبکه‌های نسل پنجم (۵G)

کیهانه رضایی

دانشجوی دکترا مدیریت دولتی (توسعه منابع انسانی)، دانشگاه آزاد اسلامی صفاشهر

kihanerezaei@gmail.com

چکیده

این مقاله به بررسی تقاطع تحول دیجیتال، اینترنت اشیاء (IoT) و شبکه‌های نسل پنجم (۵G) با تمرکز ویژه بر چالش‌های امنیتی نوظهور می‌پردازد. با گسترش بی‌سابقه دستگاه‌های متصل در بستر G۵، سطح حمله به طور نمایی افزایش یافته و زیرساخت‌های حیاتی را در معرض تهدیدات پیچیده‌تری قرار داده است. مقاله حاضر با روشی توصیفی-تحلیلی، ابتدا معماری همگرای IoT-۵G و مولفه‌های کلیدی آن را تشریح می‌کند. سپس با تحلیل طبقه‌بندی ریسک‌های امنیتی در سطوح مختلف (دستگاه، شبکه، داده و کاربر)، به شناسایی آسیب‌پذیری‌های منحصربه‌فرد این اکوسیستم می‌پردازد. در ادامه، راهکارهای نوین امنیتی شامل معماری SBA (Service-Based Architecture) در G۵، استفاده از هوش مصنوعی و یادگیری ماشین برای تشخیص ناهنجاری، رمزنگاری پیشرفته، زنجیره بلوکی (Blockchain) برای هویت‌سنجی غیرمتمرکز، و مفهوم Zero Trust Architecture مورد بررسی قرار می‌گیرند. یافته‌ها نشان می‌دهد که اگرچه G۵ با ویژگی‌هایی مانند برش شبکه (Slicing Network) و مجازی‌سازی عملکرد شبکه (NFV) انعطاف‌پذیری را افزایش می‌دهد، اما همین ویژگی‌ها نیز پیچیدگی امنیتی جدیدی ایجاد می‌کنند. نتیجه‌گیری مقاله بر لزوم اتخاذ یک رویکرد امنیتی جامع، چندلایه و انطباق‌پذیر که همزمان با تحولات تکنولوژیکی تکامل می‌یابد، تاکید می‌ورزد.

واژگان کلیدی: تحول دیجیتال، اینترنت اشیاء (IoT)، امنیت سایبری، شبکه G۵، تحلیل ریسک

دوره ۱ – شماره ۱ (پاییز ۱۴۰۴) – صفحه ۳۹ تا ۴۸

۱. مقدمه

تحول دیجیتال به عنوان یک پارادایم مسلط در قرن بیست و یکم، با ادغام فناوری‌های دیجیتال در تمامی جنبه‌های زندگی اجتماعی، اقتصادی و صنعتی، در حال بازتعریف ساختارهای سنتی است. در قلب این تحول، **اینترنت اشیاء (IoT)** قرار دارد که با اتصال میلیاردها دستگاه فیزیکی به اینترنت، امکان جمع‌آوری، تبادل و تحلیل داده را در مقیاسی بی‌سابقه فراهم می‌سازد (۱). همزمان، ظهور و گسترش **شبکه‌های ارتباطی نسل پنجم (۵G)** با وعده ارائه پهنای باند بسیار بالا، تأخیر بسیار کم و اتصال گسترده، بستر ضروری برای تحقق کامل پتانسیل IoT در کاربردهایی مانند شهرهای هوشمند، صنعت ۴.۰، حمل و نقل خودران و سلامت دیجیتال را ایجاد کرده است (۲).

با این حال، این همگرایی عمیق (IoT و ۵G) یک پارادوکس اساسی به همراه دارد: از یک سو، قابلیت‌های تحول‌آفرین و از سوی دیگر، گسترش عظیم **سطح حمله (Surface Attack)** و معرفی طیف جدیدی از **آسیب‌پذیری‌های امنیتی**. دستگاه‌های IoT اغلب با محدودیت منابع (پردازش، حافظه، انرژی) مواجهند که اجرای مکانیزم‌های امنیتی سنگین را دشوار می‌سازد (۳). شبکه ۵G نیز با معماری نرم‌افزارمحور و مجازی‌شده خود، اگرچه انعطاف‌پذیری را افزایش می‌دهد، اما به دلیل پیچیدگی و وابستگی به نرم‌افزار، ممکن است در معرض حملات جدید قرار گیرد (۴). بنابراین، امنیت در اکوسیستم IoT-۵G به یک چالش چندبعدی تبدیل شده است که نیازمند درک عمیق ریسک‌ها و توسعه راهکارهای نوین و انطباق‌پذیر است.

هدف این مقاله، ارائه یک تحلیل جامع از چالش‌های امنیتی در این اکوسیستم همگرا است. سوالات اصلی تحقیق عبارتند از: ۱) ریسک‌ها و آسیب‌پذیری‌های کلیدی در تقاطع IoT و ۵G کدامند؟ ۲) راهکارهای امنیتی نوین و امیدبخش برای کاهش این ریسک‌ها چه هستند؟ ۳) چگونه می‌توان یک چارچوب امنیتی مقاوم و مقیاس‌پذیر برای آینده تحول دیجیتال طراحی کرد؟

۲. معماری همگرای IoT و شبکه ۵G: بستر تحول و چالش

برای درک چالش‌های امنیتی، ابتدا باید معماری این اکوسیستم را تشریح کرد. یک مدل مرجع لایه‌ای برای IoT-۵G را می‌توان به صورت زیر در نظر گرفت:

- **لایه 感知 و اجرا (Layer Perception/Device)**: شامل خود دستگاه‌های IoT (سنسورها، محرک‌ها، گجت‌های پوشیدنی و ...) است. محدودیت منابع ویژگی غالب این لایه است.
- **لایه شبکه/ارتباطات (Layer Network/Communication)**: بستر اتصال دستگاه‌ها به پلتفرم‌های پردازش داده را فراهم می‌کند. این لایه در حال گذار از تکنولوژی‌هایی مانند Wi-Fi، LoRaWAN و G/LTE۴ به سمت **شبکه‌های ۵G** است. هسته اصلی نوآوری ۵G در این لایه قرار دارد.
- **لایه پلتفرم/پردازش ابری (Layer Processing Platform/Cloud)**: مسئول ذخیره‌سازی، یکپارچه‌سازی، مدیریت و تحلیل داده‌های عظیم تولیدشده توسط IoT است. این لایه از زیرساخت‌های ابری (Public, Private, Hybrid) و Computing Edge/Fog بهره می‌برد.
- **لایه کاربردی/سرویس (Layer Application/Service)**: شامل برنامه‌های نرم‌افزاری است که ارزش‌افزوده ایجاد می‌کنند (مانند مدیریت ترافیک هوشمند، مانیتورینگ سلامت از راه دور).

ویژگی‌های کلیدی شبکه 5G که بر IoT و امنیت آن تاثیر می‌گذارند عبارتند از:

۱. **برش شبکه (Slicing Network)**: ایجاد چندین شبکه مجازی مجزا و مستقل بر روی یک زیرساخت فیزیکی مشترک. این امکان، سفارشی‌سازی سرویس برای کاربردهای مختلف IoT (با نیازمندی‌های امنیتی متفاوت) را فراهم می‌کند (۵).
۲. **مجازی‌سازی عملکرد شبکه (NFV) و شبکه‌های مبتنی بر نرم‌افزار (SDN)**: جدا سازی عملکردهای شبکه از سخت‌افزار اختصاصی و اجرای آن‌ها به صورت نرم‌افزار روی سرورهای استاندارد. این امر انعطاف‌پذیری و چابکی را افزایش می‌دهد اما امنیت لایه نرم‌افزار را بحرانی می‌سازد (۶).
۳. **خدمات ارتباطی با تأخیر بسیار پایین و قابلیت اطمینان بالا (URLLC)**: ضروری برای کاربردهای حیاتی مانند جراحی از راه دور یا کنترل صنعتی، که هر گونه اختلال امنیتی می‌تواند فاجعه‌بار باشد.
٤. **اتصال گسترده ماشین‌ها (mMTC)**: پشتیبانی از اتصال چگالی بسیار بالا (تا ۱ میلیون دستگاه در کیلومتر مربع) از دستگاه‌های IoT که چالش مدیریت هویت و احراز هویت را تشدید می‌کند (۷).

۳. تحلیل ریسک‌ها و چالش‌های امنیتی در اکوسیستم IoT-5G

ریسک‌های امنیتی در این فضا چندوجهی و درهم‌تنیده هستند. در جدول ۱ مهم‌ترین این ریسک‌ها بر اساس لایه دسته‌بندی شده‌اند.

جدول ۱: طبقه‌بندی ریسک‌های امنیتی در اکوسیستم IoT-5G

لایه	ریسک‌ها و آسیب‌پذیری‌های کلیدی	نمونه حملات بالقوه	پیامدهای احتمالی
دستگاه (IoT)	• محدودیت منابع (امنیت ضعیف) • نبود مکانیزم به‌روزرسانی امن • تنظیمات ناامن پیش‌فرض • رابط‌های فیزیکی ناامن (مثلاً USB)	• بدافزار (مثل باتنت‌های Mirai) • استراق سمع فیزیکی • دستکاری داده‌های سنسور	• تبدیل دستگاه به بوت‌نت برای حملات DDoS • اخلال در عملکرد سیستم فیزیکی • نقض حریم خصوصی
شبکه (5G و ارتباطات)	• پیچیدگی و نرم‌افزارمحوری (NFV/SDN) • آسیب‌پذیری در رابط‌های جدید (مثلاً بین اسلایس‌ها) • افزایش نقاط انتهایی (Edge) برای حمله • پروتکل‌های ارتباطی ناامن (در برخی IoTها)	• حمله به لایه کنترل SDN • استراق سمع در لایه رادیویی • جعل هویت در شبکه (Impersonation) • حملات روی اسلایس‌های مجاور	• اختلال گسترده در خدمات شبکه • سرقت داده‌های حساس در حال انتقال • دسترسی غیرمجاز به منابع شبکه
پلتفرم/ابر و داده	• تمرکز داده‌های عظیم در مراکز ابری	• نقض داده‌ها (Breach Data)	• افشای انبوه اطلاعات شخصی و تجاری

• دستکاری در نتایج تحلیل‌ها • اخلال در سرویس‌های حیاتی	• تزریق کد (مثل Injection SQL) • حملات روی کانتینرها/میکروسرویس‌ها	• پیچیدگی مدیریت دسترسی در محیط‌های چند ابری/هیبریدی • آسیب‌پذیری در APIها	
• دسترسی غیرمجاز به حساب‌ها و سیستم‌ها • جعل هویت دستگاه‌ها و ایجاد بین‌الملل مخرب	• فیشینگ و مهندسی اجتماعی • سرقت یا جعل نشانه‌های احراز هویت (Tokens) • حمله به دایرکتوری هویت مرکزی	• عدم آگاهی کاربران نهایی • سیستم‌های هویت‌سنجی متمرکز و تک نقطه شکست • چالش احراز هویت میلیون‌ها دستگاه	کاربر و مدیریت هویت

چالش‌های امنیتی خاص ناشی از همگرایی IoT و G۵:

- **مقیاس و تنوع:** مدیریت امنیتی میلیاردها دستگاه ناهمگن با پروفایل‌های امنیتی مختلف، عملاً با روش‌های سنتی غیرممکن است (۸).
- **حریم خصوصی (Privacy):** داده‌های جمع‌آوری‌شده توسط IoT اغلب بسیار شخصی و حساس هستند (موقعیت مکانی، عادات سلامتی، رفتار در منزل). انتقال این داده‌ها در شبکه G۵ با سرعت بالا، نگرانی‌های مربوط به نظارت توده‌ای و سوءاستفاده از داده‌ها را افزایش می‌دهد (۹).
- **زنجیره تأمین (Chain Supply):** دستگاه‌های IoT از اجزای ساخته‌شده توسط تأمین‌کنندگان مختلف تشکیل شده‌اند. یک آسیب‌پذیری در هر نقطه از این زنجیره می‌تواند کل اکوسیستم را به خطر بیندازد (مثل آسیب‌پذیری‌های مربوط به کتابخانه‌های منبع باز) (۱۰).
- **برش شبکه (Slicing) و امنیت:** اگرچه Slicing ایزوله‌سازی منطقی ایجاد می‌کند، اما اگر آسیب‌پذیری‌ای در هایپرویزور یا لایه اشتراکی زیرساخت وجود داشته باشد، ممکن است حمله از یک اسلایس به اسلایس دیگر گسترش یابد (۱۱). همچنین، مدیریت پیکربندی امنیتی ده‌ها یا صدها اسلایس مختلف، یک چالش عملیاتی بزرگ است.

۴. راهکارهای نوین امنیتی برای اکوسیستم IoT-۵G

مقابله با چالش‌های فوق نیازمند ترکیبی از راهکارهای فنی، حاکمیتی و انسانی است. در این بخش بر رویکردهای فنی نوین تمرکز می‌شود.

۱. معماری مبتنی بر سرویس (SBA) و امنیت ذاتی در هسته G۵:

هسته G۵ بر اساس معماری مبتنی بر سرویس (SBA) طراحی شده که در آن عملکردهای شبکه به صورت ماژولار و به عنوان سرویس‌هایی با APIهای استاندارد ارائه می‌شوند. این امر امکان اعمال **سیاست‌های امنیتی دینامیک و سرویس‌محور** را فراهم می‌کند. **چارچوب امنیتی SBA** شامل مکانیزم‌هایی مانند احراز هویت و مجوزدهی یکپارچه برای همه سرویس‌ها (با استفاده از

پروتکل‌هایی مانند OAuth ۲.۰ و Connect OpenID)، رمزنگاری مبتنی بر پروفایل (برای اسلایس‌های مختلف) و نظارت مستمر بر امنیت سرویس‌ها است (۱۲).

۲. استفاده از هوش مصنوعی و یادگیری ماشین (AI/ML):

با توجه به حجم عظیم داده‌های ترافیکی و لاگ‌ها در شبکه‌های IoT-۵G، **AI و ML به عنوان نیروهای توانمندساز کلیدی** برای امنیت مطرحند.

- **تشخیص ناهنجاری (Detection Anomaly)**: مدل‌های ML می‌توانند الگوهای عادی رفتار دستگاه‌ها، کاربران و ترافیک شبکه را یاد بگیرند و هرگونه انحراف مشکوک را به سرعت شناسایی کنند (۱۳). این امر برای تشخیص بوت‌نت‌ها یا دستگاه‌های به خطر افتاده بسیار موثر است.
- **تحلیل رفتاری:** تحلیل رفتار دستگاه‌های IoT برای شناسایی فعالیت‌های غیرمعمول (مثلاً یک سنسور دما که ناگهان شروع به ارسال حجم بسیار بالایی از داده می‌کند).
- **پاسخ خودکار به حوادث (Response Automated)**: سیستم‌های AI می‌توانند پس از شناسایی تهدید، به طور خودکار اقدامات متقابل اولیه را انجام دهند (مانند قرنطینه کردن دستگاه آلوده یا مسدود کردن ترافیک مخرب) (۱۴).

۳. رمزنگاری پیشرفته و سبک‌وزن:

- **رمزنگاری سبک‌وزن (Cryptography Lightweight)**: برای دستگاه‌های IoT با منابع محدود، الگوریتم‌های رمزنگاری جدیدی (مثل استانداردهای LWC NIST) طراحی شده‌اند که امنیت قابل قبولی با مصرف کم انرژی و پردازش ارائه می‌دهند (۱۵).
- **رمزنگاری هومومورفیک (Encryption Homomorphic)**: این تکنیک امکان پردازش و تحلیل داده‌های رمزنگاری‌شده بدون نیاز به رمزگشایی آن‌ها را فراهم می‌کند، که می‌تواند حریم خصوصی داده‌های حساس IoT در محیط‌های ابری را به طور چشمگیری افزایش دهد (۱۶).
- **کیفریت‌شناسی پساکوانتومی (Cryptography Post-Quantum)**: با توجه به تهدید بالقوه رایانش کوانتومی برای الگوریتم‌های رمزنگاری فعلی، تحقیق و توسعه الگوریتم‌های مقاوم در برابر کوانتوم برای زیرساخت حیاتی IoT-۵G ضروری است (۱۷).

۴. زنجیره بلوکی (Blockchain) برای هویت‌سنجی غیرمتمرکز و اعتماد:

Blockchain می‌تواند چندین مشکل امنیتی IoT-۵G را حل کند:

- **مدیریت هویت غیرمتمرکز دستگاه‌ها:** هر دستگاه IoT می‌تواند یک هویت دیجیتال منحصربه‌فرد و غیرقابل جعل در بلاکچین داشته باشد. احراز هویت و مجوز دسترسی می‌تواند از طریق قراردادهای هوشمند (Contracts Smart) و بدون نیاز به یک مرجع مرکزی انجام شود (۱۸).
- **یکپارچگی داده‌ها و ردیابی:** می‌توان از بلاکچین برای ثبت تغییرناپذیر داده‌های حیاتی یا رویدادهای امنیتی استفاده کرد، که این امر حسابرسی و ردیابی حملات را تسهیل می‌نماید.

- **امنیت زنجیره تأمین:** تاریخچه تولید و توزیع هر جزء سخت‌افزاری یا نرم‌افزاری می‌تواند در بلاکچین ثبت شود تا اصالت آن تأیید گردد (۱۹).

۵. معماری اعتماد صفر (ZTA - Zero Trust Architecture):

پارادایم سنتی "قلعه و خندق" (اعتماد به داخل شبکه، عدم اعتماد به خارج) در محیط‌های پراکنده و پیچیده IoT-۵G ناکارآمد است. **Zero Trust** بر این اصل استوار است: **"هرگز اعتماد نکن، همیشه اعتبارسنجی کن"**. در این مدل:

- دسترسی به منابع (داده، برنامه، شبکه) بر اساس **هویت**، **موقعیت**، **سلامت دستگاه** و سایر زمینه‌ها (context) به طور دینامیک اعطا می‌شود.
- دسترسی حداقلی (Privilege Least) به شدت اجرا می‌شود.
- تمام ترافیک (حتی داخل شبکه) بازرسی و لاگ می‌شود (۲۰).
- پیاده‌سازی ZTA در IoT-۵G نیازمند ترکیبی از فناوری‌های میکروسگمنتیشن (Microsegmentation)، احراز هویت قوی چندعاملی (MFA) و سیستم‌های مدیریت هویت و دسترسی (IAM) یکپارچه است.

۶. امنیت در لبه شبکه (Security Edge):

با انتقال پردازش به لبه شبکه (Computing Edge) برای کاهش تأخیر، امنیت این گره‌های لبه (Nodes Edge) حیاتی می‌شود. راهکارها شامل سخت‌سازی (Hardening) سیستم‌های لبه، استفاده از کانتینرهای امن (مثل با استفاده از Kata Containers)، و نظارت مستمر بر این گره‌ها است (۲۱).

۷. استانداردها و چارچوب‌های امنیتی:

اتکا به استانداردهای بین‌المللی برای امنیت یکنواخت ضروری است. استانداردهایی مانند **ETSI EN ۳۰۳ ۶۴۵** برای امنیت سایبری دستگاه‌های مصرفی IoT، **۸۲۵۹** برای مدیریت ریسک امنیت سایبری IoT، و چارچوب‌های صنعتی مانند **CSDE** از **GSMA** برای ارزیابی امنیت دستگاه‌های IoT در شبکه‌های موبایل، نقشه راه مهمی ارائه می‌دهند (۲۲, ۲۳).

۵. بحث و تحلیل: سنتز چالش‌ها و راهکارها

همگرایی IoT و G۵ یک محیط پویا و پیچیده ایجاد کرده است که در آن تهدیدات به طور مستمر تکامل می‌یابند. تحلیل حاضر نشان می‌دهد که **هیچ "راه حل جادویی" واحدی** برای امنیت این اکوسیستم وجود ندارد. بلکه موفقیت در گرو اتخاذ یک **رویکرد دفاع در عمق (Defense-in-Depth)** است که چندین لایه از کنترل‌های امنیتی مکمل را ترکیب می‌کند.

نکته کلیدی این است که بسیاری از راهکارهای نوین، متقابلاً تقویت‌کننده یکدیگر هستند. به عنوان مثال:

- **AI می‌تواند ZTA را تقویت کند:** مدل‌های ML می‌توانند برای ارزیابی ریسک دسترسی در لحظه (به عنوان بخشی از ZTA) مورد استفاده قرار گیرند و تصمیمات اعطا/عدم اعطای دسترسی را پویاتر و هوشمندتر کنند (۲۴).

- **Blockchain می‌تواند زیرساخت اعتماد برای IoT-۵G فراهم کند:** با ارائه هویت غیرمتمرکز و تغییرناپذیر، بستر مناسبی برای پیاده‌سازی اصول Trust Zero (احراز هویت قوی) و نیز ثبت قابل اطمینان رویدادهای امنیتی برای تحلیل AI فراهم می‌شود (۲۵).
- **SBA و NFV/SDN چابکی امنیتی را ممکن می‌سازند:** این معماری‌ها اجازه می‌دهند سرویس‌های امنیتی (مانند فایروال‌های مجازی، سیستم‌های تشخیص نفوذ) به صورت نرم‌افزاری و به سرعت در مکان‌های مورد نیاز در شبکه مستقر شوند (مثلاً در مرز یک اسلایس خاص).

با این حال، موانع مهمی بر سر راه وجود دارد: **پیچیدگی مدیریت** این راهکارهای ترکیبی، **همکاری بین ذینفعان** مختلف (اپراتورهای شبکه، تولیدکنندگان دستگاه‌های IoT، توسعه‌دهندگان اپلیکیشن، تنظیم‌کننده‌ها)، و **کمبود شدید نیروی انسانی متخصص** در امنیت سایبری IoT و ۵G. علاوه بر این، **ملاحظات حریم خصوصی و اخلاقی** در استفاده از فناوری‌هایی مانند AI برای نظارت بر ترافیک شبکه و رفتار کاربران، نیازمند چارچوب‌های قانونی و حاکمیتی قوی است (۲۶).

۶. نتیجه‌گیری و چشم‌انداز آینده

تحول دیجیتال مبتنی بر اینترنت اشیاء و شبکه‌های ۵G، فرصت‌های بی‌نظیری برای رشد اقتصادی، بهبود کارایی و افزایش کیفیت زندگی ایجاد کرده است. اما این تحول، به بهای افزایش چشمگیر پیچیدگی و مخاطرات امنیتی تمام می‌شود. این مقاله نشان داد که ریسک‌های امنیتی در اکوسیستم IoT-۵G چندلایه، مقیاس‌پذیر و پویا هستند و از محدودیت‌های دستگاه‌های ساده تا پیچیدگی‌های شبکه‌های نرم‌افزارمحور را در بر می‌گیرند.

راهکارهای نوین از جمله امنیت ذاتی در معماری SBA، بهره‌گیری از هوش مصنوعی برای تشخیص تهدید، پیاده‌سازی معماری Zero Trust، و استفاده از فناوری‌هایی مانند بلاکچین و رمزنگاری پیشرفته، جعبه ابزار قدرتمندی را در اختیار متخصصان امنیت قرار می‌دهند. با این حال، امنیت یک مقصد نیست، بلکه یک **سفر مستمر** است.

چشم‌انداز آینده و توصیه‌ها:

۱. **تمرکز بر امنیت از طراحی (Design by Security):** اصول امنیتی باید از همان مراحل اولیه طراحی معماری شبکه ۵G، پروتکل‌های ارتباطی و دستگاه‌های IoT گنجانده شود، نه به عنوان یک افزونه پس از تولید (۲۷).
۲. **تلاش برای همگرایی استانداردها:** جامعه بین‌الملل باید برای ایجاد استانداردهای امنیتی هماهنگ و الزام‌آور برای دستگاه‌های IoT و شبکه‌های ۵G تلاش کند تا از ایجاد جزیره‌های امنیتی ناسازگار جلوگیری شود.
۳. **آموزش و آگاهی‌سازی:** آموزش متخصصان امنیت در حوزه‌های جدید و همچنین افزایش آگاهی کاربران نهایی درباره ریسک‌های دستگاه‌های متصل، امری ضروری است.
٤. **تحقیق و توسعه مستمر:** با ظهور فناوری‌های جدید مانند **۶G** (که در افق تحقیق قرار دارد) و پیشرفت در محاسبات کوانتومی، تحقیقات در زمینه رمزنگاری پساکوانتومی، امنیت شبکه‌های هوشمندتر و روش‌های جدید برای حفاظت از حریم خصوصی باید با شتاب ادامه یابد (۲۸).

۵. **همکاری بین‌المللی:** ماهیت فراگیر و بدون مرز تهدیدات سایبری، نیازمند همکاری نزدیک بین کشورها، بخش خصوصی و آژانس‌های امنیتی برای اشتراک اطلاعات تهدید و بهترین تجربیات است.

در نهایت، تضمین امنیت در عصر IoT و G۵ نه تنها یک ضرورت فنی، بلکه یک پیش‌نیاز اساسی برای تحقق وعده‌های تحول دیجیتال و ایجاد اعتماد در جامعه دیجیتال آینده است.

منابع

۱. Ashton, K. (۲۰۰۹). That 'internet of things' thing. *RFID journal*, ۲۲(۷), ۹۷-۱۱۴.

۲. Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C. (۲۰۱۴). What will ۵G be? *IEEE Journal on selected areas in communications*, ۳۲(۶), ۱۰۶۵-۱۰۸۲.

۳. Al-Fuqaha, A., Guibene, W., Mohammadi, M., Aledhari, M., & Ayyash, M. (۲۰۱۵). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, ۱۷(۴), ۲۳۴۷-۲۳۷۶.

۴. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (۲۰۱۸). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, ۷۸, ۵۴۴-۵۴۶.

۵. Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J. J., Lorca, J., & Folgueira, J. (۲۰۱۷). Network slicing for ۵G with SDN/NFV: Concepts, architectures, and challenges. *IEEE Communications Magazine*, ۵۵(۵), ۸۰-۸۷.

۶. Hawilo, H., Jammal, M., & Shami, A. (۲۰۱۴). Network function virtualization-aware orchestrator for service function chaining placement in the cloud. *IEEE Journal on Selected Areas in Communications*, ۳۲(۱۰), ۱-۱۰.

۷. ۳GPP. (۲۰۲۰). *Technical Specification Group Services and System Aspects; Security architecture and procedures for ۵G system (Release ۱۶)*. ۳GPP TS ۳۳.۵۰۱.

۸. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (۲۰۱۵). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, ۷۶, ۱۴۶-۱۶۴.

۹. Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (۲۰۱۴). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, ۷(۱۲), ۲۷۲۸-۲۷۴۲.

۱۰. Newman, L. H. (۲۰۲۰). *The Massive, Unpatchable Security Risk in the Internet of Things*. Wired.

۱۱. Li ,X ,Samaka ,M ,Chan ,H .A ,Bhamare ,D ,Gupta ,L ,Guo ,C ,& Jain ,R) .۲۰۱۷ .(Network slicing for ۵G :Challenges and opportunities .*IEEE Internet Computing* ,۲۱)۵ ,(۲۰-۲۷.

۱۲. ۳GPP) .۲۰۱۹ .(*Technical Specification Group Services and System Aspects; System architecture for the ۵G System) ۵GS) (Release ۱۶* .۳GPP TS ۲۳.۵۰۱.

۱۳. Diro ,A .A ,& Chilamkurti ,N) .۲۰۱۸ .(Distributed attack detection scheme using deep learning approach for Internet of Things .*Future Generation Computer Systems* ,۸۲ , ۷۶۱-۷۶۸.

۱۴. Hussain ,F ,Hussain ,R ,Hassan ,S .A ,& Hossain ,E) .۲۰۲۰ .(Machine learning in IoT security :Current solutions and future challenges .*IEEE Communications Surveys & Tutorials* ,۲۲)۳ ,(۱۶۸۶-۱۷۲۱.

۱۵. NIST) .۲۰۲۱ .(*Lightweight Cryptography Standardization Process* .National Institute of Standards and Technology.

۱۶. Acar ,A ,Aksu ,H ,Uluagac ,A .S ,& Conti ,M) .۲۰۱۸ .(A survey on homomorphic encryption schemes :Theory and implementation .*ACM Computing Surveys) CSUR* ,(۵۱)۴ ,(۱-۳۵.

۱۷. Bernstein ,D J ,& Lange ,T) .۲۰۱۷ .(Post-quantum cryptography .*Nature* ,۵۴۹)۷۶۷۱ ,(۱۸۸-۱۹۴.

۱۸. Dorri ,A ,Kanhere ,S .S ,Jurdak ,R ,& Gauravaram ,P) .۲۰۱۷ .(Blockchain for IoT security and privacy :The case study of a smart home .In *۲۰۱۷ IEEE International Conference on Pervasive Computing and Communications Workshops) PerCom Workshops*) (pp .۶۱۸-۶۲۳ .(IEEE.

۱۹. Khan ,M .A ,& Salah ,K) .۲۰۱۸ .(IoT security :Review ,blockchain solutions ,and open challenges .*Future Generation Computer Systems* ,۸۲ ,۳۹۵-۴۱۱.

۲۰. Rose ,S ,.Borchert ,O ,.Mitchell ,S ,& Connelly ,S) .۲۰۲۰ .(*Zero Trust Architecture* .NIST Special Publication ۸۰۰-۲۰۷.

۲۱. Roman ,R ,.Lopez ,J ,& Mambo ,M) .۲۰۱۸ .(Mobile edge computing ,fog et al :.A survey and analysis of security threats and challenges .*Future Generation Computer Systems* , ۷۸ ,۶۸۰-۶۹۸.

۲۲. ETSI) .۲۰۲۰ .(*Cyber Security for Consumer Internet of Things :Baseline Requirements* . ETSI EN ۳۰۳ ۶۴۵ V۲.۱.۱.

۲۳. GSMA) .۲۰۱۹ .(*IoT Security Guidelines for Endpoint Ecosystems* .GSM Association.

۲۴. Gilman ,E ,& Barth ,D) .۲۰۱۷ .(*Zero Trust Networks :Building Secure Systems in Untrusted Networks* .O'Reilly Media.

۲۵. Panarello ,A ,.Tapas ,N ,.Merlino ,G ,.Longo ,F ,.& Puliafito ,A) .۲۰۱۸ .(Blockchain and IoT integration :A systematic survey .*Sensors* ,۱۸)۸ ,(۲۵۷۵.

۲۶. Taddeo ,M) .۲۰۱۷ .(Data philanthropy and the design of the infrastructure for artificial intelligence .*Philosophical Transactions of the Royal Society A :Mathematical ,Physical and Engineering Sciences* ,۳۷۶)۲۱۳۳ ,(۲۰۱۷۰۳۲۳.

۲۷. Shostack ,A) .۲۰۱۴ .(*Threat Modeling :Designing for Security* .John Wiley & Sons.

۲۸. Letaief ,K .B ,.Chen ,W ,.Shi ,Y ,.Zhang ,J ,.& Zhang ,Y .J) .۲۰۱۹ .(The roadmap to ۶G :AI empowered wireless networks .*IEEE Communications Magazine* ,۵۷)۸ ,(۸۴-۹۰.

۲۹. Chettri ,L ,.& Bera ,R) .۲۰۲۰ .(A comprehensive survey on Internet of Things) IoT (toward ۵G wireless systems .*IEEE Internet of Things Journal* ,۷)۱ ,(۱۶-۳۲.

۳۰. He ,D ,.Chan ,S ,.& Guizani ,M) .۲۰۱۷ .(Security in the Internet of Things supported by mobile edge computing .*IEEE Communications Magazine* ,۵۵)۱۲ ,(۵۶-۶۱.