رایانش امن در اینترنت همه چیز

* سیدامید آذرکسب ** سیدحسین خواسته

* استاد مدعو و دانشجوی دکترای تخصصی مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران seyedomid.azarkasb@email.kntu.ac.ir

** دکترای تخصصی مهندسی کامپیوتر گرایش هوش مصنوعی، استادیار و عضو هیئت علمی دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران khasteh@kntu.ac.ir

تاریخ دریافت: ۱۴۰۰/۱۱/۲۳ تاریخ پذیرش: ۱۴۰۲/۰۶/۰۳

صص: ۹۵- ۱۰۸

چکیده

با پیشرفت فناوری و رشد چشمگیر اینترنت همه چیز، نیاز به رایانش امن در این زمینه افزایش یافته است. اینترنت همه چیز امکان اتصال و ارتباط بین اشیاء، داده‌ها، فرایندها و افراد را فراهم می‌کند، از جمله سامانه‌ها، دستگاه‌های خانگی، خودروهای هوشمند، سیستم‌های صنعتی و بسیاری دیگر. با این حجم عظیم از اشیاء متصل، امنیت اطلاعات و حریم خصوصی تبدیل به یک چالش مهم در رایانش اینترنت همه چیز شده است. در این مقاله، به بررسی مفهوم رایانش امن در اینترنت همه چیز پرداخته می‌شود. تأثیر اینترنت همه چیز بر مفهوم امنیت و نیازهای مرتبط با آن بررسی می‌شود. همچنین، روش‌ها و فناوری‌های مورد استفاده برای ایجاد رایانش امن در اینترنت همه چیز مورد بررسی قرار می‌گیرد. از جمله موضوعات مورد اشاره در این مقاله می‌توان به رمزنگاری اطلاعات، شناسایی و احراز هویت، مدیریت دسترسی، حفاظت از حریم خصوصی و تشخیص تهدیدات امنیتی اشاره کرد. علاوه بر این، چالش‌ها و معایب رایانش امن در اینترنت همه چیز نیز مورد بررسی قرار می‌گیرند. مسائلی مانند پیچیدگی محیط متصل شده، تهدیدات امنیتی پویا، نیاز به استانداردها و مسائل مرتبط با امنیت، و تأثیر تغییرات فناوری در رایانش امن مورد بحث قرار می‌گیرند. در نهایت، راهکارها و پیشنهادهایی برای بهبود رایانش امن در اینترنت همه چیز ارائه می‌شوند. این پیشنهادها شامل استفاده از رمزنگاری قوی، مدیریت دسترسی متمرکز، آموزش و آگاهی کاربران، استفاده از سیستم‌های تشخیص تهدیدات و مانیتورینگ پیشرفته است. با توجه به این مقاله، امید است که وضوح بهتری از رایانش امن در اینترنت همه چیز به دست آید و راهکارهای امنیتی مناسب برای این حوزه توسعه یابد.

واژه‌های کلیدی: اینترنت همه چیز، رایانش امن، امنیت اطلاعات، حریم خصوصی، اشیاء متصل، چالش‌های رایانش امن.

نوع مقاله: علمی

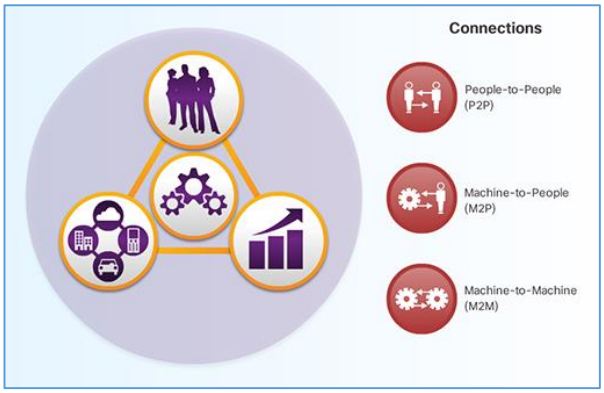
۱- مقدمه

در دنیای امروز، اینترنت همه چیز به عنوان یک پدیده فراگیر و نوآورانه در حوزه فناوری اطلاعات و ارتباطات جهانی شناخته می‌شود. اینترنت همه چیز مفهومی هست که شرکت سیسکو به منظور معرفی شکل گسترده تر و رشد یافته اینترنت اشیا مطرح کرده است [۱].

اینترنت همه چیز امکان ارتباط و اتصال همزمان بین اشیا، دستگاه‌ها، داده‌ها و افراد را فراهم می‌کند [۲]. از دستگاه‌های هوشمند خانگی و تجاری گرفته تا خودروهای هوشمند، سیستم‌های صنعتی و شهرهای هوشمند، همه به اینترنت متصل شده‌اند. با اتصال این چهار عنصر به معماری اینترنت، فضایی لایه‌ای و یکپارچه شکل می‌گیرد که در گره‌خوردن با هوش مصنوعی گستره حکمرانی جدیدی را شکل می‌دهد. در مدل

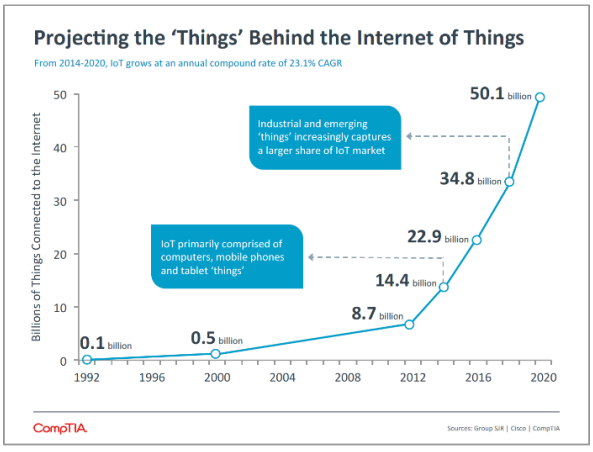
نویسنده عهده‌دار مکاتبات: سیدامید آذرکسب Seyedomid.azarkasb@email.kntu.ac.ir

کسب و کار اینترنت همه چیز افراد، جزئی از منابع هستند که در شکل ۲ قابل مشاهده است [۳].



شکل ۱. اجزای اینترنت همه چیز [۳]

آنچه اینترنت همه چیز را متمایز از اینترنت اشیاء می‌کند، این است که در اینترنت اشیا این دستگاه‌ها، ماشین یا ابزارها هستند که به یکدیگر متصل می‌شوند اما در اینترنت همه چیز، در سطحی بالاتر، باید این ارتباطات گسترده‌تر شده و مهم‌تر اینکه این ارتباطات درک شوند. در واقع آنچه چالش و شکل دهنده آینده اینترنت همه چیز است نحوه برقرار ارتباط بین دستگاهها و انسان‌هاست که شرکت‌های بسیاری در حال حل این معضل هستند [۴]. رشد سریع سرعت اتصالات در شکل ۲ مشاهده می‌گردد [۵].



شکل ۲- رشد سریع اتصالات و تعداد دستگاه‌ها [۵]

با این حجم عظیم از ارتباطات و اشتراک داده‌ها، نیازمندی‌های امنیتی در اینترنت همه چیز برجسته‌تر و حیاتی‌تر از همیشه شده است. یکی از چالش‌های اساسی در اینترنت همه چیز، مسائل امنیتی و حفاظت از اطلاعات است. با توجه به ترکیبی از اشیاء، داده‌ها، فرایندها و افراد، امنیت اینترنت همه چیز نیازمندی‌های امنیتی خاص و پوشش سطوح مدیریتی بیشتری نسبت به امنیت اینترنت اشیا دارد. بر همین اساس، حفاظت از حریم خصوصی در اینترنت همه چیز به یک موضوع مهم و حیاتی در حوزه امنیت تبدیل شده است. عدم رعایت مسائل امنیتی و نقض حریم خصوصی می‌تواند منجر به سوء استفاده از اطلاعات حساس، تهدیدات سایبری و خسارات قابل توجهی برای سازمان‌ها و افراد شود.

معماری امنیتی موجود که از منظر ارتباطات انسانی طراحی شده است، ممکن است برای پیاده‌سازی بر روی عملکرد بین اشیا مناسب نباشد. به همین دلیل، نیاز به راهکارها و فناوری‌هایی است که بتوانند امنیت و حفاظت از اطلاعات در اینترنت همه چیز را بهبود بخشند. از رمزنگاری اطلاعات و شناسایی و احراز هویت تا مدیریت دسترسی، حفاظت از حریم خصوصی و تشخیص تهدیدات امنیتی، همه این عوامل مهم در برابر تهدیدات و حملات سایبری مورد نیازند.

فرضیه ما در این مقاله این است که رایانش امن در اینترنت همه چیز نیازمندی‌های امنیتی خاص و پوشش سطوح مدیریتی بیشتری نسبت به امنیت اینترنت اشیا دارد. با توجه به ترکیبی از اشیاء، داده‌ها، فرایندها و افراد در اینترنت همه چیز، حفاظت از حریم خصوصی به یک موضوع مهم امنیتی در این حوزه تبدیل شده است. با توجه به فرضیه مطرح شده، سوال اصلی این است که چگونه می‌توان نیازمندی‌های امنیتی در رایانش امن در اینترنت همه چیز را شناسایی کرد و راهکارها و فناوری‌هایی را ارائه داد که بتوانند امنیت و حفاظت از اطلاعات و حریم خصوصی در این حوزه را بهبود بخشند؟ با بررسی مفاهیم، روش‌ها و تکنیک‌های موجود، ما به دنبال پاسخ دادن به این سوال اصلی هستیم تا بتوانیم به رایانش امن و پایدار در اینترنت همه چیز نزدیک‌تر شویم.

۲- پیش‌رانها و سطوح تاثیر اینترنت همه چیز

پیش‌ران‌های اینترنت همه چیز بر اساس آخرین دستاوردها و تحولات فناوری به شکل پویا تغییر می‌کنند. این عوامل به طور گسترده شامل موارد زیر می‌شوند:

۱.روندهای نیرومند فناوری: افزایش توان پردازش، ذخیره‌سازی و پهنای باند با هزینه کاهش یافته، رشد سریع رایانش ابری، رایانش در حرکت، قابلیت تحلیل حجم عظیمی از داده‌ها و ترکیب فناوری‌های سخت‌افزاری و نرم‌افزاری جهت ارزش‌آفرینی بیشتر از رهگذر ارتباطات.

۲.کاهش مداوم موانع ارتباطی: موانع ارتباطی از جمله محدودیت‌های پروتکل اینترنتی IPv4 و جابجایی به IPv6، کاهش تعداد آدرس‌های آی‌پی موجود، میانجی‌گرهای شبکه و سطوح اتصال بیشتر را کاهش می‌دهند. برای مثال، آدرس‌دهی IPv6 می‌تواند تعداد بسیار بیشتری (حدود ۳۴۰ میلیارد میلیارد میلیارد[۱]) از ارتباطات بین انسان‌ها، فرایندها، داده‌ها یا اشیاء را فراهم کند [۶].

۳.توسعه ضریب‌های شکلی: اندازه کوچک و شکل فشرده رایانه‌ها، حافظه‌های نازک، حسگرها و آنتن‌ها امکان اتصال اشیاء کوچک‌تر را فراهم می‌کند. امروزه رایانه‌هایی به اندازه دانه نمک قادر به جایگزینی منابع مختلف می‌باشند. این تحولات در آینده ممکن است منجر به وجود اشیاءی شود که قابلیت دیدن برای چشم انسان را نداشته و در ابعاد بسیار کوچکتر و بی‌نهایت باریک باشند.

۴.رشد سریع رسانه‌های اجتماعی: رسانه‌های اجتماعی و تحولات آنها، مثل فراهم کردن زیرساخت‌های شبکه‌ای پویا و افزایش تعاملات بین افراد، اشیاء و داده‌ها، به عنوان یک پیش‌ران مهم در اینترنت همه چیز عمل می‌کنند.

۵.توانایی تحلیل و استفاده از داده: استفاده از هوش مصنوعی، یادگیری ماشین و تحلیل داده‌های بزرگ، به ما امکان می‌دهد تا از داده‌های به دست آمده از اشیاء و دستگاه‌ها برای ارائه تصمیمات هوشمندانه و بهبود عملکرد استفاده کنیم.

این پیش‌ران‌ها در تکامل اینترنت همه چیز و اتصال اشیاء به شبکه با توجه به نیازها و تحولات فناوری بهبود می‌یابند و نقش مهمی در شکل‌دهی به آینده این حوزه ایفا می‌کنند. در ادامه ده بینش برتر مطلوب که در این حوزه می‌توانند تاثیر گذار باشد بیان می‌شود [۷]:

۱. سازمان‌های بخش دولتی و نوآوران برجسته دارای نقش بسیار مهمی در توسعه اینترنت همه چیز هستند.

۲. استفاده از استراتژیهای جامع در سطح شهرها به عنوان یک منبع ارزش در اینترنت همه چیز توصیه می‌شود.

۳. ایجاد یک شبکه قدرتمند و پایدار، امکان‌پذیری و قابلیت استفاده از اینترنت همه چیز را بهبود می‌بخشد.

۴.سازمان‌های عمومی نقشی بسیار مهم در هدایت نوآوری در حوزه اینترنت همه چیز دارند.

۵.تجزیه و تحلیل داده‌ها از طریق استفاده از تکنیک‌های مربوط به اینترنت همه چیز، تأثیر چشمگیری در بهبود عملکرد و ارزش ایجاد شده دارد.

۶.اینترنت همه چیز به صورت یک برنامه جهانی و جامع عمل می‌کند.

۷.راه حل‌های مرتبط با اینترنت همه چیز باید به صورت جامع و شامل افراد و فرایندها مورد بررسی قرار گیرند و نباید فقط به داده‌ها و اشیا متمرکز شوند.

۸.اینترنت همه چیز کمک می‌کند تا سیلوهای سازمانی را برداشته و ارتباط و همکاری میان سازمان‌ها را تسهیل کند.

۹.شفافیت و داده باز انگیزه‌بخشی برای ذینفعان و بازیگران در حوزه اینترنت همه چیز است.

۱۰. هدایت یکپارچه و در نظر گرفتن منافع عمومی قابل ملاحظه، از عوامل کلیدی موفقیت در حوزه اینترنت همه چیز می‌باشد

اینترنت همه چیز یک اکوسیستم گسترده است که از اتصالات شامل فناوری‌ها، فرایندها و مفاهیم مختلف تشکیل شده است. در دسته‌بندی‌های مختلف، اینترنت انسان‌ها، اینترنت دیجیتال، اینترنت اشیا صنعتی و فناوری‌های ارتباطی و حتی خود اینترنت به عنوان زیرمجموعه‌های اینترنت همه چیز شناخته می‌شوند. اینترنت دیجیتال به دامنه اول دیجیتال اشاره دارد، به این معنی که در اینترنت سنتی داده‌های دیجیتال به سهولت قابل دسترسی هستند. همچنین، اینترنت اشیا به اتصال دامنه فیزیکی اشیا و دستگاه‌ها مرتبط است، که در آن حسگرها و عملگرها اطلاعات را تولید می‌کنند [۸]. سازمان‌ها که از راه‌حل‌های اینترنت اشیاء بهره می‌برند، به منظور نوآوری در یک جهان متصل به یکدیگر، فرایندهای خود را تغییر می‌دهند. اینترنت همه چیز یک زیرساخت فناورانه است که سازمان‌های بخش خصوصی و دولتی را در راستای بهره‌وری، بهینه‌سازی هزینه‌ها، نوآوری، بهبود جامعه، توسعه ملی، امنیت ملی و مدیریت منابع جهانی هدایت می‌کند. اینترنت همه چیز کلیدی است که به فناوری امکان می‌دهد تا توسعه اینترنت اشیاء را با استفاده از ابزارهایی مانند متحرک سازی، ابر، داده‌های حجیم و سایر فناوری‌هایی که به ارتباط بین افراد و اشیا

[۱] رقم دقیق ۳۴۰،۲۸۲،۳۶۶،۹۲۰،۹۳۸،۴۶۳،۳۷۴،۶۰۷،۴۳۱،۷۶۸،۲۱۱،۴۵۶

کمک می‌کنند، پشتیبانی کند [۹]. سطوح تأثیر اینترنت همه‌چیز در سه سطح فرآیند تجاری، مدل تجاری و زمان تعریف می‌شوند [۱۰]. استفاده از فناوری‌های اینترنت همه چیز باعث ارتقاء محصولات، خدمات، مشتریان و تجربه‌های مرتبط در سازمان‌ها می‌شود. شرکت‌ها در حال دیجیتال شدن محصولات و فرآیندهای خود هستند و با ظهور روش‌های تجارت جدید، صنایع نیز در سطح مدل تجاری تغییر می‌کنند. به عنوان مثال، شرکت نایکی در حوزه سلامت و لباس‌های متصل به اینترنت فعالیت می‌کند و گوگل وارد حوزه خودروهای بدون سرنشین شده است. در ادامه سطح سوم نوآوری دیجیتال به وجود آمده است به دلیل نیاز به رقابت با سایر تجارت‌ها. اینترنت همه‌چیز شامل میلیون‌ها قطعه، سنسور یا حسگر جدید است که داده‌های بزرگ را فراهم می‌کنند. در حال حاضر، داده‌ها ارزشمندترین دارایی هستند و تجارت برای تحلیل و بهره‌برداری از آن‌ها نیاز به فناوری‌های ذخیره و جمع‌آوری داده دارد. همچنین، برای تبدیل داده به سرمایه، رهبران تجارت و فناوری اطلاعات نیاز به تصمیم‌گیری سریع دارند. در این راستا، ابزارهای پردازش داده مورد نیاز هستند. از سوی دیگر، دیو آرون، محقق شرکت گارتنر، تأکید می‌کند که دیجیتال بودن دیگر یک گزینه نیست و به یک واقعیت جدید تبدیل شده است. شرکت‌ها نیاز به استراتژی دیجیتال خود را دارند و رهبری قوی در این حوزه ضروری است. در نهایت، شرکت گارتنر پیش‌بینی می‌کند که شرکت‌ها از فناوری اینترنت همه‌چیز به صورت گسترده استفاده خواهند کرد و محصولات متنوعی در بازارهای مختلف عرضه خواهند کرد. این شامل استفاده از ابزارهای پزشکی پیشرفته، حسگرهای خودکارسازی در کارخانه‌ها، ربات‌ها در صنایع، بهبود محصولات کشاورزی با استفاده از سنسورها، سیستم‌های نظارتی بر زیرساخت‌ها و تعداد بیشماری از محصولات است[۱۱]. البته با اتصال ابزارهای بیشتر به اینترنت، نگرانی در مورد امنیت داده‌ها و حریم‌خصوصی نیز افزایش خواهد یافت. روشی که شرکت‌ها برای حفظ تعادل این پیشرفت‌ها و حفظ حریم‌خصوصی مشتریان، اتخاذ می‌کنند نیز خود بسیار مهم خواهد بود[۱۲].

۳- الزامات زیرساختی و پیشرفت‌های کلیدی

در راستای توسعه و پیشرفت اینترنت همه چیز، اصول و الزامات زیرساختی حائز اهمیت بالایی هستند. برای رسیدن به عملکرد بهینه و مدیریت صحیح اینترنت همه چیز، نیاز به فناوری‌ها و مفاهیم کلیدی خاصی وجود دارد. این الزامات زیرساختی و مفاهیم کلیدی، عوامل اساسی برای ایجاد ارتباط و هماهنگی بین اشیا، دستگاه‌ها و فرآیندها در سرتاسر اینترنت همه چیز محسوب می‌شوند. در این بخش از مقاله، ما به بررسی و تبیین این الزامات و مفاهیم کلیدی مورد نیاز در اینترنت همه چیز می‌پردازیم. فناوری‌هایی مانند رایانش‌های نوین ابری و مه، کلان داده، بلاکچین، احراز هویت یکپارچه، نرم‌افزارهای متن باز، فناوری فایوجی و پلتفرم اینترنت اشیاء به عنوان عناصر اصلی این الزامات مورد بررسی قرار می‌گیرند. با آشنایی و درک درست از این فناوری‌ها و مفاهیم کلیدی، می‌توانیم اینترنت همه چیز را به صورت امن، قابلیت‌پذیر و پایدار پیاده‌سازی کنیم. به منظور بررسی و تحلیل عمیق‌تر این الزامات زیرساختی و مفاهیم کلیدی، در ادامه مقاله به هر یک از آنها به صورت جداگانه و با جزئیات بیشتر خواهیم پرداخت.

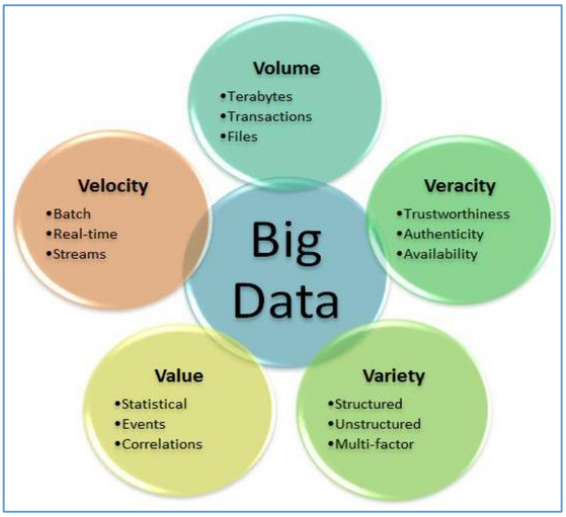
۳-۱- رایانش‌های نوین

رایانش ابری و تکامل یافته آن رایانش مه، در سطح کلان به معنای ارائه منابع محاسباتی مانند سرورها، ذخیره‌سازی داده، برنامه‌ها و سرویس‌ها از طریق اینترنت به صورت متمرکز یا محلی است [۱۳]. این رویکرد ضمن بهره‌گیری از مجازی‌سازی منابع به سازمان‌ها و کاربران امکان می‌دهد تا به صورت انعطاف‌پذیر و مقیاس‌پذیری به منابع مورد نیاز خود دسترسی داشته باشند. با استفاده از رایانشهای نوین در اینترنت همه چیز، سازمان‌ها و کاربران قادرند منابع محاسباتی را بر اساس نیازهای خود به سرعت ایجاد و مدیریت کنند. آن‌ها قادرند به راحتی منابع را افزایش داده و کاهش دهند، به صورت پرداخت متناسب با استفاده و تنظیمات سفارشی‌سازی شده به منابع دسترسی داشته باشند. این رایانشها همچنین بهبود امنیت در رایانش اینترنت همه چیز را به ارمغان می‌آورد. با استفاده از خدمات امنیتی ابری، مانند رمزنگاری داده، شناسایی دسترسی، مانیتورینگ و حفاظت از حریم خصوصی، سازمان‌ها می‌توانند از امنیت مطمئنی برخوردار شوند [۱۴].

۳-۲- کلان داده

کلان داده به مجموعه‌ای از داده‌های بزرگ و پیچیده اشاره دارد که از منابع متعددی نظیر حسگرها،

دستگاه‌های متصل به اینترنت، سامانه‌های آنلاین، شبکه‌های اجتماعی و دیگر منابع داده‌ای به دست می‌آیند. این داده‌ها به حجم عظیمی نیاز دارند که با استفاده از فناوری‌های پردازش موازی و سیستم‌های توزیع شده، ذخیره و پردازش شوند. یکی از امکانات موجود در حوزه کلان داده، نگاشت است. نگاشت به معنای تبدیل و ترسیم داده‌ها به صورتی که بتوان اطلاعات مفید و قابل فهم را از آنها استخراج کرد. این امر به واسطه استفاده از الگوریتم‌ها و تکنیک‌های مختلفی مانند تکنیک‌های ماشین بینایی ماشین، یادگیری ماشین، پردازش زبان طبیعی، استنتاج و استخراج اطلاعات انجام می‌شود. با نگاشت داده‌ها، می‌توان الگوها، روندها و اطلاعات مهم را شناسایی کرده و از آنها برای تصمیم‌گیری‌های استراتژیک و پیش‌بینی‌های دقیق استفاده کرد. در کنار نگاشت، کاهش نیز یکی دیگر از امکانات مهم در کلان داده است. با کاهش داده‌ها، حجم زیادی از اطلاعات قابل‌فهم و قابل‌استفاده حفظ می‌شود. این امر باعث می‌شود تا به جای دسترسی و پردازش همه‌ی داده‌ها، فقط داده‌های مهم و ارزشمند برای تحلیل و استفاده انتخاب شوند، که باعث افزایش سرعت پردازش و کاهش هزینه‌ها می‌شود [۱۵]. استفاده از کلان داده در رایانش امن در اینترنت همه چیز، به سازمان‌ها امکان می‌دهد تا به صورت موثرتر و هوشمندانه‌تر با داده‌ها برخورد کنند. با تحلیل کلان داده‌ها، می‌توان عملکردهای سیستم را بهبود بخشید، تشخیص تهدیدات امنیتی را سریعتر انجام داد و تصمیم‌گیری‌های استراتژیک را بر اساس اطلاعات قابل اعتماد انجام داد همان‌طور که از تعاریف کلان داده نیز برمی‌آید، پنج ویژگی یا بُعد عمومی باید در داده وجود داشته باشد که بتوان آن را کلان داده تلقی کرد. ارزش، حجم داده، نرخ تولید، تنوع و صحت که در شکل ۳ نشان داده شده است [۱۶].



شکل ۳. ابعاد عمومی کلان داده [۱۶]

۳-۳- بلاکچین

زنجیره بلوکی یا بلاکچین یک فناوری مبتنی بر دیجیتال است که به طور معمول با انتقال اطلاعات بین اعضای شبکه بدون واسطه کار می‌کند. این فناوری از یک سری بلوک‌های متصل به یکدیگر تشکیل شده است، هر بلوک حاوی اطلاعاتی از تراکنش‌ها و رکوردهای قبلی است و با استفاده از توابع رمزنگاری قابل تأیید است [۱۷]. بلاکچین به دلیل خصوصیت‌های امنیتی و شفافیتی که دارد، می‌تواند نقش مهمی در رایانش امن در اینترنت همه چیز ایفا کند. در برخی از حوزه‌ها مانند انتقال و تبادل ارزهای رمزنگاری شده، زنجیره بلوکی به عنوان یک زیرساخت امن و قابل اعتماد استفاده می‌شود. تمامی تراکنش‌ها در بلاکچین ثبت می‌شوند و نمی‌توان آنها را به‌صورت دلخواه تغییر داد، این امر باعث ایجاد اعتماد و امنیت در معاملات اینترنتی می‌شود. به‌عنوان مفهوم کلیدی در رایانش امن در اینترنت همه چیز، بلاکچین می‌تواند به حل برخی از چالش‌های امنیتی مرتبط با انتقال و ذخیره داده‌ها کمک کند. برخی از ویژگی‌های بلاکچین که در اینترنت همه چیز می‌تواند مورد استفاده قرار گیرد عبارتند از:

- امنیت: بلاکچین با استفاده از الگوریتم‌های رمزنگاری قوی و تأیید تراکنش‌ها توسط شبکه از امنیت بالایی برخوردار است. این ویژگی امنیتی بلاکچین را برای انتقال و ذخیره داده‌ها در اینترنت همه چیز مورد استفاده قرار می‌دهد.

- شفافیت: بلاکچین با ثبت تمامی تراکنش‌ها و رکوردهای قبلی در بلوک‌ها، امکان بررسی و تأیید صحت تراکنش‌ها را فراهم می‌کند. این شفافیت در انتقال داده‌ها در اینترنت همه چیز می‌تواند اعتماد بیشتری را به‌وجود آورده و فرآیندهای امنیتی را تقویت کند.
- اعتماد و همکاری: بلاکچین با ایجاد یک شبکه توزیع‌شده و بدون واسطه، اعتماد و همکاری بین اعضای شبکه را تسهیل می‌کند. در اینترنت همه چیز، امکان ایجاد همکاری بین دستگاه‌ها و اشتراک داده‌ها برای اهداف مختلف را فراهم می‌کند.

۳-۴- احراز هویت یکپارچه

احراز هویت یکپارچه در رایانش امن در اینترنت همه چیز از اهمیت بالایی برخوردار است. در این محیط پیچیده و متنوع، احراز هویت صحیح و قابل اعتماد افراد و دستگاه‌ها از اهمیت بسیاری برخوردار است. احراز هویت یکپارچه به معنای استفاده از یک سیستم واحد و یکپارچه برای تشخیص و اثبات هویت افراد و دستگاه‌ها در سراسر بستر اینترنت همه چیز است. با توجه به اینکه در اینترنت همه چیز همه جا و همیشه به هم متصل است، احراز هویت یکپارچه باعث می‌شود تا هر فرد و دستگاه تنها با یک مجموعه احراز هویت قابل اعتماد، به تمامی منابع و سرویس‌های موجود دسترسی داشته باشد. این باعث ساده‌تر و موثرتر شدن فرآیند احراز هویت و کاهش تکرار آن برای هر منبع و سرویس مختلف می‌شود. یکی از راه‌های احراز هویت یکپارچه در رایانش امن در اینترنت همه چیز استفاده از فناوری‌های شناخت بیومتری است. این فناوری‌ها، بر اساس خصوصیات منحصر به فرد فردانه‌ای مانند اثر انگشت، شناسایی چهره، اسکن عنبیه و غیره، هویت افراد را تشخیص می‌دهند. با این روش، هویت فرد براساس ویژگی‌های فیزیولوژیکی یا رفتاری مشخص می‌شود و امکان تقلب و سرقت هویت کاهش می‌یابد. همچنین، استفاده از روش‌های رمزنگاری قوی و پروتکل‌های امنیتی مطمئن می‌کند که فرآیند احراز هویت در اینترنت همه چیز به صورت ایمن و غیرقابل تغییر انجام شود. این پروتکل‌ها مانع از هرگونه نفوذ غیرمجاز و سوءاستفاده از اطلاعات هویتی می‌شوند [۱۸]. در نهایت، احراز هویت یکپارچه در رایانش امن در اینترنت همه چیز بهبود امنیت و محرمانگی اطلاعات را بهبود می‌بخشد و اطمینان می‌دهد که فقط افراد مجاز به دسترسی به منابع مورد نیاز خواهند بود. این مسئله به ویژه در محیط‌هایی که حاوی اطلاعات حساس و مهم هستند، از اهمیت بسیاری برخوردار است.

۳-۵- فناوری‌های متن باز

نرم‌افزارهای متن باز و نوآوری‌های متن باز یکی از مفاهیم کلیدی در رایانش امن در اینترنت همه چیز می‌باشند. این نوع نرم‌افزارها و نوآوری‌ها از طریق ارائه کدهای منبع باز و اجازه استفاده، توسعه و تغییر آزاد از سوی جامعه‌ی علاقمندان، توسعه می‌یابند. آن‌ها بر اساس اصول شفافیت، همکاری و به اشتراک گذاری دانش و منابع ساخته شده‌اند. استفاده از نرم‌افزارهای متن باز در رایانش امن در اینترنت همه چیز دارای مزایای فراوانی است. این نرم‌افزارها به جامعه علاقمندان امکان می‌دهند تا در بهبود و توسعه آن‌ها مشارکت کنند و از پتانسیل همکاری جمعی برای رسیدن به امنیت و کارایی بالاتر برخوردار شوند. علاوه بر این، استفاده از نرم‌افزارهای متن باز باعث افزایش شفافیت و اعتماد عمومی در رابطه با امنیت نرم‌افزارها می‌شود. نوآوری‌های متن باز نیز در راستای رایانش امن در اینترنت همه چیز بسیار حائز اهمیت هستند. این نوآوری‌ها شامل تکنیک‌ها، روش‌ها و الگوریتم‌هایی هستند که با توجه به طبیعت پویا و پیچیده اینترنت همه چیز، بهبود امنیت و محافظت از داده‌ها و دستگاه‌ها را بهبود می‌بخشند. برخی از نوآوری‌های متن باز مورد استفاده در رایانش امن شامل رمزنگاری قوی، مدیریت هویت و دسترسی، تشخیص تهدیدات، حفاظت از حریم خصوصی و مدیریت کلید است [۱۹]. از مزایای استفاده از نرم‌افزارهای متن باز می‌توان به موارد زیر اشاره کرد:

- انعطاف‌پذیری: این نرم‌افزارها قابلیت تغییر و تنظیم به نیازهای خاص را دارند و به جامعه علاقمندان اجازه می‌دهند تا در بهبود و توسعه آن‌ها مشارکت کنند.
- شفافیت: با عرضه کد منبع، شفافیت بالایی در مورد عملکرد و امنیت نرم‌افزار فراهم می‌شود. همه علاقمندان می‌توانند کد را بررسی و ارزیابی کنند و از نظرات و بازخوردهای آن‌ها برای بهبود کیفیت و امنیت نرم‌افزار استفاده کرد.
- همکاری: نرم‌افزارهای متن باز از توانمندی همکاری جمعی برای توسعه و بهبود استفاده می‌کنند. جامعه‌ی

علاقمندان می‌توانند با یکدیگر همکاری کنند و تجربیات و دانش خود را در اختیار هم قرار دهند.

-توسعه سریع: با امکان تغییر و توسعه باز نرم‌افزارها، توسعه‌دهندگان می‌توانند به سرعت به نیازهای جدید پاسخ دهند و نسخه‌های به‌روز و پیشرفته‌تر را منتشر کنند.

۶-۳-فناوری فایوجی

فناوری فایوجی یک پیشرفت بزرگ در عرصه ارتباطات بی‌سیم است و قابلیت‌های بسیاری را در اینترنت همه چیز به ارمغان می‌آورد. با عرضه شبکه فایوجی ، سرعت، پایداری، ظرفیت بالا و زمان پاسخ کمتری نسبت به نسل‌های قبلی شبکه فراهم می‌شود. این فناوری قادر است به طور همزمان با تعداد بسیار بالای دستگاه‌ها و اشیاء متصل در شبکه ارتباط برقرار کند و عملکرد صحیح و مطمئن را ارائه دهد. فناوری فایوجی اهمیت بسیاری در رایانش امن در اینترنت همه چیز دارد. از طریق ارائه ارتباطات پرسرعت و پایدار، شبکه قابلیت پشتیبانی از برنامه‌ها و سرویس‌های متنوع را فراهم می‌کند. این شبکه قادر است با سرعت فوق‌العاده بالا، حجم زیادی از داده‌ها را به سرورهای ابری منتقل کند و پردازش مورد نیاز را به طور موثر انجام دهد. همچنین، بستر ارتباطی فایوجی قابلیت ارائه خدمات امن و احراز هویت مطمئن را داراست که در حفظ حریم خصوصی و امنیت داده‌ها و اطلاعات حساس اهمیت دارد. به عنوان مثال، در اینترنت همه چیز، اشیاء متصل به شبکه فایوجی می‌توانند به طور مستقیم با سرویس‌های ابری و سرویس‌های مرتبط با رایانش امن ارتباط برقرار کنند. این امکان، به کاربران اجازه می‌دهد تا با سرعت واقعی در زمان واقعی با داده‌ها تعامل کنند و بدون تأخیر درخواست‌ها را پردازش کنند. همچنین، شبکه فایوجی قابلیت پشتیبانی از نرم‌افزارهای امن و نوآوری‌های متن باز را فراهم می‌کند که امکان توسعه و استفاده از برنامه‌های کاربردی مبتنی بر رایانش امن را ارائه می‌دهد [۲۰].

۷-۳-سکوی اینترنت اشیاء

سکوی اینترنت اشیاء یک مفهوم کلیدی در رایانش امن در اینترنت همه چیز است. یک سکوی اینترنت اشیاء عبارت است از یک زیرساخت نرم‌افزاری که امکان اتصال و مدیریت دستگاه‌های مختلف اینترنت اشیاء را فراهم می‌کند. این سکو قادر است اطلاعات حسگرها و دستگاه‌ها را جمع‌آوری، ذخیره، تجزیه و تحلیل کند و ارتباطات بین دستگاه‌ها را فراهم کند[۲۱]. این سکوها شامل لایه‌های الزامی و اختیاری است که برای عملکرد و امنیت سیستم‌های ضروری هستند. لایه‌های الزامی شامل موارد زیر است:

- لایه سنسورها و دستگاه‌ها: این لایه شامل سنسورها، دستگاه‌های اشتراکی و دستگاه‌های انتقال داده است که اطلاعات را از محیط فیزیکی به صورت دیجیتال جمع‌آوری می‌کنند و آن‌ها را برای پردازش و ارسال به لایه‌های بالاتر ارسال می‌کنند.
- لایه اتصال و شبکه: در این لایه، داده‌ها به صورت بی‌سیم یا با سیم بین دستگاه‌ها و شبکه‌ها منتقل می‌شوند. پروتکل‌های ارتباطی مانند Wi-Fi، بلوتوث و لوازم جانبی مرتبط با آن‌ها در این لایه قرار می‌گیرند.
- لایه اینترنت: در این لایه، اتصال به اینترنت و انتقال داده‌ها از طریق پروتکل‌های اینترنتی مانند TCP/IP صورت می‌گیرد. این لایه برای ارتباط با سرویس‌های ابری و سرویس‌های مرتبط با اینترنت مهم است.
- لایه سرویس‌های ابری: این لایه شامل سرویس‌های ابری است که برای پردازش داده‌ها، ذخیره‌سازی، تجزیه و تحلیل، ارائه خدمات و امنیت استفاده می‌شود. سرویس‌های ابری می‌توانند از طریق بسترهای متنوعی ارائه شوند، از جمله پلتفرم‌های ابری معروفی مانند Amazon Web Services (AWS)، Microsoft Azure و Google Cloud Platform.

در کنار لایه‌های الزامی، لایه‌های اختیاری نیز وجود دارند که بر اساس نیازها و پیشرفت‌های صنعت قابل استفاده هستند این لایه‌ها عبارتند از:

- لایه تشخیص مکان: این لایه به عنوان یک لایه اختیاری می‌تواند اطلاعات مکانی دستگاه‌ها را در اختیار قرار دهد. این اطلاعات می‌تواند برای تعیین موقعیت دقیق دستگاه‌ها و مکان‌یابی آن‌ها استفاده شود.
- لایه امنیت: این لایه شامل مجموعه اقدامات و فناوری‌ها برای حفاظت و امنیت داده‌ها و ارتباطات در سکوی اینترنت اشیاء است. امنیت در سطح فیزیکی، ارتباطات، شناسایی و احراز هویت، رمزنگاری و مدیریت دسترسی در این لایه مورد توجه قرار می‌گیرد.
- لایه تحلیل و پردازش داده‌ها: این لایه مسئول تحلیل و پردازش داده‌های جمع‌آوری شده توسط دستگاه‌ها است.

الگوریتم‌ها و روش‌های تحلیل داده برای استخراج اطلاعات مفید و الگوهای مهم از داده‌ها استفاده می‌شود.

- لایه واسط کاربری: این لایه شامل رابط‌ها و نرم‌افزارهای کاربردی است که به کاربران امکان می‌دهد با دستگاه‌های اینترنت اشیاء تعامل کنند و دسترسی به اطلاعات و کنترل برخی عملکردها را داشته باشند. جایگاه سکوی اینترنت اشیاء در شکل ۴ به نمایش در آمده است [۲۲].

شکل ۴- جایگاه سکوی اینترنت اشیاء [۲۲]

۴- کاربردها

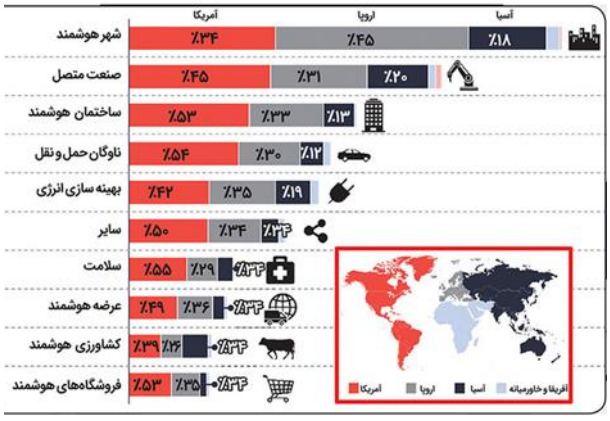
اینترنت اشیاء در حال گسترش و پیشرفت روزافزون است و به عنوان یک تکنولوژی کلیدی در بسیاری از صنایع و حوزه‌ها مورد استفاده قرار می‌گیرد. کاربردهای اینترنت همه چیز بسیار گسترده است و شامل اهم موارد زیر می‌شود:

- خانه هوشمند: اینترنت اشیاء به اتصال و کنترل دستگاه‌های خانگی از جمله روشنایی، سیستم‌های گرمایش و سرمایش، دستگاه‌های امنیتی، لوازم آشپزخانه و سایر وسایل خانه می‌پردازد. این اتصال به شبکه اینترنت به کاربران امکان کنترل هوشمند دستگاه‌های خانه خود را از راه دور فراهم می‌کند.
- شهر هوشمند: در شهر هوشمند، دستگاه‌ها و سنسورها در سراسر شهر در حال جمع‌آوری اطلاعات مربوط به ترافیک، نورپردازی، مدیریت پسماند، سیستم‌های امنیتی و سایر زیرساخت‌های شهری هستند. این اطلاعات به صورت هوشمند و تحلیل شده، کیفیت زندگی شهروندان را بهبود می‌بخشد و مدیران شهری را در اتخاذ تصمیمات بهتر و هوشمندانه یاری می‌کند و شامل پروژه‌های مرتبط با بهبود مدیریت شهری، ساماندهی ترافیک، پارکینگ هوشمند، مدیریت پسماندها، نورپردازی هوشمند و ارائه خدمات شهری بهبود یافته است.
- صنعت متصل هوشمند: در صنعت هوشمند، دستگاه‌ها و تجهیزات مختلف در یک سیستم متصل با یکدیگر هستند تا فرایندهای تولید، کنترل کیفیت، مانیتورینگ و نگهداری را بهبود بخشند. ماشین‌های هوشمند، سنسورها، ربات‌ها و دستگاه‌های دیگر در صنایع مختلف از جمله تولید خودرو، صنعت فولاد، کشاورزی و ساختمان‌های هوشمند استفاده می‌شوند. پروژه‌هایی که به هدف بهبود عملکرد و بهره‌وری در صنایع تولیدی و فرایندهای صنعتی متصل شده‌اند. این پروژه‌ها شامل مواردی مانند مانیتورینگ و کنترل هوشمند، تعمیر و نگهداری پیشگیرانه، بهبود زنجیره تأمین و بهینه‌سازی فرآیندهای تولیدی می‌باشد.
- ساختمان‌های هوشمند: پروژه‌هایی که هدفشان ارائه سیستم‌های مدیریت هوشمند برای ساختمان‌هاست. این پروژه‌ها شامل مواردی مانند مدیریت انرژی، کنترل هوشمند سیستم‌های راهبردی، ایمنی و امنیت، مانیتورینگ و کنترل هوشمند محیط ساختمان و خدمات هوشمند برای ساکنان می‌باشد.
- ناوگان حمل‌ونقل: پروژه‌هایی که به بهبود عملکرد و مدیریت ناوگان حمل‌ونقل را هدف قرار داده‌اند. این پروژه‌ها شامل مواردی مانند مدیریت ترافیک، پارکینگ هوشمند، راهبردی هوشمند، راهنمایی و رانندگی هوشمند، مانیتورینگ و ردیابی ناوگان و خدمات حمل‌ونقل هوشمند می‌باشد.
- بهینه‌سازی انرژی: پروژه‌هایی که به بهبود مدیریت و بهره‌برداری از منابع انرژی و بهینه‌سازی مصرف انرژی در سیستم‌ها و شبکه‌های مختلف می‌پردازند.
- سلامت هوشمند: اینترنت اشیاء در حوزه سلامت نقش مهمی را ایفا می‌کند. دستگاه‌های پزشکی هوشمند، سنسورهای پوشیدنی، سیستم‌های نظارت بهداشتی و سیستم‌های مدیریت بیمارستانی به ارتباط با یکدیگر و با پزشکان و بیماران متصل هستند. این اتصالات امکان مانیتورینگ سلامت، تشخیص بیماری‌ها، مدیریت بیماران و پیشگیری از بیماری‌ها را فراهم می‌کنند.
- زنجیره‌های تأمین هوشمند: پروژه‌هایی که هدفشان بهبود کارایی و شفافیت در زنجیره‌های تأمین می‌باشد. این پروژه‌ها شامل مواردی مانند ردیابی و اتصال

فرآیندها، بهبود مدیریت موجودی و کنترل هوشمند و حلقه بسته زنجیره تأمین می‌باشد.

- کشاورزی هوشمند: اینترنت اشیاء در کشاورزی نقش مهمی در بهبود کارایی و بهره‌وری محصولات دارد. سنسورها، دستگاه‌های خودکار، سیستم‌های آبیاری هوشمند و سیستم‌های کنترل محیطی در کشاورزی هوشمند استفاده می‌شوند تا نیازهای گیاهان، آبیاری، محیط رشد و کنترل آفات را بهینه کنند. پروژه‌هایی که هدفشان بهبود عملکرد و بهره‌وری در صنعت کشاورزی است. این پروژه‌ها شامل مواردی مانند مانیتورینگ محیطی، مدیریت آب و منابع، کشت و برداشت هوشمند.
- فروشگاه‌های هوشمند: بهبود تجربه خرید و خدمات هوشمند در فروشگاه‌ها.

اینها تنها برخی از کاربردهای اینترنت اشیاء هستند و بسیاری از صنایع و حوزه‌های دیگر نیز استفاده از این تکنولوژی را دارند. در هر صنعت و حوزه‌ای، می‌توان از اینترنت اشیاء برای بهبود فرآیندها، افزایش بهره‌وری، کاهش هزینه‌ها و ارائه خدمات بهتر استفاده کرد. با رشد روزافزون تعداد دستگاه‌های متصل به اینترنت و توسعه فناوری‌ها، کاربردهای اینترنت اشیاء به طور مداوم در حال افزایش است و آینده‌ای روشن و چشمگیر دارد. در شکل ۵ یک گزارش از ۱۰ مورد از محبوبترین پروژه‌های اینترنت اشیاء در سال ۲۰۱۸ را مشاهده می‌نمایید که توسط IoT Analytics ارائه شده است [۲۳].



شکل ۵. محبوبیت انواع کاربردها و سرویس‌های اینترنت اشیاء در جهان [۲۳]

این گزارش برگرفته از ۱۶۰۰پروژه مبتنی بر اینترنت اشیای انجام‌گرفته در سال ۲۰۱۸ در سرتاسر جهان است، بیشتر پروژه‌های اینترنت اشیاء که در این گزارش شناسایی شده است، در حوزه شهر هوشمند (۳۶۷ پروژه) و پس از آن صنعت متصل (۲۶۵ پروژه) و سپس پروژه‌های مرتبط با ساختمان‌های هوشمند (۱۹۳ پروژه) قرار دارند. دیگر حوزه‌ها عبارت‌اند از: ناوگان حمل‌ونقل، بهینه‌سازی انرژی، سایر، سلامت و تجهیزات پزشکی، زنجیره‌های تأمین هوشمند، کشاورزی هوشمند و درنهایت فروشگاه‌های هوشمند. بیشتر این پروژه‌ها در آمریکا (۴۵ درصد) و پس از آن اروپا (۳۵ درصد) و آسیا (۱۶ درصد) صورت گرفته است. پروژه‌های اجراشده در مناطق مختلف، تفاوت‌های معناداری با یکدیگر دارند. اکثر پروژه‌های شهر هوشمند در اروپا (۴۵ درصد) واقع شده‌اند، درحالی‌که آمریکا، به‌ویژه آمریکای شمالی، در بخش سلامت (۵۵ درصد) و بخش اتومبیل (۵۴ درصد) فعالیت بیشتری دارد. منطقه آسیا-اقیانوس آرام از نظر پروژه‌های کشاورزی هوشمند، ۳۱ درصد قوی‌تر از دیگر مناطق است. این گزارش نشان می‌دهد که اینترنت اشیاء در حوزه‌های مختلف از شهر هوشمند تا کشاورزی هوشمند و فروشگاه‌های هوشمند بسیاری از کاربردهای متنوع را در بر دارد. همچنین، نسبت پروژه‌ها بین مناطق جغرافیایی نیز نشان می‌دهد که کاربردهای متفاوت در مناطق مختلف جهان اجرا شده‌اند.

۵- چالش‌های امنیتی و حریم خصوصی، راهکارها و نقاط قوت، پیامدهای روانی، اقتصادی و اجتماعی

در حوزه رایانش امن در اینترنت همه چیز، چالش‌های امنیتی و حریم خصوصی یک نقطه کلیدی است که نیازمند توجه و بررسی دقیق است. با اتصال میلیون‌ها دستگاه و اشیا به شبکه و تبادل داده‌ها بین آنها، حفظ امنیت داده‌ها و حریم خصوصی افراد اهمیت بحرانی دارد. از رمزنگاری داده‌ها و مکانیزم‌های تشخیص تهدیدات تا مدیریت دسترسی و حفظ حریم خصوصی، تمامی این عوامل به طور جدی بررسی و مدیریت باید شوند . در این بخش از مقاله، به بررسی چالش‌های امنیت و حریم خصوصی در اینترنت همه چیز می‌پردازیم و راهکارهایی را برای بهبود این وضعیت معرفی می‌کنیم. با همراهی در ادامه مطالعه، این راهکارها و نقاط قوت در حوزه رایانش امن در اینترنت همه چیز را بیشتر خواهیم شناخت و به ارتقای امنیت و حریم خصوصی در این حوزه نزدیک خواهیم شد. در ادامه اهم چالشهای امنیتی در اینترنت همه چیز عنوان می‌شود:

۱. حفظ حریم خصوصی کاربران و محافظت از داده‌ها: یکی از چالش‌های اساسی در اینترنت همه چیز، حفظ حریم خصوصی کاربران و محافظت از داده‌ها است. با ارتباط بین میلیون‌ها دستگاه و انتقال داده‌ها، اینترنت همه چیز به مقوله امنیت و حفظ حریم خصوصی تبدیل شده است. از طریق رمزنگاری داده‌ها، استفاده از پروتکل‌های امن، مدیریت دسترسی و نظارت بر داده‌ها، می‌توان در این زمینه چالش‌ها را مدیریت کرد [۲۴].

۲. احراز هویت و مدیریت دسترسی: در اینترنت همه چیز، احراز هویت صحیح و مدیریت دسترسی متصل شدن دستگاه‌ها و کاربران بسیار اهمیت دارد. باید روش‌های قوی احراز هویت، مکانیزم‌های دسترسی مبتنی بر نقش و سیاست‌های مدیریت دسترسی را پیاده‌سازی کرد تا فقط افراد مجاز به داده‌ها دسترسی داشته باشند [۲۵].

۳. حفظ حریم خصوصی و اعتماد: با ارتباط بین دستگاه‌ها و جمع‌آوری اطلاعات شخصی، حفظ حریم خصوصی از اهمیت فراوان برخوردار است. باید سیاست‌ها و مکانیزم‌های حفظ حریم خصوصی مناسبی در نظر گرفته شود تا اطلاعات شخصی محافظت شده و اعتماد کاربران حفظ شود [۲۶].

۴. مدیریت اعتماد و ادغام سیاست‌ها: در اینترنت همه چیز، اعتماد نقش کلیدی در برقراری ارتباطات امن بین دستگاه‌ها ایفا می‌کند. راهکارهایی برای جلب اعتماد کاربران و اطمینان از امنیت ارائه وجود دارد که شامل استانداردها، تکنولوژی‌های امنیتی و سیاست‌های مناسب است [۲۷].

۵. مدیریت مجوزها و کنترل دسترسی‌ها: مدیریت مجوزها و کنترل دسترسی به داده‌ها و منابع نقش بسیار مهمی در اینترنت همه چیز دارد. اینترنت همه چیز بسیار پویا و پیچیده است و دسترسی به داده‌ها و منابع باید با مجوزهای مشخص و کنترل دقیق صورت گیرد. برای این منظور، نیاز است تا سیستم‌های مدیریت مجوزها و کنترل دسترسی ایجاد شود تا فقط کاربران و دستگاه‌های مجاز به منابع دسترسی داشته باشند. این شامل استفاده از سیاست‌های دسترسی مبتنی بر نقش، سیاست‌های دسترسی محدود به اطلاعات حساس، تشخیص و پیشگیری از دسترسی‌های غیرمجاز و مکانیزم‌های ارائه مجوزها است [۲۸].

۶. امنیت انتها به انتها: امنیت در نقاط انتهایی ارتباط بین دستگاه‌ها و میزبانهای اینترنتی بسیار حائز اهمیت است. باید از روش‌های رمزنگاری قوی، مکانیزم‌های تشخیص و پیشگیری از حملات، مانیتورینگ و نظارت بر رفتار دستگاه‌ها و مکانیزم‌های امنیتی مطمئن استفاده شود تا ارتباطات میان دستگاه‌ها به صورت امن انجام شود [۲۹].

۷. راهکارهای امنیتی مقاوم در برابر حملات: با توجه به ارتباط و اتصال دستگاه‌ها در اینترنت همه چیز، حملات امنیتی نیز افزایش یافته‌اند. لذا، راهکارهای امنیتی قوی و مقاوم در برابر حملات، از جمله استفاده از سیستم‌های تشخیص نفوذ، آنالیز هوشمند داده‌ها، استفاده از الگوریتم‌های یادگیری ماشین و راهکارهای مبتنی بر امنیت، ضروری است [۳۰].

با مدیریت این چالش‌ها و ارائه راهکارهای امنیتی مؤثر، می‌توان به ارتقای امنیت و حریم خصوصی در رایانش امن در اینترنت همه چیز کمک کرد و از پتانسیل‌های این فناوری به صورت کامل بهره‌برداری کرد. در ادامه بر اساس مطالعات انجام گرفته به برخی از این راهکارها و نقاط قوت مورد توجه در این حوزه اشاره می‌کنیم:

۱.رمزنگاری قوی: استفاده از رمزنگاری قوی در اینترنت همه چیز برای حفظ امنیت داده‌ها بسیار اهمیت دارد. رمزنگاری مبتنی بر الگوریتم‌های پیچیده و قوی می‌تواند از دسترسی غیرمجاز به داده‌ها جلوگیری کند و امنیت اطلاعات را تضمین کند.

۲.مکانیزم‌های تشخیص تهدیدات: استفاده از مکانیزم‌های تشخیص تهدیدات و نفوذ می‌تواند به مراتب امنیت سیستم را افزایش دهد. این مکانیزم‌ها مبتنی بر الگوریتم‌های هوش مصنوعی و تحلیل داده‌های بزرگ می‌توانند به شناسایی و پیشگیری از تهدیدات امنیتی کمک کنند.

۳.مدیریت دسترسی و احراز هویت: سیستم‌های مدیریت دسترسی و احراز هویت قوی و یکپارچه می‌توانند به امنیت و حفظ حریم خصوصی کاربران کمک کنند. با تعیین سطوح دسترسی، احراز هویت صحیح و مدیریت دقیق دسترسی به منابع، دسترسی غیرمجاز به داده‌ها و اشیا جلوگیری می‌شود.

۴.آموزش و آگاهی کاربران: آموزش و آگاهی کاربران در مورد مسائل امنیتی و حریم خصوصی در اینترنت همه

چیز بسیار اهمیت دارد. کاربران باید آگاهی کافی در مورد راهکارها و مراقبت‌های امنیتی داشته باشند تا بتوانند خود را در برابر تهدیدات امنیتی محافظت کنند.

۵.استفاده از تکنولوژی‌های جدید: استفاده از تکنولوژی‌های جدید مانند هوش مصنوعی، اینترنت اشیاء و بلاکچین می‌تواند در بهبود امنیت و حفظ حریم خصوصی در اینترنت همه چیز تأثیرگذار باشد. این تکنولوژی‌ها قابلیت‌های بسیاری را در جلب اعتماد و افزایش امنیت به همراه دارند.

نقاط قوت و راهکارهای فوق تنها بخشی از مجموعه‌ای از راهکارها و نقاط قوت در حوزه رایانش امن در اینترنت همه چیز هستند. با توجه به پیشرفت فناوری و تحولات مرتبط با اینترنت اشیاء، همواره نیاز به تحقیق و توسعه بیشتر در زمینه امنیت و حریم خصوصی وجود دارد. همکاری بین صنعت، دولت، و تحقیقات علمی برای شناسایی چالش‌های جدید، ارائه راهکارهای نوین، و ایجاد استانداردهای امنیتی مناسب می‌تواند بهبود قابل توجهی در این حوزه به همراه داشته باشد.

رایانش امن در اینترنت همه چیز، علاوه بر چالش‌های امنیتی، پیامدهای روانی، اقتصادی و اجتماعی متعددی نیز دارد. در ادامه به مرور برخی از این پیامدها خواهم پرداخت:

۱.پیامدهای روانی: اینترنت همه چیز و افزایش تعامل بین دستگاه‌ها و سنسورها می‌تواند به تغییر روانشناختی کاربران و افراد مرتبط با آن منجر شود. نگرانی‌های مربوط به حریم خصوصی و امنیت می‌توانند باعث ایجاد استرس و نگرانی در بین کاربران شوند. افزایش داده‌های شخصی که جمع‌آوری می‌شوند و احتمال نفوذ و دسترسی غیرمجاز به این اطلاعات می‌تواند از جمله دلایل این نگرانی‌ها باشد [۳۱]. از طرفی، اعتماد کاربران به اینترنت همه چیز وابسته به امنیت و حفاظت از اطلاعات شخصی آنان است. بنابراین، تضمین حریم خصوصی و امنیت اطلاعات می‌تواند نقش مهمی در کسب اعتماد کاربران به رایانش امن در اینترنت همه چیز ایفا کند.

۲.پیامدهای اقتصادی: با پیاده‌سازی رایانش امن در اینترنت همه چیز، امکان بهبود فرایندها، کاهش هزینه‌ها و افزایش بهره‌وری در بخش‌های مختلف وجود دارد. با اتصال دستگاه‌ها و داده‌ها به یکدیگر، امکان اشتراک گذاری داده‌ها و هماهنگی بین آنها برای بهبود فرایندها و افزایش کارایی فراهم می‌شود. به عنوان مثال، در حوزه صنعت، استفاده از سنسورها و دستگاه‌های هوشمند می‌تواند به کاهش هزینه‌های نگهداری و تعمیرات و بهبود زمانبندی تعمیرات منجر شود. همچنین، تجارت الکترونیک، بازاریابی هدفمندتر و خدمات مالی آنلاین نیز برای توسعه اقتصادی موثر هستند [۳۲]. با این حال، پیاده‌سازی و مدیریت امنیت در اینترنت همه چیز نیز هزینه‌هایی را به همراه دارد که ممکن است بر عملکرد کسب و کار و سرمایه‌گذاری‌ها تأثیرگذار باشد.

۳. پیامدهای اجتماعی: رایانش امن در اینترنت همه چیز می‌تواند تأثیرات مهمی بر جوامع و ارتباطات آنها داشته باشد. با ارتباط و همکاری بین دستگاه‌ها و سازمان‌ها، می‌توان به بهبود ارتباطات و تعاملات اجتماعی پیشرفت کرد [۳۳]. به عنوان مثال، در حوزه شهر هوشمند، ارتباط بین دستگاه‌ها و سازمان‌های شهری می‌تواند بهبودی در مدیریت ترافیک، پارکینگ هوشمند و مصرف انرژی منجر شود. همچنین، در حوزه بهداشت و سلامت، اینترنت اشیاء می‌تواند بهبودی در ارائه خدمات بهداشتی و پزشکی، پیشگیری از بیماری‌ها و پایش بهداشتی داشته باشد. با این حال، باید توجه داشت که این تغییرات نیز نیازمند تأمین امنیت و حریم خصوصی افراد است تا از سوءاستفاده و خطرات احتمالی جلوگیری شود.

از اینرو با توجه به موضوعات برشمرده شده برای موفقیت رایانش امن در اینترنت همه چیز لازم است تا پیامدهای روانی، اقتصادی و اجتماعی مرتبط با آن نیز به درستی مدیریت شوند.

۶- نیازها و الزامات امنیتی اینترنت همه چیز

در حوزه رایانش امن در اینترنت همه چیز، الزامات امنیتی یک نقش حیاتی در حفظ امنیت و حریم خصوصی اطلاعات و دستگاه‌ها دارند. با رشد روزافزون اینترنت اشیاء و اتصال همه‌چیز به هم، این الزامات بیش از پیش اهمیت یافته‌اند. اما برای ایجاد یک سیستم رایانش امن در اینترنت همه چیز، ضروری است که نیازهای کلیدی و الزامات مرتبط با امنیت مورد توجه قرار گیرند. در این بخش از مقاله، به تفکیک نیازها و الزامات امنیتی در اینترنت همه چیز پرداخته می‌شود. نیازها شامل حفاظت از حریم خصوصی، تشخیص و پیشگیری از تهدیدات، احراز هویت و مدیریت دسترسی است. از سوی دیگر، الزامات شامل رمزنگاری، مانیتورینگ و تشخیص تهدیدات

و حفظ امنیت فیزیکی است. با رعایت این الزامات و نیازها، می‌توان به ایجاد یک بستر امن و قابل اعتماد برای اینترنت همه چیز پیشرفت کرده و از پتانسیل‌های این فناوری بهره‌برداری کامل و امنیتی مطلوب داشت.

۱. نیازها:

- حفاظت از حریم خصوصی: اینترنت همه چیز حاوی اطلاعات حساسی است که باید محافظت شوند. نیازمندیم که امنیتی فراهم شود که از دسترسی غیرمجاز به اطلاعات حساس جلوگیری کند.

- تشخیص و پیشگیری از تهدیدات: با افزایش تعداد دستگاه‌ها و اشیا متصل به اینترنت، تهدیدات امنیتی نیز افزایش می‌یابند. بنابراین، نیازمندیم به راهکارهایی که قادر به تشخیص و پیشگیری از تهدیدات امنیتی باشند.

- مدیریت دسترسی: برای حفظ امنیت در اینترنت همه چیز، نیازمندیم تا دسترسی به دستگاه‌ها و اطلاعات محدود و کنترل شده شود. مدیریت دسترسی کاربران و اشیا باید به صورت دقیق و امن انجام شود.

- احراز هویت: احراز هویت افراد و دستگاه‌ها می‌تواند به عنوان یکی از نیازهای امنیتی مهم در اینترنت همه چیز مطرح شود. تعیین هویت صحیح و قابل اعتماد باعث می‌شود تا تهدیدات امنیتی کاهش یابند و دسترسی غیرمجاز به داده‌ها جلوگیری شود.

۲.الزامات امنیتی:

- رمزنگاری: یکی از الزامات امنیتی مهم در اینترنت همه چیز است. داده‌ها باید به صورت رمزنگاری شده انتقال یابند تا از دسترسی غیرمجاز جلوگیری شود.

- مانیتورینگ و تشخیص تهدیدات: نیازمندیم تا مکانیزم‌هایی در نظر بگیریم که قادر به مانیتورینگ و تشخیص تهدیدات امنیتی در شبکه و دستگاه‌ها باشند. این مکانیزم‌ها باید بتوانند به صورت زمان‌بندی شده، بهبود پیشگیری و پاسخگویی به تهدیدات را فراهم کنند.

- حفظ امنیت فیزیکی: علاوه بر امنیت داده‌ها و شبکه،

- حفظ امنیت فیزیکی دستگاه‌ها و سخت‌افزار ضروری می‌باشد.

۷- بحث و نتیجه گیری

در این مقاله، به بررسی مفهوم و اهمیت رایانش امن در اینترنت همه چیز پرداختیم. با رشد چشمگیر اینترنت همه چیز و ارتباط بین اشیاء، داده‌ها، افراد و فرایندها، امنیت اطلاعات به یک چالش بزرگ تبدیل شده است. از اطلاعات حساس کاربران گرفته تا دسترسی غیرمجاز و تهدیدات امنیتی متعدد، اینترنت همه چیز نیازمند راهکارهای امنیتی قوی است. سپس به بررسی چالش‌های امنیتی و حریم خصوصی در اینترنت همه چیز پرداخته شد. حفظ امنیت داده‌ها، احراز هویت و مدیریت دسترسی، حفظ حریم خصوصی و تشخیص تهدیدات امنیتی، بخش‌های کلیدی در رایانش امن در اینترنت همه چیز هستند. ما درک کردیم که با پیچیدگی و حجم زیاد دستگاه‌ها و داده‌ها، راهکارهای قوی و مکانیزم‌های مدیریتی مورد نیاز هستند. علاوه بر این، در این مقاله به بررسی نیازها و الزامات امنیتی اینترنت همه چیز پرداختیم. از احراز هویت و مدیریت دسترسی تا رمزنگاری اطلاعات و مدیریت اعتماد، این الزامات برای ایجاد یک محیط امن و مطمئن در اینترنت همه چیز بسیار حیاتی هستند. در نهایت، راهبردها و راهکارهایی برای بهبود رایانش امن در اینترنت همه چیز ارائه شد. استفاده از رمزنگاری قوی، مدیریت دسترسی متمرکز، آموزش و آگاهی کاربران، استفاده از سیستم‌های تشخیص تهدیدات و مانیتورینگ پیشرفته، راهکارهایی هستند که می‌توانند بهبود قابل توجهی در امنیت و حریم خصوصی در رایانش امن در اینترنت همه چیز ایجاد کنند. با توجه به این مقاله، امیدواریم که خوانندگان توانایی تشخیص و پیاده‌سازی راهکارهای امنیتی مناسب را در رایانش امن در اینترنت همه چیز به دست آورند. با رعایت این راهکارها و گذر از موانع پیاده‌سازی، امکان بهره‌برداری کامل از پتانسیل‌های این فناوری را در زمینه امنیت و حریم خصوصی به وجود خواهیم آورد.

منابع

1.j. Macaulay, L. Buckalew, G. Chung, “Internet of Everything in Logistics”, a collaborative report by DHL and Cisco on implications and use cases for the logistics industry, 2015.

2.M. Sergey, S. Nikolay, E.sergery, “Cyber Security Concept for Internet of Everything (IoE)”, IEEE Systems of Signal Synchronization, Generating and Processing in Telecommunications, Kazan, Russia, 2017.

3.OpenLearn, “What is the IoE?”, Free learning from The Open University, https://www.open.edu/openlearn/mod/oucontent/view.php?id=48444&printable=1, 2023.

4.A. Majeed, R. Bhana, A. Ui, M.L. Williams, “Devising a Secure Architecture of Internet of Everything (IoE) to Avoid the Data Exploitation in Cross Culture Communications”, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, pp. 328- 332, 2016.

5.CompTIA, “Sizing Up the Internet of Things”, Research Report,https://connect.comptia.org/content/research/sizing-up-the-internet-of-things, 2015.

6.J. Bradley, J. Barbier, D. Handler, “Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion”, Cisco White Paper, 2013.

7.j. Bradley, L. Buckalew, J. Loucks, J. Macaulay, “Internet of Everything in the Public Sector: Generating Value in an Era of Change Top 10 Insights”, Cisco report, 2014.

8.R. Buyya, A.V. Dastjerdi, “Internet of Things Principles and Paradigms”, Morgan Kaufmann is an imprint of Elsevier, ISBN: 9780128053959, 2016.

9.D.J. Langleya, J.V. Doorn, I.C.L. Ng, S. Stieglitz, A. Lazovik, A. Boonstra, “The Internet of Everything: Smart Things and Their Impact on Business Models”, ElSEVIER, Journal of Business Research, Vol. 122, pp. 853-863, 2021.

10.A.A. Hamza, I.T. Abdel-Halim, M.A.Sobh, A.M. Bahaa-Eldin, “A Survey and Taxonomy of Program Analysis for IoT Platforms”, ELSEVIER, Ain Shams Engineering Journal, Vol. 12, No. 4, 2021.

11.Gartner, “Internet of Things (IoT) - Key Business Insights”, https://www.gartner.com/en/information-technology/insights/internet-of-things, 2022.

12.S. Agarwal, S. Markkar, D-T. Tran, “Privacy Vulnerabilities and Data Security Challenges in the IoT”, 1st Edition by CRC Press, 234 pages, 47 B/W Illustrations, 2021.

13.S.O. Azarkasb, S.H. Khasteh, “Advancing Intrusion Detection in Fog Computing: Unveiling the Power of Support Vector Machines for Robust Protection of Fog Nodes against XSS and SQL Injection Attacks”, Journal of Engineering Research and Reports, Vol. 25, No. 3, pp. 59-84, 2023.

14.H. Rajashree R, Sundarakantham K, Sivasankar E, M. Shalinie S, “A Hybrid Deep Learning Framework for Privacy Preservation in Edge Computing”, ELSEVIER, Computer & Security, Vol. 129, 2023.

15.S.O. Azarkasb, M. Amiri, S.H. Khasteh, “Unsupervised Fuzzy-Multi-Core Aspect Sentiment Analysis for Big Data of Online News Users' Persian Opinions”, Asian Journal of Research in Computer Science, Vol. 16, No. 3, pp. 50-64, 2023.

16.C.L. Stergiou, E. Bompoli, K.E. Psannis, “Security and Privacy Issues in IoT-Based Big Data Cloud Systems in a Digital Twin Scenario”, Applied Sciences, MDPI, Vol. 13, No.2, 2023.

17.L. Lantz, D. Cawrey, “Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications”, O'Reilly Media, Book, ISBN: 9781492054702, 281 Pages, 2022.

18.E. Osmanoglu, “Identity and Access Management: Business Performance through Connected Intelligence”,

Zualkernan, “Internet of things (IoT) security: Current Status, Challenges and Prospective Measures”, IEEE 10th International Conference for Internet Technology and Secured Transactions, London, UK, 2015.
28. A. Khan, K. Salah, “IoT Security: Review, Blockchain Solutions, and Open Challenges”, ELSEVIER, Future Generation Computer Systems, Vol. 82, pp. 395411, 2017.
29. I. Yaqoob, E. Ahmed, M.H.U. Rehman, A.I.A. Ahmed, “The Rise of Ransomware and Emerging Security Challenges in the Internet of Things”, ELSEVIER, Computer Networks, Vol. 129, pp. 444-458, 2017.
30. Moganedi, S, J. Mtsweni, “Beyond the Convenience of the Internet of Things: Security and Privacy Concerns”, IEEE IST-Africa Week Conference, Windhoek, Namibia, 2017.
31. A. Oulasvirta, T. Rattenbury, L. Ma, E. Raita, “Habits Make Smartphone Use More Pervasive”, Personal and Ubiquitous Computing, Vol. 16, pp. 105-114, 2012.
32. World Economic Forum, “The Global Risks Report 2023”, 18th Edition, INSIGHTREPOR, 98 Pages, https://www.weforum.org/reports/global-risks-report-2023/, 2023.
33. S. Zuboff, “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”, New York, Public Affairs, ISBN: 9781610395694, 704 Pages, 2019.

Syngress, Book, ISBN: 9780124104334, 648 Pages, 2013.
19. M. Bazzell, “Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information”, CCI Publishing, Book, ISBN: 9781494275358, 402 Pages, 2014.
20. A.Gohar, G. Nencioni, “The Role of 5G Technologies in a Smart City: The Case for Intelligent Transportation System”, Sustainability, MDPI, 24 Pages, 2021.
21. M. Kranz, “Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry”, WILEY, Book, ISBN: 9781119285663, 272 Pages, 2016.
22. Pandey, A., “IoT Platforms”, Published in BlogsCord, 2020.
23. M.H. Miraz, M. Ali, P.S. Excell, R. Picking, “Internet of Nano-Things, Things and Everything: Future Growth Trends”, Future Internet, Vol.10, No.8, 2018.
24. Farooq, M.U, M. Wassem, A. Khairi, P.S. Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (IoT)”, International Journal of Computer Applications, Vol. 111, No.7, pp.1-6, 2015.
25. R. Roman, P. Najera, J. Lopez, “Securing the Internet of Things”, IEEE Computer, Vol. 44, No. 9. pp. 51-58, 2011.
26. S.O. Azarkasb, S. Sedighian kasha, S.O. Khasteh, “A Network Intrusion Detection Approach at the Edge of Fog”, IEEE 26th International Computer Conference, Computer Society of Iran, 2021.
27. R. Mahmoud, T. Yousuf, F. Aloul, I.