

چهارمین کنفرانس بین المللی
مهندسی و فناوری اطلاعات

ارتقای امنیت و حریم خصوصی اینترنت اشیا: نقش انقلابی فناوری های بلاک چین

سید جواد میرعابدینی

هیئت علمی کامپیوتر، هیئت علمی دانشگاه آزاد اسلامی، واحد تهران مرکزی
j_mirabedini@iauctb.ac.ir

علیرضا رحیمی پور انارکی

دانشجوی کارشناسی ارشد مهندسی نرم افزار، واحد تهران مرکز، دانشگاه آزاد اسلامی
arrahimipourdev@gmail.com

فاطمه سادات صدر طباطبایی

دانشجوی کارشناسی ارشد مهندسی نرم افزار، واحد تهران مرکز، دانشگاه آزاد اسلامی
fatemesadrtatabayai@gmail.com

الهام پیلور

دانشجوی کارشناسی ارشد مهندسی نرم افزار، واحد تهران مرکز، دانشگاه آزاد اسلامی
elipilevar@gmail.com

چکیده

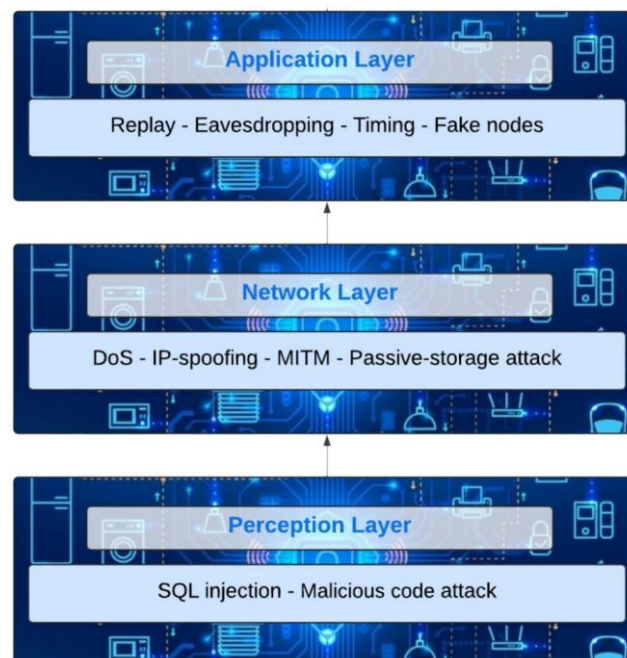
اینترنت اشیا (Internet of Things) به شبکه‌ای از دستگاه‌های هوشمند اشاره دارد که به صورت گسترده به تبادل داده می‌پردازند. رشد سریع این فناوری، در کنار مزایای فراوان، چالش‌های مهمی در زمینه امنیت و حریم خصوصی ایجاد کرده است. روش‌های سنتی امنیت سایبری به دلیل ساختار متمرکز و ضعف در برابر تهدیدات نوظهور، برای حفاظت از اکوسیستم IoT ناکافی هستند. در این میان، فناوری بلاک چین با ویژگی‌هایی مانند عدم تمرکز، شفافیت، تغییرناپذیری و استفاده از اجماع توزیع شده، به عنوان راهکاری نوین برای ارتقای امنیت و اعتماد در IoT مطرح شده است. این مقاله با روش تحقیق کتابخانه‌ای و تحلیلی، به بررسی نقش بلاک چین در بهبود امنیت و حریم خصوصی در معماری چندلایه IoT می‌پردازد. پس از مرور چالش‌های امنیتی، قابلیت‌های بلاک چین در پاسخ به این چالش‌ها تبیین می‌شود. همچنین یک چارچوب مفهومی برای ادغام این دو فناوری ارائه و یافته‌های پژوهش‌های اخیر در این حوزه تحلیل می‌گردد. نتایج نشان می‌دهد بلاک چین می‌تواند دستکاری داده‌ها را دشوار، مدیریت هویت را تقویت و دسترسی غیرمجاز را محدود کند. در پایان، پیشنهادهایی برای آینده شامل استفاده از الگوریتم‌های اجماع سبک و بهبود مقیاس پذیری ارائه می‌شود.

واژگان کلیدی: اینترنت اشیا - بلاک چین - امنیت سایبری - حریم خصوصی - قرارداد هوشمند - معماری غیرمتمرکز - کنترل دسترسی - احراز هویت - اجماع توزیع شده - تمامیت داده

مقدمه

با گسترش روزافزون اینترنت اشیا (IoT)، میلیاردها دستگاه هوشمند - از حسگرها و ابزار پوشیدنی گرفته تا لوازم خانگی و سیستم‌های صنعتی - به اینترنت متصل شده و به تبادل داده مشغول‌اند. بر اساس گزارش‌ها، شمار دستگاه‌های IoT متصل به شبکه تا سال ۲۰۲۵ به ده‌ها میلیارد خواهد رسید که نشان‌دهنده نفوذ عمیق این فناوری در زندگی روزمره و صنایع مختلف است. این اتصال گسترده و تعامل خودکار بین دستگاه‌ها مزایایی چون بهینه‌سازی فرآیندها، پایش بلادرنگ و ارائه خدمات هوشمند را به همراه دارد. با این حال، ابعاد وسیع و ماهیت توزیع‌شده IoT آن را به هدفی جذاب برای مهاجمان سایبری تبدیل کرده است. در سال‌های اخیر، حملات متعددی علیه دستگاه‌ها و شبکه‌های IoT گزارش شده که از نفوذ به حریم خصوصی کاربران تا مختل کردن زیرساخت‌های حیاتی را شامل می‌شود.

شکل ۱ معماری لایه‌ای IoT و نمونه‌ای از حملات رایج در هر لایه را نشان می‌دهد. همان‌طور که مشاهده می‌شود، در لایه ادراک (دستگاه‌ها) حملاتی نظیر تزریق کد مخرب و نفوذ به حسگرها محتمل است؛ در لایه شبکه حملاتی چون حملات منع خدمت (DoS)، جاسوسی و مرد میانی (MITM) رخ می‌دهد و در لایه کاربرد نیز حملاتی از قبیل جعل هویت، استراق سمع و حملات بازپخش مشاهده می‌شود. این تهدیدات متنوع، طراحی یک مدل امنیتی جامع برای IoT را دشوار ساخته و اعتماد به سامانه‌های مبتنی بر IoT را کاهش داده است.



(ادراک، IoT، شکل ۱ - لایه‌های معماری اینترنت اشیا و تهدیدات امنیتی مربوط به هر لایه: این تصویر ساختار سه‌لایه‌ای رایج در معماری شبکه، کاربرد) را نشان می‌دهد و نمونه‌ای از حملات شایع در هر لایه مانند حملات فیزیکی، حملات مرد میانی، و نفوذ به حریم خصوصی را نمایش می‌دهد.

با وجود به کارگیری روش های مرسوم امنیت شبکه (مانند دیوارهای آتش، پروتکل های رمزنگاری TLS و مراکز صدور گواهی دیجیتال) در سامانه های IoT، موارد متعددی از نقص امنیتی مشاهده شده است. برای مثال، استفاده از نسخه های قدیمی TLS یا تکیه بر مراکز گواهی معتبری که بعدها به خطر افتاده اند، اتصالات IoT را در برابر حملاتی نظیر حمله مرد میانی یا نشن داده آسیب پذیر کرده است. علت اصلی ناکافی بودن رویکردهای سنتی را می توان در ماهیت متمرکز بسیاری از زیرساخت های IoT جستجو کرد. تمرکزگرایی به این معناست که اغلب داده های حسگرها و دستگاه ها به یک سرور یا سامانه مرکزی ارسال و در آن جا پردازش و ذخیره می شوند. چنین نقطه تمرکزی می تواند هدف حمله قرار گیرد یا در صورت نفوذ، منجر به افشای گسترده اطلاعات شود. همچنین اعتماد بیش از حد به نهادهای مرکزی برای تأیید هویت و کنترل دسترسی، خود یک نقطه ضعف محسوب می شود؛ چرا که اگر نهاد مرکزی مختل یا فاسد شود، کل سیستم در معرض خطر قرار می گیرد. در این میان، فناوری بلاک چین با ویژگی های بی نظیر خود به عنوان راهکاری غیرمتمرکز برای رفع این معضلات پدیدار شده است. بلاک چین یک دفتر کل توزیع شده و تغییرناپذیر است که تراکنش ها و داده ها را در زنجیره ای از بلوک های به هم پیوسته ذخیره می کند. هر بلوک شامل مجموعه ای از تراکنش ها، یک برچسب زمانی (Timestamp) و هش رمزنگاری شده ای از بلوک قبلی است و بدین ترتیب دستکاری یا حذف اطلاعات ثبت شده عملاً غیرممکن می شود. در بلاک چین به دلیل توزیع کپی دفترکل بین گره های متعدد، هیچ نهاد واحدی کنترل انحصاری بر داده ها ندارد و تلاش برای تقلب یا حمله به شبکه بسیار دشوار است. این مشخصات دقیقاً همان چیزی است که اکوسیستم IoT به آن نیاز دارد: زیرساختی غیرمتمرکز برای ذخیره و تبادل امن داده ها که بتواند در برابر نفوذ، دستکاری و خرابی یک نقطه مقاومت کند. به بیان دیگر، بلاک چین می تواند با حذف نقاط تمرکز، اعتماد توزیع شده ای بین اجزای IoT ایجاد کند که طی آن دستگاه ها بدون نیاز به واسطه مرکزی، به یکدیگر اعتماد کنند و تعامل داشته باشند.

افزون بر عدم تمرکز، بلاک چین قابلیت های ارزشمند دیگری نیز دارد. شفافیت و قابلیت ممیزی یکی از آنهاست؛ تمامی تراکنش های ثبت شده در زنجیره بلوکی برای اعضای مجاز شبکه قابل مشاهده و بررسی است که این امر احتمال تقلب یا فعالیت های مخرب پنهانی را کاهش می دهد. همچنین مکانیزم های اجماع در بلاک چین (مانند اثبات کار و اثبات سهام) تضمین می کنند که تنها تراکنش های معتبر و مورد توافق اکثریت گره ها به دفترکل اضافه شوند. بدین ترتیب تمامیت داده ها حفظ شده و داده های نادرست یا دستکاری شده جایی در سیستم نخواهند داشت. ویژگی دیگر، امکان استفاده از قراردادهای هوشمند (Smart Contracts) است که به صورت خودکار اجرا شده و می توانند برای اعمال سیاست های امنیتی (نظیر کنترل دسترسی یا احراز هویت) در شبکه IoT به کار گرفته شوند. تمامی این قابلیت ها نشان می دهد که بلاک چین می تواند پاسخی جامع به چالش های امنیتی و حریم خصوصی IoT باشد.

بر این اساس، فرضیه اساسی این پژوهش آن است که ادغام فناوری بلاک چین با زیرساخت های IoT می تواند به طور چشمگیری امنیت و حریم خصوصی را ارتقا دهد و اعتماد از دست رفته را به این حوزه بازگرداند. برای بررسی این فرضیه، ساختار مقاله حاضر به شرح زیر است: ابتدا در بخش بعدی پیشینه پژوهش و مطالعات مرتبط مرور می شود تا تصویری از وضعیت کنونی امنیت IoT و تلاش های انجام شده برای بهبود آن با بلاک چین به دست آید. سپس در بخش چارچوب مفهومی، یک مدل مفهومی پیشنهادی برای ترکیب این دو فناوری ارائه می گردد. در بخش روش تحقیق، رویکرد و مراحل انجام پژوهش تشریح می شود. مهم ترین بخش مقاله، تحلیل یافته ها است که تأثیرات بلاک چین بر جنبه های مختلف امنیت و حریم خصوصی IoT را با استناد به شواهد پژوهشی ارزیابی می کند. در نهایت، نتیجه گیری و پیشنهادات آتی ارائه خواهد شد. امید است این پژوهش بتواند گامی موثر در تبیین نقش انقلابی بلاک چین در حوزه امنیت IoT برداشته و مسیر تحقیقات و پیاده سازی های آتی را روشن نماید.

مرور ادبیات پژوهش (پیشینه پژوهش)

چالش‌های امنیتی و حریم خصوصی در اینترنت اشیا معماری IoT معمولاً به صورت چندلایه شامل لایه ادراک (دستگاه‌ها و حسگرها)، لایه شبکه (درگاه‌ها، ارتباطات و اینترنت) و لایه کاربرد (نرم‌افزارها و سرویس‌ها) توصیف می‌شود. هر یک از این لایه‌ها با تهدیدات امنیتی خاصی مواجه هستند که می‌تواند عملکرد کل سامانه را به خطر بیندازد. در لایه ادراک، دستگاه‌های IoT به دلیل منابع محدود محاسباتی و انرژی، اغلب از پروتکل‌ها و مکانیزم‌های امنیتی ساده‌ای استفاده می‌کنند یا حتی فاقد هرگونه رمزنگاری هستند. این مسئله آن‌ها را در برابر دست‌کاری فیزیکی، نصب بدافزار یا نفوذ مستقیم آسیب‌پذیر می‌کند. برای مثال، یک مهاجم می‌تواند با دسترسی فیزیکی به حسگر، داده‌های آن را تغییر داده یا از کار بیندازد. یا در حملات تزریق کد مخرب، کدهای غیرمجاز را در سفت‌افزار (firmware) دستگاه کاشته و کنترل آن را به دست گیرد. در لایه شبکه، ارتباطات بی‌سیم میان دستگاه‌ها و سرورها ممکن است هدف استراق سمع (Eavesdropping) یا رهگیری توسط مهاجم میانی قرار گیرد؛ در این حالت مهاجم می‌تواند داده‌های حساس (مانند اطلاعات حسگر پزشکی یا داده‌های خانه هوشمند) را شنود کرده یا تغییر دهد. حملات جعل هویت و IP-spoofing نیز رایج‌اند که مهاجم در آن با جعل آدرس یا هویت یک گره معتبر، دسترسی غیرمجاز به شبکه پیدا می‌کند. علاوه بر این، حملات منع سرویس (DoS/DDoS) با هدف از کارانداختن شبکه IoT نیز تهدید جدی به شمار می‌روند؛ در این حملات مهاجم با ارسال سیل‌آسای درخواست‌ها یا داده‌های زائد به یک گره یا سرور مرکزی، منابع آن را اشباع کرده و کارکرد عادی را مختل می‌کند. در لایه کاربرد که داده‌های IoT در اپلیکیشن‌ها و سرویس‌ها پردازش می‌شوند، چالش حریم خصوصی داده‌ها پررنگ می‌شود. برای مثال، نشت داده‌های جمع‌آوری‌شده توسط دستگاه‌های IoT (مانند موقعیت مکانی یا اطلاعات سلامتی) می‌تواند حریم خصوصی افراد را به خطر بیندازد. همچنین وجود گره‌های جعلی یا بدخواه در سطح کاربرد می‌تواند منجر به تصمیم‌گیری‌ها و خروجی‌های نادرست در سیستم‌های IoT (مثل شبکه برق هوشمند یا سیستم حمل‌ونقل) شود.

مطالعات متعددی برای دسته‌بندی و تحلیل این تهدیدات صورت گرفته است. به عنوان نمونه، گوگوث و همکاران (۲۰۲۳) در یک مقاله مروری، انواع مسائل امنیتی IoT را به تفکیک هر لایه بررسی کرده‌اند و نشان می‌دهند رایج‌ترین حملات شامل نشت داده، حملات مرد میانی، تزریق گره مخرب، فیشینگ و جعل هویت است. آن‌ها همچنین خاطرنشان کرده‌اند که هر یک از این ضعف‌ها می‌تواند اثربخشی سیستم‌های IoT را مختل کرده و خطر افشای حریم خصوصی کاربران را افزایش دهد. ضعف در احراز هویت دستگاه‌ها و اطمینان از هویت ارسال‌کننده و دریافت‌کننده داده، یکی از مشکلات اساسی است؛ بسیاری از دستگاه‌های IoT به راحتی فریب مهاجمان را خورده و داده‌ها را در اختیار آنان قرار می‌دهند یا دستوراتشان را اجرا می‌کنند. مشکل دیگر، یکپارچگی و تمامیت داده‌ها (Data Integrity) است. با توجه به نبود مکانیزم‌های ضد دستکاری قوی، داده‌های ارسال‌شده توسط حسگر یا ذخیره‌شده در سرور مرکزی می‌تواند طی مسیر یا در مقصد تغییر یابد، بدون اینکه تشخیص داده شود. این امر برای کاربردهای حساس (مثل پزشکی یا صنایع) می‌تواند عواقب وخیمی داشته باشد. مسئله اعتماد نیز در شبکه‌های IoT مطرح است؛ چگونه می‌توان به داده‌هایی که توسط صدها یا هزاران دستگاه مختلف تولید می‌شود اعتماد کرد و مطمئن بود که جعلی یا تغییر یافته نیستند؟ این موضوع به ویژه در محیط‌های چندذی‌نفع (multi-stakeholder) نظیر زنجیره تامین یا شهر هوشمند اهمیت دارد که در آن دستگاه‌ها و سامانه‌ها متعلق به سازمان‌های مختلف با سطح اعتماد متفاوت هستند.

به طور خلاصه، IoT با چالش‌های امنیت، امانت‌داری داده و حریم خصوصی مواجه است که ناشی از مقیاس بزرگ، ناهمگونی دستگاه‌ها، منابع محدود آن‌ها و معماری متمرکز اغلب سیستم‌های فعلی است. پژوهش‌های اخیر بر لزوم رویکردهای نوین برای ایمن‌سازی IoT تأکید دارند؛ رویکردهایی که بتوانند ضمن حفظ عملکرد و مقیاس‌پذیری، مشکلات فوق را برطرف سازند. در این راستا، فناوری بلاک‌چین به عنوان یکی از امیدبخش‌ترین راهکارها مورد توجه محققین قرار گرفته است.

مفاهیم و قابلیت‌های بلاک‌چین مرتبط با امنیت IoT

بلاک‌چین یک فناوری دفتر کل توزیع شده است که نخستین بار با ظهور ارزهای دیجیتال (مانند بیت‌کوین) مطرح شد. در بلاک‌چین، به جای اتکا به یک پایگاه داده مرکزی، اطلاعات در شبکه‌ای از گره‌ها (Nodes) نگهداری می‌شود و همه گره‌ها در تأیید و ثبت اطلاعات مشارکت دارند. این ساختار غیرمتمرکز، بلاک‌چین را در برابر خرابی یا حمله به یک نقطه بسیار مقاوم می‌سازد؛ چرا که حتی در صورت از دسترس خارج شدن یک یا چند گره، سایر گره‌ها نسخه‌ای از اطلاعات را در اختیار دارند و شبکه به کار خود ادامه می‌دهد. ویژگی کلیدی دیگر بلاک‌چین تغییرناپذیری (Immutability) داده‌هاست. هر رکورد (تراکنش) پس از تأیید و اضافه شدن به زنجیره بلوکی، عملاً غیرقابل تغییر یا حذف است مگر با صرف توان محاسباتی عظیم و جلب رضایت اکثریت گره‌ها. این خاصیت با استفاده از پیوند رمزنگاری بین بلوک‌ها حاصل می‌شود؛ به طوری که هر بلوک حاوی هش بلوک قبلی است و هرگونه دستکاری در محتویات یک بلوک، زنجیره هش‌ها را ناهمخوان کرده و توسط سایر گره‌ها رد می‌شود. برای IoT، این بدان معناست که داده‌های حسگرها یا رخدادهای ثبت شده در بلاک‌چین همواره قابل پیگیری و ممیزی بوده و تضمین می‌شود که پس از ثبت، بدون توافق جمعی قابل تغییر نیستند. در نتیجه، تمامیت داده (data integrity) حتی در محیط‌های خصمانه حفظ خواهد شد.

عدم تمرکز (Decentralization) و اجماع توزیع شده از دیگر ارکان بلاک‌چین هستند که مستقیماً به بهبود امنیت IoT کمک می‌کنند. الگوریتم‌های اجماع نظیر اثبات کار (PoW) و اثبات سهام (PoS) مکانیزمی فراهم می‌کنند تا گره‌های شبکه به اتفاق نظر درباره وضعیت دفتر کل برسند. در IoT سنتی، تصمیم‌گیری برای تأیید داده‌ها یا دسترسی‌ها معمولاً برعهده یک سرور مرکزی است، اما در بلاک‌چین این نقش به کل شبکه توزیع می‌شود؛ لذا هیچ گره متخصصی به تنهایی نمی‌تواند سیستم را فریب دهد مگر آن‌که به منابع اکثریت شبکه دست یابد که بسیار غیرمحتمل است. این تاب‌آوری در برابر تبانی و حملات داخلی خصوصاً برای IoT مهم است، زیرا احتمال وجود گره‌های ناامن یا مخرب در شبکه‌های بزرگ IoT منتفی نیست. بلاک‌چین با مشارکت جمعی گره‌ها در نظارت و تأیید، جلوی اثرگذاری آن‌ها را می‌گیرد. از سوی دیگر، شفافیت (Transparency) بلاک‌چین موجب می‌شود همه ذینفعان به تاریخچه تراکنش‌ها دسترسی (مشروط) داشته باشند و این اعتماد به داده‌ها را افزایش می‌دهد. برای مثال، در یک شبکه IoT مرتبط با زنجیره تأمین کالا، استفاده از بلاک‌چین به همه طرف‌ها (تولیدکننده، حمل‌کننده، فروشنده و ...) امکان می‌دهد مسیر جابه‌جایی کالا و وضعیت سنسورهای مرتبط (دما، رطوبت و غیره) را در هر لحظه به صورت شفاف مشاهده کنند. این شفافیت علاوه بر بهبود اعتماد و همکاری بین طرف‌ها، امکان کشف سریع هرگونه دستکاری یا خرابکاری را فراهم می‌کند.

قراردادهای هوشمند یکی دیگر از قابلیت‌های مهم بلاک‌چین هستند که می‌توانند در IoT کارگشا باشند. قرارداد هوشمند در واقع قطعه کدی است که روی بلاک‌چین ذخیره شده و پس از برآورده شدن شرایط از پیش تعیین شده، به طور خودکار اجرا می‌شود. در زمینه IoT، از قراردادهای هوشمند می‌توان برای خودکارسازی فرایندهای امنیتی بهره برد. به عنوان نمونه، یک قرارداد هوشمند می‌تواند به عنوان سیستم کنترل دسترسی عمل کند؛ بدین صورت که فقط در صورت ارائه کلید یا اعتبار دیجیتال معتبر، اجازه دسترسی یک دستگاه به داده یا سرویس را صادر کند و تمام این فرایند به شکل خودکار و توزیع شده انجام شود. یا در بحث مدیریت هویت و احراز هویت دستگاه‌ها، قراردادهای هوشمند می‌توانند ثبت و تأیید هویت دستگاه‌های جدید را در شبکه IoT بر عهده بگیرند و به محض تشخیص یک دستگاه ناشناخته یا نامعتبر، آن را از تعامل با سایرین بازدارند. پژوهش‌لی و همکاران (۲۰۲۳) یک سامانه مبتنی بر بلاک‌چین پیشنهاد داده‌اند که با ترکیب رمزنگاری مبتنی بر خصوصیات (CP-ABE) و قراردادهای هوشمند، کنترل دسترسی به داده‌ها و توافق کلید را در محیط IoT امکان‌پذیر ساخته است. آنها برای ارزیابی امنیتی، آنالیزهای رسمی و غیررسمی انجام داده‌اند که نشان می‌دهد سیستم پیشنهادی در برابر حملاتی نظیر ردیابی و حدس کلید مقاوم است.

ویژگی دیگر بلاک چین که به حریم خصوصی مرتبط است، استفاده از کلیدهای عمومی ناشناس برای شناسایی کاربران/دستگاهها است. در بسیاری از بلاک چینها، هویت واقعی افراد پنهان و تنها آدرسهای دیجیتال (مشتق شده از کلید عمومی) آنها دیده می شود. این خصوصیت می تواند تا حدی ناشناس بودن در تبادل داده های IoT را تضمین کند؛ به نحوی که دستگاهها بدون افشای هویت واقعی صاحبشان، با یکدیگر تعامل امن داشته باشند. البته بلاک چین ذاتاً شفاف است و همه تراکنشها به صورت زنجیره ای قابل ردیابی اند، لذا برای حفظ کامل حریم خصوصی، ممکن است نیاز به تکنیکهای مکمل باشد (مثل رمزنگاری پیشرفته یا ساختارهای زنجیره بلوکی خصوصی). اما حتی در ساده ترین حالت، حذف سرورهای مرکزی که معمولاً حجم بالایی از داده های شخصی کاربران IoT را در خود متمرکز می کنند، خود گامی مثبت در جهت ارتقای حریم خصوصی محسوب می شود. به عنوان مثال، در یک خانه هوشمند اگر تبادل داده بین دستگاهها (ترموستات، دوربین، قفل درب و غیره) به صورت مستقیم و نظریه نظیر بر بستر بلاک چین انجام شود، نیازی به ارسال تمام داده ها به سرویس ابری شرکت سازنده نخواهد بود؛ در نتیجه ریسک افشای اطلاعات خصوصی به علت نفوذ به سرور ابری یا سوءاستفاده شرکت واسطه، به میزان چشمگیری کاهش می یابد.

جدول ۱ - ویژگی های بلاک چین و مزایای آن در امنیت و حریم خصوصی

ویژگی بلاک چین	مزیت برای امنیت/حریم خصوصی
عدم تمرکز و توزیع شدگی	حذف نقطه ضعف مرکزی و افزایش تاب آوری در برابر حملات؛ ایجاد اعتماد توزیع شده بین دستگاهها
تغییرناپذیری داده ها	حفظ تمامیت داده های حسگرها؛ جلوگیری از دستکاری یا حذف سوابق و امکان ممیزی کامل
شفافیت و ممیزی پذیری	قابلیت ردیابی تراکنشها و فعالیت دستگاهها؛ افزایش اعتماد و کشف سریع رفتارهای مشکوک
قراردادهای هوشمند	خودکارسازی کنترل دسترسی و احراز هویت؛ اجرای بی درنگ سیاستهای امنیتی بدون نیاز به واسطه
رمزنگاری و امضای دیجیتال	تضمین محرمانگی و اصالت داده های تبادلی؛ جلوگیری از جعل هویت و دسترسی غیرمجاز به اطلاعات

جدول ۱ به طور خلاصه برخی از ویژگی های کلیدی بلاک چین و نقش آنها در بهبود امنیت و حریم خصوصی IoT را نشان می دهد. همان طور که ملاحظه می شود، این ویژگی ها مستقیماً به مقابله با چالش هایی که پیش تر ذکر شد کمک می کنند.

جدول ۲ - مقایسه امنیت سنتی در IoT با بلاک چین

ویژگی امنیتی	IoT رویکرد سنتی در	رویکرد مبتنی بر بلاک چین
کنترل دسترسی	متمرکز (سرور مرکزی)	توزیع شده (قرارداد هوشمند)
تمامیت داده ها	آسیب پذیر در مسیر انتقال	تغییرناپذیر با هش رمزنگاری
احراز هویت	مبتنی بر گواهی مرکزی	DID مبتنی بر کلید عمومی و
ممیزی تراکنش	دشوار و غیرشفاف	شفاف و قابل رهگیری
وابستگی به واسطه ثالث	بالا	بسیار پایین

چهارمین کنفرانس بین المللی
مهندسی و فناوری اطلاعات

جدول ۲ مقایسه‌ای بین رویکردهای امنیتی سنتی در اینترنت اشیا و راهکارهای نوین مبتنی بر بلاک‌چین ارائه می‌دهد. همان‌طور که مشاهده می‌شود، در روش‌های سنتی، بسیاری از وظایف امنیتی همچون احراز هویت، کنترل دسترسی و مدیریت داده‌ها به صورت متمرکز انجام می‌شود که خود منشأ تهدیدات مختلف است. در مقابل، بلاک‌چین با بهره‌گیری از ساختار توزیع‌شده و قراردادهای هوشمند، امکان اجرای مکانیزم‌های امنیتی به صورت غیرمتمرکز و مقاوم در برابر نفوذ را فراهم می‌سازد.

پژوهش‌های پیشین در زمینه ادغام بلاک‌چین و IoT

از حدود سال ۲۰۱۶ میلادی، ایده بهره‌گیری از بلاک‌چین برای رفع مشکلات امنیتی IoT مطرح شد. در سال‌های اخیر (به‌ویژه از ۲۰۲۰ به بعد) این حوزه توجه زیادی را در جامعه پژوهشی به خود جلب کرده و مقالات مروری و طرح‌های نوآورانه متعددی ارائه شده است. در این بخش به برخی از مهم‌ترین مطالعات اخیر که بنیان فکری این پژوهش را شکل داده‌اند، اشاره می‌کنیم. یکی از کارهای شاخص، مطالعه مروری سیستماتیک (SLR) توسط المری و الجییمان (۲۰۲۴) است. این مطالعه با بررسی جامع تحقیقات موجود، نتیجه می‌گیرد که ادغام بلاک‌چین با IoT می‌تواند چالش‌های امنیتی و اعتماد را تا حد زیادی برطرف کند. یافته‌های کلیدی آن‌ها نشان می‌دهد بلاک‌چین می‌تواند از دستکاری داده‌ها جلوگیری کرده، مدیریت هویت را تقویت و تراکنش‌های شفاف و قابل‌راستی‌آزمایی را در شبکه IoT میسر کند. همچنین این تحقیق به جنبه‌های پایداری نیز توجه کرده و مطرح می‌کند که بهبود امنیت از طریق بلاک‌چین، به بهینه‌سازی مصرف منابع و افزایش تاب‌آوری سیستم‌هایی مانند زنجیره تامین و شبکه برق هوشمند منجر می‌شود. از سوی دیگر، شکاف‌ها و چالش‌های باز پژوهشی نظیر مقیاس‌پذیری و کارایی نیز شناسایی شده که در بخش‌های بعدی به آن‌ها بازخواهیم گشت.

در یک مقاله مروری دیگر، گوگوت و همکاران (۲۰۲۳) ضمن برشمردن تهدیدات IoT، راه‌حل‌های مبتنی بر بلاک‌چین را نیز دسته‌بندی کرده‌اند. آن‌ها ویژگی‌های امنیتی بلاک‌چین (همانند آنچه در جدول ۱ آمد) و چالش‌های ناشی از ادغام این دو فناوری را بررسی نموده‌اند. همچنین پروتکل‌های اجماع مختلف، تکنیک‌های امنیتی موجود و شاخص‌های ارزیابی امنیت در این حوزه را مرور کرده‌اند. نتیجه‌گیری کارشان مؤید این است که بلاک‌چین یک راه‌حل بالقوه قوی برای مسائل امنیتی IoT است، اما در عین حال مسائل بازی مانند مقیاس‌پذیری، سربار عملکرد و برخی ملاحظات حریم خصوصی باید در تحقیقات آینده مد نظر قرار گیرد.

از منظر ارائه راهکار، تحقیقات کاربردی متعددی انجام شده است. آل‌صدآوی و همکاران (۲۰۲۱) یک معماری ترکیبی سه‌لایه برای ادغام بلاک‌چین و IoT پیشنهاد داده‌اند که در آن از رایانش ابری محلی (Cloudlet) و Dew Computing استفاده شده است. هدف آن‌ها ارتقای کارایی احراز هویت، ذخیره‌سازی داده و بهبود امنیت و عملکرد سیستم بوده است. معماری پیشنهادی آل‌صدآوی با بهره‌گیری از بلاک‌چین، به دنبال تحقق مقاومت در برابر خطا، کارایی، مقیاس‌پذیری، امنیت و ذخیره‌سازی غیرمتمرکز داده‌ها در محیط IoT بوده است. این رویکرد نشان می‌دهد که حتی در سطح معماری نیز می‌توان بلاک‌چین را به عنوان ستون فقرات یک سیستم IoT امن در نظر گرفت.

در حوزه احراز هویت، دیپ و همکاران (۲۰۲۴) یک روش احراز هویت توزیع‌شده مبتنی بر بلاک‌چین برای خدمات IoT معرفی کرده‌اند. آن‌ها اهمیت امنیت IoT را یادآور شده و طرحی تلفیقی ارائه نموده‌اند که بلاک‌چین را با سامانه IoT ترکیب می‌کند تا احراز هویت دستگاه‌ها به شکل امن و سریعی انجام شود. این روش در شبیه‌سازی‌های انجام‌شده ارزیابی گردیده و نتایج نشان داده است که با استفاده از آن، کنترل دسترسی و تبادل داده امن‌تر انجام شده و اعتماد بین گره‌ها تقویت می‌شود. به بیان دیگر، اهداف امنیت و اعتماد در محیط IoT از طریق بهبود سازوکارهای احراز هویت و تبادل داده تحقق یافته است.

محمدی و ملکی نیا (۱۴۰۱) نیز در یک پژوهش کنفرانسی فارسی، پس از تبیین مشکلات امنیتی IoT و معرفی اجمالی بلاکچین، چند نمونه از تحقیقات انجام شده در این حوزه را بررسی کرده اند. در جمع بندی کار آن ها آمده است که بلاکچین با ویژگی های منحصر به فردش می تواند به عنوان ابزاری مهم در تقویت امنیت اینترنت اشیا در برابر تهدیدات مختلف و کاهش ریسک ها ایفای نقش کند. همچنین به برخی چالش های استفاده از بلاکچین (احتمالاً مواردی چون مقیاس پذیری و هزینه) اشاره شده است. از میان کاربردهای مشخص IoT، حوزه هایی مانند زنجیره تأمین، شهر هوشمند، انرژی هوشمند و بهداشت بیشتر مورد توجه پژوهشگران قرار گرفته است. به عنوان مثال، لوکل و همکاران (۲۰۲۰) با هدف ایجاد اعتماد در اکوسیستم های IoT، اصول طراحی برای کاربردهای IoT مبتنی بر بلاکچین را بررسی کرده اند. آن ها در مقاله خود بر مؤلفه های اعتماد تمرکز نموده و نتیجه گرفته اند که سیستم های IoT وقتی بر بستر بلاکچین سوار شوند، می توانند به الزامات اعتماد (شامل محرمانگی، صحت و دسترس پذیری داده CIA - بهتر پاسخ دهند. همچنین نشان داده اند که وابستگی به سرورهای ابری متمرکز کاهش یافته و بلاکچین می تواند تضمین کننده ویژگی های محرمانگی، تمامیت و دسترس پذیری داده های IoT باشد. در حوزه کنترل دسترسی سبک وزن، سان و همکاران (۲۰۲۱) سیستمی ارائه داده اند که به دستگاه های IoT اجازه می دهد در نقش گره های تخصصی بلاکچین عمل کنند. راهکار آن ها با کاهش افزونگی زنجیره بلوکی و ترکیب کنترل دسترسی مبتنی بر خصوصیات (ABAC) و امضاهای مبتنی بر هویت، موفق شده است امنیت را بهبود بخشد و انواع مختلفی از حملات) از جمله حملات منع سرویس توزیع شده (DDoS) - را به طور کارا دفع کند. این دستاورد حائز اهمیت است زیرا یکی از نگرانی ها در به کارگیری بلاکچین برای IoT، افزونگی داده ها و سربار ناشی از ذخیره بلاک ها در دستگاه های کم ظرفیت بود؛ اما راهکار سان و همکاران نشان داد می توان با طراحی مناسب، این نگرانی را تا حدی برطرف ساخت.

نمونه های فوق بخش کوچکی از انبوه پژوهش های این حوزه هستند. با مرور ادبیات می توان دریافت که اجماع عمومی میان محققین بر مزایای چشمگیر بلاکچین برای امنیت IoT است؛ با این حال، هر مطالعه به جنبه خاصی پرداخته و گاهی نتایج متفاوتی در زمینه کارایی و محدودیت ها گزارش می شود. از این رو، نیاز به یک جمع بندی جامع از این دستاوردها و نیز شناسایی خلأ های پژوهشی وجود دارد. مقاله حاضر با تکیه بر چنین پشتوانه ای، در بخش های بعد تلاش می کند تصویری یکپارچه از چارچوب مفهومی تلفیق بلاکچین و IoT و نیز یافته های تجربی و تحلیلی مربوطه ارائه دهد.

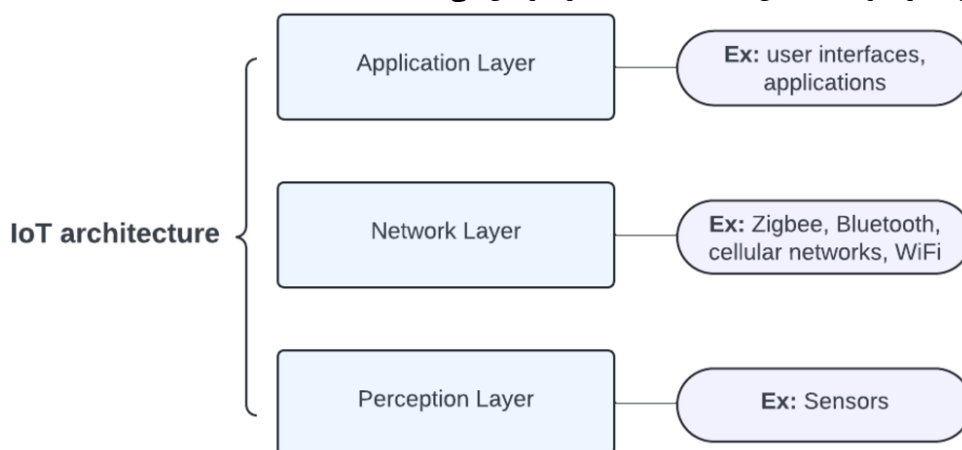
چارچوب مفهومی پیشنهادی

با توجه به مباحث پیشین، چارچوب مفهومی این پژوهش بر اساس ادغام لایه های معماری IoT با یک لایه امنیتی مبتنی بر بلاکچین بنا شده است. شکل ۲ نمایی کلی از این چارچوب را نشان می دهد که در آن یک «ماژول IoT» شامل دستگاه ها و حسگرها در تعامل با یک «بلاکچین» قرار گرفته است. در این طرح، بلاکچین به عنوان زیرساخت اعتماد عمل کرده و ویژگی هایی مانند دفترکل توزیع شده، شفافیت، قراردادهای هوشمند، عدم تمرکز و تغییرناپذیری را فراهم می کند. داده های تولید شده توسط دستگاه های IoT پیش از ارسال به بلاکچین، به صورت امن (مثلاً رمزگذاری شده) درآمده و سپس در قالب تراکنش به شبکه بلاکچین منتقل می شوند. شبکه بلاکچین که می تواند خصوصی/ائتلافی باشد (با حضور ذینفعان مشخص) یا عمومی (باز برای همه)، تراکنش دریافتی را از طریق مکانیزم اجماع تأیید و در بلاک جدیدی ثبت می کند. هر بلاک جدید به زنجیره اضافه شده و بین گره های بلاکچین توزیع می شود. بدین ترتیب داده های IoT در بستری امن ثبت شده و قابل حذف یا تغییر نیستند.

شکل ۲: چارچوب مفهومی یکپارچه سازی بلاکچین با IoT - بلاکچین به عنوان لایه امنیت و اعتماد عمل می کند و با فراهم کردن دفترکل توزیع شده (Ledger) و قابلیت هایی چون عدم تمرکز، شفافیت، تغییرناپذیری و قراردادهای هوشمند، به

چهارمین کنفرانس بین المللی
مهندسی و فناوری اطلاعات

ماژول های IoT امکان می دهد داده های خود را به صورت رمزنگاری شده تبادل کنند. این معماری از دسترسی غیرمجاز به داده ها جلوگیری کرده و اعتماد بین دستگاه های IoT را افزایش می دهد.



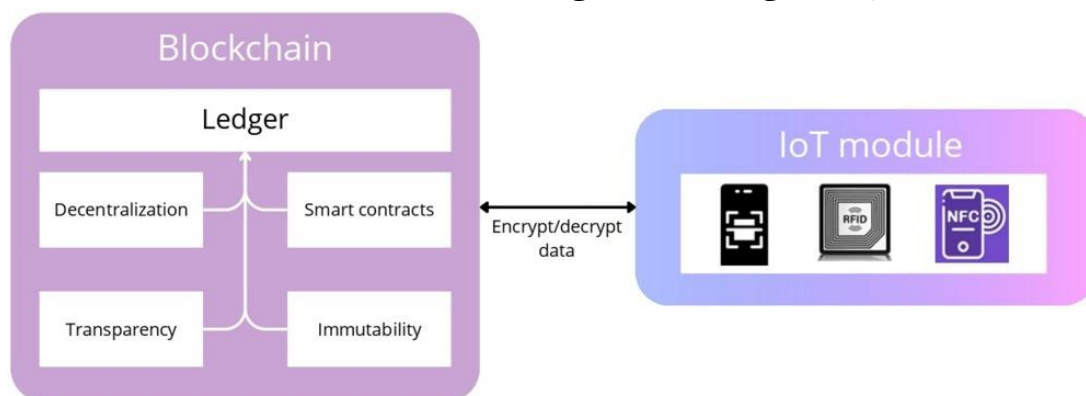
شکل ۲ – جریان احراز هویت و ثبت تراکنش در شبکه بلاک چینی مبتنی بر IoT: این نمودار فرایند احراز هویت یک دستگاه IoT و ثبت داده آن در دفترکل توزیع شده بلاک چین را نمایش می دهد؛ شامل امضای دیجیتال، تأیید تراکنش از طریق اجماع و ذخیره سازی ایمن داده.

در چارچوب پیشنهادی، هر دستگاه IoT یک هویت دیجیتال مبتنی بر کلید عمومی در بلاک چین دارد. این هویت در زمان ثبت دستگاه در شبکه توسط قرارداد هوشمند یا سازوکار ثبت اختراع تعیین می شود و می تواند به صورت گواهی دیجیتال غیرمتمرکز (مثلاً DID – Decentralized Identifier) پیاده سازی شود. هر بار که دستگاه IoT داده ای تولید می کند (مثلاً اندازه گیری یک سنسور محیطی)، ابتدا آن داده را با کلید خصوصی خود امضا می کند تا اصالت و یکپارچگی آن تضمین شود. سپس داده ممکن است رمزگذاری شود (در صورت حساس بودن، برای حفظ حریم خصوصی) و به همراه امضای دیجیتال در یک تراکنش بلاک چین قرار گیرد. این تراکنش به شبکه ارسال شده و بین ماینرها/تأییدکنندگان پخش می شود. پس از طی فرایند اجماع (مثلاً اعتبارسنجی امضا و اطمینان از عدم تناقض)، تراکنش در بلاک جدید ثبت و به زنجیره اضافه می گردد. در سمت دیگر، هر کاربر یا برنامه کاربردی که مجاز به دریافت این داده ها باشد، می تواند بلاک چین را خوانده و داده رمزنگاری شده را (در صورت داشتن کلید لازم) رمزگشایی نماید و از صحت امضای آن اطمینان حاصل کند. به این ترتیب، حتی اگر ارتباط شبکه ای دستگاه تا مقصد ناامن باشد، داده ثبت شده در بلاک چین دستکاری نشده و قابل اعتماد خواهد بود.

مدل امنیتی در این چارچوب از دو بخش مکمل تشکیل شده است: یکی امن سازی دستگاه ها و ارتباطات IoT (از طریق امضا، رمزنگاری و پروتکل های امنیتی پایه) و دیگری حفظ امنیت و اعتماد در سطح شبکه کلان (از طریق بلاک چین و اجماع توزیع شده). ترکیب این دو، یک راهکار انتها-به-انتها ارائه می دهد. به عنوان مثال، اگر مهاجمی سعی در جعل هویت یک دستگاه داشته باشد، به دلیل نداشتن کلید خصوصی آن دستگاه، امضای معتبری نخواهد داشت و تراکنش جعلی او توسط گره های بلاک چین رد می شود. یا اگر مهاجم داده ای ارسال شده را در میان راه تغییر دهد، امضای دیجیتال تطابق نخواهد داشت و بلاک چین آن را نمی پذیرد. حتی در سناریویی که یک دستگاه IoT به تصرف مهاجم درآید و داده های نادرست ارسال کند، امکان ممیزی و ردیابی منبع داده (از طریق تاریخچه تراکنش های بلاک چین) وجود دارد و می توان دستگاه مخرب را شناسایی و از شبکه حذف کرد. بنابراین، چارچوب پیشنهادی سطوح مختلفی از دفاع را فراهم می سازد.

نکته مهم دیگر مقیاس پذیری است. در معماری پیشنهادی، بسته به حجم دستگاه ها و نرخ تولید داده، می توان از بلاک چین های مقیاس پذیر یا فناوری های دفترکل توزیع شده جایگزین استفاده کرد. برای شبکه های IoT بزرگ (شامل میلیون ها دستگاه)، ممکن است به کارگیری یک بلاک چین منفرد کافی نباشد؛ لذا روش هایی چون شاردینگ (Sharding) یا

استفاده از گراف جهت‌دار غیرمدور (DAG) پیشنهاد می‌شود که در آن تراکنش‌ها به صورت موازی و غیرزنجیره‌ای تأیید شوند. اما برای سادگی مدل مفهومی، در شکل ۲ یک زنجیره بلوکی واحد به تصویر کشیده شده است. این زنجیره می‌تواند پیاده‌سازی‌های متنوعی داشته باشد: از پلتفرم‌های متن‌باز موجود (مثل اتریوم، هایپرلجر یا پلتفرم‌های خاص IoT) گرفته تا زنجیره‌های خصوصی سفارشی که تنها نودهای مربوط به یک سازمان یا کنسرسیوم در آن عضو هستند. انتخاب پلتفرم وابسته به سناریوی کاربردی خواهد بود (برای مثال در کاربردهای صنعتی شاید بلاک‌چین کنسرسیومی ترجیح داده شود، در حالی که برای شهر هوشمند یک بلاک‌چین عمومی با مشارکت همگانی مناسب باشد).



شکل ۳ – چارچوب مفهومی پیشنهادی برای ادغام بلاک‌چین با اینترنت اشیا: در این معماری، بلاک‌چین به عنوان لایه امنیتی در تعامل با قرار می‌گیرد و با فراهم‌سازی قابلیت‌هایی مانند عدم تمرکز، اجماع توزیع‌شده و قراردادهای هوشمند، زیرساختی امن و IoT دستگاه‌های قابل اعتماد برای تبادل داده ایجاد می‌کند.

به طور خلاصه، چارچوب مفهومی این پژوهش در صدد است IoT را از طریق لایه بلاک‌چین مقاوم‌سازی کند؛ به طوری که امنیت، حریم خصوصی و اعتماد به صورت درونی در معماری شبکه گنجانده شود نه اینکه بعداً از طریق وصله‌های متمرکز برقرار گردد. این چارچوب نقطه شروعی برای تحقق سیستم‌های IoT امن در مقیاس بزرگ است و در بخش بعدی، روش تحقیق برای بررسی و ارزیابی این چارچوب تشریح می‌شود.

روش تحقیق

رویکرد تحقیق در این مطالعه به صورت کیفی و توصیفی-تحلیلی بوده و بر مطالعات کتابخانه‌ای و مروری نظام‌مند متکی است. شکل کلی روش تحقیق به مراحل زیر قابل تفکیک است:

۱. تعریف مسئله و فرضیه پژوهش: ابتدا با مطالعه گزارش‌ها و مقالات اولیه، خلأهای امنیتی در حوزه IoT شناسایی و ایده بهره‌گیری از بلاک‌چین به عنوان راه‌حل ممکن مطرح شد. فرضیه‌ای که هدایتگر پژوهش بوده این است که بلاک‌چین نقشی انقلابی در ارتقای امنیت و حریم خصوصی IoT دارد.

۲. گردآوری منابع مرتبط (۲۰۲۰ به بعد): به منظور اطمینان از بروز بودن مباحث، صرفاً منابع منتشرشده طی پنج سال اخیر (۲۰۲۰ تا ۲۰۲۵ میلادی) مورد بررسی قرار گرفت. پایگاه‌های معتبر IEEE, Elsevier (ScienceDirect), Springer, ACM برای مقالات انگلیسی و پایگاه‌هایی نظیر سیویلیکا، مگایران و نشریات علمی داخلی برای منابع فارسی جستجو شدند. از ترکیب کلمات کلیدی مرتبط (IoT, Security, Privacy, Blockchain) و معادل‌های فارسی آنها (در عنوان و چکیده مقالات استفاده گردید. پس از جستجوی گسترده، حدود ۵۰ منبع اولیه انتخاب شدند.

چهارمین کنفرانس بین المللی
مهندسی و فناوری اطلاعات

۳. غربالگری و انتخاب نهایی منابع: در مرحله بعد با مطالعه چکیده و اجمالی مقالات، منابع خیلی عمومی یا نامرتبط حذف و بر مقالات پژوهشی متمرکز بر امنیت/حریم خصوصی IoT مبتنی بر بلاک چین تمرکز شد. همچنین اولویت به مقالات ژورنالی با کیفیت (Q1/Q2) و کنفرانس‌های معتبر داده شد. در نهایت حدود ۳۰ منبع برای مطالعه عمیق برگزیده شدند که شامل چندین مقاله مروری شاخص و تعدادی مقاله پژوهشی با مدل‌ها یا نتایج تجربی بود.

۴. مطالعه عمیق و یادداشت‌برداری: مقالات منتخب به دقت مطالعه شدند. نکات کلیدی هر مقاله شامل اهداف، روش، نتایج و نقاط قوت/ضعف یادداشت و در یک ماتریس مقایسه درج گردید. به طور خاص، برای هر پژوهش مشخص شد که کدام جنبه از امنیت IoT (احراز هویت، تمامیت، محرمانگی، دسترس‌پذیری، اعتماد، ...) را مدنظر قرار داده و چگونه بلاک چین در راهکار پیشنهادی به کار رفته است.

۵. ساخت چارچوب مفهومی: بر پایه مفاهیم به دست آمده از ادبیات، چارچوب مفهومی ترکیبی بلاک چین IoT-طراحی شد (که در بخش قبل ارائه گردید). این چارچوب جنبه‌های مختلف از سطح دستگاه تا شبکه را پوشش می‌دهد. برای اعتبارسنجی اولیه چارچوب، منطبق بودن آن با نمونه‌های مطرح شده در منابع (مانند معماری‌های پیشنهاد شده توسط سایرین) بررسی شد تا از جامعیت آن اطمینان حاصل شود.

۶. تحلیل تطبیقی و استدلالی: در بخش تحلیل یافته‌ها، بر اساس شواهد گردآوری شده از مقالات، نقش بلاک چین در بهبود هر یک از شاخص‌های امنیت و حریم خصوصی IoT مورد بحث قرار گرفت. این تحلیل به صورت استدلالی و با ارجاع به نتایج کمی/کیفی گزارش شده در منابع انجام شد. همچنین چالش‌های احتمالی یا مواردی که بلاک چین به تنهایی قادر به حل آن نیست نیز شناسایی و تحلیل گردید.

۷. جمع‌بندی و پیشنهادات: در پایان، با جمع‌بندی یافته‌ها، میزان تأیید فرضیه پژوهش (مؤثر بودن بلاک چین در ارتقای امنیت IoT) سنجیده شد. سپس پیشنهاداتی برای تحقیقات آتی و همچنین برای به کارگیران صنعتی IoT ارائه گردید.

این روش تحقیق به ما امکان داد تا ضمن دست‌یابی به درکی جامع از وضعیت دانش در حوزه مورد نظر، از ترکیب نتایج پژوهش‌های مختلف برای استنتاج نتیجه‌گیری‌های کلی‌تر استفاده کنیم (رویکرد فراترکیب). به بیان دیگر، با تحلیل مقایسه‌ای مطالعات مختلف، سعی شده است الگوهای مشترک در موفقیت‌ها و شکست‌های به کارگیری بلاک چین در IoT استخراج شود. مثلاً این که کدام مکانیزم‌های امنیتی بیشتر بهبود یافته‌اند یا کدام چالش‌ها کماکان باقی مانده‌اند. محدودیت اصلی پژوهش حاضر ماهیت نظری و کتابخانه‌ای آن است؛ به این معنی که ما به طراحی یک چارچوب و استنتاج از پژوهش‌های دیگر اکتفا کرده‌ایم و پیاده‌سازی عملی یا شبیه‌سازی مستقلی انجام نداده‌ایم. با این حال، اعتبار نتایج به سبب اتکا بر داده‌ها و نتایج مقالات معتبر، بالاست و می‌تواند مبنای تحقیقات تجربی آینده قرار گیرد.

تحلیل یافته‌ها

در این بخش، بر مبنای مطالعات بررسی شده و چارچوب مفهومی ارائه شده، تأثیرات به کارگیری بلاک چین بر امنیت و حریم خصوصی IoT را در چند محور کلیدی تحلیل می‌کنیم. محورهایی که در ادامه می‌آیند عمدتاً منعکس‌کننده معیارهای امنیت اطلاعات (مانند محرمانگی، صحت، دسترس بودن) و ملزومات حریم خصوصی و اعتماد در

سیستم‌های IoT هستند. برای هر محور، شواهد و نمونه‌هایی از پژوهش‌های اخیر ذکر شده و سپس جمع‌بندی تحلیلی ارائه می‌گردد.

بهبود تمامیت و غیر قابل تغییر بودن داده‌ها

تمامیت داده (Data Integrity) به معنای مصون ماندن اطلاعات از هرگونه تغییر یا خراب‌شدگی غیرمجاز است. در IoT سنتی، به دلیل نبود زیرساخت دفتر کل توزیع‌شده، داده‌های جمع‌آوری‌شده غالباً در مسیر انتقال یا در مخزن مرکزی آسیب‌پذیرند و ممکن است دستکاری شوند. ورود بلاک‌چین به این حوزه تأثیر قابل توجهی بر بهبود تمامیت داده داشته است. همان‌طور که پیش‌تر اشاره شد، بلاک‌چین با ساختار زنجیره‌ای خود هرگونه دستکاری در بلوک‌های قبلی را غیرممکن می‌سازد. بنابراین اگر داده‌های حسگرها مستقیماً (یا پس از تجمیع محلی) در یک بلاک‌چین ذخیره شوند، اطمینان حاصل می‌شود که آن داده‌ها بعداً بدون مجوز اکثریت تغییر نمی‌کنند. پژوهش‌های متعددی این مزیت را تأیید کرده‌اند. برای مثال، در مطالعه مروری المری و الجعیمان (۲۰۲۴) ذکر شده که یکی از یافته‌های اصلی ادغام بلاک‌چین با IoT، جلوگیری از دستکاری داده‌ها و تضمین تمامیت آنها است. همچنین محمدی و ملکی‌نیا (۱۴۰۱) در مقاله خود بلاک‌چین را مکانیزمی برای انتقال داده‌های محافظت‌شده در IoT معرفی کرده‌اند؛ بیان می‌کنند که مسئولیت بلاک‌چین در IoT اعطای روشی جهت اطمینان از انتقال امن داده‌هاست که تلویحاً به حفظ تمامیت و محرمانگی اشاره دارد.

علاوه بر مقاومت در برابر تغییر، قابلیت ممیزی و شفافیت بلاک‌چین کمک می‌کند که هر تغییری در داده‌ها (در صورت وقوع) فوراً آشکار شود. هر ذی‌نفع می‌تواند تاریخچه ثبت داده حسگر را در بلاک‌چین دنبال کند و اگر مغایرتی مشاهده شد، این مغایرت نشان‌دهنده یک رخداد غیرمجاز است. در سیستم‌های سنتی معمولاً کشف تغییر یا نشت داده نیازمند مکانیزم‌های الحاقی (مثل سیاهه‌های ثبت وقایع در سرور مرکزی) است که ممکن است خود در معرض حذف یا تغییر باشند. بلاک‌چین با ثبت تغییرات به صورت توزیع‌شده و غیرقابل حذف، مسیر حسابرسی مطمئنی ایجاد می‌کند.

جمع‌بندی: شواهد نشان می‌دهد استفاده از بلاک‌چین، تمامیت داده‌های IoT را تا حد زیادی تضمین می‌کند. هرچند باید توجه داشت که بلاک‌چین تغییرناپذیری داده‌های پس از ثبت را فراهم می‌کند؛ یعنی اگر داده اشتباهی توسط یک حسگر (مثلاً تحت تأثیر نقص یا حمله) تولید و به‌درستی در بلاک‌چین ثبت شود، بلاک‌چین آن را عیناً حفظ می‌کند. بنابراین صحت منبع داده (sensor trustworthiness) خارج از حیطه بلاک‌چین است. اما مکانیزم‌هایی مثل قراردادهای هوشمند اعتبارسنجی یا مدل‌های اعتماد مبتنی بر بلاک‌چین می‌توانند مکمل باشند تا داده‌های ورودی قبل از ثبت اعتبارسنجی شوند. به طور کلی، نقطه قوت اصلی بلاک‌چین در این محور، حذف امکان اعمال تغییر پنهانی در اطلاعات و فراهم کردن رهگیری کامل تغییرات است.

مدیریت هویت و کنترل دسترسی توزیع‌شده

یکی از دغدغه‌های اساسی امنیت IoT، اطمینان از این است که فقط دستگاه‌ها و کاربران مجاز به منابع و داده‌های IoT دسترسی داشته باشند. سامانه‌های سنتی معمولاً از سرورهای احراز هویت و مدیریت دسترسی متمرکز بهره می‌برند که همان‌طور که گفته شد، می‌تواند گلوگاه و نقطه شکست باشد. رویکرد مبتنی بر بلاک‌چین به سمت

مدیریت هویت غیرمتمرکز (Decentralized Identity Management) و کنترل دسترسی توزیع شده حرکت می کند. بدین معنا که به جای یک سرور واحد، شبکه بلاک چین بر اساس توافق جمعی هویت ها را تأیید و سطوح دسترسی را تعیین می کند.

در سال های اخیر الگوهای مختلفی برای این موضوع ارائه شده است. یکی از این الگوها، استفاده از توکن ها یا گواهی های دیجیتال مبتنی بر بلاک چین برای احراز هویت دستگاه ها است. به عنوان مثال، هوایات و همکاران (۲۰۲۳) یک چارچوب احراز هویت مبتنی بر بلاک چین ارائه داده اند که از رمزنگاری AES برای محرمانگی داده نیز بهره می برد. سیستم آنها داده های رمزنگاری شده IoT را در محیط ابری ذخیره می کند اما از بلاک چین برای مدیریت کلید و تأیید هویت استفاده می نماید. این راهکار تلاش کرده ضمن حفظ امنیت، بار محاسباتی احراز هویت را کاهش دهد. نتایج این تحقیق نشان داد که عملکرد IoT با کاهش نیاز به رمزنگاری های مکرر بهبود یافته، اگرچه در شرایط بار بسیار بالا کماکان کمی تأخیر مشاهده شده است.

در حوزه کنترل دسترسی (Access Control)، قراردادهای هوشمند به عنوان ابزار پیاده سازی سیاست ها به کار رفته اند. برای نمونه، همان طور که در بخش قبل ذکر شد، لی و همکاران (۲۰۲۳) از قرارداد هوشمند به همراه رمزنگاری مبتنی بر صفات برای کنترل دسترسی بهره گرفته اند. رویکردهای دیگری نیز وجود دارد که به جای قرارداد هوشمند، از لیست های کنترل دسترسی توزیع شده (DACL) بر بستر بلاک چین استفاده می کنند؛ بدین صورت که هر منبع (مثلاً یک حسگر یا عملگر) یک ورودی در بلاک چین دارد که مجاز بودن یا نبودن دسترسی سایر هویت ها به آن را مشخص می کند. هر زمان نیاز به به روز رسانی سیاست دسترسی باشد، یک تراکنش جدید ثبت و وضعیت دسترسی تغییر می یابد. چنین سیستمی در برابر تغییرات غیرمجاز مقاوم است، زیرا فقط صاحبان مجاز (از طریق کلید خصوصی) قادر به تغییر سیاست خواهند بود و تمامی تغییرات در تاریخچه ثبت می شود.

اعتماد پذیری احراز هویت نیز با بلاک چین افزایش می یابد. وقتی یک دستگاه جدید می خواهد به شبکه IoT بپیوندد، به جای اینکه صرفاً به یک دروازه اعتماد کند، می تواند توسط چندین گره تأیید هویت شود. این کاهش وابستگی به یک نهاد، احتمال نفوذ مهاجم با جعل هویت را کم می کند. پژوهش دیپ و همکاران (۲۰۲۴) که پیش تر اشاره شد، نشان داد احراز هویت توزیع شده به کمک بلاک چین می تواند هم سریع باشد و هم امنیت را افزایش دهد. در واقع، نتایج شبیه سازی آنها تأیید کرد که زمان انجام احراز هویت همچنان در سطح قابل قبول بلادرنگ باقی می ماند و همزمان سیستم در برابر نفوذ و جعل هویت ایمن تر شده است.

یک نکته مهم در اینجا، مقیاس پذیری مکانیزم های هویت و دسترسی است. بلاک چین های عمومی نظیر اتریوم اگر مستقیماً برای صدور توکن های دسترسی استفاده شوند، ممکن است کارمزدها (gas) و تأخیر تأیید بلاک مشکل ساز شود. راهکارهایی چون استفاده از زنجیره های جانبی یا شبکه های مجاز (permissioned) برای IoT پیشنهاد شده که تعداد محدودی گره معتبر وظیفه اجماع را برعهده دارند و بنابراین سرعت بالاتری دارند. برخی تحقیقات از مدل های اجماع سریع تر) مثل PBFT یا Raft برای شبکه های بلاک چینی کوچک مخصوص IoT بهره گرفته اند تا تأخیر احراز هویت را به حداقل برسانند.

جمع بندی: بلاک چین توانمندی قابل توجهی در توزیع فرآیندهای احراز هویت و کنترل دسترسی در IoT دارد. این امر باعث حذف نقاط شکست مرکزی، افزایش اعتماد به مکانیزم های هویتی و مانع گذاری بیشتر در برابر نفوذگران

چهارمین کنفرانس بین المللی
مهندسی و فناوری اطلاعات

می‌شود. البته چالش‌هایی مانند هزینه محاسباتی الگوریتم‌های اجماع و مدیریت کلید در مقیاس بزرگ وجود دارد که باید با انتخاب پلتفرم و پروتکل مناسب مرتفع گردد. در مجموع، یافته‌ها نشان می‌دهد که شبکه‌های مبتنی بر بلاک‌چین می‌توانند امنیت لایه دسترسی IoT را به طور چشمگیری تقویت کنند به طوری که دسترسی غیرمجاز و جعل هویت به مراتب دشوارتر از قبل شود.

ارتقای محرمانگی داده‌ها و حفظ حریم خصوصی

حریم خصوصی در IoT بیشتر ناظر بر محرمانگی (Confidentiality) داده‌های شخصی و کنترل مالکیت بر داده‌هاست. نگرانی اصلی این است که اطلاعات حساس جمع‌آوری‌شده توسط حسگرها (از وضعیت سلامتی تا رفتارهای روزمره کاربران) به دست افراد یا نهادهای غیرمجاز بیفتد یا بدون رضایت مالک مورد استفاده قرار گیرد. استفاده از بلاک‌چین در نگاه اول ممکن است با چالش حریم خصوصی همراه باشد زیرا بلاک‌چین شفاف است و تمام داده‌های ثبت‌شده (مگر اینکه رمز شوند) در دید همه اعضای شبکه قرار می‌گیرد. اما راهکارهای مختلفی برای رفع این نگرانی در تحقیقات ارائه شده است. معمول‌ترین راه، رمزنگاری داده‌های حساس قبل از ثبت در بلاک‌چین است. به این ترتیب، خود بلاک‌چین تنها حاوی داده‌های رمزنگاری‌شده یا هش داده‌هاست و چنانچه شخصی به داده نیاز داشته باشد، صرفاً در صورت داشتن کلید می‌تواند آن را رمزگشایی کند. این روش البته مبادله کلید امن بین فرستنده و گیرنده را می‌طلبد که خود می‌تواند با قرارداد هوشمند تسهیل شود.

عدم حضور سرور مرکزی در معماری بلاک‌چین-محور، خود به بهبود حریم خصوصی کمک می‌کند. چرا که بسیاری از موارد نقض حریم خصوصی در IoT امروزه به دلیل تجمع حجم بالایی از داده‌های کاربران در سرورهای ابری شرکت‌هاست که هدف هکرها قرار می‌گیرد یا حتی توسط شرکت بهره‌بردار نادرسر می‌شود. در رویکرد بلاک‌چین، هر کاربر می‌تواند داده‌های خود را به صورت رمزشده روی دفترکل توزیع‌شده قرار دهد و تنها به افراد یا سرویس‌های مشخصی اجازه رمزگشایی بدهد. به این مدل گاهی مالکیت داده توسط خود کاربر (self-sovereign data) نیز گفته می‌شود. مثال خانه هوشمند که قبلاً آورده شد را می‌توان تعمیم داد: معامله مستقیم بین دستگاه‌های IoT (مثلاً قفل درب هوشمند با تلفن همراه صاحبخانه) بدون عبور از سرور ثالث، هم امنیت را بالا می‌برد هم حریم خصوصی را حفظ می‌کند.

علاوه بر این، فناوری‌های پیشرفته‌تری نیز در برخی تحقیقات به کار رفته‌اند. برای نمونه، استفاده از اثبات‌های دانش صفر (Zero-Knowledge Proofs) یا رمزنگاری چندجانبه امن (MPC) روی بلاک‌چین می‌تواند امکان پردازش یا تأیید یک شرایط را بدون افشای داده خام میسر کند. تصور کنید در IoT سلامت، بخواهیم تأیید کنیم فشار خون ثبت‌شده یک بیمار در محدوده نرمال است یا خیر، بدون اینکه مقدار دقیق فشار خون (که حریم خصوصی بیمار است) برای کسی فاش شود. الگوریتم‌های رمزنگاری پیشرفته می‌توانند این امر را با اثبات روی زنجیره انجام دهند. البته این موارد هنوز در مرحله تحقیقاتی هستند و به پیاده‌سازی‌های عملی گسترده راه نیافته‌اند.

نتایج گزارش‌شده در منابع حاکی از بهبود نسبی حریم خصوصی با به‌کارگیری بلاک‌چین است. برای مثال، در مطالعه مروری ۲۰۲۳ (گوگو و همکاران) اشاره شده که نشت حریم خصوصی یکی از انگیزه‌های اصلی روی آوردن به بلاک‌چین در IoT بوده است و بلاک‌چین با حذف واسطه‌های غیرقابل اعتماد و فراهم کردن ابزارهای رمزنگاری قوی،

چهارمین کنفرانس بین المللی
مهندسی و فناوری اطلاعات

ریسک افشای اطلاعات خصوصی را کاهش می‌دهد. همچنین سولتان و همکاران (یکی از مراجعی که در یک مقاله فارسی توسط غفاری ۱۴۰۳ آورده شده) به صراحت IoT را از منظر مسائل حریم خصوصی بررسی کرده و بلاک‌چین را به عنوان یکی از راه‌حل‌های نویدبخش ذکر کرده است.

در عین حال، محدودیت‌های بلاک‌چین در حفظ حریم خصوصی را نباید نادیده گرفت. اگر طراحی سامانه درست انجام نشود، ممکن است حتی اثر معکوس داشته باشد؛ چون بلاک‌چین تمام تعاملات را ثبت و دائمی می‌کند. مثلاً تصور کنید دستگاه‌های یک کاربر همیشه تراکنش‌هایی را به آدرس بلاک‌چین او ارسال کنند، حتی اگر محتوای تراکنش رمز شده باشد، الگوی تراکنش‌ها می‌تواند اطلاعاتی درباره رفتار او افشا کند (تحلیل ترافیک). بنابراین برای کاربردهای با حساسیت حریم خصوصی بالا، احتمالاً ترکیب بلاک‌چین با شبکه‌های ناشناس‌ساز تراکنش (مثل شبکه تور یا الگوریتم‌های mixnet) یا استفاده از بلاک‌چین‌های ویژه حفظ حریم خصوصی (مانند زی‌کش یا مونرو که آدرس‌ها و مقادیر را مخفی می‌کنند) ضرورت یابد. این موضوع در پیشنهادات پژوهش حاضر نیز ذکر خواهد شد.

جمع‌بندی: بلاک‌چین از دو طریق اصلی به حفظ بهتر حریم خصوصی در IoT کمک می‌کند: اول با کاهش نیاز به اعتماد به واسطه‌های متمرکز (که ممکن است نقض حریم خصوصی کنند)؛ دوم با امکان‌پذیر کردن اعمال سیاست‌های رمزنگاری و ناشناس‌سازی بر روی یک زیرساخت توزیع‌شده. در عین حال، بهره‌گیری کامل از مزایای بلاک‌چین در این زمینه مستلزم طراحی دقیق (مثلاً عدم قرار دادن داده حساس به صورت رمز نشده روی زنجیره) و شاید استفاده ترکیبی از پروتکل‌های حفظ حریم خصوصی باشد. نتایج پژوهش‌های بررسی‌شده غالباً نشان می‌دهد که با بلاک‌چین می‌توان حریم خصوصی کاربران IoT را بهتر از معماری‌های سنتی صیانت کرد مشروط بر آن‌که چالش شفافیت ذاتی بلاک‌چین با تدابیر رمزنگاری مرتفع شود.

ایجاد اعتماد و کاهش وابستگی به نهادهای مرکزی

اعتماد (Trust) در سیستم‌های IoT به این معناست که ذینفعان مختلف (دستگاه‌ها، کاربران، سرویس‌ها) بتوانند بدون نیاز به شناسایی کامل و ارتباطات دوطرفه قبلی، به درستی عملکرد و صحت داده‌های یکدیگر تکیه کنند. در وضع موجود، اعتماد معمولاً از طریق نهادهای ثالث ایجاد می‌شود؛ برای مثال، سازنده دستگاه با به‌روزرسانی‌های نرم‌افزاری و گواهی‌های امنیتی اعتماد را ایجاد می‌کند، یا ارائه‌دهنده پلتفرم IoT نقش داور و میانجی را دارد. اما این مدل اعتماد متمرکز با افزایش مقیاس IoT دچار مشکل می‌شود؛ چرا که همه طرف‌ها حاضر به اعتماد به یک نهاد واحد نیستند یا در مواردی آن نهاد خود قابل اعتماد نیست.

بلاک‌چین از ابتدا برای ایجاد اعتماد بدون اعتماد به یک نهاد مرکزی طراحی شده است. این پارادوکس ظاهری در عمل از طریق ترکیبی از شفافیت، تغییرناپذیری و اجماع توزیع‌شده حاصل می‌شود که پیش‌تر شرح داده شد. بنابراین انتظار می‌رود افزودن بلاک‌چین به IoT بتواند سطح اعتماد را در اکوسیستم IoT بالا ببرد. شواهد متعددی این موضوع را تأیید می‌کنند. برای مثال، پژوهش لوکل و همکاران (۲۰۲۰) که در بخش پیشینه اشاره شد، هدف اصلی خود را ایجاد اعتماد در اکوسیستم IoT با استفاده از بلاک‌چین قرار داده بود. آن‌ها نشان دادند که با تعریف اصول طراحی مناسب (نظیر داده‌های مشترک مبتنی بر دفترکل، اجماع بر رویدادهای مهم و قراردادهای روشن میان طرف‌ها) می‌توان یک محیط IoT خلق کرد که حتی بین سازمان‌های مختلف نیز اعتماد برقرار باشد. در حوزه زنجیره

چهارمین کنفرانس بین المللی
مهندسی و فناوری اطلاعات

تأمین نیز بلاکچین موفق شده اعتماد بین شرکت‌های متعدد را (که هر یک ممکن است به دیگری اعتماد کامل نداشته باشد) ایجاد کند، به گونه‌ای که همگی به داده‌های ثبت‌شده درباره محموله‌ها اعتماد می‌کنند و نیاز کمتری به بازرسی‌های مستقل یا اسناد کاغذی حس می‌شود.

کاهش وابستگی به نهادهای مرکزی یکی از آثار جانبی مثبت بلاکچین در IoT است که در چند مطالعه مورد اشاره قرار گرفته. برای مثال، Lock et al. (2020) مطرح می‌کنند که با بکارگیری بلاکچین در برنامه‌های IoT، وابستگی به سرورهای ابر متمرکز کم شده و بسیاری از وظایف مدیریت داده و امنیت توسط شبکه بلاکچین انجام می‌شود. این عدم وابستگی نه تنها احتمال نقطه شکست منفرد را کاهش می‌دهد (که مبحث امنیتی است)، بلکه جنبه اعتماد را نیز پوشش می‌دهد: کاربران دیگر مجبور نیستند به یک شرکت مرکزی برای حفظ امنیت داده‌هایشان اعتماد کنند، بلکه این اعتماد به شکل توزیع‌شده و بر پایه شفافیت سیستماتیک ایجاد می‌شود. در واقع اعتماد از اعتماد به فرد/سازمان تبدیل به اعتماد به فناوری/پروتکل می‌شود.

البته اعتمادسازی بلاکچین نیز محدودیت‌هایی دارد. ذکر این نکته مهم است که بلاکچین اعتماد را به طور کامل حذف نمی‌کند بلکه آن را بازتوزیع می‌کند. مثلاً در یک بلاکچین خصوصی، اعتماد به همه اعتبارسنج‌های شبکه (هرچند متعدد باشند) لازم است. یا در یک بلاکچین عمومی مانند اتریوم، باید به مکانیزم‌های اجماع و اکوسیستم توسعه آن اعتماد داشت که از مسیر خود منحرف نشود. با این وجود، مدل اعتماد بلاکچین به مراتب کم‌ریسک‌تر و شفاف‌تر از مدل سنتی است و امکان تخلف یا خیانت را تا حد زیادی کاهش می‌دهد.

جمع‌بندی: حضور بلاکچین در معماری IoT به شکل ملموسی اعتماد میان اجزای ناهمگن و ناآشنا را افزایش می‌دهد. دستگاه‌ها می‌توانند به داده‌های دریافتی از دیگر دستگاه‌ها اعتماد کنند چون می‌دانند که این داده‌ها در یک ساختار توزیع‌شده تأیید شده و تغییرناپذیر ثبت شده‌اند. کاربران و سازمان‌ها نیز می‌توانند به فرآیندهای خودکار شبکه اعتماد کنند بدون اینکه مجبور باشند به یک شخص ثالث متکی باشند. بنابراین بلاکچین نقش یک منبع حقیقت (Source of Truth) مشترک را بازی می‌کند که همه به آن رجوع کرده و به آن اعتماد می‌کنند. این دقیقاً تحول بنیادینی است که انتظار می‌رود بلاکچین در اینترنت اشیا رقم بزند و بسیاری از موانع همکاری و یکپارچگی را در اکوسیستم‌های بزرگ مرتفع سازد.

هزینه‌ها، مقیاس‌پذیری و چالش‌های باقی‌مانده

برای تکمیل بحث، باید به جنبه‌های چالشی و محدودیت‌های به‌کارگیری بلاکچین در IoT نیز بپردازیم؛ چرا که یک فناوری هرچند مزایای امنیتی داشته باشد، در صورت عدم تطابق با محدودیت‌های فنی IoT ممکن است عملاً قابل استفاده نباشد. مهم‌ترین چالش‌هایی که در منابع مختلف به آن اشاره شده عبارت‌اند از: مقیاس‌پذیری، توان و انرژی، تأخیر (Latency) و سازگاری با دستگاه‌های محدود.

۱. مقیاس‌پذیری: شبکه‌های بلاکچین فعلی (مثل بیت‌کوین و اتریوم) از نظر تعداد تراکنش در ثانیه و تأخیر تأیید، نمی‌توانند بار میلیون‌ها دستگاه IoT را تحمل کنند. بسیاری از دستگاه‌های IoT به شکل پیوسته داده تولید می‌کنند که اگر همه آن‌ها بخواهد وارد بلاکچین شود، حجم عظیمی خواهد بود. لذا پژوهشگران در پی راهکارهای مقیاس‌پذیری هستند. استفاده از شاردینگ (تقسیم شبکه بلاکچین به بخش‌های کوچکتر که هر کدام بخشی از تراکنش‌ها را پردازش می‌کنند) یکی از پیشنهادات است. همچنین بهره‌گیری از معماری‌های مبتنی بر DAG (گراف جهت‌دار) مانند IOTA پیشنهاد شده که ذاتاً

چهارمین کنفرانس بین المللی
مهندسی و فناوری اطلاعات

برای IoT طراحی شده و با افزایش تعداد گره‌ها، کارایی آن افت نمی‌کند. در منابع دیده می‌شود که هنوز تحقیقات کافی در زمینه الگوریتم‌های اجماع مقیاس پذیر برای IoT صورت نگرفته و این یک فرصت پژوهشی است.

۲. مصرف توان و انرژی: بسیاری از دستگاه‌های IoT با باتری کار می‌کنند و باید مصرف انرژی بسیار بهینه‌ای داشته باشند. پروتکل‌های بلاک‌چین اگر نیاز به ارتباط و پردازش مداوم داشته باشند، ممکن است باتری دستگاه را به سرعت خالی کنند. به ویژه الگوریتم‌هایی مانند PoW به هیچ عنوان برای IoT مناسب نیستند. در مقابل، اثبات سهام (PoS) یا اثبات اعتبار مفید (PoU) و سایر روش‌های کم‌مصرف‌تر پیشنهاد می‌شوند. برای مثال، یک ایده این است که خود دستگاه‌های IoT نقش ماینر را نداشته باشند، بلکه صرفاً تراکنش‌ها را امضا و ارسال کنند و تعداد محدودی گره قدرتمندتر (مثلاً دروازه‌ها یا سرورها) وظیفه اجماع را انجام دهند. این هنوز یک سیستم غیرمتمرکز است اما لزوماً هر سنسور ساده درگیر اجماع نمی‌شود. همچنین تحقیقات به سمت پروتکل‌های اجماع سبک که با چند پیام ساده به توافق می‌رسند در حال پیشرفت است.

۳. تاخیر: برخی کاربردهای IoT (مثل کنترل صنعتی یا سیستم‌های ایمنی) تحمل تاخیر حتی در حد چند ثانیه را ندارند. بلاک‌چین‌های فعلی معمولاً تاخیرهایی در حد ثانیه یا دقیقه دارند (مثلاً میانگین زمان بلاک در اتریوم ~ ۱۵ ثانیه است). برای رفع این مشکل، پیشنهاد شده از الگوریتم‌های اجماع سریع‌نهایی‌شونده استفاده شود. الگوریتم‌های BFT (تحمل خطای بیزانس) کلاسیک مانند PBFT، کاندیداهای خوبی هستند چون می‌توانند در کمتر از ثانیه به اجماع برسند اما معمولاً در شبکه‌های کوچک کاربرد دارند. ترکیب BFT با شبکه‌های بزرگ هنوز چالش برانگیز است. الگوریتم RAFT نیز برای برخی سناریوهای IoT مناسب دیده شده چرا که ساختاری سلسله‌مراتبی دارد و می‌تواند کنترل‌شده تاخیر را پایین نگه دارد. پژوهشگران توصیه می‌کنند اجماع‌های بهینه‌شده برای تاخیر برای IoT مورد بررسی قرار گیرد.

۴. حملات و محدودیت‌های خارج از بلاک‌چین: باید توجه داشت که بلاک‌چین نمی‌تواند همه انواع حملات را حل کند. به عنوان مثال، حملات فیزیکی به دستگاه IoT (مثل دزدیدن یا خراب کردن آن) یا نفوذ بدافزاری به دستگاه را بلاک‌چین مستقیماً جلوگیری نمی‌کند. همچنین حملات لایه شبکه مانند مسدودسازی سیگنال رادیویی (jamming) یا حملات سیلابی علیه پهنای باند شبکه همچنان در حضور بلاک‌چین ممکن است. بلاک‌چین در لایه بالاتر عمل می‌کند و تضمین می‌دهد که اگر ارتباطی برقرار شد، امن است و داده‌ها تغییر نمی‌کنند؛ اما مثلاً اگر یک سنسور به کلی از شبکه جدا شد، بلاک‌چین نمی‌تواند آن را نجات دهد. بنابراین، برای امنیت جامع IoT، بلاک‌چین باید در کنار تدابیر دیگر (نظیر سخت‌سازی دستگاه‌ها، روش‌های کشف نفوذ، شبکه‌های مقاوم) به کار گرفته شود.

در جمع‌بندی این بخش، می‌توان گفت یافته‌های این پژوهش تأیید می‌کند که بلاک‌چین علی‌رغم مزایای بسیار، نوشاروی همه دردهای امنیتی IoT نیست. اما نقاط ضعف و چالش‌های مشخصی وجود دارد که با تحقیق و توسعه بیشتر می‌توان آن‌ها را تخفیف داد. برخی از این مسیرهای بهبود و پیشنهادات در بخش بعدی ارائه خواهد شد. نکته خوشبینانه این است که بسیاری از چالش‌های ذکر شده، راه‌حل‌های بالقوه قابل پیاده‌سازی دارند (مثلاً الگوریتم‌های اجماع سبک، ساختارهای زنجیره‌ای جدید یا ادغام با تکنیک‌های رمزنگاری). لذا مسیر آینده پژوهش در این حوزه روشن بوده و انتظار می‌رود با پیشرفت در این زمینه‌ها، بلاک‌چین بتواند نقش خود را به طور کامل‌تر و موثرتری در اکوسیستم IoT ایفا کند.

نتیجه‌گیری

با توجه به تحلیل‌های انجام‌شده، می‌توان نتیجه گرفت که فناوری بلاک‌چین یک راهکار انقلابی و تحول‌آفرین برای ارتقای امنیت و حریم خصوصی در اینترنت اشیا است. در ابتدای مقاله دیدیم که IoT به دلیل گستردگی و ذات غیرمتمرکز خود با چالش‌های امنیتی متعددی روبروست که روش‌های سنتی به سختی از پس آن برمی‌آیند. این چالش‌ها شامل احراز هویت و کنترل دسترسی، تمامیت و محرمانگی داده‌ها، حفظ حریم خصوصی کاربران و ایجاد اعتماد میان اجزای ناشناس شبکه بود.

چهارمین کنفرانس بین المللی
مهندسی و فناوری اطلاعات

مطالعات پیشین تأیید کردند که تداوم وضعیت کنونی می‌تواند مانعی در گسترش IoT باشد، چرا که نگرانی‌های امنیتی و اعتماد، پذیرش عمومی این فناوری را کند می‌کند.

در این پژوهش، بلاک‌چین به عنوان پاسخی جامع به این نگرانی‌ها مورد بررسی قرار گرفت. ویژگی‌های بنیادین بلاک‌چین یعنی عدم تمرکز، شفافیت، تغییرناپذیری و اجماع توزیع‌شده دقیقاً در نقطه مقابل ضعف‌های معماری‌های متمرکز IoT قرار دارند و بدین ترتیب یک هم‌افزایی مثبت بین این دو فناوری به وجود می‌آورند. نتایج بررسی منابع و تحلیل مفهومی نشان داد که ادغام بلاک‌چین در لایه‌های مختلف IoT می‌تواند:

۱- تمامیت و صحت داده‌های IoT را تضمین کند و مانع دستکاری یا جعل اطلاعات شود
۲- احراز هویت و کنترل دسترسی را به صورت توزیع‌شده و امن بهبود بخشد و از ورود دستگاه‌ها/افراد غیرمجاز به شبکه جلوگیری کند

۳- محرمانگی داده‌ها و حریم خصوصی را با حذف واسطه‌های غیرضروری و استفاده از رمزنگاری مناسب حفظ نماید

۴- اعتماد بین بازیگران مختلف اکوسیستم IoT را افزایش داده و نیاز به اتکا به نهادهای مرکزی را کاهش دهد. در کنار این مزایا، چالش‌ها و محدودیت‌هایی نیز شناسایی شد – مانند مسائل مقیاس‌پذیری و سربار – که قابل حل هستند و نباید مانع به‌کارگیری اصولی بلاک‌چین شوند.

به بیان دیگر، فرضیه پژوهش مبنی بر نقش انقلابی بلاک‌چین در بهبود امنیت و حریم خصوصی IoT مورد تأیید قرار گرفت. بلاک‌چین می‌تواند پارادایم امنیتی حاکم بر IoT را از مدل اعتماد متمرکز به مدل اعتماد توزیع‌شده تغییر دهد و بدین ترتیب زیرساختی فراهم آورد که در برابر طیف وسیعی از تهدیدات مقاوم‌تر است. البته، این به معنای حل آنی تمام مشکلات نیست؛ بلکه بلاک‌چین را باید به عنوان یکی از اجزای اصلی راه‌حل در کنار سایر تمهیدات امنیتی به کار گرفت. به عنوان مثال، تجهیز دستگاه‌های IoT به ماژول‌های رمزنگاری، به‌روزرسانی منظم نرم‌افزار دستگاه‌ها، آموزش کاربران، و نظارت بر شبکه نیز همچنان ضروری خواهد بود. اما بلاک‌چین بستر پایه‌ای را مهیا می‌کند که تمامی این اقدامات بر روی آن اثربخشی بسیار بیشتری خواهند داشت.

در پایان، این تحقیق بینشی جامع نسبت به وضعیت فعلی و آتی بلاک‌چین در اینترنت اشیا ارائه داد. سازمان‌ها و صنایع می‌توانند با بهره‌گیری از یافته‌های این پژوهش، جهت‌گیری استراتژیک خود را به سمت استفاده از بلاک‌چین در پروژه‌های IoT سوق دهند تا هم امنیت را ارتقا دهند و هم اعتماد مشتریان و کاربران را جلب نمایند. از منظر آکادمیک نیز راه برای تحقیقات پیشرفته‌تر – چنان‌که در ادامه پیشنهاد خواهد شد – هموار است.

پیشنهادهای

بر اساس آموخته‌های این پژوهش، در این بخش چند پیشنهاد عملی و پژوهشی برای آینده ارائه می‌شود تا به پیاده‌سازی بهتر راهکارهای بلاک‌چینی در حوزه IoT و رفع چالش‌های باقیمانده کمک کند:

بهینه‌سازی تأخیر برای کاربردهای بلادرنگ: پیشنهاد می‌شود الگوهای ترکیبی آنی طراحی شوند که در آن‌ها تراکنش‌های حیاتی (مثلاً هشدارهای پزشکی یا صنعتی) خارج از زنجیره اصلی ولی با تضمین‌های بلاک‌چینی پردازش شوند (برای مثال کانال‌های وضعیت یا زنجیره‌های جانبی سریع). همچنین بررسی پروتکل‌هایی مانند Raft یا IBFT در بستر IoT واقعی، می‌تواند راهگشا باشد که چه میزان کاهش تأخیر حاصل می‌شود.

ادغام روش‌های حفظ حریم خصوصی پیشرفته: به جامعه پژوهشی توصیه می‌شود برای حل نگرانی شفافیت بلاک‌چین، از فناوری‌هایی نظیر اثبات دانش صفر، امضای حلقوی، CoinJoin و سایر تکنیک‌های حفظ حریم خصوصی در طراحی

چهارمین کنفرانس بین المللی
مهندسی و فناوری اطلاعات

بلاک چین های خاص IoT بهره گیرند. چنین رویکردی امکان اشتراک گذاری داده های حساس را بدون افشای محتوای آنها فراهم می کند و موانع پذیرش را در حوزه هایی مانند سلامت الکترونیک برطرف می سازد. طراحی معماری های ترکیبی Cloud-Blockchain-IoT در عمل، احتمالاً بهره گیری ترکیبی از رایانش ابری و بلاک چین بهترین نتایج را دهد. پیشنهاد می شود مدل هایی توسعه یابد که در آن ابر نقش ذخیره سازی و پردازش سنگین را بر عهده دارد اما بلاک چین کنترل امنیت و اعتماد را مدیریت می کند. این معماری ها باید به گونه ای باشند که اگر بخش ابری دچار نفوذ شد، بلاک چین کماکان جلوی آسیب به تمامیت و اعتماد سیستم را بگیرد. استاندارد سازی و چارچوب های قانونی: برای تسریع پذیرش صنعتی، نیاز به تدوین استانداردهای باز برای یکپارچه سازی IoT و بلاک چین است. سازمان های استاندارد (IEEE, ISO) و ... و در داخل کشور نهادهایی چون سازمان فناوری اطلاعات (می توانند پروتکل های مرجع در این زمینه منتشر کنند. همچنین از دید حاکمیتی، قوانین و چارچوب هایی باید تعریف شود که استفاده از بلاک چین در حوزه هایی مانند داده های شخصی، با حفظ ملاحظات حقوقی (مثل حریم خصوصی، مالکیت داده) صورت گیرد.

انجام پروژه های پایلوت در مقیاس کوچک: برای ارزیابی عملی مزایا و معایب، پیشنهاد می شود صنایع مختلف (مثلاً شرکت های برق، لجستیک، بهداشت) پروژه های آزمایشی کوچکی راه اندازی کنند که در آنها بلاک چین در کنار سامانه IoT واقعی به کار گرفته شده است. اندازه گیری معیارهایی چون کاهش حوادث امنیتی، بهبود زمان تشخیص ایراد، افزایش رضایت کاربران و ... در این پایلوت ها می تواند مطالعه موردی ارزشمندی ارائه کند و در صورت موفقیت، راه را برای گسترش هموار نماید. آموزش نیروی انسانی و افزایش آگاهی: نهایتاً پیشنهاد می شود برنامه های آموزشی (در دانشگاه ها و صنایع) برای آشنایی با مفاهیم بلاک چین و کاربردهای آن در IoT تدوین گردد. تربیت متخصصانی که در هر دو حوزه دانش کافی داشته باشند، تضمین می کند که در سال های آتی بتوان پروژه های پیچیده ادغام این دو فناوری را به خوبی مدیریت و اجرا کرد. با اجرای پیشنهادات فوق، انتظار می رود ظرف چند سال آینده شاهد بالغ شدن اکوسیستم ترکیبی Blockchain-IoT باشیم؛ به طوری که امنیت و اعتماد به عنوان قابلیت های ذاتی در اینترنت اشیا مطرح شده و کاربران بدون دغدغه های کنونی از مزایای تجهیزات هوشمند بهره مند شوند. استمرار پژوهش های بین رشته ای در این زمینه قطعاً دستاوردهای جدیدی به همراه خواهد داشت و نقش انقلاب آفرین بلاک چین در دنیای IoT را بیش از پیش نمایان خواهد ساخت.

- منابع :

۱. حمداله محمدی، محمد ملکی نیا. (1401) حفظ حریم خصوصی در اینترنت اشیا با استفاده از بلاک چین. مجموعه مقالات سیزدهمین کنفرانس بین المللی نوآوری و تحقیق در علوم مهندسی.
۲. رضا غفاری. (1403) ارتقای امنیت و حریم خصوصی در اینترنت اشیا براساس تکنولوژی بلاک چین. فصلنامه Arman Process، دوره ۵، شماره ۴، صفحه ۱۳-۲۲.
۳. چرا بلاک چین آینده امنیت و حریم خصوصی داده ها است؟ (1400).
۴. بلاک چین در اینترنت اشیا (IoT)؛ امنیت و ارتباطات غیرمتمرکز. (1401).

5. L. Da Xu, Y. Lu, L. Li (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(14), 10452–10473.
6. M. A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian (2021). A survey on the adoption of blockchain in IoT: Challenges and solutions. Blockchain: Research and Applications, 2, 100006.
7. A. Al Sadawi, M. S. Hassan, M. Ndiaye (2021). A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. IEEE Access, 9, 54478–54497.

8. B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, A. H. Gandomi (2020). Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal*, 8(2), 881–888.
9. V. Gugueoth, S. Safavat, S. Shetty, D. Rawat (2023). A review of IoT security and privacy using decentralized blockchain techniques. *Computer Science Review*, 50, 100585, 1–16.
10. S. Almarri, A. Aljughaiman (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. *Sustainability*, 16(23), 10177.
11. A. Deep, A. Perrusquía, L. Aljaburi, S. Al-Rubaye, W. Guo (2024). A Novel Distributed Authentication of Blockchain Technology Integration in IoT Services. *IEEE Access*, 12, 9550–9562.
12. J. Lee, M. Kim, K. Park, et al. (2023). Blockchain-based data access control and key agreement system in IoT environment. *Sensors*, 23(11), 5173.
13. J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, N. Harth (2020). Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications. *IEEE Transactions on Engineering Management*, 67(4), 1256–1270.
14. S. Sun, R. Du, S. Chen, W. Li (2021). Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain. *IEEE Access*, 9, 36868–36878.
15. A. K. Al Hwaitat, M. A. Almaiah, A. Ali, et al. (2023). A new blockchain-based authentication framework for secure IoT networks. *Electronics*, 12(17), 3618.
16. E. A. Shamar, A. T. Zahary, A. A. Al-Shargabi (2020). A survey of IoT security: threats, challenges and solutions.
17. M. Banerjee, J. Lee, K.-K. R. Choo (2018). A blockchain future for internet-of-things security: a position paper. *Digital Communications and Networks*, 4(3), 149–160.
18. H. B. Hassen, N. Ayari, B. Hamdi (2020). A home health IoT system applied to congestive heart failure.
19. S. Tuli, N. Basumatary, S. S. Gill, M. Kahani, R. Buyya (2019). HealthFog: Blockchain-based deep learning approach for privacy-preserving healthcare in smart cities.
20. A. Sultan, M. A. Mushtaq, M. Abubakar (2020). IoT security issues via blockchain: a systematic review.