ارائه یک مدل برای امنیت سایبری شرکت‌ها با استفاده از بلاک‌چین

یاشار ابری[1]، عباس قدیم پور شبلو[1]

[1]دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران، ایران
{yasharabri,ghadimpourshablo}@ut.ac.ir

چکیده

این مقاله به ارائه یک مدل هوشمند برای ارتقا امنیت سایبری شرکت‌ها با استفاده از تکنولوژی بلاک‌چین و یادگیری ماشین می‌پردازد. ابتدا مفهوم امنیت سایبری و اهمیت آن برای حفاظت از داده‌های شرکت‌ها و جلوگیری از حملات سایبری موردبحث قرار می‌گیرد. سپس به بررسی نقش یادگیری ماشین در بهبود امنیت سایبری اینترنت اشیا پرداخته می‌شود و تکنیک‌های یادگیری ماشینی برای کاهش حملات سایبری مطرح می‌شود. بخش بعد به معرفی بلاک‌چین به‌عنوان یک تکنولوژی نوظهور در امنیت سایبری می‌پردازد که از ویژگی‌های شفافیت و تغیر ناپذیری برای جلوگیری از دستکاری داده‌ها بهره می‌برد. در ادامه مزایا و معایب بلاک‌چین به‌عنوان یک تکنولوژی غیرمتمرکز و نقش آن در تأمین امنیت شبکه‌های اینترنت اشیا توضیح داده می‌شود. در انتها معماری پیشنهادی این پژوهش برای مدیریت جریان داده‌های IoT با استفاده از بلاک‌چین و پردازش ابری معرفی می‌گردد. این معماری از دولایه بلاک‌چین اولیه و ثانویه برای پردازش و ذخیره‌سازی داده‌ها استفاده می‌کند که با فایروال و سیستم‌های تشخیص نفوذ ترکیب شده و داده‌ها با پردازش در محیط ابری، از طریق قراردادهای هوشمند تأیید می‌شوند. در نتایج مزایا و چالش‌های عملکرد اجزای ساختاری مدل پیشنهادی بیان شده و پیشنهادهایی برای آینده امنیت سایبری بلاک‌چینی برای شرکت‌ها در پایان ذکر شده است.

کلمات کلیدی: امنیت سایبری، بلاک‌چین، حملات سایبری، اینترنت اشیا، یاد گیری ماشین، هوش مصنوعی، سیستم تشخیص نفوذ.

۱ مقدمه

با افزایش اخیر وابستگی جوامع به فناوری‌های ابری به همراه نیاز انسان‌ها به ارتباط و اشتراک گذاری سایبری داده‌ها از طریق شبکه‌های دیجیتالی، نیاز به شبکه اینترنت و دستگاه‌های اینترنت اشیا (IoT)[1] از جمله

[1]Internet of Things

گوشی‌ها و کامپیوترهای هوشمند، لوازم صنعتی و خانگی الکترونیکی ضروری است و در عملکرد تجارت به صورت ویژه مطرح هستند. تبادلات انواع داده‌های تراکنشی و اجتماعی باعث پیشرفت سریع بازارهای تجاری شده و برای تسهیل روندهای عرضه، به دنبال توسعه سریع تکنولوژی‌های نوظهور در فضای سایبر[۲] هستند. در محیط خانگی نیز اشتراک‌گذاری رسانه‌های دیجیتال (که بیشتر شامل تصویر، ویدئو، صدا و اسناد است) از طریق خدمات پیام‌رسانی سایبری برای تکنولوژی اطلاعات، آموزش، ورزش، بهداشت و علوم اجتماعی انجام می‌شود، به لحاظ فیزیکی با کمک دستگاه‌های IoT صورت می‌پذیرد که قادرند انتقال داده‌ها را به صورت لحظه‌ای در سراسر جهان از طریق اینترنت همه‌چیز و ابر[۳] به صورت مؤثر و کارآمدی انجام دهند.

در زمینه صنعت نیز شبکه‌های اینترنت اشیا، رابط‌های برنامه‌نویسی کاربردی و حسگرهای هوشمند موجب شده‌اند که کار از راه دور در عرصه الکترونیک فراهم شود. به عنوان مثال مشاهده اسناد، تراکنش‌ها، اطلاعیه‌ها و دسترسی‌هایی که یک شخص به صورت حضوری در محل کار شرکت می‌توانست انجام دهد با ورود به یک کنترل پنل مجازی قابل استفاده است که این مورد می‌تواند موجب تسهیل فعالیت و ارتباطات تجاری شود. اما در طرف دیگر فعالیت‌های مجرمانه‌ای که پتانسیل تخریب گسترده دارند، بر حفاظت و محرمانگی داده‌های اشتراک‌گذاری شده شرکت‌ها تاثیر می‌گذارند و منجر به آسیب، بروز مشکلات قانونی و اخلاقی با زیان‌های مالی قابل توجه می‌شوند. به عنوان نمونه حملات محروم‌سازی از سرویس (DDoS)[۴] می‌توانند معماری‌های داده، شبکه‌ها و زیرساخت‌های خدماتی کسب‌وکارها را در مقیاس وسیعی مختل کنند. به همین جهت با توجه به افزایش وابستگی جوامع به تبادل و پردازش اطلاعات شناسایی شخصی از طریق اینترنت، اعتماد به سیستم‌های تجاری معتبر به مسئله اصلی تبدیل شده است. برای مثال هنگامی که یک کاربر تصمیم می‌گیرد برای یک خرید آنلاین اطلاعات شبکه اجتماعی، ایمیل، موارد شخصی و محرمانه مانند رمز را به اشتراک بگذارد، بایستی ضمن اطلاع از ماهیت و قصد جرایم سایبری به سیستم پرداختی مورد نظر اعتماد داشته باشد. در سمت دیگر، کسب‌وکارها، شرکت‌ها و موسسات دانشگاهی برای خدمت‌رسانی جهانی از تکنولوژی‌های ترکیبی هوش مصنوعی، داده‌های بزرگ[۵] و بلاک‌چین برای اعتبارسنجی و تایید داده‌ها استفاده می‌کنند تا بتوانند جرایم و حملات سایبری را به طور قابل توجهی کاهش دهند. یکی از روش‌ها قرداد هوشمندی است که در تهیه و اخذ رضایت یک سند قانونی یا گواهی دیجیتال استفاده می‌شود که روشی مبتنی بر شواهد[۶] و شفاف برای ارزش قانونی و افزایش اعتبار یک تراکنش مالی ارائه می‌کند. به عنوان یکی از وظایف بلاک‌چین، قرارداد هوشمند اعتبارسنجی، اجرا و سپس از طریق شبکه همتا به همتا به عنوان یک تکنولوژی دفتر کل توزیع‌شده به اشتراک گذاشته می‌شود تا شفافیت[۷] و پاسخگویی را برای طرفین تجاری فراهم کند. در استفاده از عناصر امنیت سایبری، این ملزومات فنی به مدیریت موثر عملیات سخت‌افزاری، رابط‌های فیزیکی، نرم افزاری و توسعه تصمیمات داخلی اینترنت اشیا کمک می کند. استانداردهای پروتکل‌های ارتباطی شبکه،

[2] Cyber space
[3] cloud
[4] Distributed Denial of Service
[5] big data
[6] evidence-based method
[7] transparency

کنترل دسترسی به داده‌ها، رمزنگاری و آموزش کارکنان به ارتباطات مطمئن‌تر از لحاظ امنیت سایبری کمک می‌کند و حملات ارتباطی شبکه در حضور اشخاص خرابکار ثالث را به حداقل می‌رساند [۴].

با این حال برای بهره‌برداری و صحت‌سنجی ارزش داده‌های با حجم و تنوع زیاد، مفاهیمی مانند داده‌های بزرگ، هوش مصنوعی، یادگیری ماشینی[۸]، الگوریتم‌ها و تکنیک‌های تحلیلی مورد استفاده قرار می‌گیرند تا بتوانند پردازش حجم عظیمی از داده‌های عمومی، خصوصی و حساس شبکه‌های دیجیتال را انجام دهند. اما این امر به طور فزاینده‌ای خطر نفوذ داده‌های اشتباه، ویروس‌ها و حملات مخرب را افزایش می‌دهد و به همین جهت حفاظت از سیستم‌ها و داده‌ها در برابر اختلالات و تخریب‌ها دارای اهمیت است [۶]. به عبارت دیگر استفاده از این تکنولوژی‌ها در پردازش داده‌های عمومی، خصوصی و همچنین تاریخچه اقدامات کاربران ممکن است باعث ایجاد و آشکار شدن چالش‌ها و آسیب‌پذیری‌هایی شود که می‌تواند کاربران یا گروها را بیشتر در معرض حملات سایبری قرار دهد. برای پیشگیری از این موضوع، استفاده از هوش مصنوعی و یادگیری ماشینی می‌تواند به افزایش استفاده از این فناوری برای ایمن سازی و حفاظت از داده‌ها کمک کند [۷]. شبکه‌های مولد تخاصمی که اخیرا در بحث امنیت سایبری بیشتر مطرح می‌شوند [۲] می‌توانند در شناسایی و تشخیص حملات سایبری و آموزش بهتر نقش مهمی ایفا کنند [۱].

سیستم‌های بلاک‌چین و وظایف و روش‌های آن‌ها از مفاهیمی مانند ارزهای رمزنگاری شده (مانند تتر، اتریوم و بیت‌کوین) به عنوان جایگزینی برای ارزهای بین‌المللی، پروتکل‌های اجماع نماینده، امضاهای ناشناس، ذخیره‌سازی خارج از زنجیره و اثبات‌های بدون دانش تعاملی استفاده می‌کنند. این موارد زمانی که با حسابرسی‌های داخلی شرکت‌ها، اجرای دستورالعمل‌ها، ارائه مراقبت های ایمنی و عملکرد خدمات امنیتی برای انجام فعالیت‌های قانونی و داخلی همراه باشد، اعتبار ناشناس بودن و شفافیت را ارائه می‌کند. این سیستم از دید طراحی نیاز به اعتماد ندارد و وعده انجام تراکنش‌های عادلانه و شفاف را می‌دهد.

بر اساس موارد فوق، این پژوهش تلاش می‌کند یک چارچوب هوشمند را پیشنهاد دهد که به شناسایی و تشخیص بسته‌های داده شبکه‌ای که ممکن است خطرساز باشد کمک می‌کند. بلاک‌چین و قرارداد هوشمند به عنوان حامل داده‌ها و برای ارزیابی، اعتبارسنجی و آزمایش با پروتکل‌های کنترلی از پیش تعیین‌شده در نظر گرفته می‌شود. برای به حداقل رساندن دخالت انسانی، یک رویکرد خودکار هوشمند در جمع‌آوری داده‌های شبکه‌ای در فواصل زمانی از پیش تعیین‌شده به کار می‌رود. در نهایت داده‌های رویدادی بررسی و ارزیابی می‌شوند و تحلیل نتایج ارائه می‌شود.

۲ امنیت سایبری برای شرکت‌ها

شرکت‌های مختلفی در جهان، از جمله شرکت‌های استارتاپی ایران که در زمینه سفارش آنلاین خدمات یا محصولات فعالیت می‌کنند، با افزایش تهدیدات در سال‌های اخیر در تعریف و درک امنیت سایبری با چالش‌هایی مواجه شده‌اند. کمیسیون اروپا حداقل معیارها را برای هر شرکتی که کمتر از ۲۵۰ نفر استخدام می‌کند تعیین کرده است [۸]. این چالش‌ها در شرکت‌ها هم عملیاتی و هم تجاری هستند و به استفاده

[8] Machine Learning

از مکانیزم‌های تشخیص نفوذ[9] همراه با تکنیک‌های هوش مصنوعی و یادگیری ماشینی در حفاظت از داده‌هایشان تاکید دارند. برای شرکت‌ها این یک اولویت شده است که بتوانند روش‌های نفوذ، تشخیص و پیشگیری را جهت تحقق امنیت و ایمن نگهداشتن داده‌ها که با اینترنت و اشیا واقعی ادغام شده‌اند را بشناسند. همچنین درک اینکه چگونه تکنیک‌های یادگیری ماشین و هوش مصنوعی می‌توانند به ایمن کردن و دفاع در برابر حملات روز صفر (که حملات پیش‌بینی نشده هستند) کمک کنند اهمیت یافته است.

در سال ۲۰۲۱ Rawindaran و همکاران [۴] یک سناریوی تجربی ارائه دادند که در آن مدل‌های تشخیص و جلوگیری از نفوذ مقایسه شده و دیدگاه‌های شرکت‌ها نیز مورد بررسی قرار گرفته است. این مطالعه به بررسی رویکردهای مختلف در شناسایی روش‌ها و دستگاه‌هایی که می‌توانند در تشخیص و محافظت در برابر هرگونه نفوذ به شبکه می‌پردازد. در این مقاله همچنین به درک تلاش‌ها برای محافظت از داده‌ها و اینکه چگونه تصمیمات و رویه‌های دولتی اتحادیه اروپا می‌تواند در این فرایند کمک کند را مورد بررسی قرار داده است [۱۰]. چرا که اتحادیه اروپا نه تنها شرکت‌های مستقر در اروپا، بلکه شرکت‌های کشورهای دیگر مانند شرکت‌های آمریکایی که خواستار ارائه محصولات و خدمات در این قاره هستند را مجاب به پذیرش قوانینی می‌کند که به دنبال حفظ حریم خصوصی، حمایت از مصرف کننده یا حفظ محیط زیست و یا شکستن بازارهای انحصاری می‌کند. درست است که برخی از قوانین اهداف دیگری دنبال می‌کنند ولی در عمل بخش‌هایی دارند که می‌توانند برای امنیت سایبری هم مفید واقع شوند.

۱.۲ نقش امنیت سایبری در مقابل حملات به شرکت‌ها

Rawindaran و همکاران [۴] همچنین تاثیر سطح تهدیدات حملات مختلف مانند باج‌افزار، فیشینگ، بد افزار و مهندسی اجتماعی را با دستگاه‌های متن‌باز و نیز سیستم‌های تشخیص نفوذ شبکه (NIDS)[10] تجاری مقایسه کردند و متوجه شدند اگرچه سیستم‌های متن باز به صورت رایگان در دسترس هستند اما برای پیاده‌سازی و تعریف قوانین به عنوان یک راهکار تجاری نیاز به سطح خاصی از تخصص دارند. در حالی که سیستم تجاری مطرح و جهت‌دهنده بازار به دلیل تخصص فنی و جایگاه خود قادر به ادغام با این سیستم‌های متن باز و استفاده از آن‌ها به نفع خود است. به عبارت دیگر علاوه بر امکانات تجاری قادر به پوشش امکانات آن‌ها نیز هست.

رویکردهای یادگیری ماشینی مانند مدل‌های مبتنی بر امضا و مدل‌های مبتنی بر قوانین ناهنجاری برای مقابله با حملات در امنیت سایبری استفاده می‌شود [۹]. مدل‌های تشخیص مبتنی بر امضا[11] فقط قادر به شناسایی حملاتی بودند که از قبل شناخته شده بودند، در حالی که سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری[12] امکان شناسایی حملات ناشناخته را نیز دارند [۱۱]. سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری امکان شناسایی حملاتی را فراهم می‌کنند که امضای آنها در داده‌های آموزشی یا فایل‌های قوانین

[9] Intrusion Detection
[10] Network Intrusion Detection System
[11] signature based detection
[12] Anomaly-based intrusion detection system

وجود نداشته است و به همین جهت برای حملات روز صفر نیز مناسب هستند. اما در حال حاضر هزینه‌های اجرا و قدرت پردازشی مورد نیاز برای سیستم‌های مبتنی بر ناهنجاری بسیار بالاست و به همین دلیل پیاده‌سازی آن‌ها در شرکت‌های تجاری متوسط امکان‌پذیر به نظر نمی‌رسد. اما در دوران کنونی تولیدکنندگان مختلفی به دنبال ساخت پردازنده‌های پیشرفته‌تر برای هوش مصنوعی هستند و در صورتی که تعداد زیادی از آن‌ها با قیمت پایین‌تری به بازار عرضه شود، در زمینه امنیت سایبری نیز شرکت‌های بیشتری قادر به راه‌اندازی بخش امنیت سایبری مبتنی بر هوش مصنوعی خواهند بود.

۲.۲ یادگیری ماشین و تأثیر آن بر امنیت سایبری اینترنت اشیا

با گسترش امکانات تکنولوژی اطلاعات، تکنولوژی دیجیتال هم به رشد ادامه داده و دستگاه‌های بیشتری به اینترنت متصل شدند به طوری که دسترسی آزادانه به داده‌های بسیاری فراهم است که خود امکان انجام فعالیت‌های بیشتری را فراهم می‌کند. فعالیت‌ها خودشان می‌توانند به پیش‌بینی نتایج کمک کنند [۵]. بنابراین الگوریتم‌های ریاضی یادگیری ماشینی مختلفی برای استفاده در طبقه‌بندی داده‌ها مانند درخت‌های تصمیم‌گیری[۱۳] و شبکه‌های عصبی[۱۴] به کار گرفته می‌شوند. این الگوریتم‌ها با پردازش و مدیریت داده‌ها می‌توانند نتیجه و پیش‌بینی موردنیاز برای کمک به رشد اقتصادی در جامعه‌های پیشرفته را نشان دهند. و البته بحث‌هایی درباره استفاده غیراخلاقی و جاه‌طلبانه از این داده‌های آماری مطرح بوده است. قابلیت‌های یادگیری ماشینی فراتر از تسلط بر سرگرمی‌های انسان شده‌اند و در کارهای روزمره و رویدادها نفوذ کرده‌اند که در کنار مزیت‌هایش می‌تواند زنگ خطری برای جوامع بشری نیز باشد.

۳.۲ یادگیری ماشینی برای کاهش حملات سایبری

یادگیری ماشینی شامل سه دسته یادگیری نظارت شده، یادگیری بدون نظارت و یادگیری تقویتی است که می‌تواند در شناسایی فعالیت‌های جعلی یا جرایم سایبری، پیام‌های اسپم و هرز و اخبار جعلی استفاده شود. برخی از نرم‌افزارهایی که شرکت‌ها استفاده می‌کنند به طور هوشمندانه‌ای الگوریتم هایی مانند شبکه‌های عصبی، شبکه‌های عمیق[۱۵] و بیزی را در خود جای داده‌اند که فرصتی شده است تا شرکت‌ها بیشتر با آن‌ها آشنا شوند. امروزه استفاده از سیستم‌های تشخیص و پیشگیری از نفوذ (IDPS)[۱۶] چه با استفاده از سیستم‌های تجاری یا متن باز با دانش یادگیری ماشینی و هوش مصنوعی همراه شده است. با هوشمندتر شدن هکرها و افزایش استفاده آن‌ها از ربات‌های نرم افزاری، روش‌های حمله آنها نیز پیچیده‌تر شده است و به همین دلیل شرکت‌های تجاری مجبور هستند به راهکارهای یادگیری ماشینی و هوش مصنوعی برای محافظت از داده‌ها و سیستم‌های خود متکی شوند. سیستم IDPS قادر است با استفاده از یادگیری ماشینی الگوهای مخرب را در مقایسه با الگوهای معتبر در اینترنت شناسایی کند. همان‌گونه که گفته شد یادگیری ماشینی از طریق

[13] Decision Trees
[14] Neural Networks
[15] Deep Networks
[16] Intrusion Detection and Prevention System

شناسایی ناهنجاری در تشخیص حملات روز صفر موثرتر از روش مبتنی بر امضا عمل کرده است و در امنیت سایبری شرکت‌های اروپایی هم نقش موثری داشته است. شکاف قابل توجهی در زمینه امنیت سایبری وجود دارد که نیازمند مشارکت‌های دانش محور جامعه برای مقاوم‌سازی این سیستم‌ها در آینده است.

۴.۲ امنیت سایبری و یادگیری ماشینی تخاصمی

با افزایش استفاده از یادگیری ماشین در سیستم‌های تشخیص نفوذ و سیستم‌های تشخیص و پیشگیری از نفوذ که در بسته‌های امنیت سایبری مورد استفاده توسط شرکت‌ها تعبیه می‌شوند، نوع جدیدی از حملات به نام یادگیری ماشینی تخاصمی شناسایی شده است. در سال ۲۰۲۱ در مقاله‌ای توسط Anthi و همکاران [۳] مطرح شده که با معرفی سیستم‌های تشخیص و پیشگیری نفوذ مبتنی بر یادگیری ماشینی، حملات جدیدی به وجود آمده‌اند که سعی در شکستن الگوریتم‌های یادگیری ماشینی و ایجاد راه‌های نفوذ به این سیستم‌های دفاعی نفوذ دارند. این امر مدل‌های یادگیری الگوریتم‌های یادگیری ماشینی را در معرض حملاتی قرار می‌دهد که اغلب به عنوان یادگیری ماشینی تخاصمی شناخته می‌شوند و هدف آن بهره‌گیری از نقاط ضعف مدل از پیش‌آموزش دیده و ضعف‌های بین داده‌های آموزشی است. شرکت‌ها باید آگاهی خود را نسبت به اهمیت یادگیری ماشینی و هوش مصنوعی در حفظ امنیت سایبری افزایش دهند و این نکته را نیز در نظر داشته باشند که با افزایش این گونه سیستم‌های دفاعی شبکه، حملات جدید علیه آنها نیز افزایش خواهد یافت و برای این موضوع آمادگی ایجاد کنند.

توجه داشته باشید که در بخش نتایج، انواع سناریوهای حمله در امنیت سایبری و نقش مدل پیشنهادی بلاک چین شرح داده شده است.

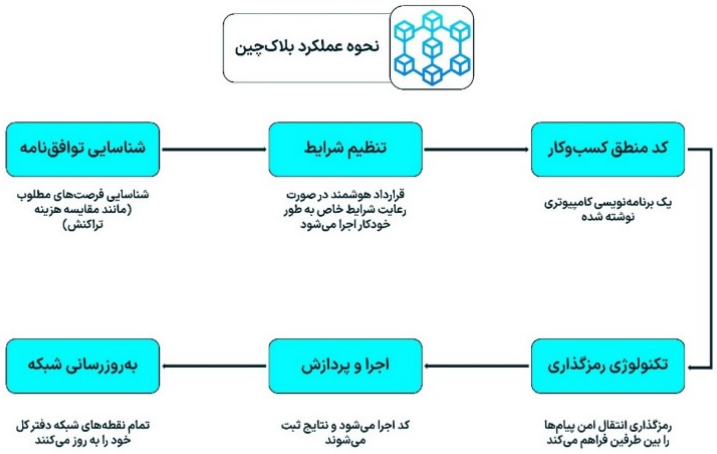
۳ بلاک‌چین

یکی از پر بحث‌ترین تکنولوژی‌های دفتر کل توزیع شده، بلاک‌چین است که برای اطمینان یافتن از یکپارچگی ذخیره‌سازی و تبادل داده‌ها در محیط‌های پراکنده و توزیع‌شده است که نیاز به اعتمادسازی ندارد. به عبارتی دیگر بلاک‌چین یک دفتر کل غیرمتمرکز و همتا به همتا است [۱۷] که می‌تواند داده‌های قابل اعتماد را میان شرکت‌کنندگان غیرقابل اعتماد و تا حدی ناشناس در یک شبکه امکان‌پذیر کند. سیستم‌های محبوب بلاک‌چین مانند اتریوم و هایپرلجر (هایپرلدگر) برای پیاده‌سازی بسیاری از نرم‌افزارهای مبتنی بر بلاک‌چین ساخته شده‌اند. بسیاری از مقالات نمونه‌های اولیه و راه‌حل‌های آزمایشی مبتنی بر بلاک‌چین را برای مشکلات سیستم‌های محاسباتی پیچیده پیشنهاد می‌کنند که اکثر این راه‌حل‌های آزمایشی بر روی اتریوم و هایپرلجر توسعه یافته‌اند. هایپرلجر به دلیل سهولت توسعه نرم افزار قابلیت تعامل‌پذیری و سفارشی‌سازه گسترده را دارد (جدول ۱).

دو ویژگی اصلی یک بلاک‌چین تغییرناپذیری و غیرمتمرکز بودن آن است که از این ویژگی‌ها بسیاری از بخش‌ها از جمله تجارت و خدمات پرداخت که در شکل ۱ فرآیند آن توضیح داده شده است، و در بهداشت و درمان برای بهبود عملیات عملکردی‌شان بهره می‌برند. با اینکه بلاک‌چین هنوز هم تکنولوژی نسبتا جدیدی

جدول ۱: مقایسه ویژگی‌های دو شبکه بلاک‌چین اتریوم و هایپرلجر

ویژگی	اتریوم	هایپرلجر
نوع دفتر کل	بدون نیاز به اجازه	نیاز به اجازه
توسعه‌دهندگان	توسعه‌دهندگان اتریوم	بنیاد لینوکس
ارز دیجیتال	اتر	ندارد
توان عملیاتی	حدود ۲۰ تراکنش در ثانیه	حدود ۲۰۰۰ تراکنش در ثانیه
مکانیسم اجماع	اثبات کار	مکانیسم قابل اتصال
قرداد هوشمند	دارد	دارد
زبان برنامه‌نویسی قرارداد هوشمند	Solidity	Java or Golang or NodeJS
نوع اپلیکیشن	دارای دامنه گسترده	دارای دامنه گسترده



شکل ۱: نمایی از عملکرد یک شبکه بلاک‌چین

است اما تعداد قابل توجهی از مقالات تحقیقاتی نشان می‌دهد که هنوز هم قابلیت ایجاد تحول‌های جدید را داراست و برای نمونه برخی استفاده از آن را جهت تحول اینترنت نیز پیشنهاد داده‌اند.

۱.۳ استفاده از بلاک‌چین در امنیت سایبری

مهم است بررسی کنیم که چگونه تکنولوژی‌های نوظهور مانند بلاک‌چین می‌توانند راه‌حل‌هایی برای کاهش تهدیدات امنیت سایبری جدید ارائه دهند و پژوهش‌های زیادی در زمینه مطالعه چگونگی ارائه زیرساخت‌های قوی امنیت اینترنت توسط این تکنولوژی وجود دارد [۱۳]. بلاک‌چین به دلیل اینکه پراکنده و گسترده است و دارنده‌های مختلف و مستقل آن در شبکه یک نسخه کامل از اطلاعات را در هربار به‌روزرسانی از آن ذخیره می‌کنند به همین جهت یک تکنولوژی غیرمتمرکز محسوب می‌شود که کسی نمی‌تواند ادعای تصاحب شبکه و یا داشتن حق امتیاز آن را داشته باشد و یا حتی کاربران را از دسترسی به اطلاعات شبکه و تراکنش‌های انجام شده منع کند چون که این موارد به صورت شفاف ثبت شده و قابل نمایش است. این ویژگی‌ها به خودی

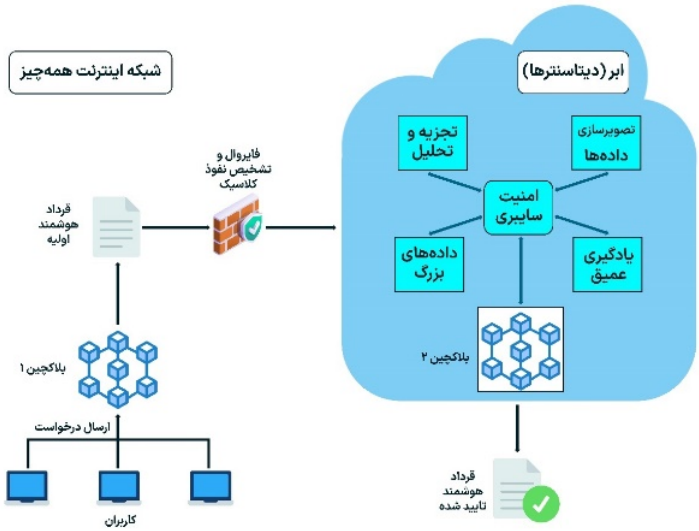
خود می‌تواند از لحاظ امنیت سایبری مزایایی برای کاهش آسیب‌پذیری‌ها داشته باشد و به همین جهت است که عده‌ای از متخصصان و محققان امنیت سایبری پیشنهاد تبدیل شبکه‌های کلاسیک غیربلاک‌چینی را به بلاک‌چین می‌دهند در حالی‌که شاید از لحاظ ظاهری و در صورت در نظر نگرفتن مسائل امنیتی نیازی به استفاده از بلاک‌چین مشاهده نشود.

۲.۳ معایب بلاک‌چین

غیرمتمرکز بودن و تغییر ناپذیری از ویژگی‌های اصلی بلاک‌چین مطرح شد ولی باید توجه داشت که اگر چنانچه شخص حقیقی یا حقوقی بتواند بیشتر از نصف دستگاه‌های متصل به شبکه را به دست آورد در این صورت ممکن است بتواند شبکه را به خطر انداخته و با آسیب‌پذیری مواجه کند چرا که صحت داده‌های شبکه با اکثریت دستگاه‌های پردازشی و ذخیره‌سازی تایید می‌شود. بلاک‌چین معایب دیگری هم دارد، از جمله تاخیر بالا و نیاز به منابع سخت‌افزاری پردازشی زیاد. برخی از راه‌حل‌های عملی در این زمینه تکنیک‌های نوآورانه را برای حل مشکلات بحرانی امنیت سایبری پیشنهاد می‌کنند ولی ممکن است این راه‌حل‌ها نیاز به تغییراتی در زیرساخت‌های سیستم‌های موجود داشته باشند که انجام آن‌ها امکان‌پذیر نباشد یا آزمایش کارایی و اثربخشی آن‌ها در مقایسه با سیستم‌های امنیت سایبری سنتی دشوار باشد [۱۲].

۳.۳ بلاک‌چین و اینترنت اشیا

در جهانی که پیوستگی با اینترنت اشیا رو به افزایش است، نیاز به بهبود امنیت سایبری نیز بسیار مهم است. همان‌طور که Pinno و همکاران [۱۶] و همچنین Mandrita و همکاران [۱۵] شرح داده‌اند حملات سایبری که آسیب پذیری‌های دستگاه‌های اینترنت اشیا را مورد استفاده قرار می‌دهند نگرانی‌های جدی در این عرصه ایجاد کرده و تقاضا برای استراتژی‌های مناسب جهت کاهش تهدیدات را افزایش داده است. کسب اطمینان از یکپارچگی داده‌ها و شناسایی و پیشگیری از بدافزارها از موضوعات تحقیقاتی جذاب در این حوزه هستند [۱۴]. لازم به ذکر است که بلاک‌چین نمی‌تواند خطرات سایبری را به طور کامل از بین ببرد، اما می‌تواند به طور قابل توجهی تهدیدات سایبری را با ویژگی های اصلی خود کاهش دهد و در ترکیب با سایر سیستم‌های امنیت سایبری مفید واقع شود. در حالی که اکثر سیستم‌های تکنولوژی اطلاعات با استفاده از تکنیک‌های رمزنگاری پیشرفته ساخته شده‌اند، ولی به واسطه‌های مرکزی مانند مرجع گواهی نامه‌ها وابسته هستند تا بتوانند یکپارچگی مدیریت داده‌هایشان را تضمین کنند و این باعث می‌شود طرف‌های مخرب بتوانند از ضعف‌های این روابط بهره برده و سیستم‌ها را با تهدیدات سایبری مانند حملات محروم‌سازی از سرویس، بدافزار، باج‌افزار، استراق داده‌ها و ... مختل کنند. اما در بلاک‌چین به دلیل غیرمتمرکز بودن این مشکلات قابل حل است.



شکل ۲: اجزای اصلی مدل پیشنهادی معماری بلاک‌چین در مدیریت جریان داده‌های اینترنت اشیاء با کمک پردازش ابری امنیت سایبری

۴ روش‌شناسی : ارائه یک راهکار هوشمند

برای فراهم آوردن مسئولیت‌پذیری، شفافیت و پیگیری سیستم از منظر ترافیک شبکه، سیستم‌های دفتر کل (به نوعی دیتابیس) توزیع شده غیرمتمرکز می‌توانند در تجارت الکترونیک به ویژه موارد امنیتی، بهداشتی و زیرساختی به کار گرفته شوند تا از پایداری تکنولوژی بلاک‌چین همراه با تجارت الکترونیک اطمینان حاصل شود. در حال حاضر تحقیق و بررسی تاثیرگذاری شبکه‌های غیرمتمرکز بلاک‌چینی در سطح جهانی است که هم‌زمان کاربردهای آن در بخش‌های دانشگاهی، عمومی و خصوصی مورد استفاده قرار می‌گیرد.

در شکل ۲ مدلی پیشنهادی برای معماری مدیریت داده‌ها نشان داده‌ایم که اجزای کلیدی این ساختار در ادامه توضیح داده و تحلیل می‌شود.

شبکه اینترنت اشیا (IoT)

در ابتدا کاربران از طریق شبکه اینترنت اشیا درخواست‌های خود را به سیستم ارسال می‌کنند. این درخواست‌ها می‌تواند شامل داده‌هایی باشد که باید به بلاک چین افزوده شوند، یا قراردادهای هوشمندی که قرار است اجرا شوند. البته هدف اصلی کاربران از این داده‌ها در نهایت می‌تواند ارسال یا دریافت ارزش پولی برای انجام تجارت یا به روزرسانی اطلاعات حساب‌شان باشد. این شبکه به عنوان رابط میان کاربران و سیستم امنیتی عمل کند.

بلاک‌چین اولیه و قرداد هوشمند اولیه

داده‌های ارسال شده در بلاک چین اول پس از تایید تبدیل به قرداد هوشمند اولیه می‌شود و داده‌های آن ثبت می‌شود. قرارداد هوشمند مسئول مدیریت و اعتبارسنجی اولیه داده‌ها است. مطابق با تحقیقات مرتبط با کاربرد قردادهای هوشمند در بلاک‌چین، این لایه جهت اطمینان از صحت داده‌ها و جلوگیری از حملات مبتنی بر داده‌های جعلی عمل می‌کند. بلاک‌چین اولیه می‌تواند به عنوان یک زنجیره عمومی یا خصوصی عمل کند. در این مرحله قابلیت ردگیری و شفافیت داده‌ها تصمین می‌گردد. نسخه‌ای از قرارداد هوشمند اولیه به عنوان داده ورودی به سمت دیتاسنترها جهت پردازشی ابری و صحت‌سنجی بیشتر از لحاظ امنیت سایبری ارسال می‌شود.

فایروال و سیستم تشخیص نفوذ کلاسیک

در معماری مطرح شده در این پژوهش مطابق دیاگرام شکل ۲، پیش از اینکه قرارداد هوشمند اولیه وارد ابر یا همان دیتاسنتر (مرکز داده) شود، ابتدا از طریق یک فایروال و سیستم تشخیص و پیشگیری نفوذ (IDPS) عبور می‌کنند. این سیستم‌ها به عنوان یک خط دفاعی عمل کرده و تلاش می‌کنند ترافیک داده‌های مخرب یا نفوذهای احتمالی را مسدود کنند. این مرحله مطابق با پژوهش‌های مربوط به امنیت شبکه و تشخیص نفوذ در محیط‌های ابری است که امنیت اولیه شبکه‌های توزیع‌شده را تأمین می‌کند.

انتقال داده‌ها به ابر (دیتاسنترها)

پس از پردازش داده‌های اولیه در بلاک‌چین اولیه، اطلاعات به محیط ابری یا همان دیتاسنترهای بزرگ منتقل می‌شوند. در این محیط داده‌ها وارد مراحل تحلیل پیشرفته می‌شوند که عبارتند از:

تصویرسازی داده‌ها: داده‌ها با استفاده از ابزارهای تصویری تحلیل می‌شوند تا الگوها و اطلاعات کلیدی شناسایی شود. در این مرحله تصویرسازی داده‌های بلاک‌چین و تحلیل داده‌ها در محیط‌های ابری صورت می‌پذیرد.

داده‌های بزرگ: استفاده از داده‌های بزرگ قابلیت تحلیل مقادیر زیادی از اطلاعات را فراهم می‌آورد. این بخش بر اساس مطالعات در زمینه تحلیل داده‌های کلان در امنیت سایبری و بلاک چین عمل می‌کند.

یادگیری عمیق: داده‌ها از طریق الگوریتم‌های یادگیری ماشینی به ویژه یادگیری عمیق پردازش می‌شوند. این روش‌ها به سیستم کمک می‌کنند تا حملات سایبری جدید یا الگوهای غیرعادی در داده‌ها را تشخیص دهند.

امنیت سایبری: تجزیه و تحلیل موارد ذکر شده امنیت داده‌ها و شبکه را تأمین می‌کند. علاوه بر آن می‌توان دیگر روش‌های سایبری نظیر رمزنگاری و مکانیسم‌های بازدارنده در برابر حملات را جهت ارتقا

بیشتر امنیت سایبری به کار برد. اما در صورتی که بررسی‌های لازم برای نبودن اتلاف و هزینه اضافی و عدم اختلال با دیگر موارد تایید شود. پس از این مرحله داده‌ها به سمت بلاک‌چین ثانویه ارسال می‌شود.

بلاک‌چین ثانویه و قرارداد هوشمند تایید شده

پس از پردازش‌های ابری، داده‌ها به بلاک چین دوم منتقل می‌شوند. این بلاک‌چین به عنوان لایه دوم امنیتی عمل کرده و داده‌های پردازش شده را ذخیره می‌کند. با ترکیب این بلاک چین اول و دوم، یک سیستم دوتایی برای مدیریت داده‌ها شکل می‌گیرد که قابلیت اطمینان، شفافیت بیشتر و امنیت بالاتر را فراهم می‌آورد. پس از عبور داده‌ها از بلاک‌چین ثانویه و انجام پردازش‌های امنیتی، قرارداد هوشمند نهایی تایید شده و نتیجه به کاربران ارسال می‌شود. این مرحله نهایی تایید امنیت، صحت داده‌ها و اطلاعات و موفقیت‌آمیز بودن فرآیند را انجام و اطلاع می‌رساند.

۵ نتایج

سناریوهای حمله در امنیت سایبری و نقش مدل پیشنهادی بلاک چین

در ادامه به بررسی انواعی از حملات سایبری و نقشی که مدل پیشنهادی بلاک چینی این پژوهش (که در بخش نتایج ارائه خواهد شد) می‌تواند در جلوگیری از آنها ایفا کند می‌پردازیم. این مدل در بخش روش‌شناسی به تفصیل ارائه شد.

حملات تزریق SQL (SQL Injection Attack)

این حملات زمانی رخ می‌دهد که فرد مهاجم تلاش می‌کند تا با تزریق کدهای مخرب به SQL، پایگاه داده سرور اطلاعاتی را نمایش دهد که مهاجم قادر به مشاهده، ویرایش و حذف جداول پایگاه داده باشد. بلاک‌چین به دلیل ساختار خاص بلوکی خود که هر بلوک دارای رمزگذاری خاص هستند و هر یک از این توالی اعداد به توالی اعداد بلوک‌های دیگر به صورت زنجیروار وابسته هستند. این موضوع موجب می‌شود تا تغییر یا پاک کردن اطلاعات برای فرد مهاجم امکان پذیر نباشد چرا که با تاریخچه و اطلاعات دیگر بلوک‌ها مطابقت نخواهد داشت. ضمنا بلوک‌های قبل‌تر قابلیت ویرایش ندارند که امنیت داده‌ها را تضمین می‌کند.

حملات شنود مرد میانی (Man-in-the-Middle Attack)

در این نوع از حملات که به آن حمله شنود نیز گفته می‌شود، مهاجم تلاش می‌کند اطلاعات بین مشتری و سرور یا هاست شرکت مربوطه را سرقت کند و به طور غیرمجاز به اطلاعات رد و بدل شده دسترسی داشته باشد. راه حلی که بلاک‌چین برای این موضوع ارائه می‌دهد در نوع خود جالب است. می‌توان گفت در سیستم بلاک‌چینی اطلاعات به دو دسته شفاف و دسته خصوصی تقسیم می‌شوند که بلاک‌چین تنها اطلاعات شفاف را دریافت، پردازش و ثبت می‌کند و نیازی به اطلاعات خصوصی کاربر ندارد و این موارد ناشناس باقی می‌ماند. این مورد در عملکرد شرکت‌ها نیز موثر است زیرا اولا شرکت‌ها را مجاب می‌کند تا سیستم خود را به گونه‌ای

تغییر دهند که کمترین نیاز به اطلاعات حساس داشته باشند و از طرفی شفاف بودن اطلاعات موجب می‌شود که شرکت بعدها در خصوص گزارش‌دهی سالانه خود نظیر گزارش عملکرد خود به سهامداران یا رسانه‌ها زیر سوال نرود و نیز نگرانی کمتری بابت افشا شدن اطلاعات محرمانه کاربران داشته باشد که همه این موارد می‌تواند هزینه‌های آماری و امنیتی شرکت را کاهش دهد.

قابلیت‌های پیشرفته مدل بلاک‌چین پیشنهادی

یکی از ویژگی‌های کلیدی مدل پیشنهادی این پژوهش، استفاده از دو بلاک‌چین مجزا برای افزایش امنیت است. مدل پیشنهادی این پژوهش به دلیل داشتن ۲ عدد بلاک‌چین این امکان را دارد که مثلا داده‌هایی در بلاک‌چین ۱ ثبت کند که به تنهایی قابل استفاده و دارای مفهوم نباشد و برای دانستن آنها نیاز به اطلاعات ثبت شده نظیر به نظیر در بلاک چین ۲ باشد. که این مورد نیز می‌تواند مانند رمزگذاری پروتکل‌ها امنیت اتصالات و حریم خصوصی بیشتری برای کاربران و مشتریان شرکت به ارمغان بیاورد.

مقابله با دیگر انواع حملات سایبری

علاوه بر حملات مذکور، مدل پیشنهادی در انوع دیگری از حملات سایبری نیز می‌تواند نقش ایفا کند به عنوان مثال اگر شرکت برای کاربر لینک قرارداد یا تراکنش ثبت شده در بلاک چین‌ها یا حتی یکی از بلاک‌چین‌ها را ارسال کند که خود کاربر هم آن را چک کند، در این صورت حملات فیشینگ (Attack Pishing) با هدف جعل و شبیه‌سازی برای مهاجمان دشوار خواهد شد. یا چنانچه برای هر مرحله از فرآیند مثلا برای ثبت در بلاک چین ۱ و بلاک چین ۲ از کاربر رمزعبورهای جداگانه و متفاوت از هم درخواست شود در این صورت حملات بروت فورس (Brute Force) نیز برای هکرها سخت‌تر خواهد شد. در نهایت مواردی ذکر شده تنها بخشی از ایده‌ها و قابلیت‌هایی است که می‌توان روی ساختار دیاگرامی مدل پیشنهادی این پژوهش پیاده سازی کرد و پیاده‌سازی سایر موارد و ارتقاء بستگی به خلاقیت و نوآوری تیم‌های نرم‌افزاری شرکت‌های مربوطه خواهد داشت.

۶ نتیجه‌گیری

برای ایجاد یک استراتژی تاثیرگذار بر امنیت سایبری برای شرکت‌های تجاری، سازمان‌ها و دانشگاه‌ها، نیاز به ایجاد ابتکارات مالی برای هزینه‌های پردازشی سخت‌افزاری کلیدی است. آگاهی و آموزش مدیران، با نظارت و حمایت بیشتر از کاربران برای ادغام موثرتر امنیت سایبری و بلاک‌چین مورد نیاز است. با اولویت دادن به شناسایی و پیشگیری از نفوذ در سطح شرکت‌های تجاری خصوصی و حتی در سطح سازمان‌ها و موسسات دانشگاهی می‌تواند در ارتقا و حفظ تمام مزایای حفاظت‌های امنیت سایبری در مقابل حملات و جرایم سایبری نقش داشته باشند. این باعث کاهش قابل توجه آسیب‌پذیری‌های شبکه، جلوگیری از دسترسی غیرمجاز به داده‌های حساس و تضمین عملکرد سیستم‌های مهم و حیاتی می‌شود. این امر نه تنها اعتماد کاربران به امنیت زیرساخت‌ها را افزایش می‌دهد، بلکه هزینه‌های مربوط به نفوذ، حملات و بازیابی داده‌ها را نیز می‌تواند

کاهش دهد و محیطی امن‌تر برای تبادل اطلاعات فراهم کند. تلاش‌های همراه با مسئولیت‌پذیری و شفافیت، همچنین نیاز به ارزیابی مداوم قوانین، سیستم‌ها و نتایج آن با سرمایه‌گذاری از بخش‌های عمومی و خصوصی دارد.

به‌طور کلی ساختار ارائه شده در این پژوهش بر اساس تلاش‌ها و تحقیقات پیشرفته در زمینه یکپارچه‌سازی بلاک‌چین با امنیت سایبری، اینترنت اشیا، یادگیری ماشین و تحلیل داده‌های کلان شکل گرفته است. مطالعات بسیاری که در این پژوهش بررسی شد در تلاش بودند اثربخشی اجزای به کار رفته در این معماری را نشان دهند. البته هنوز تاخیر در شبکه‌های بلاک‌چین، چالش‌های واقعی را برای پذیرش این تکنولوژی برای شرکت‌های تجاری ایجاد می‌کند. با افزایش ارتباطات دیجیتال و غیرمتمرکز شدن مراکز داده‌ها، مجموعه وسیع‌تری به مشارکت‌کنندگان و اشتراک‌گذاری و همکاری‌شان اضافه خواهد. با این حال، این سیستم‌های دیجیتال از نظر امنیت سایبری بلوغ لازم را ندارند و به طور اجتناب‌ناپذیر فضای حمله‌ای برای مهاجمان ایجاد می‌کنند. در این مقاله چندین مشکل امنیتی در سیستم‌های دیجیتال و به تبع آن داده‌ها محاسباتی و مکانیسم‌های اعتماد برجسته شد. این چالش‌ها منجر به تکامل راه‌حل‌های فنی شده‌اند، به طوری که راه‌حل‌های کنونی به قدری متنوع هستند که می‌توانند از پیشرفته‌ترین راه‌حل‌ها برای شرکت‌های بزرگ گرفته تا ابتدایی‌ترین راه‌حل‌ها را برای شرکت‌های کوچک ارائه کنند. به عنوان مثال در همین مدل ارائه شده در این پژوهش (شکل ۲)، چنانچه شرکتی قادر به تأمین همه سخت‌افزارها و نرم‌افزارهای موردنیاز نباشد می‌تواند با کاستن برخی از اجزای مدل و تبدیل آن به یک سیستم کوچک‌تر کماکان از کارایی آن در امنیت سایبری بهره‌مند شوند. ما معتقدیم که نتیجه تحقیقات بیشتر برای ارائه راهکارهای نوآورانه برای امنیت سایبری موجب بهبود و ایجاد سیستم‌های سایبری امن‌تر خواهد گشت که امنیت داده‌های جامعه را به ارمغان می‌آورد.

سپاسگزاری

از همه پژوهشگران عزیز که یافته‌های خود را به صورت رایگان در اینترنت به اشتراک گذاشته‌اند و موجب آشنایی نویسندگان با این حیطه گردید و همچنین از آشنایان و اساتید محترم دانشگاه تهران سپاس‌گزاری و قدردانی می‌کنیم.

مراجع

[1] M. Sabuhi, M. Zhou, C.-P. Bezemer, and P. Musilek, ‘Applications of generative adversarial networks in anomaly detection: a systematic literature review’, Ieee Access, vol. 9, pp. 161003–161029, 2021.

[2] W. Lim, K. Y. S. Chek, L. B. Theng, and C. T. C. Lin, ‘Future of generative adversarial networks (GAN) for anomaly detection in network security: A review’, Computers Security, p. 103733, 2024.

[3] Anthi E, Williams L, Rhode M, Burnap P, Wedgbury A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems. J Inf Secur Appl. 2021;58:102717.

[4] Rawindaran N, Jayal A, Prakash E. Artificial intelligence and machine learning within the context of cyber security used in the UK SME Sector. In: AMI 2021— the 5th advances in management and innovation conference 2021. Cardiff Metropolitan University. 2021.

[5] Are Your Operational Decisions Data-Driven? 2021. https://www. potentiaco.com/what-is-machine-learning-definition-typesappli cations-and-examples/. Accessed 11 Jul 2021.

[6] Gallaher MP, Link AN, Rowe B. Cyber security: economic strategies and public policy alternatives. Chentanham: Edward Elgar Publishing; 2008.

[7] Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC. A survey of intrusion detection in Internet of Things. J Netw Comp Appl. 2017;84:25–37.

[8] Cressy R, Olofsson C. European SME Financing: An Overview. Small Business Economics, 1997. pp 87–96

[9] Dunham K, Melnick J. Malicious bots: an inside look into the cyber-criminal underground of the internet. Boca Raton: Auerbach Publications; 2008.

[10] General Data Protection Regulations (GDPR). https://ico.org.uk/ for-organisations/guide-to-dataprotection/guide-to-the-generaldata-protectionregulation-gdpr/. Accessed 16-10-2020.

[11] Kabiri P, Ghorbani AA. Research on intrusion detection and response: a survey. Int J Netw Secur. 2005;1(2):84–102.

[12] Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Comput Surv. 2019;52:3.

[13] Salman T, Zolanvari M, Erbad A, Jain R, Samaka M. Security services using blockchains: a state of the art survey. IEEE Commun Surv Tutor. 2019;21(1):858–80.

[14] Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Celebrating 40 years of telecommunications policy—a retrospective and prospective view. Telecommun Policy. 2017;41(10):1027–38.

[15] Mandrita B, Junghee L, Choo KKR. A blockchain future for internet of things security: a position paper. Dig Commun Netw. 2018;4(3):149–60.

[16] Pinno OJA, Gregio ARA, De Bona LCE. ControlChain: blockchain as a central enabler for access control authorizations in the IoT. In: GLOBECOM 2017—2017 IEEE global communications conference; 2017. pp. 1–6.

[17] Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData Congress); 2017. pp. 557–64.