به‌کارگیری فناوری زنجیره‌بلوکی در ارتقاء سامانه‌های آگاهی وضعیتی سایبری

محدثه کاظمی[۱]، رحیم اصغری[۲]، حسین خالقی بیزکی[۳].

۱- دانشجوی کارشناسی ارشد، دانشگاه صنعتی مالک اشتر تهران. ایران.

۲- استادیار مجتمع دانشگاهی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر تهران. ایران.

۳- استاد مجتمع دانشگاهی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر تهران. ایران.

چکیده

با پیشرفت زیرساخت‌های حیاتی و توسعه به‌کارگیری فناوری اطلاعات در سازمان‌ها، حملات سایبری نیز در حال پیشرفت بوده و روزبه‌روز پیچیده‌تر می‌شوند. تبادل اطلاعات امن و به‌کارگیری سامانه‌های هوش تهدیدات سایبری می‌تواند کمک قابل‌توجهی به بهبود امنیت فضای تبادل اطلاعات در شرکت‌ها نماید که در سال‌های اخیر از اهمیت بسیار بالایی برخوردار بوده است. اگر سازمان‌ها بتوانند الگوهای هکرها یا مهاجمان سایبری را یاد بگیرند، می‌توانند به‌طور مؤثر به دفاع از خود پرداخته و خطرهای تأثیرگذار بر روی کسب‌وکار خود را کاهش دهند. از دیگر دلایل اهمیت هوش تهدیدات سایبری کمک به شرکت‌ها در پیش‌گیری از خروج داده‌ها می‌باشد. همچنین، سازمان‌ها می‌توانند با همکاری و تبادل اطلاعات با یکدیگر، به‌طور مؤثرتری از هوش تهدید برای پیش‌گیری از تهدیدهای آتی استفاده نمایند. به این منظور از روش‌های مختلفی جهت اشتراک گذاری بهتر داده‌های هوش تهدید و درنتیجه بهبود آگاهی وضعیتی سایبری استفاده‌شده است. در این مقاله، آگاهی وضعیتی سایبری و چالش‌های این حوزه بررسی شده و راهکارهای پیشنهادی مرتبط با بهبود آگاهی وضعیتی سایبری با استفاده از فن‌آوری زنجیره بلوکی و قراردادهای هوشمند معرفی‌شده است.

کلمات کلیدی: آگاهی وضعیتی سایبری، هوش تهدید سایبری، زنجیره بلوکی، قراردادهای هوشمند، اتریوم، EOS.

۱. مقدمه

آگاهی وضعیتی سایبری ادراکی از وضعیت‌های تهدید و امنیت به همراه ارزیابی تأثیرات کنونی و آینده آن‌ها است. در سال‌های اخیر، محققان در زمینه‌ی آگاهی وضعیتی ابزارهای پیچیده‌ای در بسیاری از موارد کاربردی ایجاد کرده‌اند. عواملی مانند سرعت رویدادها، سرریز شدن داده‌ها و کمبود معنا، ارزیابی آگاهی وضعیتی هم‌زمان از عملیات سایبری را دشوار می‌کند. ما در برخورد با داده‌هایی که اغلب مبهم و نادقیق هستند، باید بر اطلاعات ناکامل تکیه کنیم تا بتوانیم حملات واقعی را کشف کنیم و از طریق مدیریت ریسک مناسب، از رخ دادن یک حمله جلوگیری کنیم [1].

در بحث امنیت سایبری، بر روی شناسایی و دفاع از داده‌های خصوصی سازمان‌ها تمرکز می‌کنیم. هنگامی‌که مهاجمان به این فضای دفاعی نفوذ می‌کنند، سازمان‌ها با یکدیگر هماهنگ می‌شوند تا از وقوع این رخنه جلوگیری کنند؛ اگر در مقابل یک تهدید خاص بخشی از دانش در دسترس باشد، دفاع بهتری صورت می‌گیرد. از هوش تهدید سایبری می‌توان برای درک و پیش‌بینی بهتر این رفتارهای مخرب استفاده کرد تا در کوتاه‌ترین زمان بهترین تصمیم اتخاذ شود. هوش تهدید سایبری ماهیت بسیار حساسی دارد و اگر به شیوه‌ای نادرست مدیریت شود و یا مورد نفوذ واقع‌شده باشد می‌تواند منجر به از دست

[1] m.kazemi710913@gmail.com
[2] meisam.mathhome@gmail.com
[3] bizaki@yahoo.com

رفتن داده‌ها و یا درآمد شرکت‌ها شود. مراکز اشتراک‌گذاری و تحلیل اطلاعات[1]، امکانی را فراهم می‌آورند تا اطلاعاتی در مورد علل اصلی، رویدادها و تهدیدها و همچنین تجربه، دانش و تحلیل اطلاعات، میان سازمان‌های مختلف به اشتراک گذاشته شود. در این مراکز، سازمان‌ها رویدادها را تحت شرایطی خاص به تیم‌های امنیت رایانه و واکنش نسبت به حوادث[2] ملیِ خود گزارش دهند؛ اگر ارائه‌ی گزارش و بررسی رویداد به‌درستی توسط نهاد مربوطه انجام نشده باشد، می‌تواند موجبات تحریم مقامات ذیصلاح را فراهم آورد [2, 3, 4]. اشتراکِ داوطلبانه‌ی ناموفق، علل ریشه‌ایِ متفاوتی ازجمله عدم اعتماد و انگیزه میان سازمان‌های شرکت‌کننده، عدم تقارن میان تولیدکننده و مصرف‌کننده و عدم اعتماد به صحت داده‌های CTI باشد. شرکت‌ها باید قادر باشند مدارک موثق برای گزارش دهی دقیق ارائه کنند تا بتوان از جریمه شدن جلوگیری کرد و بتوان از داده به‌عنوان مدرک در دادگاه استفاده کرد. همچنین باید از دسترسی پایدار و یکپارچگی داده گزارش‌شده اطمینان حاصل کرد [3].

از طرفی تحلیل گران سایبری روزانه حجم زیادی از گزارش‌های تهدید را دریافت می‌کنند و برای مدیریت و دسته‌بندی این گزارش‌ها دچار چالش‌هایی می‌شوند. گزارش‌های تهدید وارد فرآیندهای سازمانی مانند جمع‌آوری، استفاده، بایگانی و حذف می‌شوند. جهت تصمیم‌گیری و مدیریت صحیح این گزارش‌ها و درنتیجه ارتقای سطح آگاهی وضعیتی سایبری، نیاز به سیستمی می‌باشد که بتوانند فاصله‌ی میان داده‌های سایبری و ادراک از موقعیت موجود را پر کنند.

برای آنکه بتوان تمام چالش‌های باز را به‌طور هم‌زمان تحت پوشش قرارداد، روش‌هایی مبتنی بر زنجیره بلوکی ارائه‌شده که علاوه بر ایجاد شرایط اشتراک گذاری داوطلبانه در محیطی امن، به دسته‌بندی و مدیریت رویدادها نیز کمک می‌کند.

در ادامه روش‌های نوین جهت رفع چالش‌های باز و پژوهش‌های مرتبط با این حوزه معرفی‌شده و مقالات عنوان‌شده مورد بررسی قرار می‌گیرند.

۲. مروری بر آگاهی وضعیتی سایبری

در این بخش سعی شده مراجع مرتبط در حوزه آگاهی وضعیتی سایبری بررسی و چالش‌های موجود شفاف گردد. همچنین مقالات زنجیره بلوکی و قراردادهای هوشمند مورد مطالعه قرارگرفته و در ادامه پژوهش‌های نوین در جهت بهبود آگاهی وضعیتی سایبری با استفاده از قراردادهای هوشمند بررسی و نتایج کارهای مختلف در کنار هم مقایسه و ارزیابی‌شده است. امنیت سایبری، حوزه‌ای است که در آن‌یک یا چند تحلیل‌گر بر زیرساخت‌ها و شبکه‌های پیچیده رایانه‌ای نظارت دارند تا امکان فعالیت عادی و امن شبکه فراهم و از آن در برابر استفاده غیرمجاز دفاع شود. برای ایجاد آگاهی وضعیتی، باید تحلیل‌گران و مدافعان حوزه سایبری، ترافیک غیرعادی را شناسایی کرده و با طبقه‌بندی ترافیک ناخواسته، نفوذ را گزارش داده، میزبان‌ها و موجودیت‌های هک شده را تشخیص دهند [1].

فرآیند اشتراک‌گذاریِ هوش تهدید سایبری، این پتانسیل را دارد که به فرآیندی مؤثر تبدیل شود؛ فرآیندی که می‌تواند برای سازمان‌ها امکانی را فراهم آورد تا قادر باشند خیلی سریع نسبت به فعالیت‌های مخربی که ممکن است شبکه‌ی آن‌ها را تهدید کنند، واکنش نشان دهند. اگرچه، بسیاری از فروشندگان و سازمان‌ها به‌منظور حمایت از فرآیند اشتراک‌گذاریِ هوش تهدید سایبری، محصولاتی را تولید کرده‌اند اما هنوز هم مشکلات قابل‌توجهی در این حوزه وجود دارد. اندسلی[3] تعاریف قابل‌بحث و پایه‌ای برای فنون آگاهی وضعیتی به‌ویژه در محیط‌های پویا ارائه کرده است. یکی از این تعاریف پراستفاده که در سال ۱۹۹۵ ارائه‌شده به این صورت است:

[1] Information Sharing and Analysis Centers (ISACs)
[2] Computer Security Incident Response Team (CSIRT)
[3] Endsly

"آگاهی وضعیتی عبارت است از درک (دریافت[1]) عناصر و اجزای محیط در ظرفی از زمان و مکان، تفسیر و فهم[2] معانی جزئیات دریافتی و پیش‌بینی یا تجسم[3] وضعیت آن‌ها در آینده نزدیک."

۲-۱- نیازمندی‌های آگاهی وضعیتی

برای تضمین توسعه فن‌آوری در دفاع سایبری ابتدا باید نیازمندی‌های آگاهی وضعیتی در این حیطه به‌طور کامل درک شوند. برای این منظور باید ابتدا موارد زیر به‌خوبی درک شده و توسعه داده شوند:

آگاهی از وضعیت کنونی (درک وضعیت): شامل دو بخش تعیین و شناسایی است. منظور از تعیین، تعیین نوع حمله است که قاعدتاً باید پاسخگوی سؤالاتی از قبیل "منبع حمله کجاست؟"، "حمله‌کننده کیست؟" و "هدف حمله چیست؟" باشد؛ و منظور از شناسایی، فقط شناسایی نوع حمله است.

آگاهی از اثرات حمله (ارزیابی حمله): این جنبه از آگاهی وضعیتی سایبری، ارزیابی اثر نامیده می‌شود. خودارزیابی اثر نیز از دو بخش تشکیل می‌گردد:

- ارزیابی اثر کنونی
- ارزیابی اثر آینده

در ارزیابی اثر آینده، این سؤال مطرح است که اگر حمله‌کننده به‌طور پیوسته به حمله‌ی خود ادامه دهد، در آینده میزان اثرگذاری او چگونه خواهد بود؟ آنالیز آسیب‌پذیری جنبه پیشرفته ارزیابی اثر است که در این حالت تجسم اثر آینده حملات نیز میسر خواهد شد. ارزیابی اثر آینده، شامل ارزیابی تهدید هم هست.

از نحوه تکامل وضعیت‌ها آگاه باشید. ردیابی جزء اصلی این جنبه است.

از رفتار رقیب (دشمن) آگاه باشید.

آگاهی از اینکه چرا و چگونه موقعیت کنونی رخ‌داده: جنبه دیگری از آگاهی وضعیت است که نیاز به تحلیل علت و معلولی دارد.

آگاهی از میزان کیفیت و قابلیت اطمینان به مؤلفه‌های اطلاعاتی آگاهی وضعیتی: این جنبه از آگاهی وضعیتی منجر به دانایی و هوشمندی در تصمیمات خواهد شد. این جنبه به‌عنوان بخشی از درک وضعیت یا شناسایی نیز محسوب می‌شود.

ارزیابی آینده محتمل و قابل‌باور با توجه به وضعیت کنونی: این جنبه از آگاهی وضعیتی از فن‌آوری‌های متعددی برای تجسم اقدامات و فعالیت‌های حمله‌کننده‌ها و تجسم مسیرهای احتمالی شکل‌گرفته است. درک نیت، فرصت و توانمندی حمله‌کننده نیز ازجمله محورهای کلیدی این جنبه است.

این فرآیند، مبنای درک وضعیت فعلی آگاهی وضعیتی سایبری در شبکه‌ها هست و نقطه شروعی برای تحقیقات و پژوهش‌های آتی محسوب می‌شود.

برای ایجاد یک آگاهی وضعیتی مناسب، به‌تمامی این جنبه‌ها به‌صورت یکپارچه و در قالب یک راه‌حل نیاز است و استفاده از هرکدام از آن‌ها به‌تنهایی کارایی چندانی ندارد. در این حوزه همواره با تهدیدات مختلفی مواجه هستیم که این تهدیدات ممکن است تصادفی و یا هدفمند باشند؛ بنابراین از یک سیستم آگاهی وضعیتی ایده آل انتظار می‌رود که خودآگاه و خود محافظ بوده و نیازی به دخالت انسان نداشته باشد [5].

[1] Perception
[2] Comprehension
[3] Projection

۲-۲- چالش‌های آگاهی وضعیتی سایبری

باوجوداینکه ذهن انسان به‌گونه‌ای طراحی‌شده که بتواند بر پایه مجموعه‌ای از فرآیندهای شناختی، مدل‌های ذهنی و شِماهای حاصل از تجربه، آگاهی وضعیتی را به شکل مناسبی استخراج کند، اما دنیای هوشمند عملیات سایبری این فرآیند را به‌صورت جدی تحت تأثیر قرار می‌دهد. ترکیب اثرات حاصل از پویایی و پیچیدگی شبکه، بردارهای پیچیده و پیوسته متغیر حمله، رویدادهایی که در سطح هزارم ثانیه رخ می‌دهند، نرخ پایین سیگنال به نویز در فضای سایبری و لختی بسیار بالا بین زمان معرفی یک بدافزار و زمان رویداد حمله، همگی باعث شده‌اند تا دست‌یابی بی‌درنگ به آگاهی وضعیتی در عملیات سایبری بسیار دشوار باشد و چالش‌برانگیز شود. از طرفی نبود ابزارهای یکپارچه و مناسب به‌گونه‌ای که بتوانند این شکاف را پر کنند از اهمیت ویژه‌ای برخوردار بوده و پرداختن به این مسئله برای حصول آگاهی وضعیتی موردنیاز در عملیات سایبری بسیار حیاتی است. ابزارهای یکپارچه باید قادر باشند به کاربر سایبری در گردآوری مجموعه جامعی از اطلاعات موردنیاز کمک کنند، داده‌ها را برای درک اثرات حملات روی عملیات و مأموریت‌ها تبدیل نمایند و از دفاع فعال و پیش‌دستانه در شبکه نیز پشتیبانی کنند.

- هم‌بندی پویا و پیچیده سامانه‌های سایبری
- سرعت تغییر فن‌آوری‌ها
- نرخ پایین سیگنال به نویز
- حملات مخفی و بمب‌های ساعتی
- تهدیدات چندوجهی با تغییرپذیری سریع
- سرعت رویدادها
- ابزارهای غیر یکپارچه
- وفور داده و کمبود معنا
- خودکارسازی و کاهش آگاهی وضعیتی
- عدم قطعیت در آگاهی وضعیتی سایبری

یکی از مهم‌ترین مشکلات در حوزه آگاهی وضعیتی سایبری عدم اطمینان به اطلاعات جمع‌آوری‌شده است که منجر به عدم قطعیت و درنتیجه منجر به انحراف آگاهی وضعیتی می‌شود. نبود داده و آگاهی کامل، موضوع عدم قطعیت را با مشکل بیشتری مواجه می‌کند.

آگاهی وضعیتی سایبری با حداقل دو هدف ارتقای هوش ماشینی در حفاظت از خود و خودآگاهی وضعیتی و خودکارسازی فرآیندهای آگاهی وضعیتی شناختی، نیاز به روش‌شناسی کل‌نگری دارد که سه مؤلفه درک، فهم و تجسم را باهم در نظر بگیرد و باید عدم قطعیت را از طریق فرضیه‌ها و استدلال‌ها مدیریت کند. همچنین آگاهی وضعیتی سایبری با دونقطه نظر مواجه است. دیدگاه چرخه عمر که شامل سازوکار آماده‌سازی برای هر فاز از فرآیند آگاهی وضعیتی سایبری بوده و دیدگاه شناخت انسانی نیز شامل نظریه‌ها و فنونی برای یکپارچه‌سازی تحلیل‌گرهای انسانی در چارچوب کلی آگاهی وضعیتی سایبری است [1].

۲-۳- ابزارهای برتر تحلیل هوش تهدید

هوش تهدید در حوزه‌ی امنیت سایبری توسط ابزارهای تحلیل رخدادهای سایبری ایجادشده است. برای مثال، ابزار موتور تحلیل مشارکتی برای آگاهی موقعیتی و واکنش به رخدادها، برای متخصصان امنیت که وظایف رسیدگی به رخدادهای سایبری را در سطوح ملی و بین‌المللی انجام می‌دهند پشتیبانی تحلیلی فراهم می‌کند و تشخیص ارتباطات ضمنی بین

قطعه‌های موجود اطلاعات را تسهیل می‌کند. سامانه CAESAIR[1] از تکنیک‌های گوناگون همبستگی اطلاعات امنیت پشتیبانی می‌کند و قابلیت‌های واردکردن قابل تنظیم را از بسیاری از منابع مرتبط با امنیت، شامل یک ذخیره‌گاه سفارشی، فیلدهای هوش متن‌باز و بولتن‌های امنیت فناوری اطلاعات و همچنین یک کتابخانه‌ی آسیب‌پذیری استانداردشده، فراهم می‌کند.

ابزار متن‌باز IntelMQ که به‌صورت مشارکتی توسط تیم واکنش به حوادث رایانه‌ای استرالیا و شرکای دیگر باهدف تجزیه کردن و کشف ارتباط رخدادهای سایبری توسعه داده‌شده است.

سکوی اشتراک‌گذاری اطلاعات بدافزار MISP[2]، ابزار متن‌باز دیگری است که همبستگی خودکار داده‌ها را از طریق یافتن ارتباطات بین خصیصه‌ها و شناساگرهای بدافزار، عملیات یا تحلیل‌های حمله ایجاد می‌کند. این ابزار، از یک پایگاه داده‌ی شناساگر استفاده می‌کند تا اطلاعات فنی و غیر فنی درباره‌ی نمونه‌های بدافزار، رخدادها، حمله‌کننده‌ها و هوش را ذخیره کند و همچنین یک تابع تسهیم را برای تسهیل تبادل داده‌ها با استفاده از مدل‌های توزیع گوناگون، به کار می‌گیرد.

۳. استفاده از زنجیره بلوکی برای رفع چالش‌های هوش تهدید سایبری

فن‌آوری زنجیره بلوکی این پتانسیل را دارد که بتواند در فرآیندهای سنتیِ مالی و تجاری، اختلال ایجاد نماید و هدف از آن، ایجاد شیوه‌هایی جدیدتر برای مبادله‌ی داده‌ها و ارائه‌ی سطح بالاتری از استقلال برای دارایی‌های داده‌ها هست. این امر از طریق ابزارهایی همچون پروتکل‌های رمزنگاری، مکانیسم‌های اجماع، استفاده از لایه‌ای که به‌منظور عدم انکار افزوده‌شده است و همچنین استفاده از خصوصیات تغییرناپذیری و خصوصیات امنیتی انجام می‌شود؛ یعنی ابزارهایی که فن‌آوری را به برنامه‌ی اشتراک‌گذاریِ هوش تهدید سایبری قرض می‌دهند [6].

انتخاب فن‌آوری زنجیره بلوکی به‌عنوان بستری برای اشتراک‌گذاری داده‌های سایبری، باوجود ویژگی‌های همچون حسابداری، مدیریت هویت، در دسترس بودن و امکان ایجاد و اجرای برنامه‌های غیرمتمرکز مانند قراردادهای هوشمند، می‌تواند تا حد زیادی چالش‌های موجود را رفع کند. در ادامه پژوهش‌های مرتبط در این حوزه معرفی می‌گردد.

ویژگی‌های زنجیره بلوکی و انجام معاملات به‌طور مستقیم و بدون واسطه و افزایش اعتماد و اطمینان بین طرف‌های درگیر در معاملات، باعث شده از این فن‌آوری برای بهبود آگاهی وضعیتی به‌خصوص در حوزه‌ی سایبری نیز استفاده شود. مدل مرجع آگاهی وضعیتی شامل ۴ مرحله‌ی "درک، فهم، پیش‌بینی و تصمیم" می‌باشد. بهبود درروند هر مرحله منجر به کسب آگاهی وضعیتی بهتر خواهد شد. در حوزه‌ی سایبری، اطلاع از تهدیدهای ممکن در شبکه و روش‌های مقابله با این تهدیدات اهمیت ویژه‌ای دارد (مرحله "درک"). همچنین حجم اطلاعاتی که در این خصوص وارد سازمان‌ها می‌شود زیاد است و جمع‌آوری، دسته‌بندی و رسیدگی به این اطلاعات، زمان زیادی نیاز دارد.

در چند سال اخیر چند پژوهش‌گر ارتقای آگاهی وضعیتی سایبری را با استفاده از قراردادهای هوشمند مورد بررسی قرار داده و دقت و عملکرد روش‌های ذکرشده در بهبود مراحل مختلف آگاهی وضعیتی را ارزیابی کرده‌اند. در مقاله‌ی شبکه‌های عصبی، بعد از تحلیل و دسته‌بندی گزارش‌های دریافتی، برای مدیریت چرخه زندگی گزارش‌ها، از قراردادهای هوشمند بر بستر پلتفرم اتریوم استفاده‌شده است. در دومین پژوهش، با استفاده از پروتکل TLP، اشتراک‌گذاری گزارش‌ها در کانال‌های خصوصی در هایپرلجر بررسی‌شده و در مقاله انگیزه‌های نامتمرکز برای گزارش دهی، از پلتفرم EOS برای ثبت‌نام، اشتراک‌گذاری، خرید و به‌طورکلی تمام اقدامات شبکه استفاده‌شده است.

[1] Collaborative Analysis Engine for The Situational Awareness and Incident Response (CAESAIR)
[2] Malware Information Sharing Platform (MISP)

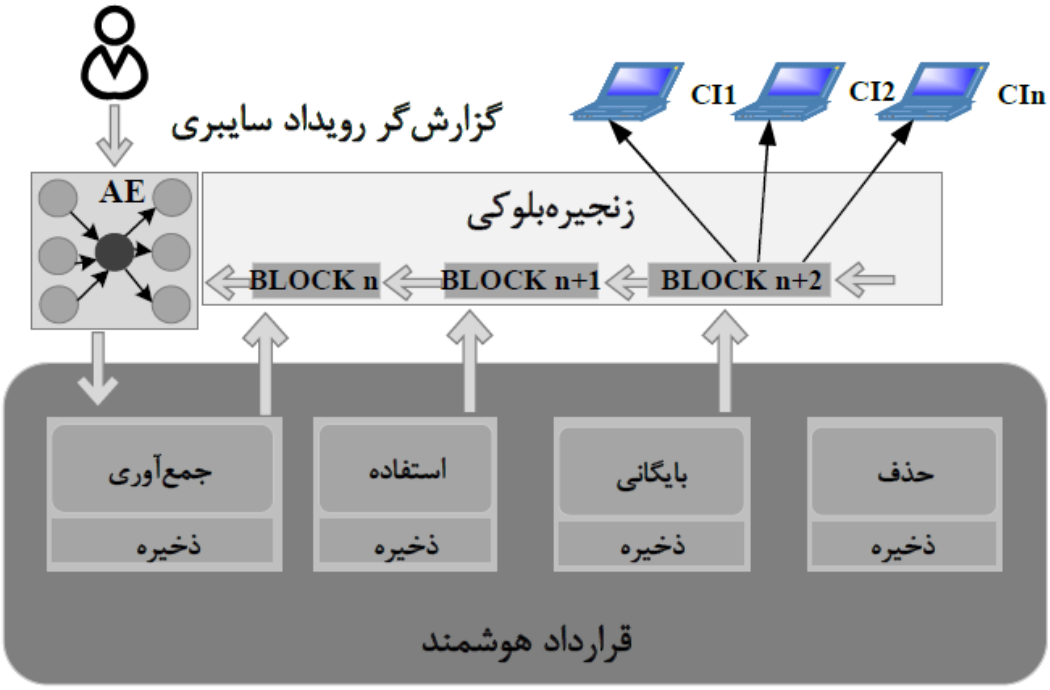
۳-۱- شبکه‌های عصبی و روش‌های مبتنی بر زنجیره بلوکی برای هوش تهدید سایبری و آگاهی موقعیتی

در سال ۲۰۱۸، رومن گراف و رأس کینگ[1] در [2]، طرحی را برای مدیریت رخدادها ارائه دادند. همان‌طوری که ذکر شد، تحلیل‌گران مرکز عملیات امنیتی روزانه حجم زیادی از گزارش‌های تهدید را دریافت می‌کنند و برای سازمان‌دهی این رخدادها دچار چالش‌هایی می‌شوند. تحقیق ارائه‌شده در این مقاله برای کمک به ایجاد سیستمی طراحی‌شده است که با تحلیل و دسته‌بندی رخدادهای سایبری ایجادشده از طریق جست‌وجو در رخدادهای سایبری مشابه، می‌تواند بر آگاهی وضعیتی سایبری اثر بگذارد و از طریق مدیریت چرخه‌ی زندگی رخداد، به‌صورت خودکار یک تحلیل‌گر سایبری را پشتیبانی خواهد کرد.

در این رویکرد، حملات سایبری تنها با توجه به سطح تهدیدشان دسته‌بندی می‌شوند. گزارش‌های رخدادهای سایبری جمع‌آوری، تحلیل و سپس منقضی می‌شوند. دسته‌بندی داده‌ها به یک شرکت یا مرکز عملیات امنیتی این امکان را می‌دهد که منابع خود را بر روی ارزشمندترین یا اضطراری‌ترین رخدادها متمرکز کند و به رخدادهای کم‌ارزش‌تر به‌صورت خودکار رسیدگی کند تا در زمان و سایر هزینه‌ها، صرفه‌جویی نماید.

در این سیستم تحلیل هوش تهدید سایبری، روند و دستورالعمل رسیدگی به رخدادها با استفاده از یک‌زبان برنامه‌نویسی قرارداد هوشمند (زبان سالیدیتی) توصیف‌شده است و قرارداد هوشمند ایجادشده در یک نمونه‌ی زنجیره بلوکی (یک شبکه‌ی خصوصی اتریوم) بارگذاری می‌شود. کد مبدأ این قرارداد هوشمند، قوانین و دستورها را تعریف می‌کند؛ برای این سیستم، قراردادهای هوشمند جمع‌آوری[2]، استفاده[3]، بایگانی[4] و حذف[5]، ایجادشده است (شکل ۱). وضعیت قراردادهای هوشمند بر روی زنجیره بلوکی ذخیره‌شده و برای تمام اعضای ثبت‌شده آشکار و قابل‌دسترسی است. کد قرارداد هوشمند به‌صورت موازی توسط شبکه‌ای از ماینرها و با توجه به الگوریتم اجماع، بر اساس خروجی اجرا می‌شود. اجرای قرارداد هوشمند منجر به به‌روزرسانی وضعیت آن قرارداد در زنجیره بلوکی می‌شود. گزارش رخدادی که توسط یکی از کاربران (متخصصان امنیت که از زیرساخت‌های حیاتی حفاظت می‌کنند) تولیدشده باشد در قرارداد هوشمند بررسی می‌شود و به‌صورت خودکار، با توجه به دستورات کد شده، به آن رسیدگی می‌شود.

[1] Roman Graf, Ross King
[2] Acquisition
[3] Use
[4] Archival
[5] Disposal



شکل ۱: استفاده از قردادهای هوشمند برای طبقه‌بندی اطلاعات و مدیریت چرخه زندگی [2]

تحلیل با یک گزارش رخداد سایبری آغازشده که توسط یکی از سهام‌داران در شبکه‌ی CI ایجادشده است. تحلیل رخداد می‌تواند برای مقادیر بزرگ داده‌ها با استفاده از یک پایگاه دانش[1] کامل و با به‌کاربردن یکی از ابزارهای تحلیل رخداد در دسترس، انجام شود.

۱. اجرای کار با خواندن گزارش رخداد و تجزیه محتوای گزارش آغاز می‌شود.
۲. داده‌های ورودی به همراه تنظیمات پروفایل فرد متخصص که به سازمان وابسته است، با استفاده از تکنیک کیسه‌ی کلمات[2] به یک بردار دو-دویی[3] تبدیل می‌شوند.
۳. در این گام داده‌ها نرمال‌سازی[4] می‌شوند.
۴. در فرمت کدگزاری‌شده[5] به خود رمزگذار[6] داده می‌شود.
۵. سپس کلمات با بیشترین تکرار در اسناد کامپایل شده است. بردار باقیمانده شامل تعداد کلمات صرف‌نظر از تکرارشان است. از یک شمارنده‌ی دو-دویی استفاده‌شده؛ اگر تعداد ظهور کلمه‌ای بیشتر از صفر بود، با ۱ و اگر کلمه‌ی داده‌شده در متن اصلی ظاهرنشده بود با 0 نشانه‌گذاری می‌شود. همچنین به کلمات توقف (کلماتی که هیچ قدرت تمایز کننده‌ای ندارند، مثلاً بندها و گزاره‌های رایج) توجه نمی‌شود. برای دست‌یابی به عملکرد و مقیاس‌پذیری معقول، هر بردار به یک بردار بسیار کوچک‌تر که همچنان شامل اطلاعات کافی راجع به محتوای سند است، کاهش می‌یابد.

[1] Knowledge Base (KB)
[2] Bag of Words
[3] Binary Vector
[4] Normalize
[5] Encode
[6] Auto Encoder (AE)

در گام بعدی، شبکه‌ی عصبی آموزش می‌بیند تا بردار ورودی خود را به‌عنوان بردار خروجی بازتولید کند. این کار شبکه را مجبور می‌کند تا حداکثر اطلاعاتی را که ممکن است در ۱۰ عدد در گلوگاه مرکزی فشرده کند. این ۱۰ عدد نتیجه‌ای از آموزش خود رمزگذار عمیق و روش خوبی برای مقایسه‌ی اسناد به‌صورت سریع و مقیاس‌پذیر با استفاده از روش تشابه کسینوس است.

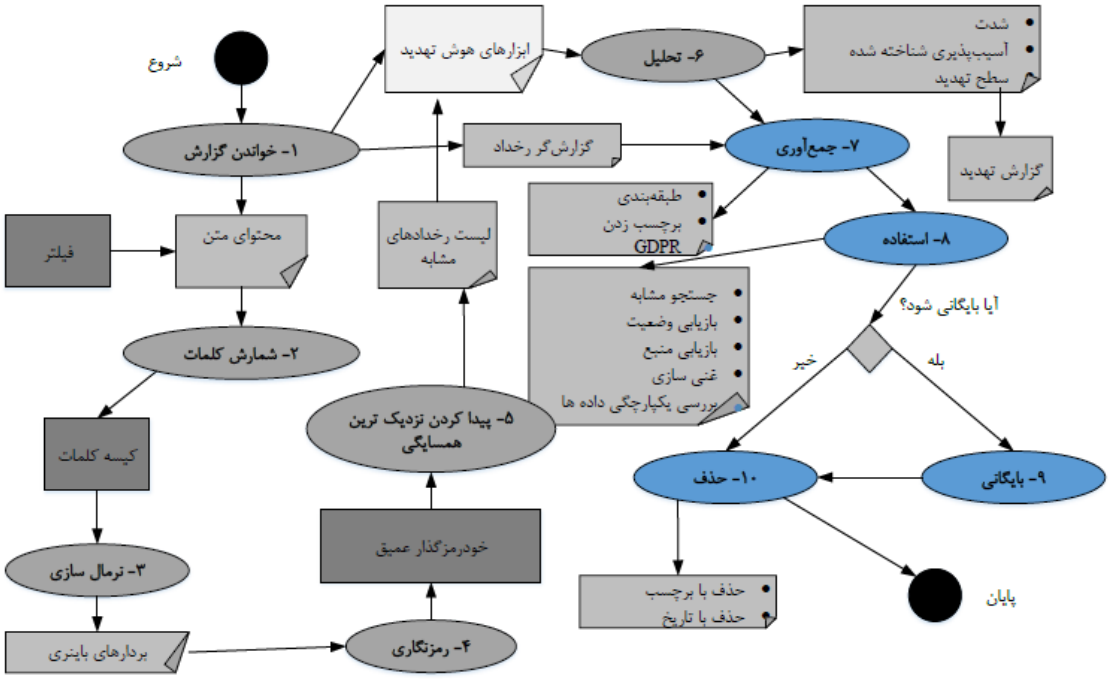
۶. در این مرحله، رخدادهای مرتبط تشخیص داده‌شده با تنظیمات مؤسسه‌ای ادغام می‌شود و طبق معادله (۱) سطح اولویت (مقدار 0 به نشانه‌ی کم بودن و یا ۱ به نشانه‌ی زیاد بودن) به رخداد داده‌شده اعمال می‌شود.

معادله‌ی (۱) سطح اولویت رخداد P را نشان می‌دهد که یا مقدار 0 به نشانه‌ی کم بودن و یا ۱ به نشانه‌ی زیاد بودن را برمی‌گرداند. سطح اولویت یک تابع از سنجه‌های[1] ارزیابی رخداد تجمیع است که به نشان‌گرهای پایه مانند تعداد رخدادهای مرتبط، I_r، تعداد کلمات مرتبط، W_r، تعداد کلمات اصلی، W_0، واژه‌های مهم تشخیص داده‌شده، T_s، و امتیاز آسیب‌پذیری، V_s، وابسته است.

$$P = (Ir,\ Wr,\ Wo,\ Ts,\ Vs) \qquad (۱)$$

در این بخش، کاربرد قراردادهای هوشمند برای دسته‌بندی و مدیریت گزارش رخدادهایی که به‌وسیله‌ی خود رمزگذار به‌عنوان تهدیدهای با اولویت بالا برچسب‌گذاری شده‌اند ارزیابی می‌شود. قراردادهای هوشمند می‌توانند برای موارد روبرو استفاده شود: تخمین زدن اینکه رخداد سایبری گزارش‌شده از اهمیت بالایی برخوردار است یا خیر، حذف آن بعد از گذشت مقداری از زمان که از پیش تعیین‌شده است، علامت‌گذاری آن با «به دست آمد»، جست‌وجو بر اساس علامت‌گذاری‌ها، اختصاص قوانین دسترسی (محرمانه، خصوصی، حساس، عمومی)، چک کردن جامعیت داده‌ها به‌صورت دوره‌ای (پیشگیری از مخدوش‌شدن به‌صورت دستی یا سخت‌افزاری) و تعیین منشأ داده‌ها. هدف صرفه‌جویی در فضای ذخیره، بهبود عملکرد و به‌روز نگه‌داشتن اطلاعات به‌صورت مطمئن و از طریق بهره‌مندی از طبیعت توزیع‌شده‌ی فن‌آوری زنجیره بلوکی است. هنگامی‌که یک قرارداد هوشمند فراخوانی می‌شود، نتیجه‌ی تحلیل به‌صورت خودکار و از طریق سازوکار ذاتی زنجیره بلوکی، بین تمام شرکت‌کنندگان پخش می‌شود.

[1] Metric



شکل ۲: جریان کار برای طبقه‌بندی و مدیریت چرخه زندگی حوادث سایبری با استفاده از خود رمزگذار عمیق و قراردادهای هوشمند [2]

همان‌طوری که در شکل ۲ دیده می‌شود، از چهار قرارداد هوشمند برای فرآیند رخداد سایبری استفاده شده است. جریان کار پس از مراحل دسته‌بندی که توسط خود رمزگذار انجام‌شده است، با تحلیل گزارش رخداد از طریق خواندن و تجزیه کردن محتوای گزارش که با نتایج دسته‌بندی غنی‌شده است، ادامه می‌یابد.

داده‌های ورودی به همراه تنظیمات مخصوص سازمانی برای پروفایل فرد متخصص به اولین قرارداد هوشمند که از یکی از ابزارهای هوش تهدید استفاده می‌کند، داده می‌شوند. دسته‌بندی با به‌کارگیری متن رخداد انجام می‌شود که در آن، متن به کلمات یا عبارت‌ها تقسیم می‌شوند و واژه‌های خاص به دسته‌های کم‌اهمیت، دارای اهمیت متوسط و بااهمیت جداسازی می‌شوند. نقاط ریسک از طریق تعداد واژه‌هایی که در گزارش رخداد برای هر سطح تهدید مشمول شده‌اند، محاسبه می‌شوند. برای محاسبه‌ی سطح تهدید، یا از طریق اعمال آستانه برای هر سطح، سطح تهدید را تخمین زده می‌شود و یا از روش وزن‌دار فرمول ۲ استفاده می‌کنیم که در آن نقاط محاسبه‌شده در هر سطح تهدید را در یک ضریب ثابت ضرب شده که نشان‌دهنده‌ی وزن سطح تهدید مربوطه است. مقیاس سطح تهدید بین ۱ تا ۳ است که در آن ۱ تهدید کم و ۳ تهدید شدید است. نقاط ریسک که با RP نشان داده‌ایم، جمع نقاط با ریسک بالا H_{rp} ضربدر وزن تهدید زیاد HT_w، نقاط با ریسک متوسط M_{rp} ضربدر وزن تهدید متوسط MT_w و نقاط با ریسک کم L_{rp} ضربدر وزن تهدید کم LT_w است.

$$RP = H_{rp} * HT_w + M_{rp} * MT_w + L_{rp} * LT_w \quad (۲)$$

Where $HT_w = 3, MT_w = 2\ and\ LT_w = 1.$

$$T_l = \begin{cases} 3(high) & if\ RP > HT_t, \\ 2(middle) & if\ RP > MT_t\ ,. \\ 1(low) & else\ RP \le MT_t \end{cases} \quad (۳)$$

Where$HT_t = 10\ and\ MT_t = 3.$

در عبارت بالا$HT_w = 3$، $MT_w = 2$، $LT_w = 1$ و $HT_t = 10$ و $MT_t = 3$ است. سطح تهدید T_1 می‌تواند با استفاده از آستانه‌های تهدید زیاد HT_t و تهدید متوسط MT_t و همچنین نقاط ریسک وزن‌دار RP از فرمول (۲) و (۳) بدست بیاید.

۷. گام جمع‌آوری به وظایف مختلفی تقسیم می‌شود. دسته‌بندی خودکار با توجه به سطح تهدید، یکی از سه سطوح تهدید را تعریف می‌کند: سطح «بالا» که نیازمند واکنش سریع و گام‌های میانی و فرآیند تریاژ است، سطح «متوسط» که در آن شناسایی شناساگر خرابی[1] یا سنجه‌هایی که آسیب‌پذیری‌های ممکن را شناسایی می‌کنند، فرض شده است و نیازمند به‌روزرسانی است، سطح «پایین» نیز اطلاعات و امنیت سایبری را هدف می‌گیرد و نیاز به توجه دارد اما لزوماً یک تهدید نیست. علامت‌گذاری به این معنی است که علامت‌های مشخص می‌توانند به یک گزارش اختصاص یابند تا باعث شوند آن گزارش راحت‌تر پیدا شوند، جابجا شوند و یا بعداً حذف شوند. ممکن است لازم باشد پیش از ذخیره‌سازی نسخه‌ی نرمال شده‌ی گزارش رخدادها، برای حفاظت از داده‌های شخصی، اطلاعات شخصی از آن‌ها حذف شوند (مقررات عمومی حفاظت از اطلاعات[2]).

۸. در گام استفاده، جریان کار از جست‌وجوی تشابه، بازیابی وضعیت و منبع به‌صورت خودکار و همچنین غنی‌سازی و بررسی دوره‌ای داده‌ها و فراداده‌ها به‌منظور جامعیت داده‌ها (با استفاده از چکیده گزارش رخداد) پشتیبانی می‌کند.

۹. در آخر، بسته به سطح تهدید پس از گذشت دوره‌ای از زمان، رخداد می‌تواند بایگانی (گام ۹) یا حذف شود، مثلاً با توجه به تاریخ یا علامت (گام ۱۰).

روش پیشنهادشده در این پژوهش، تحلیل آگاهی موقعیتی را کم‌هزینه‌تر می‌کند و با ظرفیت پذیرش بالاتری عمل خواهد کرد.

۳-۲- یک مدل شبکه‌ایِ جدید برای اشتراک‌گذاری هوش تهدید سایبری با استفاده از فن‌آوری زنجیره بلوکی

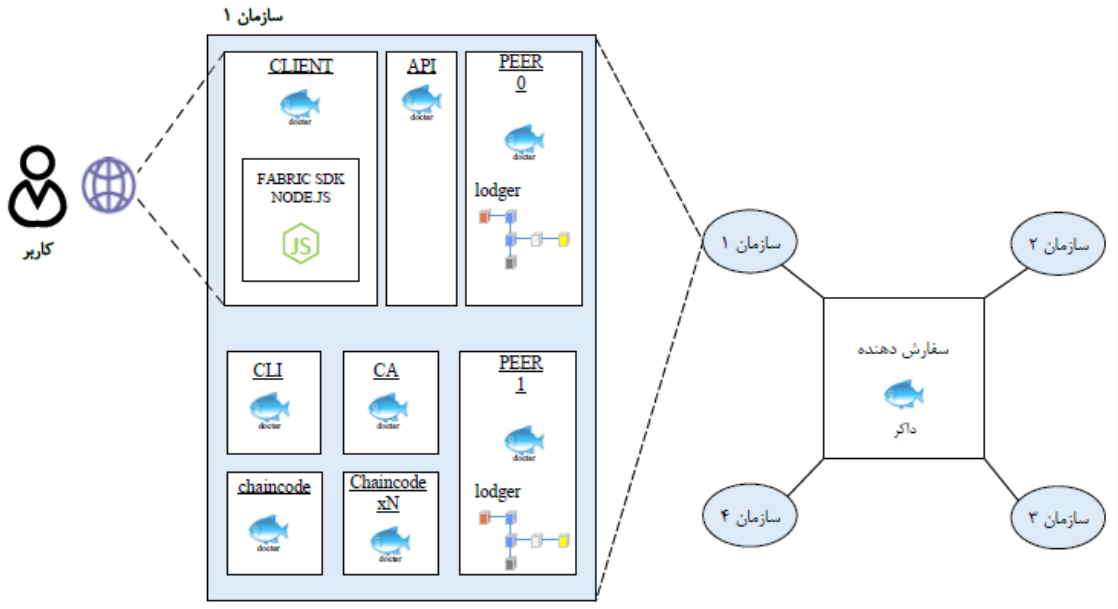
در سال ۲۰۱۹، دایر هومن، ایان شیل و کریستینا تورپ[3]، در [6]، مدل جدیدی برای اشتراک‌گذاری هوش تهدید سایبری طراحی و با استفاده از مشخصات و ابزارهای زنجیره بلوکی منبع باز هایپر لجر فابریک، پیاده‌سازی کردند که با استفاده از قابلیت‌های کانال فابریک، به یک بخش‌بندی موفقیت‌آمیز از شبکه دست‌یافت؛ بخش‌بندی که به جوامع و مشارکت‌کننده‌های معتبر این امکان را می‌دهد تا ضمن مشارکت در شبکه‌ی کلی، بتوانند داده‌های بسیار حساس را به‌صورت

[1] Indicator of Corruption (IOC)
[2] General Data Protection Regulation (GDPR)
[3] Daire Homan, Ian Shiel, Christina Thorpe

خصوصی میان خودشان توزیع کنند. پروتکل چراغ راهنمایی[1] همراه با کدهای زنجیره‌ای فابریک و همچنین قراردادهای هوشمند، برای اجرای قوانین اشتراک‌گذاری در شبکه مورداستفاده قرارگرفته است. این امر به‌منظور محافظت از مشارکت‌کنندگان در برابرِ اشتراک‌گذاری داده‌های بسیار حساس با مشارکت‌کنندگان نامعتبر، انجام‌شده است.

توپولوژی شبکه در شکل ۳ نشان داده‌شده است. همچنین شرکت‌کنندگان و کانال‌های فابریک طبق جدول ۱ و ۲ تعریف‌شده‌اند. کدهای زنجیره‌ای، بر اساس اطلاعات هوش تهدید سایبری که در داخل کانال‌ها منتشرشده‌اند و همچنین بر اساس پروتکل چراغ راهنمایی، قوانینی را تنظیم می‌کنند.

اگر یک شیء داده‌ی STIX شامل پروتکل TLP به‌صورت TLP:green باشد، آنگاه سبز بودنِ رنگ چراغ راهنمایی نشان‌دهنده‌ی این است که اطلاعات مجاز هستند تا آزادانه به اشتراک گذاشته شوند. پارامتر "tlp: green" نشان‌دهنده‌ی این است که دسترسی به این اطلاعات برای تمام مشارکت‌کنندگان رایگان است. "tlp: amber" نشان‌دهنده‌ی این است که این اطلاعات فقط باید در یک کانال خاص و صرفاً با افراد مجاز به اشتراک گذاشته شوند و پارامتر "tlp: red" نشان‌دهنده‌ی این است که این اطلاعات از حساسیت بالایی برخوردار هستند و فقط باید با اشخاص مجاز یا قابل‌اعتماد به اشتراک گذاشته شوند.



شکل ۳: توپولوژی شبکه [6]

مؤلفه‌های فیزیکی و محیطی تشکیل‌دهنده‌ی شبکه (طبق شکل ۳-۳ و توپولوژی شبکه) در ادامه آماده است:

۱. مؤلفه سفارش‌دهنده
۲. همتایان
۳. مرجع صدور گواهی (CA[2])

[1] Traffic Light Protocol (TLP)
[2] Certificate Authority

۴. کد زنجیره‌ای
۵. API[1]
۶. سرویس‌گیرنده (کلاینت)
۷. CLI[2]

جدول ۱. شرکت‌کنندگان [6]

Participants	
Org	**Description**
CSIRT-IE	Representing the national incident response team for Ireland.
CSIRT-UK	Representing the national incident response team for the United Kingdom.
CSIRT-BE	Representing the national incident response team for the Belgium.
PRIV-ORG	Representing a private commercial entity within the network.

جدول ۲: کانال‌های شبکه [6]

Channels		
Channel	**Participants**	**Description**
All-Chan	CSIRT-IE, CSIRT-UK, CSIRT-BE, PRIV-ORG	All participants have access.
CSIRT-Chan	CSIRT-IE, CSIRT-UK, CSIRT-BE	All Incident response teams have access.
EU-Chan	CSIRT-IE, CSIRT-BE	All European entities have access (for demonstration purposes CSIRT-UK will be omitted from this channel).
Priv-Chan	CSIRT-IE, PRIV-ORG	Private channel between a private organisation and another public organisation they are in partnership with.

در این پژوهش نشان داده‌شده که شاخص سازش (IOC) در یک شبکه زنجیره بلوکی (بر اساس میزان حساسیت داده، در جامعه‌ی قابل‌اعتماد و حتی بین ۲ یا چند سازمان خاص)، به اشتراک گذاشته‌شده است و هر یک از مشارکت‌کنندگان به داده‌های STIX[3] موجود در دفتر کل خود دسترسی دارند. علاوه بر این، در مورد داده‌های حساس یا بسیار حساس، سازمان-هایی که در این کانال مشارکت نمی‌کنند نمی‌توانند این قالب‌های داده را مشاهده کرده و یا بر روی آن‌ها کوئری اجرا کنند.

[1] Application Programming Interface
[2] Command-line interface
[3] Structured Threat Information Expression (STIX)

۳-۳- سامانه‌های غیرمتمرکز برای گزارش دهی هوش تهدید و تبادل اطلاعات

در سال ۲۰۲۰، فلوریان منگز، بندیکت پوتز، گونتر پرنول[1]، در [3] پلتفرم DEALER[2] را برای اشتراک‌گذاری CTI معرفی کردند. در این پروژه، تبادل اطلاعات هوش تهدید سایبری به دو حوزه‌ی مختلف تقسیم می‌شود: گزارش دهی اجباری و تبادل اطلاعات CTI انگیزه محور، همچنین ترکیبی از هر دو روش باید به‌صورت اختیاری امکان‌پذیر باشد.

در گزارش دهی متعهدانه رویدادهای امنیتی، مواردی از قبیل نظارت بر دسترسی مناسب عامل اصلی به داده‌ها، اثبات ارسال‌کننده گزارش و اطمینان از صحت داده موردنظر هستند. هر تبادل اطلاعات در مورد رویدادهای امنیتی با ریسک‌های متعددی همراه است. ممکن است اطلاعات زیرساخت شرکت یا مسائل مهم شرکت منتشر شود و حملات به آن شرکت را تسهیل کند. همچنین هزینه‌های گزارش دهی شامل گردآوری، پردازش و استفاده از داده مربوطه نیز منجر به کاهش انگیزه برای گزارش دهی متعهدانه شده است. از طرفی مزیت‌های مشارکت در پلتفرم تبادل داده اغلب مواقع به‌سختی تعیین می‌شوند، به‌خصوص با جرائم قانونی نسبتاً کم برای گزارش‌های حذف‌شده. از این نکات می‌توان نتیجه گرفت که شرکت‌ها دارای انگیزه ذاتی کمتری برای گزارش رویدادهای خود هستند، درحالی‌که انگیزه برای استفاده از اطلاعات از پلتفرم گزارش دهی احتمال دارد که زیاد باشد. درنتیجه، یک سیستم انگیزه محور که هر فرد را در چنین پلتفرمی تشویق می‌کند که فعالانه مشارکت کند می‌تواند به‌عنوان شرط ضروری دیگری برای عملکرد پایدار چنین پلتفرمی عمل کند.

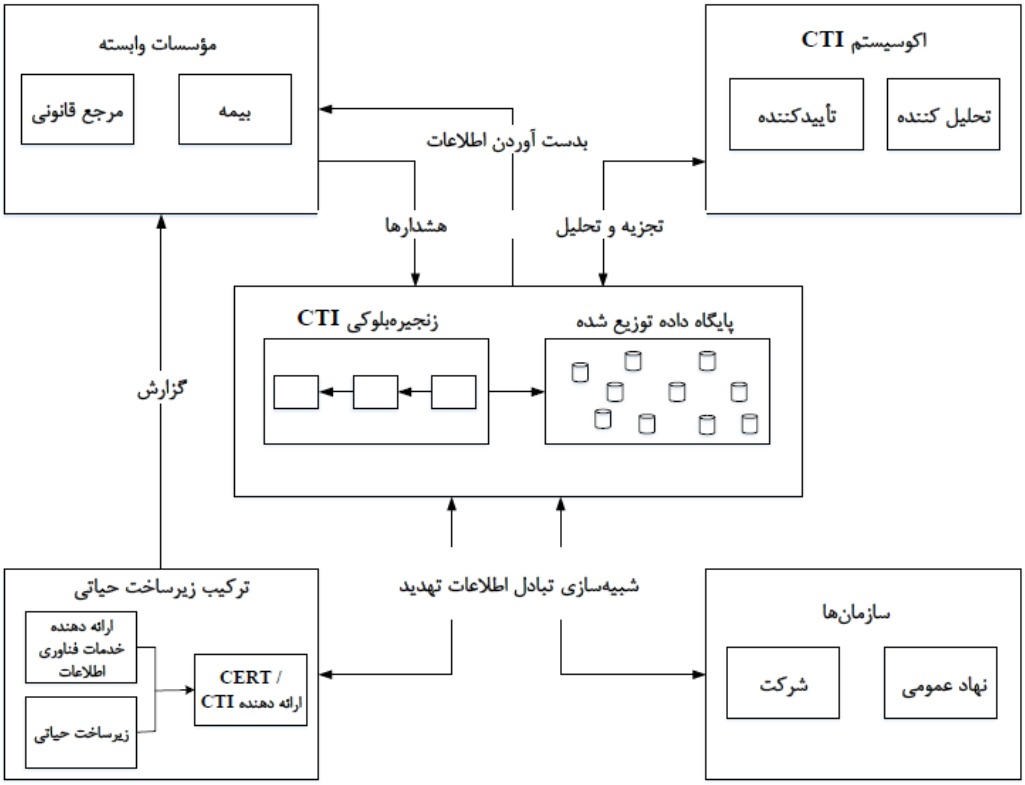
سیستم DEALER یک سیستم انگیزه محور است که مشخصات آن به شرح زیر خواهد بود:

۱) مؤلفه‌های اصلی سیستم DEALER

همان‌طوری که در شکل ۴ نشان داده‌شده سیستم DEALER شامل مؤلفه‌های زیر هست:

- مرکز سیستم: زنجیره بلوکی و یک دیتابیس پراکنده (IPFS)
- نقطه آغاز ترکیب‌های زیرساخت اصلی شامل: زیرساخت حیاتی، تأمین‌کننده خدمات IT، تأمین‌کننده CTI
- تأمین اطلاعات برای سازمان‌ها یا مؤسسات مربوطه: مرجعیت قانونی، مراکز بیمه و شرکت‌ها و مراکز عمومی علاقه‌مند به مشارکت
- اکوسیستم CTI: فراهم نمودن تحلیل‌ها و خدمات در سیستم

[1] Florian Menges, Benedikt Putz, Günther Pernul
[2] **D**ecentralized Inc**E**ntives for Thre**A**t Inte**L**lig**E**nce **R**eporting and Exchange



شکل ۴: مفهوم اشتراک‌گذاری هوش تهدید در پلتفرم DEALER [3]

۲) مفهوم کلی DEALER:

- گزارش دهی رویداد قانونی: داده‌های منتقل‌شده گردآوری می‌شوند و به شکلی رمز می‌شوند که فقط مقام دریافت-کننده می‌تواند به آن دسترسی یابد.
- تبادل اطلاعات مبتنی بر انگیزه: افراد می‌توانند اطلاعات را پیشنهاد دهند و در مورد رویدادهای امنیتی آن‌ها را تقاضا کنند.

بخش‌های اصلی پلتفرم شامل سه مؤلفه‌ی اصلی است: قرارداد هوشمند روی زنجیره بلوکی EOS بر اساس کد C++، منبع ذخیره داده IPFS و DAPP.

طی پنج فرآیند اصلی ثبت‌نام، اشتراک‌گذاری، خرید، تأیید و عادلانگی، اعضای پلتفرم می‌توانند داده‌های خود را با بقیه اعضا به اشتراک بگذارند. همان‌طوری که پیش‌ازاین ذکر شد اشتراک‌گذاری در این پلتفرم به‌صورت متعهدانه و یا انگیزه محور خواهد بود. هر عضو یا سازمان بعد از دریافت تهدید و اعمال فرآیندهای لازم، گزارش تهدید را در پلتفرم DEALER منتشر کند.

۳) فرآیندهای اصلی مربوط به پلتفرم:

- **ثبت‌نام:**

ابتدا افراد باید ثبت‌نام کنند تا قادر باشند روی بازار نامتمرکز فعالیت کنند. هر فرد دارای حساب با مقداری توکن است که ممکن است در تجارت‌ها از آن‌ها استفاده شود. برای جلوگیری از حملات مربوط به این بخش، نیازمند توکن ثابت اولیه Si هستیم تا حسابی برای کاربر بسازیم. حساب کاربر توسط پلتفرم مدیریت می‌شود.

تأیید کنندگان به‌صورت جداگانه در زمان ثبت‌نام موردبررسی قرار می‌گیرند (توسط توسعه‌دهنده پلتفرم)، زیرابه آن‌ها

دسترسی رایگان به اطلاعات رویداد داده‌شده است و باید آن را به‌روز کنند. تأیید کنندگان مناسب می‌توانند به‌عنوان‌مثال فروشندگان داده‌های CTI، CERT ها یا متخصصین فعالیت‌های امنیتی باشند.

✓ هدف تأیید کنندگان:

- جلوگیری از سوءاستفاده
- اطمینان از علاقه ذاتی به تحلیل رویدادهای امنیتی و داشتن تخصص فنی لازم برای ارزیابی اطلاعات رویداد

▪ **اشتراک‌گذاری:**

فرآیند اشتراک‌گذاری در شکل ۵ نشان داده‌شده است و شامل مراحل زیر می‌باشد:

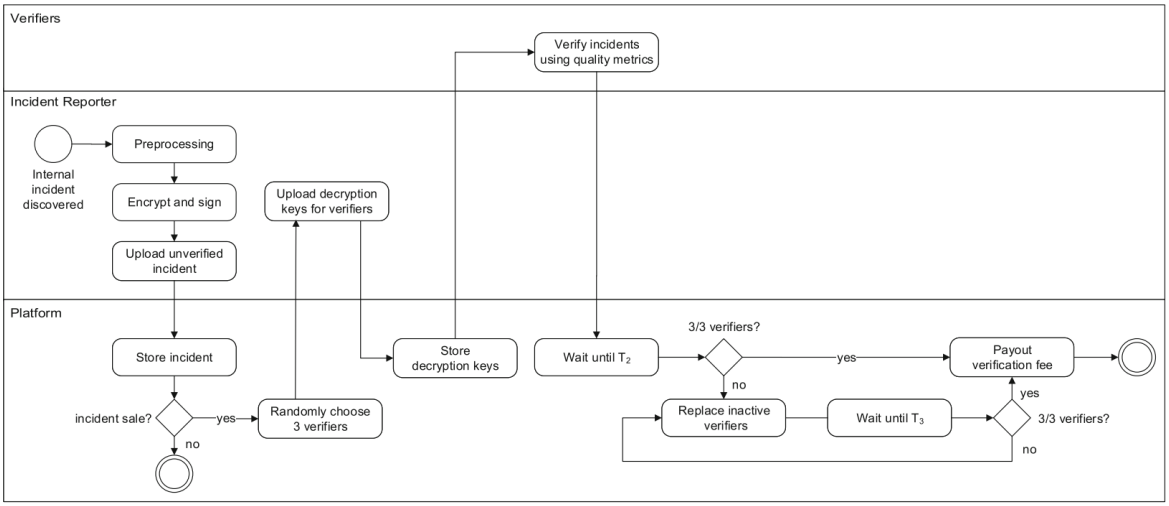
➢ شناسایی رویداد
➢ بارگذاری داده
➢ تأیید
➢ بررسی در پلتفرم

مراحل ذکرشده با جزئیات شرح داده می‌شود:

۱. پردازش اولیه: حذف داده‌های شخصی از رویدادها و رمزنگاری با کلید k
۲. اختصاص قیمت فروش Ps به Metadata
۳. ارسال تراکنش امضاشده به پلتفرم
۴. پرداخت مبلغ تأیید Pv برای فروش رویداد توسط فروشنده ($Pv = 0.6\ Ps$)
۵. انتخاب ۳ تأییدکننده تصادفی و ارسال ۳ کلید K_{v1}, K_{v2}, K_{v3} برای تأیید کننده‌ها توسط فروشنده (کلیدها توسط کلید عمومی هر تأییدکننده رمز شده است و پلتفرم را در زمان $T1$ مطلع می‌سازد.)
۶. تأیید کنندگان رویداد بارگذاری شده را توسط کلید خصوصی خود رمزگشایی و بازیابی کرده و مقدار اولیه را در پلتفرم تخصیص می‌دهند.
۷. اگر همه‌ی نتایج تا زمان $T2$ دریافت شوند، مبلغ تأیید Pv بین تأیید کنندگان به‌طور برابر تقسیم می‌شود.

*اگر تا زمان $T3$ رویداد تأیید نشود ممکن است از پلتفرم حذف شود و به ازای هر تأییدکننده‌ای که پاسخ نداده، مبلغ برگشت داده می‌شود.

*برای موارد محرمانه ممکن است تأییدکننده‌ای نباشد و فقط یک کلید برای مقام مربوطه بارگذاری شود.



شکل ۵: اشتراک‌گذاری داده‌های CTI در پلتفرم DEALER [3]

- **تأیید:**

✓ تأیید کیفیت داده (از ۱ تا ۵) برای کنترل رویداد و تهیه فایل راهنمای خریداران

✓ موارد زیر به‌عنوان راهنمای تأیید عمل می‌کنند:

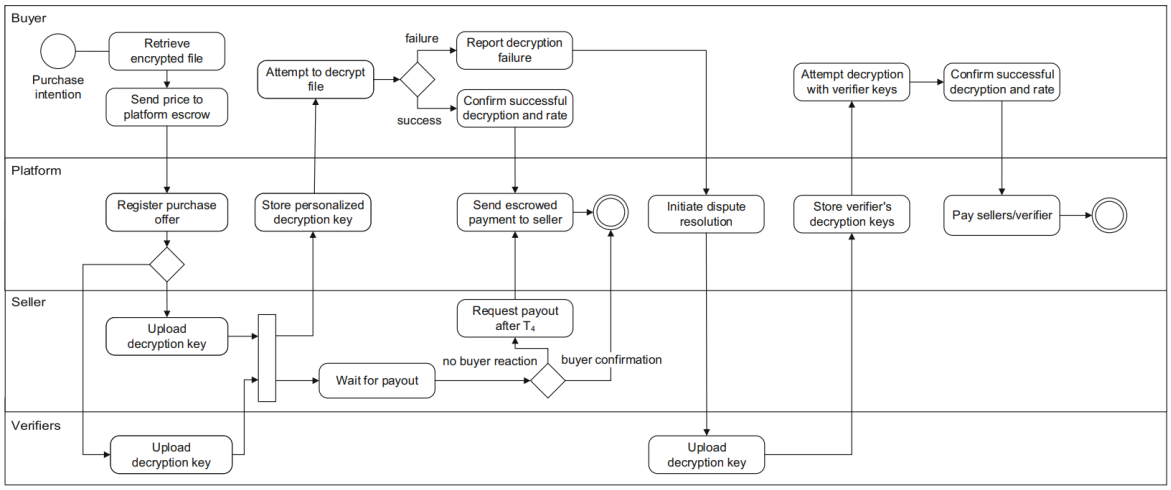
۱. سازگاری با داده‌های مربوط به رویدادهای قبلی فروشنده (بررسی یکپارچگی داده)
۲. بررسی شباهت داده‌ها و رویدادهای تأییدشده (جلوگیری از تکرار)
۳. ارزیابی شاخص‌های کیفیت هوشمند متعدد (سه دامنه اصلی شرایط کیفی)

- اطلاعات مربوط به داده‌های موجود: نمایش دقیق اطلاعات ذخیره‌شده
- نمایش شیء درداده: مرتبط بودن داده ذخیره‌شده در خصوص موقعیت شرح داده‌شده
- کامل بودن اطلاعات در دسترس: بررسی اینکه آیا مقدار مناسبی از داده‌ها برای نمایش وقایع استفاده‌شده است یا خیر

- **خرید:**

خرید رویداد در فرآیند شکل ۶ با خریدار بالقوه‌ای آغاز می‌شود که رویدادهای بارگذاری شده قبلی را بررسی می‌کند. بدین منظور بخش ظاهری پلتفرم، جستجوی هوشمند را پیشنهاد می‌کند و بخش دستی را فیلتر می‌کند.

۱. بازیابی رویداد رمز شده برای تأیید در دسترس بودن آن توسط خریدار
۲. پرداخت توکن باقیمت فروش Ps به پلتفرم
۳. ثبت یا بارگذاری پیشنهاد خرید
۴. انتشار کلید رمزگشایی توسط فروشنده یا تأیید کنندگان
۵. درصورتی‌که رمزگشایی موفق داشته باشیم، خریدار پلتفرم را با ارسال پیام تأیید به همراه رتبه‌بندی رویداد آگاه می‌سازد.
۶. اگر رمزگشایی انجام نشود، خریدار پلتفرم را درباره خطا آگاه می‌سازد که فرآیند حل اختلاف را آغاز می‌کند.
۷. شروع فرآیند حل اختلاف
۸. بارگذاری کلیدها توسط تأیید کنندگان دیگر (Pd به‌عنوان پاداش، این مبلغ از قیمت فروش کم می‌شود جهت جریمه فروشندگان ناصادق $Pd \sim 0.10\ Ps$ <<<)
۹. درصورتی‌که عدم پاسخگویی خریدار تا زمان $T4$، فروشنده توکن های خود را پس می‌گیرد.



شکل ۶: خرید داده‌های CTI در پلتفرم DEALER [3]

- **عدالت:**

همیشه حداقل یک تأییدکننده صادق وجود دارد که کلید رمزنگاری معتبر را ارائه می‌کند.

✓ عادل بودن فروشنده

۱. احتمال اینکه خریدار بعد از دریافت کلید با پاسخ ندادن تقلب کند، بعد از زمان $T4$، فروشنده درصورتی‌که عدم دریافت پاسخ خریدار، هزینه را پس می‌گیرد.
۲. خریدار انگیزه‌ای برای ارائه گزارش نادرست در مورد رفتار نامناسب فروشنده ندارد.
۳. اگر با تأیید ارتباط برقرار نشود، بازهم خریدار نمی‌تواند توکن‌های پرداختی را پس بگیرد.

✓ عادل بودن خریدار

۱. خریدار همیشه کلید رمزگشایی را دریافت می‌کند. حتی اگر فروشنده تلاش کند با انتشار کلید نادرست تقلب کند، خریدار با ایجاد فرآیند حل اختلاف، کلید صحیح را از تأیید کننده‌ها دریافت می‌کند.
۲. امکان اینکه فروشنده و تأیید کننده‌ها همه کلید نادرست ارسال کنند، بر اساس ۲ ویژگی زیر وجود ندارد:

- تخصیص تصادفی تأیید کننده‌ها برای رویدادهایی که احتمال هماهنگ شدن فروشنده-خریدار را کم می‌کنند و ساختارهای انحصاری تکراری و زمان‌بر هستند.
- رفتار نامناسب از طریق شرایط ثبت نامی شناسایی می‌شود که در راستای احتمال حذف شدن است.

در این پلتفرم با توجه به ایجاد انگیزه مالی و تبادل اطلاعات، میزان به اشتراک‌گذاری CTI بالا می‌رود. همچنین با توجه به این‌که روی زنجیره بلوکی می‌باشد اطمینان و اعتماد در شبکه بالاست.

۴. نتیجه‌گیری و پیشنهادها

در این مقاله، لزوم توجه به آگاهی وضعیتی سایبری و چالش‌های پیش روی به اشتراک‌گذاری داده‌های هوش تهدید بررسی شد. سپس مروری بر پژوهش‌های صورت گرفته جهت رفع این چالش‌ها انجام شد. همان‌طور که در بخش ۳-۶ و کارهای انجام‌شده عنوان شد، استفاده از زنجیره بلوکی به‌عنوان بستری امن برای اشتراک‌گذاری داده‌های CTI و نیز ایجاد انگیزه و اعتماد، منجر به ارتقای هوش تهدید سایبری می‌شود. همچنین با توجه به حجم بالای داده‌های CTI دریافتی، استفاده از قراردادهای هوشمند به دسته‌بندی این داده‌ها و درنهایت به تصمیم‌گیری سریع و درست در صورت وقوع تهدید کمک می‌کند.

طرح‌های معرفی‌شده در کنار مزایایی که ایجاد کرده همچنان با چالش‌هایی مواجه است. در طرح ارائه‌شده توسط دایر هومن، ایان شیل و کریستینا تورپ در [6]، مدل اشتراک‌گذاری اطلاعات با استفاده از پروتکل TLP روی هایپرلجر که یک زنجیره خصوصی می‌باشد ارائه‌شده است که بر اساس تگ داده، اشتراک‌گذاری در کانال‌های خاص صورت می‌گیرد. ولی در این طرح انگیزه لازم برای اشتراک‌گذاری داده‌ها وجود ندارد. درنتیجه نیاز به پلتفرمی برای اشتراک‌گذاری با هزینه اندک ولی باانگیزه به دست آوردن سود مالی و اطلاعات هست مشابه طرحی که در مقاله [3]، معرفی شد

در طرح ارائه‌شده توسط رومن گراف و راس کینگ در [2] و استفاده از خود رمزگذار عمیق برای دسته‌بندی گزارش‌ها بر اساس سطح تهدید، از پلتفرم اتریوم استفاده‌شده است. زنجیره بلوکی اتریوم همانند زنجیره بلوکی EOS عمومی هست ولی اتریوم و EOS تفاوت‌های عمده‌ای دارند که در جدول ۳ آمده است.

در اتریوم با توجه به سازوکار اثبات کار برای تأیید بلوک‌ها، حدود ۱۰ تا ۲۰ تراکنش در ثانیه تأیید می‌شود ولی در EOS، مکانیسم اجماع بر اساس اثبات سهام است که باعث می‌شود توافق زودتر در شبکه ایجاد شود و مقیاس‌پذیری بالا رود. در EOS تعداد تراکنش‌هایی که در مدت یک ثانیه تأیید می‌شود بالای ۴۰۰۰ می‌باشد و پیش‌بینی‌شده این عدد به ۱ میلیون تراکنش در ثانیه نیز برسد. همچنین در اتریوم برای تأیید تراکنش‌ها باید هزینه گس پرداخت شود و اگر تعداد تراکنش‌ها در

شبکه بالا باشد تأیید تراکنش‌ها در مدت کمتر به میزان گس بستگی دارد. در EOS هزینه تراکنش تقریباً رایگان است و مدت‌زمان تأیید تراکنش بین ۱ تا ۲ ثانیه می‌باشد. این مقایسه برتری EOS بر اتریوم را در انجام حجم بالای تراکنش‌ها و کارمزد کم نشان می‌دهد.

یکی از مواردی که می‌تواند در بالا رفتن میزان اشتراک‌گذاری تأثیرگذار باشد، عمومی بودن زنجیره بلوکی است ولی این ویژگی می‌تواند منجر به سوءاستفاده در شبکه نیز شود.

در طرح DEALER، بعد از گزارش رویداد، سه تأییدکننده تصادفی انتخاب می‌شوند که به اطلاعات کامل رویداد دسترسی رایگان دارند. از طرفی در سازمان‌های حساس، بهتر است به دلیل مسائل امنیتی گزارش تهدید به‌صورت خصوصی و فقط بین شرکت‌های از پیش تعیین‌شده منتشر شود.

در این طرح استفاده از هایپرلجر به‌عنوان زنجیره بلوکی کنسرسیوم بررسی‌شده و به دلایلی استفاده از آن مقدور نبوده است. این موانع شامل از دست رفتن حمایت توکن اصلی، عدم وجود ابزار برای تبادل توکن‌ها برای واحد مالی موردنظر و مانعی برای ورود بود. نتایج بعدی برای هزینه‌های اولیه بالا و هزینه‌های تعمیرات برای به‌روزرسانی‌ها و نظارت بودند، درحالی‌که در دسترس بودن به دلیل تعداد محدود گره‌های زنجیره بلوکی کمتر است. زنجیره بلوکی عمومی توسط ماینرهای مستقلی عمل می‌کنند که از طریق پاداش‌هایی که توسط پروتکل اصلی دریافت می‌کنند انگیزه می‌گیرند؛ بنابراین زیرساخت زنجیره بلوکی از قبل در دسترس است، اما دستمزدهای تراکنش باید به سازندگان پلتفرم پرداخت شوند. همچنین زنجیره بلوکی عمومی تعداد زیادی از گره‌های پراکنده را فراهم می‌کنند که دسترسی بالا را ممکن می‌سازند، درحالی‌که پراکندگی توکن را می‌توان با استفاده مشخص از معاملات کنونی کنترل کرد.

فضای ذخیره‌سازی EOS.IO یک پلتفرم برای میزبانی داده‌های عمومی است. کاربرانی که نیاز به حریم خصوصی دارند ممکن است از یک الگوریتم ذخیره‌سازی پیش از آپلود کردن فایل‌هایشان استفاده کنند. درحالی‌که محتوای فایل رمزگذاری شده خواهد بود، هویت حساب زنجیره بلوکی که فایل را آپلود کرده است برای همه قابل‌مشاهده خواهد بود [3]. با توجه به دسترسی بالا و ایجاد انگیزه دریافت پاداش، در طرح ارائه‌شده در مقاله DEALER از زنجیره عمومی استفاده‌شده است ولی مشکل محرمانه ماندن اطلاعات همچنان وجود دارد و پژوهش‌های آتی با هدف رفع این چالش‌ها و ارائه‌ی مدلی برای اشتراک‌گذاری امن داده‌های CTI خواهد بود.

جدول ۳: مقایسه زنجیره بلوکی اتریوم و EOS

نام ارز دیجیتال	اتریوم (ETH)	ایاس (EOS)
مکانیزم شبکه	گواهی اثبات کار (PoW)	گواهی اثبات سهام محول شده (DPoS)
ارزش بازار	۴۴۱ میلیارد دلار	۵.۰۳ میلیارد دلار
عرضه کل	۱۱۷,۳۵۲,۴۳۱ میلیون ETH	۱,۰۳۳,۰۸۹,۵۴۱ میلیارد EOS
تاریخ ساخت	جولای سال ۲۰۱۵ میلادی	ژوئن سال ۲۰۱۷ میلادی
تیم توسعه دهنده	Ethereum Foundation	Block.one
کارمزد تراکنش ها	متغیر (بستگی به شلوغی شبکه دارد)	رایگان
هزینه های سالیانه شبکه	۱۱ درصد که صرف هزینه های برق می‌شود	۵ درصد که صرف توسعه شبکه می‌شود
زمان لازم برای تایید یک تراکنش	۵ تا ۴۰ ثانیه	۱.۵ ثانیه
پهنای باند شبکه	۱۰ تراکنش در ثانیه (TPS)	بیش از ۳۰۰ هزار تراکنش در ثانیه (TPS)

۵. فهرست مراجع

[۱] علی جبار رشیدی، کوروش داداش تبار احمدی و بهزاد نظر پور؛ آگاهی وضعیتی سایبری، دانشگاه صنعتی مالک اشتر.

[2] Graf, Roman, and Ross King. "Neural network and blockchain based technique for cyber threat intelligence and situational awareness." 2018 10th International Conference on Cyber Conflict (CyCon). IEEE, 2018.

[3] Menges, Florian, Benedikt Putz, and Günther Pernul. "DEALER: decentralized incentives for threat intelligence reporting and exchange." International Journal of Information Security 20.5 (2021): 741-761.

[4] Riesco, Raúl, Xavier Larriva-Novo, and Víctor A. Villagrá. "Cybersecurity threat intelligence knowledge exchange based on blockchain." Telecommunication Systems 73.2 (2020): 259-288.

[5] Barford, Paul, et al. "Cyber SA: Situational awareness for cyber defense." Cyber situational awareness. Springer, Boston, MA, 2010. 3-13.

[6] Homan, Daire, Ian Shiel, and Christina Thorpe. "A New Network Model for Cyber Threat Intelligence Sharing using Blockchain Technology." 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2019.