مطالعات مهندسی صنایع و مدیریت تولید

دوره ۸، شماره ۱، بهار ۱۴۰۱

صفحات ۲۳۰- ۲۱۹

Online ISSN: ٢٤٧٦-٤٣٧X

Print ISSN: ٢٥٣٨-٢٠٦٣

www.irijournals.com

فناوری کنترل دستیابی به شبکه هوشمند فاقد مرز با در نظر گرفتن وضعیت امنیت شبکه‌ای

محمد باروت کوب

کارشناسی ارشد مکاترونیک دانشگاه آزاد اسلامی واحد اهر

چکیده

توسعه سریع تولید انرژی جدید، گسترش دامنه کنترل سیستم نظارت بر قدرت، ساختار پیچیده‌تر، اقدامات حفاظتی موجود برای مقاومت در برابر حملات شبکه پیچیده دشوار است. در مطالعه ما یک فناوری کنترل دستیابی فاقد مرز بر اساس وضعیت امنیت شبکه‌ای هوشمند پیشنهاد کرده‌ایم. بر اساس مکانیزم اعتماد صفر، پیش‌تشخیص کد مخرب درهم‌سازی پویا چند عاملی سخت‌افزار پیشنهاد شده است و مدل رفتار غیرعادی و تمیز کردن هوشمند ابرداده‌های شبکه چند بعدی مبتنی بر داده‌کاوی عمیق و تجزیه و تحلیل نمودار ایجاد می‌شود که دقت را بهبود می‌بخشد. مکان ترافیک غیرعادی، ردیابی و قابلیت ردیابی است و دقت آن به ۹۷. ۷۴ درصد می‌رسد.

واژه‌های کلیدی: آگاهی موقعیتی، امنیت شبکه‌ای، شبکه هوشمند، کنترل دستیابی فاقد مرز.

مقدمه

توسعه سریع تولید انرژی جدید، گسترش دامنه کنترل سیستم نظارت بر قدرت، ساختار پیچیده‌تر، اقدامات حفاظتی موجود برای مقاومت در برابر حملات شبکه پیچیده دشوار است. ما محاسبه جریان کامل و استراتژی پیش‌انسداد را برای تحلیل رفتار کاربر شرکت‌های شبکه برق طراحی کردیم و روش تجزیه و تحلیل رفتار موجودیت شبکه و روش تشخیص افزونگی داده‌ها را بر اساس تجزیه و تحلیل گراف و داده‌کاوی عمیق پیشنهاد کردیم. معماری امنیتی شبکه تطبیقی و تحقیقات اطلاعات ترافیکی و پیش انسداد محقق شده است و میانگین دقت تحلیل رفتار فیزیکی بیش از ۹۰٪ است. از ابعاد جمع آوری داده ها، تشخیص، تجزیه و تحلیل، طراحی فن آوری تجزیه و تحلیل چند انجمنی ناهنجاری پیچیده مبتنی بر چند بعدی، همراه با ویژگی های رفتار کاربر و ویژگی های تجاری شرکت های شبکه برق، تحقیق جریان و استراتژی پیش انسداد را مطرح می کند. تجزیه و تحلیل رفتار کاربر شرکت های شبکه برق، از طریق استخراج ویژگی های ابزار، ویژگی های اثر انگشت، قانون هدف، قانون زمان و سایر اطلاعات، رفتار موجودیت شبکه داده کاوی عمیق، تجزیه و تحلیل تصویر چند بعدی جامع از منابع حمله مشکوک، از یک طرف،، برای برچسب زدن منابع حمله. از سوی دیگر، برای تحلیل محاسباتی امتیازدهی تهدید استفاده می شود. از طریق فناوری تشخیص چند پایه، فناوری خوشه‌بندی بدون نظارت، و تحلیل همبستگی مبتنی بر نمودار، از ابعاد چندگانه برای تشخیص رفتار غیرعادی، تجزیه و تحلیل مسیر حمله، تعیین محل منبع واقعی حمله، دستیابی به معماری امنیتی شبکه تطبیقی و تحقیقات اطلاعات ترافیکی و پیش انسداد

برخی از مدل ها در تحقیقات حاضر ارائه شده است. Koudai Hatakeyama پیشنهاد می‌کند که مدل مرزی کنترل دسترسی را برای محافظت از منابع شبکه، با استفاده از شبکه منبع درخواست‌های دسترسی به عنوان یکی از عوامل کلیدی برای تصمیم‌گیری مجوز، فراهم می‌کند. این استراتژی با محو شدن روزافزون مرزهای شبکه شبکه هوشمند [۱] پشتیبانی خواهد شد. Mauro Lemus Alarcon استدلال می کند که عدم اعتماد ذاتی بین حافظان داده و مصرف کنندگان/کاربران داده ها منجر به یک روش کارگزاری کاملاً دستی و صادقانه برای دسترسی و پردازش داده های محافظت شده شده است. این رویکرد دستی منجر به پردازش داده‌ها کندتر می‌شود و سربار مورد نیاز برای پرداختن به اطمینان مورد نیاز برای شنیدن داده‌ها و انطباق با استانداردهای امنیت داده را افزایش می‌دهد [۲]. جینگ‌هوی لی استدلال می‌کند که اعتماد و اعتبار همیشه کلیدواژه‌های محاسباتی و ارتباطات بوده‌اند. با این حال، تحقیقات کمی برای بررسی تعاریف آنها و نحوه طراحی سیستم های قابل اعتماد وجود دارد. Jinghui Li جنبه های مختلف اعتماد مورد استفاده در رشته های مختلف را بررسی می کند [۳].
Abhishek Kumar استدلال می‌کند که داده‌های رفتار کاربر برای فناوری کنترل دسترسی قابل توجه است. نیکلاس هاندجا پیشنهاد می‌کند که با رایج‌تر شدن ادراک گروهی، آن‌ها به اهداف مکرر تبدیل می‌شوند. جلوگیری از حملات به سیستم های تشویقی دشوار است زیرا مهاجمان مجبور نیستند داده های مخرب را برای اهداف حمله مرتکب شوند. داده ها اغلب کاملاً معتبر هستند، بنابراین کار قبلی روی اعتماد و یکپارچگی داده ها از این حملات جلوگیری نکرد [۵]. Elliott Wen پیشنهاد می کند که WebAssembly نسل جدیدی از قالب های بایت کد سطح پایین است که به طور گسترده در برنامه های کاربردی مرورگر محور استفاده می شود [۶]. شیرشک راجا ماسکی استدلال می کند که سیستم های حمل و نقل هوشمند (ITS)[1] باید ایمن، مستقل، قادر به شناسایی سطوح ایمنی جاده ها و ارائه خدمات برای بهبود تجربه انسانی باشند [۷].

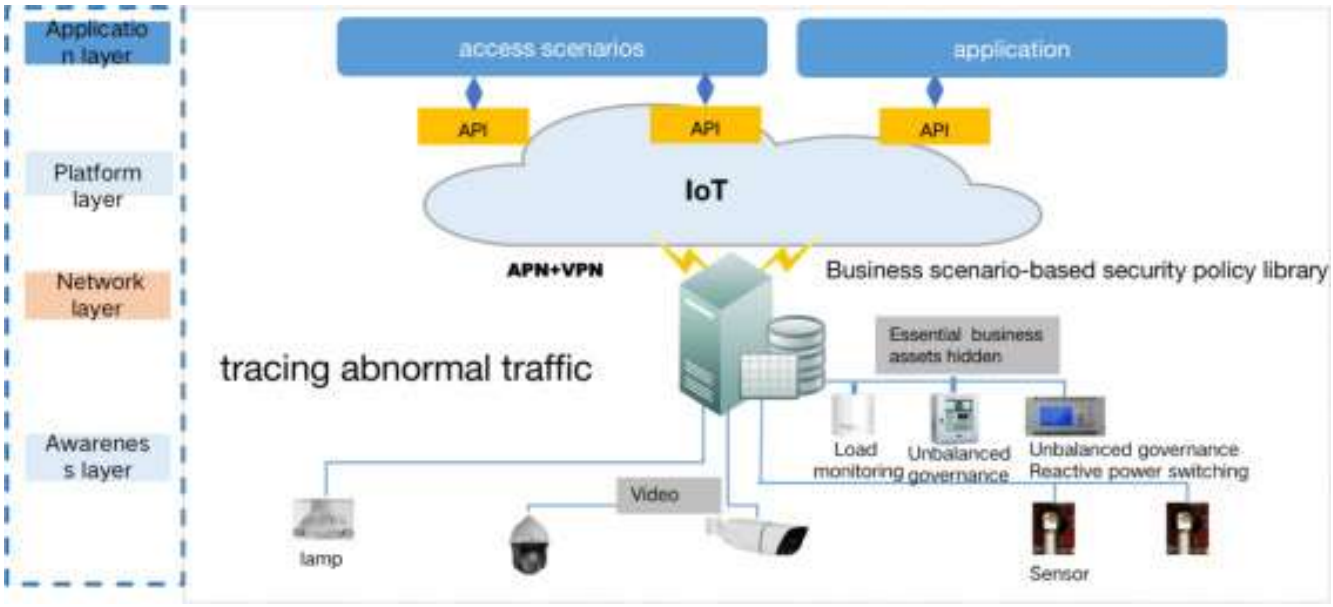
[1] Intelligent transportation systems

آگاهی موقعیتی امنیت شبکه‌اینترنت اشیا (IoT) جزء مهم شبکه هوشمند است. نیر بیتانسکی استدلال می‌کند که بسیاری از رمزنگاری مدرن، که با رمزنگاری کلید عمومی شروع می‌شوند و فراتر می‌روند، بر اساس دشواری مسائل ساختاریافته (عمدتاً جبری)، مانند تجزیه علی، معکوس گسسته، یا جستجوی بردارهای کوتاه شکل است [۸]. دانیل جوست معتقد است که یک تعریف ترکیبی از امنیت، که گاهی به عنوان یک تعریف مبتنی بر آنالوگ از آن یاد می شود، تضمین امنیتی قوی ای را ارائه می دهد که در هر زمینه ای اعمال می شود [۹]. Srinath Setty Spartan را معرفی می‌کند، یک سری جدید با دانش صفر از پارامترهای دانش غیر تعاملی مختصر (zkSNARKs) برای رضایت از محدودیت رتبه-۱ (R1CS)، یک زبان کامل NP برای ارضای مدار حسابی تعمیم‌یافته [۱۰]. جی. آرتور دیویس استدلال می‌کند که هنگام طراحی لوله‌ها، شیرها، مخازن و سایر اجزای حیاتی برای ایمنی بیشتر، بدون محدود کردن اتلاف مایعات، مراقبت ویژه‌ای لازم است [۱۱]. Avijit Mondal استدلال می کند که محاسبات ابری آخرین پیشرفت در صنعت IT است که به عنوان محاسبات بر اساس تقاضا نیز شناخته می شود [۱۲]. K. S. Niraja پیشنهاد می کند که اینترنت اشیا (IoT) یک فناوری است که از بسیاری از فناوری های بین رشته ای تشکیل شده است [۱۳].

فناوری کنترل دسترسی و فناوری‌های آگاهی موقعیتی امنیت شبکه در شبکه هوشمند تحقیق می‌شوند. لی دبلیو یک الگوریتم یادگیری تقویتی عمیق را بر اساس الگوی محاسبات لبه گرادیان خط مشی قطعی عمیق چندعاملی (MADDPG) پیشنهاد کرد [۱۴]. Ge، L پیشنهاد کرد که چارچوب شاخص را در حالی که به مسائل کلیدی ابهام امتیازدهی متخصص انسانی و کمبود داده در مناطق خاص SDN رسیدگی می‌کند، پیاده‌سازی کند [۱۵]. Magdi S. Mahmoud پیشنهاد کرد که یک جفت تنگاتنگ بین فناوری‌های اطلاعات و ارتباطات و سیستم‌های فیزیکی نگرانی‌های امنیتی جدیدی را معرفی می‌کند و نیازمند بازنگری در اهداف و روش‌های رایج است. رویکردهای امنیتی موجود یا غیرقابل اجرا هستند، قابل دوام نیستند، به اندازه کافی مقیاس پذیر نیستند، ناسازگار هستند، یا برای مقابله با چالش های ناشی از محیط های بسیار پیچیده مانند شبکه هوشمند کافی نیستند [۱۶]. آپاسانی، B استفاده از داده‌های مدل رقومی ارتفاع (DEM) توپوگرافی سطح را برای تعیین مکان‌های بهینه برای قرارگیری PMU پیشنهاد کرد. فن آوری مایکروویو برای ارتباط داده های سنکروفازور یکی دیگر از کمک های مهم انجام شده در این مقاله است [۱۷].

فناوری کنترل دسترسی بدون مرز شبکه هوشمند

بر اساس آگاهی موقعیتی از امنیت شبکه شبکه هوشمند، ما بهبود فناوری کنترل دسترسی بدون مرز را مطالعه می کنیم. ما یک استراتژی حفاظت از امنیت بصری امنیت شبکه و فناوری کنترل مبتنی بر کاربرد چند سناریویی شبکه برق را پیشنهاد می‌کنیم، پیش‌تشخیص کدهای مخرب مبتنی بر تقلب دینامیکی چند عاملی سخت‌افزار را پیشنهاد می‌کنیم، مدلی از رفتار غیرعادی ابرداده شبکه چند بعدی را ایجاد می‌کنیم. قابلیت ردیابی و پاکسازی هوشمند مبتنی بر داده کاوی عمیق و تجزیه و تحلیل گراف، تحقق پیشگیری و کنترل تطبیقی و کنترل دسترسی بدون مرز در کاربرد چند صحنه ای شبکه برق، ساختن یک سیستم کنترل دسترسی بر اساس هویت به جای موقعیت شبکه، و ایجاد سطح در معرض دارایی های اصلی تجارت پنهان خطر دسترسی غیرمجاز را با دقت ۹۹. ۹۹ درصد در مکان یابی، ردیابی و ردیابی ترافیک غیرعادی کاهش دهید (شکل ۱ را ببینید).



شکل ۱. فناوری کنترل دسترسی بدون مرز شبکه هوشمند مبتنی بر آگاهی موقعیتی امنیت شبکه.

A ردیابی سطوح چند بعدی موجود در کنترل دسترسی بدون مرز شبکه هوشمند، فناوری،

x ردیابی رفتار غیرعادی ابرداده شبکه است،

y ردیابی غیرعادی فراداده شبکه است.

$$A=\begin{cases}\iint_D f(x,y)=dxdy\\ \iint_D f(x',y')=dx'dy'\\ \iint_D f(x'',y'')=dx''dy''\end{cases} \qquad (1)$$

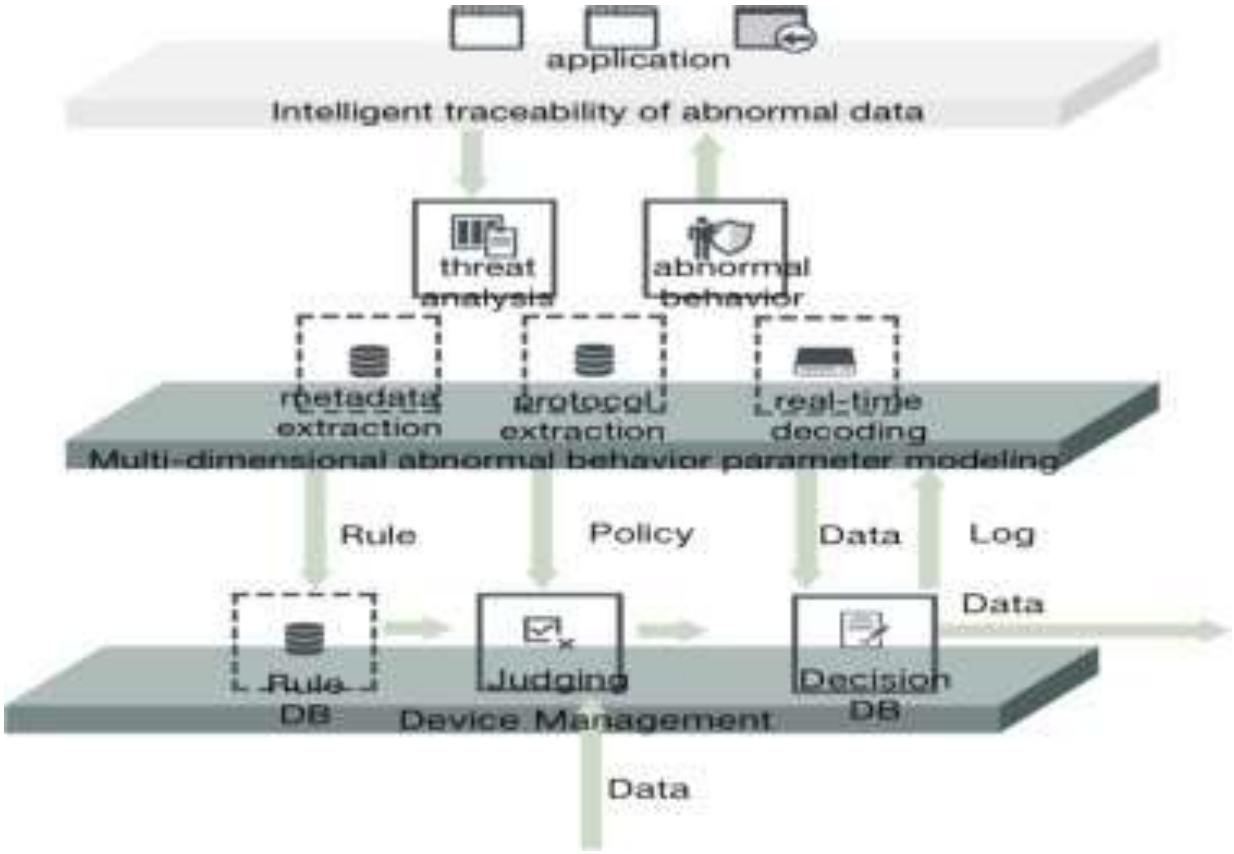
ما راهبرد استراتژی حفاظت از امنیت بصری و فناوری کنترل را ارائه می دهیم که امنیت شبکه چند سناریویی شبکه برق را در نظر می گیرد، اثربخشی تیم عملیات امنیتی شرکت را برای مدیریت خط مشی حفاظت امنیتی و زیرساخت های امنیتی حل می کند، و تأثیر موثر را درک می کند. پیوند یکپارچه خط مشی عملکردی و سوئیچ یک کلیک سیاست امنیتی در یک سناریوی چند کسب و کار، و به سرعت نیازهای حفاظت از امنیت محیط تکرار سناریوی چند کسب و کار را برآورده می کند. بر اساس فناوری کنترل امنیت چند سناریویی هماهنگ‌سازی خط‌مشی امنیت بصری، سیاست‌های امنیتی زیادی برای یک گره امنیتی شبکه در یک سناریوی زیرساخت فناوری اطلاعات ترکیبی وجود دارد. برای تنظیم چنین خط مشی امنیتی، پرسنل عملیات اغلب تنها با توجه به تجربه می توانند در تمام جنبه های سیستم خط مشی امنیتی را تنظیم کنند، یک خط مشی عملکردی را نمی توان به طور موثر یکپارچه و مرتبط کرد، امنیت شبکه و خطرات تداوم کسب و کار، نمی تواند به یکپارچه دست یابد. ترتیب سیاست امنیتی و عملیات و نگهداری ساده. از طریق فناوری هماهنگ سازی خط مشی امنیت بصری برای توسعه کتابخانه سیاست امنیتی مبتنی بر سناریوهای تجاری، پیکربندی الگوهای طرح بندی خط مشی امنیتی، طراحی آرایش زنجیره خط مشی بصری، از طریق توسعه یک الگوی توصیف خط مشی یکپارچه برای توصیف همه سناریوهای سیاست امنیتی قابل اجرا، مانند رویداد بزرگ. حفاظت، انطباق، و دیگر حفاظت، دسترسی عملیاتی، دسترسی تجاری، و سناریوهای دیگر، مربوط به زنجیره اجرای سیاست امنیتی ویرایش فرآیند دسترسی شی هدف؛ سوئیچ یک کلیک سیاست

امنیتی را برای برآورده کردن سناریوی چند کسب و کار، برآورده کردن سریع نیازهای حفاظت از امنیت با سناریوی تجاری، کاهش تا حد زیادی کار عملیات و تعمیر و نگهداری، بهبود بهره وری کار درک کنید.
جایی که

- α کتابخانه سیاست های امنیتی مبتنی بر سناریوهای تجاری است،
- a حفاظت امنیتی است،
- b سناریوی چند کسب و کار است.

$$\alpha = \begin{cases} \dfrac{f(b)-f(a)}{F(b)-F(a)} = \dfrac{f'(\xi)}{F'(\xi)} \\ \dfrac{f(b')-f(a')}{F(b')-F(a')} = \dfrac{f'(\xi')}{F'(\xi')} \\ \dfrac{f(b'')-f(a'')}{F(b'')-F(a'')} = \dfrac{f'(\xi'')}{F'(\xi'')} \end{cases} \qquad (2)$$

ما مدل ردیابی و پاکسازی هوشمند را بر اساس Spark و رفتار غیرعادی ابرداده شبکه چند بعدی مبتنی بر داده ایجاد کرده‌ایم و یک استراتژی تشخیص و کنترل ترافیک در سطح شبکه را بر اساس فناوری کاوشگر ترافیک توزیع شده پیشنهاد کرده‌ایم تا نمایه‌سازی تمام میدان بسته‌های ترافیک را محقق کنیم. تمیز کردن داده های کثیف و کنترل تشخیص ترافیک داده های غیرعادی در سراسر شبکه. بر اساس فناوری کاوشگر جریان توزیع شده، استراتژی تشخیص و کنترل کل ترافیک شبکه، تشخیص و کنترل کل ترافیک شبکه، از طریق پروب ترافیک شبکه، از طریق آینه سازی بای پس، و با توجه به وضعیت واقعی شرکت، طراحی و کنترل شبکه توزیع می شود. محیط کسب و کار قدرت و فناوری نظارت بر جریان Netflow و ترکیب با فناوری نظارت بر ترافیک مبتنی بر SNMP برای جمع آوری تمام ترافیک شبکه ذخیره سازی، از طریق رمزگشایی بلادرنگ پروتکل شبکه، استخراج ابرداده، ایجاد یک گزارش کامل، پروتکل، بسته همه شاخص میدانی به سرعت ابرداده‌های شبکه چند بعدی را استخراج کنید، و مدل‌سازی پارامترهای رفتار غیرعادی چند بعدی و پاک‌سازی داده‌های کثیف را انجام دهید، داده‌های ترافیک غیرعادی را تجزیه و تحلیل کنید، و به تشخیص، کنترل و قابلیت ردیابی هوشمند ترافیک شبکه داده غیرعادی در محیط کسب و کار پی ببرید (نگاه کنید به شکل ۲).



شکل ۲. مدل ردیابی و تمیز کردن هوشمند.

$f(x)$ قابلیت ردیابی هوشمند ترافیک داده های غیرعادی در سراسر شبکه است،

x متا دیتای شبکه چند بعدی است،

y متا دیتای رفتار غیرعادی چند بعدی است.

$$f(x)=\frac{d^2y}{dx^2}+P(x)\frac{dy}{dx}+Q(x)y \qquad (3)$$

ما یک الگوریتم تجزیه و تحلیل تهدید شبکه جامع و فناوری درک جریان کامل را بر اساس تشخیص بسته های عمقی ارائه می دهیم، به دستیابی به داده های عظیم سرویس برق و تجزیه و تحلیل تشخیصی با کارایی بالا و درک دقیق تهدیدات پی می بریم، و تجزیه و تحلیل همبستگی و هشدار اولیه را انجام می دهیم. داده‌های غیرعادی، خطرات امنیتی شبکه را پیش‌بینی می‌کند، نظارت بر عملکرد چند جهته و پردازش بهینه‌سازی و درک تهدید امنیت شبکه همه جانبه را برآورده می‌کند. بر اساس فناوری تجزیه و تحلیل جریان کامل و الگوریتم آگاهی موقعیتی امنیت شبکه همه جانبه، لایه کاربردی فناوری تشخیص و کنترل ترافیک بر فناوری موتور تشخیص بسته درجه با کارایی بالا متکی است تا به جمع آوری به موقع داده های عظیم، شناسایی دقیق و واقعی دست یابد. تجزیه و تحلیل تشخیصی زمان، شناسایی موثر همه جانبه ترافیک پروتکل، برای کمک به مدیران شبکه برای جلوگیری از خطرات امنیتی شبکه، نظارت بر عملکرد چند جهته و بهینه سازی، برای دستیابی به شناسایی بیش از ۱۰۰۰ نوع پروتکل شبکه. با رمزگشایی بیش از ۲۰۰ پروتکل رایج شبکه مانند HTTP، SMTP/POP/IMAP، DNS و غیره، می توان رفتار و محتوای کار تحت این پروتکل ها را به دقت شناسایی کرد و این رفتارها را می توان به طور

کامل بازیابی کرد و ترافیک شبکه را از جهش بینایی سطح "خون" به سطح "ژن". انواع رفتارهای غیرعادی در یک نگاه، انواع تهدیدات شبکه ادراک همه جانبه را تهدید می کند. ارزش استفاده از شبکه و قابلیت‌های امنیتی شرکت خود را در سراسر جهان بهبود بخشید.

۳. مقایسه کاربردهای عملکرد تشخیص ایمنی

برای محیط شبکه شبکه هوشمند با اعتماد صفر، توسعه سیستم تشخیص امنیت مبتنی بر فناوری تجسم، از طریق فناوری تجسم، به مسیر دسترسی، ترافیک دسترسی، رفتار دسترسی غیرعادی کاربر نمایش بصری، اما همچنین وضعیت دستگاه آنلاین، آمار، اجرای سیاست، اجرا دسترسی خواهد داشت. مسیر و سایر ارائه‌های بصری، برای کمک به اپراتورهای امنیتی درک شهودی‌تر، جامع‌تر از دسترسی به بدنه اصلی وضعیت و رفتار امنیتی، یافتن نقاط خطر سریع‌تر و دقیق‌تر، راه‌اندازی پاسخ امنیتی، حمایت از تصمیم‌های امنیتی. ویژگی هایی که مؤلفه تشخیص امنیتی باید پیاده سازی کند باید شامل الزامات زیر باشد (جدول ۱ و ۲ را ببینید).

جدول ۱. مقایسه مقوله و کاربردهای تابع.

Psa	Psa را به عنوان دقت فناوری دسترسی بدون مرز تحت یک معماری شبکه امنیتی با اعتماد صفر تنظیم کنید
Pes	Pes را به عنوان دقت فعال کردن دسترسی ایمن تجاری برای چند سناریو تنظیم کنید
Psc	Psc را به عنوان دقت ابزارها به عنوان تماس ایمن با داده ها تنظیم کنید
Pcb	Pcb را به عنوان دقت کنترل متمرکز تجاری بایگانی تنظیم کنید
Fsa	Fsa را به عنوان نیاز تابع دقت دسترسی ایمن در هر امنیتی تنظیم کنید
Fes	Fes را به عنوان الزام عملکرد تضمین ثبات و امنیت لینک دسترسی تنظیم کنید
Fsc	Fsc را به عنوان نیاز تابع فعال کردن احراز هویت و تأیید مجوز و کنترل دسترسی پویا تنظیم کنید
Fcb	Fcb را به عنوان نیاز عملکردی برای تحقق وحدت امنیت و راحتی کنترل کسب و کار تنظیم کنید

جدول ۲. مقایسه کاربردهای عملکرد تشخیص ایمنی.

دسته بندی	الزامات عملکردی	سیستم تست سنجی	راه حل اعتماد صفر Trx	افزایش متریک
Psa	Fsa	91. 2%	95. 7%	4. 5%
Pes	Fes	90. 7%	92. 6%	1. 9%
Psc	Fsc	91. 6%	93. 8%	2. 2%
Pcb	Fcb	90. 0%	94. 6%	4. 6%

۳. ۱. پیاده سازی فناوری دسترسی بدون مرز

تحت معماری شبکه امنیتی صفر اعتماد، فناوری تونل Unicom با دروازه دسترسی صفر اعتماد در محیط های مختلف مدیریت یکپارچه سیستم های تجاری توزیع می شود، همزمان، استفاده از دروازه ها به IP واقعی سیستم های تجاری، مخفی کردن پورت. برای اطمینان از امنیت استقرار کسب و کار در هر دسترسی به محیط، دفاع موثر در برابر نشت داده ها، از دست دادن داده ها، حملات DDoS، حملات APT و سایر تهدیدات امنیتی. در عین حال، سیاست های دسترسی از IP محور به هویت محور تغییر کرده است و احراز هویت دسترسی با تغییرات مکرر در سیاست ها تغییر نمی کند. جداسازی مرزی به طور همزمان به کاربران امکان دسترسی انعطاف پذیر، راحت و ایمن تر به سیستم های مختلف تجاری را می دهد.

۳. ۳. روش پیاده سازی برای تماس های امنیتی داده ها

سناریوی تماس امنیتی داده‌ها، انواع واسطها را تطبیق می‌دهد، زمانی که برنامه تجاری نیاز به فراخوانی قابلیت‌های خدمات ثبت‌شده دارد، واسط یکپارچه تماس می‌گیرد، نیاز به گنجاندن شناسه تماس‌گیرنده و اطلاعات Token در امضا، دروازه‌ای برای احراز هویت و تأیید مجوز است. در طول فرآیند فراخوانی داده های برنامه، موتور ارزیابی اعتماد پویا برنامه دسترسی خارجی را ارزیابی می کند، رفتار فراخوانی را شناسایی می کند و کنترل دسترسی پویا را از طریق موتور کنترل دسترسی انجام می دهد.

۳. ۴. اجرای کنترل متمرکز کسب و کار

راه حل کنترل هویت یکپارچه مبتنی بر امنیت صفر اعتماد، از طریق احراز هویت یکپارچه، مدیریت هویت یکپارچه، مدیریت مرجع متمرکز، کنترل متمرکز کسب و کار، قابلیت های حسابرسی جامع، برای دستیابی به وحدت امنیت و راحتی، برای اطمینان از دسترسی ایمن به کسب و کار. این طرح گسترش هویت را به افراد، دستگاه‌ها، برنامه‌ها گسترش می‌دهد و کنترل دسترسی تطبیقی را بر اساس چارچوب مجوز نقش، ترکیبی از اطلاعات آگاه از زمینه (IP، موقعیت جغرافیایی، شبکه دسترسی، زمان، وضعیت امنیت دستگاه و غیره) انجام می‌دهد. در همان زمان، این برنامه انباشته میدان های کنترل باد (نقشه دانش، تجزیه و تحلیل گروه همتا، و سایر قابلیت ها) را برای دستیابی به یک حسابرسی متمرکز و ارزیابی هوشمند از کل انسان، تجهیزات، خطر دسترسی ترکیب می کند، به طوری که امنیت را می توان مشاهده کرد. . از طریق کنترل تجاری، برنامه های کاربردی سیستم تجاری، برنامه های کاربردی API و سایر برنامه ها را می توان به صورت متمرکز مدیریت کرد.

۴. مقایسه برنامه عملکرد حفاظت امنیتی را محاسبه کنید

با توجه به سناریوی کاربردی عملی پیکربندی دروازه هوشمند، توسعه اجزای حفاظت امنیتی تعبیه شده سبک وزن، تحقق عملکردهای احراز هویت، ممیزی امنیتی، دسترسی امنیتی، حفاظت هستی شناختی، و حفاظت از فرآیند دروازه هوشمند کل شبکه دامنه، ایجاد یک شبکه امنیتی قابل اعتماد از تجهیزات حسی کل شبکه دامنه و تضمین جمع آوری، پردازش و ارسال ایمن داده های نظارتی تولید مانند محیط و ویدئو به پلت فرم شبکه قدرت. این پروژه فناوری کنترل دسترسی بدون مرز را بر اساس آگاهی موقعیتی امنیت شبکه هوشمند، تحقق پیشگیری و کنترل تطبیقی و کنترل دسترسی بدون مرز در کاربردهای

چند سناریویی شبکه برق، حل مشکل تهدید حمله در تمام مراحل زنجیره حمله پیچیده را پیشنهاد می‌کند. و عملکرد اجزای امنیتی باید شامل الزامات زیر باشد.

جدول ۳. مقایسه کاربرد عملکرد حفاظت امنیتی

Pb	Pb را به عنوان دقت بر اساس فناوری کنترل دسترسی بدون مرز آگاهی موقعیتی امنیت شبکه شبکه هوشمند تنظیم کنید، داده ها به طور معتبری منتقل می شوند.
Pa	Pa را به عنوان دقت تحقق پیشگیری و کنترل تطبیقی و کنترل دسترسی بدون مرز برای چند سناریوی شبکه برق و دسترسی ایمن و قابل اعتماد تنظیم کنید.
Ps	Ps را به عنوان دقت حل مشکل تهدید حمله در تمام مراحل زنجیره حمله پیچیده تنظیم کنید و نظارت قابل اعتماد را اعمال کنید.
Pc	Pc را به عنوان دقت بررسی خط پایه انطباق تنظیم کنید
Pm	Pm را به عنوان دقت نظارت بر امنیت ترمینال حساس تنظیم کنید
Fb	Fb را به عنوان الزامات کاربردی برای تحقق انتقال رمزگذاری شده داده های ترمینال و درک محرمانه بودن، یکپارچگی و در دسترس بودن داده ها در زمان واقعی تنظیم کنید.
Fa	Fa را به عنوان الزامات کاربردی برای تحقق دسترسی مطمئن امنیت ترمینال، اجتناب از رابط ریسک، یافتن به موقع خطر امنیتی سمت لبه و مسدود کردن تنظیم کنید.
Fs	Fs را به عنوان الزامات عملکردی پیاده سازی نظارت بر امنیت برنامه، بر اساس شناسایی و طبقه بندی برنامه، تجزیه و تحلیل آماری نمونه گیری داده ها، نظارت بر وضعیت برنامه، و حفظ وابستگی ها تنظیم کنید.
Fc	Fc را به عنوان الزامات عملکردی مطابق با استانداردهای انطباق بر اساس الزامات پایه حفاظتی سطح، الزامات گسترش شبکه، و چک‌های پایه تعریف شده توسط کاربر تنظیم کنید.
Fm	Fm را به عنوان الزامات عملکردی برای تحقق بخشیدن به لینک ورودی دروازه هوشمند نظارت بر امنیت عملیات ترمینال ادراکی و اندازه گیری مداوم تنظیم کنید.

جدول ۴. مقایسه عملکرد حفاظت از امنیت.

دسته بندی	الزامات عملکردی	سیستم تست سنجی	راه حل اعتماد صفر Trx	افزایش متریک
Pb	Fb	97. 7%	93. 6%	4. 1%
Pa	Fa	96. 5%	92. 4%	4. 1%
Ps	Fs	97. 9%	93. 2%	5. 7%
Pc	Fc	98. 2%	92. 6%	5. 6%
Pm	Fm	98. 4%	92. 7%	5. 7%

۴. ۱. اجرای انتقال مطمئن داده

برای پایانه‌های شبکه که از طریق شبکه‌های خط ثابت ارتباط برقرار می‌کنند، تونل‌های IPSEC-VPN مبتنی بر الگوریتم‌های رمزنگاری داخلی در سمت دسترسی لبه شبکه از طریق دروازه دسترسی امنیتی شبکه لبه ارائه می‌شوند که با دروازه امنیتی شبکه با کارایی بالا متصل می‌شود. در لبه پلت فرم برای دستیابی به انتقال داده قابل اعتماد.

برای پایانه‌های شبکه که از طریق شبکه‌های سلولی قابل دسترسی هستند، ادغام میان‌افزار پایانه‌ها برای پشتیبانی از SSL-VPN SDK الگوریتم‌های رمزنگاری داخلی برای اطمینان از محرمانه بودن انتقال، تأیید یکپارچگی، و در دسترس بودن پایدار، و برای دستیابی به انتقال داده قابل اعتماد از طریق پیوند با عملکرد بالا مورد نیاز است. دروازه های امنیتی شبکه مستقر در لبه پلت فرم.

۴. ۲. اجرای دسترسی مطمئن امن

دروازه دسترسی ایمن شبکه سمت لبه عملکرد دسترسی بدون کلاینت را فراهم می کند، جایگزینی تقلبی، دستگاه های خصوصی و آسیب پذیر را مسدود می کند تا از تهاجم غیرقانونی شبکه دسترسی به شبکه جلوگیری کند.
شبکه دروازه دسترسی به امنیت به طور منظم در ترمینال شبکه آسیب پذیری و آسیب پذیری اسکن، تشخیص آسیب پذیری و یا نسخه های ترمینال شبکه بسیار کم و هشدار به موقع، یادآوری ترمینال شبکه برای ارتقاء یا وصله آسیب پذیری بی درنگ.

۴. ۳. اجرای نظارت قابل اعتماد را اعمال کنید

تجزیه و تحلیل ترافیک کسب و کار شبکه های مختلف، و ایجاد پرتره ترافیک کسب و کار شبکه، تشکیل برچسب های داده های کسب و کار شبکه، و با توجه به برچسب برای توسعه استراتژی کنترل دسترسی مربوطه، نظارت مستمر بر وضعیت برنامه، حفظ وابستگی.

۴. ۴. روش اجرای تأیید خط پایه انطباق

راستی‌آزمایی پایه پایانه‌های شبکه شناخته‌شده از طریق کتابخانه‌های خط پایه انطباق حسگر موجود.
از طریق پایانه‌های پویا، ترافیک، برچسب‌های رفتار، پایانه‌های شبکه ناشناخته به‌عنوان خطوط پایه جدید مدل‌سازی می‌شوند، خطوط پایه رفتاری جدید شکل می‌گیرند، و پایگاه‌های اطلاعاتی خط پایه انطباق به طور مداوم غنی می‌شوند.
به طور منظم خط پایه را با توجه به ویژگی های رفتار جریان کسب و کار تنظیم کنید.

۴. ۵. روش اجرای نظارت بر امنیت ترمینال درک شده

از طریق پلت فرم مدیریت امنیت شبکه، دروازه دسترسی امنیتی شبکه پیکربندی اتاق توزیع به طور جامع مدیریت می شود و ترمینال حسی در حال اجرا در زیر دروازه نظارت و به طور مداوم اندازه گیری می شود.
دروازه دسترسی امنیت شبکه از حالت عملیات آفلاین پشتیبانی می کند، در حالت آفلاین، می تواند عملیات نظارت بر امنیت ترمینال شبکه دروازه و اندازه گیری مداوم را تکمیل کند.

۵. نتیجه گیری

ما به طور خلاقانه ترکیبی از الگوریتم‌های مبتنی بر NLP و هوشمند را برای فناوری تشخیص ناهنجاری ترافیک برنامه‌های کاربردی وب پیشنهاد کرده‌ایم تا به طیف کاملی از محافظت از برنامه‌های وب هوشمند در زمان واقعی ۷/۲۴ دست یابیم. بر اساس فناوری بازرسی مبتنی بر هوش مشخصه و شهرت، فناوری نوآورانه ترکیب پردازش زبان طبیعی (NLP) و یک الگوریتم هوشمند برای تشخیص نفوذ ترافیک در برنامه‌های کاربردی وب، تجزیه و تحلیل عمق ترافیک چند سطحی و چند دانه‌ای اعمال می‌شود. انجام، همبستگی هوشمند پویا و تجزیه و تحلیل حفاری برای داده های ترافیک شبکه انجام می شود، نرخ نشت ویژگی های سنتی و فناوری تشخیص شهرت کاهش می یابد، مکان، ردیابی و قابلیت ردیابی ترافیک غیرعادی مشخص می شود و منبع و نوع کاربرد شبکه ترافیک مشخص می شود. در همان زمان، زمان وقوع و زمان وجود ثبت شد و دقت نتایج تشخیص بهینه شده با الگوریتم به ۹۷. ۷۴ درصد رسید.

References

[1] Koudai Hatakeyama, Daisuke Kotani, Yasuo Okabe, Zero trust federation: Sharing context under user control towards zero trust in identity federation, in: IEEE international conference on pervasive computing and communications, 2021.

[2] Mauro Lemus Alarcon, Minh Nguyen, Saptarshi Debroy, Naga Ramya Bhamidipati, Prasad Calyam, Trust model for efficient honest broker based healthcare data access and processing, in: IEEE international conference on pervasive computing and communications, 2021.

[3]Jinghui Li, Bifei Mao, Zhizhang Liang, Zeqi Zhang, Qiushi Lin, Trust, and trustworthiness: What they are and how to achieve them, in: IEEE international conference on pervasive computing and communications, 2021.

[4] Abhishek Kumar, Tristan Braud, Sasu Tarkoma, Pan Hui, Trustworthy AI in the age of pervasive computing and big data, in: IEEE international conference on pervasive computing and communications, 2020.

[5] Nicholas Handaja, Brent Lagesse, CAPP: A context-aware proof of presence for crowdsensing incentives, in: IEEE international conference on pervasive computing and communications, 2020.

[6] Elliott Wen, Gerald Weber, Wasmachine: Bring IoT up to speed with A WebAssembly OS, in: IEEE international conference on pervasive computing and communications, 2020.

[7] Shirshak Raja Maskey, Shahriar Badsha, Shamik Sengupta, Ibrahim Khalil, BITS: Blockchain based intelligent transportation system with outlier detection for smart city, in: IEEE international conference on pervasive computing and communications, 2020.

[8] Nir Bitansky, Akshay Degwekar, Vinod Vaikuntanathan, Structure vs. hardness through the obfuscation lens, in: International cryptology conference, 2021.

[9] Daniel Jost, Ueli Maurer, Overcoming impossibility results in composable security using interval-wise guarantees, in: International cryptology conference, 2020.

[10] Srinath Setty, Spartan: Efficient and general-purpose zkSNARKs without trusted setup, in: International cryptology conference, 2020.
[11] J. Arthur Davis, Angelin Gladys Jesudoss, Naveen Watson, Balaji Dhanasekaran, Automated flow management device for oman water networking system, in: International conference on computer communication and informatics, 2020.
[12] Avijit Mondal, Subrata Paul, Radha Tamal Goswami, Sayan Nath, Cloud computing security issues & challenges: A review, in: International conference on computer communication and informatics, 2020.
[13] K. S. Niraja, Sabbineni Srinivasa Rao, Security challenges and counter measures in internet of things, in: International conference on computer communication and informatics, 2020.
[14] Lei W., Wen H., Wu J., Hou W., MADDPG-based security situational awareness for smart grid with intelligent edge, Appl Sci, 11 (7) (2021), p. 3101
[15] Ge L., Li Y., Li S., et al., Evaluation of the situational awareness effects for smart distribution networks under the novel design of indicator framework and hybrid weighting method, Front Energy, 15 (2021), pp. 143-158
[16] Mahmoud Magdi S., Xia Yuanqing, Chapter 7 - smart grid infrastructures, Networked control systems, Butterworth-Heinemann (2019), pp. 315-349
[17] Appasani B., Jha A. V., Mishra S. K., et al., Communication infrastructure for situational awareness enhancement in WAMS with optimal PMU placement, Prot Control Mod Power Syst, 6 (2021), p. 9