بسمه‌تعالی

گزارش و تحلیل مقاله

Block-SDoTCloud: Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network

تعریف مسئله و هدف اصلی مقاله

امروزه فضای ذخیره‌سازی ابری (CS[1]) به عنوان یکی از منابع کلیدی ارائه شده توسط رایانش ابری شناخته شده است که در آن داده‌ها در یک سرور از راه دور ذخیره می‌شوند و می‌توانند از طریق اینترنت از سرور بازیابی شوند. CS را به چهار دسته شخصی، عمومی، خصوصی و ترکیبی تقسیم می‌کنند و تحت چهار لایه مانند دسترسی، کاربرد، مدیریت و ذخیره‌سازی کار می‌کند. رایانش ابری به کاربران و نهادهای تجاری اجازه می دهد تا داده‌هایی در ابر ذخیره کنند و این می‌تواند نگرانی‌های امنیتی مانند محافظت از داده‌ها، محرمانگی و یکپارچگی داده‌ها را ایجاد کند.

فناوری نوظهور شبکه نرم‌افزارمحور می‌تواند به عنوان راه‌حلی برای حل چنین مشکلاتی مورد استفاده قرار گیرد. اگر مهاجمان به مرکز داده دسترسی پیدا کنند، در بخش خاصی از شبکه محدود می‌شوند که تاثیر آن‌ها را محدود می‌کند. اما فناوری شبکه نرم‌افزارمحور به تنهایی نمی‌تواند مسائل امنیتی ذخیره‌سازی ابری را حل کند زیرا با ادغام شبکه نرم‌افزارمحور و فضای ذخیره‌سازی ابر، آسیب‌پذیری‌های حمله DDoS، ایجاد می‌شود. از طرف دیگر، زنجیره بلوکی یکی دیگر از فناوری‌های برجسته ای است که برای حل این مشکل به کار گرفته می‌شود. ویژگی اصلی زنجیره بلوکی این است که به محض ذخیره‌سازی داده‌ها در داخل زنجیره بلوکی، اصلاح آن بسیار دشوار است. هر بلوک شامل برخی از داده ها، hash بلوک و hash بلوک قبلی و بخش تراکنش‌ها است. hash اساسا برای شناسایی بلوک با تمام محتوای آن استفاده می‌شود و منحصر به فرد است. با این شیوه، داده‌های تراکنش‌ها به طور ایمن در بخش تراکنش‌ها، ذخیره می‌شود.

در تحقیقات پیشین، به برخی از مطالعات سیستماتیک در زمینه همین تکنولوژی‌های نوظهور می‌پردازیم:

- ایجاد خوشه توزیع‌شده کنترل‌کننده که به میزان قابل توجهی تاخیر متوسط و فقدان بسته‌ها را کاهش می‌دهد.
- با ادغام دو تکنولوژی شبکه‌های نرم‌افزارمحور و شبکه سنسور بیسیم، مدل SDWSN جهت شناسایی تهدیدها، چالش‌ها و راه‌حل‌های احتمالی در این دو تکنولوژی ارایه شده است.
- معرفی معماری اینترنت اشیا برپایه شبکه نرم‌افزارمحور و زنجیره بلوکی
- پیشنهاد معماری DistBlockSDN با NFV برای یک شهر هوشمند

[1] Cloud Storage

- ارائه رویکردی مبتنی بر زنجیره بلوکی جهت ارائه خدمات اشتراک داده بهتر به شبکه اینترنت اشیا
- مطالعه در یکپارچه‌سازی زنجیره بلوکی با ابر اشیا[1]
- ارائه یک مدیریت داده قابل کنترل برای زنجیره بلوکی که به صورت کارا در شبکه ابری قابل استفاده است.

بر اساس تجزیه و تحلیل مطالعات پیشین به این نتایج می‌رسیم:

- شبکه نرم‌افزارمحور می‌تواند برای کاهش مسائل امنیتی درون شبکه به کار گرفته شود.
- زنجیره بلوکی در ادغام با شبکه نرم‌افزارمحور برای محافظت بهتر از شبکه اینترنت اشیا کاربرد دارد.
- زنجیره بلوکی جهت اشتراک داده با CS، امکان یکپارچگی دارند.
- راه‌حل‌های پیشین تا حدی می‌توانند ایمنی، محرمانگی، پایداری و مقیاس‌پذیری را فراهم آورند.

معماری پیشنهادی این مقاله مبتنی بر زنجیره بلوکی، Block-SDoTCloud، یک معماری قوی برای ذخیره داده دورن ابر است که توان محاسباتی کمتری در برابر دیگر روش‌ها، نیاز دارد. در این مدل، فناوری شبکه نرم‌افزارمحور، جلوی حملات سایبری را گرفته و فناوری زنجیره بلوکی محرمانگی و اعتماد داخل شبکه را حفظ می‌کند. هم‌چنین، تهدید امنیتی DDoS به دلیل استفاده از فناوری زنجیره بلوکی، کاهش می‌یابد. در نگاه کلی این معماری، امنیت و محرمانگی داده‌ها را در مقابل دیگر روش‌ها، بهتر فراهم می‌کند.

راه‌حل پیشنهادی مقاله برای مسئله

معماری و لایه‌های راه‌حل پیشنهادی این مقاله در تصویر- ۱ به نمایش در آمده است. در ادامه به بررسی هر بخش می‌پردازیم.

لایه ادراک[2]

لایه ادراک در پایین‌ترین لایه معماری هدف قرار دارد و این لایه داده‌های دنیای واقعی را درک می‌کند. این لایه تعامل مستقیم با محیطی که کاربرد اینترنت اشیا در آن پیاده سازی شده است، دارد. تقریبا همه حسگرها و تجهیزات جمع‌آوری اطلاعات در لایه درک متصل هستند. در این لایه، عناصر سنجشگر، داده‌ها را به صورت بلادرنگ جمع‌آوری می‌کنند و اطلاعات را برای پردازش بیشتر به پروتکل شبکه نرم‌افزارمحور تحویل می‌دهند. داده‌های جمع‌آوری شده توسط این لایه شناسایی شده و با تعیین هویت نسبی، منتقل می‌شوند.

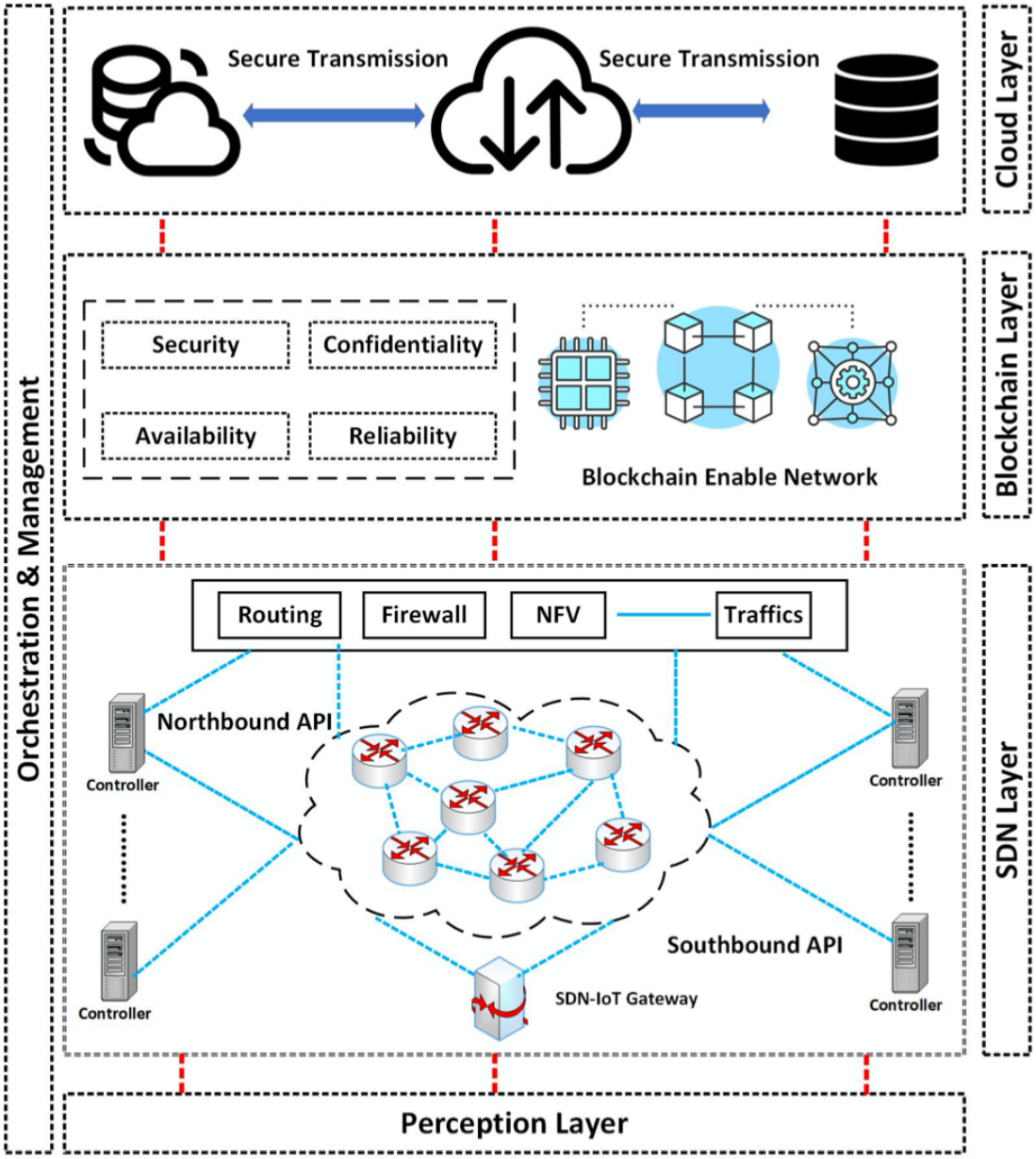
لایه زیرساخت/شبکه‌های اینترنت اشیا

تجهیزات انتقال داده مثل سوییچ‌ها، مسیریاب‌ها و...، می‌توانند از طریق دروازه‌های شبکه نرم‌افزارمحور، داده‌ها را منتقل کنند. داده‌های دستگاه‌های اینترنت اشیا از طریق کنترل‌کننده پویای شبکه نرم‌افزارمحور و از طریق پروتکل OpenFlow، مدیریت می‌شوند. مدل پیشنهادی این مقاله با امنیت، رسیدن داده‌ها را به لایه هدف میسر می‌کند. داده‌های اینترنت اشیا پس از ساماندهی در شبکه نرم‌افزارمحور، به صورت داخلی یا خارجی، در بستر ذخیره‌سازی ابری شبکه‌های زنجیره بلوکی جهت کسب امنیت بیشتر، ذخیره می‌شوند.

---

[1] Blockchain with Cloud of Things (BCoT)

[2] Perception



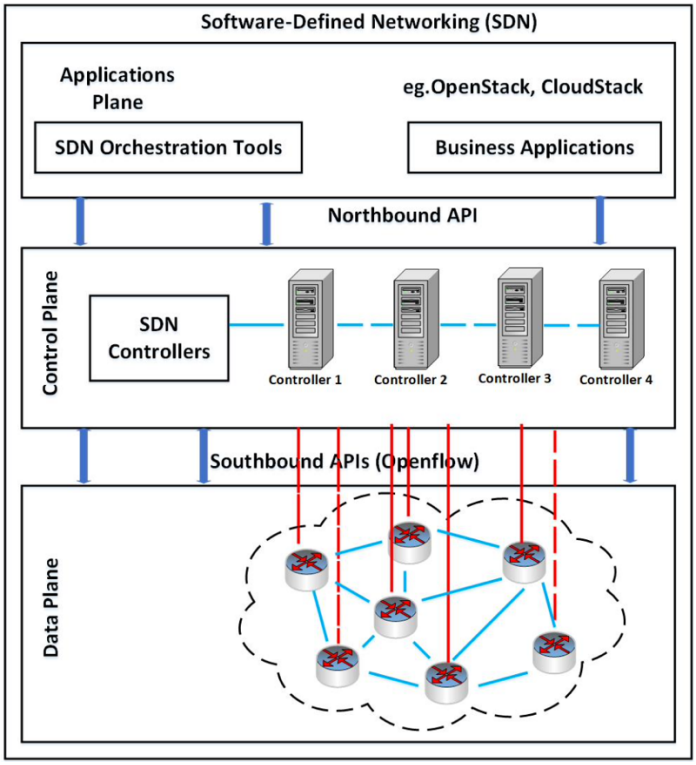
تصویر- ۱

امنیت مبتنی بر شبکه نرم‌افزارمحور در ابر

شبکه نرم‌افزارمحور می‌تواند خطرات امنیتی، تهدیدهای جدید و انواع مختلف حملات را بر خلاف مدل شبکه رایج فعلی، کنترل کند. شبکه نرم‌افزارمحور از صفحات داده، کنترل و برنامه، همان‌طور که در تصویر- ۲ نشان داده شده است، تشکیل شده است:

- صفحه داده: پایین‌ترین صفحه در معماری است. در این بخش دو نوع سوییچ نرم‌افزاری که معمولا مبتنی بر لینوکس هستند و یا سوییچ‌های سخت‌افزاری قرار می‌گیرند. برای امنیت بیشتر، دستگاه‌های شبکه و کنترل‌کننده‌ها با شیوه TLS، ارتباط دارند. این صفحه با صفحه کنترل، از طریق پروتکل OpenFlow در ارتباط هستند. صفحه داده وظیفه ضبط تمامی داده‌ها را در جهان ابر، برعهده دارد.

- صفحه کنترل: این صفحه ستون فقرات اصلی معماری شبکه نرم‌افزارمحور است. این صفحه بین صفحه برنامه و زیرساخت قرار می‌گیرد. برای ارتباط صحیح سه رابط Southbound، Northbound و Eastbound را ارائه می‌دهد. این صفحه چارچوب شبکه را بهبود می‌بخشد که داده‌ها متنوع و قابل اعتماد را در فضای CS قرار گیرند.
- صفحه برنامه: بالاترین صفحه در معماری است. این لایه امکان مدیریت پویا قوانین جریان‌های داده، را فراهم می‌کند. صفحه برنامه، خدمات شبکه را کنترل و برنامه وی اشیا انتقال فیزیکی یا اشیا مجازی بهبود می‌بخشد. سپس از تجزیه و تحلیل داده‌های شبکه یا وظایف پیشرفته‌ای که قرار است در مراکز داده بزرگ انجام شود، برای پیکربندی و مدیریت سطح بالای شبکه استفاده می‌کند. این صفحه، بهینه‌سازی هوشمند، مدیریت تحرک، تعادل بار، مسیریابی، سوییچینگ، قابلیت اطمینان و نظارت بر شبکه را در ابر شبکه‌های اینترنت اشیا، فراهم می‌کند.



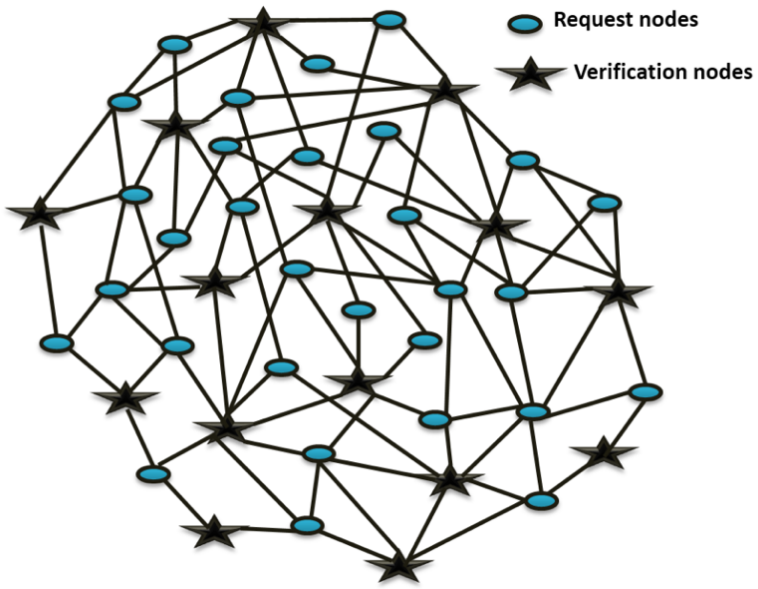
تصویر- ۲

رویکرد شبکه زنجیره بلوکی

زنجیره بلوکی نوع خاصی از دفتر[1] یا بانک اطلاعاتی است که امکان توزیع و مقاومت در برابر مخاطرات ضمن افزودن عملیات مختلف را دارد. همان‌طور که در تصویر- ۳ نشان داده شده است، به گره استخراج‌کننده یا تاییدکننده و عضو عمومی یا گره درخواست‌کننده وابسته است.

[1] Ledger

زنجیره بلوکی می‌تواند به شیوه کارا، کنترل دسترسی و امنیت سیستم مورد نظر را فراهم کند. تراکنش‌ها را در دفتری امن قرار می‌دهد. زنجیره بلوکی از یک پایگاه داده یا فضای ذخیره‌سازی مرکزی جهت ذخیره فعالیت کاربران، استفاده نمی‌کند.



تصویر- ۳

هر بلوک می‌تواند به طور دقیق از چندین تراکنش تشکیل شود. علاوه بر این، یک زنجیره Hash در هر بلوک گروه‌بندی می‌شود. هر بلوک شامل یک timestamp، داده‌ها، Hash فعلی و داده‌های قبلی مثل معاملات مستعد تداخل، است. در این شرایط، واضح است که فناوری زنجیره بلوکی می‌تواند در معماری این مقاله برای اطمینان از کنترل دسترسی در ساختار ذخیره‌سازی ابری ارائه شده، استفاده شود. دستاورد این رویکرد، امنیت گسترده و سیاست دسترسی بی نظیر به طور کارآمد است.

مدیریت CS و سرویس‌ها

در این مقاله، مدل پیشنهادی خدمات مختلف را در محیط ذخیره سازی ابر، بر اساس رویکرد توزیع شده زنجیره بلوکی، بهبود می‌بخشد. معماری شبکه نرم‌افزارمحور مبتنی بر زنجیره بلوکی مزایایی مانند انعطاف‌پذیری، قابلیت دسترسی، امنیت، حفظ حریم خصوصی، ذخیره دقیق منابع بی‌شمار را در بستر ذخیره‌سازی ابری فراهم می‌کند. زنجیره بلوکی به تنهایی و بدون همکاری شبکه نرم‌افزارمحور، نمی‌تواند قابلیت اطمینان، کنترل‌کننده‌های بسیار پایدار و متمرکز را فراهم کند و همچنین توانایی تعادل بار را در معماری ارائه شده، افزایش دهد.

پیاده‌سازی راه‌حل پیشنهادی

در این بخش به ارزیابی راه‌کار پیشنهادی از طریق پیاده‌سازی در محیط آزمایشی می‌پردازیم.

تنظیمات شبیه‌سازی

در شبیه‌سازی از Mininet-Wifi به عنوان یک بستر تقلید و پروتکل شبکه نرم‌افزارمحور مبتنی بر OpenFlow برای تولید نتایج استفاده شده است. به علاوه، از پلتفرم Wireshark برای تجزیه و تحلیل بسته‌ها در شبکه IoT-SDN استفاده شده است. پارامترهای شبیه‌سازی، در تصویر- ۴ نشان داده شده است.

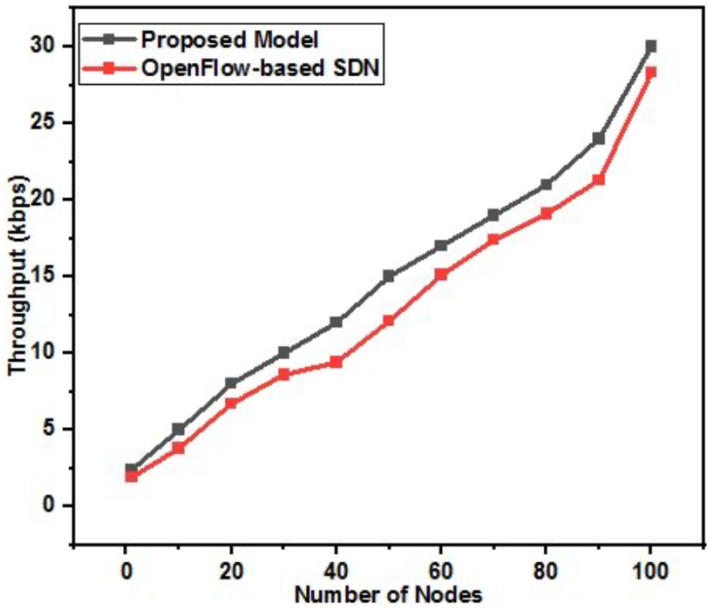
Parameters	Parameter Values
Emulator	Mininet 2.2.1
Packet Analyzer	Wireshark
Language	Python
Simulation Area	2500m X 2500m
Number of nodes	1-100
Simulation Times	400s
Data Rate	10Mbps
Packet Size	512 bytes
Routing Protocol	OpenFlow

تصویر- ۴

ارزیابی کارایی

ارزیابی کارایی روش پیشنهادی از منظر پارامترهای مختلفی بررسی شده است:

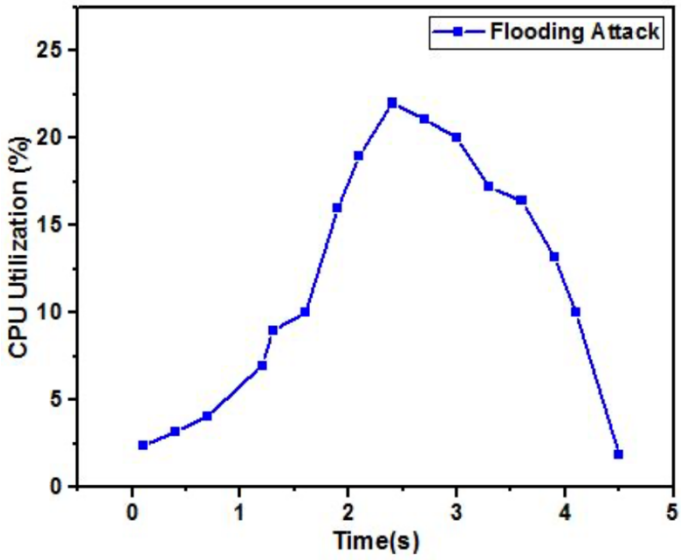
- تحلیل نرخ برونداد
- میزان استفاده از پردازنده
- زمان پاسخ
- عملیات انتقال فایل



تصویر- ۵

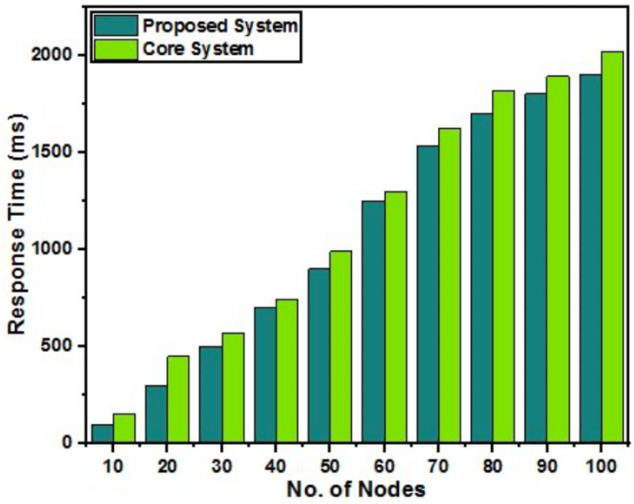
در مرحله اول ارزیابی، نرخ برونداد بر اساس تعداد گره‌ها تجزیه و تحلیل شده است (تصویر- ۵). مقایسه بین شبکه نرم‌افزارمحور مبتنی بر OpenFlow و مدل به نمایش درآمده است. بر این اساس، در دو حالت، نرخ

برونداد تقریبا یکسان است. وقتی تعداد گره‌ها افزایش می‌یابد، نرخ برونداد نیز افزایش می‌یابد. در کنار این مقایسه، از دید محرمانگی و امنیت، معماری پیشنهادی، عملکرد بسیار بهتری نسبت به عملکرد شبکه نرم‌افزارمحور مبتنی بر OpenFlow نشان می‌دهد.



تصویر- ۶

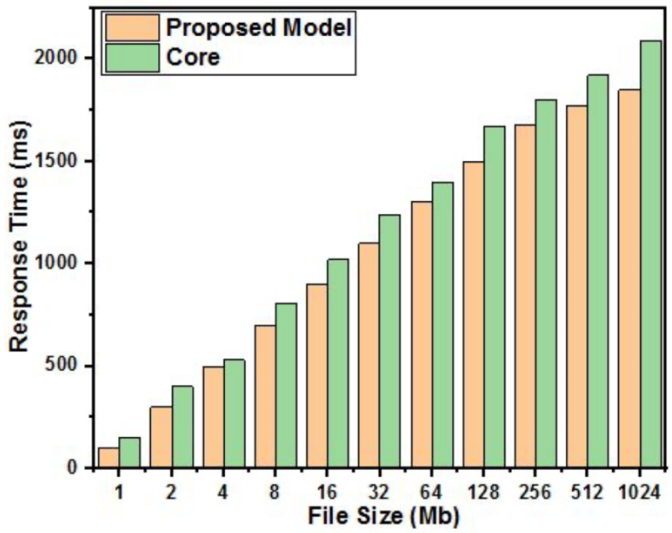
تصویر- ۶ تجزیه و تحلیل استفاده از پردازنده مرکزی برای حملات DDoS را هنگام اجرای مداوم برنامه‌های مختلف نشان می‌دهد. علاوه بر این ، در هنگام حمله DDoS ، مجموعه یادگیری برای ضبط استفاده از پردازنده استفاده شده است. در زمان ۲.۴ ثانیه، این حمله تقریبا شروع می‌شود و با گذر زمان، سرعت حمله نیز افزایش می‌یابد. مشاهده می‌شود با ادامه حمله پس از یک زمان مشخص، راه‌حل پیشنهادی به طور موثر در برابر این حمله محافظت می‌کند.



تصویر- ۷

در تصویر- ۷ زمان پاسخ بر اساس تعداد گره ها نشان داده شده است. هرچه تعداد گره‌ها افزایش می‌یابد، زمان پاسخ نیز برای هر دو حالت، افزایش می‌یابد. پیشنهادی این مقاله، عملکرد بهتری را در مقایسه با مدل اصلی

موجود در صورت حملات متعدد بیشتر نشان می‌دهد. در نتیجه، همه گره‌ها با استفاده از معماری ارائه شده در بستر ابری سریع پاسخ می‌گیرند.



تصویر- ۸

تصویر- ۸ زمان عملیات انتقال فایل با حجم‌های متفاوت را در حالت هسته (سیستم پایه) و روش پیشنهادی مقاله، نشان می‌دهد. با افزایش حجم فایل، زمان انتقال نیز در حال افزایش است ولی سیستم پیشنهادی، بهتر کار می‌کند. مدل ارائه شده در این مقاله، قادر به انتقال سریع‌تر یک فایل بزرگ نسبت به سیستم موجود بر اساس هسته است. در نتیجه می‌توان از سیستم پیشنهادی برای انتقال ایمن و سریع فایل‌ها استفاده کرد.

نقاط قوت و ضعف مقاله

نقاط قوت این مقاله:

- کارایی خوب در مقایسه با سیستم پایه از نظر زمان پاسخ و قدرت انتقال فایل
- واکنش مناسب در مقابله با حمله DDoS در شبیه‌سازی‌ها
- امکان تجهیز شبکه‌های نرم‌افزارمحور به راه‌حل پیشنهادی بدون نیاز به تغییر در زیرساخت‌ها

نقاط ضعف این مقاله:

- محول شدن محاسبات به لایه‌های بالا و ابر و عدم استفاده از محاسبات لبه
- شبیه‌سازی و کارایی سیستم در مقابل دیگر حملات معروف، بررسی نشده است.

جمع‌بندی و پیشنهادات برای کارهای آتی

ذخیره‌سازی ابری با تهدیدات و چالش‌های زیادی مانند امنیت، حریم خصوصی، دسترسی، سازگاری، کنترل و قابلیت اطمینان روبرو است. در این مقاله برای بهبود امنیت CS، معماری Block-SDoTCloud پیشنهاد شده است. فرایند توزیع شده مبتنی بر زنجیره بلوکی با شبکه نرم‌افزارمحور هدایت شده تا به طور موثر امنیت، ثبات، قابلیت اطمینان، محرمانگی و دسترسی به خدمات را برای کاربران افزایش دهد.

در تکمیل این راه‌کار مواردی را به صورت کار آتی می‌توان در نظر گرفت:

- در نظر گرفتن تهدیدات و حملات دیگر به جز حمله DDoS برای ارزیابی راه‌حل پیشنهادی
- ترکیب ایده این مقاله با تکنولوژی های مه و محاسبات لبه
- استفاده از قدرت محاسبات لبه در پردازش‌های سیستم به جای استفاده از ابر

مشخصات دقیق مقاله

A. Rahman, M. J. Islam, M. Saikat Islam Khan, S. Kabir, A. I. Pritom and M. Razaul Karim, "Block-SDoTCloud: Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network," 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020, pp. 1-6