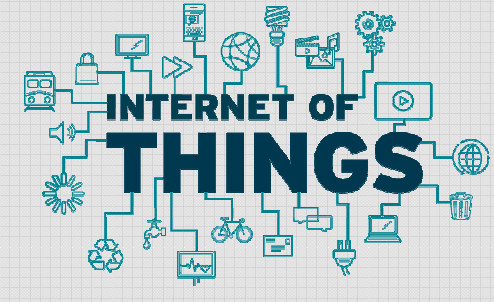


Block-SDoTCloud: Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network

محمد سعید انصاری

دانشجوی دکتری معماری کامپیوتر

استاد گرامی: خانم دکتر جاسبی

تعریف مسئله

- امروزه فضای ذخیره‌سازی ابری (CS) 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، بازیابی شوند.
- 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.

تعریف مسئله

- 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.

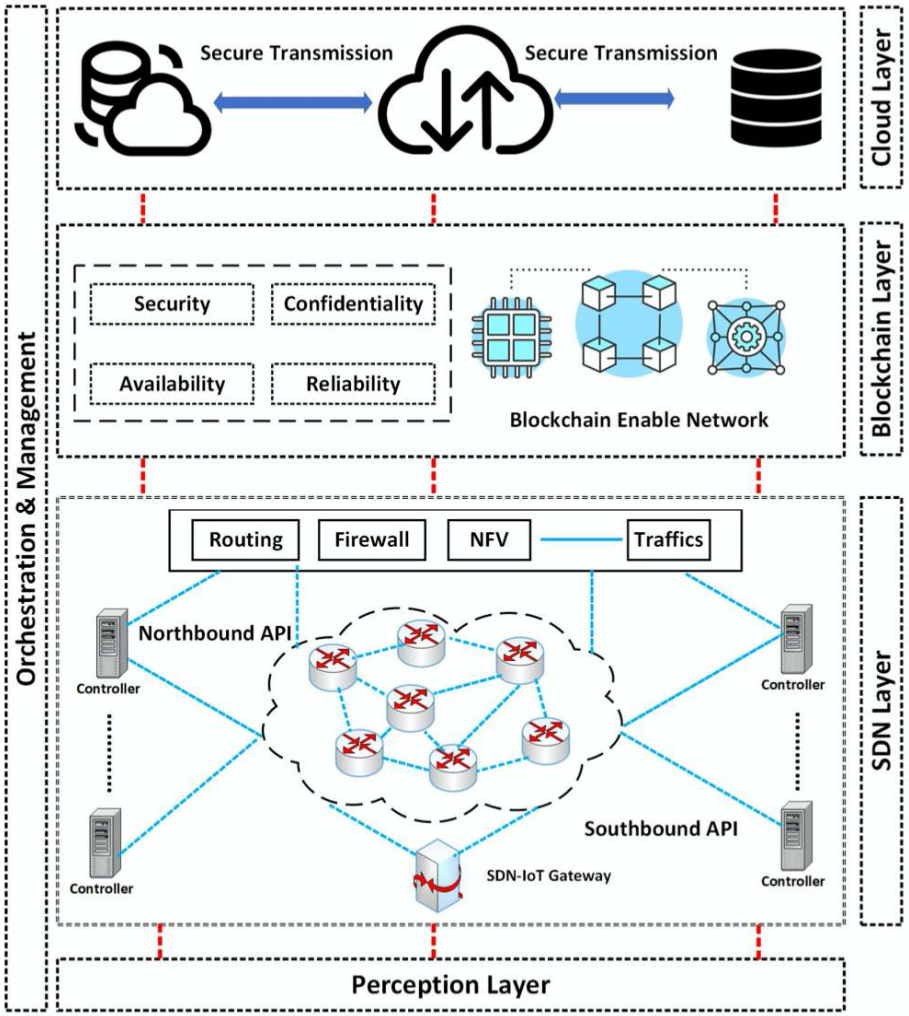
تحقیقات پیشین

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

راه‌حل پیشنهادی

- 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.

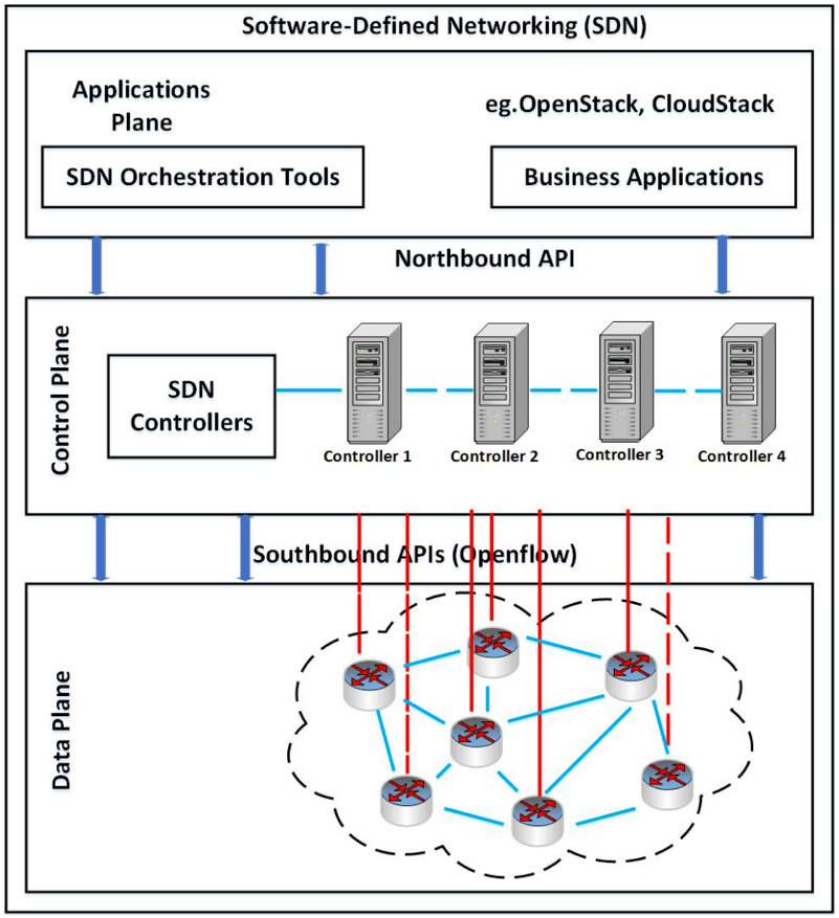
معماری
راه‌حل پیشنهادی



معماری
راه‌حل پیشنهادی

- لایه ادراک
  - پایین‌ترین لایه معماری هدف
  - تعامل مستقیم با محیطی که کاربرد اینترنت اشیا در آن پیاده سازی شده
  - در این لایه، عناصر سنجشگر، داده‌ها را به صورت بلادرنگ جمع‌آوری می‌کنند و اطلاعات را برای پردازش بیشتر به پروتکل شبکه نرم‌افزارمحور تحویل می‌دهند.
- لایه زیرساخت/شبکه‌های اینترنت اشیا
  - تجهیزات انتقال داده مثل سوییچ‌ها، مسیریاب‌ها و...، که 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.

معماری
راه‌حل پیشنهادی



- امنیت مبتنی بر شبکه

نرم‌افزارمحور در ابر:

- صفحه داده
- صفحه کنترل
- صفحه برنامه

معماری
راه‌حل پیشنهادی

- رویکرد شبکه زنجیره بلوکی
  - زنجیره بلوکی نوع خاصی از دفتر یا بانک اطلاعاتی است که امکان توزیع و مقاومت در برابر مخاطرات ضمن افزودن عملیات مختلف را دارد.
  - فناوری زنجیره بلوکی در معماری این مقاله برای اطمینان از کنترل دسترسی در ساختار ذخیره‌سازی ابری ارائه شده، استفاده می‌شود.
- مدیریت CS و سرویس‌ها
  - 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.

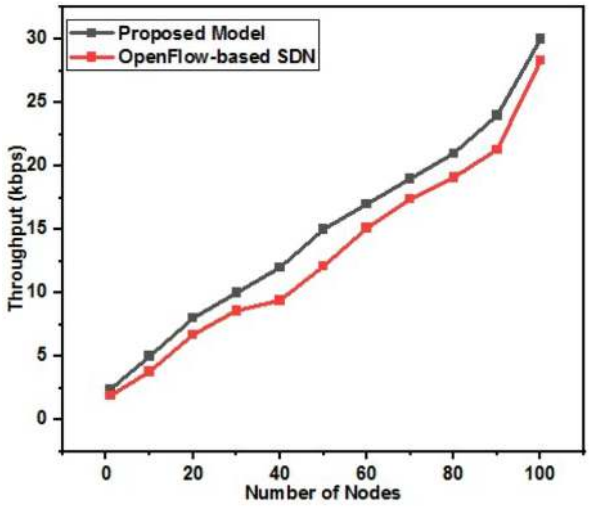
ارزیابی
راه‌حل پیشنهادی

- محیط تست

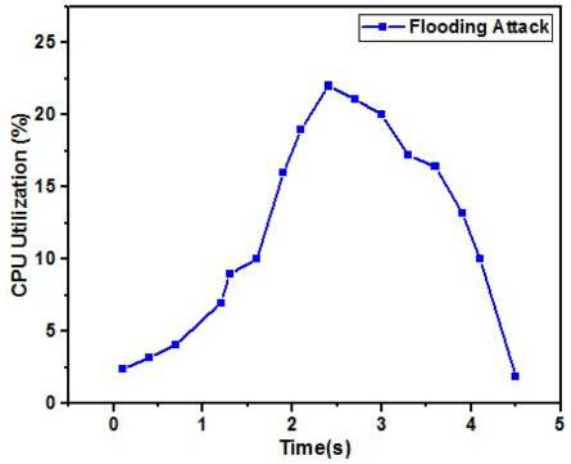
Parameters	Parameter Values
Emulator	Mininet 2.2.1
Packet Analyzer	Wireshark
Language	Python
Simulation Area	2500m X 2500m
Number of nodes	1-100
Simulation Times	400s
Data Rate	10Mbps
Packet Size	512 bytes
Routing Protocol	OpenFlow

پیاده‌سازی راه‌حل پیشنهادی

- نرخ برون‌داد

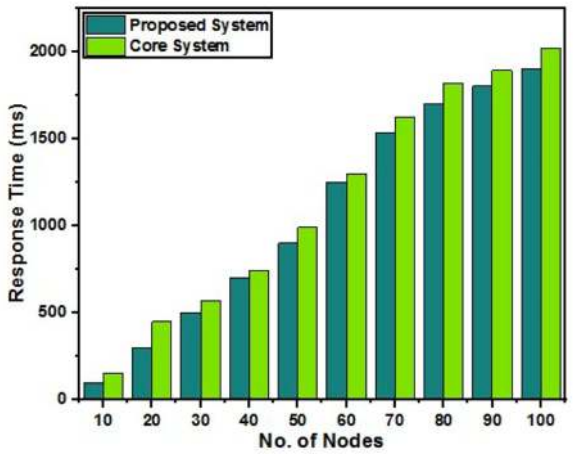


- استفاده از پردازنده مرکزی برای حملات DDoS را هنگام اجرای مداوم برنامه‌های مختلف

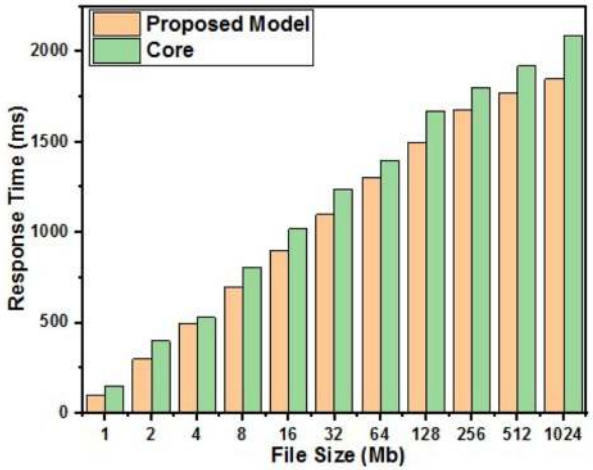


پیاده‌سازی
راه‌حل پیشنهادی

- زمان پاسخ بر اساس تعداد گره ها



- زمان عملیات انتقال فایل با حجم‌های متفاوت



نقاط قوت و ضعف

- نقاط قوت:
  - 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:
  - 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.

پیشنهادات برای کارهای آتی

- 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

مرجع

- 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

با تشکر از توجه شما

؟