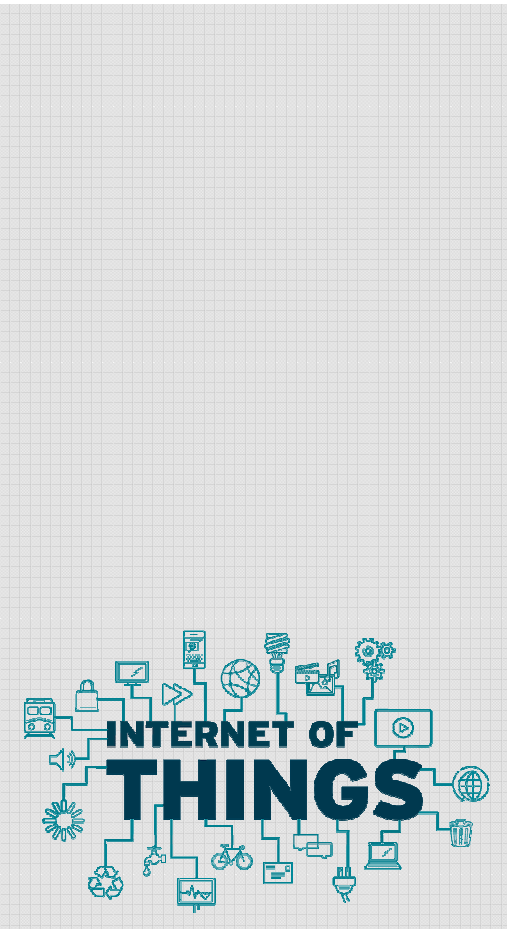


A Blockchain Architecture for SDN-enabled Tamper-Resistant IoT Networks

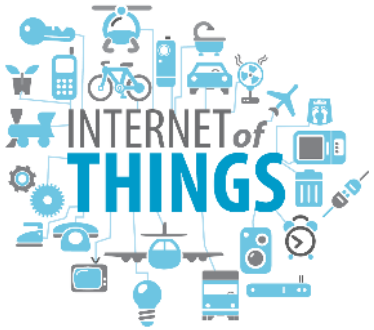
محمد سعید انصاری

دانشجوی دکتری معماری کامپیوتر

استاد گرامی: خانم دکتر جاسبی

تعریف مسئله

- مدل‌های موجود ارتباطات اینترنت اشیا، مانند:
  - زیرساخت‌های امنیتی متمرکز بر ابر،
- به دلیل
  - محدودیت در منابع و
  - انعطاف‌پذیری،
- توانایی حفظ امنیت و حریم خصوصی در اینترنت اشیا را ندارند.
- این ضعف باعث قرارگرفتن تجهیزات اینترنت اشیا در معرض
  - حملات جعل و
  - ارتقا امتیازات



تعریف مسئله

- یک جایگزین جذاب، زنجیره بلوکی است که زیرساختی غیرمتمرکز برای مقابله با حملات DDoS و مقابله با خطر یک نقطه شکست ارایه می‌کند.
- شبکه‌های نرم‌افزارمحور به دلیل محول کردن محاسبات به ابر و لبه شبکه، در رفع نیازهای اینترنت اشیا، کمک زیادی می‌کنند.
- هم‌چنین، شبکه‌های نرم‌افزارمحور در زمانی خرابی گره‌ها، به دلیل هدایت و تقسیم بار، جریان‌ها را به مقصد رسانده و نیازمندی‌های QoS را برطرف می‌کند.

تحقیقات پیشین

- استفاده از زنجیره بلوکی برای ایجاد بستری امن در ارتباطات اینترنت اشیا:
  - استفاده از الگوریتم‌های PoT و PoL که مه را به عنوان لایه میانی مرتبط کننده تجهیزات اینترنت اشیا و ابر به کار می‌برد.
  - معرفی چارچوب Devify برای ساخت شبکه‌های اینترنت اشیا مورد اعتماد قابل همکاری به شیوه غیر متمرکز که مدل هستی‌شناسی وب اشیا را برای توسعه برنامه‌های ابری زنجیره بلوکی اینترنت اشیا، پذیرفته است.
  - شناسه یکتای رمزشده به نام Trust Bit (TB) جهت ارتباطات غیر متمرکز وسایل نقلیه هوشمند که از طریق یک سیستم پاداش برای حفظ جزییات TB و پخش TB در زمان اتصال موفق و مورد اعتماد، کار می‌کند.

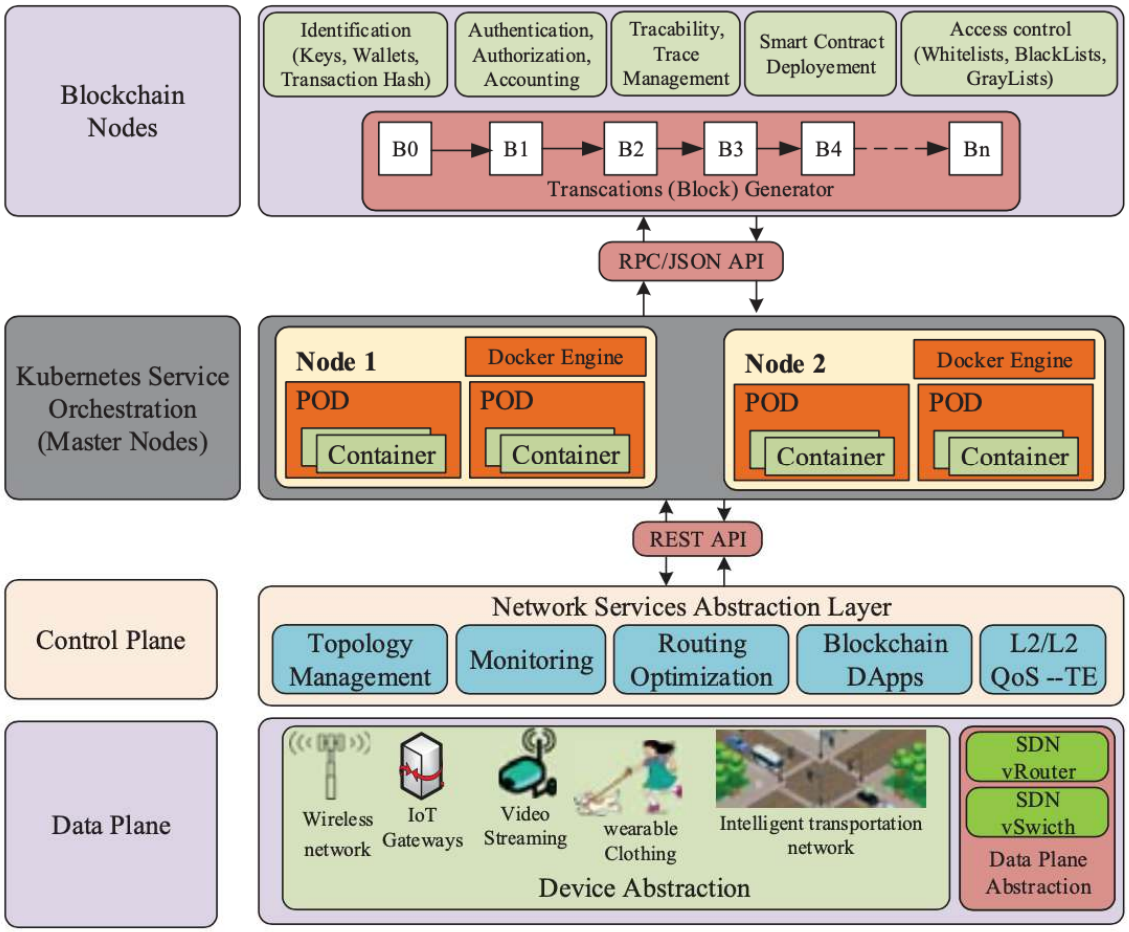
تحقیقات پیشین

- ادغام زنجیره بلوکی و شبکه نرم‌افزارمحور که باعث انعطاف‌پذیری، کارایی، دسترس‌پذیری و امنیت می‌شود:
  - خودکارسازی روند شک کردن، تایید و اعتماد به سرویس‌های وب اینترنت اشیا جهت حفاظت از آن‌ها در مقابل حملات
  - مجازی‌سازی منابع اینترنت اشیا با ترکیب زنجیره بلوکی و شبکه نرم‌افزارمحور با اجرای ارتباطات مبتنی بر مجوز هنگام تهیه منابع
  - پیشنهاد چارچوب ChainGuard روی کنترل‌کننده Floodlight برای فیلتر کردن و ردگیری بسته‌های نامتعارف و جلوگیری از رفتارهای مخرب منابع آسیب پذیر

روش پیشنهادی

- روش پیشنهادی این مقاله:
  - یک معماری مبتنی بر زنجیره بلوکی برای اعمال امنیت بر تراکنش‌های اینترنت اشیا با پیاده‌سازی برنامه‌ای غیرمتمرکز آگاه بر شبکه‌های نرم‌افزارمحور ارایه شده است که به گوش دادن به گره‌های استخراج‌کننده، گزارش IPاهای مشکوک و اعتبارسنجی بسته‌های ناشناخته می‌پردازد.
  - این معماری الگوریتم اجماع PoA را معرفی می‌کند که دستگاه‌های مشکوک هوشمند اینترنت اشیا را نشان داده و آن‌ها را تحت قرارداد هوشمند، گزارش می‌کند.

معماری
راه‌حل پیشنهادی



معماری راه‌حل پیشنهادی

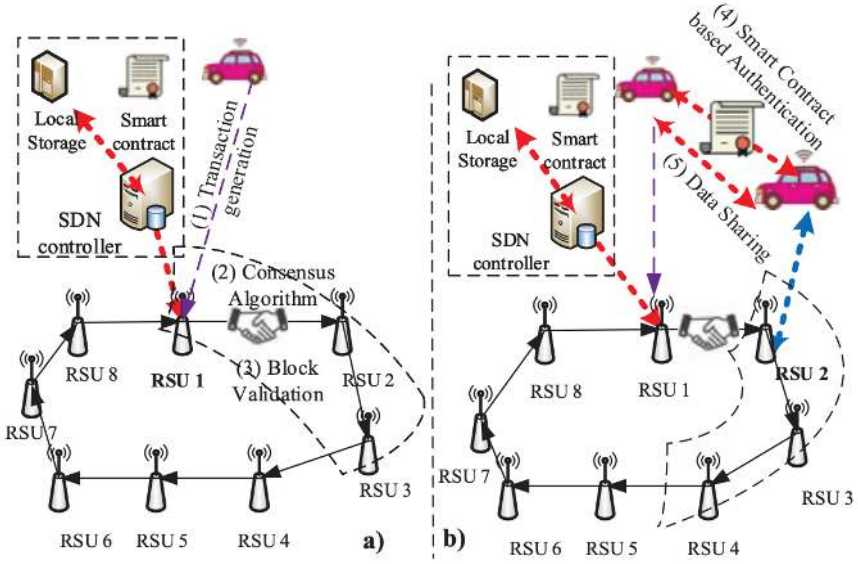
- طراحی سیستم:
  - گره‌های زنجیره بلوکی، یعنی استخراج‌کنندگان و مشتریان، از IPFS برای همکاری با قراردادهای هوشمند و معاملات زنجیره بلوکی استفاده می‌کنند.
- مدیریت جریان:
  - واحد Identification: با استفاده از کلید عمومی و خصوصی دسترسی کاربر/گره را مدیریت می‌کند.
  - واحد AAA: واحدی جهت احراز هویت، اعطای دسترسی و نگهداری حساب‌ها بر پایه زنجیره بلوکی است.
  - واحد Traceability: این واحد وظیفه دنبال کردن کامل روند تراکنش‌ها از گره مبدا ایجادکننده تا تمامی فرآیندهای روی زیرساخت زنجیره بلوکی را برعهده دارد.
  - واحد Smart Contract: وظیفه تعامل بین توابع قرارداد و گره‌های اینترنت اشیا از ایجاد تا پیاده‌سازی را برعهده دارد.

معماری راه‌حل پیشنهادی

- الگوریتم اجماع:
  - با استفاده از الگوریتم PoA، تعداد N گره معتمد، انتخاب می‌شود.
  - برای اعمال امنیت شبکه، PoA تعدادی از گره‌های واجد شرایط اینترنت اشیا را از قبل برای اعتبار سنجی تراکنش‌ها، طبق قوانین سخت انتخاب می‌کند.
  - ابتدا گره‌ها بر اساس پارامترهای QoS مثل پهنای باند بیشتر، تاخیر کمتر و منابع سخت‌افزاری بیشتر، انتخاب می‌شوند.
  - این گره‌ها می‌توانند خود تعداد محدودی از سرگروه‌ها که مجموعه‌ای از اختیارات را برای حفظ و کار شبکه دارند را انتخاب کنند.

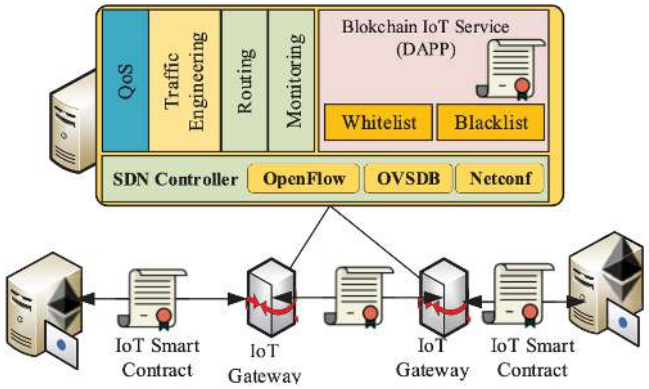
کاربردهای راه‌حل پیشنهادی

- اینترنت وسایل نقلیه مبتنی بر Blockchain-SDN
  - شبکه‌های توزیع شده، سیستم‌های مختلف اینترنت اشیا مانند اتومبیل‌های متصل، عابر پیاده، جاده‌ها و سیستم‌های پارکینگ را به هم متصل می‌کند.
  - معاملات جعلی به راحتی توسط خوشه فهرست شده گره‌های VANET قابل تشخیص است.



کاربردهای راه‌حل پیشنهادی

- افزایش امنیت بین دروازه‌های اینترنت اشیا
  - کنترل کننده شبکه نرم‌افزارمحور یک برنامه غیرمتمرکز مبتنی بر Python را پیاده سازی می کند که با Ethereum Web3 API ادغام شده تا ترافیک را فیلتر کرده و گره‌های مشکوک اینترنت اشیا را شناسایی کند.
  - این یک شیوه همکاری برای ایجاد لیست سفید یا سیاه از آدرس‌های IP دروازه‌های اینترنت اشیا مشکوک را فراهم می‌کند.
  - در این رویکرد، وظیفه ذخیره آدرس‌های IP در لیست سیاه و سفید به VNFها سپرده می‌شود.



نقاط قوت و ضعف

- نقاط قوت:
  - ارائه راه‌کاری که قابلیت پیاده‌سازی در محیط واقعی دارد.
  - کنترل دسترسی به صورت جامع بدون نیاز به تعریف قوانین در هر یک از اجزای شبکه به صورت جداگانه و مدیریت مرکزی قوانین بر اساس شبکه‌های نرم‌افزارمحور
  - راه‌کار ارائه شده، امکان پیاده‌سازی در محیط‌های موجود بدون نیاز به تغییر در سمت کاربر و در ذات پروتکل OpenFlow را دارد که در مقایسه با دیگر مقاله‌ها امکان استفاده و تست آن را در انواع محیط موجود فراهم می‌آورد.
- نقاط ضعف:
  - میزان تاخیر و سربار احتمالی حاصل از این معماری در مقایسه با دیگر روش‌ها، بررسی نشده است.
  - در این مقاله نتایج تست و پیاده‌سازی احتمالی اعلام نشده است و معلوم نیست در شرایط بار زیاد این سامانه و معماری چه واکنشی نشان خواهد داد.
  - در این راه‌کار یک کنترلر برای یک شبکه بزرگ داریم که در صورت بروز اختلال در آن، کلیه عملکردهای شبکه مختل خواهد شد. برای مباحث redundancy پیشنهادی در نظر گرفته نشده است.

پیشنهادات برای کارهای آتی

- پیاده‌سازی و مقایسه راه‌کار پیشنهادی این مقاله با روش‌های دیگر در چندین کاربرد واقعی مانند:
  - شبکه VANET
  - شبکه مراقبت‌های بهداشتی
- استفاده از روش‌های یادگیری ماشین در بهبود عملکرد تشخیص گره‌های مخرب
- مقایسه الگوریتم اجماع PoA که در این مقاله پیشنهاد شده با دیگر الگوریتم‌ها و مقایسه نتایج به دست آمده

مرجع

- A. Hakiri, B. Sellami, S. Ben Yahia and P. Berthou, "A Blockchain Architecture for SDN-enabled Tamper-Resistant IoT Networks," 2020 Global Information Infrastructure and Networking Symposium (GIIS), 2020, pp. 1-4

با تشکر از توجه شما

؟