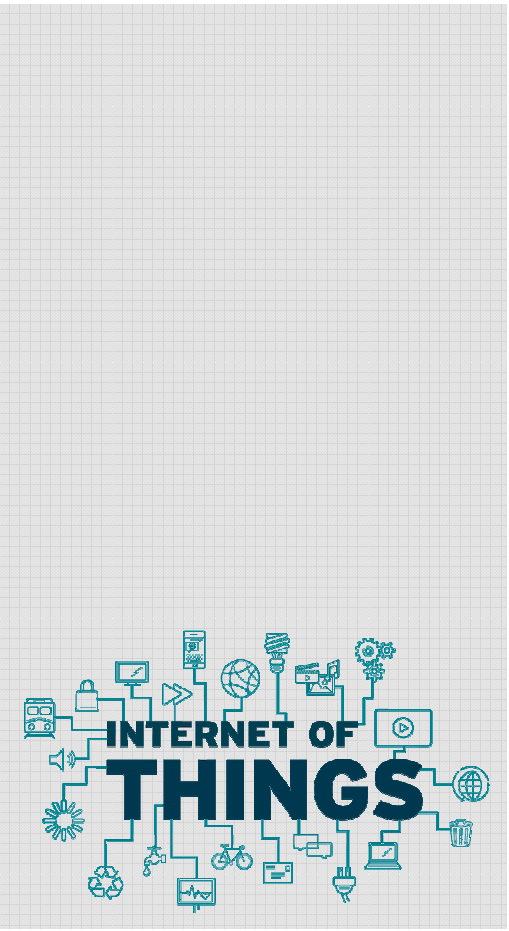


Blockchain based secure IoT data sharing framework for SDN-enabled smart communities

محمد سعید انصاری

دانشجوی دکتری معماری کامپیوتر

استاد گرامی: خانم دکتر جاسبی

تعریف مسئله

- وقتی دستگاه‌های اینترنت اشیا، داده‌ها را در شبکه نرم‌افزارمحور به اشتراک می‌گذارند، شبکه نرم‌افزارمحور چالش‌هایی را در امنیت داده نشان می‌دهد:
  - کنترل‌کننده شبکه نرم‌افزارمحور متمرکز است و از یک نقطه بالقوه از حملات مانند DoS رنج می برد.
  - لایه برنامه در شبکه نرم‌افزارمحور به برنامه‌های مختلف فروشندگان اجازه می‌دهد تا منابع شبکه را مدیریت و تنظیم کنند. هنگامی که شبکه نرم‌افزارمحور سیاست‌های مناسب دسترسی را برای این برنامه‌ها تنظیم نکرده باشد، ممکن است باعث دسترسی نامناسب به داده‌های شبکه شده و امنیت داده‌ها را تهدید کند.

تحقیقات پیشین

- زنجیره بلوکی برای شبکه‌های نرم‌افزارمحور:
  - استفاده از شبکه نرم‌افزارمحور و زنجیره بلوکی برای اطمینان از امنیت و حریم خصوصی دستگاه‌های اینترنت اشیا در جوامع هوشمند
  - تلفیق فناوری‌های شبکه نرم‌افزارمحور و زنجیره بلوکی، یک معماری شبکه ترکیبی برای شهر هوشمند ساخته است. این چارچوب شامل یک شبکه اصلی با گره‌های استخراج کننده و یک شبکه لبه‌ای است که با کنترل‌کننده‌های شبکه نرم‌افزارمحور فعال می شود.
  - با استفاده از زنجیره بلوکی، شبکه نرم‌افزارمحور و فنآوری‌های محاسبات مه، یک چارچوب ابری برای اینترنت اشیا، پیشنهاد شده است. این زنجیره بلوکی برای ثبت پرداخت معاملات منابع ابری بین ارائه‌دهندگان خدمات و کاربران به کار گرفته شد.

تحقیقات پیشین

- رمزگذاری مجدد پروکسی PRE:
  - مکانیسم SDSM سرویس داده امن در محاسبات ابری موبایل است. این سازوکار از IBPRE استفاده می‌کند و به سرورهای ابری امکان مدیریت تفویض داده برای کاربران را می‌دهد.
  - پروژه Nucypher یک پروژه فعال است که به عنوان یک سیستم مدیریت کلید غیرمتمرکز، معرفی شده است. هدف این پروژه، حل مسئله سیستم مدیریت کلید قابل اعتماد و متمرکز در فضای ابری است.

روش پیشنهادی

- افزایش امنیت اطلاعات در شبکه نرم‌افزارمحور هنگام به اشتراک گذاری داده‌ها در دستگاه‌های اینترنت اشیا، بسیار مهم است.
- برای مقابله با این چالش امنیتی، در طراحی پیشنهادی این مقاله، از فناوری زنجیره بلوکی و یک رمزنگاری اولیه به نام PRE استفاده شده است.
- ادغام زنجیره بلوکی با شبکه نرم‌افزارمحور قادر به حل مشکلات شبکه نرم‌افزارمحور متمرکز است.
- بنابراین، در این مقاله از فناوری زنجیره بلوکی برای مدیریت هویت دستگاه‌های اینترنت اشیا هوشمند در جوامع هوشمند استفاده می‌شود که می‌تواند اصالت دستگاه‌ها را افزایش داده و خطر ابتلا به یک نقطه حمله را کاهش دهد.

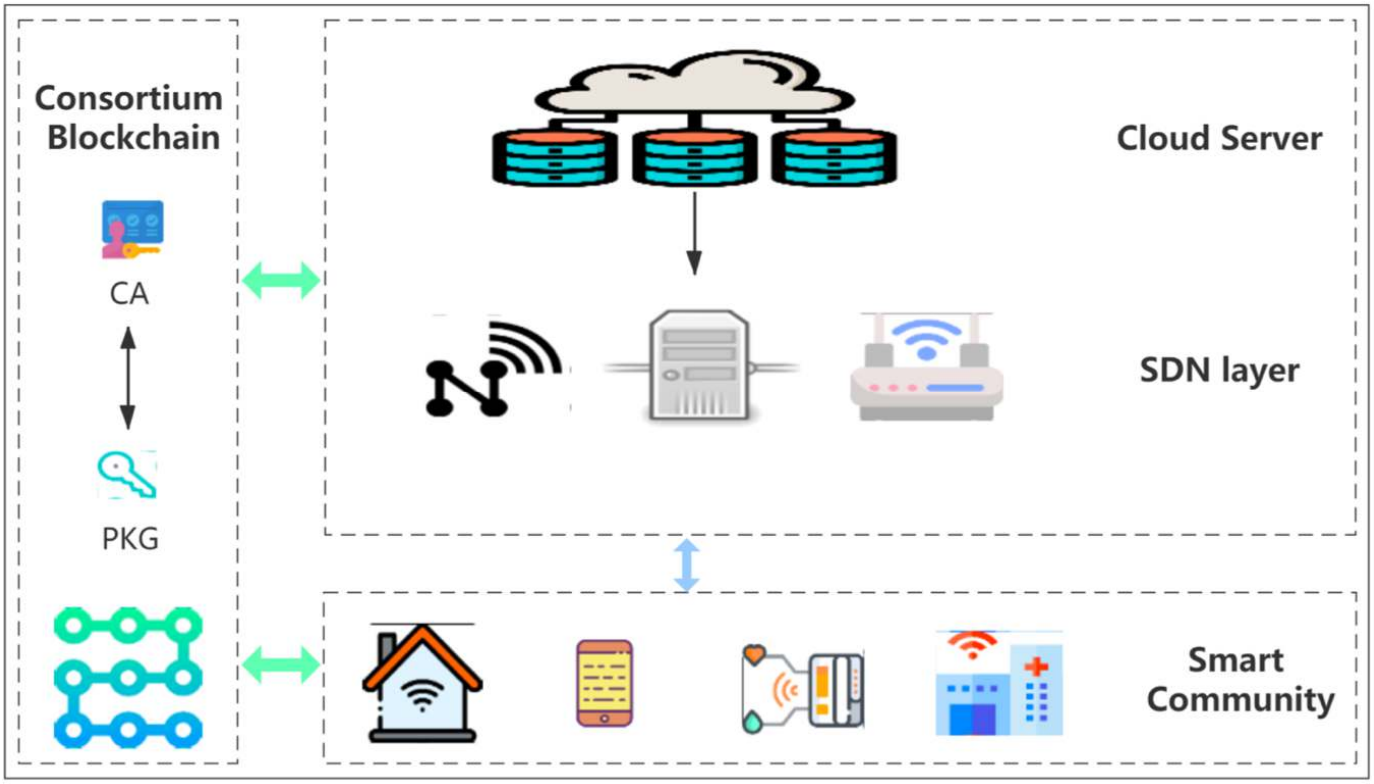
روش پیشنهادی

- PRE یک شیوه رمزنگاری ابتدایی کلید عمومی است که در آن یک مالک داده می‌تواند توانایی رمزگشایی داده‌های خود را به درخواست‌کنندگان دیگر داده، واگذار کند.
- پس از این‌که یک پروکسی نیمه مطمئن، متن رمز را که در کلید عمومی مالک است مجددا رمزگذاری می‌کند، یک درخواست کننده داده می‌تواند متن رمز جدید را از طریق کلید مخفی خود رمزگشایی کند.
- روش IBPRE نوعی از PRE است که دارندگان داده و درخواست‌کنندگان هویت خود را به عنوان کلید عمومی می گیرند و دیگر به زیرساخت کلید عمومی نیازی ندارند.

روش پیشنهادی

- در این مقاله به سه دلیل الگوریتم IBPRE انتخاب شده است:
  - طرح IBPRE به طور موثر امنیت و حریم خصوصی اشتراک داده‌ها را بین هر دو موجودیت در شبکه ناهمگن و غیرقابل اعتماد، تضمین می‌کند. بنابراین، این طرح برای به اشتراک‌گذاری داده‌ها بین دستگاه‌ها در جوامع هوشمند مجهز به شبکه نرم‌افزارمحور، مناسب است.
  - تجهیزات داده‌های خود را توسط IBPRE رمزگذاری کرده و در سرورهای ابری ذخیره می‌کنند. آن‌ها نیازی به بارگیری داده‌های رمزگذاری شده در هنگام اشتراک با سایر دستگاه‌ها ندارند، که این امر روند به اشتراک‌گذاری داده‌ها را در مقایسه با سایر طرح‌ها ساده می‌کند.
  - IBPRE بهبود PRE است که از شر PKI خلاص می‌شود و مدیریت گواهینامه را در PRE تسهیل می‌کند.

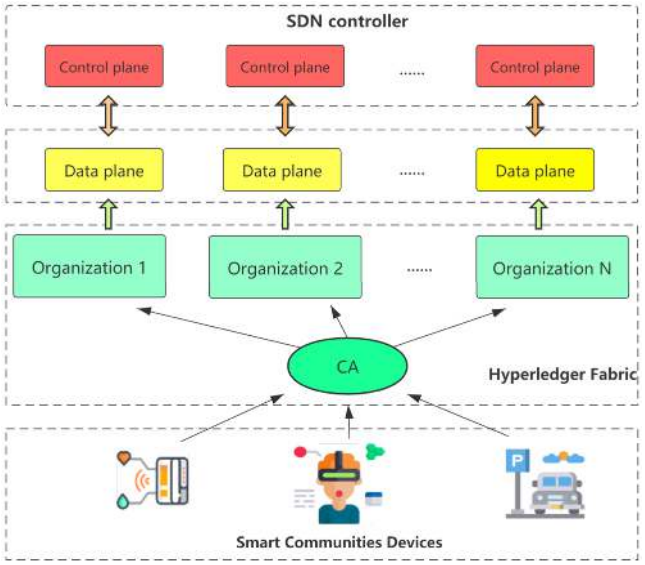
معماری
راه‌حل پیشنهادی



معماری
راه‌حل پیشنهادی

- این چارچوب از سه قسمت تشکیل شده است:
  - جوامع هوشمند
  - ابر با قابلیت شبکه نرم‌افزارمحور
    - سرور ابری شامل برخی از سرورهای مرکزی ارائه‌دهندگان خدمات ابری و اپراتورهای شبکه است که منابع محاسباتی و ذخیره‌سازی دستگاه‌های اینترنت اشیا را فراهم می‌کند.
  - شبکه زنجیره بلوکی
    - شبکه زنجیره بلوکی، کلید رمزگذاری در الگوریتم IBPRE را به طور ایمن مدیریت می‌کند.
    - به علاوه، زنجیره بلوکی کل فرآیند به اشتراک‌گذاری داده‌ها را بین دو دستگاه ضبط می‌کند. داده‌های موجود در زنجیره بلوکی شفاف و قابل کنترل و ردیابی هستند.

معماری
راه‌حل پیشنهادی

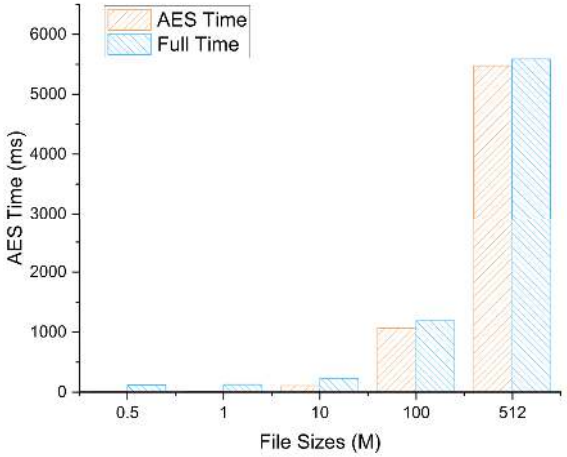


- شبکه نرم‌افزارمحور قدرت گرفته از زنجیره بلوکی در جوامع هوشمند
  - از Hyperledger Fabric، نوعی زنجیره بلوکی کنسرسیوم، به عنوان شبکه زنجیره بلوکی در نظر گرفته شده است.
  - همه دستگاه‌های جوامع هوشمند برای دریافت گواهینامه‌ها و کلیدهای خود در راستای بهبود احراز هویت و قابلیت اطمینان هنگام ورود به سیستم، باید در Fabric CA ثبت نام کنند.
  - با این کار بر مسئله حملات DoS به شبکه اینترنت اشیا غلبه خواهد شد.

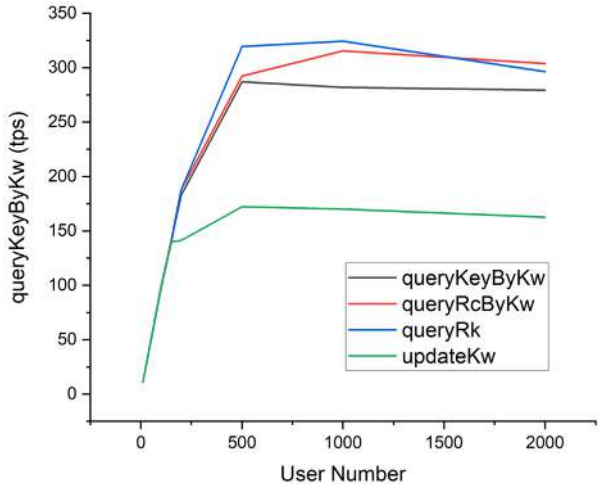
پیاده‌سازی راه‌حل پیشنهادی

- محیط تست
  - یک سرور ابری برای ذخیره سازی و کنترل سیستم: مشخصات سرور ابری CPU Intel Core i7-8700 و ۸ گیگابایت RAM، است.
  - بستر شبکه نرم‌افزار محور: از Mininet برای شبیه‌سازی شبکه و OpenDaylight به عنوان کنترل‌کننده استفاده می‌شود.
  - از Hyperledger Fabric نسخه ۱.۲.۰ استفاده می‌شود و چندین گره از جمله ۱ سفارش‌دهنده، ۴ همتا و ۲ CA برای دو سازمان در شبکه، نصب شده است.
  - طرح IBPRE با استفاده از کتابخانه JPBC پیاده می‌شود.
  - طول کلید خصوصی برای یک شناسه خاص و کلید AES برای رمزگذاری داده‌ها، ۱۲۸ بایت تنظیم شده است.

پیاده‌سازی
راه‌حل پیشنهادی



- نرخ برون‌داد رمزگذاری



- نرخ برون‌داد صدا زدن قرارداد هوشمند

نقاط قوت و ضعف

- نقاط قوت:
  - استفاده از زنجیره بلوکی در اعطای مجوز به تجهیزات اینترنت اشیا، ارتباطی پایدار و امن را در مقابل روش‌های سنتی ایجاد می‌کند.
  - الگوریتم IBPRE پیشنهادی این مقاله با سربار کم و به صورت قابل اعتماد، امنیت ارتباطات را تضمین می‌کند.
  - روش ایجاد کلید خصوصی در الگوریتم IBPRE با استفاده از زنجیره بلوکی و تعدادی تابع جهت پرس‌وجو پیاده‌سازی شده است که علاوه بر راحتی کار و کاهش پیچیدگی‌ها، باعث عدم نیاز به زیرساخت‌های سنگین کلید عمومی است.
  - راه‌کار پیشنهادی بدون نیاز به تغییرات در سطوح شبکه نرم‌افزارمحور، قابلیت سوار شدن بر شبکه‌های موجود را دارد.
- نقاط ضعف:
  - راه‌کار پیشنهادی به صورت جامع و کامل در چندین سناریو واقعی ارزیابی نشده است تا بار و شرایط احتمالی بررسی شود و میزان کارایی واقعی به دست آید.

پیشنهادات برای کارهای آتی

- تست و بررسی چارچوب پیشنهادی به صورت کامل و جامع در چندین سناریوی واقعی
- بررسی و ارزیابی مزایای استفاده از روش IBPRE در ساختارهای مختلف جوامع هوشمند
- ترکیب و جایگزینی روش محاسبات ابری این مقاله با روش‌های جدیدی محاسبات لبه

مرجع

- Y. Gao, Y. Chen, H. Lin and J. J. P. C. Rodrigues, "Blockchain based secure IoT data sharing framework for SDN-enabled smart communities," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 514-519

با تشکر از توجه شما

؟