بسمه‌تعالی

گزارش و تحلیل مقاله

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

تعریف مسئله و هدف اصلی مقاله

جوامع هوشمند، با تعامل و کنترل از راه دور دستگاه‌های اینترنت اشیا از طریق اینترنت، خدمات را برای ساکنان خانه‌های هوشمند، حمل و نقل هوشمند، مراقبت‌های بهداشتی و غیره، ارائه می‌دهند. در شبکه‌های ناهمگن اینترنت اشیا، دستگاه‌های اینترنت اشیا، حجم زیادی از داده‌های بلادرنگ را تولید و به دستگاه‌های دیگر برای به اشتراک گذاری داده‌ها یا ابرها برای محاسبه و ذخیره سازی، ارسال می‌کنند. رویکرد شبکه نرم‌افزارمحور در شبکه‌های اینترنت اشیا برای کاهش پیچیدگی شبکه و تأخیر ارتباطی استفاده می‌شود.

شبکه نرم‌افزارمحور، صفحه داده و صفحه کنترل را از طریق یک کنترل‌کننده شبکه نرم‌افزارمحور جدا می‌کند و قابلیت برنامه‌ریزی شبکه را برای کاربران فراهم می‌کند. با این وجود، 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. مهاجمان می‌توانند دستگاه‌های اینترنت اشیا را که به خطر افتاده و غیرمجاز هستند کنترل کنند تا به کنترل‌کننده شبکه نرم‌افزارمحور نفوذ کرده و منجر به نشت داده شوند.
- 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.

بنابراین، 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[1] استفاده شده است.

ادعا می‌شود که فناوری زنجیره بلوکی هم در دانشگاه و هم در صنعت بی اعتماد است. سوابق موجود در زنجیره بلوکی قابل پیگیری هستند و نمی‌توان آن‌ها را دستکاری کرد. زنجیره بلوکی کنسرسیوم یکی از سه نوع زنجیره بلوکی دارای مجوز صدور گواهینامه[2] برای اجازه اعضا در شبکه زنجیره بلوکی است. ادغام زنجیره بلوکی با شبکه نرم‌افزارمحور قادر به حل مشکلات شبکه نرم‌افزارمحور متمرکز است. بنابراین، در این مقاله از

[1] Proxy Re-Encryption

[2] Certificate Authority (CA)

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.

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[1] نوعی از PRE است که دارندگان داده و درخواست‌کنندگان هویت خود را به عنوان کلید عمومی می گیرند و دیگر به زیرساخت کلید عمومی[2] نیازی ندارند.

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.

روش IBPRE برای تایید اعتبار کاربران نیاز به سازنده کلید خصوصی[3] دارد که کلیدها را برای کاربران ساخته و نگهداری می‌کند. اگر اعضای کنجکاو یا مخرب به کنترل سازنده کلید خصوصی دسترسی پیدا کنند، توانایی دسترسی به داده‌های کاربران را خواهند داشت. جهت حل این مشکل، زنجیره بلوکی برای مدیریت کلیدهای رمزگذاری داده‌های دستگاه و ضبط دسترسی کلیدها برای درک مسئولیت‌پذیری و افزایش امنیت، استفاده می‌شود.

در تحقیقات پیشین استفاده از زنجیره بلوکی برای شبکه‌های نرم‌افزارمحور و PRE را بررسی می‌کنیم.

زنجیره بلوکی برای شبکه‌های نرم‌افزارمحور

جوامع هوشمند از کاربردهای مهم اینترنت اشیا است. با این حال، تحقیقات کمی در مورد استفاده از فناوری های زنجیره بلوکی و شبکه نرم‌افزارمحور در جوامع هوشمند متمرکز شده است.

- در یکی از تحقیقات پیشین، استفاده از شبکه نرم‌افزارمحور و زنجیره بلوکی برای اطمینان از امنیت و حریم خصوصی دستگاه‌های اینترنت اشیا در جوامع هوشمند مورد بررسی قرار گرفت. شبکه نرم‌افزارمحور برای ایجاد انزوا و محافظت در برابر حملات DoS مورد استفاده قرار گرفت، در حالی که

[1] Identity-based Proxy Re-Encryption (IBPRE)

[2] Public Key Infrastructure (PKI)

[3] Private Key Generator (PKG)

زنجیره بلوکی برای دستیابی به هماهنگی و توافق توزیع شده در جوامع هوشمند مورد استفاده قرار گرفت.

در بیشتر مطالعات سعی شده است از فناوری‌های زنجیره بلوکی و شبکه نرم‌افزارمحور برای شهر هوشمند یا کل محیط اینترنت اشیا استفاده شود.

- 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 این حال، این طراحی را در Ethereum، یک بستر عمومی زنجیره بلوکی که دارای عملکرد محدود و مسائل مربوط به مجوز برای دستگاه‌های اینترنت اشیا است، شبیه‌سازی کردند.
- در کارهای قبلی با استفاده از زنجیره بلوکی، شبکه نرم‌افزارمحور و فنآوری‌های محاسبات مه، یک چارچوب ابری برای اینترنت اشیا، پیشنهاد کردند. این زنجیره بلوکی برای ثبت پرداخت معاملات منابع ابری بین ارائه‌دهندگان خدمات و کاربران به کار گرفته شد. شبکه نرم‌افزارمحور فعال شده در گره‌های مه در شبکه لبه‌ای برای پردازش داده‌های دستگاه‌های اینترنت اشیا به صورت محلی تنظیم شده است. از آن‌جا که این چارچوب در زنجیره بلوکی عمومی پیاده سازی می شود، موضوعات مشابه معماری سابق قبلی را دارد.
- ترکیب شبکه نرم‌افزارمحور و زنجیره بلوکی، مدیریت ترافیک اینترنت اشیا را به صورت خودکار در شبکه های لبه ای اعمال می‌کند. از این رو، این طراحی می‌تواند قابلیت اطمینان و اعتبار دستگاه‌های اینترنت اشیا را بهبود بخشد. علاوه بر این، مقیاس‌پذیری و امنیت کل شبکه اینترنت اشیا قابل ارتقا است.

رمزگذاری مجدد پروکسی PRE

روش PRE اولین بار حدود دو دهه پیش ارائه شد. در ابتدا این روش در محرمانگی داده‌ها و کنترل دسترسی در رایانش ابری، محبوب شد.

- SDSM یک مکانیسم سرویس داده امن در محاسبات ابری موبایل است. این سازوکار از IBPRE استفاده می‌کند و به سرورهای ابری امکان مدیریت تفویض[1] داده برای کاربران را می‌دهد. این بدان معنی است که سرورهای ابری قادر به کنترل دسترسی به داده ها هستند و کاربران ابر اعتماد می‌کنند که در مورد داده‌های آن‌ها کنجکاو نیست.
- Nucypher یک پروژه فعال است که به عنوان یک سیستم مدیریت کلید[2] غیرمتمرکز، معرفی شده است. هدف این پروژه، حل مسئله سیستم مدیریت کلید قابل اعتماد و متمرکز در فضای ابری است. این روش کلیدهای رمزگذاری را مدیریت کرده و داده‌ها را بر اساس زنجیره بلوکی بین دو موجودیت به اشتراک می‌گذارد.

[1] Delegation

[2] Key Management System (KMS)

راه‌حل پیشنهادی مقاله برای مسئله

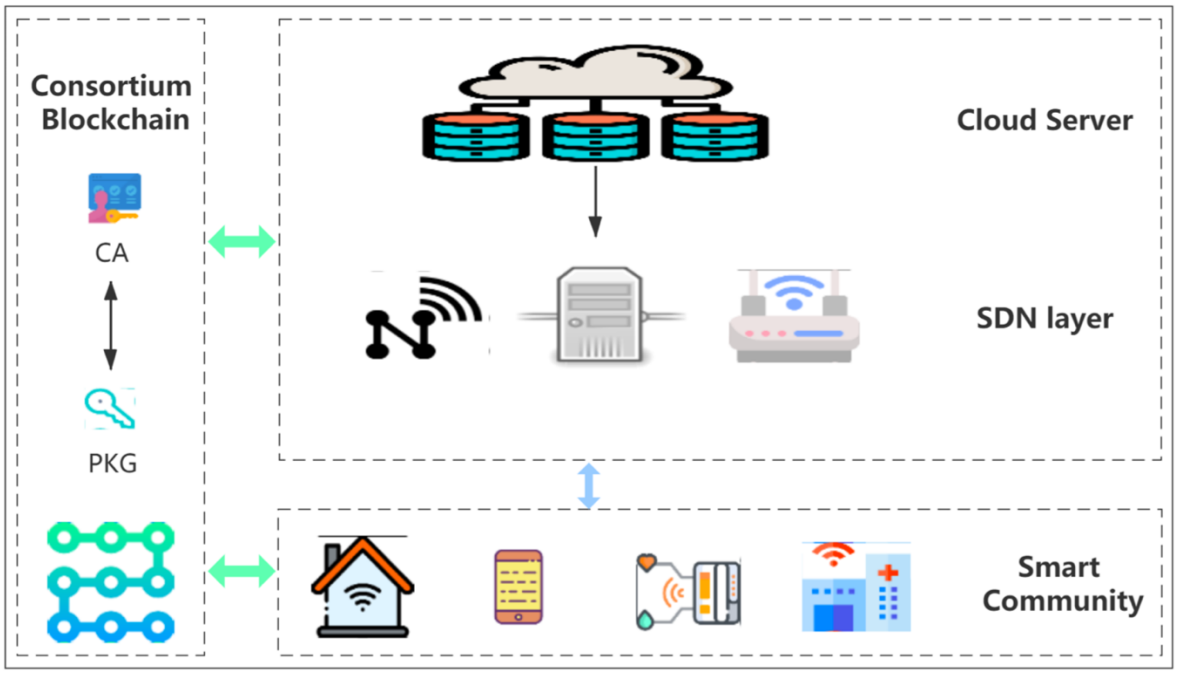
تصویر- ۱ چارچوب پیشنهادی اشتراک داده مبتنی بر زنجیره بلوکی را در جوامع هوشمند مجهز به شبکه نرم‌افزارمحور نشان می‌دهد. این چارچوب از سه قسمت تشکیل شده است:

- جوامع هوشمند
- ابر با قابلیت شبکه نرم‌افزارمحور
- شبکه زنجیره بلوکی

در لایه پایین این چارچوب، جوامع هوشمند مثل خانه‌های هوشمند، تلفن‌های هوشمند، دستگاه‌های پوشیدنی، سنسورها و مراقبت‌های بهداشتی هوشمند، قرار دارد.

ابر دارای قابلیت شبکه نرم‌افزارمحور از سرور ابر و لایه شبکه نرم‌افزارمحور تشکیل شده است. 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. لایه شبکه نرم‌افزارمحور با کنترل‌کننده شبکه نرم‌افزارمحور فعال شده و یک شبکه قابل برنامه‌ریزی با برخی پروتکل ها مانند OpenFlow، ارائه می‌دهد.

شبکه زنجیره بلوکی یک الگوریتم IBPRE را با خود ادغام می‌کند تا امنیت و حریم خصوصی داده‌های دستگاه‌های کاربر را تضمین کند. به جز دو دستگاه، هیچ شخص ثالث دیگری نمی‌تواند اطلاعات مفیدی را از داده‌های رمزگذاری شده به‌دست آورد. 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.



تصویر- ۱

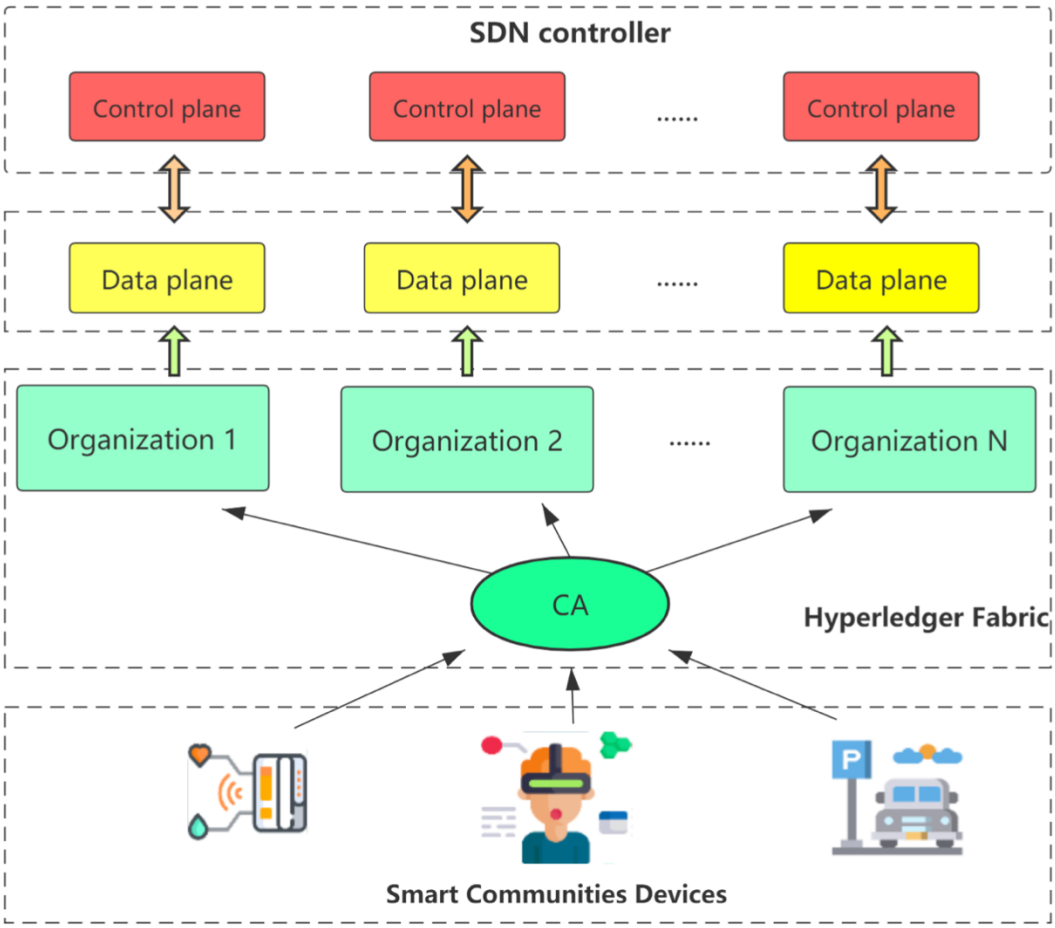
شبکه نرم‌افزارمحور قدرت گرفته از زنجیره بلوکی در جوامع هوشمند

معرفی مفهوم زنجیره بلوکی از مقاله‌ای در سال ۲۰۰۸ آغاز شد. به عنوان یک دفتر توزیع شده، تمام رویدادهایی که در زنجیره بلوکی اتفاق می‌افتد ثبت می‌شود و توسط شرکت‌کنندگان قابل خواندن است. داده های موجود در زنجیره بلوکی به دلیل سازگاری توزیع شده و سازوکارهای اجماع خاص، نمی‌توانند دستکاری شوند. به همین دلیل، فناوری زنجیره بلوکی می‌تواند امنیت یکپارچگی داده‌ها، قابلیت ردیابی و پاسخ‌گویی را فراهم کند.

زنجیره بلوکی به طور معمول سه نوع دارد:

- زنجیره بلوکی عمومی: به همه مردم دنیا امکان دسترسی و تعامل با آن را می‌دهد.
- زنجیره بلوکی کنسرسیوم: در انجمن‌هایی استفاده می‌شود که از چندین شرکت یا سازمان تشکیل شده‌اند و یک مرجع صدور گواهینامه برای تایید هویت شرکت‌کنندگان و اعطای کنترل دسترسی برای آن‌ها وجود دارد.
- زنجیره بلوکی خصوصی: توسط یک شرکت یا تیم داخلی پذیرفته می‌شود.

در چارچوب پیشنهادی این مقاله، Hyperledger Fabric، نوعی زنجیره بلوکی کنسرسیوم، به عنوان شبکه زنجیره بلوکی در نظر گرفته شده است.



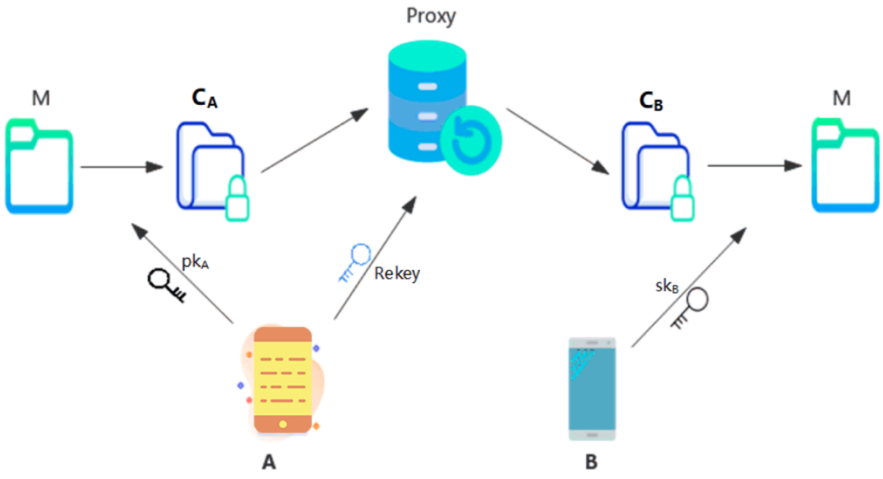
تصویر- ۲

در تصویر- ۲ روند ثبت و تایید دستگاه اینترنت اشیا در Fabric CA برای بهبود امنیت شبکه نرم‌افزارمحور به نمایش درآمده است. در جوامع هوشمند، تکنیک شبکه نرم‌افزارمحور، دستگاه‌های کلان اینترنت اشیا را کنترل می‌کند و خدمات هدایت جریان را ارائه می‌دهد. با این وجود، کنترل‌کننده شبکه نرم‌افزارمحور در برابر حمله واحد مانند DoS یا DDoS از دستگاه‌های کلان در جوامع هوشمند، آسیب‌پذیر است. در این مقاله، زنجیره بلوکی تمام دستگاه‌ها را از طریق مرجع صدور گواهی، مجاز می‌کند. 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. به علاوه، زنجیره بلوکی روند به اشتراک‌گذاری داده‌ها بین دو دستگاه اینترنت اشیا را کنترل و ضبط می‌کند. علاوه بر این، هر زمان دستگاهی می‌خواهد با یک قرارداد هوشمند در زنجیره بلوکی تماس برقرار کند، مرجع صدور گواهی، عضویت آن دستگاه را بررسی می‌کند. برخی از قراردادهای طراحی شده این طرح، گواهینامه‌های تماس گیرنده را بررسی می‌کنند که آیا هویت تماس‌گیرنده با پارامترهای قرارداد مطابقت دارد یا خیر.

اشتراک امن داده در جوامع هوشمند قدرت گرفته از زنجیره بلوکی و PRE

روش PRE و IBPRE

PRE اولین بار در سال ۱۹۹۸ توسط Blaze، Bleumer و Strauss پیشنهاد شد. پس از رمزگذاری مجدد متن فرستنده تحت کلید عمومی فرستنده با کلید رمزگذاری مجدد، گیرنده می‌تواند متن رمز جدید را مستقیماً با کلید خصوصی خود رمزگشایی کند. در این فرآیند، پروکسی نمی‌تواند چیزی از متن رمز و کلید رمزگذاری مجدد، یاد بگیرد.



تصویر- ۳

روند کلی PRE بین دو دستگاه تلفن همراه در تصویر- ۳ نشان داده شده است. دستگاه A را به عنوان فرستنده که مالک داده است و دستگاه B را به عنوان درخواست کننده داده فرض می‌کنیم:

- دستگاه A، داده خود M را با کلید عمومی خود pk_A رمز کرده و متن C_A به دست می‌آید.

- زمانی‌که دستگاه A می‌خواهد M را با B به اشتراک گذارد، کلید رمزگذاری مجدد Rekey را با استفاده از کلید خصوص خود sk_A و کلید عمومی B یعنی pk_B می‌سازد.
- A متن C_A و Rekey را به پروکسی که می‌تواند یک سرور لبه باشد، ارسال می‌کند.
- پروکسی C_A را با Rekey رمزگذاری مجدد کرده و حاصل که C_B است را به B ارسال می‌کند.
- B با استفاده از کلید خصوصی خود sk_B متن CB را بازگشایی می‌کند و M را به دست می‌آورد.

در طرح IBPRE، دستگاه A و دستگاه B می‌توانند هویت خود را به عنوان کلید عمومی خود برای رمزگذاری داده‌ها در نظر بگیرند. هویت‌ها می‌توانند شناسه دستگاه، شماره سریال از سازنده دستگاه یا هویت از زنجیره بلوکی هنگام ثبت دستگاه ها در زنجیره بلوکی باشند. در IBPRE، برای احراز هویت کاربران، تولید کلیدهای خصوصی برای کاربران و نگهداری کلیدها، به سازنده کلید خصوصی، نیاز است.

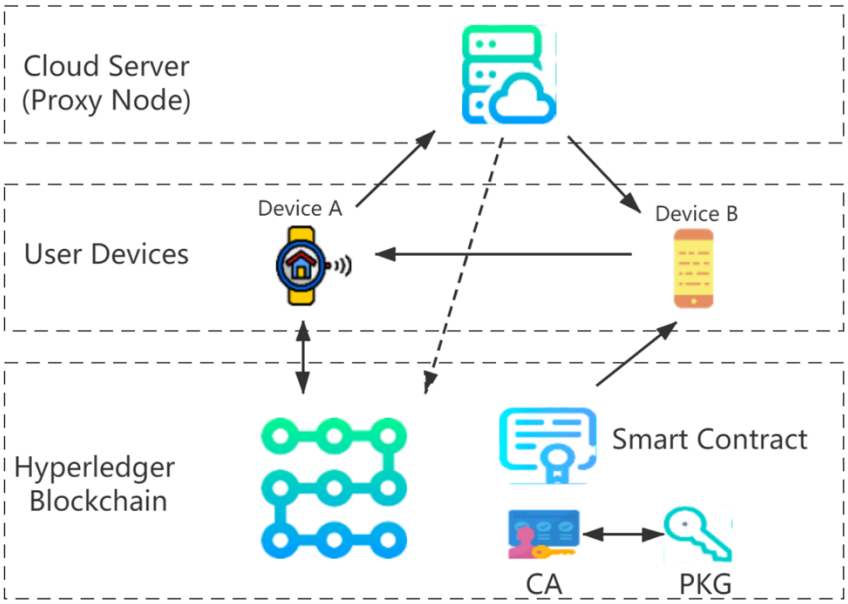
در این چارچوب الگوریتم IBPRE و زنجیره بلوکی Fabric ترکیب شده است:

- IBPRE برای اشتراک امن کلیدهای داده بین دو موجودیت در یک شبکه پیچیده و ناهمگن اینترنت اشیا استفاده می‌شود.
- از Fabric برای ذخیره کلیدهای داده و ثبت تمام وقایع در طول روند اشتراک، استفاده می‌شود.
- PKG در IBPRE از طریق Fabric CA مدیریت می‌شود. در این سیستم، PKG سرویسی است که توسط CA کنترل می‌شود و فقط برای کاربران کلید تولید می‌کند.
- Fabric CA برای تایید اعتبار کاربران، ارسال درخواست به PKG و دریافت پاسخ از PKG استفاده می‌شود.

زنجیره بلوکی و IBPRE برای طرح امن اشتراک اطلاعات

چهار موجودیت در چارچوب اشتراک اطلاعات این مقاله وجود دارد (تصویر- ۴):

- مالک داده: کسی که داده را جهت ذخیره یا اشتراک، نگهداری می‌کند که در سناریوی جوامع هوشمند، می‌تواند دستگاه‌های اینترنت اشیا باشد مانند دستگاه A در تصویر- ۴.
- درخواست‌کننده داده: کسی که داده‌ی مالک داده را مورد درخواست قرار می‌دهد که می‌تواند دیگر دستگاه‌های اینترنت اشیا باشد.
- سرور ابری: وظیفه ذخیره داده‌های رمزشده و اجرای الگوریتم رمزگذاری مجدد برای دستگاه‌ها را برعهده دارد.
- زنجیره بلوکی Hyperledger: این زنجیره بر اساس نیاز، متناسب‌سازی شده است و دارای چند عملکرد پایه‌ای در این چارچوب است:
  - ذخیره کلیدهای رمزگذاری و سایر اطلاعات حیاتی دستگاه‌ها برای دستیابی به امنیت
  - نگهداری سوابق در فرآیند به اشتراک‌گذاری برای حسابرسی داده و منشا آن
  - احراز هویت دستگاه‌ها و اعطای کنترل دسترسی داده‌ها در زنجیره بلوکی به آن‌ها از طریق Fabric CA



تصویر- ۴

در تصویر- ۵، به مخففهای استفاده شده، اشاره شده است.

Notation	Description
ID_A, Sk_A	Data owner's public key and private key
ID_B, Sk_B	Data requestor's public key and private key
F	Data for storing or sharing
F_k	Symmetric key for data encryption
F_{hash}	Data hash
F_{kw}	Data keywords
CT_f	Encrypted Data
CT_{fk}	Encrypted symmetric key
$Rekey_{A \to B}$	Re-encryption key from owner to a requestor
CT_{rfk}	Re-encrypted CT_{fk}

تصویر- ۵

همان‌طور که در مثال هم گفته شده، ۷ فاز در این سیستم وجود دارد:

- Setup
- UserRegistration
- Encrypt: شامل FileEncrypt، KeyEncrypt و InfoUpload
- ReKeyGen
- ReEncrypt
- FirstDecrypt
- SecondDecrypt

طراحی قرارداد هوشمند برای اشتراک امن داده‌ها در جوامع هوشمند مجهز به شبکه نرم‌افزارمحور

چهار سیستم قرارداد هوشمند، برای این مقاله طراحی شده است:

- queryKeyByKw(ownerId,keywords): این تابع مقادیر CT_{fk} و F_{hash} را برای ownerID برمی‌گرداند.
- queryRekey(ownerId, requestorId): این تابع یک کلید برای رمزگذاری مجدد از مالک داده به درخواست‌کننده داده، برمی‌گرداند.
- queryRCT ByKw(requestorId, keywords): این تابع مقادیر CT_{rfk} و F_{hash} را برای یک requestorID خاص برمی‌گرداند.
- updateKw(id, keywords, newKeywords): این تابع کلمات کلیدی قدیمی را با کلمات جدید، جایگزین می‌کند.

پیاده‌سازی راه‌حل پیشنهادی

در این بخش، نتایج تعدادی آزمایش را در مورد طرح IBPRE و قراردادهای هوشمند طراحی شده این مقاله در زنجیره بلوکی، بررسی می‌کنیم.

این سیستم شامل دو محیط است:

- 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.

در شبکه زنجیره بلوکی ، 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 می‌شود. برای ثبت مجدد دستگاه و ثبت نام در Fabric CA و تماس با قراردادهای هوشمند، یک SDK Fabric به زبان جاوا انتخاب می‌شود.

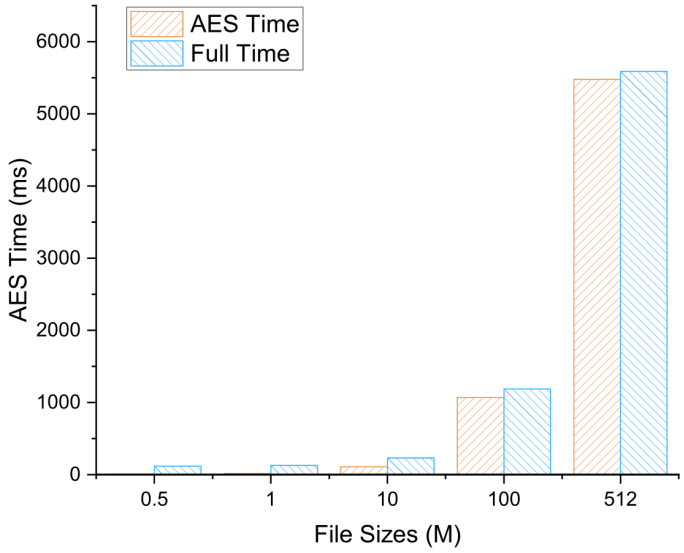
طرح IBPRE با استفاده از کتابخانه JPBC[1] پیاده می‌شود. طول کلید خصوصی برای یک شناسه خاص و کلید AES برای رمزگذاری داده‌ها، ۱۲۸ بایت تنظیم شده است.

نرخ برون‌داد رمزگذاری

این آزمایش به بررسی رمزگذاری فایل‌ها در اندازه‌های مختلف و بارگذاری کلیدهای رمزنگاری در زنجیره بلوکی، می‌پردازد. اندازه فایل از ۵۱۲ کیلوبایت تا ۵۱۲ مگابایت تنظیم شده در حالی که اندازه کلید روی ۱۲۸ بایت، تنظیم شده است. در تصویر- ۶ میزان زمان رمزگذاری AES و زمان کامل به همراه رمزگذاری IBPRE و ضبط کلیدها در Fabric، نشان داده شده است. در حالی که هزینه ضبط در Fabric به طور پیوسته حفظ می‌شود، هزینه رمزگذاری افزایش می‌یابد. زمان بارگذاری کلید رمزنگاری در زنجیره بلوکی در اندازه‌های

[1] Java Paring-Based Cryptography Library

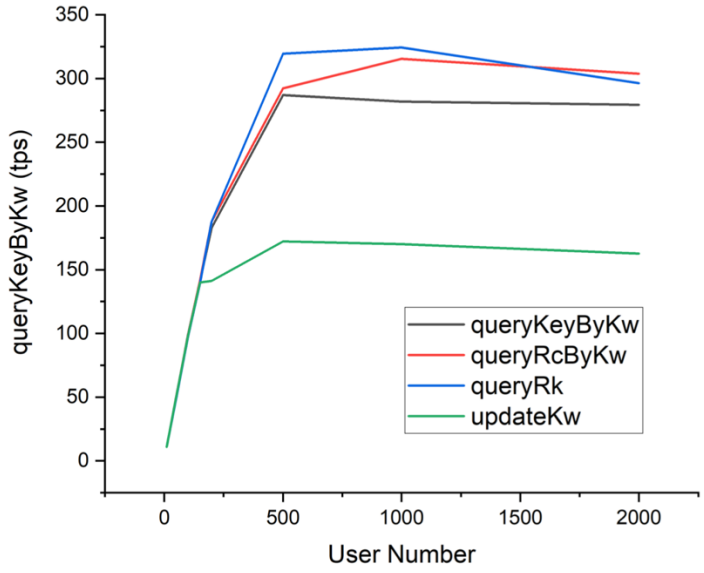
مختلف کلید، از ۶۴ بایت تا ۵۱۲ بایت، آزمایش شد. نتیجه نشان می‌دهد که در هر حال برای اضافه کردن کلیدها در زنجیره بلوکی حدود ۱۱۰ میلی ثانیه هزینه می‌شود.



تصویر- ۶

نرخ برون‌داد صدا زدن قرارداد هوشمند

چهار قرارداد هوشمند برای کارهای خاص در زنجیره بلوکی طراحی شد. از آن‌جا که قراردادهای هوشمند می‌توانند توسط تمام اعضای معتبر در Fabric اجرا شوند، آزمایشی از عملکرد اجرای قراردادها در تصویر- ۷ نشان داده شده است. نمودار حاکی از انواع صدا زدن قراردادهای مختلف در دستگاه‌های مختلف کاربر به صورت همزمان است. با افزایش تعداد درخواست‌های همزمان، در ابتدا توان عملیاتی به سرعت افزایش می‌یابد اما هنگامی که این عدد به حدود ۵۰۰ می‌رسد، به نظر می‌رسد tps سه قرارداد پرس‌وجو به نقطه اشباع حدود ۳۰۰ رسیده و قرارداد بروزرسانی تقریبا به ۱۶۰ tps می‌رسد.



تصویر- ۷

نقاط قوت و ضعف مقاله

نقاط قوت این مقاله:

- 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 این مقاله:

- 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.

جمع‌بندی و پیشنهادات برای کارهای آتی

در این مقاله یک مدل اشتراک داده ایمن برای جوامع هوشمند دارای شبکه نرم‌افزارمحور با استفاده از زنجیره بلوکی و IBPRE معرفی شده است. شبکه نرم‌افزارمحور برای انتقال جریان به صورت محلی پیاده‌سازی می‌شود. داده‌های رمزگذاری‌شده دستگاه‌ها به یک سرور ابری برون سپاری می‌شوند و IBPRE برای به اشتراک‌گذاری ایمن کلیدهای فایل رمزنگاری بین دارندگان داده و دیگران، برگزیده می‌شود. کاربران می‌توانند کلیدهای رمزنگاری شده را در زنجیره بلوکی بارگذاری کرده و با زنجیره بلوکی ارتباطی مانند جستجو و به‌روزرسانی سوابق موجود در آن توسط قراردادهای هوشمند طراحی شده، داشته باشند. نتایج آزمایشات نشان می‌دهد که پیشنهاد این مقاله دارای عملکرد خوب و توان عملیاتی بالا است.

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

- 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

مشخصات دقیق مقاله

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