RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks

طرح بررسی یکپارچگی داده از راه دور مبتنی بر بلاکچین برای اینترنت اشیا در شبکه های G۵

Huaqun Wang

Parallel Distrib. Comput

2021

سوال اصلی مطرح شده در مقاله

- یکی از اصلی ترین کاربرد شبکه های همراه نسل ۵ ،اینترنت اشیا (IoT) است.
- دستگاه های ترمینال اینترنت اشیا داده های بزرگی ایجاد می کنند.
- دستگاه های متصل به اینترنت اشیا باید سبک بوده و از نگهداری حجم زیادی از داده اجتناب کنند
- با توجه به اینکه فضای ابری از کنترل کاربر خارج است، قابلیت اطمینان و امنیت داده از اهمیت بالایی برخوردار است
- یکپارچگی داده های جمع آوری شده از راه دور از اهمیت بالایی برخوردار است

در این طرح یک روش یکپارچگی داده از راه دور مبتنی بر بلاکچین برای داده های بزرگ ارائه شده است.

چالش مسئله

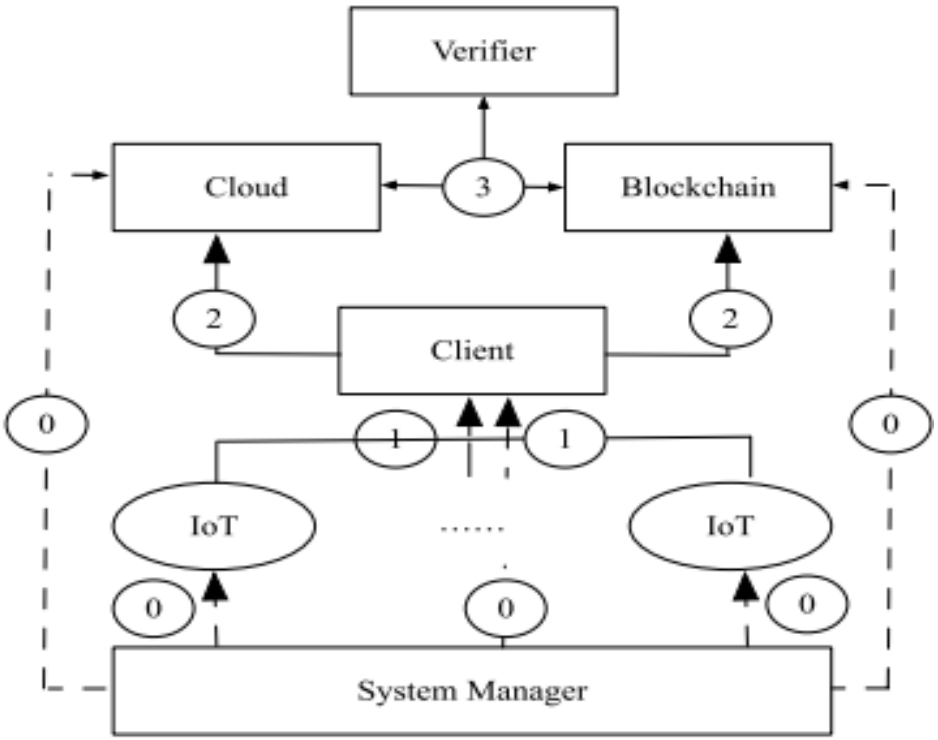
- اینترنت اشیا را می توان در زمینه های تجاری و امنیت هوشمند استفاده کرد
- در زمان جمع آوری اطلاعات فرآهم شده در این بسترها ، چالش اصلی یکپارچگی و امنیت و احراز هویت ارسال کننده داده می باشد.

ضرورت حل مسئله

بلاکچین به عنوان یک دفتر توزیع شده دارای ویژگی های تمرکززدایی ، عدم دستکاری ، فضای ذخیره سازی توزیع شده می باشد.

- برای اولین بار فناوری بلاک چین در رمز ارزها به کار برده شده است
- هر بلاک شامل یک عدد است که با محاسبه این عدد به یک hash واحد در بلوک ها می رسیم
- بلوک های متصل به شبکه با محاسبه این hash به صورت زنجیره وار با یکدیگر ارتباط دارند
- از این روش می توان در احراز هویت و صحت سنجی اطلاعات شبکه اینترنت اشیا استفاده کرد

روش ارائه شده در مقاله



راه حل پیشنهادی برای حل مسئله

- مرحله اول : مدیر سیستم پارامترهای محاسبات را مقداردهی می کند و در همین زمان اطلاعات توسط اینترنت اشیا تولید شده می شود.
- مرحله دوم: دستگاه های اینترنت اشیا داده های خود را برای ایستگاه های کاری ارسال می کنند.
- مرحله سوم: در این مرحله ایستگاه های کاری داده ها را دسته بندی و پردازش می کنند و جهت ارسال به فضای ابری با استفاده از زنجیره بلوک ها آماده می کنند.
- مرحله چهارم : در این مرحله با استفاده از محاسبات انجام شده از طریق زنجیره بلوک صحت یکپارچگی داده ها در این مرحله بررسی و تایید می شود.

نقاط قوت و ضعف مقاله

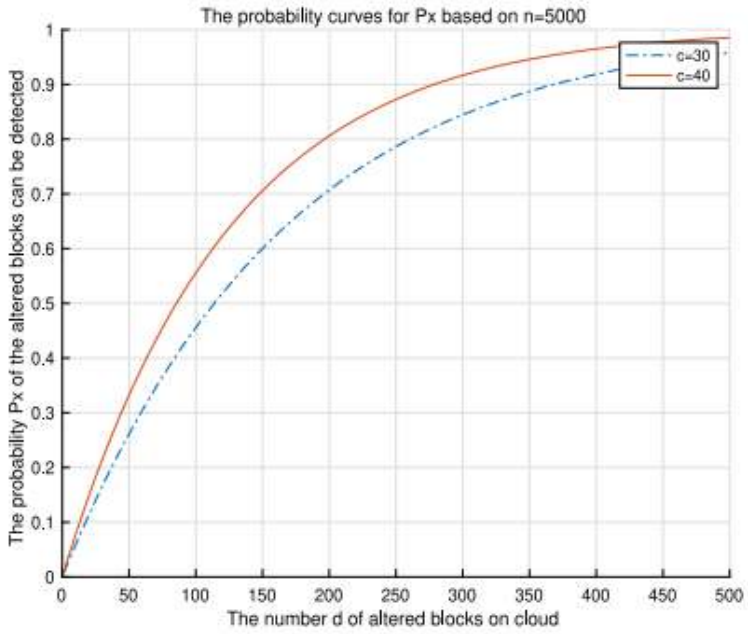
مزایای این طرح :

- کارامد کردن روش های یکپارچگی داده بین کاربر و فضای ابری
- یک مدل ساخت یافته برای امنیت اطلاعات
- استفاده از روش های رمز نگاری قوی مثل rsa256
- هزینه ارتباطی بهینه نسب به روش های مشابه

نقاط ضعف :

- طرح پیشنهادی هم باید سمت کلاینت و هم فضای ابری پیاده سازی شود که در این صورت یکپارچگی شبکه تحت تاثیر قرار گرفته و کلیه عناصر متصل به شبکه باید از این روش استفاده کنند.
- هزینه محاسباتی بالا به خصوص در مواقعی که در آخرین مرحله صحت سنجی یکپارچگی داده ، خطا در صحت اطلاعات تشخیص داده شود ، ارسال و کلیه محاسبات باید مجدد از اول بررسی شود که این مورد باعث سربار هزینه با استفاده از این روش پیشنهادی است.

نتایج شبیه سازی



شکل ۳منحنی احتمال PX برای کشف خرابی داده

نتایج شبیه سازی

Table 2
Computation cost of the parties (F = 1T bit, c = 50).

Size of l	*Cloud*	*Blockchain*	*Client*	*Verifier*
32 768(2^{15})	0.6702 s	0.0835 s	137.5732 s	0.6201 s
65 536(2^{17})	2.3254 s	0.3145 s	113.3259 s	2.1372 s
524 288(2^{19})	8.1773 s	1.023 s	100.7351 s	6.7715 s

شکل ۴ محاسبه هزینه پردازش داده ها با این روش